Trend Micro Healthcare Compliance Solutions

How Trend Micro's innovative security solutions help healthcare organizations address risk and compliance challenges.

Deep Security

"Advanced protection for systems in the dynamic datacenter—from virtual desktops to physical, virtual or cloud servers."

Overview of Features

Deep Security is a platform for server security, combining a bi-directional stateful firewall with intrusion detection and prevention, web application protection, integrity monitoring, log inspection, and agentless anti-malware. Collectively these security modules within Deep Security provide a comprehensive solution set for data centers and hosting environments.

Agentless Anti-malware

The agentless anti-malware module, developed in conjunction with VMware, allows for agentless anti-malware protection delivered as a virtual appliance. The virtual appliance hooks into the other virtual machines running, offering the same protection expected from a traditional agent but with a lower cost of ownership and increased performance.

From a resource perspective, agentless anti-malware requires fewer CPU cycles and less RAM than traditional agents. Because an agent is not being installed on every piece of hardware, it is also easier to manage and maintain, offering both real and opportunity cost savings.

Agentless anti-malware also offers enhanced security over traditional agents. By isolating the anti-malware from where the malware resides—the virtual machines which are the targets—malware is limited in terms of what it can do to modify or prevent the anti-malware from doing its job. The segregation in virtual machines prevents root access for instance which may block anti-malware in more traditional implementations.

Generally speaking, the functionality of this type of anti-malware is similar to that of anti-malware deployed as an agent. Deep Security protects against malicious code by using malware signatures to ensure the machine is free from malware. Trend Micro is able to differentiate itself however by leveraging the threat intelligence in the cloud provided by the Smart Protection Network. Each virtual appliance and implementation of Deep Security's anti-malware module acts as a conduit, benefiting from the massive amount of analytics, intelligence, and processing capabilities of Trend Micro's network to protect organizations. New signatures and general updates can also be pushed more rapidly and with greater ease.

Deep Packet Inspection

Deep Packet Inspection is an important module within Deep Security in that it is itself an overarching solution with sub-modules which provide protection: intrusion detection and prevention, web application protection, application control, and a bidirectional stateful firewall. Deep Packet Inspection is similarly offered as a virtual appliance like the anti-malware module; however DPI may also be deployed as a traditional agent on its own or in tandem with the virtual appliance. The hybrid model of deployment provides even greater security and protection by providing coverage on virtual machines where an agent doesn't exist and providing insurance in the event an agent fails or is attacked, allowing for the virtual appliance to step in and provide coverage.

Intrusion Detection and Prevention

Anti-malware is a fundamental protection all organizations should implement for both servers and end user devices. However, anti-malware is restricted in that it largely needs to know about a virus to protect against it. Many viruses now are zero day, meaning they are out in the wild before organizations and professionals know about it and can protect against it with anti-malware signatures. This leaves a window of opportunity for the malware and a window of vulnerability for the organization.

Intrusion Detection and Prevention (IDS / IPS) provides network based protection for potential OS and application vulnerabilities. IDS / IPS works by looking at the underlying vulnerability that malware would attack, thus preventing malicious attempts from penetrating machines and offers specific rules which inspect the network for malicious patterns. This first layer of protection is the firewall—it locks down the system by limiting the incoming and outgoing traffic type, direction and state. Building off of this, the packet itself is also analyzed, evaluating the header and body to determine if there is any evidence of malicious intent, looking for things like protocol anomalies which indicate malicious modification to evade traditional detection systems. IDS / IPS also provides virtual patching of vulnerabilities. As described above, zero day attacks are increasing in prevalence, making it difficult to secure a system before a patch is available, and in many cases patches for legacy systems never become available. Medical devices are prime examples of this issue as the hospitals and system administrators are often not allowed to make any updates to the underlying operating system. Other systems may be patchable however the IT administrators have a near impossible time deploying the patches due to the high availability requirements of the device as needed by the physicians to administer care. IDS / IPS addresses these issues because it can filter the malicious packets before they can exploit a system.

