Security Standards Compliance
NIST Framework for Improving
Critical Infrastructure Cybersecurity

Trend Micro Products
(Custom Defense, Cloud and Data Center Security, Complete User Protection)

Version 1.2

Prepared by:
BD Pro
www.BDPro.ca
The Presidential Executive Order 13636 required the development of this voluntary risk-based cybersecurity framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. This Framework for Improving Critical Infrastructure Cybersecurity (FICIC), was created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without intending to place additional regulatory requirements on Critical Infrastructure (CI) enterprises. This NIST framework includes “informative references” to industry best practice security frameworks1 2 3 4 5 6 which are used by many of these enterprises.

Many of the NIST-FICIC cyber security controls address the need for organizations to detect and effectively respond to security incidents including those related to advanced persistent threats. The standard provides a foundation of security controls for incorporating into an organization’s overall security requirements baseline for mitigating risk and improving systems and application security in their physical and virtualized environments. CI enterprises using this standard also have obligations to be able to demonstrate compliance in the context of their own continuous improvement program in the constantly changing modern threat environment. From a security product vendor’s viewpoint, there is also a need to clearly demonstrate to such users of their products, how their products will, help satisfy the NIST-FICIC enterprise and product specific security requirements.

Virtualized servers and cloud computing environments, are being implemented by Critical Infrastructure enterprises and by their Cloud Service Providers. They face many of the same security challenges as their physical counterparts and additionally have to contend with a number of security concerns specific to the virtual environment such as: inter VM traffic, resource contention, blurring of system and network security boundaries, mixed trust levels, security zoning, and separation of duties. In particular, organizations need to specifically protect their sensitive information assets in the virtualized multi-tenant cloud environment where the physical storage locations are unknown to them and distributed across the cloud.

Trend Micro Solutions
Trend Micro, the leader in cloud and data center security, provides solutions to help address many needs in the NIST-FICIC cyber security controls. Trend Micro solutions provide layered security to protect information on mobile devices, endpoints, gateways, servers and public cloud environments, with centralized visibility and control. Trend Micro solutions contain security products that are organized into three logical portfolios based on customer needs:

References:
A. Framework for Improving Critical Infrastructure Cybersecurity, NIST, Version 1.0, 12 Feb 2014
B. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 12 Feb 2013

1 Control Objectives for Information and Related Technology (COBIT 5)
2 Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC)
4 ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
6 NIST SP 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations, 15 Jan 2014
**C1 - Custom Defense** – Designed to support organizations on their journey to the cloud, Trend Micro’s Custom Defense solution enables organizations to detect, adapt and respond to targeted attacks and advanced persistent threats, ensuring their valuable information is protected. Unlike other solutions, it received the top score in Breach Detection from NSS labs, a single hardware appliance monitors at the network edge to detect incoming attacks, and within the network to detect lateral movement, across over 80 protocols and applications. The Custom Defense solution enables a rapid response to targeted attacks when it works with other Trend Micro solutions and third party products to provide a connected threat defense.

Functionality of security products in this portfolio include: Advanced, targeted threat detection; Customizable sandboxes for accurate analysis with custom signatures available to other security products; Actionable insight provided from global threat intelligence; Integration with leading SIEM solutions; Single appliance monitors multiple ports/protocols; and Automated, customized security updates.

**The Product: Deep Discovery Inspector** is the key security product within the C1 - Custom Defence portfolio with its combined functionality of Virtual Analysis (sandbox threat behavior simulation), Advanced Threat Scans, and APT Detection has been certified to the ISO 15408 Common Criteria EAL2 level. The primary Deep Discovery Inspector modules include:

- **Management Console**, provides a built-in online management console through which users can view system status, configure threat detection, configure and view run reports, administer Deep Discovery Inspector, and obtain help.
- **Virtual Analyzer**, provides a virtualized environment where untrusted files can be safely inspected.
- **Network Content Correlation Engine** is a module that implements rules or policies defined by Trend Micro. Trend Micro regularly updates these rules after analyzing patterns and trends that new and modified viruses exhibit.
- **Advance Threat Scan Engine** is a file-based detection-scanning engine that has true file type, multi-packed files, and IntelliTrap detection. The scan engine performs actual scanning across the network and uses a virus pattern file to analyze the files passing through the network. The virus pattern file contains binary patterns of known viruses. Trend Micro regularly releases new virus pattern files when new threats are detected.
- **Network Virus Scan** uses a combination of patterns and heuristics to proactively detect network viruses. It monitors network packets and triggers events that can indicate an attack against a network. It can also scan traffic in specific network segments.

**C2 - Cloud and Data Center Security** – Trend Micro is the leader in cloud and datacenter security. Designed to support organizations on their journey to the cloud, Trend Micro’s Cloud and Data Center Security solution provides the most complete set of security capabilities to protect servers and applications in physical, virtual and cloud environments. Unlike other solutions, automated policy and lifecycle management dramatically reduces risk and cost, and the solution is available as software or as a service. Heralded as the #1 global provider of server security for four years running and the leading provider of security for VMware, AWS and Microsoft Azure, the solution enables a rapid response to targeted attacks when it works with other Trend Micro solutions and third party products to provide a connected threat defense.

Functionality of security products in this portfolio include: Comprehensive protection across physical, virtual, and cloud architectures; Automated protection from vulnerabilities provided with virtual patching; Agent-less security for VMware; Easy multi-tenant and service provider management; Optimized, automated security for VMware, Amazon Web Services and Microsoft Azure; Open: Microsoft, Linux, Solaris, Unix, VMware, Citrix.

**The Products: Deep Security** provides, in both virtualized and physical environments, the combined functionality of a Common Criteria EAL2 validated Firewall, Anti-Virus, Deep Packet Inspection, Integrity Monitoring, Log Inspection, Role Based Access Control (RBAC) and support for multi-tenant virtual environments. The primary Deep Security modules include:

- Firewall Module centralizes management of server firewall policy using a bidirectional stateful firewall. Supports virtual machine zoning and prevents denial of service attacks. Provides broad coverage for all IP-based protocols and frame types as well as fine-grained filtering for ports and IP and MAC addresses.
- Anti-malware Module provides both real-time and on-demand protection against file-based threats, including threats commonly referred to as malware, viruses, Trojans, and spyware. To identify threats, Anti-Malware checks files against a comprehensive threat database, portions of which are hosted on servers or kept locally as updatable patterns. Anti-Malware also checks files for certain characteristics, such as compression and known exploit code. To address threats, Anti-Malware selectively performs actions that contain and remove the threats while minimizing system impact. Anti-Malware can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.
- Recommendation Scans identifies known vulnerabilities. The operation scans the operating system and also installed applications. Recommendation Scans automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security
signatures, engines, patterns, and rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits.

- Integrity Monitoring Module detects and reports malicious and unexpected changes to files and systems registry in real time, and is available in agentless form factor. Provides administrators with the ability to track both authorized and unauthorized changes made to the instance. The ability to detect unauthorized changes is a critical component in a cloud security strategy as it provides the visibility into changes that could indicate the compromise of an instance.
- Log Inspection Module provides visibility into important security events buried in log files. Optimizes the identification of important security events buried in multiple log entries across the data center. Forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving. Leverages and enhances open-source software available at OSSEC.
- Intrusion Prevention Module is both an Intrusion Detections System (IDS) and an Intrusion Prevention System (IPS) which protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network. Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.

Web Reputation Module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of Web sites that users are attempting to access. The Web site's reputation is correlated with the specific Web reputation policy enforced on the computer. Depending on the Web Reputation Security Level being enforced, Deep Security will either block or allow access to the URL.

**C3 - Complete User Protection** - Designed to support organizations on their journey to the cloud, Trend Micro's Complete User Protection solution provides a broad range of security capabilities to protect users and their information across every endpoint and application, providing multiple layers of threat protection. Unlike other solutions, users can be managed from a single pane of glass, it has flexible software, as a service, and hybrid deployment models, and it uses constantly evolving next-generation security techniques to deliver top ranked industry test results. The solution enables a rapid response to targeted attacks when it works with other Trend Micro solutions and third party products to provide a connected threat defense.

Functionality of security products in this portfolio include: Layered security from mobile devices to gateways; Transparent, real-time protection; Unified dashboard with centralized policy control; Modular, lightweight and efficient; Flexible deployment: on premise or security as a service; Specialized plug-ins for Exchange, Domino, SharePoint; Open: Win, Mac, iOS, Android, Blackberry…; Powers IBM™ Endpoint Protection

**The Products:** The key end point security products within the [C3 - Complete User Protection](http://www.trendmicro.com/us/business/complete-user-protection/index.html) portfolio are listed below. The high-level functional details for current versions of these products are provided on Trend Micro's [Complete User Protection](http://www.trendmicro.com/us/business/complete-user-protection/index.html) web site.

- Control Manager
- Data Loss Prevention
- Deep Discovery Advisor
- Endpoint Application Control
- Endpoint Encryption
- IM Security
- IM Security for Microsoft Lync
- InterScan Messaging Security Suite (IMSS)
- InterScan Web Security Appliance
- InterScan Web Security for Virtual Appliances
- Mobile Security for Enterprises
- OfficeScan
- PortalProtect
- PortalProtect for Microsoft Sharepoint

---

ScanMail Suite for IBM Domino
ScanMail Suite for Microsoft Exchange

Vulnerability Protection

These C1, C2 and C3 products and other Trend Micro web services can be integrated into various enterprise architectures to effectively minimize the organization’s cyber security risks. Such Trend Micro web services include:

- **Control Manager** provides a centralized management function for Deep Discovery Inspector (and other Trend Micro products).
- **Smart Protection Network** provides a URL and file reputation rating service.
- **TrendLabs** is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.
- **Threat Management Services** provides organizations with an effective way to discover, mitigate, and manage stealthy and zero-day internal threats. Threat Management Services brings together security experts and a host of solutions to provide ongoing security services. These services ensure timely and efficient responses to threats, identify security gaps that leave the network vulnerable to threats, help minimize data loss, significantly reduce damage containment costs, and simplify the maintenance of network security.
- **Threat Management Service Portal** is an on premise or hosted service which receives logs and data from registered products (DDI) and creates reports to enable product users to respond to threats in a timely manner and receive up-to-date information about the latest and emerging threats.
- **Threat Connect** correlates suspicious objects detected in the organizations environment and threat data from the Trend Micro Smart Protection Network. By providing on-demand access to Trend Micro intelligence databases, Threat Connect enables an organization to identify and investigate potential threats to their environment.
- **Mobile App Reputation Services (MARS)** collects data about detected threats in mobile devices. Mobile App Reputation Service is an advanced sandbox environment that analyzes mobile app runtime behavior to detect privacy leaks, repacked mobile apps, third-party advertisement SDKs, vulnerabilities, and app categories.
- **Threat Mitigator** receives mitigation requests from Deep Discovery Inspector after a threat is detected. Threat Mitigator then notifies the Threat Management Agent installed on a host to run a mitigation task.
- **Mitigation (Module) Devices** performs threat cleanup activities on network endpoints.

