MEDITOLOGY SERVICES

Addressing Compliance in Healthcare

How healthcare organizations can address IT security and compliance requirements with Trend Micro security solutions

September 10, 2018

Prepared for

TREND MICRO™

Introduction

This report delivers a path for identifying and protecting the vast healthcare ecosystem from the plethora of cyber threats and challenges as we venture further into uncharted cyberspace. We will survey the landscape of healthcare security regulations and enforcement alongside emerging technologies, escalating attacks and breaches of patient information and systems. We will discuss innovations in information security risk management, security automation, and leading practices for prioritizing limited resources to protect and defend critical healthcare assets and delivery systems. To aid in ensuring fast, effective, and comprehensive protection against advanced threats and cybercriminals, consider Trend Micro's leading security offerings so more time and energy is spent on patient care, and less on ever-present security risks. This reports maps Trend Micro's solutions for protecting hybrid cloud workloads, users, and networks to HIPAA, NIST, HITRUST, PCI-DSS and GDPR regulations.

State of Security in Healthcare

The healthcare industry faces significant challenges —with Office of Civil Rights (OCR) fines and settlements, never-ending regulations, and the rise of security breaches all maligning against companies and individuals. In conjunction with these difficulties, there's simply never enough money in the budget to hire new & specialized personnel to limit these risks and address important infrastructure gaps, nor is there ample time or budget space to purchase or develop a new tool to automate important security processes and save valuable time. Between the years 2011 to 2016 alone, there was an overall increase of (OCR) settlements by 333% and fines levied against companies outside of compliance regulation standards were increased by 281%.[1]

Emerging Regulations and Industry Trends

Let's face it, everything we touch nowadays has the ability to connect to the internet one way or another, and despite the threat that presents, the same can be said when we enter a healthcare space. With Internet of Things(IoT), Industrial Internet of Things (IIoT), and Medical Device Inventory Management (MDiM) devices capable of artificial intelligence and data analytics, we need a way to effectively manage these devices, ourselves, and our organizations within one powerful centrally located management system.

The largest of 2018's emerging trends include;

- 3rd Party Risk Management (3PRM) Programs
- Achievement of a certification or adherence to a security framework such as National Institute of Standards and Technology (NIST) or the Health Information Trust Alliance (HITRUST)
- Outsourcing of security functions to expert managed security firms, security automation, and privileged access controls.

With options like these, organizations can gather a better understand of who they are dealing with, where their data lives, and address their capacity to automate tasks and expand their capabilities.

[1] Office of Civil Rights, U.S. Department of Health & Human Services Website. "Resolution Agreements and Civil Money Penalties", June 2017. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/complianceenforcement/agreements/index.html

Breaches on the Rise

It’s no secret 2017 was a very bad year for multiple organizations due to malware attacks, and this will only get worse in the years to come. The broad spectrum of cyber-attacks is frequently misinterpreted to assume a majority of breaches are caused via malware or other aggressive malicious activity—in fact these are comparatively rare next to insider misuse and other variations of information theft, which are responsible for the majority of breach activity. Incidents of both insider misuse and information theft, which represent a broad spectrum of activities, are projected to double in 2018 due to an overall lack of awareness and security controls within most healthcare organizations. We should be focusing on reducing relevant risks and the implementation of easily maintained compliance controls rather than facing fines, breaches, and possible loss of Public Health information (PHI) data—such breaches have lost 176,709,305 million patient records since 2009[2], at an increasing cost of $380 per record[3] Beyond this, the overall cost of a breach has increased year to year at a rate of 2.5 times more than any other industry, a fact consistently on the rise for the past seven (7) years. [4]

Risk Management Security Skills

In addition to the rising threat of breaches, a consistent lack of budget, and increased penalties or fines from compliance regulators, the IT security industry as a whole continues to face issues recruiting and keeping qualified talent—in large part due to financial restrictions in an overly competitive market. The Cybersecurity staffing gap continues to grow year over year: in 2014 we faced a substantial gap of 23%, yet now in 2018 there is a 51% gap[5]. This information points to the reality that far too many organizations are unable to meet their internal staffing needs and thus leave them vulnerable—these shortages dangerously increase risk from personnel workload, noncompliant behavior, and the resulting potential for exploitation. It also identifies an opportunity for security companies to explore the offering of specialized services around security management to the market.

Addressing Compliance

In 2017, the OCR conducted their own state of the Healthcare Industry compliance evaluation to establish a proper baseline for the healthcare industry and how compliance practices are adapting to new and emerging threats in the market.

[2] HIPAA Journal, “Healthcare Data Breach Statistics”, 2018. Retrieved From: https://www.hipaajournal.com/healthcare-data-breach-statistics

[3] Elizabeth Snell, Health IT Security, “How much do healthcare data breaches cost organizations?”, Feb. 5, 2018. Retrieved From: https://healthitsecurity.com/news/how-much-do-healthcare-data-breaches-cost-organizations.

[4] Elizabeth Snell, Health IT Security, “Healthcare Data Breach Costs Highest For 7th Straight Year”, June 20, 2017, Retrieved from: https://healthitsecurity.com/news/healthcare-data-breach-costs-highest-for-7th-straight-year

[5] Jon Oltsik, CSO,” Research suggests cybersecurity skills shortage is getting worse” Jan. 11, 2018. Retrieved From: https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html

Prior to this evaluation, it was determined that over 73% of all audited organizations scored below average on the OCR Risk Management Ratings. Moreover, only 12% of all organizations scored above medium score range. Regrettably, not a single organization of the 157 evaluated in total were able to achieve the highest possible score.

Most organizations were deemed insufficiently capable of maintaining the majority of security and compliance regulations and requirements. In particular, responding to and granting patients' the right to access their PHI requests, including designated third-party access, was the worst scored area of regulation evaluation. The OCR's 2017 audit report revealed that many organizations, policies and implementation procedures did not sufficiently address breach notifications, risk analysis, or risk management issues and concerns.

Trend Micro Security Solutions for the Healthcare Industry

The threats facing the healthcare industry and the organizations therein are numerous and constantly evolving, and when combined with staffing shortages, financial constraints, and mounting regulatory pressure, amount to a set of major challenges. Trend Micro, a security market leader with 30 years of experience, offers multiple flexible solutions designed to address current & emerging threats, streamline operations, and deal with increasingly complex compliance requirements. With Trend Micro's solutions powered by their XGen security strategy, healthcare organizations are able to identify and monitor risks across user, network, and hybrid cloud environments, reducing threats in real-time while providing central visibility and the ability to investigate newly discovered issues. With threat information automatically shared across security tools and environments, Trend Micro helps to more effectively manage an organization's at-risk assets and mitigate threats, reduce the strain on existing staff, and more easily address industry regulations and standards including HIPAA, NIST, PCI-DSS, HITRUST and the General Data Protection Regulation (GDPR). Trend Micro offers a wide range of solutions to assist with compliance against various regulations and standards. These solutions address many requirements of industry accepted frameworks that have been mapped to regulations and standards. Please see the table at the end of this document, where Trend Micro's capabilities have been mapped to important healthcare frameworks & regulations HITECH, as well as other important global regulations.

Securing Hybrid Cloud Security Workloads

Trend Micro's Hybrid Cloud Security solution, powered by Trend Micro Deep Security, provides adaptive protection for systems and applications across physical, virtual, cloud and container workloads. With this comprehensive solution, healthcare organizations can control operating costs while improving performance with security optimized for VMware virtual environments, the cloud (AWS, Microsoft Azure), and Docker containers. With a single agent, the solution delivers:

- Malware Prevention (anti-malware, behavioral analysis, machine learning & web reputation),
- Network Security (Intrusion Prevention, Firewall, vulnerability analysis),
- System Security (application control, integrity monitoring, & log inspection).

To understand how the Hybrid Cloud Security Solution maps to HITRUST, HIPAA, and other regulations, click here

Protecting Users

Trend Micro's User Protection Solution offers smarter, portable security accessible where your users work and go. It is an interconnected security solution that shares intelligence across security layers, so you can consolidate your view of user activity across all threat vectors. It delivers:

- Better protection by integrating security management and analysis across multiple layers of protection needed to defend against advanced threats,
- Simple, enterprise-wide visibility with intuitive, customizable interfaces, configurable data displays, and reports to speed compliance and investigation, and
- Simplified, user-based management that allows healthcare organizations to manage multiple security layers on-site or in the cloud.

To simplify the purchasing process for healthcare organizations, Trend Micro delivers a comprehensive suite of products for protecting endpoints, either as software or as a service.

To understand how the User Protection Solution maps to HITRUST, HIPAA, and other regulations, click here

Defending Networks

The Trend Micro Network Defense Solution is a family of security products that enable healthcare organizations to rapidly detect, analyze, and respond to targeted attacks and advanced threats.

Trend Micro™ Deep Discovery™ is an advanced threat protection platform that enables healthcare customers to detect, analyze, and respond to stealthy, targeted attacks. It uses specialized detection engines, custom sandboxing and global threat intelligence from the Trend Micro™ Smart Protection Network™ to defend against attacks that are invisible to standard security products. Deep Discovery uniquely detects and identifies evasive threats in real time, then provides the in-depth analysis and relevant actionable intelligence that will protect organizations from attack.

TippingPoint is a proven wire-speed Next-Generation Intrusion Prevention System (NGIPS) that proactively detects and prevents vulnerabilities, network exploits, and delivers identity and application awareness to enable contextual visibility and enforcement. Integrated with Deep Discovery for network-wide breach detection, the solution identifies targeted attacks and advanced threats, including proactive threat prevention at the perimeter and inside the network.

To understand how the Network Defense Solution maps to HITRUST, HIPAA, and other regulations, click here

Find out more about Trend Micro security solutions at www.trendmicro.com

Hybrid Cloud Protection Solution

Standards Equivalency Report

September 2018

HITRUST CSF v9.1

EU General Data Protection Regulation (GDPR)

HIPAA Security Rule

HIPAA Breach Notification Rule

PCI Data Security Standard v3.2

National Institute of Standards & Technology (NIST)

Prepared By

MEDITOLOGY SERVICES

Hybrid Cloud Protection Solution

Standards Equivalency Report

PREFACE

This report maps Trend Micro’s Hybrid Cloud Security Solution to the HITRUST v9.1 standard, highlighting specific products in the solution and the level (in brackets) relevant under HITRUST v9.1. In addition, where relevant, specific areas under HIPAA, PCI DSS v3.2, GDPR, and multiple NIST frameworks are highlighted for applicability.