Web Application Protection

The Web Application Protection module of Deep Security works to block attacks against web application vulnerabilities, for example cross-site scripting and SQL injection. According to Verizon's 2011 Data Breach Investigations Report, SQL injection accounted for 14% of breaches and 24% of breached records in 2010. SQL injection also represents one of the most common means of malware infecting a system initially.[1]

[1] "2011 Data Breach Investigations Report", Verizon Business, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

WAP similarly analyzes the packets coming into the application to identify patterns which are indicative of malicious activities. For instance, if there is a web application with an input form that does not properly validate what is entered, a hacker can exploit the application by entering actual SQL code. This befuddles the application into executing commands on the database which, if done correctly, could return sensitive information stored by the database. WAP checks the packets and commands to verify the input is valid, preventing privileged access to the application, operating system, and data.

Application Control

Application Control is the third pillar of Deep Packet Inspection. AC prevents unwanted applications from running and communicating on the organization's network. This provides both security protections and allows for better management of employee productivity. For example, if an organization wants to prevent all peer to peer (P2P) applications from running, AC is able to determine if any communications are part of the P2P application, subsequently blocking all of those communications. In a 2009 study by Dartmouth[2], documents posted on P2P networks were recovered for all ten of the top publicly traded healthcare firms. In one instance, a hospital system was leaking a spreadsheet with 82 pieces of health information on each of its 20,000 patients.

Out of the box, Trend Micro provides policies and rules to prevent common and known malicious and unproductive applications. Organizations can further customize this list for their environment to account for applications specific to them.

Integrity Monitoring

Integrity Monitoring detects attempts to make changes to critical system files and can report those changes real-time. Trend Micro provides rules and policies for a pre-specified list of files and folders, constantly monitoring and maintaining an audit trail of when the access occurred and what attributes were modified. Since rules and regulations vary by organization, the product offers the ability to tag events manually or automatically monitor against similar events. It can also work with syslog and popular SIEM products to further archive and aggregate events for further analysis.

Integrity Monitoring is implemented and operates as an agent on each physical or virtual machine. Deep Security is capable of providing integrity monitoring recommendations based on the operating system and applications installed, which streamlines the workflow in enterprise environments.

Log Inspection

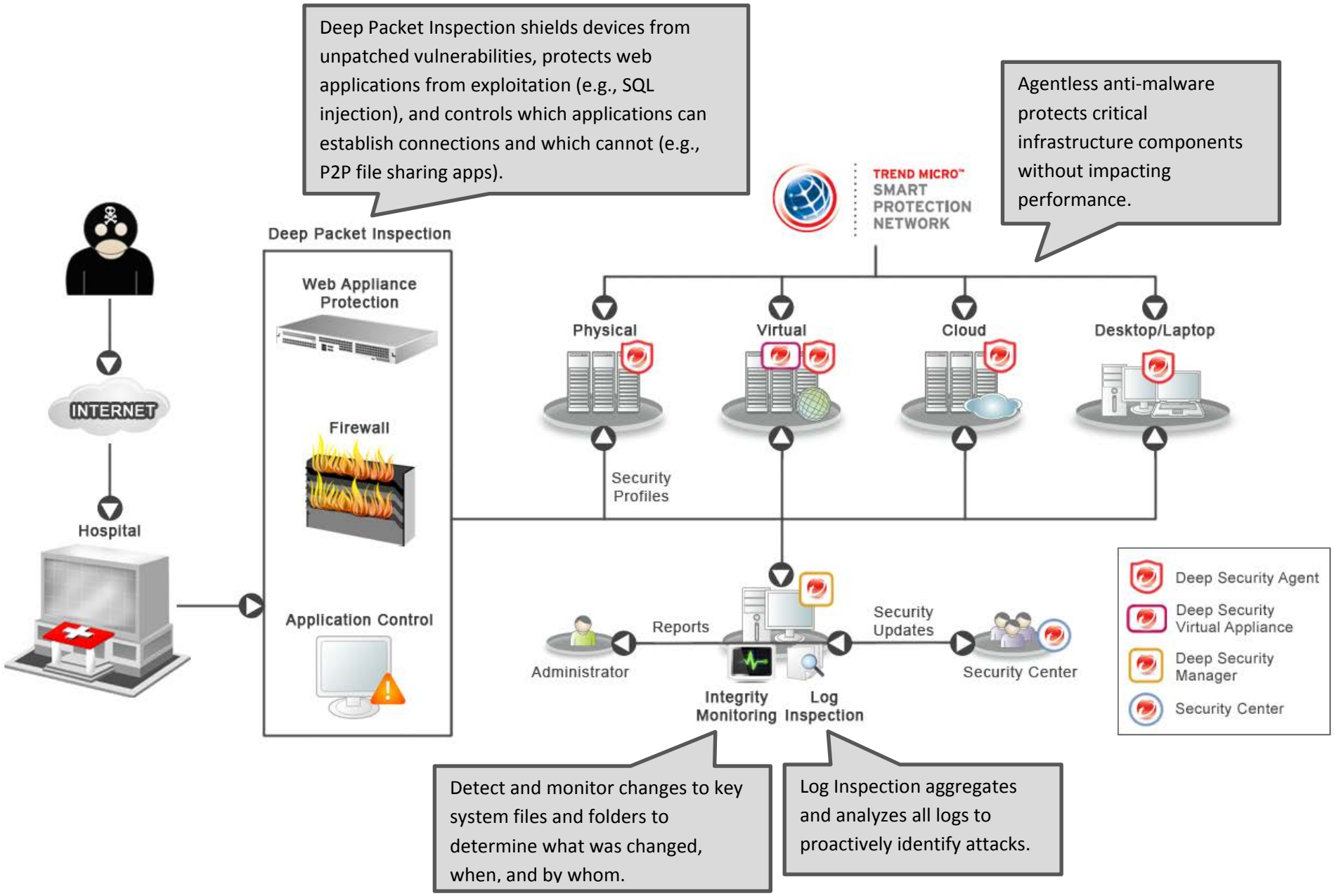
The Log Inspection module enhances all other modules of Deep Security along with the other solutions mentioned in this paper among many others. Log Inspection aggregates and analyzes logs to identify and distinguish key system events that may otherwise be lost in the sea of log files and data most organizations must deal with. For example, many attacks exploit multiple vulnerabilities. In the case of malware, roughly half are injected by a remote attacker taking advantage of a remote access exploit.[3] So, if an organization's systems become infected with a specific type of malware, the log inspection utility can expose those logs along with other systems and events triggered to understand higher level,

