



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



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

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">01.c Privilege Management *Required for HITRUST v9.1 Certification (Page 1 of 2)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (3) Smart Check (2) Server Protect for Storage (2) Control Manager (1)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">HIPAA Security Rule PCI DSS v3.2 NIST</p>
---	---	---

HIPAA Security Rule
<p>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.</p> <p>HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)</p> <p>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</p> <p>HIPAA § 164.308(a)(4)(ii)(A): Implement isolating health care clearinghouse functions (required)</p> <p>HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)</p> <p>HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)</p> <p>HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable)</p> <p>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)</p> <p>HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.</p> <p>HIPAA § 164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.</p>

PCI Data Security Standard v3.2
<p>7.1: Limit access to system components and cardholder data to only those individuals whose job requires such access</p> <p>7.1.1: Define access needs for each role</p> <p>7.1.2: Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities</p> <p>7.1.3: Assign access based on individual personnel's job classification and function.</p> <p>7.1.4: Require documented approval by authorized parties specifying required privileges</p> <p>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.</p> <p>7.2.1: Access control system must include coverage of all system components</p> <p>7.2.2: Access control system must include assignment of privileges to individuals based on job classification and function</p> <p>7.2.3: Access control system must include default "deny-all" setting</p> <p>A.1.1: Ensure that each entity only runs processes that have access to that entity's cardholder data environment.</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">01.c.Privilege Management *Required for HITRUST v9.1 Certification (Page 2 of 2)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (3) Smart Check (2) Server Protect for Storage (2) Control Manager (1)</p>	<p style="text-align: center;"><u>Additional Frameworks</u></p> <p style="text-align: center;">HIPAA Security Rule PCI DSS v3.2 NIST</p>
---	---	--

National Institute of Standards & Technology (NIST) (2/2)
<p>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</p> <p>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.</p> <p>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</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">01.I Remote Diagnostic and Configuration Port Protection *Required for HITRUST v9.1 Certification (Page 1 of 1)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (3)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">HIPAA Security Rule NIST</p>
--	---	--

<p style="text-align: center;">HIPAA Security Rule</p> <p>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.</p>
--

<p style="text-align: center;">National Institute of Standards & Technology (NIST) (2/2)</p> <p>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</p> <p>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</p> <p>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</p>
--

Standards Equivalency Report

Hybrid Cloud Security Solution

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

EU General Data Protection Regulation (GDPR)
<p>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;</p>

HIPAA Security Rule
<p>HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.</p>

PCI DSS v3.2 Subsection
<p>1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.</p>

National Institute of Standards & Technology (NIST)
<p>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</p> <p>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</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">01.v Information Access Restriction *Required for HITRUST v9.1 Certification (Page 1 of 2)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (1) Smart Check (1) Server Protect for Storage (1) Control Manager (2)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">GDPR (EU) HIPAA Security Rule PCI DSS v3.2 NIST</p>
---	---	---

<p>EU General Data Protection Regulation (GDPR)</p>
<p>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:</p> <p>(a) the pseudonymization and encryption of personal data;</p>

<p>HIPAA Security Rule</p>
<p>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)</p> <p>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</p> <p>HIPAA § 164.308(a)(4)(ii)(A): Implement isolating health care clearinghouse functions (required)</p> <p>HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)</p> <p>HIPAA § 164.308(a)(4)(ii)(C): Implement access establishment and modification (addressable)</p> <p>HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.</p> <p>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)</p> <p>HIPAA § 164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.</p> <p>HIPAA § 164.312(a)(2)(ii): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.</p> <p>HIPAA § 164.312(a)(2)(iv): Implement maintenance records (addressable)</p>

<p>PCI Data Security Standard v3.2</p>
<p>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.</p> <p>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).</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

National Institute of Standards & Technology (NIST)
<p>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</p> <p>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</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p>06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification (Page 1 of 3)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Control Manager (2)</p>	<p style="text-align: center;"><u>Additional Frameworks</u></p> <p style="text-align: center;">GDPR (EU) PCI DSS v3.2 NIST</p>
---	--	--