Critical Infrastructure enterprises Institutions, which use either the ISO / IEC 27002 standard or the NIST SP 800-53 standard in their enterprise-wide cyber security risk management programs, can also leverage the referenced whitepapers which address Trend Micro products’ compliancy to these two international standards.
## DE.AE Detect / Anomalies and Events

Anomalous activity is detected in a timely manner and the potential impact of events is understood

<table>
<thead>
<tr>
<th>DE.AE-2 Detect / Anomalies and Events</th>
<th>Custom Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected events are analyzed to understand attack targets and methods</td>
<td><strong>Deep Discovery Inspector</strong> monitors the organizations information system to detect and analyze attacks and provide indicators of potential attack through the Advanced Threat Scan Engine using a combination of file-based detection scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks.</td>
</tr>
<tr>
<td></td>
<td>Deep Discovery detection engines deliver expanded APT detection capabilities, including a customizable virtual analyzer and updated inspection and correlation rules designed to detect malicious content, communication, and behavior during every stage of an attack sequence. Deep Discovery Inspector increases the level of monitoring provided whenever there is an indication of increased risk to the organizations operations and assets.</td>
</tr>
<tr>
<td></td>
<td><strong>Cloud and Data Center Security</strong></td>
</tr>
<tr>
<td></td>
<td>Deep Security supports this control through the combined functionality of Deep Packet Inspection, Firewall, Anti-Virus, Integrity Monitoring, and Log Inspection. The ability to analyze, assess, and respond quickly to new or emerging threats and provide corrections to vulnerabilities is supported by the Trend Micro Smart Protection Network.</td>
</tr>
<tr>
<td></td>
<td>Deep Packet Inspection (DPI) provides an IDS/IPS capability, which protects operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injection and cross-site scripting. Security updates that provide protection against newly discovered vulnerabilities are automatically delivered to host machines. Detailed event records are produced, which provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit. The Deep Packet Inspection module is available in both the Deep Security Agent and Deep Security Virtual Appliance for VMware ESX/ESXi.</td>
</tr>
<tr>
<td></td>
<td>The Firewall module is enterprise-grade, bi-directional, and stateful. It is used to limit communication by source and destination port, IP, MAC addresses, and is protocol aware.</td>
</tr>
<tr>
<td></td>
<td>By limiting traffic, the attack surface of systems is reduced, and the risk of unauthorized access to the system is also reduced. Reconnaissance detection is supported by the ability to detect reconnaissance activities such as port scans. The stateful firewall is available in both the Agent and Appliance for VMware ESX/ESXi.</td>
</tr>
<tr>
<td></td>
<td>Anti-Virus, upon detection of a file-based virus, Deep Security performs the actions specified by the authorized systems or Deep Security Administrator. Actions are administratively configurable on a Virtual Machine through the DSA or on a DSVA basis and consist of:</td>
</tr>
<tr>
<td></td>
<td>- Clean the virus from the file,</td>
</tr>
<tr>
<td></td>
<td>- Quarantine the file, and</td>
</tr>
<tr>
<td></td>
<td>- Delete the file.</td>
</tr>
<tr>
<td></td>
<td>The Anti-Virus module performs real-time, scheduled, and on-demand scans for file-based viruses based upon known signatures, and carries out scheduled scans at the time and frequency configured by the authorized administrator, in the physical or in the virtualized environment at the hypervisor level.</td>
</tr>
<tr>
<td></td>
<td>Integrity Monitoring monitors critical system objects such as files, folders, registry entries, processes, services, and listening ports. An integrity monitoring object baseline consists of a combination of the following object attributes; Created, Last Modified, Last Accessed, Permissions, Owner, Group, Size, Hash (SHA1,SHA256,MD5), Flags, SymLinkPath, Inode Number, Device Number, Blocks Allocated.</td>
</tr>
<tr>
<td></td>
<td><strong>Complete User Protection</strong></td>
</tr>
<tr>
<td></td>
<td>Within the Complete User Protection suite there are a number of products, such as the InterScan Messaging Security, InterScan Web Security, ScanMail for Microsoft Exchange, ScanMail for IBM Domino, which make use of the Deep Discovery Analyzer/Advisor product to provide an automatic, in-depth simulation analysis of potentially malicious attachments. The Deep Discovery Analyzer/Advisor provides analysis of executables and common office documents in a secure sandbox environment. It allows organizations to create and analyze multiple customized target images that precisely match their host environments. The Custom Threat Intelligence analyzes logs of Trend Micro products and third-party solutions combined with Trend Micro threat intelligence to provide in-depth insights for risk-based incident assessment, containment and remediation.</td>
</tr>
</tbody>
</table>
In context of the referenced NIST SP800-53r4 guidance, each of the Trend Micro products that support the Smart Protection Strategy within Cloud and Data Center Security (Deep Security), Custom Defence (Deep Discovery Inspector) and Complete User Protection (Endpoint Security, Collaboration Security, Gateway Security, and Data Loss Prevention) provide information on security incidents, maintaining records about each incident, and the status of the incident or security event.

Specifically, the Control Manager provides a centralized and aggregated view of the incident and security event data collected from each registered Trend Micro product. The Control Manager provides a view and correlation of information system activity and security event information across an organizations infrastructure from Boundary gateways to end user devices. The Control Manager web based management console is a single monitoring point for antivirus and content security products and services throughout the network. Control Manager enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points.

The referenced NIST SP800-53r4 IR-8 Incident Response Plan states that an organization, as part of the Incident Response Plan, “Provides metrics for measuring the incident response capability within the organization”

In this context Control Manager provides the following security event and incident metrics to an organizations management team:

Spyware/Grayware Detection Reports
- Spyware/Grayware detected
- Most commonly detected Spyware/Grayware (in the last 10, 25, 50,100 days)
- Detected Spyware/Grayware list for all entities

Virus Detection Reports
- Viruses detected
- Most commonly detected viruses (in the last 10, 25, 50, 100 days)
- Virus infection list for all entities

Comparative Reports
- Spyware/Grayware, grouped by (Day, Week, Month)
- Viruses, grouped by (Day, Week, Month)
- Damage cleanups, grouped by (Day, Week, Month)
- Spam, grouped by (Day, Week, Month)

Vulnerability Reports
- Machine risk level assessment
- Vulnerability assessment
- Most commonly cleaned infections (in the last 10, 25, 50, 100 days)
- Worst damage potential vulnerabilities (in the last 10, 25, 50, 100 days)
- Vulnerabilities ranked by risk level
### DE.AE-4 Detect / Anomalies and Events

**Impact of events is determined**

<table>
<thead>
<tr>
<th>Control</th>
<th>Trend Micro Solution Compliancy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Custom Defense</strong></td>
<td><strong>Deep Discovery Inspector</strong> monitors the organizations information system to detect attacks and indicators of potential attack through the Advanced Threat Scan Engine using a combination of file-based detection scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks. Deep Discovery detection engines deliver expanded APT detection capabilities, including a customizable virtual analyzer and updated inspection and correlation rules designed to detect malicious content, communication, and behavior during every stage of an attack sequence. Deep Discovery Inspector increases the level of monitoring provided whenever there is an indication of increased risk to the organizations operations and assets. Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.</td>
</tr>
</tbody>
</table>
| **Cloud and Data Center Security** | **Deep Security** supports and satisfies this requirement through the combined functionality of Deep Packet Inspection, Firewall, Anti-Virus, Integrity Monitoring, and Log Inspection. The ability to respond quickly to new or emerging threats and provide corrections to vulnerabilities is supported by the Trend Micro Smart Protection Network.  
Deep Packet Inspection (DPI) provides an IDS/IPS capability, which protects operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injection and cross-site scripting. Security updates that provide protection against newly discovered vulnerabilities are automatically delivered to host machines. Detailed event records are produced, which provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit. The Deep Packet Inspection module is available in both the Deep Security Agent and Deep Security Virtual Appliance for VMware ESX/ESXi.  
The Firewall module is enterprise-grade, bi-directional, and stateful. It is used to limit communication by source and destination port, IP, MAC addresses, and is protocol-aware. By limiting traffic, the attack surface of systems is reduced, and the risk of unauthorized access to the system is also reduced. Reconnaissance detection is supported by the ability to detect reconnaissance activities such as port scans. The stateful firewall is available in both the Agent and Appliance for VMware ESX/ESXi.  
Anti-Virus, upon detection of a file-based virus, Deep Security performs the actions specified by the authorized systems or Deep Security Administrator. Actions are administratively configurable on a Virtual Machine through the DSA or on a DSVA basis and consist of:  
a) Clean the virus from the file,  
b) Quarantine the file, and  
c) Delete the file.  
The Anti-Virus module performs real-time, scheduled, and on-demand scans for file-based viruses based upon known signatures, and carries out scheduled scans at the time and frequency configured by the authorized administrator, in the physical or in the virtualized environment at the hypervisor level.  
Integrity Monitoring monitors critical system objects such as files, folders, registry entries, processes, services, and listening ports. An integrity monitoring object baseline consists of a combination of the following object attributes; Created, Last Modified, Last Accessed, Permissions, Owner, Group, Size, Hash (SHA1,SHA256,MD5), Flags, SymLinkPath, Inode Number, Device Number, Blocks Allocated. |
| **Complete User Protection** | **OfficeScan** can display impact notification for all virus/malware related events, depending on the severity levels.  
**InterScan Messaging Security** tracks system events and records their impact in terms of the time of system events such as user access, and modification of rules. Through policy events InterScan Messaging Security provides impact event information on the policy rules that were triggered, the actions taken, and the message details.  
**Control Manager**: To assist in determining the impact of security events across an organization Control Manager provides a view and correlation of information system activity and security event information collected from all registered products. Specifically, it provides DLP Incident Investigation information about DLP incidents based on incident status, severity levels, and managed users and DLP incidents, template matches, and incident sources. Threat Detection provides aggregated detections of security threats, in terms of Top Threats, and Threat Statistics, which provides the number of threat detections and the ratio of threats compared to the total number of detections. C&C Callback Events provides the number of callback attempts based on compromised hosts or callback addresses. |
<table>
<thead>
<tr>
<th>DE.AE-5 Detect / Anomalies and Events</th>
<th>Custom Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident alert thresholds are</td>
<td><strong>Deep Discovery Inspector</strong>: When an identified object is detected, Deep Discovery Inspector displays the following alert thresholds and information about the file:</td>
</tr>
<tr>
<td>established</td>
<td>High Risk - The file exhibited highly suspicious characteristics in this environment - take immediate action;</td>
</tr>
<tr>
<td></td>
<td>Medium Risk - The file exhibited moderately suspicious characteristics in this environment - investigate when able, advise users to take precaution;</td>
</tr>
<tr>
<td></td>
<td>Low Risk - The file exhibited mildly suspicious characteristics in this environment - investigate if the object is related to known threats or highly suspicious objects; or</td>
</tr>
<tr>
<td></td>
<td>No Risk - The file did not exhibit suspicious characteristics in this environment - no further action necessary</td>
</tr>
</tbody>
</table>

| Cloud and Data Center Security       | Deep Security records security Events when a protection module Rule or threshold condition is triggered, and System Events when administrative or system-related Events occur (like a User signing in or Agent software being upgraded.) Events can occur many times on a daily basis and do not necessarily require individual attention. Most Events that take place on a computer are sent to the Deep Security Manager during the next heartbeat operation except some will be sent right away if Communication settings allow Relays/Agents/Appliances to initiate communication. By default, the Deep Security Manager collects Event logs from the Agents/Appliances at every heartbeat. The Event data is used to populate the various reports, graphs, and charts in the Deep Security Manager. |

| Complete User Protection             | **Vulnerability Protection**: There are over 30 conditions that trigger Alerts and trigger the sending of an email. The Alert Configuration display provides a list of all Alerts and the conditions when an Alert will be triggered if the corresponding situation or incident arises. |
|                                      | **Data Loss Prevention** Endpoint detects digital assets and automatically takes actions specified in organizational policies, from blocking and logging to encrypting and alerting. Displays summaries of DLP incidents over a range of time (seven days by default) plus system status. As this control references NIST SP800-53r4 IR-8 Incident Response Plan which states that an organization, as part of the Incident Response Plan, "Provides metrics for measuring the incident response capability within the organization" please see the response to DE.AE-3 for additional product capabilities for this control. |
DE.CM Detect / Security Continuous Monitoring

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE.CM-1 Detect / Security Continuous Monitoring</td>
<td>The network is monitored to detect potential cybersecurity events</td>
</tr>
</tbody>
</table>

**Custom Defense/Cloud and Data Center Security**

This control references NIST SP800-53r4 SI-4 Information Systems Monitoring, please see the response to DE.AE-4 for the list of network monitoring capabilities provided by Deep Security, and Deep Discovery Inspector.

