Addressing Server Security and Compliance Challenges of MAS TRM Guidelines

July 2013
INTRODUCTION

The advancement of information technology (IT) has brought upon rapid changes to the way the financial industry conducts business and manages systems and operations. IT is no longer a support function within a financial institution (FI) but a key enabler. There is a high demand placed on IT for contacting and supporting customers as well as regulating security compliance. In 2001, The Monetary Authority of Singapore (MAS) created the Internet Banking Technology Risk Management (IBTRM) Guidelines to assist banks in establishing a sound framework of risk management principles and security best practices. MAS enhanced the guidelines in 2013 creating the Technology Risk Management (TRM) Guidelines. This new version addresses modern information threats and comprehensive security practices in the financial sector, widening the application of the guidelines to include all financial institutions. The objectives include:

- Establishing a sound and robust technology risk management framework
- Strengthening system security, reliability, resiliency, and recoverability
- Deploying strong authentication to protect customer data, transactions, and systems

To undertake these initiatives, FIs are responsible for understanding the risks associated with deploying advanced technology and online systems to reach customers. FIs need to provide adequate and robust risk management systems that are as crucial as the operating processes that manage these risks. Major topics include:

- Oversight of Technology Risks by Board of Directors and Senior Management
- Technology Risk Management Framework
- Management of IT Outsourcing Risks
- Acquisition and Development of Information Systems
- IT Service Management
- Systems Reliability, Availability and Recoverability
- Operational Infrastructure Security Management
- Data Centres Protection and Controls
- Access Control
- Online Financial Services
- Payment Card Security (ATM, Credit and Debit Cards)
- IT Audit
**ABOUT THIS REPORT**

This paper outlines how Trend Micro Deep Security, the industry’s leading server security solution, can help ensure regulatory compliance and the security of both the data center and mission-critical servers with a single, centrally managed solution. An extensive mapping of requirements from the TRM Guidelines to the functions provided by Deep Security demonstrates how Trend Micro can assist financial institutions in addressing the challenges faced by IT in risk management and compliance.
ADDRESSING SERVER SECURITY IN FINANCIAL INSTITUTIONS

Adhering to regulatory compliance is a top priority for today’s financial institutions in order to achieve business objectives. As the financial institution infrastructure embraces virtualization, mobility, and cloud computing, mission-critical servers and applications are becoming increasingly vulnerable to modern threats. In this regard, MAS TRM Guidelines have significantly emphasized the seriousness of server security. The financial services industry must employ an appropriate security strategy to safeguard business operations and provide clear visibility regarding cyber threats and server protection.

The three main challenges to server security in the financial sector include data center applications, mobile and online services, and cyber threats. The management of these security risks must be quick and efficient to mitigate the multitude of negative effects these threats may cause.

Challenges to Modern Data Center Applications

Organizations are evolving their data center applications to improve resource utilization, increase business agility, and reduce costs. However, threats are emerging that attempt to exploit weaknesses in the changing security infrastructure:

- Virtualization – Virtualization adds complexity, scalability, and management challenges. Implementing virtualization without considering its impact on the surrounding IT resources can lead to catastrophic failures.

- Vulnerability – Legacy operating systems and unpatched applications are vulnerable. Threats can target vulnerabilities on DMZ servers and steal sensitive data or perform unauthorized system changes.

- Operational Risks – Careless operation can introduce unauthorized changes that affect business-critical applications causing an increase in overall infrastructure downtime. Recent industry research\(^1\) indicates that businesses lose an average of about $5,000 per minute during an outage.

>> See MAS TRM Guidelines: Chapter 5, 7, 8, 9, 10, and 11

Security Concerns for Mobile & Online Services

Digital banking services have become the leading channels for transacting and managing accounts, providing a great value to customers anytime and anywhere. However, as more customers adopt mobile and online banking behaviors, security concerns grow significantly and are a top priority. A recent Trend Micro study reported\(^2\) a 417% increase of mobile malware applications in the APAC region in Q2, 2012. These threats included emerging Automatic Transfer System attacks and Advanced Persistent Threats (APTs), which consequently lead to identity theft and sensitive information leakage.