EU General Data Protection Regulation (GDPR) (1/2)
<p>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</p> <p>GDPR Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')</p> <p>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.</p> <p>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.</p> <p>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</p> <p>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.</p> <p>GDPR Article 27(1): Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.</p> <p>GDPR Article 27(2): The obligation laid down in paragraph 1 of this Article shall not apply to: GDPR 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.</p> <p>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.</p> <p>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.</p> <p>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</p> <p>GDPR Article 37(1): The controller and the processor shall designate a data protection officer in any case where: GDPR 37.1A/B/C</p> <p>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.</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p>06.d Data Protection and Privacy of Covered Information *Required for HITRUST v9.1 Certification (Page 2 of 3)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Control Manager (2)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">GDPR (EU) PCI DSS v3.2 NIST</p>
---	--	---

EU General Data Protection Regulation (GDPR) (2/2)
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>GDPR Article 39(1): The data protection officer shall have at least the following tasks: (GPDRA 39.1.A/B/C/D/E)</p> <p>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.</p>

PCI Data Security Standard v3.2
<p>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.</p> <p>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.</p> <p>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</p>

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)
<p>LEVEL ONE:</p> <p>NIST Cybersecurity Frameworks</p> <p>ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p> <p>PR.DS-1: Data-at-rest is protected</p> <p>PR.DS-2: Data-in-transit is protected</p> <p>NIST SP 800-53 R4 AR-1: Governance and privacy program</p> <p>NIST SP 800-53 R4 AR-2: Privacy impact and risk assessment</p> <p>NIST SP 800-53 R4 SC-12(1): Cryptographic key establishment and management availability</p> <p>NIST SP 800-53 R4 SC-28: Protection of information at rest</p> <p>NIST SP 800-53 R4 SC-28(1): Cryptographic protection</p> <p>LEVEL TWO (Additional to One):</p> <p>NIST SP 800-53 R4 SI-12: Information handling and retention</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

HIPAA Security Rule
<p>HIPAA § 164.308(a)(1)(ii)(D): Implement information system activity review(s)</p> <p>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.</p> <p>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.</p>

PCI Data Security Standard v3.2
<p>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</p> <p>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</p>

National Institute of Standards & Technology (NIST)
<p>LEVEL ONE:</p> <p>NIST Cybersecurity Frameworks</p> <p>DE. DP-1: Roles and responsibilities for detection are well defined to ensure accountability</p> <p>DE. DP-4: Event detection information is communicated</p> <p>ID.RA-6: Risk responses are identified and prioritized</p> <p>NIST SP 800-53 R4 AR-4: Privacy monitoring and auditing</p> <p>LEVEL TWO (Additional to One)</p> <p>NIST Cybersecurity Frameworks</p> <p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</p> <p>NIST SP 800-53 R4 CA-1: Security assessments and authorization policies and procedures</p> <p>NIST SP 800-53 R4 CA-7: Continuous monitoring</p> <p>NIST SP 800-53 R4 CA-7(1): Independent assessments</p> <p>NIST SP 800-53 R4 RA-5: Vulnerability scanning</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">06.h Technical Compliance Checking *Required for HITRUST v9.1 Certification (Page 1 of 1)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Smart Check (2) Server Protect for Storage (1) Control Manager (2)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">HIPAA Security Rule NIST</p>
--	---	--

<p style="text-align: center;">HIPAA Security Rule</p> <p>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.</p>
--

<p style="text-align: center;">National Institute of Standards & Technology (NIST)</p> <p>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</p> <p>LEVEL TWO (Additional to One): NIST SP 800-53 R4 CA-2(2): Specialized assessments NIST SP 800-53 R4 CA-7: Continuous monitoring</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">08.b Physical Entry Controls *Required for HITRUST v9.1 Certification (Page 1 of 2)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (2)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">HIPAA Security Rule PCI DSS v3.2 NIST</p>
--	---	---

<p>HIPAA Security Rule</p>
<p>HIPAA § 164.310(a)(1): Limit physical access to the data center facilities while ensuring that authorized access is allowed.</p> <p>HIPAA § 164.310(a)(2)(iii): Implement access control and validation procedures (addressable)</p> <p>HIPAA § 164.310(b): Implement policies and procedures to specify proper use of, and access to, workstations and electronic media.</p> <p>HIPAA § 164.310(C): Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.</p>