**Complete User Protection**

Products within the Complete User Protection solution which address this control includes:

- **InterScan Web Security Appliance**: Monitors more than 1000 Internet protocols and applications, including instant messaging, peer-to-peer, social networking applications, and streaming media for cybersecurity related events.

- **InterScan Messaging Security**: makes use of the Deep Discovery Analyzer product to provide advanced visualization and investigation tools that monitor, explore, and diagnose security events within the corporate network. Custom Threat Analysis is an automatic in-depth simulation analysis of potentially malicious attachments, including executables and common office documents in a secure sandbox environment. It allows organizations to create and analyze multiple customized target images that precisely match their host environments. Custom Threat Intelligence analyzes logs of Trend Micro products and third-party solutions combined with Trend Micro threat intelligence to provide in-depth insights for risk-based incident assessment, containment and remediation.

- **OfficeScan**: monitors and protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution OfficeScan consists of the OfficeScan agent program that resides at the endpoint and a server program that manages all agents. The OfficeScan agent guards and monitors the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent. OfficeScan performs real-time monitoring, provides event notification.

- **Data Loss Prevention** allows organizations to monitor the flow of sensitive information over the network. Using customizable data identifiers, templates, and policies to monitor, define, and detect organizational sensitive data from intentional or accidental loss.

- **Control Manager**: web based management console provides a single monitoring point for antivirus and content security products and services throughout the network. Control Manager enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points.
<table>
<thead>
<tr>
<th>NIST Framework for Improving CI Cybersecurity - Control</th>
<th>Trend Micro Solution Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE.CM-4 Detect / Security Continuous Monitoring</td>
<td>Custom Defense</td>
</tr>
<tr>
<td>Malicious code is detected</td>
<td>Deep Discovery Inspector</td>
</tr>
</tbody>
</table>

Deep Discovery Inspector supports this control for malicious code detection and protection. Deep Discovery Inspector detection engines deliver expanded APT and targeted attack detection including custom virtual analyzer and new discovery and correlation rules designed to detect malicious content, communication, and behavior across every stage of an attack sequence. The Advanced Threat Scan Engine uses a combination of file-based detection scanning and heuristic rule-based scanning in order to detect and document exploits and other threats used in targeted attacks. The Virtual Analyzer is a secure virtual environment used to manage and analyze suspicious network and file samples. Sandbox images allow observation of file and network behavior in a natural setting without any risk of compromising the network. Virtual Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings.

Deep Discovery Advisor is a hardware appliance that provides sandboxing, deep threat analysis, and local security updates in a unified intelligence platform that is the heart of Trend Micro Custom Defense. Custom Threat Analysis provides automatic in-depth simulation analysis of potentially malicious attachments, including executables and common office documents in a secure sandbox environment. It allows customers to create and analyze multiple customized target images that precisely match their host environments. Custom Threat Intelligence links information on attacks in an organization's environment with extensive Trend Micro threat intelligence to provide in-depth insights for risk-based incident assessment, containment and remediation. Adaptive Security Updates issues custom security updates on new C&C server locations and malicious download sites found during sandbox analysis for adaptive protection and remediation by ScanMail, Trend Micro endpoint and gateway products.

Cloud and Data Center Security

Deep Security provides the introspection security safeguard for Anti-Malware - the Anti-Malware can be configured to provide:

- The applicable real-time policies that apply during different periods of the day/week;
- The policy for full scheduled or manual scans;
- Exclusions of file types and directories; and
- Real-time behavior (scanning reads and/or writes) and applicable actions.

Upon detection of a file-based virus, Deep Security performs the actions specified by the authorized administrator. Actions are administratively configurable on a virtual or physical machine through the DSA or on a DSVA basis and consist of:

a) Clean the virus from the file,
b) Quarantine the file, and
c) Delete the file

Deep Security is able to collect an audit event from a computer indicating detection of a virus. The event identifies the computer originating the audit event, the virus that was detected and the action taken by the Deep Security. Deep Security sends an alarm to the authorized administrator and records the attempt as a system data record.

Deep Security can apply NSX Security Tags to protected VMs upon detecting a malware threat.

Further support for compliance with this control is achieved through the Trend Micro Smart Protection Network, which uses a global network of threat intelligence sensors to continually update email, web, and file reputation databases in the cloud, identifying and blocking threats in real time before they reach the organization requiring the protection.
DE-CM-4 (cont.)

**Complete User Protection**

The following products within the Complete User Protection solution detect malicious code:

- **Endpoint Application Control** prevents potential damage from unwanted or unknown applications executing on endpoints and protects users from inadvertently executing malicious software.

- **OfficeScan** protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution OfficeScan consists of the OfficeScan agent program that resides at the endpoint and a server program that manages all agents. The OfficeScan agent guards and monitors the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent. OfficeScan carries out various time based scans, such as Real Time Scan, which is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If OfficeScan detects no security risk, the file remains in its location and users can proceed to access the file. If OfficeScan detects a security risk or a probable virus/malware/malicious code, it displays a notification message, showing the name of the infected file and the specific security risk.

- **Vulnerability Protection** identifies malicious software accessing the network and reduces the vulnerability exposure of an organization’s servers. Increases visibility into, or control over, applications accessing the network.

- **ScanMail Suite for Microsoft Exchange** protects an organization’s servers in real time against email based viruses/malware, trojans, worms, spyware/grayware, and other types of malicious code. When integrated with Trend Micro Deep Discovery Advisor, ScanMail quarantines suspicious attachments for automatic sandbox execution analysis which occurs in-line without impacting the delivery of majority of messages.

- **PortalProtect for Microsoft Sharepoint** can scan URLs in Web content to detect malicious URLs, it takes an actions, such as: block or pass, as pre-configured by the administrator. PortalProtect can block files based on the file extension, file name, or true file type. When it detects a file type, it takes an action, such as: quarantine or delete, as pre-configured by the administrator. Scanning employs the latest version of the Trend Micro scan engine to detect viruses and other malicious code. When PortalProtect detects a virus or malicious code, it performs a number of actions like: quarantine or delete, according to how the administrator has it configured.

- **IM Security for Microsoft Lync** provides threat and data protection for Microsoft Lync servers. Providing top-rated malware and ULR filtering to block phishing messages and malicious file transfers.
<table>
<thead>
<tr>
<th>DE.CM-5 Detect / Security Continuous Monitoring</th>
<th>Trend Micro Solution Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized mobile code is detected</td>
<td></td>
</tr>
</tbody>
</table>

This control references NIST SP800-53R4 SC-18 Mobile Code which is defined as "Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices."

### Custom Defense

**Deep Discovery Inspector** assists with this control by providing advanced and customizable sandboxing for the detonation of suspicious files and applications detected between or within networks across all ports and the 80+ most common protocols in use by organizations.

### Cloud and Data Center Security

**Deep Security.** Intrusion Prevention is a high-performance deep packet inspection engine, which intelligently examines the content of network traffic entering and leaving hosts. The traffic is inspected for protocol deviations, content that signals an attack, or policy violations. Intrusion Prevention protects operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injection and cross-site scripting. Detailed events provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit.

### Complete User Protection

Within the Complete User Protection solution the following products detect unauthorized mobile code:

- **OfficeScan** provides protection against unauthorized mobile code by detecting ActiveX malicious code: Code that resides on web pages that execute ActiveX controls.
  - Boot sector virus: A virus that infects the boot sector of a partition or a disk.
  - COM and EXE file infector: An executable program with .com or .exe extension.
  - Java malicious code: Operating system-independent virus code written or embedded in Java™. Macro virus: A virus encoded as an application macro and often included in a document.
  - VBScript, JavaScript or HTML virus: A virus that resides on web pages and downloaded through a browser.

**InterScan Messaging Security** detects malicious email content and allows an organization to configure the types of messages that are allowed to pass through the SMTP gateway. Types of malicious and unauthorized mobile code detected include programs and documents with embedded macros, messages with HTML script files, HTML links, Java applets, or ActiveX controls.

**ScanMail Suite for Microsoft Exchange** can detect unauthorized mobile code such as script viruses/malware in script programming languages, such as Visual Basic Script, JavaScript and ActiveX embedded in HTML documents.

**ScanMail Suite for IBM Domino** can be configured to block unauthorized mobile code such as Java, Javascript, ActiveX, and Visual Basic Script.

**PortalProtect** detects a file type (java, javascript,VBA, ActiveX) that matches a blocking configuration, it executes an action to protect the SharePoint environment. The type of action it executes depends on the type of scan it is performing (real-time, manual, or scheduled) and the type of actions that have been configured for that scan (block or pass). Each time PortalProtect executes an action, it logs the event.

**IM Security for Microsoft Lync** provides protection against unauthorized mobile code, such as java, javascript, VBA, and ActiveX, when IM is used to transfer a file between users.

**Mobile Security For Enterprises** can block or enable, through the Data Protection Policy or the Samsung KNOX Workspace Policy, Javascript.

**InterScan Web Security Virtual Appliance** (IWSVA) Applets and ActiveX scanning detects and blocks malicious Java applets and unsecured ActiveX controls at the Internet gateway, preventing them from infiltrating an organization's network and performing unauthorized acts on client workstations.

<table>
<thead>
<tr>
<th>DE.CM-6 Detect / Security Continuous Monitoring</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>External service provider activity is monitored to detect potential cybersecurity events</td>
<td></td>
</tr>
</tbody>
</table>

### Custom Defense/Cloud and Data Center Security

This control references NIST SP800-53R4 SI-4 Information Systems Monitoring, please see the response to DE.AE-4 for the list of network monitoring capabilities provided by Deep Security, and Deep Discovery Inspector.

### Complete User Protection

Complete User Protection products, through continuous monitoring, facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. Complete User Protection, products include EndPoint Security, Email and Collaboration Security, Central Management (Control Manager), Mobile Security, and Secure Gateway provides access to security-related information, including cybersecurity events, on a continuing basis through reports/dashboards, this gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions.
### DE.CM-7 Detect / Security Continuous Monitoring

**NIST SP800-53R4 SI-4 Information Systems**

NIST SP800-53R4 SI-4 Information Systems Monitoring supplemental guidance states that "information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software)."

---

### DE.CM-8 Detect / Security Continuous Monitoring

**Vulnerability scans are performed**

NIST SP 800-53R4 RA-5 Vulnerability Scanning supplemental guidance states that "vulnerability scanning includes, (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms."

---

### Custom Defense / Cloud and Data Center Security / Complete User Protection

**Intrusion Detection** is provided by Deep Discovery Inspector. The Deep Discovery Inspector, Intrusion Detection System (IDS) protects organization's IT networks. This solution is deployed offline in the IT network of customers to monitor network traffic. It can identify both file-based and network-based attacks and malicious behavior;

**Intrusion Prevention** is provided by Deep Security and Vulnerability Protection products. The Deep Security Intrusion Prevention Module protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network. Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets. Deep Security also provides the Integrity Monitoring module, which allows organizations to monitor specific areas on a computer for changes. Deep Security has the ability to monitor installed software, running services, processes, files, directories, listening ports, registry keys, and registry values. It functions by performing a baseline scan of the areas on the computer specified in the assigned rules and then periodically rescanning those areas to look for changes. The Deep Security Manager ships with predefined Integrity Monitoring Rules and new Integrity Monitoring Rules are provided in Security Updates.; and

**Malicious code protection** is provided by a number of Trend Micro products such as, OfficeScan, InterScan Messaging Security, Deep Discovery Inspector and the Deep Security solution.