For more information on Trend Micro’s Hybrid Cloud Security Solution, please visit https://www.trendmicro.com/en_us/business/products/hybrid-cloud.html

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
01.c Privilege Management *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Deep Security (3) Smart Check (2) Server Protect for Storage (2) Control Manager (1)	**HIPAA Security Rule** **PCI DSS v3.2** NIST

HIPAA Security Rule

HIPAA § 164.308(a)(3)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI for all those permitted within the workforce and prevent those within the workforce who are not permitted to access ePHI.

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient’s role

HIPAA § 164.308(a)(4)(ii)(A): Implement isolating health care clearinghouse functions (required)

HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)

HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)

HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable)

HIPAA § 164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)

HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.

HIPAA § 164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

PCI Data Security Standard v3.2

7.1: Limit access to system components and cardholder data to only those individuals whose job requires such access

7.1.1: Define access needs for each role

7.1.2: Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities

7.1.3: Assign access based on individual personnel’s job classification and function.

7.1.4: Require documented approval by authorized parties specifying required privileges

7.2: Establish an access control system(s) for systems components that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed.

7.2.1: Access control system must include coverage of all system components

7.2.2: Access control system must include assignment of privileges to individuals based on job classification and function

7.2.3: Access control system must include default “deny-all” setting

A.1.1: Ensure that each entity only runs processes that have access to that entity’s cardholder data environment.

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
01.c Privilege Management *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Deep Security (3) Smart Check (2) Server Protect for Storage (2) Control Manager (1)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (2/2)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-4: Access permissions are managed, incorporate the principles of least privilege and separation of duties
NIST SP 800-53 R4 AC-3: Access enforcement

NIST SP 800-53 R4 AC-6: Least privilege

NIST SP 800-53 R4 AC-6(1): Authorize access to security functions

LEVEL TWO (Additional to One): NIST Cybersecurity Frameworks

R.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.DS-5: Protections against data leaks are implemented

PR.PT-4: Communications and control networks are protected
NIST SP 800-53 R4 AC-10: Concurrent session control

NIST SP 800-53 R4 AC-2: Account management

NIST SP 800-53 R4 AC-21: Information sharing

NIST SP 800-53 R4 AC-3(7): Role-based access control

NIST SP 800-53 R4 AC-6(2): Non-privileged access for nonsecurity functions.

LEVEL THREE (Additional to Two)

NIST Cybersecurity Frameworks

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
NIST SP 800-53 R4 AC-6(10): Prohibit non-privileged users from executing privileged functions.

NIST SP 800-53 R4 AC-6(5): Privileged accounts

NIST SP 800-53 R4 AC-6(9): Auditing use of privileged functions

NIST SP 800-53 R4 CM-7: Least functionality

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
01.l Remote Diagnostic and Configuration Port Protection *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (3)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.310(a)(2)(iii): Implement access control and validation procedures (addressable) HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media. HIPAA § 164.310(C): Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

National Institute of Standards & Technology (NIST) (2/2)

LEVEL ONE:

NIST Cybersecurity Frameworks
PR.AC-2: Physical access to assets is managed and protected
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
NIST SP 800-53 R4 PE-3(1): Information system access

LEVEL TWO (Additional to One)

NIST Cybersecurity Frameworks
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
NIST SP 800-53 R4 CM-7: Least functionality
NIST SP 800-53 R4 MA-4: Nonlocal maintenance
NIST SP 800-53 R4 MA-4(2): Document nonlocal maintenance
NIST SP 800-53 R4 MA-4(3): Comparable security/sanitization

LEVEL THREE (Additional to Two)

NIST Cybersecurity Frameworks
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.
ID.AM-2: Software platforms and applications within the organization are inventoried
ID.AM-3: Organizational communication and data flows are mapped
PR. IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
PR. IP-3: Configuration change control processes are in place
NIST SP 800-53 R4 CM-7(1): Periodic review
NIST SP 800-53 R4 CM-7(2): Prevent program execution
NIST SP 800-53 R4 CM-7(4): Unauthorized software/blacklisting
NIST SP 800-53 R4 CM-7(5): Authorized software/whitelisting

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
01.n Privilege Management *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Deep Security (2) Control Manager (2)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** **NIST**

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1)(a): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.

PCI DSS v3.2 Subsection

1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

PR.AC-3: Remote access is managed

PR.AC-5: Network integrity is protected

PR.DS-5: Protections against data leaks are implemented

PR.PT-4: Communications and control networks are protected

NIST SP 800-53 R4 SC-7: Boundary protection

NIST SP 800-53 R4 SC-7(5): Deny by default / allow by exception

LEVEL TWO (Additional to One)

NIST Cybersecurity Frameworks

DE.CM-1: The network is monitored to detect potential cybersecurity events

PR.DS-2: Data-in-transit is protected

PR. IP-3: Configuration change control processes are in place

NIST SP 800-53 R4 AC-17: Remote access

NIST SP 800-53 R4 AC-17(3): Managed access control points

NIST SP 800-53 R4 AC-2(11): Usage conditions

NIST SP 800-53 R4 SC-7(3): Access points

NIST SP 800-53 R4 SC-7(4): External telecommunications services

NIST SP 800-53 R4 SC-7(7): Prevent split tunneling for remote devices

NIST SP 800-53 R4 SC-7(8): Route traffic to authenticated proxy servers

NIST SP 800-53 R4 SC-8: Transmission confidentiality and integrity

PMI DSP Framework PR.DS-1:Encryption

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard

01.v Information Access Restriction
*Required for HITRUST v9.1 Certification
(Page 1 of 2)

Trend Micro Offering (HITRUST level)

Deep Security (1)
Smart Check (1)
Server Protect for Storage (1)
Control Manager (2)

Additional Frameworks

GDPR (EU)
HIPAA Security Rule
PCI DSS v3.2
NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.308(a)(3)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI for all those permitted within the workforce and prevent those within the workforce who are not permitted to access ePHI. HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)
HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient’s role
HIPAA § 164.308(a)(4)(ii)(A): Implement isolating health care clearinghouse functions (required)
HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)
HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)
HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.
HIPAA § 164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)
HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.
HIPAA § 164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
HIPAA § 164.312(a)(2)(iv): Implement maintenance records (addressable)

PCI Data Security Standard v3.2

12.3.10: For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

8.7: All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: All user access to, user queries of, and user actions on databases are through programmatic methods. Only database administrators have the ability to directly access or query databases. Application IDs for database applications can only be used by the applications (and not by individual users or other non- application processes).

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
01.v Information Access Restriction *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Deep Security (1) Smart Check (1) Server Protect for Storage (1) Control Manager (2)	GDPR (EU) HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-4: Access permissions and authorizations are managed, incorporate the principles of least privilege and separation of duties

PR.DS-5: Protections against data leaks are implemented

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

NIST SP 800-53 R4 AC-14: Permitted actions without identification or authentication

NIST SP 800-53 R4 AC-6: Least privilege

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

PR.DS-1: Data-at-rest is protected

NIST SP 800-53 R4 AC-1: Access control policy and procedures

NIST SP 800-53 R4 AC-3: Access enforcement

NIST SP 800-53 R4 DM-1: Minimization of personally identifiable information

NIST SP 800-53 R4 SC-13: Cryptographic protection

NIST SP 800-53 R4 SC-15: Collaborative computing devices

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification **(Page 1 of 3)**	Deep Security (2) Control Manager (2)	**GDPR (EU)** PCI DSS v3.2 NIST

EU General Data Protection Regulation (GDPR) (1/2)

GDPR Article 5(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

GDPR Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

GDPR Article 6(1)(a): Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purpose.

GDPR Article 24(1): Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

GDPR Article 25(1): Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

GDPR Article 25(2): The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. 2That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. 3In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

GDPR Article 27(1): Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

GDPR Article 27(2): The obligation laid down in paragraph 1 of this Article shall not apply to: GDPRA 27.2.A or B GDPR Article 27(3): The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, are.

GDPR Article 27(4): The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

GDPR Article 27(5): The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate

GDPR Article 37(1): The controller and the processor shall designate a data protection officer in any case where: GDPRA 37.1A/B/C

GDPR Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification **(Page 2 of 3)**	Deep Security (2) Control Manager (2)	**GDPR (EU)** **PCI DSS v3.2** NIST

EU General Data Protection Regulation (GDPR) (2/2)

GDPR Article 37(3): Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organizational structure and size.

GDPR Article 37(4): In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

GDPR Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

GDPR Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

GDPR Article 38(1): The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

GDPR Article 38(2): The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

GDPR Article 38(3): The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. 2He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. 3The data protection officer shall directly report to the highest management level of the controller or the processor.

GDPR Article 38(5): The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

GDPR Article 38(6): The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

GDPR Article 39(1): The data protection officer shall have at least the following tasks: (GPDRA 39.1.A/B/C/D/E)

GDPR Article 39(2): The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

PCI Data Security Standard v3.2

3.1: Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements Specific retention requirements for cardholder data Processes for secure deletion of data when no longer needed A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

3.4: Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One-way hashes based on strong cryptography, (hash must be of the entire PAN) Truncation (hashing cannot be used to replace the truncated segment of PAN) Index tokens and pads (pads must be securely stored) Strong cryptography with associated key-management processes and procedures.

3.4.1: If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification **(Page 3 of 3)**	Deep Security (2) Control Manager (2)	GDPR (EU) PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

PR.DS-1: Data-at-rest is protected

PR.DS-2: Data-in-transit is protected

NIST SP 800-53 R4 AR-1: Governance and privacy program

NIST SP 800-53 R4 AR-2: Privacy impact and risk assessment

NIST SP 800-53 R4 SC-12(1): Cryptographic key establishment and management availability

NIST SP 800-53 R4 SC-28: Protection of information at rest

NIST SP 800-53 R4 SC-28(1): Cryptographic protection

LEVEL TWO (Additional to One):

NIST SP 800-53 R4 SI-12: Information handling and retention

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
06.g Compliance with Security Policies and Standards *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Deep Security (2) Control Manager (2)	**HIPAA Security Rule** **PCI DSS v3.2** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(1)(ii)(D): Implement information system activity review(s)

HIPAA § 164.308(a)(2): Designate a HIPAA compliance security official who is responsible for developing and implementing the data center's security policies and procedures.

HIPAA § 164.308(a)(8): Perform a periodic assessment of how well the data center's security policies and procedures meet the requirements of the Security Rule.

