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

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	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) Deep Discovery Analyzer (2) Deep Discovery Inspector (2) TippingPoint IPS (2) Security Mgt. System (2)	**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 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)(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 Discovery Analyzer (1) Deep Discovery Inspector (1) TippingPoint IPS (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	Trend Micro Offering (HITRUST level)	Additional Frameworks
09.m Network Controls *Required for HITRUST v9.1 Certification **(Page 3 of 3)**	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**

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