---

**Scanning for vulnerabilities associated with patch levels is carried out by Deep Security and Deep Discovery Inspector:**

**Scanning for functions, ports, protocols, and services is carried out by Deep Security, Vulnerability Protection, Deep Discovery Inspector, OfficeScan, InterScan Messaging Security, ScanMail Suite for Microsoft Exchange, PortalProtect for Microsoft Sharepoint, IM Security for Microsoft Lync, InterScan Web Security as a Service, and the InterScan Web Security Virtual Appliance:**

**Scanning for improperly configured or incorrectly operating information flow control mechanisms is carried out by Deep Security, Vulnerability Protection, Data Loss Prevention, Deep Discovery Inspector,**

**Deep Security** can run Recommendation Scans on computers to identify known vulnerabilities. The operation scans the operating system and also installed applications. Based on what is detected, Deep Security will recommend security rules that should be applied. Recommendations Scans, support this control by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, and to automatically apply Deep Security rules/filters to detect/prevent exploitation of the identified vulnerabilities.

**Vulnerability Protection** provides agent-based protection for an organization’s computers. The product organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information.
DE.DP Detect / Detection Processes

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events

| DE.DP-2 Detect / Detection Processes | The applicable requirements indicated in this control will generally be determined by organizations carrying out security assessments. This ability to detect security events and provide reports/dashboards on them on a continuing basis is supported by a number of Trend Micro products. These products include Control Manager, Deep Discovery Inspector, Vulnerability Protection, Deep Security, InterScan Web Security Virtual Appliance, OfficeScan, Mobile Security, and ScanMail for Microsoft Exchange. |
| DET-2 Detect / Detection Processes | Detection activities comply with all applicable requirements |
| The NIST Standard SP 800-53 R4 CA-7 Continuous Monitoring, which is referenced by this control, states "Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions." |
| The applicable requirements indicated in this control will generally be determined by organizations carrying out security assessments. This ability to detect security events and provide reports/dashboards on them on a continuing basis is supported by a number of Trend Micro products. These products include Control Manager, Deep Discovery Inspector, Vulnerability Protection, Deep Security, InterScan Web Security Virtual Appliance, OfficeScan, Mobile Security, and ScanMail for Microsoft Exchange. |
| DE.DP-4 Detect / Detection Processes | Custom Defense |
| DET-4 Detect / Detection Processes | Deep Discovery Inspector employs threat detections, which includes information on: Malicious Content, Malicious Behavior, Suspicious Behavior, Exploits, Grayware, Web Reputation, and Disruptive Applications. This threat data can be sent to a centralized logging server for correlation, reporting and archiving with audit record data to support organizational processes for investigation and response to suspicious activities. Deep Discovery Inspector also supports this requirement by providing indicators of compromise (IOC) information to other Trend and third-party security systems such as SIEMs, firewalls and intrusion prevention systems. Deep Discovery Inspector further supports this control by using the least disruptive action of sending email notifications to incident response personnel for the following network events: |
| Event detection information is communicated to appropriate parties | - Threat Events - The number of threat events that reached the configured threshold; |
| The NIST standard SP800-53 r4 SI-4(5) defines "Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging." | - High Risk Hosts Detections - Deep Discovery Inspector identified a high-risk host the information system network; |
| | - Suspicious Hosts Detections - The number of suspicious hosts reached the threshold; |
| | - High Network Traffic - The network traffic volume reached the threshold; |
| | - File Analysis Status - Virtual Analyzer was unable to analyze files; |
| | - Virtual Analyzer Detections - Virtual Analyzer detected malicious content in a sample; |
| | - Deny List - A detection matched an object in the user-defined Deny List; and |
| | - Retro Scan Detections - Retro Scan detected historical callback attempts to C&C servers in the Trend Micro global intelligence list. |
| | Cloud and Data Center Security |
| | Deep Security supports and provides statistical and trending information on vulnerabilities at various levels, including raw network packet data, malware and anti virus signature file updates and effectiveness, this information can be used by an organization to determine the efficiency of the mechanisms in place to counter threats. Deep Security provides real time Integrity Monitoring to monitor entity changes and raise Integrity Monitoring events when changes are detected. Events are forwarded in real time via syslog to the SIEM or when the next heartbeat communication (configurable) to the Deep Security Manager occurs. Deep Security Log Inspection forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving. |
Complete User Protection
The following Complete User Protection products provide event and alert generation and the capability to send the information to organizational appointed personnel:

- **OfficeScan** agent reports to the parent server from which it was installed. The agent sends events and status information to the server in real time. Examples of events are virus/malware detection, agent startup, agent shutdown, start of a scan, and completion of an update.
- **Vulnerability Protection** provides event logging integration with SIEM tools.
- **Endpoint Application Control** provides event notification through a simplified dashboard and management console.
- **InterScan Messaging Security Suite (IMSS)**, sends an email or SNMP notification to specific organizational users upon the occurrence of the following categories of events: Systems Status, Scheduled Update Event; Scanner Update Result; Deep Discovery Advisor Settings, and Smart Scan Event. IMSS will trigger a notification message and also customize the message content for each event.
- **ScanMail for Microsoft Exchange** sends event notifications and timely alerts to administrators or other designated individuals whenever significant system events or outbreak activities occur.
- When **ScanMail for IBM Domino** detects a virus or other threat infection in a mail, attachment, or document, can automatically alert, by email or IBM Instant Messaging and Web Conferencing, the organizational persons designated.
- **PortalProtect** for Microsoft Sharepoint event notifications may be sent to the administrator(s) or other specified recipients. With PortalProtect, notifications can be sent through email, Simple Network Management Protocol (SNMP) Trap, or the Windows Event Log.
- **IM Security** sends alerts and notifications through one of the following methods: Session Initiation Protocol (SIP); Simple Mail Transfer Protocol (SMTP); Simple Network Management Protocol (SNMP) and Windows event log.
- **Control Manager** can notify individuals or groups of recipients about events that occur in the Control Manager network. Configure Event Center to send notifications through the following methods: Email, Windows Event Log; SNMP Trap; Pager; Trigger Application; MSN Messenger; and Syslog.
- **Mobile Security** can be configured to send event notifications via email or SMS text messages to an administrator and/or users: Administrator Notifications/Reports - sends email notifications and reports to the administrator when any system abnormality occurs; User Notifications - sends email and or text messages to notify mobile devices to download and install Mobile Device Agent.
- **InterScan Web Security Virtual Appliance (IWSVA)** can issue several types of notifications in response to program or security event. Administrator notifications are sent through email to the designated administrator contact. User notifications are presented in the requesting client's browser.
<table>
<thead>
<tr>
<th>NIST Framework for Improving CI Cybersecurity - Control</th>
<th>Trend Micro Solution Compliancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE.DP-5 Detect / Detection Processes</td>
<td>The output from systems monitoring tools such as, intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring and network monitoring are all product capabilities within the Trend Micro, Custom Defense, Cloud &amp; Data Center Security, and Complete User Protection solutions. The outputs of the products listed, as part of the Custom Defense, Cloud &amp; Data Center Security, and Complete User Protection solutions, provide input to the continuous improvements of the products and their capabilities.</td>
</tr>
<tr>
<td>Detection processes are continuously improved</td>
<td>Custom Defense:</td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Inspector monitors the organizations information system to detect attacks and indicators of potential attack through the Advanced Threat Scan Engine using a combination of file-based detection scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks. Deep Discovery detection engines deliver expanded APT detection capabilities, including a customizable virtual analyzer and updated inspection and correlation rules designed to detect malicious content, communication, and behavior during every stage of an attack sequence. Deep Discovery Inspector increases the level of monitoring provided whenever there is an indication of increased risk to the organizations operations and assets.</td>
</tr>
<tr>
<td>NIST Standard SP800-53 r4 SI-4 Information Systems Monitoring, supplemental guidance provides &quot;Output from system monitoring serves as input to continuous monitoring and incident response programs.&quot;</td>
<td>Cloud and Data Center Security:</td>
</tr>
<tr>
<td></td>
<td>Deep Security supports this control through the combined functionality of Deep Packet Inspection, and the Firewall. The ability to respond quickly to new or emerging threats and provide corrections to vulnerabilities is also supported by the Trend Micro Smart Protection Network. Deep Packet Inspection (DPI) provides an IDS/IPS capability, which protects operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injection and cross-site scripting. Security updates that provide protection against newly discovered vulnerabilities are automatically delivered to host machines. Detailed event records are produced, which provide valuable information, including the source of the attack, the time, and what the potential intruder was attempting to exploit. The Deep Packet Inspection module is available in both the Deep Security Agent and Deep Security Virtual Appliance for VMware ESX/ESXi. The Firewall module is enterprise-grade, bi-directional, and stateful. It is used to limit communication by source and destination port, IP, MAC addresses, and is protocol-aware. By limiting traffic, the attack surface of systems is reduced, and the risk of unauthorized access to the system is also reduced. Reconnaissance detection is supported by the ability to detect reconnaissance activities such as port scans. The stateful firewall is available in both the Agent and Appliance for VMware ESX/ESXi.</td>
</tr>
<tr>
<td></td>
<td>Complete User Protection:</td>
</tr>
<tr>
<td></td>
<td>Please see RS.MI-3 Respond / Mitigation - Newly identified vulnerabilities are mitigated or documented as accepted risks for the Complete User Protection capability coverage for this control.</td>
</tr>
</tbody>
</table>

NIST Standard SP800-53 r4 RA-5 is referenced in this control: RA-5 states "Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms."
### ID.RA Identity / Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

| ID.RA-2 Identity / Risk Assessment | Threat Connect correlates suspicious objects detected in an organization’s environment and threat data from the Trend Micro Smart Protection Network, by providing on-demand access to Trend Micro intelligence databases, Threat Connect enables an organization to identify and investigate potential threats to their environment. Furthermore, automated correlation facilitates the immediate generation of reports containing detailed threat analyses and remediation recommendations. These reports provide the situational awareness that need to be implemented for a more focused response and remediation activities, and improve an organization’s overall security posture. **Threat Connect** correlates suspicious objects detected in an organization’s environment and threat data from the Trend Micro Smart Protection Network, by providing on-demand access to Trend Micro intelligence databases, Threat Connect enables an organization to identify and investigate potential threats to their environment. Furthermore, automated correlation facilitates the immediate generation of reports containing detailed threat analyses and remediation recommendations. These reports provide the situational awareness that need to be implemented for a more focused response and remediation activities, and improve an organization’s overall security posture. **Trend Micro Smart Protection Network** is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and Web threats. It powers both on-premise and hosted solutions to protect users whether they are on the network, at home, or on the go. Trend Micro Smart Protection Network uses light-weight clients to access its unique in-the-cloud correlation of email, Web and file reputation technologies, as well as threat databases. Protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for those who use it. The smart scan solution uses the Smart Protection Network for in-the-cloud protection. Smart Protection Services provide anti-malware signatures, Web reputation, and threat databases that are stored in-the-cloud. Smart protection uses file reputation technology to detect security risks and Web reputation to proactively block malicious Web sites. File reputation technology works by off-loading a large number of anti-malware signatures that were previously stored on endpoint computers to the Smart Protection Network or Smart Protection Servers. Web reputation technology hosts URLs that were previously stored on the Smart Protection Network, to the Smart Protection Servers. Both technologies ensure smaller bandwidth consumption when updating patterns or querying URL validity. Additionally, Trend Micro continues to harvest information anonymously sent from Trend Micro products worldwide to proactively determine each new threat. **Trend Micro Smart Feedback** provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer’s routine reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides “better together” security, much like an automated neighborhood watch that involves the community in the protection of others. Because the gathered threat information is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer’s personal or business information is always protected. In addition comprehensive security vulnerability including new vulnerability information is available at the Trend Micro website. [http://www.trendmicro.com/vinfo](http://www.trendmicro.com/vinfo)

Security information includes:
- List of malware and malicious mobile code currently active or "in the wild"
- Computer malware hoaxes
- Internet threat advisories
- Malware weekly report
- Threat Encyclopedia, which includes a comprehensive list of names and symptoms for known malware, spam, malicious URLs, and known vulnerabilities, plus writeups on web attacks and online trends.