PCI Data Security Standard v3.2

12.11: Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: Daily log reviews Firewall rule-set reviews Applying configuration standards to new systems Responding to security alerts Change management processes

12.11.1: Additional requirement for service providers only: Maintain documentation of quarterly review process to include: Documenting results of the reviews Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE. DP-1: Roles and responsibilities for detection are well defined to ensure accountability

DE. DP-4: Event detection information is communicated

ID.RA-6: Risk responses are identified and prioritized

NIST SP 800-53 R4 AR-4: Privacy monitoring and auditing

LEVEL TWO (Additional to One)

NIST Cybersecurity Frameworks

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

NIST SP 800-53 R4 CA-1: Security assessments and authorization policies and procedures

NIST SP 800-53 R4 CA-7: Continuous monitoring

NIST SP 800-53 R4 CA-7(1): Independent assessments

NIST SP 800-53 R4 RA-5: Vulnerability scanning

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
06.h Technical Compliance Checking *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Deep Security (2) Smart Check (2) Server Protect for Storage (1) Control Manager (2)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(1)(ii)(D): Implement information system activity review(s)

HIPAA § 164.308(a)(8): Perform a periodic assessment of how well the data center's security policies and procedures meet the requirements of the Security Rule.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.CM-8: Vulnerability scans are performed

ID.RA-1: Asset vulnerabilities are identified and documented

ID.RA-6: Risk responses are identified and prioritized

PR. IP-12: A vulnerability management plan is developed and implemented

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

NIST SP 800-53 R4 CA-2: Security assessments

LEVEL TWO (Additional to One):

NIST SP 800-53 R4 CA-2(2): Specialized assessments

NIST SP 800-53 R4 CA-7: Continuous monitoring

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
08.b Physical Entry Controls *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (2)	**HIPAA Security Rule** **PCI DSS v3.2** NIST

HIPAA Security Rule

HIPAA § 164.310(a)(1): Limit physical access to the data center facilities while ensuring that authorized access is allowed.

HIPAA § 164.310(a)(2)(iii): Implement access control and validation procedures (addressable)

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.

HIPAA § 164.310(C): Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

PCI Data Security Standard v3.2

9.1: Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment

9.2: Develop procedures to easily distinguish between onsite personnel and visitors, to include: Identifying onsite personnel and visitors (for example, assigning badges) Changes to access requirements Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).

9.3: Control physical access for onsite personnel to sensitive areas as follows: Access must be authorized and based on individual job function. Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

9.4: Implement procedures to identify and authorize visitors.

9.4.1: Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.

9.4.2: Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.

9.4.3: Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.

9.4.4: A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
08.b Physical Entry Controls *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (2)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (2/2)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

DE. DP-2: Detection activities comply with all applicable requirements

PR.AC-2: Physical access to assets is managed and protected

NIST SP 800-53 R4 MA-2: Controlled maintenance

NIST SP 800-53 R4 PE-2: Physical access authorizations

NIST SP 800-53 R4 PE-3: Physical access control

NIST SP 800-53 R4 PE-8: Visitor access records

LEVEL TWO (Additional to One)

NIST Cybersecurity Frameworks

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

RS.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

NIST SP 800-53 R4 PE-6: Monitoring physical access

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
08.d Protecting Against External and Environmental Threats *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (2)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.310(a)(1): Limit physical access to the data center facilities while ensuring that authorized access is allowed.
HIPAA § 164.310(a)(2)(ii): Implemented facility security plan (addressable)
HIPAA § 164.310(a)(2)(iii): Implement access control and validation procedures (addressable)

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks
PR. IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
NIST SP 800-53 R4 PE-1: Physical and environmental protection policy and procedures
NIST SP 800-53 R4 PE-13: Fire protection
NIST SP 800-53 R4 PE-13(1): Detection devices/systems

LEVEL TWO (Additional to One):

NIST SP 800-53 R4 AT-3(1): Role-based security training: environmental controls
NIST SP 800-53 R4 PE-13(3): Automatic fire suppression

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.n Security of Network Services *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (2)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.308(b)(1): A covered entity or business associate may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances in the form of a written contract or other agreement.

HIPAA § 164.308(b)(3): Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

HIPAA § 164.314(a)(1): The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

HIPAA § 164.314(a)(2)(ii): In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section;

National Institute of Standards & Technology (NIST)

LEVEL ONE

NIST Cybersecurity Frameworks

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

ID.AM-4: External information systems are catalogued Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities

PR.PT-4: Communications and control networks areprotected

NIST SP 800-53 R4 CA-3: System interconnections

NIST SP 800-53 R4 SA-9: External information system services

LEVEL TWO (Additional to One)

NIST Cybersecurity Frameworks

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

ID.AM-3: Organizational communication and data flows are mapped

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

NIST SP 800-53 R4 CA-3(5): Restrictions on external system connections

NIST SP 800-53 R4 SA-9(2): Identification of functions/ports/protocols/services

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 1 of 3)**	Deep Security (2) Smart Check (1) Server Protect for Storage (1) Control Manager (2)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1)(a): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data;

GDPR Article 32(1)(b): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

HIPAA Security Rule

HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.
HIPAA § 164.312(c)(1): Implement policies and procedures to protect ePHI from alteration or destruction in an unauthorized manner.
HIPAA § 164.312(c)(2): Establish mechanisms to authenticate those seeking access to ePHI (addressable).
HIPAA § 164.312(d): Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
HIPAA § 164.312(e)(1): Implement technical security measures to guard against unauthorized access or manipulation to ePHI that is being transmitted over an electronic communications network.
HIPAA § 164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted ePHI is not modified without detection until disposed of (addressable)
HIPAA § 164.312(e)(2)(ii): Establish a mechanism to encrypt ePHI whenever it is deemed appropriate (addressable)

PCI Data Security Standard v3.2 (1/2)

1.1: Establish and implement firewall and router configuration standards that include the following:
1.1.1: A formal process for approving and testing all network connections and changes to the firewall and router configurations
1.1.2: Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
1.1.3: Current diagram that shows all cardholder data flows across systems and networks
1.1.4: Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
1.1.5: Description of groups, roles, and responsibilities for management of network components
1.1.6: Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
1.1.7: Requirement to review firewall and router rule sets at least every six months

(Continued next page....)

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 2 of 3)**	Deep Security (2) Smart Check (1) Server Protect for Storage (1) Control Manager (2)	GDPR (EU) HIPAA Security Rule **PCI DSS v3.2** **NIST**

PCI Data Security Standard v3.2 (2/2)

1.2: Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

1.2.2: Secure and synchronize router configuration files.

1.2.3: Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

1.3: Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.3.1: Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2: Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.3: Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

1.3.4: Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

1.3.5: Permit only “established” connections into the network.

1.3.6: Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

1.3.7: Do not disclose private IP addresses and routing information to unauthorized parties.

11.1: Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

11.4: Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises

2.1.1: For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

4.1.1: Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

9.1.3: Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines

National Institute of Standards & Technology (NIST) (1/2)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

DE.CM-1: The network is monitored to detect potential cybersecurity events

ID.AM-3: Organizational communication and data flows are mapped

PR.DS-2: Data-in-transit is protected

PR.DS-5: Protections against data leaks are implemented

PR. IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

NIST SP 800-53 R4 AC-18: Wireless access

NIST SP 800-53 R4 AC-18(1): Authentication and encryption

NIST SP 800-53 R4 SI-4: Information system monitoring

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 3 of 3)**	Deep Security (2) Smart Check (1) Server Protect for Storage (1) Control Manager (2)	GDPR (EU) HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (2/2)

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks Subsections

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.AC-5: Network integrity is protected

NIST SP 800-53 R4 AC-17: Remote access

NIST SP 800-53 R4 CA-3: System interconnections

NIST SP 800-53 R4 CM-3: Configuration change control

NIST SP 800-53 R4 IA-3: Device identification and authentication

NIST SP 800-53 R4 SC-19: Voice over internet protocol

NIST SP 800-53 R4 SC-20: Secure name/address resolution service (authoritative source)

NIST SP 800-53 R4 SC-7: Prevent split tunneling for remote devices

NIST SP 800-53 R4 SC-7(5): Deny by default/allow by exception

NIST SP 800-53 R4 SC-8: Transmission confidentiality and integrity

NIST SP 800-53 R4 SC-8(1): Cryptographic or alternate physical protection

NIST SP 800-53 R4 SC-8(2): Pre/post transmission handling

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.aa Audit Logging *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)	**HIPAA Security Rule** **PCI DSS v3.2** NIST

HIPAA Security Rule

HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable) HIPAA § 164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

PCI Data Security Standard v3.2

10.1: Implement audit trails to link all access to system components to each individual user

10.2: Implement automated audit trails for all system components to reconstruct the following events:

10.2.1: All individual user accesses to cardholder data

10.2.2: All actions taken by any individual with root or administrative privileges

10.2.4: Invalid logical access attempts

10.2.5: Use of and changes to identification and authentication mechanisms— including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges

10.2.6: Initialization, stopping, or pausing of the audit logs

10.2.7: Creation and deletion of system-level objects

10.3.1: Record audit trail entries for user identification.

10.3.2: Record audit trail entries for type(s) of event.

10.3.3: Record audit trail entries for date and time.

10.3.4: Record audit trail entries for success or failure indication.

10.3.5: Record audit trail entries for origination of event.

10.3.6: Record audit trail entries for identity or name of affected data, system component, or resource

10.3.7: Record audit trail entries for system or component

10.5: Secure audit trails so they cannot be altered.

10.7: Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)

A.1.3: Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.aa Audit Logging *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Framework

DE.CM-1: The network is monitored to detect potential cybersecurity events

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

NIST SP 800-53 R4 AR-4: Privacy monitoring and auditing

NIST SP 800-53 R4 AU-11: Audit record retention

NIST SP 800-53 R4 AU-3: Content of audit records

NIST SP 800-53 R4 AU-8: Time stamps

NIST SP 800-53 R4 AU-9: Protection of audit information

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

DE.CM-1: The network is monitored to detect potential cybersecurity events

NIST SP 800-53 R4 AC-6(9): Auditing use of privileged functions

NIST SP 800-53 R4 AU-2: Audit events

NIST SP 800-53 R4 AU-2(3): Review and updates

NIST SP 800-53 R4 AU-5: Response to audit processing failures

NIST SP 800-53 R4 AU-5(4): Shutdown on failure

NIST SP 800-53 R4 AU-9(4): Access by subset of privileged users

NIST SP 800-53 R4 AU-9(5): Dual authorization

LEVEL THREE (Additional to Two):

NIST SP 800-53 R4 AC-2(4): Automated audit actions

NIST SP 800-53 R4 AU-3(1): Additional audit information

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.ab Monitoring System Use *Required for HITRUST v9.1 Certification **(Page 1 of 3)**	Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)	**HIPAA Security Rule** **PCI DSS v3.2** NIST

HIPAA Security Rule

HIPAA § 164.308(a)(1)(ii)(D): Implement information system activity review(s)

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient's role

HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)

HIPAA § 164.308(a)(5)(ii)(B): Implement protection from malicious software (addressable)

HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable)

HIPAA § 164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

PCI Data Security Standard v3.2

10.6: Review logs and security events for all system components to identify anomalies or suspicious activity.