[2] http://dartmed.dartmouth.edu/fall09/html/vs_stanching.php
[3] http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

related security events occurring in the organization—allowing the organization to determine that it doesn't just have a malware problem but also has a remote access vulnerability.

As alluded to above, Log Inspection can easily hook into anything that produces a syslog or custom APIs can be written to connect with applications or other security event management systems. Log Inspection works as an agent on a machine.

Integrating into a Healthcare Environment



Compliance Mapping

Deep Security Product Feature(s)	HITRUST CSF 2011 Control Reference	HIPAA Security Rule Specification	HITECH Breach Notification Specification	PCI DSS v2 Specification	§ 495.6 (Stage 1) Meaningful Use Stage 1 Measure
Agentless Anti-malware for VMware	01.v Information Access Restriction - Level 2 09.j Controls Against Malicious Code - Level 1 / 2 09.k Controls Against Mobile Code - Level 1 / 2	(a)(5)(ii)(B) Protection from malicious software (Addressable)	Regulation not covered	2.2.3 Configure system security parameters to prevent misuse. 5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs	(d)(15)(ii) / (f)(14)(ii) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process
Intrusion Detection and Prevention	09.k Controls Against Mobile Code - Level 1 / 2 09.m Network Controls - Level 3 09.x Electronic Commerce Services - Level 2 09.ab Monitoring System Use - Level 2 / 3 09.ad Administrator and Operator Logs - Level 2 10.m Control of Technical Vulnerabilities - Level 1 / 2 11.a Reporting Information Security Events - Level 2	Regulation not covered	Regulation not covered	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 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ	(d)(15)(ii) / (f)(14)(ii) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process

			1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.) 1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks 2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. 2.2.3 Configure system security parameters to prevent misuse.