\(^1\) Emerson Network Power Report, “Understanding the Cost of Data Center Downtime: An Analysis of the Financial Impact of Infrastructure Vulnerability”, 2011

\(^2\) Trend Micro, “2012 Q2 APAC Threat Landscape Report”
Attackers’ tactics involve:

- Interception of valuable information when a customer performs financial transactions
- The insertion of malicious code into applications to obtain the customer’s account access data
- Fraudulent withdrawals

>> See MAS TRM Guidelines: Chapter 9, and 12

**Evolving Cyber Threats**

Because banking systems are critical national assets, hackers are targeting large banking institutions worldwide. A single paralysis of the system can cause large-scale damage to the economic activities of a country. According to the following news report, hackers launched a broad cyber campaign to disrupt banks’ websites and corporate networks repeatedly in the USA over the past year:

“…unexplained outages on the Bank of America and JPMorgan Chase’s websites...The industry’s Financial Services Information Sharing and Analysis Center raised its cyber threat level from "elevated" to "high". – reported by V3.co.uk³

Concern about the recent trend in cyber attacks is high and the fear of becoming a victim of cyber fraud could drive customers away from using Internet-based commerce systems, resulting in a major impact to financial sectors. Like many modern societies, Singapore considers cyber threats one of the most serious security challenges it faces. A survey⁴ of 150 CIOs and CTOs in the finance and banking sector in Asia found 70% of Singapore technology experts are more concerned about cyber security threats than their regional counterparts such as Hong Kong (60%) and Japan (42%). Due to the overwhelming increase of cyber attacks that could trigger a widespread financial crisis, the primary concern of financial institutions is to improve system resiliency and protect the interests of customers.

>> See MAS TRM Guidelines: Chapter 9, 10, 12, and 13

---

³ V3.co.uk, “Finance industry’s cyber taskforce puts banks on high alert for attacks”, 20 Sep 2012
SOLUTIONS FOR DEFENSE AND THE COMPLIANCE IMPERATIVE

TREND MICRO DEEP SECURITY

Comprehensive Security Platform for Physical, Virtual, and Cloud Servers

Trend Micro Deep Security provides a comprehensive server security platform designed to protect physical and virtualized data centers from data breaches and business disruptions while enabling compliance. Its agentless solution simplifies security operations while accelerating the ROI of virtualization and cloud projects. Tightly integrated modules easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops. The solution allows organizations to tailor their own security with any combination of agentless and agent-based protection, including anti-malware, web reputation, firewall, intrusion prevention, integrity monitoring, and log inspection. The result is an adaptive and efficient server security platform that protects mission-critical applications and data from breaches and business disruptions without expensive emergency patching.

Enhanced Virtualization and Cloud Security

With integrated security designed for virtual servers, organizations can remain secure without sacrificing performance or management. Deep Security provides full protection to virtual environments to increase the efficiency of cloud computing.

1. Proven and comprehensive agentless security platform - Deep Security integrates with VMware vShield and other APIs to provide agentless anti-malware, web threat protection, integrity monitoring, intrusion prevention, and firewall in a single virtual appliance for the entire vSphere server. Customers receive stronger security for each virtual machine (VM) without increasing their digital footprint, along with significantly easier manageability,
greater resource efficiency, and higher levels of VM density. Thousands of real world deployments and third-party tests show that Deep Security’s agentless architecture can support VM densities several times higher than traditional agent-based solutions.

2. Extending to the Cloud - Deep Security integrates with VMware vCloud Director and Amazon Web Services (AWS) enabling organizations to extend their corporate security policies to workloads in the public cloud and manages both data center and cloud workloads through a single pane of glass. Deep Security also supports a true multi-tenant architecture allowing separate tenants or business units to manage policies independently and in a self-service manner. Automated deployment of Deep Security components supports elasticity and a cloud-scaling of the security infrastructure, while management APIs support integration into modern cloud management infrastructure.

3. Ultimate flexibility - Deep Security flexibly deploys in either virtual appliance or agent-based form to fit physical, virtual, private cloud, and public cloud environments. The virtual appliance can also deploy in coordination with selected in-guest agents for in-depth defense and scalability. If the in-guest agent is removed, the virtual appliance automatically steps in and protects the VM.

4. Cloud Data Protection - Deep Security integrates with Trend Micro™ SecureCloud for additional data security that is critical in multi-tenant cloud environments. SecureCloud adds encryption and policy-based key management that enables you to protect and manage access to critical data residing in and moving between your data center and private cloud environments.

Powered by the Trend Micro Smart Protection Network

Unlike most competitors, Trend Micro leverages threat intelligence from the cloud. This means that the continuously growing files containing deterministic signatures of known malware variants are not distributed to every enforcement point, including guest VMs. Instead, threat intelligence is available as a signature lookup service in the private or public cloud. This approach eliminates the delay caused by pushing signature updates to enforcement points and allows Trend Micro customers to benefit from a faster time to protect. The Smart Protection Network-enabled enforcement points can also provide immediate feedback to Trend Micro after detecting suspicious behavior or files, which in turn drastically accelerates the global availability of threat intelligence.