10.6.1: Review the following at least daily: All security events Logs of all system components that store, process, or transmit CHD and/or SAD Logs of all critical system components Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/ IPS), authentication servers, e-commerce redirection servers, etc.).

10.6.2: Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.

10.6.3: Follow up exceptions and anomalies identified during the review process.

10.8: Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: Firewalls IDS/IPS FIM Anti-Virus Physical access controls Logical access controls Audit logging mechanisms Segmentation controls (if used)

10.8.1: Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from reoccurring Resuming monitoring of security controls

11.5: Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.ab Monitoring System Use *Required for HITRUST v9.1 Certification **(Page 2 of 3)**	Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (1/2)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE. DP-2: Detection activities comply with all applicable requirements

DE. DP-3: Detection processes are tested

DE-AE-3: Event data are collected and correlated from multiple sources and sensors

DE-DP-5: Detection processes are continuously improved

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

LEVEL TWO (Additional to One)

NIST Cybersecurity Frameworks

DE.AE-2: Detected events are analyzed to understand attack targets and methods

DE.CM-1: The network is monitored to detect potential cybersecurity events

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

RS.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

NIST SP 800-53 R4 AR-4: Privacy monitoring and auditing

NIST SP 800-53 R4 AU-2: Audit events

NIST SP 800-53 R4 AU-3: Content of audit records

NIST SP 800-53 R4 AU-7: Audit reduction and report generation

NIST SP 800-53 R4 AU-7(1): Automatic processing

NIST SP 800-53 R4 PE-6: Monitoring physical access

NIST SP 800-53 R4 SI-4: Information system monitoring

NIST SP 800-53 R4 SI-4(2): Automated tools for real-time analysis

LEVEL THREE (Additional to Two)

NIST Cybersecurity Frameworks

DE.CM-4: Malicious code is detected

NDE.DP-2: Detection activities comply with all applicable requirements

DE. DP-4: Event detection information is communicated

ID.RA-1: Asset vulnerabilities are identified and documented

RS.AN-1: Notifications from detection systems are investigated

RS.CO-2: Incidents are reported consistent with established criteria

(Continued on next page...)

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.ab Monitoring System Use *Required for HITRUST v9.1 Certification **(Page 3 of 3)**	Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (2/2)

LEVEL THREE (Cont.)

NIST SP 800-53 R4 AC-2(12): Account monitoring / atypical use

NIST SP 800-53 R4 AU-6: Audit review, analysis, and reporting

NIST SP 800-53 R4 AU-6(1): Process integration

NIST SP 800-53 R4 AU-6(3): Correlate audit repositories

NIST SP 800-53 R4 AU-6(9): Correlation with information from nontechnical sources

NIST SP 800-53 R4 SI-3: Malicious code protection

NIST SP 800-53 R4 SI-4(1): System-wide intrusion detection systems

NIST SP 800-53 R4 SI-4(3): Automated tool integration

NIST SP 800-53 R4 SI-4(4): Inbound and outbound communications traffic

NIST SP 800-53 R4 SI-4(5): System-generated alerts

NIST SP 800-53 R4 SI-7(2): Software, firmware, and information integrity

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
10.m Control of Technical Vulnerabilities *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Deep Security (3) Smart Check (2) Server Protect for Storage (3) Control Manager (2)	**HIPAA Security Rule** **PCI DSS v3.2** NIST

HIPAA Security Rule

HIPAA § 164.308(a)(8): Perform a periodic assessment of how well the data center's security policies and procedures meet the requirements of the Security Rule.

PCI Data Security Standard v3.2

11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

11.2.1: Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.

11.2.2: Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

11.2.3: Qualified personnel perform internal and external scans, and rescans as needed, after any significant change.

11.3: Implement a methodology for penetration testing that includes the following: Is based on industry-accepted penetration testing approaches (for example, NIST SP800- 115) Includes coverage for the entire CDE perimeter and critical systems Includes testing from both inside and outside the network Includes testing to validate any segmentation and scope-reduction controls Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 Defines network-layer penetration tests to include components that support network functions as well as operating systems Includes review and consideration of threats and vulnerabilities experienced in the last 12 months Specifies retention of penetration testing results and remediation activities results.

11.3.1: Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.2: Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.3: Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

11.3.4: If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/ methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

11.3.4.1: For service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.

2.2: Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry accepted system hardening standards.

2.2.2: Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

2.2.3: Implement additional security features for any required services, protocols, or daemons that are considered to be insecure

6.1: Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as high, medium, or low) to newly discovered security vulnerabilities.

6.2: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release

6.4.5: Change control procedures must include the following:

6.4.5.1: Documentation of impact.

6.4.5.2: Documented change approval by authorized parties.

6.4.5.3: Functionality testing to verify that the change does not adversely impact the security of the system.

6.4.5.4: Back-out procedures.

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
10.m Control of Technical Vulnerabilities *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Deep Security (3) Smart Check (2) Server Protect for Storage (3) Control Manager (2)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

ID.RA-1: Asset vulnerabilities are identified and documented

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources

ID.RA-4: Potential business impacts and likelihoods are identified

ID.RA-6: Risk responses are identified and prioritized

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

NIST SP 800-53 R4 RA-5: Vulnerability scanning

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

DE.CM-8: Vulnerability scans are performed

DE. DP-5: Detection processes are continuously improved

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

PR. IP-12: A vulnerability management plan is developed and implemented

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

RS.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

NIST SP 800-53 R4 CM-6: External service provider activity is monitored to detect potential cybersecurity events

NIST SP 800-53 R4 CM-7: Least functionality

NIST SP 800-53 R4 SI-5: Security alerts, advisories, and directives

LEVEL THREE (Additional to Two):

NIST Cybersecurity Frameworks

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

NIST SP 800-53 R4 CA-2: Security assessments

NIST SP 800-53 R4 CA-7: Continuous monitoring

NIST SP 800-53 R4 CA-8: Penetration testing

NIST SP 800-53 R4 RA-5(1): Update tool capability

NIST SP 800-53 R4 RA-5(2): Update by frequency / prior to new scan / when identified

NIST SP 800-53 R4 RA-5(4): Discoverable information

NIST SP 800-53 R4 RA-5(5): Privileged access

NIST SP 800-53 R4 SI-2: Flaw remediations

NIST SP 800-53 R4 SI-2(1): Central management

NIST SP 800-53 R4 SI-2(2): Automated flaw remediation status

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
00.a Information Security Management Program *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)	**GDPR (EU)** **HIPAA Security Rule** NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 24(1): Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. 2Those measures shall be reviewed and updated where necessary.

GDPR Article 25(1): Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.308(a)(1)(i): Risk analysis (required) HIPAA § 164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity

HIPAA § 164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

HIPAA § 164.308(a)(8): Evaluation

HIPAA § 164.312(a)(2)(ii): Emergency access procedure (required)

HIPAA § 164.316(b)(1): Standard: documentation

HIPAA § 164.316(b)(2)(iii): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Standards Equivalency Report

Hybrid Cloud Security Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
00.a Information Security Management Program *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)	GDPR (EU) HIPAA Security Rule **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE):
NIST Cybersecurity Framework
ID. GV-1: Organizational cybersecurity policy is established and communicated.
ID. GV-4: Governance and risk management processes address cybersecurity risks.
NIST SP 800-53 R4 PM-1: Information security program plan.

LEVEL TWO (Additional to One):
NIST Cybersecurity Frameworks
PR. IP-7: Protection processes are improved

LEVEL THREE (Additional to Two):
NIST Cybersecurity Frameworks
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established
PR.AT-1: All users are informed and trained
PR.AT-2: Privileged users understand their roles and responsibilities
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PR.AT-4: Senior executives understand their roles and responsibilities
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities
NIST SP 800-53 R4 PM-13: Information security workforce
NIST SP 800-53 R4 PM-2: Senior information security officer

TREND MICRO™

User Protection Solution

Standards Equivalency Report

September 2018

HITRUST CSF v9.1

EU General Data Protection Regulation (GDPR)

HIPAA Security Rule

HIPAA Breach Notification Rule

PCI Data Security Standard v3.2

National Institute of Standards & Technology (NIST)

Prepared By

MEDITOLOGY
SERVICES

User Protection Solution

Standards Equivalency Report

PREFACE

This report maps Trend Micro’s User Protection Solution to the HITRUST v9.1 standard, highlighting specific products in the solution and the level (in brackets) relevant under HITRUST v9.1. In addition, where relevant, specific areas under HIPAA, PCI DSS v3.2, GDPR, and multiple NIST frameworks are highlighted for applicability.

For more information on Trend Micro’s User Protection Solution, please visit: https://www.tre ndmicro.com/en_us/business/products/user-protection.html.

Standards Equivalency Report

User Protection Solution

HITRUST Standard

01.c Privilege Management
*Required for HITRUST v9.1 Certification
(Page 1 of 2)

Trend Micro Offering (HITRUST Level)

Control Manager (1)
Data Loss Prevention (1)
Email (1)
Endpoint (1)
Web Security (1)

Additional Frameworks

HIPAA Security Rule
PCI DSS v3.2
NIST

HIPAA Security Rule

HIPAA § 164.308(a)(3)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI for all those permitted within the workforce and prevent those within the workforce who are not permitted to access ePHI.

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA §164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient’s role

HIPAA § 164.308(a)(4)(ii)(A): Implement isolating health care clearinghouse functions (required)

HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)

HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)

HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable)

HIPAA § 164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)

HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.

HIPAA § 164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

PCI Data Security Standard v3.2

7.1 : Limit access to system components and cardholder data to only those individuals whose job requires such access

7.1.1 : Define access needs for each role

7.1.2 : Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities

7.1.3 : Assign access based on individual personnel’s job classification and function.

7.1.4 : Require documented approval by authorized parties specifying required privileges

7.2 : Establish an access control system(s) for systems components that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed.

7.2.1 : Access control system must include coverage of all system components

7.2.2 : Access control system must include assignment of privileges to individuals based on job classification and function

7.2.3 : Access control system must include default “deny-all” setting

A.1.1: Ensure that each entity only runs processes that have access to that entity’s cardholder data environment.

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.c Privilege Management *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Control Manager (1) Data Loss Prevention (1) Email (1) Endpoint (1) Web Security(1)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-4: Access permissions are managed, incorporate the principles of least privilege and separation of duties

NIST SP 800-53 R4 AC-3: Access enforcement

NIST SP 800-53 R4 AC-6: Least privilege

NIST SP 800-53 R4 AC-6(1): Authorize access to security functions

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

R.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.DS-5: Protections against data leaks are implemented

PR.PT-4: Communications and control networks are protected

NIST SP 800-53 R4 AC-10: Concurrent session control

NIST SP 800-53 R4 AC-2: Account management

NIST SP 800-53 R4 AC-21: Information sharing

NIST SP 800-53 R4 AC-3(7): Role-based access control

NIST SP 800-53 R4 AC-6(2): Non-privileged access for nonsecurity functions.