---

Document TMIC-005-NFCI  Version 1.2,  June 2015  18
<table>
<thead>
<tr>
<th>ID.RA-3</th>
<th>Identity / Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats, both internal and external, are identified and documented</td>
<td></td>
</tr>
</tbody>
</table>

**Control Manager** as a central management service to the Custom Defense, Cloud and Data Center Security, and Complete User Protection solutions, has the ability to indicate the number of security threats detected over 90 days and displaying the threats and the user details in the Security Threats screen. Control Manager counts and consolidates detections having these types of threats:
- Virus/Malware;
- Spyware / Grayware;
- Content violation;
- Spam;
- Phishing email;
- Web violation;
- Web violation;
- DLP incident;
- C&C callback;
- Behavior Monitoring violation; and
- Firewall violation.

Trend Micro provides registered customers with services that help identify the threats that threaten their systems. Within the central management Control Manager the following warn of potential or emerging virus or malware outbreaks by identifying the source of the outbreak:
- Schedules Outbreak Prevention Policy downloads: Control Manager can inform an organization if it downloads Outbreak Prevention Policies that correspond to an ongoing virus outbreak. To receive notification about this event, enable Active Outbreak Prevention Policy received at the Event Center.
- Special Virus Alert: This Control Manager feature, configured at the Event Center, warns an organization when a Trend Micro product detects an outbreak causing virus on your network.

<table>
<thead>
<tr>
<th>PR.DS Protect / Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PR.DS-1</th>
<th>Protect / Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data-at-rest is protected</td>
<td></td>
</tr>
</tbody>
</table>

NIST SP800-53r4 SC-28 is referenced by this control SC-28 states “This control addresses the confidentiality and integrity of information at rest and covers user information and system information”.

**Cloud and Data Center Security**

The Deep Security solution provides Integrity Monitoring of critical systems related information detecting when a system’s critical configuration file or rule set has been modified.

**Complete User Protection**

Trend Micro Endpoint Encryption ensures privacy and protection of data at rest by encrypting data stored on endpoints, files, and folders, removable media in a variety of platform options. Endpoint Encryption provides granular policy controls and flexibly integrates with other Trend Micro management tools, including Control Manager and OfficeScan. Endpoint Encryption implements FIPS 140-2 hardware-based or software-based encryption that is fully transparent to end users, without disrupting productivity. Once deployed, automated reporting, auditing, and policy synchronization with Endpoint Encryption PolicyServer simplifies endpoint security management.

Endpoint Encryption can be used for File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system or as Full Disk Encryption to secure data files, applications, registry settings, temporary files, swap files, print spoolers, and deleted files on any Windows endpoint. Strong preboot authentication restricts access vulnerabilities until the user is validated.
<table>
<thead>
<tr>
<th>PR.DS-5</th>
<th>Protect / Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Custom Defense</strong></td>
<td>Deep Discovery Inspector provides IT administrators with critical security information, alerts, and reports and deploys in offline monitoring mode. It monitors network traffic by connecting to the mirror port on a switch for minimal or no network interruption. Deep Discovery Inspector detects and identifies evasive threats in real-time, along with providing in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.</td>
</tr>
<tr>
<td><strong>Cloud and Data Center Security</strong></td>
<td>Deep Security provides agentless and agent-based protection for physical, virtual, and cloud-based computers. Protection includes:</td>
</tr>
<tr>
<td>- Anti-Malware;</td>
<td>- <strong>Integrity Monitoring</strong> and</td>
</tr>
<tr>
<td>- Web Reputation;</td>
<td>- <strong>Log Inspection.</strong></td>
</tr>
<tr>
<td>- Firewall;</td>
<td>Deep Security firewall solution, provides subnetwork controls that architecturally separate the public front end systems from the internal networks.</td>
</tr>
<tr>
<td>- Intrusion Detection and Prevention;</td>
<td><strong>Complete User Protection</strong></td>
</tr>
<tr>
<td><strong>Cloud and Data Center Security</strong></td>
<td><strong>Data Loss Prevention</strong> safeguards an organization’s digital assets against accidental or deliberate data leakage. DLP allows an organization to:</td>
</tr>
<tr>
<td><strong>Cloud and Data Center Security</strong></td>
<td>- Identify the digital assets to protect;</td>
</tr>
<tr>
<td><strong>Complete User Protection</strong></td>
<td>- Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices; and</td>
</tr>
<tr>
<td><strong>Complete User Protection</strong></td>
<td>- Enforce compliance to established privacy standards</td>
</tr>
<tr>
<td><strong>Complete User Protection</strong></td>
<td><strong>OfficeScan</strong> Device Control regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.</td>
</tr>
<tr>
<td><strong>InterScan Messaging Security</strong></td>
<td><strong>InterScan Messaging Security</strong> monitors keywords or expressions to prevent information leaks, block spam, or block derogatory messages from entering or moving in an organizations network.</td>
</tr>
<tr>
<td><strong>InterScan Web Security Virtual Appliance</strong></td>
<td><strong>ScanMail Suite for Microsoft Exchange</strong> includes default content filtering data leakage prevention policies. There are 10 default data leakage prevention policies configured by region. Compared to standard content filtering policies, keywords in the data leakage prevention policies are regular expression description strings and not the actual keyword.</td>
</tr>
<tr>
<td><strong>InterScan Web Security Virtual Appliance</strong></td>
<td><strong>ScanMail for IBM Domino</strong> integrates the latest Data Loss Prevention (DLP) scan engine, which provides more than 200 predefined DLP templates. The DLP filter allows an organization to define a set of DLP rules and combine multiple rules using logical operations. The enhanced DLP Filter also allows an organization to perform manual and scheduled scanning for the non-mail documents within the Notes database.</td>
</tr>
<tr>
<td><strong>InterScan Web Security Virtual Appliance</strong></td>
<td><strong>IM Security for Microsoft Lync</strong> can be configured to work with the Data Loss Prevention safeguards which allow an organization to protect sensitive data against accidental or deliberate leakage.</td>
</tr>
<tr>
<td><strong>InterScan Web Security Virtual Appliance</strong></td>
<td><strong>InterScan Web Security Virtual Appliance</strong> includes default content filtering data leakage prevention policies. There are 10 default data leakage prevention policies configured by region. Compared to standard content filtering policies, keywords in the data leakage prevention policies are regular expression description strings and not the actual keyword. IWSVA removes the XFF HTTP header from the HTTP request and prevents the privacy information of a client from leaking upstream. When IWSVA detects data leakage that violates a security policy, the application sends and administrator notification through email and a user notification message in the requesting client’s browser.</td>
</tr>
<tr>
<td><strong>InterScan Web Security Virtual Appliance</strong></td>
<td><strong>InterScan Web Security Virtual Appliance</strong> includes default content filtering data leakage prevention policies. There are 10 default data leakage prevention policies configured by region. Compared to standard content filtering policies, keywords in the data leakage prevention policies are regular expression description strings and not the actual keyword. IWSVA removes the XFF HTTP header from the HTTP request and prevents the privacy information of a client from leaking upstream. When IWSVA detects data leakage that violates a security policy, the application sends and administrator notification through email and a user notification message in the requesting client’s browser.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PR.DS-6</th>
<th>Protect / Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trend Micro products are downloaded or distributed on media with a SHA256 checksum.</strong></td>
<td><strong>Integrity checking mechanisms are used to verify software, firmware, and information integrity</strong></td>
</tr>
</tbody>
</table>
# PR.IP - Protect / Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

<table>
<thead>
<tr>
<th>PR.IP-7 Protect / Information Protection Processes and Procedures</th>
<th>Custom Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection processes are continuously improved</td>
<td>Deep Discovery Inspector: Produces reports that use forensic analysis and threat correlations for an in-depth analysis of event logs to identify the threats more precisely. The reports are designed to assist the administrator determine the types and frequency of threat incidents affecting the network. Daily administrative reports enable IT administrators to track the status of threats, while weekly and monthly executive reports keep executives informed about the overall security posture of the organization. The reports available in Deep Discovery Inspector include:</td>
</tr>
<tr>
<td>From NIST SP800-53 r4 PM-6: “Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.”</td>
<td>- Scheduled Reports: Daily, weekly, and monthly reports are designed to provide the correlated threat information.</td>
</tr>
<tr>
<td></td>
<td>- On-Demand Reports: Reports that can be generated as needed that are designed to provide detailed information about specific files.</td>
</tr>
<tr>
<td></td>
<td>- Virtual Analyzer Reports: Virtual Analyzer reports are designed to provide detailed information about specific files.</td>
</tr>
<tr>
<td></td>
<td>DeepSecurity: Provides a higher-level view of the log data, where the information is summarized, and presented in a more easily understood format. The DeepSecurity Reports fill this role, allowing an administrator to display detailed summaries on computers, Firewall and Intrusion Prevention Event Logs, Events, Alerts, etc. In the Reports page, an administrator can select various options for the report to be generated. A Firewall Report, will display a record of Firewall Rule and Firewall Stateful Configuration activity over a configurable date range. By reviewing scheduled reports that have been emailed by the Deep Security Manager to Users, by logging into the system and consulting the dashboard, by performing detailed investigations by drilling-down to specific logs, and by configuring Alerts to notify Users of critical events, an organization can remain apprised of the continuous health and status of their network.</td>
</tr>
<tr>
<td></td>
<td>Complete User Protection</td>
</tr>
<tr>
<td></td>
<td>InterScan Messaging Security creates a number of reports which provide a measure of effectiveness of the controls:</td>
</tr>
<tr>
<td></td>
<td>- Policy and Traffic summary - Shows the total number and size of incoming and outgoing messages. Shows the number of messages matching specific scanning conditions;</td>
</tr>
<tr>
<td></td>
<td>- Virus and Malicious Code summary: Shows a summary of the virus message count by actions;</td>
</tr>
<tr>
<td></td>
<td>- Spam Summary: Shows a summary of the total spam message count by antispm engine, Email reputation, IP profiler, and actions;</td>
</tr>
<tr>
<td></td>
<td>- Sender IP Address Blocking summary: Includes &quot;IP Profiler Summary&quot; and &quot;Email Reputation IP Blocking Summary&quot;. The former shows a summary of the total number of sender connections that reached IP Profiler and are blocked by the different IP Filtering rules. The latter shows the total sender connections that reached Email reputation and are blocked by Email reputation.</td>
</tr>
<tr>
<td></td>
<td>ScanMailSuite for Microsoft Exchange monitors the current status of features and the number of security threats. Generated reports include the number of occurrences of following incidents:</td>
</tr>
<tr>
<td></td>
<td>- ScanMail detects a virus/malware;</td>
</tr>
<tr>
<td></td>
<td>- detected viruses/malware that could not be cleaned;</td>
</tr>
<tr>
<td></td>
<td>- detected spyware/grayware;</td>
</tr>
<tr>
<td></td>
<td>- detected advanced threats;</td>
</tr>
<tr>
<td></td>
<td>- attachments blocked by the attachment blocking policy;</td>
</tr>
<tr>
<td></td>
<td>- spam messages detected by content scanning;</td>
</tr>
<tr>
<td></td>
<td>- phishing messages detected by content scanning;</td>
</tr>
<tr>
<td></td>
<td>- content filtering rule violations detected;</td>
</tr>
<tr>
<td></td>
<td>- suspicious URLs detected by Web reputation;</td>
</tr>
<tr>
<td></td>
<td>- Data Loss Prevention policy incidents detected;</td>
</tr>
<tr>
<td></td>
<td>- Email reputation detections of messages from spam sources;</td>
</tr>
<tr>
<td></td>
<td>- message bodies and attachments not scanned as specified by the Scan Restriction Criteria.</td>
</tr>
</tbody>
</table>
NIST Framework for Improving CI Cybersecurity - Control | Trend Micro Solution Compliancy

PR.PT Protect / Protective Technology
Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

| PR.PT-1 Protect / Protective Technology | Control Manager provides this capability for registered Trend Micro products. Using Ad Hoc Queries administrators can pull, through this quick method, information directly from the Control Manager database. The database contains all log and audit information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Ad Hoc Queries provide a very powerful tool for administrators. While querying data, administrators can filter the query criteria so only the data they need returns. Administrators can export the data to CSV or XML format for further analysis or save the query for future use. Control Manager also supports sharing saved queries with other users so others can benefit from useful queries. |
| Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | NIST SP800-53r4 AU-3(2) states "The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event." The following Complete User Protection products provide coverage of this control: |

**Control Manager** provides this capability for registered Trend Micro products. Using Ad Hoc Queries administrators can pull, through this quick method, information directly from the Control Manager database. The database contains all log and audit information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Ad Hoc Queries provide a very powerful tool for administrators. While querying data, administrators can filter the query criteria so only the data they need returns. Administrators can export the data to CSV or XML format for further analysis or save the query for future use. Control Manager also supports sharing saved queries with other users so others can benefit from useful queries.