<p>PCI Data Security Standard v3.2</p>
<p>9.1: Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment</p> <p>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).</p> <p>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.</p> <p>9.4: Implement procedures to identify and authorize visitors.</p> <p>9.4.1: Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.</p> <p>9.4.2: Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.</p> <p>9.4.3: Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.</p> <p>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</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

National Institute of Standards & Technology (NIST) (2/2)
<p>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</p> <p>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</p>

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

National Institute of Standards & Technology (NIST)
<p>LEVEL ONE:</p> <p>NIST Cybersecurity Frameworks</p> <p>PR. IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met</p> <p>NIST SP 800-53 R4 PE-1: Physical and environmental protection policy and procedures</p> <p>NIST SP 800-53 R4 PE-13: Fire protection</p> <p>NIST SP 800-53 R4 PE-13(1): Detection devices/systems</p> <p>LEVEL TWO (Additional to One):</p> <p>NIST SP 800-53 R4 AT-3(1): Role-based security training; environmental controls</p> <p>NIST SP 800-53 R4 PE-13(3): Automatic fire suppression</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">09.n Security of Network Services *Required for HITRUST v9.1 Certification (Page 1 of 1)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Smart Check (2) Server Protect for Storage (2) Control Manager (2)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">HIPAA Security Rule NIST</p>
---	---	--

<p style="text-align: center;">HIPAA Security Rule</p> <p>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.</p> <p>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).</p> <p>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.</p> <p>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;</p>

<p style="text-align: center;">National Institute of Standards & Technology (NIST)</p> <p>LEVEL ONE</p> <p>NIST Cybersecurity Frameworks</p> <p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p> <p>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</p> <p>ID.AM-4: External information systems are catalogued Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established</p> <p>PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities</p> <p>PR.PT-4: Communications and control networks are protected</p> <p>NIST SP 800-53 R4 CA-3: System interconnections</p> <p>NIST SP 800-53 R4 SA-9: External information system services</p> <p>LEVEL TWO (Additional to One)</p> <p>NIST Cybersecurity Frameworks</p> <p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p> <p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</p> <p>ID.AM-3: Organizational communication and data flows are mapped</p> <p>ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.</p> <p>NIST SP 800-53 R4 CA-3(5): Restrictions on external system connections</p> <p>NIST SP 800-53 R4 SA-9(2): Identification of functions/ports/protocols/services</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">09.m Network Controls *Required for HITRUST v9.1 Certification (Page 1 of 3)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Smart Check (1) Server Protect for Storage (1) Control Manager (2)</p>	<p style="text-align: center;"><u>Additional Frameworks</u></p> <p style="text-align: center;">GDPR (EU) HIPAA Security Rule PCI DSS v3.2 NIST</p>
---	---	--

EU General Data Protection Regulation (GDPR)
<p>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;</p> <p>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;</p>

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

PCI Data Security Standard v3.2 (1/2)
<p>1.1: Establish and implement firewall and router configuration standards that include the following:</p> <p>1.1.1: A formal process for approving and testing all network connections and changes to the firewall and router configurations</p> <p>1.1.2: Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks</p> <p>1.1.3: Current diagram that shows all cardholder data flows across systems and networks</p> <p>1.1.4: Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone</p> <p>1.1.5: Description of groups, roles, and responsibilities for management of network components</p> <p>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.</p> <p>1.1.7: Requirement to review firewall and router rule sets at least every six months</p> <p>(Continued next page....)</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">09.m Network Controls *Required for HITRUST v9.1 Certification (Page 2 of 3)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (2) Smart Check (1) Server Protect for Storage (1) Control Manager (2)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">GDPR (EU) HIPAA Security Rule PCI DSS v3.2 NIST</p>
---	---	---