Deep Packet Inspection

Deep Packet Inspection is the central module within Deep Security. It provides the necessary contextual information to the following sub-modules that provide protection:

- Intrusion detection and prevention
- Web application protection
- Application protection
• Bi-directional stateful firewall

Deep Packet Inspection examines all incoming and outgoing traffic, including SSL traffic, for protocol deviations, content that signals an attack, and policy violations. The module operates in two modes—detection and prevention—to protect operating system and enterprise application vulnerabilities. Deep Packet Inspection also protects web applications from application-layer attacks, including SQL injections and cross-site scripting. Detailed events provide valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators receive notifications automatically via alerts when an incident occurs. DPI provides intrusion detection and prevention, web application protection, and application control.

This module can deploy as a standalone traditional agent or in tandem with the virtual appliance to extend protection to physical and virtualized servers. The hybrid deployment model enables even greater security by protecting virtual machines where an agent does not exist, and providing coverage in the event an agent fails or is attacked.

**Intrusion Detection and Prevention**

Anti-malware is a fundamental security technology that all organizations should implement for both servers and end-user devices. However, because of the deterministic signature approach that is the base for malware detection, this technology has limited value when it comes to detecting previously unknown threats. Today’s financially-motivated, highly-knowledgeable, and well-funded attackers exploit zero-day vulnerabilities. Zero-day refers to the time between the exposure of software vulnerabilities and the time in which an exploit targeting a vulnerability becomes available. In many cases, the exploit exists “in the wild” before a patch is created to address the vulnerability. This leaves a window of opportunity for attackers and a window of vulnerability for the organization.

Intrusion Detection and Prevention through Deep Packet Inspection provides protection to customers during that window of vulnerability. The Intrusion Detection and Prevention module works by shielding the underlying vulnerability, for example, a Windows service running on a server. The virtual patch that Deep Security deploys prevents exploits from leveraging the nature of the vulnerability, and protects both the machine and operating system without even having to identify malware. Virtual patching also covers legacy systems, which are major targets of zero-day attacks.

IDS/IPS offers specific rules that look at traffic entering the network to determine if the communication is a threat. The first layer of protection is the firewall, which keeps known good packets flowing through and prevents known bad packets from getting in by blocking vulnerable ports and running services. The firewall also examines the packet itself—evaluating the header and body to determine if there is any evidence of malicious intent, and looking for red flags like protocol anomalies that indicate a modification for the evasion of traditional detection systems.
Web Application Protection

The Web Application Protection module of Deep Security is designed to specifically block attacks on web applications, including cross-site scripting, SQL injections, and many others.

Web Application Protection analyzes the network communication to and from web applications to identify patterns that signal malicious activities. For instance, if a web application does not properly validate the content provided in an input form, a hacker can exploit the application by entering actual SQL code. This causes the application to execute commands on the database, which if done correctly, can return sensitive information stored in the database. Deep Security checks the packets and commands to verify the validity of the provided information, thus preventing privileged access to the application, operating system, and data.

Application Control

Application Control is the third pillar of Deep Packet Inspection. It prevents unwanted applications from running and communicating on the organization’s network to provide security and optimize employee productivity. If, for example, an organization wants to prevent peer-to-peer (P2P) applications from running, Deep Security Application Control identifies and blocks communications that are part of the applications.

Trend Micro provides out-of-the-box policies and rules to prevent common malicious and unproductive applications. Organizations can further customize this list to include applications specific to their environment.

Integrity Monitoring

The Integrity Monitoring module detects attempts to make changes to critical system and application files. Trend Micro provides rules and policies for a pre-specified list of files and folders, constantly monitoring and maintaining an audit trail of who accessed the file, when the file access occurred, and what changes were made. Because Integrity Monitoring operates at the file level, it offers flexibility and control to optimize the monitoring activities for your unique environment. This includes the ability to include or exclude files and wildcard file names, and to include or exclude subdirectories in scan parameters. Integrity Monitoring also provides the flexibility to create custom rules for unique requirements.

Integrity Monitoring operates as agent-based and agentless on physical or virtual machines where monitoring is conducted.