LEVEL THREE (Additional to Two):

NIST Cybersecurity Frameworks

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

NIST SP 800-53 R4 AC-6(10): Prohibit non-privileged users from executing privileged functions.

NIST SP 800-53 R4 AC-6(5): Privileged accounts

NIST SP 800-53 R4 AC-6(9): Auditing use of privileged functions

NIST SP 800-53 R4 CM-7: Least functionality

Standards Equivalency Report

User Protection Solution

HITRUST Standard

01.e Review of User Access Rights
*Required for HITRUST v9.1 Certification
(Page 1 of 1)

Trend Micro Offering (HITRUST Level)

Control Manager (1)
Data Loss Prevention (1)
Email (1)
Endpoint (1)
Web Security(1)

Additional Frameworks

HIPAA Security Rule
NIST

HIPAA Security Rule

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(3)(ii)(B): Implement workforce clearance procedure(s) (addressable)

HIPAA § 164.308(a)(3)(ii)(C): Implement termination procedures (addressable)

HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient's role

HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)

HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)

HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable)

HIPAA § 164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

NIST SP 800-53 R4 PS-4: Personnel screening

NIST SP 800-53 R4 PS-5: Personnel transfer

LEVEL TWO (Additional to One):

NIST SP 800-53 R4 AC-2: Account management

Standards Equivalency Report

User Protection Solution

HITRUST Standard

01.j User Authentication for External Connections
*Required for HITRUST v9.1 Certification
(Page 1 of 2)

Trend Micro Offering (HITRUST Level)

Control Manager (1)
Data Loss Prevention (1)
Email (1)
Endpoint (1)
Web Security(1)

Additional Frameworks

HIPAA Security Rule
PCI DSS v3.2
NIST

HIPAA Security Rule

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.
HIPAA § 164.312(d): Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

PCI Data Security Standard v3.2

12.3.9: Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.

8.1.5: Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: Enabled only during the period needed and disabled when not in use. Monitored when in use.

8.3.1 : Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

8.3.2 : Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.j User Authentication for External Connections *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Control Manager (1) Data Loss Prevention (2) Email (1) Endpoint (1) Web Security(1)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Framework
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-3: Remote access is managed
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
PR.PT-4: Communications and control networks are protected
NIST SP 800-53 R4 AC-17: Remote access
NIST SP 800-53 R4 AC-18: Wireless access
NIST SP 800-53 R4 IA-2: Identification and authentication (organizational users)
NIST SP 800-53 R4 IA-3: Device identification and authentications
NIST SP 800-53 R4 IA-8: Identification and authentication (non-organizational users)

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks
DE.CM-1: The network is monitored to detect potential cybersecurity events
PR.DS-2: Data-in-transit is protected
NIST SP 800-53 R4 AC-17(2): Protection of confidentiality/integrity using encryption
NIST SP 800-53 R4 AC-2: Account management
NIST SP 800-53 R4 CM-2: Baseline configuration
NIST SP 800-53 R4 CM-2(2): Automation support for accuracy/currency
NIST SP 800-53 R4 IA-5(11): Hardware token-based authentication
NIST SP 800-53 R4 IA-8(1): Acceptance of PIV credentials from other agencies
NIST SP 800-53 R4 IA-8(2): Acceptance of third-party credentials
NIST SP 800-53 R4 IA-8(3): Use of FICAM-approved products
NIST SP 800-53 R4 IA-8(4): Use of FICAM-issued profiles

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.l Remote Diagnostic and Configuration Port Protection *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (3) Data Loss Prevention (3) Email (1) Endpoint (2) Web Security(1)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.310(a)(2)(iii): Implement access control and validation procedures (addressable)

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.

HIPAA § 164.310(C): Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Framework Subsections

PR.AC-2: Physical access to assets is managed and protected

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

NIST SP 800-53 R4 PE-3(1): Information system access

LEVEL TWO (Additional to One):

NIST Cybersecurity Framework Subsections

PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

NIST SP 800-53 R4 CM-7: Least functionality

NIST SP 800-53 R4 MA-4: Nonlocal maintenance

NIST SP 800-53 R4 MA-4(2): Document nonlocal maintenance

NIST SP 800-53 R4 MA-4(3): Comparable security/sanitization

LEVEL THREE (Additional to Two):

NIST Cybersecurity Framework Subsections

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

ID.AM-2: Software platforms and applications within the organization are inventoried

ID.AM-3: Organizational communication and data flows are mapped

PR. IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

PR. IP-3: Configuration change control processes are in place

NIST SP 800-53 R4 CM-7(1): Periodic review

NIST SP 800-53 R4 CM-7(2): Prevent program execution

NIST SP 800-53 R4 CM-7(4): Unauthorized software/blacklisting

NIST SP 800-53 R4 CM-7(5): Authorized software/whitelisting

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.n Privilege Management *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (2) Data Loss Prevention (2) Web Security (1)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** **NIST**

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1)(a): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.

PCI Data Security Standard v3.2

1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

National Institute of Standards & Technology (NIST)

LEVEL ONE:
NIST Cybersecurity Frameworks
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.
PR.AC-3: Remote access is managed
PR.AC-5: Network integrity is protected
PR.DS-5: Protections against data leaks are implemented
PR.PT-4: Communications and control networks are protected
NIST SP 800-53 R4 SC-7: Boundary protection
NIST SP 800-53 R4 SC-7(5): Deny by default / allow by exception

LEVEL TWO (Additional to One):
NIST Cybersecurity Frameworks
DE.CM-1: The network is monitored to detect potential cybersecurity events
PR.DS-2: Data-in-transit is protected
PR. IP-3: Configuration change control processes are in place
NIST SP 800-53 R4 AC-17: Remote access
NIST SP 800-53 R4 AC-17(3): Managed access control points
NIST SP 800-53 R4 AC-2(11): Usage conditions
NIST SP 800-53 R4 SC-7(3): Access points
NIST SP 800-53 R4 SC-7(4): External telecommunications services
NIST SP 800-53 R4 SC-7(7): Prevent split tunneling for remote devices
NIST SP 800-53 R4 SC-7(8): Route traffic to authenticated proxy servers
NIST SP 800-53 R4 SC-8: Transmission confidentiality and integrity PMI
DSP Framework PR.DS-1: Encryption

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.o Network Routing Control *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (1) Data Loss Prevention (1) Web Security (1)	**HIPAA Security Rule** **PCI DSS v3.2** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(3)(ii)(B): Implement workforce clearance procedure(s) (addressable)

HIPAA § 164.312(c)(2): Establish mechanisms to authenticate those seeking access to ePHI (addressable).

HIPAA § 164.312(e)(1): Implement technical security measures to guard against unauthorized access or manipulation to ePHI that is being transmitted over an electronic communications network.

PCI Data Security Standard v3.2

1.2: Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-5: Network integrity is protected

PR.DS-5: Protections against data leaks are implemented

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.v Information Access Restriction *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (1) Web Security(1)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.308(a)(3)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI for all those permitted within the workforce and prevent those within the workforce who are not permitted to access ePHI.

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient's role

HIPAA § 164.308(a)(4)(ii)(A): Implement isolating health care clearinghouse functions (required) **HIPAA § 164.308(a)(4)(ii)(B):** Implement access authorization (addressable)

HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.

HIPAA § 164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)

HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.

HIPAA § 164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

HIPAA § 164.312(a)(2)(iv): Implement maintenance records (addressable)

PCI Data Security Standard v3.2

12.3.10: For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

8.7: All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: All user access to, user queries of, and user actions on databases are through programmatic methods. Only database administrators have the ability to directly access or query databases. Application IDs for database applications can only be used by the applications (and not by individual users or other non- application processes).

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.v Information Access Restriction *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (1) Web Security(1)	GDPR (EU) HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks Subsections

PR.AC-4: Access permissions and authorizations are managed, incorporate the principles of least privilege and separation of duties.

PR.DS-5: Protections against data leaks are implemented

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

NIST SP 800-53 R4 AC-14: Permitted actions without identification or authentication

NIST SP 800-53 R4 AC-6: Least privilege

LEVEL TWO (Additional to One):

NIST Cybersecurity Framework Subsection

PR.DS-1: Data-at-rest is protected

NIST SP 800-53 R4 AC-1: Access control policy and procedures

NIST SP 800-53 R4 AC-3: Access enforcement

NIST SP 800-53 R4 DM-1: Minimization of personally identifiable information

NIST SP 800-53 R4 SC-13: Cryptographic protection

NIST SP 800-53 R4 SC-15: Collaborative computing devices

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.x Mobile Computing and Communications *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (1) Web Security(1)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** **NIST**

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.
HIPAA § 164.310(C): Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

PCI Data Security Standard v3.2

1.4: Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: Specific configuration settings are defined. Personal firewall (or equivalent functionality) is actively running. Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.
9.5: Physically secure all media.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

PR.AC-2: Physical access to assets is managed and protected

PR.AT-1: All users are informed and trained

PR.DS-1: Data-at-rest is protected

PR. IP-1:A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

NIST SP 800-53 R4 AC-19: Access control for mobile devices

NIST SP 800-53 R4 AC-19(5): Full device/container-based encryption

NIST SP 800-53 R4 CM-2(7): Configure systems, components, or devices for high-risk areas

NIST SP 800-53 R4 SI-4: Information system monitoring

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
01.y Teleworking *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Data Loss Prevention (1)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(3)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI for all those permitted within the workforce and prevent those within the workforce who are not permitted to access ePHI.

HIPAA § 164.308(a)(3)(ii)(B): Implement workforce clearance procedure(s) (addressable)

HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)

HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)

HIPAA § 164.310(a)(2)(i): Implement contingency operations (addressable)

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-2: Physical access to assets is managed and protected

PR.AC-3: Remote access is managed

PR.AT-1: All users are informed and trained

PR.DS-1: Data-at-rest is protected

PR.DS-2: Data-in-transit is protected

PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

PR. IP-1:A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

NIST SP 800-53 R4 AC-17: Remote access

NIST SP 800-53 R4 AC-17(2): Protection of confidentiality/integrity using encryption

NIST SP 800-53 R4 AT-2: Security awareness training

NIST SP 800-53 R4 IA-2: Identification and authentication (organizational users)

NIST SP 800-53 R4 PE-17: Alternate work site

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
06.c Protection of Organizational Records *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (1) Data Loss Prevention (1) Web Security (1)	**HIPAA Breach Notif. Rule** **PCI DSS v3.2** **NIST**

HIPAA Breach Notification Rule

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(3)(ii)(B): Implement workforce clearance procedure(s) (addressable)

HIPAA § 164.312(c)(2): Establish mechanisms to authenticate those seeking access to ePHI (addressable).