PCI Data Security Standard v3.2 (2/2)
<p>1.2: Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.</p> <p>1.2.2: Secure and synchronize router configuration files.</p> <p>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.</p> <p>1.3: Prohibit direct public access between the Internet and any system component in the cardholder data environment.</p> <p>1.3.1: Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.</p> <p>1.3.2: Limit inbound Internet traffic to IP addresses within the DMZ.</p> <p>1.3.3: Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.</p> <p>1.3.4: Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.</p> <p>1.3.5: Permit only "established" connections into the network.</p> <p>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.</p> <p>1.3.7: Do not disclose private IP addresses and routing information to unauthorized parties.</p> <p>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.</p> <p>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</p> <p>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.</p> <p>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.</p> <p>9.1.3: Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines</p>

National Institute of Standards & Technology (NIST) (1/2)
<p>LEVEL ONE:</p> <p>NIST Cybersecurity Frameworks</p> <p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p> <p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p> <p>ID.AM-3: Organizational communication and data flows are mapped</p> <p>PR.DS-2: Data-in-transit is protected</p> <p>PR.DS-5: Protections against data leaks are implemented</p> <p>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)</p> <p>NIST SP 800-53 R4 AC-18: Wireless access</p> <p>NIST SP 800-53 R4 AC-18(1): Authentication and encryption</p> <p>NIST SP 800-53 R4 SI-4: Information system monitoring</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

National Institute of Standards & Technology (NIST) (2/2)
<p>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</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

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

National Institute of Standards & Technology (NIST)
<p>LEVEL ONE:</p> <p>NIST Cybersecurity Framework</p> <p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p> <p>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</p> <p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p> <p>NIST SP 800-53 R4 AR-4: Privacy monitoring and auditing</p> <p>NIST SP 800-53 R4 AU-11: Audit record retention</p> <p>NIST SP 800-53 R4 AU-3: Content of audit records</p> <p>NIST SP 800-53 R4 AU-8: Time stamps</p> <p>NIST SP 800-53 R4 AU-9: Protection of audit information</p> <p>LEVEL TWO (Additional to One):</p> <p>NIST Cybersecurity Frameworks</p> <p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p> <p>NIST SP 800-53 R4 AC-6(9): Auditing use of privileged functions</p> <p>NIST SP 800-53 R4 AU-2: Audit events</p> <p>NIST SP 800-53 R4 AU-2(3): Review and updates</p> <p>NIST SP 800-53 R4 AU-5: Response to audit processing failures</p> <p>NIST SP 800-53 R4 AU-5(4): Shutdown on failure</p> <p>NIST SP 800-53 R4 AU-9(4): Access by subset of privileged users</p> <p>NIST SP 800-53 R4 AU-9(5): Dual authorization</p> <p>LEVEL THREE (Additional to Two):</p> <p>NIST SP 800-53 R4 AC-2(4): Automated audit actions</p> <p>NIST SP 800-53 R4 AU-3(1): Additional audit information</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">09.ab Monitoring System Use *Required for HITRUST v9.1 Certification (Page 1 of 3)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">HIPAA Security Rule PCI DSS v3.2 NIST</p>
---	---	---

HIPAA Security Rule
<p>HIPAA § 164.308(a)(1)(ii)(D): Implement information system activity review(s)</p> <p>HIPAA § 164.308(a)(3)(ii)(A): Implement authorization and/or supervision (addressable)</p> <p>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</p> <p>HIPAA § 164.308(a)(4)(ii)(B): Implement access authorization (addressable)</p> <p>HIPAA § 164.308(a)(5)(ii)(B): Implement protection from malicious software (addressable)</p> <p>HIPAA § 164.308(a)(5)(ii)(C): Implement log-in monitoring (addressable)</p> <p>HIPAA § 164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.</p>

PCI Data Security Standard v3.2
<p>10.6: Review logs and security events for all system components to identify anomalies or suspicious activity.</p> <p>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.).</p> <p>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.</p> <p>10.6.3: Follow up exceptions and anomalies identified during the review process.</p> <p>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)</p> <p>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</p> <p>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</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