**NIST SP800-53r4 AU-3(2) states "The information system provides centralized management and configuration of the content to be captured in audit records generated by ______."**

**Custom Defense**
- **Deep Discovery Inspector** supports this control by enabling organizations to audit and log security related events through inspection of network traffic between and within an organizations network including: communications or links to suspicious/malicious endpoints, suspicious/malicious network traffic, and infected files. Logs include, time stamps, source and destination addresses, identifiers, event descriptions, success/fail indications, rules involved. Security event information can be integrated with an organization's SIEM product if required.
- Deep Discovery Inspector, Detection Logs can be queried for additional information, by detection types (Threats, Disruptive Applications, Malicious URLs, Virtual Analysis, Correlated Incidents, and Custom Detections), and time range.

**Cloud and Data Center Security**
- **Deep Security** supports this control by enabling organizations to audit and log security related events through inspection of host-based network traffic for malicious activity, key files for changes, and system logs for indicators of suspicious activity. Logs include for example, time stamps, source and destination addresses, identifiers, event descriptions, success/fail indications, rules involved. Security event information can be integrated with an organization's SIEM product if required.
- Deep Security further supports this control through the defined audit events and the ability to carry out specific queries against the audit logs simplifying the ability to locate the information of interest. In addition, deep packet inspection permits the capture of event data, at the packet level, which can be analysed for additional audit data relating to the security event

**Complete User Protection**
- **OfficeScan**: Provides the following security incident logs: Virus/Malware; Spyware/Grayware; Firewall; Web Reputation; Suspicious Connection; C&C Callback; Behavior Monitoring; DLP; and Device Control logs
- **Vulnerability Protection**: Allows an organization to display detailed summaries on computers, Firewall and Intrusion Prevention Event Logs, Events, Alerts, etc. In the Reports page, an organization can select various options for the report to be generated. A Firewall Report for example displays a record of Firewall Rule and Firewall Stateful Configuration activity over a configurable date range. The Vulnerability Protection product allows detailed investigations by drilling-down to specific logs, and by configuring Alerts to notify Users of critical events.
- **Endpoint Application Control**: Records security relevant events related to server, agents, and policies. The following event are logged: Policy violations; Administrator activities; Endpoint events; and Server events.
- **Endpoint Encryption**: the Endpoint Encryption, PolicyServer enforces secure authentication and provides real-time auditing and reporting tools. PolicyServer records log events using predefined criteria including access attempts, system errors, modifications to users or groups, policy changes, and compliance issues.
- **Data Loss Prevention**: Provides a Log Query screen to query the following logs that DLP has generated over time: Policy Deployment; DLP Incidents; Server Status; System Events; and Security Audit.
- **Interscan Messaging Security**: Provides Centralized Logging and Reporting, a consolidated, detailed report provides top usage statistics and key mail usage data. Centralized logging allows administrators to quickly audit message-related activities. IMSS Mail Auditing and Tracking provides detailed logging for all messages to track and identify message flow related issues.
- **ScanMail Suite for Microsoft Exchange**: ScanMail Suite audit event log tracking includes: the virtual server name; user name; current time of Audit Event; remote host IP address; event type (Three types: log in/out, configuration, operation). ScanMail records detailed event tracking logs for Search & Destroy. Because Search & Destroy allows administrators to view and delete Exchange components from users mailboxes, a comprehensive audit trail of Search & Destroy operations is useful in case of user misunderstandings.
PR.PT-1 (cont.)

**PortalProtect:** Provides comprehensive information about various scans. It saves this information to a database. The following is a listing of the information contained within the various log types:
- Security risk scan logs—contains information about the: Date & Time, Violator, Security Risk Name, Action, File Name, and Location. The Security risk scan logs can be filtered for: All; Detected virus/malware; Uncleanable virus/malware and Detected spyware/grayware.
- File blocking logs—contains information about the: Date & Time, Violator, Policy Name, Action, File Name, Triggered File Type/Name, and Location.
- Content Filtering logs—contains information about the: Date & Time, Violator, Policy Name, Action, File name/Web Content Title, Triggered Keywords, and Location.
- Web reputation logs—contains information about the: Date & Time, Violator, Risk Level, Web Content Title, Suspicious URL, Action, and Location.
- Update logs—contains information about the: Date & Time, and Description.
- Scan events logs—contains information about the: Date & Time, and Description.
- Backup logs—contains information about the: Date & Time, Violator, Security Risk Name, File Name, Location, and Backup Path.
- Unscannable files logs—contains information about the: Date & Time, Location, Violator, Reason, File Name, and Action.
- Event tracking logs—contains information about the: Username, Event time, IP address, Event type, Source type, and Description.
- Data protection logs—contains information about the: Date & Time, Violator, Policy Name, Action, File Name/Web Content Title, Template(s), and Location.

**IM Security for Microsoft Lync:** Logs are time-sequential records of IM Security events. These events refer to actions initiated by either a user or the IM Security server. IM Security allows you to query unformatted logs or display them through reports. Logs are stored in the IM Security database. The following logs are available:
- Virus Scan - Indicates the source of the infection or intrusion;
- File Blocking - Enumerates blocked files with matching File Blocking rules;
- Content Filtering for files logs - Enumerates files with matching Content Filtering rules;
- Content Filtering for IM logs - Enumerates messages with matching Content Filtering rules;
- Data Loss Prevention for files - Enumerates files that triggered Data Loss Prevention policies;
- Data Loss Prevention for IM - Enumerates messages that triggered Data Loss Prevention policies;
- Web Reputation for IM - Enumerates messages that contain web threats (malicious URL addresses);
- Web Reputation for file - Enumerates files that contain web threats (malicious URL addresses);
- Communication Control - Displays the contacts that triggered the “Block” action of a Communication Control policy;
- Update - Indicates the types of updates performed, including the result;
- Event tracking - Provides information about all console operations.
- Control Manager: Displays auditing information related to managed products. The product auditing event log data includes:
- Received - Displays the time that Control Manager receives data about the managed product event.
- Generated - Displays the time that the managed product generates data about the event.
- Host Displays one of the following: The host name of the server on which the managed product installs; or The host name of a computer with an engine (for example OfficeScan client) installed.
- User - Displays account information.
- Event Category - Displays the category of event that occurred. Example: management console access
- Event Level - Displays the severity of an event.
- Event Description - Displays the description a managed product provides for the event.

**Mobile Security for Enterprise:** The Mobile Device Agents generate malware protection logs, web threat protection logs, policy violation logs, and event logs. The log data is sent to the Mobile Security Server, which enables Mobile Device Agent logs to be stored on a central location. This allows an organization to assess the protection policies and identify mobile devices at a higher risk of infection or attack. The logs generated are:
- Malware Protection Log - Mobile Device Agent generates a log when malware is detected on the mobile device;
- Web Threat Protection Log - Mobile Device Agent generates a log when it blocks a dangerous or malware infected Web page;
- Event Log - These logs are generated when certain actions are taken by the server and the Mobile Device Agent;
- Policy Violation Log - These logs include information about the policy compliant status of the Mobile Device Agents.
### PR.PT-1 (cont.)

**InterScan Web Security Virtual Appliance:** The audit log contains information that describes any configuration changes that users make to the application. This includes any configuration changes relating to: User Identification; Policy Acknowledgement; Authentication White List; Policy Deployment; Database Connection; Quarantine Management; System Time; Scheduled Times; Register to Control Manager; Web Security Hybrid; Replication Configuration; Central Log/Reporting; Scan Method; and proxy auto config (PAC) Files Management.

**Complete User Protection**

**OfficeScan** protects removable media by scanning for boot viruses before shutting down the endpoint. This prevents any virus/malware from executing when a user reboots the endpoint from the disk. It scans the boot sector of the USB storage device after plugging in: Automatically scans only the boot sector of a USB storage device every time the user plugs it in (Real-time Scan). Scans all files in removable storage devices after plugging in: Automatically scans all files on a USB storage device every time the user plugs it in (Real-time Scan).

**Endpoint Encryption** ensures privacy by encrypting data stored on endpoints, files and folders, and removable media (USB drives) in a variety of platform options. End users also have the flexibility to locally manage File Encryption by encrypting individual files, folders, or removable media on the fly, safeguarding their data regardless of where it travels. There is also the ability to disable optical and USB drives. Through Control Manager the Endpoint Encryption can also be controlled to disable access and encryption to optical drives and USB devices.

**Data Loss Prevention Endpoint** helps organizations protect sensitive information from accidental disclosure and intentional theft. DLP Endpoint prevents loss of sensitive data through endpoint-based enforcement and accurate fingerprinting and content matching technology. DLP Endpoint detects digital assets and automatically takes actions specified in an organization's policies, from blocking and logging to encrypting and alerting. This includes end user device control, with support for storage devices: CD/DVD, USB and non-storage devices: COM and LPT ports, infrared and imaging devices, modems, PCMCIA card, print screen key.

### PR.PT-2 Protect / Protective Technology

**Removable media is protected and its use restricted according to policy**

**Custom Defense**

**Deep Discovery Inspector** provides IT administrators with critical security information, alerts, and reports and deploys in offline monitoring mode. It monitors network traffic by connecting to the mirror port on a switch for minimal or no network interruption. Deep Discovery Inspector detects and identifies evasive threats in real-time, along with providing in-depth analysis and actionable intelligence needed to discover, prevent, and contains attacks against corporate data. Deep Discovery Inspector also detects and denies outgoing malicious traffic or traffic to known malicious destinations. Deep Discovery Inspector displays all hosts with Command & Control (C&C) callbacks detected by network scanning, Deny List matches, and Virtual Analyzer detections. Viewing hosts with C&C callbacks in the past 1 hour, 24 hours, 7 days, or 30 days allows system or network administrators to take appropriate action (blocking network access, isolating computers according to IP address) in order to prevent malicious operations from affecting hosts. The detected callback type can be viewed for detailed information about the hosts and the callbacks.

**Cloud and Data Center Security**

**Deep Security** solution provides host based boundary protection through the host application stateful inspection firewall, through the host deep packet inspection, and through web reputation services. This can be implemented at the server or workstation level in the physical or virtual environments. Deep Security provides agentless and agent-based protection for physical, virtual, and cloud-based network interfacing computers. Protection includes: Anti-Malware; Web Reputation; Firewall; Intrusion Detection and Prevention; Integrity Monitoring; and Log Inspection.

Deep Security further supports this control by its support of VMware's NSX, taggng infected virtual machines and allowing them to be automatically quarantined.

Deep Security firewall solution provides subnetwork controls that architecturally separate the public front end systems from the internal networks. The firewall can be used to limit the rules to analysis and assess the inbound and outbound communications at specific "choke" points in the systems architecture.

Deep Security also supports Application Control rules that can provide protection in regards to outbound traffic. Rules can be defined to detect allowed protocols over unexpected ports which may be an indication of malware attempting to call home to a command and control server. The product has the ability to detect and control unexpected protocol traffic on servers - for example, observing FTP traffic originating from an Exchange server.