Log Inspection

The Log Inspection module enhances all other modules of Deep Security by providing an unprecedented level of visibility. Log Inspection aggregates, analyzes, and correlates logs from multiple sources to identify key system events that may otherwise get lost in the vast amount of data most organizations must deal with. This module is particularly important because many attacks exploit multiple vulnerabilities. If an organization’s systems become infected with a specific type of malware, the Log Inspection utility can correlate logs of various systems and the events triggered to provide an understanding of high-level, related security events occurring in the organization.
This correlation may also point not only to the malware infection, but also to the root cause of the infection, such as a remote access vulnerability.

Deep Security Log Inspection easily analyzes logs from multiple sources beyond Trend Micro products, including syslog or custom APIs. Adapters for connecting with applications and other security event management systems can easily be written due to the module’s flexible architecture. Like Integrity Monitoring, Log Inspection works as an agent on a machine.
Recommendation for Extended Reading

Developing a comprehensive and regulatory compliance server security strategy within an organization is not just about security control and detection on server itself. Financial institutions also require incorporating a multi-layered security and appropriate incident management strategy to combat modern threats from cyber space. For extended study, please refer to the following Trend Micro white papers: “Addressing Data Protection and Compliance Challenges of MAS TRM Guidelines” and “Addressing Cyber Threats and Security Incident Management and Compliance Challenges of MAS TRM Guidelines”.

**TRM GUIDELINES COMPLIANCE MAPPING**

The following table covers compliance mapping for TRM Guidelines against Deep Security functionalities and the following security standards:

**PCI-DSS**
The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

**ISO 27001:2005**
ISO/IEC 27001 formally specifies a management system intended to bring information security under explicit management control. As a formal specification, ISO/IEC 27001 mandates specific requirements.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7 IT SERVICE MANAGEMENT</td>
<td>Deep Security Integrity Monitoring and Log Inspection features provide alerts regarding the modification of critical system files, configuration files, or content files. You can configure it to adapt to changes in the management process of the organization. Key benefits:</td>
<td>11.5</td>
<td>A.10.10.2</td>
</tr>
</tbody>
</table>
| 7.1.1 The FI should establish a change management process to ensure that changes to production systems are assessed, approved, implemented and reviewed in a controlled manner. | – Monitors critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes  
– Monitors for any unauthorized changes to the hypervisor, thereby extending security and compliance of virtualized systems to the hypervisor  
– Reduces administrative overhead with trusted event tagging that automatically replicates actions for similar events across the entire data center  
– Simplifies administration by greatly reducing the number of known good events through automatic cloud-based whitelisting from Trend Micro Certified Safe Software Service | | |
### MAS TRM Guidelines

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3.8 Being able to maintain customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of the FI. FIs should include in their incident response procedures a predetermined action plan to address public relations issues.</td>
<td>Deep Security and Deep Discovery provide effective functionalities (Anti-malware, HIPS, DPI, Integrity Monitoring, Log Inspection features) for supporting threat identification and incident analysis. The technology gains visibility into the corporation's true security posture and provides in-depth analysis and actionable intelligence to prevent and discover potential hacking or intrusion. Deep Security protects business-critical servers and detects system anomalies through reporting unauthorized change and suspicious activity information. Detailed, server-level security events are provided to a SIEM system, including ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic, and other systems through multiple integration options.</td>
<td>12.9.5</td>
<td>A.10.6.1, A.10.6.2</td>
</tr>
</tbody>
</table>