HIPAA § 164.312(e)(1): Implement technical security measures to guard against unauthorized access or manipulation to ePHI that is being transmitted over an electronic communications network.

PCI Data Security Standard v3.2

1.2: Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-5: Network integrity is protected

PR.DS-5: Protections against data leaks are implemented

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
06.c Protection of Organizational Records *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (2) Data Loss Prevention (2) Email (2) Endpoint (2) Web Security(2)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** **NIST**

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymization and encryption of personal data;

HIPAA Breach Notification Rule

HIPAA § 164.414(a): A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

PCI Data Security Standard v3.2

3.1: Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements Specific retention requirements for cardholder data Processes for secure deletion of data when no longer needed A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

ID.AM-5: Resources are prioritized based on their classification, criticality, and business value

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

ID. GV-4: Governance and risk management processes address cybersecurity risks

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

NIST SP 800-53 R4 AU-9: Protection of audit information

NIST SP800-53 R4 RA-2: Security categorization

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

PS.DS-3: Assets are formally managed throughout removal, transfers, and disposition

NIST SP 800-53 R4 DM-2: Data retention and disposal

NIST SP 800-53 R4 AU-11: Audit record retention

NIST SP 800-53 R4 DM-2(1): Data retention system configuration

NIST SP 800-53 R4 SI-12: Information handling and retention

Standards Equivalency Report

User Protection Solution

HITRUST Standard
06.e Prevention of Misuse of Information Assets *Required for HITRUST v9.1 Certification **(Page 1 of 1)**

Trend Micro Offering (HITRUST Level)

Control Manager (2)
Data Loss Prevention (2)
Email (2)
Endpoint (2)
Web Security(2)

Additional Frameworks
HIPAA Security Rule **PCI DSS v3.2** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(1)(ii)(C): Implement risk analysis (required)

HIPAA § 164.308(a)(1)(ii)(D): Implement information system activity review(s) (required)

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient's role

HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)

HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media

PCI Data Security Standard v3.2

12.3.1: Usage policy exists for explicit approval by authorized parties

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Framework

DE.CM-1: The network is monitored to detect potential cybersecurity events

DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

PR. IP-11: Cybersecurity is included in human resources practices

NIST SP 800-53 R4 PL-4: Rules of behavior

NIST SP 800-53 R4 PS-6: Access agreements

NIST SP 800-53 R4 PS-8: Personnel sanctions

LEVEL TWO (Additional to One):

NIST Cybersecurity Framework

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

NIST SP 800-53 R4 AC-8: System use notification

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification **(Page 1 of 3)**	Control Manager (2) Data Loss Prevention (2) Email (2)	**GDPR (EU)** PCI DSS v3.2 NIST

EU General Data Protection Regulation (GDPR) (1/2)

GDPR Article 5(1)(f): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

GDPR Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

GDPR Article 6(1)(a): Processing shall be lawful only if and to the extent that at least one of the following applies: **(a)** the data subject has given consent to the processing of his or her personal data for one or more specific purpose.

GDPR Article 24(1): Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

GDPR Article 25(1): Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

GDPR Article 25(2): The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. **2)** That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. **3)** In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

GDPR Article 27(1): Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

GDPR Article 27(2): The obligation laid down in paragraph 1 of this Article shall not apply to: GDPRA 27.2.A or B

GDPR Article 27(3): The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behavior is monitored, are.

GDPR Article 27(4): The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

GDPR Article 27(5): The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

GDPR Article 37(1): The controller and the processor shall designate a data protection officer in any case where: GDPRA 37.1A/B/C

GDPR Article 37(2):A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification **(Page 2 of 3)**	Control Manager (2) Data Loss Prevention (2) Email (2)	**GDPR (EU)** **PCI DSS v3.2** NIST

EU General Data Protection Regulation (GDPR) (2/2)

GDPR Article 37(3): Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organizational structure and size GDPR Article 37(4): In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. 2The data protection officer may act for such associations and other bodies representing controllers or processors.

GDPR Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

GDPR Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

GDPR Article 38(1): The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

GDPR Article 38(2): The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

GDPR Article 38(3): The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. 2He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. 3The data protection officer shall directly report to the highest management level of the controller or the processor.

GDPR Article 38(5): The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

GDPR Article 38(6): The data protection officer may fulfil other tasks and duties. 2The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

GDPR Article 39(1): The data protection officer shall have at least the following tasks: (GPDRA 39.1.A/B/C/D/E)

GDPR Article 39(2): The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

PCI Data Security Standard v3.2

3.1: Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements Specific retention requirements for cardholder data Processes for secure deletion of data when no longer needed A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

3.4: Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: One-way hashes based on strong cryptography, (hash must be of the entire PAN) Truncation (hashing cannot be used to replace the truncated segment of PAN) Index tokens and pads (pads must be securely stored) Strong cryptography with associated key-management processes and procedures.

3.4.1: If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification **(Page 3 of 3)**	Control Manager (2) Data Loss Prevention (2) Email (2)	GDPR (EU) PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

PR.DS-1: Data-at-rest is protected

PR.DS-2: Data-in-transit is protected

NIST SP 800-53 R4 AR-1: Governance and privacy program

NIST SP 800-53 R4 AR-2: Privacy impact and risk assessment

NIST SP 800-53 R4 SC-12(1): Cryptographic key establishment and management availability

NIST SP 800-53 R4 SC-28: Protection of information at rest

NIST SP 800-53 R4 SC-28(1): Cryptographic protection

LEVEL TWO (Additional to One):

NIST SP 800-53 R4 SI-12: Information handling and retention

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
09.j Controls Against Malicious Code *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (1) Web Security(1)	**HIPAA Security Rule** **PCI DSS v3.2** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(5)(i): Provide for appropriate authorization and supervision of workforce members who work with ePHI and train all workforce members regarding security policies and procedures.
HIPAA § 164.308(a)(5)(ii)(B): Implement protection from malicious software (addressable)

PCI Data Security Standard v3.2

5.1: Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

5.1.1: Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

5.1.2: For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
5.2: Ensure that all anti-virus mechanisms are maintained as follows: Are kept current, perform periodic scans Generate audit logs which are retained per PCI DSS Requirement 10.7.
5.3: Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Framework Subsections
DE.CM-4: Malicious code is detected
PR.AC-4:Access permissions and authorizations are managed, incorporate the principles of least privilege and separation of duties
PR.AT-1: All users are informed and trained
NIST SP 800-53 R4 CM-11: User-installed software
NIST SP 800-53 R4 SI-3: Malicious code protection

LEVEL TWO (Additional to One):

NIST SP 800-53 R4 SC-2: Application partitioning
NIST SP 800-53 R4 SI-16: Memory protection
NIST SP 800-53 R4 SI-3(1): Malicious code central management
NIST SP 800-53 R4 SI-3(2): Malicious code automatic updates
NIST SP 800-53 R4 SI-8: Spam protection
NIST SP 800-53 R4 SI-8(1): Spam protection central management
NIST SP 800-53 R4 SI-8(2): Spam protection automatic updates

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
09.k Controls Against Mobile Code * Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (2) Web Security(2)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(5)(ii)(B): Implement protection from malicious software (addressable)

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Framework Subsections
DE.CM-4: Malicious code is detected
DE.CM-5: Unauthorized mobile code is detected
NIST SP 800-53 R4 SC-18: Mobile code
NIST SP 800-53 R4 Si-3: Malicious code protection

LEVEL TWO (Additional to One):

NIST Cybersecurity Framework Subsection
PR.DS-7: The development and testing environment(s) are separate from the production environment
NIST SP 800-53 R4 CM-2(6): Development and test environments
NIST SP 800-53 R4 CM-3: Configuration change control
NIST SP 800-53 R4 SC-18(3): Prevent downloading/execution
NIST SP 800-53-R4 SC-2: Application partitioning
NIST SP 800-53 R4 SC-3: Security function isolation

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
09.n Security of Network Services *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (2) Data Loss Prevention (2) Email (2) Endpoint (2) Web Security(2)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.308(b)(1): A covered entity or business associate may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances in the form of a written contract or other agreement.

HIPAA § 164.308(b)(3): Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

HIPAA § 164.314(a)(1): The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

HIPAA § 164.314(a)(2)(ii): In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section;

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events

ID.AM-4: External information systems are catalogued

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities

PR.PT-4: Communications and control networks are protected

NIST SP 800-53 R4 CA-3: System interconnections

NIST SP 800-53 R4 SA-9: External information system services

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

ID.AM-3: Organizational communication and data flows are mapped

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

NIST SP 800-53 R4 CA-3(5): Restrictions on external system connections

NIST SP 800-53 R4 SA-9(2): Identification of functions/ports/protocols/services

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 1 of 3)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (1)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1)(a): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data;

GDPR Article 32(1)(b): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

HIPAA Security Rule

HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.

HIPAA § 164.312(c)(1): Implement policies and procedures to protect ePHI from alteration or destruction in an unauthorized manner.

HIPAA § 164.312(c)(2): Establish mechanisms to authenticate those seeking access to ePHI (addressable).

HIPAA § 164.312(d): Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

HIPAA § 164.312(e)(1): Implement technical security measures to guard against unauthorized access or manipulation to ePHI that is being transmitted over an electronic communications network.

HIPAA § 164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted ePHI is not modified without detection until disposed of (addressable)

HIPAA § 164.312(e)(2)(ii): Establish a mechanism to encrypt ePHI whenever it is deemed appropriate (addressable)

PCI Data Security Standard v3.2 (1/2)

1.1 : Establish and implement firewall and router configuration standards that include the following:

1.1.1 : A formal process for approving and testing all network connections and changes to the firewall and router configurations

1.1.2 : Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks

1.1.3 : Current diagram that shows all cardholder data flows across systems and networks

1.1.4 : Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

1.1.5 : Description of groups, roles, and responsibilities for management of network components

1.1.6 : Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.

1.1.7 : Requirement to review firewall and router rule sets at least every six months

(Continued next page....)

Standards Equivalency Report

User Protection Solution

HITRUST Standard	**Trend Micro Offering (HITRUST Level)**	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 2 of 3)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (1)	GDPR (EU) HIPAA Security Rule **PCI DSS v3.2** **NIST**

PCI Data Security Standard v3.2 (2/2)

1.2 : Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

1.2.2 : Secure and synchronize router configurationfiles.