---

**Document TMIC-005-NFCI Version 1.2, June 2015**
Complete User Protection

**Interscan Messaging Security Suite** (IMSS) delivers protection on a single, highly scalable platform with centralized management for comprehensive email security at the gateway. Many types of file attachments, such as executable programs and documents with embedded macros, can harbor viruses. Messages with HTML script files, HTML links, Java applets, or ActiveX controls can also perform harmful actions. IMSS allows an organization to configure the types of messages that are allowed to pass through the SMTP gateway. IMSS performs virus detection using Trend Micro scan engine and a technology called pattern matching. The scan engine compares code in files traveling through your gateway with binary patterns of known viruses that reside in the pattern file. If the scan engine detects a match, it performs the actions as configured in the policy rules. The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks. The C&C Contact Alert Services allows IMSS to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files. IMSS analyzes email messages and their attachments, traveling to and from your network, for appropriate content.

**InterScan Web Security Virtual Appliance** stops threats at the gateway before they get to an organization’s endpoints. It delivers real-time protection against the full scope of malicious code, and other web threats, using anti-malware, the strongest advanced threat protection, URL filtering, and web reputation. InterScan Web Security leverages the real-time protection of Trend Micro’s global Smart Protection Network, ensuring organization are protected against new emerging threats.

**OfficeScan**: Web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis.

**Vulnerability Protection**: Determines when a Stateful Configuration is in effect on a computer, packets are analyzed within the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols (e.g. UDP and ICMP) a pseudo-stateful mechanism is implemented based on historical traffic analysis. Vulnerability Protection is a standalone product replacement for the Intrusion Defense Firewall (OfficeScan module).
RS.AN Respond / Analysis

Analysis is conducted to ensure adequate response and support recovery activities.

| RS.AN-2 Respond / Analysis | Overview – The compliancy statements provided below provide product details to assist an organization understand how the impact of an incident is communicated, by letting the organization know how wide spread the incident is, the systems that are affected, and the severity of the incident etc. The compliancy statements also provide details about what and how the products operate and how the customer will know and understand the full impact of the incident.

**Custom Defense**

**Deep Discovery Inspector** can support this control for incident handling through the capabilities of the Virtual Analyzer function, which includes the following features:
- Threat execution and evaluation summary;
- In-depth tracking of malware actions and system impact;
- Discovery of network connections initiated;
- Indications provided of system file/Registry modification;
- System injection behavior detection;
- Identification of malicious destinations and command-and-control (C&C) servers;
- Exportable forensic reports and PCAP files; and
- Generation of complete malware intelligence for immediate local protection.

Deep Discovery Inspector also supports this control by automatically detecting suspicious/malicious network traffic incidents indicative of networks under attack or which have been breached.

In the event of a security incident Deep Discovery Inspector provides Indicators Of Compromise (IOC) information to other Trend Micro and third-party security systems such as SIEMs, firewalls and intrusion prevention systems.

Deep Discovery Inspector further supports this control again through the Virtual Analyzer capability which provides indications of a security incident such as an attack and alerts the organization to the attack. The organization itself is responsible for the handling of the attack and mitigation strategies to be implemented to ensure continuity of operations.

**Cloud and Data Center Security**

**Deep Security** raises alerts when incidents occur that require special attention. Alerts can be raised due to security Events such as the detection of malware or an abnormal restart on a protected computer, or they can be system events. Deep Security can be configured to send email notifications when specific Alerts are raised. Deep Security Recommendation Scan supports this control by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits. Deep Security further supports this control through it’s support of VMware’s NSX by tagging infected virtual machines allowing them to be automatically quarantined.

**Complete User Protection**

**OfficeScan:** OfficeScan protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. To contain outbreaks, OfficeScan enforces outbreak prevention policies and isolates infected computers until they are completely risk-free.

The OfficeScan Damage Cleanup Services cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, viral files) through a fully automated process. To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following: Detects and removes live Trojans; Kills processes that Trojans create; Repairs system files that Trojans modify and Deletes files; and applications that Trojans drop.

The OfficeScan Web reputation technology proactively protects agent computers within or outside the corporate network from malicious and potentially dangerous websites. Web reputation breaks the infection chain and prevents downloading of malicious code.

The OfficeScan Firewall protects agents and servers on the network using stateful inspections and high performance network virus scans. Create rules to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.
The OfficeScan Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage. Data Loss Prevention allows administrators to: Identify the digital assets to protect; Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email messages and external devices; and Enforce compliance to established privacy standards.

The OfficeScan Device Control regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

The OfficeScan Behavior Monitoring constantly monitors agents for unusual modifications to the operating system or on installed software.

**Vulnerability Protection** provides a security incident handling capability through the firewall component which detects, analysis and prevents denial of service attacks and through the Intrusion Prevention module which provides security incident handling capability against known and zero-day attacks. Using vulnerability rules to shield known attacks. Detects and defends against SQL injection attacks, cross site scripting attacks and shield (contains) vulnerabilities until code fixes can be completed. The Intrusion Prevention module also identifies malicious software accessing the organizations network and reduces the vulnerability exposure of the organizations servers.

**Data Loss Prevention** uses five content-aware mechanisms to identify and protect digital assets stored on laptops, desktops, servers, and (with Network Monitor) in network traffic.

- **Expression matching**: DLP identifies digital assets using predefined and customized expressions. Expression matching is best used with structured content, such as credit card numbers, national ID numbers, or phone numbers.
- **File attribute matching**: DLP identifies digital assets using file attributes, such as file type and file size. DLP performs true file type detection to determine the correct file type even if the extension is altered.
- **Fingerprint matching**: DLP acquires fingerprints from a stored document and compares these with fingerprints acquired from a transmitted file. If the number of common fingerprints matches the number specified in a template, DLP determines that the transmitted file is sensitive. Fingerprint matching works best with unstructured content.
- **Keyword list matching**: DLP identifies digital assets using predefined and customized keyword lists.
- **Template matching**: DLP identifies digital assets using predefined and customized templates that combine data identifiers (expressions, file attributes, fingerprints, and keyword lists) with operators (such as AND and OR) to form condition statements. If conditions are met, DLP takes actions based on policy settings.

**InterScan Messaging Security Suite (IMSS)** integrates antivirus, anti-spam, anti-phishing, and content filtering technology for complete email protection. This software solution features antivirus and zero-day protection to block known and potential viruses. IMSS performs virus detection using the scan engine and a technology called pattern matching. The scan engine compares code in files traveling through an organization's gateway with binary patterns of known viruses that reside in the pattern file. If the scan engine detects a match, it performs the actions as configured in the policy rules.

The Advanced Threat Scan Engine ATSE uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks. ATSE detects and identifies both known and unknown advanced threats, protecting an organization's system from new threats that have yet to be added to patterns.

C&C Contact Alert Services allows IMSS to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects. C&C Contact Alert Services provides IMSS with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks.

IMSS analyzes email messages and their attachments, traveling to and from an organizations network, for appropriate content. Content that is deemed inappropriate, such as personal communication, large attachments, and so on, can be blocked or deferred effectively using IMSS. By flooding a mail server with large attachments, or sending messages that contain multiple viruses or recursively compressed files, individuals with malicious intent can disrupt mail processing. IMSS allows an organization to configure the characteristics of messages that they want to stop at the SMTP gateway, thus reducing the chances of a DoS attack. Many types of file attachments, such as executable programs and documents with embedded macros, can harbor viruses. Messages with HTML script files, HTML links, Java applets, or ActiveX controls can also perform harmful actions. IMSS allows an organization to configure the types of messages that are allowed to pass through the SMTP gateway.
IMSS provides tools to enforce and ensure compliance with existing organizational acceptable usage policies - non-business-related email traffic has become a problem in many organizations. Spam messages consume network bandwidth and affect employee productivity. Some employees use company messaging systems to send personal messages, transfer large multimedia files, or conduct personal business during working hours.

IMSS provides tools for monitoring and blocking content to help reduce the risk that messages containing inappropriate or confidential material will be allowed through an organizations email gateway.

By auto-deleting messages that contain mass-mailing viruses, an organization can avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value. The identities of known mass mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs ActiveUpdate Servers. An organization can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.

IMSS’s ability to protect an organizations environment against spyware and other types of grayware enables them to significantly reduce security, confidentiality, and legal risks to the organization.

IMSS can make use of the detection technology used by Spam Prevention Solution (SPS) based on content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high-performance, real-time detection that is highly adaptable, even as spam senders change their techniques.

IMSS with the web-based End User Quarantine management console, end-users can manage messages that IMSS quarantines.

In addition to SMTP traffic, IMSS can also scan POP3 messages at the gateway as messaging clients in the organizations network retrieve them.

IMSS can make use of the Outbreak Prevention Services delivered through Trend Micro Control Manager which reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in IMSS to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available.

**ScanMail Suite for Microsoft Exchange:** Protects an organizations Exchange mail servers. Once installed, ScanMail can protect servers from viruses/malware, Trojans, worms, spyware/grayware and malicious URLs. ScanMail also sustains business and network integrity by filtering spam messages and messages containing undesirable or unwanted content. ScanMail notifications send timely alerts to administrators or other designated individuals whenever significant system events or outbreak activities occur. When an attack occurs, it is vital that administrators receive early warning to prevent the attack from spreading. Trend Micro recommends setting ScanMail to send alerts to key network security professionals when outbreak conditions threaten the network. Outbreak Alert can be used to set ScanMail to automatically notify designated individuals.

- Antivirus features include - SMTP scanning (Transport scanning) and store level scanning; Leveraging Microsoft Virus Scanning API to scan messages at a low-level in the Exchange store; Detect and take action against viruses/malware, Trojans, and worms; Detect and take action against spyware/grayware;
- Use true file type recognition to detect falsely labeled files; Use Trend Micro recommended actions or customize actions against viruses/malware; and Detect all macro viruses/malware and remove them or use heuristic rules to remove them.
- The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.
- ScanMail incorporates IntelliTrap technology. Use IntelliTrap to scan for packing algorithms to detect packed files. Enabling IntelliTrap allows ScanMail to take user-defined actions on infected attachments and to send notifications to senders, recipients, or administrators.
- Trust Scan Once ScanMail scans a message on an Edge or Hub Transport server, ScanMail adds scan information to the message. When the message reaches the Mailbox, ScanMail evaluates the scan information to prevent redundant use of resources. ScanMail only scans the message if the message was scanned with an older scan engine or pattern file or if ScanMail has not previously scanned the message.
- ScanMail separates the unscannable message count from the virus/malware count. Unscannable files can be files that fall outside of the Scan Restriction Criteria, encrypted files, or password protected files.
PortalProtect for Microsoft SharePoint: is a server-based security solution for Microsoft Windows SharePoint Services 3/4, including Microsoft Office SharePoint Server. Trend Micro designed PortalProtect to provide protection against attacks from viruses and other security threats. It provides real-time background scanning of all content whenever its checked-in, checked-out or published to a SharePoint Server. It also provides manual and scheduled scanning of content stored in the SharePoint Services SQL content store. The security incident handling, detection and analysis, containment, eradication and recovery includes:

- Antivirus: Uses proactive multi-threaded scanning to detect and clean viruses in real-time from multiple access points when authors check documents in or out, or when someone opens it for reading. Uses Trend Micro IntelliScan™ to detect and scan true file types regardless whether the file extension was changed;
- Detects and removes potentially harmful macros viruses; Uses ActiveAction to sort threats into such categories such as viruses, malicious macro codes, and additional threats.
- File Blocking: Uses file blocking during a virus outbreak to temporarily block all files types as designated by the administrator; Provides policy based file blocking that is integrated with Microsoft Active Directory users/groups or SharePoint users/groups.
- Content Filtering Scans: Whenever a file or Web content is uploaded or posted to SharePoint sites, Content Filtering evaluates it according to user-defined policies. Each policy contains a list of keywords and phrases. Content filtering compares the file or Web content with the list of these keywords and phrases and takes the pre-selected action against it in real-time.
- Web Reputation Filtering: Web reputation scans URLs contained in Web content and applies configurable actions when malicious URLs are detected. Additionally, this enhancement enables the user to select both manual and scheduled scans for Web Reputation.
- Quarantine Management: Quarantine Management provides the functionality to manage all quarantined files in a farm even though they were quarantined by a different PortalProtect on different server. The PortalProtect administrator can query, delete, restore or download quarantined files.
- Data Protection: PortalProtect enables an organization to use data protection policies and compliance patterns to detect sensitive data in both documents and Web content.