### 9 OPERATIONAL INFRASTRUCTURE SECURITY MANAGEMENT

| 9.0.1 The IT landscape is vulnerable to various forms of cyber attacks, and the frequency and malignancy of attacks are increasing. It is imperative that FIs implement security solutions at the data, application, database, operating systems and network layers to adequately address and contain these threats. | To defend organizations from various forms of cyber attacks, financial institutions must actively protect themselves through continuous monitoring of security controls in critical host, network, and data environments. The most important security controls include antivirus, host-based IDS/IPS, DLP, Integrity Monitoring, and network traffic monitoring. Deep Security provides in-depth defense for servers and applications. Other Trend Micro solutions provide complimentary protections at data and network layers, please refer to the following white papers:  
- Trend Micro MAS TRM Guidelines Compliance Solutions – Addressing Data Protection and Compliance Challenges of MAS TRM Guidelines  
- Trend Micro MAS TRM Guidelines Compliance Solutions – Addressing Cyber Threats and Security Incident Management Compliance Challenges of MAS TRM Guidelines | 12.9.5               | A.10 A.12.6.1          |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3.1 The FI should configure IT systems and devices with security settings that are consistent with the expected level of protection. The FI should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment.</td>
<td>Deep Security Integrity Monitoring and Log Inspection features monitor critical configuration files and security settings of operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes.</td>
<td>11.5</td>
<td>A.10.10.2</td>
</tr>
<tr>
<td>9.3.3 The FI should deploy anti-virus software to servers, if applicable, and workstations. The FI should regularly update anti-virus definition files and schedule automatic anti-virus scanning on servers and workstations on a regular basis.</td>
<td>Deep Security provides agent and agent-less anti-virus/malware features for protecting physical, virtual, and cloud servers. It can optimize security operations to avoid antivirus storms commonly seen in full system scans and pattern updates. Trend Micro has multinational research, development and support centers to continuously monitor the threat landscape across the globe. Deep Security automatically receives latest vulnerability information and signatures from the centers to cope with latest threats.</td>
<td>5.1 5.2</td>
<td>A.10.4</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------</td>
<td>----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>9.4.2 The FI should deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting.</td>
<td>Deep Security provides Intrusion Prevention feature defends against SQL injection, cross-site scripting, and other web application vulnerabilities. In addition, Deep Security provides Virtual Patching feature to shield vulnerabilities of known but unpatched systems and applications. Therefore, it eliminates the operational pains of emergency patching, frequent patch cycles, and costly system downtime.</td>
<td>6.6</td>
<td>12.6.1</td>
</tr>
<tr>
<td>9.5.1 The FI should establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches. To implement security patches in a timely manner, the FI should establish the implementation timeframe for each category of security patches.</td>
<td>FI should establish its own patch management procedure. Deep Security can be a supplementary tool which provides Virtual Patching feature to shield vulnerabilities of known but unpatched systems and applications. Therefore, it eliminates the operational pains of emergency patching, frequent patch cycles, and costly system downtime.</td>
<td>6.1</td>
<td>12.4.1 12.5.1</td>
</tr>
</tbody>
</table>
9.6.1 Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt detection of unauthorised or malicious activities by internal and external parties, the FI should establish appropriate security monitoring systems and processes.

With the tightly integrated modules, Deep Security helps ensure server, application, and data security across multiple platforms from known and zero-day attacks:

**Anti-Malware** – detects and removes malware in real time with minimal performance impact. It protects physical servers and virtual machines against viruses, spyware, trojans and other malware with zero in-guest footprint.

**Web Application Protection** – defends against SQL injection attacks, cross-site scripting attacks, and other web application vulnerabilities, and shields these vulnerabilities until code fixes are completed. Deep Security also protects against vulnerabilities in the operating system and web infrastructure.

**Integrity Monitoring, Log Inspection** – provide immediate insight into suspicious activity that might be occurring in your web environment. Monitoring and detecting suspicious behavior is a key element in identifying data breach attempts.

**Bi-directional Stateful Firewall** – shields known and unknown vulnerabilities in web, applications, and operating systems. The agent also implements Deep Packet Inspection on network traffic to prevent denial-of-service attacks and detects reconnaissance scans. Deep Security provides rule-based protection for managing appropriate connections and alerting on suspicious behavior without sacrificing system flexibility.