National Institute of Standards & Technology (NIST) (1/2)
<p>LEVEL ONE:</p> <p>NIST Cybersecurity Frameworks</p> <p>DE. DP-2: Detection activities comply with all applicable requirements</p> <p>DE. DP-3: Detection processes are tested</p> <p>DE-AE-3: Event data are collected and correlated from multiple sources and sensors</p> <p>DE-DP-5: Detection processes are continuously improved</p> <p>ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed</p> <p>LEVEL TWO (Additional to One)</p> <p>NIST Cybersecurity Frameworks</p> <p>DE.AE-2: Detected events are analyzed to understand attack targets and methods</p> <p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p> <p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</p> <p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p> <p>RS.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams</p> <p>NIST SP 800-53 R4 AR-4: Privacy monitoring and auditing</p> <p>NIST SP 800-53 R4 AU-2: Audit events</p> <p>NIST SP 800-53 R4 AU-3: Content of audit records</p> <p>NIST SP 800-53 R4 AU-7: Audit reduction and report generation</p> <p>NIST SP 800-53 R4 AU-7(1): Automatic processing</p> <p>NIST SP 800-53 R4 PE-6: Monitoring physical access</p> <p>NIST SP 800-53 R4 SI-4: Information system monitoring</p> <p>NIST SP 800-53 R4 SI-4(2): Automated tools for real-time analysis</p> <p>LEVEL THREE (Additional to Two)</p> <p>NIST Cybersecurity Frameworks</p> <p>DE.CM-4: Malicious code is detected</p> <p>NDE.DP-2: Detection activities comply with all applicable requirements</p> <p>DE. DP-4: Event detection information is communicated</p> <p>ID.RA-1: Asset vulnerabilities are identified and documented</p> <p>RS.AN-1: Notifications from detection systems are investigated</p> <p>RS.CO-2: Incidents are reported consistent with established criteria</p> <p>(Continued on next page...)</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

National Institute of Standards & Technology (NIST) (2/2)
<p>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</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p style="text-align: center;">10.m Control of Technical Vulnerabilities *Required for HITRUST v9.1 Certification (Page 1 of 2)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p style="text-align: center;">Deep Security (3) Smart Check (2) Server Protect for Storage (3) Control Manager (2)</p>	<p style="text-align: center;">Additional Frameworks</p> <p style="text-align: center;">HIPAA Security Rule PCI DSS v3.2 NIST</p>
--	--	--

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
<p>11.2: Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.</p> <p>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.</p> <p>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.</p> <p>11.2.3: Qualified personnel perform internal and external scans, and rescans as needed, after any significant change.</p> <p>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.</p> <p>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).</p> <p>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).</p> <p>11.3.3: Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>2.2.2: Enable only necessary services, protocols, daemons, etc., as required for the function of the system.</p> <p>2.2.3: Implement additional security features for any required services, protocols, or daemons that are considered to be insecure</p> <p>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.</p> <p>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</p> <p>6.4.5: Change control procedures must include the following:</p> <p>6.4.5.1: Documentation of impact.</p> <p>6.4.5.2: Documented change approval by authorized parties.</p> <p>6.4.5.3: Functionality testing to verify that the change does not adversely impact the security of the system.</p> <p>6.4.5.4: Back-out procedures.</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

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

National Institute of Standards & Technology (NIST)
<p>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</p> <p>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</p> <p>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</p>

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)
<p>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.</p> <p>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</p> <p>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;</p>

HIPAA Security Rule
<p>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</p> <p>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).</p> <p>HIPAA § 164.308(a)(8): Evaluation</p> <p>HIPAA § 164.312(a)(2)(ii): Emergency access procedure (required)</p> <p>HIPAA § 164.316(b)(1): Standard: documentation</p> <p>HIPAA § 164.316(b)(2)(iii): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.</p>

Standards Equivalency Report

Hybrid Cloud Security Solution

<p style="text-align: center;">HITRUST Standard</p> <p>00.a Information Security Management Program *Required for HITRUST v9.1 Certification (Page 2 of 2)</p>	<p style="text-align: center;">Trend Micro Offering (HITRUST level)</p> <p>Deep Security (3) Smart Check (3) Server Protect for Storage (3) Control Manager (3)</p>	<p style="text-align: center;">Additional Frameworks</p> <p>GDPR (EU) HIPAA Security Rule NIST</p>
--	---	--

National Institute of Standards & Technology (NIST)
<p>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.</p> <p>LEVEL TWO (Additional to One): NIST Cybersecurity Frameworks PR. IP-7: Protection processes are improved</p> <p>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</p>