1.2.3 : Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

1.3 : Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.3.1 : Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2 : Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.3 : Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

1.3.4 : Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

1.3.5 : Permit only “established” connections into the network.

1.3.6 : Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

1.3.7 : Do not disclose private IP addresses and routing information to unauthorized parties.

11.1:Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

11.4: Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises

2.1.1: For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

4.1.1: Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

9.1.3:Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines

National Institute of Standards & Technology (NIST) (1/2)

LEVEL ONE:

NIST Cybersecurity Framework Subsections

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

DE.CM-1: The network is monitored to detect potential cybersecurity events

ID.AM-3: Organizational communication and data flows are mapped

PR.DS-2: Data-in-transit is protected

PR.DS-5: Protections against data leaks are implemented

PR. IP-1:A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

NIST SP 800-53 R4 AC-18: Wireless access

NIST SP 800-53 R4 AC-18(1): Authentication and encryption

NIST SP 800-53 R4 SI-4: Information system monitoring

Standards Equivalency Report

User Protection Solution

HITRUST Standard	**Trend Micro Offering (HITRUST Level)**	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 3 of 3)**	Control Manager (2) Data Loss Prevention (2) Email (1) Endpoint (1)	GDPR (EU) HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (2/2)

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks Subsections

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

PR.AC-5: Network integrity is protected

NIST SP 800-53 R4 AC-17: Remote access

NIST SP 800-53 R4 CA-3: System interconnections

NIST SP 800-53 R4 CM-3: Configuration change control.

NIST SP 800-53 R4 IA-3: Device identification and authentication

NIST SP 800-53 R4 SC-19: Voice over internet protocol

NIST SP 800-53 R4 SC-20: Secure name/address resolution service (authoritative source)

NIST SP 800-53 R4 SC-7: Prevent split tunneling for remote devices

NIST **SP 800-53 R4 SC-7(5):** Deny by default/allow by exception

NIST SP 800-53 R4 SC-8: Transmission confidentiality and integrity

NIST SP 800-53 R4 SC-8(1): Cryptographic or alternate physical protection

NIST SP 800-53 R4 SC-8(2): Pre/post transmission handling

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
09.ab Monitoring System Use *Required for HITRUST v9.1 Certification **(Page 1 of 3)**	Control Manager (3) Data Loss Prevention (3) Email (1) Endpoint (1) Web Security(1)	**HIPAA Security Rule** **PCI DSS v3.2** NIST

HIPAA Security Rule

HIPAA § 164.308(a)(1)(ii)(D): Implement information system activity review(s)

HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)

HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient's role

HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)

HIPAA § 164.308(a)(5)(ii)(B): Implement protection from malicious software (addressable)

HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable)

HIPAA § 164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

PCI Data Security Standard v3.2

10.6: Review logs and security events for all system components to identify anomalies or suspicious activity

10.6.1: Review the following at least daily: All security events Logs of all system components that store, process, or transmit CHD and/or SAD Logs of all critical system components Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/ IPS), authentication servers, e-commerce redirection servers, etc.).

10.6.2: Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.

10.6.3: Follow up exceptions and anomalies identified during the review process.

10.8: Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: Firewalls IDS/IPS FIM Anti-Virus Physical access controls Logical access controls Audit logging mechanisms Segmentation controls (if used)

10.8.1: Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from reoccurring Resuming monitoring of security controls

11.5: Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
09.ab Monitoring System Use *Required for HITRUST v9.1 Certification **(Page 2 of 3)**	Control Manager (3) Data Loss Prevention (3) Email (1) Endpoint (1) Web Security(1)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (1/2)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE. DP-2: Detection activities comply with all applicable requirements

DE. DP-3: Detection processes are tested

DE-AE-3: Event data are collected and correlated from multiple sources and sensors

DE-DP-5: Detection processes are continuously improved

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

DE.AE-2: Detected events are analyzed to understand attack targets and methods

DE.CM-1: The network is monitored to detect potential cybersecurity events

DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

RS.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

NIST SP 800-53 R4 AR-4: Privacy monitoring and auditing

NIST SP 800-53 R4 AU-2: Audit events

NIST SP 800-53 R4 AU-3: Content of audit records

NIST SP 800-53 R4 AU-7: Audit reduction and report generation

NIST SP 800-53 R4 AU-7(1): Automatic processing

NIST **SP 800-53 R4 PE-6:** Monitoring physical access

NIST SP 800-53 R4 SI-4: Information system monitoring

NIST SP 800-53 R4 SI-4(2): Automated tools for real-time analysis

LEVEL THREE (Additional to Two):

NIST Cybersecurity Frameworks

DE.CM-4: Malicious code is detected

NDE.DP-2: Detection activities comply with all applicable requirements

DE. DP-4: Event detection information is communicated

ID.RA-1: Asset vulnerabilities are identified and documented

RS.AN-1: Notifications from detection systems are investigated

RS.CO-2: Incidents are reported consistent with established criteria

(Continued on next page...)

Standards Equivalency Report

User Protection Solution

HITRUST Standard	Trend Micro Offering (HITRUST Level)	Additional Frameworks
09.ab Monitoring System Use *Required for HITRUST v9.1 Certification **(Page 3 of 3)**	Control Manager (3) Data Loss Prevention (3) Email (1) Endpoint (1) Web Security(1)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (2/2)

LEVEL THREE (Cont.):

NIST SP 800-53 R4 AC-2(12): Account monitoring / atypical use

NIST SP 800-53 R4 AU-6: Audit review, analysis, and reporting

NIST SP 800-53 R4 AU-6(1): Process integration

NIST SP 800-53 R4 AU-6(3): Correlate audit repositories

NIST SP 800-53 R4 AU-6(9): Correlation with information from nontechnical sources

NIST SP 800-53 R4 SI-3: Malicious code protection

NIST SP 800-53 R4 SI-4(1): System-wide intrusion detection systems

NIST SP 800-53 R4 SI-4(3): Automated tool integration

NIST SP 800-53 R4 SI-4(4): Inbound and outbound communications traffic

NIST SP 800-53 R4 SI-4(5): System-generated alerts

NIST SP 800-53 R4 SI-7(2): Software, firmware, and information integrity

Standards Equivalency Report

User Protection Solution

HITRUST Standard

10.f Policy on the Use of Cryptographic Controls
*Required for HITRUST v9.1 Certification
(Page 1 of 1)

Trend Micro Offering (HITRUST Level)

Control Manager (2)
Data Loss Prevention (2)

Additional Frameworks

GDPR (EU)
HIPAA Security Rule
PCI DSS v3.2
NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1)(a): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.312(a)(2)(iv): Implement maintenance records (addressable)

HIPAA § 164.312(e)(2)(ii): Establish a mechanism to encrypt ePHI whenever it is deemed appropriate (addressable)

PCI DSS v3.2

3.5.1: Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date Description of the key usage for each key. Inventory of any HSMs and other SCDs used for key management

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks
PR.DS-1: Data-at-rest is protected
PR.DS-2: Data-in-transit is protected
NIST SP 800-53 R4 MP-1: Media protection policy and procedures
NIST SP 800-53 R4 SC-1: System and communications protection policy and procedures
NIST SP 800-53 SC-13: Cryptographic protection

LEVEL TWO (Additional to One):

NIST Cybersecurity Framework
ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

Network Defense Solution

Standards Equivalency Report

September 2018

HITRUST CSF v9.1

EU General Data Protection Regulation (GDPR)

HIPAA Security Rule

HIPAA Breach Notification Rule

PCI Data Security Standard v3.2

National Institute of Standards & Technology (NIST)

Prepared By

MEDITOLOGY
SERVICES

Network Defense Solution

Standards Equivalency Report

PREFACE

This report maps Trend Micro's Network Defense Solution to the HITRUST v9.1 standard, highlighting specific products in the solution and the level (in brackets) relevant under HITRUST v9.1. In addition, where relevant, specific areas under HIPAA, PCI DSS v3.2, GDPR, and multiple NIST frameworks are highlighted for applicability.

For more information on Trend Micro's Network Defense Solution, please visit https://www.trendmicro.com/en_us/business/products/network.html

Network Defense Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
01.v Information Access Restriction *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Control Manager (2) Deep Discovery Analyzer (1) Deep Discovery Inspector (1) TippingPoint IPS (2) Security Mgt. System (2)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a) the pseudonymization and encryption of personal data;

HIPAA Security Rule

HIPAA § 164.308(a)(3)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI for all those permitted within the workforce and prevent those within the workforce who are not permitted to access ePHI.
HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision(addressable)
HIPAA § 164.308(a)(4)(i): Implement HIPAA-compliant policies and procedures for authorizing access to ePHI only when such access is appropriate, based on the user or recipient's role
HIPAA § 164.308(a)(4)(ii)(A): Implement isolating health care clearinghouse functions (required)
HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)
HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)
HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.
HIPAA § 164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)
HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.
HIPAA § 164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
HIPAA § 164.312(a)(2)(iv): Implement maintenance records (addressable)

PCI Data Security Standard v3.2

12.3.10: For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

8.7: All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: All user access to, user queries of, and user actions on databases are through programmatic methods. Only database administrators have the ability to directly access or query databases. Application IDs for database applications can only be used by the applications (and not by individual users or other non- application processes).