				11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date	
Web Application Protection	09.x Electronic Commerce Services - Level 2 09.z Publicly Available Information - Level 1 10.b Input Data Validation - Level 1 10.m Control of Technical Vulnerabilities - Level 2	Regulation not covered	Regulation not covered	6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. 6.5.2 Buffer overflow 6.5.5 Improper error handling 6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2) 6.5.7 Cross-site scripting (XSS) 6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	(d)(15)(ii) / (f)(14)(ii) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process

				6.5.9 Cross-site request forgery (CSRF) 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known of the following either attacks by methods: - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes - Installing a web-application firewall in front of public-facing web application 11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date	

Application Control	01.i Policy on Use of Network Services - Level 1 / 2 01.l Remote Diagnostic and Configuration Port Protection - Level 3 01.n Network Connection Control - Level 1 / 2 01.v Information Access Restriction - Level 2 09.m Network Controls - Level 1 / 3 09.w Interconnected Business Information Systems - Level 2 / 3 09.ab Monitoring System Use - Level 3 10.m Control of Technical Vulnerabilities - Level 2	Regulation not covered	Regulation not covered	1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations. 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment 2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. 2.2.3 Configure system security parameters to prevent misuse.	(d)(15)(ii) / (f)(14)(ii) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process

				11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date	
Bidirectional Stateful Firewall	01.i Policy on Use of Network Services - Level 1 / 2 01.l Remote Diagnostic and Configuration Port Protection - Level 2 / 3 01.n Network Connection Control - Level 1 / 2 01.y Teleworking - Level 1 09.m Network Controls - Level 1 / 2 / 3 09.w Interconnected Business Information Systems - Level 2 / 3 09.x Electronic Commerce Services - Level 2 10.m Control of Technical Vulnerabilities - Level 2	Regulation not covered	Regulation not covered	1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations. 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment	(d)(15)(ii) / (f)(14)(ii) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process

			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 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ 1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.) 1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks

				2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known of the following either attacks by methods: - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes - Installing a web-application firewall in front of public-facing web application"	

Integrity Monitoring	0.a Information Security Management Program - Level 2 / 3 01.c Privilege Management - Level 3 01.s Use of System Utilities - Level 2 06.d Data Protection and Privacy of Covered Information - Level 1 09.m Network Controls - Level 3 09.x Electronic Commerce Services - Level 1 09.z Publicly Available Information - Level 1 09.ab Monitoring System Use - Level 1 / 2 / 3 09.ac Protection of Log Information - Level 3 09.ad Administrator and Operator Logs - Level 1 / 2 10.c Control of Internal Processing - Level 1 10.j Access Control to Program Source Code - Level 2	(a)(1)(ii)(D) Information system activity review (Required) (c)(1) Integrity (c)(2) Mechanism to authenticate electronic protected health information (Addressable) (e)(2)(i) Integrity controls (Addressable)	Regulation not covered	1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations. 2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. 2.2.3 Configure system security parameters to prevent misuse. 10.2.2 All actions taken by any individual with root or administrative privilege 10.2.6 Initialization of the audit logs 10.2.7 Creation and deletion of system-level objects 10.3.6 Identity or name of affected data, system component, or resource.	(d)(15)(ii) / (f)(14)(ii) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process

				10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert) 10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). 11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date

				11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly 12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures)	
Log Inspection	01.c Privilege Management - Level 1 09.a Documented Operations Procedures - Level 1 09.aa Audit Logging - Level 1 / 2 / 3 09.ab Monitoring System Use - Level 1 / 2 / 3 10.h Control of Operational Software - Level 2 10.j Access Control to Program Source Code - Level 2 11.e Collection of Evidence - Level 1 / 2	(a)(5)(ii)(C) Log-in monitoring (Addressable) (a)(1)(ii)(D) Information system activity review (Required) (b) Logging	Regulation not covered	10.3.1 User identification 10.3.2 Type of event 10.3.3 Date and time 10.3.4 Success or failure indication 10.3.5 Origination of event 10.3.6 Identity or name of affected data, system component, or resource. 10.5.1 Limit viewing of audit trails to those with a job-related need 10.5.2 Protect audit trail files from unauthorized modifications	(d)(15)(ii) / (f)(14)(ii) Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process

				10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter 10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN 10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). 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 back-up). 12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures)	

Future Trends

While many of the modules within Deep Security already are offered as virtual appliances—anti-malware and deep packet inspection—there is still room to transition those modules only offered as an installed agent. Looking forward, Trend Micro is focused on evolving all of the Deep Security modules into virtual agents to provide protections for both virtual machines and standalone systems.

Generally speaking, because Deep Security is a framework, or platform whereby modules plug into the overarching solution, expect Deep Security to continue to grow in capability with new modules plugging in to provide comprehensive coverage across physical and virtual server environments.