IM Security for Microsoft Lync - Instant messaging can mean instant exposure to fast-moving attacks designed to spread malware, lure victims to malicious sites, and steal data. Trend Micro IM Security for Microsoft Lync Server secures real-time IM communications by stopping the wide range of threats. In-the-cloud Web Reputation blocks links to malicious sites before the links can be delivered. Signature-independent

Custom Defense

Deep Discovery Inspector: Produces reports that use forensic analysis and threat correlations for an in-depth analysis of event logs to identify the threats more precisely. The reports are designed to assist the administrator determine the types and frequency of threat incidents affecting the network. Daily administrative reports enable IT administrators to track the status of threats, while weekly and monthly executive reports keep executives informed about the overall security posture of the organization.

The reports available in Deep Discovery Inspector include:
- Scheduled Reports: Daily, weekly, and monthly reports are designed to provide the correlated threat information.
- On-Demand Reports: Reports that can be generated as needed that are designed to provide detailed information about specific files.
- Virtual Analyzer Reports: Virtual Analyzer reports are designed to provide detailed information about specific files.

Cloud and Data Center Security

Deep Security through the Integrity Monitoring capability detects and reports malicious and unexpected changes to files and systems registry in real time. This provides administrators with the ability to forensically track both authorized and unauthorized changes made to the instance. The ability to detect unauthorized changes is a critical component as it provides the visibility into changes that could indicate the compromise of an instance.

Complete User Protection

OfficeScan - After a Data Loss Prevention incident occurs, OfficeScan logs the incident details in a specialized forensic database. OfficeScan also creates an encrypted file containing a copy of the sensitive data which triggered the incident and generates a hash value for verification purposes and to ensure the integrity of the sensitive data. OfficeScan creates the encrypted forensic files on the agent machine and then uploads the files to a specified location on the server.

Data Loss Prevention - The DLP Server stores both incident logs and forensic data in a local file system. DLP automatically encrypts the forensic data with a pre-defined password and securely stores the data on the DLP server.

ScanMail Suite for Microsoft Exchange when integrated with Virtual Analyzer can produce exportable forensic reports and PCAP files.
### NIST Framework for Improving CI Cybersecurity - Control

#### Trend Micro Solution Compliancy

<table>
<thead>
<tr>
<th>RS.AN-4 Respond / Analysis</th>
<th>See response to RS.AN-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents are categorized consistent with response plans</td>
<td></td>
</tr>
</tbody>
</table>

#### RS.CO Respond / Communications

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies

<table>
<thead>
<tr>
<th>RS.CO-2 Respond / Communications</th>
<th>See the response to DE.AE-2 for IR-8 Incident Response Plan coverage.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events are reported consistent with established criteria</td>
<td></td>
</tr>
<tr>
<td>The referenced NIST SP800-53r4 IR-6 Supplemental Guidance states &quot;Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling&quot;. IR-6 Incident Reporting - is not applicable, it is outside of the reporting of Trend Micro products.</td>
<td></td>
</tr>
</tbody>
</table>

#### RS.MI Respond / Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

<table>
<thead>
<tr>
<th>RS.MI-1 Respond / Mitigation</th>
<th>See response to RS.AN-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents are contained</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RS.MI-2 Respond / Mitigation</th>
<th>See response to RS.AN-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents are mitigated</td>
<td></td>
</tr>
</tbody>
</table>
RS.MI-3 Respond / Mitigation

Recently identified vulnerabilities are mitigated or documented as accepted risks.

The referenced NIST SP800-53r4 CA-7 states "Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information."

NIST SP800-53r4 RA-5 Vulnerability Scanning states "Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD)."

The referenced NIST SP800-53 RA-5 Vulnerability Scanning states "Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms;"

Custom Defense

Deep Discovery Inspector can automatically schedule the generation of Host Severity Reports, which provide information about threat detections by host. These threats are mapped to threat life cycle rules to determine overall host vulnerability levels, and then displayed in summary and detailed sub reports.

Cloud and Data Center Security

Deep Security Recommendation Scan supports this requirement by allowing organizations to automate scanning of systems and patch levels against the latest Critical Vulnerability and Exposure (CVE) database, to automatically apply Deep Security rules/filters to detect/prevent exploitation of these vulnerabilities and to produce audit logs and reports which can be used to support a continuous monitoring program or audits. Deep Security also assists in satisfies this control by the firewall module which will detect reconnaissance activities of intruders and provide an indication that such activity is taking place to the systems administrator. The Deep Security solution further supports and provides statistical and trending information on vulnerabilities at various levels, including raw network packet data, malware and anti-virus signature file updates and effectiveness, this information can be used to determine the efficiency of the mechanisms in place to counter threats.

The Deep Security, Recommendation Scan, Policies and Rules can be updated to reflect new software being installed on a computer, new operating system vulnerabilities being discovered or because a previously vulnerability was corrected by an operating system or software service pack. Because of the dynamic nature of the security requirements on a computer, the Recommendation Scans can be run on a regular/automated basis as a scheduled task, which will assess the current state of the computer and compare it against the latest Deep Security protection module updates to see if the current security Policy needs to be updated. In addition Deep Security can be configured to automatically assign and unassign Rules after a Recommendation Scan.

Deep Security supports compliance with this control by providing the audit and log information on when vulnerabilities are identified. In addition when a new vulnerability is identified Deep Security provides updated patches to close down this newly discovered vulnerability automatically.

Complete User Protection

OfficeScan: A security risk outbreak occurs when detections of virus/malware, spyware/grayware, and shared folder sessions over a certain period of time exceed a certain threshold. There are several ways to mitigate, respond to, and contain outbreaks in the network, including:

Enabling OfficeScan to monitor the network for suspicious activity; Blocking critical agent endpoint ports and folders; Sending outbreak alert messages to agents; and Cleaning up infected endpoints.

Event Monitoring provides a more generic approach to protecting against unauthorized software and malware attacks as accepted risks. It monitors system areas for certain events, allowing administrators to regulate programs that trigger such events. When Event Monitoring detects a monitored system event, it performs the action configured for the event. The following lists possible actions that administrators can take on monitored system events.

- Assess - OfficeScan always allows programs associated with an event but records this action in the logs for assessment;
- Allow - OfficeScan always allows programs associated with an event;
- Ask when necessary - OfficeScan prompts users to allow or deny programs associated with an event and add the programs to the exception list if the user does not respond within a certain time period, OfficeScan automatically allows the program to run. The default time period is 30 seconds;
- Deny - OfficeScan always blocks programs associated with an event and records this action in the logs. When a program is blocked and notifications are enabled, OfficeScan displays a notification on the OfficeScan computer.

The OfficeScan firewall is a stateful inspection firewall; it monitors all connections to the OfficeScan agent and remembers all connection states. It can identify specific conditions in any connection, predict what actions should follow, and detect disruptions in a normal connection. Therefore, effective use of the firewall not only involves creating profiles and policies, but also analyzing connections and filtering packets that pass through the firewall.

The OfficeScan firewall also includes an Intrusion Detection System (IDS). When enabled, IDS can help identify patterns in network packets that may indicate an attack on the OfficeScan agent.

Vulnerability Protection: Recommendation Scans - The security Policy that is assigned to the computer is made up of a collection of Rules and settings designed for a computer running the Windows Desktop 7 operating system. However, a static Policy can soon fall out of date. This can be because of new software being installed on the computer, new operating system vulnerabilities being discovered for which Trend Micro has created new protection Rules, or even because a previous vulnerability was corrected by an operating system or software service pack. Because of the dynamic nature of the security requirements on a computer, Recommendation Scans should be run regularly, which will assess the current state of the computer and compare it against the latest Vulnerability Protection, protection module updates to see if the current security Policy needs to be updated.

| **RS.MI-3 (cont.)** | **Endpoint Encryption**: Provides a Patch Management function when Full Disk Encryption is implemented.  
**Data Loss Prevention**: The complete DLP Endpoint solution employs a client-server architecture with a software agent, server, remote crawler, and Web-based console. The Web console supports an administrative workflow (flow control) for defining digital assets, creating confidential rules, deploying policies to agents, performing data discovery scans, monitoring, and reporting.  
**InterScan Messaging Security**: Makes use of the Advanced Threat Scan Engine (ATSE). ATSE identifies both known and unknown advanced threats, and uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks. Major features include: Detection of zero-day threats; Detection of embedded exploit code; Detection rules for known vulnerabilities;  
and Enhanced parsers for handling file deformities.  
**ScanMail for Microsoft Exchange**: This product produces Vulnerability Reports which provide new vulnerability and risk information to management teams based on: Machine risk level assessment; Vulnerability assessment; Most commonly cleaned infections; Worst damage potential vulnerabilities; and Vulnerabilities ranked by risk level.  
This product also makes use of the Advanced Threat Scan Engine (ATSE) to carry out the: Detection of zero-day threats; Detection of embedded exploit code; Detection rules for known vulnerabilities; and Enhanced parsers for handling file deformities.  
**PortalProtect for Microsoft Sharepoint**: PortalProtect provides comprehensive information about various scans. It saves this information to a database, which can be queried for analysis. For example, an analysis of the Security Risk scan logs can show the most common viruses and scan actions and see which users are introducing viruses to the network. This product uses both notification and logs to identify new vulnerabilities in an organizations SharePoint environment. It documents and sends reports to share vulnerability information to other security team members.  
**IM Security for Microsoft Lync**: This product makes use of Data Loss Prevention Policies to allow companies to monitor the flow of sensitive information over the network. Policy rules, through use of Data Loss Prevention templates, help to manage the distribution of sensitive data across the network. Administrators can scale policies to apply to the entire company, groups, or specific endpoints.  
To provide current information about the security and vulnerabilities of the Lync Server environment, IM Security is preconfigured to generate reports based on Virus Scan, File Blocking, Content Filtering (file transfers and instant messages), URL filtering (Web Reputation), Data Loss Prevention, and server traffic. Reports can be generated on demand or scheduled on a daily, weekly, or monthly basis.  
**Control Manager**: can correlate the output from registered products including Deep Discovery Inspector and Deep Security to determine the presence of multi-vulnerability / multi-hop attack vectors. The Control Manager is a central management console that manages the registered Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Control Manager enables system administrators to monitor and report on activities such as infections, security violations, vulnerabilities (known and new) or virus/malware entry points. System administrators can download and deploy update components and patches throughout the network, helping ensure that protection is consistent and up to date.  
**Mobile Security for Enterprises**: Provides an overview of mobile devices status and component details. Specific to this control it scans for patch levels and indicates if a mobile device is:  
- Healthy - components on the mobile device are up-to-date;  
- Non Compliant - Mobile device is enrolled to the Mobile Security Server, but does not comply with the server policies;  
- Out-of-Sync - Mobile device is enrolled to the Mobile Security Server but either the components or the policies are out of date;  
- Inactive - Shows that the mobile device is not yet enrolled to the Mobile Security Server.  
- In terms of patch management there is the ability to view the mobile device program patch and component update status:  
  - Current version; Up-to-Date; Out-of-Date; Update Rate; Upgraded; Not Upgraded; and Upgrade Rate.  
**InterScan Web Security Virtual Appliance**: Scans for functions, ports, protocols, and services that should not be accessible to users or devices through: Web Reputation; Upload Scanning; HTTPS Decryption Scanning; FTP Scanning; Application Control; HTTP Inspection; URL Monitoring; Download Scanning; URL Filtering; Spyware Scanning; and Java Applet and ActiveX Scanning. |

---

Document TMIC-005-NFCI  
Version 1.2, June 2015  

32