9.6.3 The FI should implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the identification of unauthorised changes.

Deep Security Integrity Monitoring and Log Inspection features monitor critical configuration files and security settings of operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6.1 Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt detection of unauthorised or malicious activities by internal and external parties, the FI should establish appropriate security monitoring systems and processes.</td>
<td>With the tightly integrated modules, Deep Security helps ensure server, application, and data security across multiple platforms from known and zero-day attacks: <strong>Anti-Malware</strong> – detects and removes malware in real time with minimal performance impact. It protects physical servers and virtual machines against viruses, spyware, trojans and other malware with zero in-guest footprint. <strong>Web Application Protection</strong> – defends against SQL injection attacks, cross-site scripting attacks, and other web application vulnerabilities, and shields these vulnerabilities until code fixes are completed. Deep Security also protects against vulnerabilities in the operating system and web infrastructure. <strong>Integrity Monitoring, Log Inspection</strong> – provide immediate insight into suspicious activity that might be occurring in your web environment. Monitoring and detecting suspicious behavior is a key element in identifying data breach attempts. <strong>Bi-directional Stateful Firewall</strong> – shields known and unknown vulnerabilities in web, applications, and operating systems. The agent also implements Deep Packet Inspection on network traffic to prevent denial-of-service attacks and detects reconnaissance scans. Deep Security provides rule-based protection for managing appropriate connections and alerting on suspicious behavior without sacrificing system flexibility.</td>
<td>5.1 5.2</td>
<td>10.4</td>
</tr>
<tr>
<td>9.6.3 The FI should implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the identification of unauthorised changes.</td>
<td>Deep Security Integrity Monitoring and Log Inspection features monitor critical configuration files and security settings of operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes.</td>
<td>11.5</td>
<td>A.10.10.2</td>
</tr>
</tbody>
</table>
--- | --- | --- | ---
9.6.4 The FI should perform real-time monitoring of security events for critical systems and applications, to facilitate the prompt detection of malicious activities on these systems and applications. | Deep Security and Deep Discovery provide effective functionalities (Anti-malware, HIPS, DPI, Integrity Monitoring, Log Inspection features) for supporting threat identification and incident analysis. The technology gains visibility into corporation’s true security posture and provides in-depth analysis and actionable intelligence to prevent and discover potential hacking or intrusion. Deep Security protects business-critical servers and detects system anomalies through reporting unauthorized change and suspicious activity information. Detailed, server-level security events are provided to a SIEM system, including ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic, and other systems through multiple integration options. Deep Discovery focuses on identifying attack incidents by detecting and analyzing malicious content, communications, and behavior indicative of advanced malware or attacker activity across every stage of the attack sequence. | 12.9.5 | A.10.6.1 A.10.6.2

9.6.5 The FI should regularly review security logs of systems, applications and network devices for anomalies. | With the Log Inspection feature, Deep Security helps administrators to select and transfer important log entries from operating systems and applications to the SIEM and Deep Security administration server. | 10.6 | A.10.10.2

9.6.6 The FI should adequately protect and retain system logs to facilitate any future investigation. When determining the log retention period, the FI should take into account statutory requirements for document retention and protection. | Using Deep Security, administrators can transfer log entries to SIEM or the Deep Security management system promptly. | 10.5.3 | A.10.10.3
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12 ONLINE FINANCIAL SERVICES</td>
<td>Deep Security Integrity Monitoring and Log Inspection features monitor critical configuration files and security settings of operating system and application files to ensure system integrity of online financial services.</td>
<td>11.5</td>
<td>A.10.10.2</td>
</tr>
<tr>
<td>12.1.4 ... The FI should implement physical and logical access security to allow only authorised staff to access its systems. The FI should also implement appropriate processing and transmission controls to protect the integrity of systems and data.</td>
<td>With the tightly integrated modules, Deep Security helps ensure server, application, and data security across multiple platforms from known and zero-day attacks: <strong>Web Application Protection</strong> – defends against SQL injection attacks, cross-site scripting attacks, and other web application vulnerabilities, and shields these vulnerabilities until code fixes are completed. Deep Security also protects against vulnerabilities in the operating system and web infrastructure. <strong>Integrity Monitoring, Log Inspection</strong> – provide immediate insight into suspicious activity that might be occurring in your web environment. Monitoring and detecting suspicious behavior is a key element in identifying data breach attempts. <strong>Bi-directional Stateful Firewall</strong> – shields known and unknown vulnerabilities in web, applications, and operating systems. The agent also implements Deep Packet Inspection on network traffic to prevent denial-of-service attacks and detects reconnaissance scans. Deep Security provides rule-based protection for managing appropriate connections and alerting on suspicious behavior without sacrificing system flexibility of online financial services.</td>
<td>5.1 5.2 6.1 6.2 6.5.7 6.6 8.5.13</td>
<td>A.6.1.7 A.10.4 A.11.4.2 A.11.5.1 A.12.4.1 A.12.5.1 A.12.6.1</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------</td>
<td>----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>13 PAYMENT CARD SECURITY (ATM, CREDIT AND DEBIT CARDS)</strong></td>
<td></td>
<td>11.5</td>
<td>A.10.10.2</td>
</tr>
<tr>
<td>13.2.2 To secure consumer confidence in using these systems, the FI should consider putting in place the following measures to counteract fraudsters’ attacks on ATMs and payment kiosks:</td>
<td>Deep Security provides the Integrity Monitoring feature to alert modification of critical system files, configuration files, or content files in ATMs that are compliant with the security requirements of FI’s change management process. Deep Security can integrate with SIEM solutions to enhance incident response and process automation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Install detection mechanisms and send alerts to appropriate staff at the FI for follow-up response and action;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2013 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.