Network Defense Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
01.v Information Access Restriction *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Control Manager (2) Deep Discovery Analyzer (2) Deep Discovery Inspector (2) TippingPoint IPS (2) Security Mgt. System (2)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** **NIST**

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

PR.AC-4: Access permissions and authorizations are managed, incorporate the principles of least privilege and separation of duties PR.DS-5: Protections against data leaks are implemented

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

NIST SP 800-53 R4 AC-14: Permitted actions without identification or authentication

NIST SP 800-53 R4 AC-6: Least privilege

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

PR.DS-1: Data-at-rest is protected

NIST SP 800-53 R4 AC-1: Access control policy and procedures

NIST SP 800-53 R4 AC-3: Access enforcement

NIST SP 800-53 R4 DM-1: Minimization of personally identifiable information

NIST SP 800-53 R4 SC-13: Cryptographic protection NIST

SP 800-53 R4 SC-15: Collaborative computing devices

Network Defense Solution

HITRUST Standard

09.j Controls Against Malicious Code
*Required for HITRUST v9.1 Certification
(Page 1 of 1)

Trend Micro Offering (HITRUST level)

Control Manager (2)
Deep Discovery Analyzer (2)
Deep Discovery Inspector (2)
TippingPoint IPS (2)
Security Mgt. System (2)

Additional Frameworks

HIPAA Security Rule
PCI DSS v3.2
NIST

HIPAA Security Rule

HIPAA § 164.308(a)(5)(i): Provide for appropriate authorization and supervision of workforce members who work with ePHI and train all workforce members regarding security policies and procedures.
HIPAA § 164.308(a)(5)(ii)(B): Implement protection from malicious software (addressable)

PCI Data Security Standard v3.2

5.1: Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
5.1.1: Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
5.1.2: For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.
5.2: Ensure that all anti-virus mechanisms are maintained as follows: Are kept current, perform periodic scans Generate audit logs which are retained per PCI DSS Requirement 10.7.
5.3: Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

National Institute of Standards & Technology (NIST)

LEVEL ONE:
NIST Cybersecurity Frameworks
DE.CM-4: Malicious code is detected
PR.AC-4: Access permissions and authorizations are managed, incorporate the principles of least privilege and separation of duties
PR.AT-1: All users are informed and trained
NIST SP 800-53 R4 CM-11: User-installed software
NIST SP 800-53 R4 SI-3: Malicious code protection

LEVEL TWO (Additional to One):
NIST SP 800-53 R4 SC-2: Application partitioning
NIST SP 800-53 R4 SI-16: Memory protection
NIST SP 800-53 R4 SI-3(1): Malicious code central management
NIST SP 800-53 R4 SI-3(2): Malicious code automatic updates
NIST SP 800-53 R4 SI-8: Spam protection
NIST SP 800-53 R4 SI-8(1): Spam protection central management
NIST SP 800-53 R4 SI-8(2): Spam protection automatic updates

Network Defense Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.k Controls Against Mobile Code *Required for HITRUST v9.1 Certification **(Page 1 of 1)**	Control Manager (2) Deep Discovery Analyzer (1) Deep Discovery Inspector (1) TippingPoint IPS (2) Security Mgt. System (2)	**HIPAA Security Rule** **NIST**

HIPAA Security Rule

HIPAA § 164.308(a)(5)(ii)(B): Implement protection from malicious software (addressable)

National Institute of Standards & Technology (NIST)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.CM-4: Malicious code is detected

DE.CM-5: Unauthorized mobile code is detected

NIST SP 800-53 R4 SC-18: Mobile code

NIST SP 800-53 R4 Si-3: Malicious code protection

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

PR.DS-7: The development and testing environment(s) are separate from the production environment

NIST SP 800-53 R4 CM-2(6): Development and test environments

NIST SP 800-53 R4 CM-3: Configuration change control

NIST SP 800-53 R4 SC-18(3): Prevent downloading/execution

NIST SP 800-53 R4 SC-2: Application partitioning

NIST SP 800-53 R4 SC-3: Security function isolation

Network Defense Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 1 of 3)**	Control Manager (2) Deep DiscoveryAnalyzer(1) Deep Discovery Inspector(1) TippingPointIPS(2) Security Mgt. System (2)	**GDPR (EU)** **HIPAA Security Rule** **PCI DSS v3.2** NIST

EU General Data Protection Regulation (GDPR)

GDPR Article 32(1)(a): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymization and encryption of personal data;

GDPR Article 32(1)(b): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

HIPAA Security Rule

HIPAA § 164.312(c)(1): Implement policies and procedures to protect ePHI from alteration or destruction in an unauthorized manner.
HIPAA § 164.312(c)(2): Establish mechanisms to authenticate those seeking access to ePHI (addressable).
HIPAA § 164.312(d): Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
HIPAA § 164.312(e)(1): Implement technical security measures to guard against unauthorized access or manipulation to ePHI that is being transmitted over an electronic communications network.
HIPAA § 164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted ePHI is not modified without detection until disposed of (addressable)
HIPAA § 164.312(e)(2)(ii): Establish a mechanism to encrypt ePHI whenever it is deemed appropriate (addressable)

PCI Data Security Standard v3.2 (1/2)

1.1: Establish and implement firewall and router configuration standards that include the following:
1.1.1: A formal process for approving and testing all network connections and changes to the firewall and router configurations
1.1.2: Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
1.1.3: Current diagram that shows all cardholder data flows across systems and networks
1.1.4: Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
1.1.5: Description of groups, roles, and responsibilities for management of network components
1.1.6: Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
1.1.7: Requirement to review firewall and router rule sets at least every six months

(Continued next page....)

Network Defense Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 2 of 3)**	Control Manager (2) Deep DiscoveryAnalyzer(1) Deep Discovery Inspector(1) TippingPointIPS(2) Security Mgt. System (2)	GDPR (EU) HIPAA Security Rule **PCI DSS v3.2** **NIST**

PCI Data Security Standard v3.2 (2/2)

1.2: Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

1.2.2: Secure and synchronize router configuration files.

1.2.3: Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

1.3: Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.3.1: Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2: Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.3: Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

1.3.4: Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.

1.3.5: Permit only “established” connections into the network.

1.3.6: Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

1.3.7: Do not disclose private IP addresses and routing information to unauthorized parties.

11.1: Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

11.4: Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises

2.1.1: For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

4.1.1: Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

9.1.3: Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines

National Institute of Standards & Technology (NIST) (1/2)

LEVEL ONE:

NIST Cybersecurity Frameworks

DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed. DE.CM-1: The network is monitored to detect potential cybersecurity events

ID.AM-3: Organizational communication and data flows are mapped

PR.DS-2: Data-in-transit is protected

PR.DS-5: Protections against data leaks are implemented

PR. IP-1:A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

NIST SP 800-53 R4 AC-18: Wireless access

NIST SP 800-53 R4 AC-18(1): Authentication and encryption

NIST SP 800-53 R4 SI-4: Information system monitoring

Network Defense Solution

HITRUST Standard

09.m Network Controls
*Required for HITRUST v9.1 Certification
(Page 3 of 3)

Trend Micro Offering (HITRUST level)

Control Manager (2)
Deep Discovery Analyzer (1)
Deep Discovery Inspector (1)
TippingPoint IPS (2)
Security Mgt. System (2)

Additional Frameworks

GDPR (EU)
HIPAA Security Rule
PCI DSS v3.2
NIST

National Institute of Standards & Technology (NIST) (2/2)

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-5: Network integrity is protected
NIST SP 800-53 R4 AC-17: Remote access
NIST SP 800-53 R4 CA-3: System interconnections
NIST SP 800-53 R4 CM-3: Configuration change control
NIST SP 800-53 R4 IA-3: Device identification and authentication
NIST SP 800-53 R4 SC-19: Voice over internet protocol
NIST SP 800-53 R4 SC-20: Secure name/address resolution service (authoritative source)
NIST SP 800-53 R4 SC-7: Prevent split tunneling for remote devices
NIST SP 800-53 R4 SC-7(5): Deny by default/allow by exception
NIST SP 800-53 R4 SC-8: Transmission confidentiality and integrity
NIST SP 800-53 R4 SC-8(1): Cryptographic or alternate physical protection
NIST SP 800-53 R4 SC-8(2): Pre/post transmission handling

Network Defense Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
10.m Control of Technical Vulnerabilities *Required for HITRUST v9.1 Certification **(Page 1 of 2)**	Control Manager (2) Deep Discovery Analyzer (3) Deep Discovery Inspector(3) TippingPoint IPS(3) Security Mgt. System (3)	**HIPAA Security Rule** **PCI DSS v3.2** NIST

HIPAA Security Rule

HIPAA § 164.308(a)(8): Perform a periodic assessment of how well the data center's security policies and procedures meet the requirements of the Security Rule.

PCI Data Security Standard v3.2

11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

11.2.1: Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.

11.2.2: Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

11.2.3: Qualified personnel perform internal and external scans, and rescans as needed, after any significant change.

11.3: Implement a methodology for penetration testing that includes the following: Is based on industry-accepted penetration testing approaches (for example, NIST SP 800- 115) Includes coverage for the entire CDE perimeter and critical systems Includes testing from both inside and outside the network Includes testing to validate any segmentation and scope-reduction controls Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 Defines network-layer penetration tests to include components that support network functions as well as operating systems Includes review and consideration of threats and vulnerabilities experienced in the last 12 months Specifies retention of penetration testing results and remediation activities results.

11.3.1: Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.2: Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

11.3.3: Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.

11.3.4: If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/ methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

11.3.4.1: For service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.

2.2: Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry accepted system hardening standards.

2.2.2: Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

2.2.3: Implement additional security features for any required services, protocols, or daemons that are insecure

6.1: Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as high, medium, or low) to newly discovered security vulnerabilities.

6.2: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release

6.4.5: Change control procedures must include the following:

6.4.5.1: Documentation of impact.

6.4.5.2: Documented change approval by authorized parties.

6.4.5.3: Functionality testing to verify that the change does not adversely impact the security of the system.

6.4.5.4: Back-out procedures.

Network Defense Solution

HITRUST Standard	Trend Micro Offering (HITRUST level)	Additional Frameworks
10.m Control of Technical Vulnerabilities *Required for HITRUST v9.1 Certification **(Page 2 of 2)**	Control Manager (2) Deep Discovery Analyzer (3) Deep Discovery Inspector(3) TippingPoint IPS(3) Security Mgt. System (3)	HIPAA Security Rule PCI DSS v3.2 **NIST**

National Institute of Standards & Technology (NIST) (2/2)

LEVEL ONE:

NIST Cybersecurity Frameworks

ID.RA-1: Asset vulnerabilities are identified and documented

ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources

ID.RA-4: Potential business impacts and likelihoods are identified

ID.RA-6: Risk responses are identified and prioritized

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

NIST SP 800-53 R4 RA-5: Vulnerability scanning

LEVEL TWO (Additional to One):

NIST Cybersecurity Frameworks

DE.CM-8: Vulnerability scans are performed

DE. DP-5: Detection processes are continuously improved

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk

PR. IP-12: A vulnerability management plan is developed and implemented

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

RS.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

NIST SP 800-53 R4 CM-6: External service provider activity is monitored to detect potential cybersecurity events

NIST SP 800-53 R4 CM-7: Least functionality

NIST SP 800-53 R4 SI-5: Security alerts, advisories, and directives

LEVEL THREE (Additional to Two):

NIST Cybersecurity Frameworks

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

NIST SP 800-53 R4 CA-2: Security assessments

NIST SP 800-53 R4 CA-7: Continuous monitoring

NIST SP 800-53 R4 CA-8: Penetration testing

NIST SP 800-53 R4 RA-5(1): Update tool capability

NIST SP 800-53 R4 RA-5(2): Update by frequency / prior to new scan / when identified

NIST SP 800-53 R4 RA-5(4): Discoverable information

NIST SP 800-53 R4 RA-5(5): Privileged access

NIST SP 800-53 R4 SI-2: Flaw remediations

NIST SP 800-53 R4 SI-2(1): Central management

NIST SP 800-53 R4 SI-2(2): Automated flaw remediation status