FISMA / NIST 800-53 REVISION 3 COMPLIANCE

Mandated by the Federal Information Security Management Act (FISMA) of 2002, the National Institute of Standards and Technology (NIST) created special publication 800-53 to provide guidelines on security controls for Federal Information Systems. The risk management framework in 800-53 Revision 3 provides civilian federal agencies with guidelines for breaking down FISMA into areas of IT controls that can be implemented as policy, and assessed for compliance. The guidelines apply to all components of an information system that process, store, or transmit federal information.

DEEP SECURITY HELPS MEET NIST 800-53 REVISION 3 REQUIREMENTS

Trend Micro Deep Security is server and application protection software that allows systems to become self-defending. It is integral to datacenter modernization initiatives including virtualization and cloud computing, as well as to addressing compliance requirements. Government agencies can include Deep Security as a key component of their strategies and processes to help assure service levels, policy compliance and appropriate risk management, secure assets and services, and reduce the cost and complexity of heterogeneous IT infrastructure management

Deep Security helps ensure compliance across the following NIST 800-53 Revision 3 control classes and families:

- *Access control*
- *Audit & accountability*
- *Certification accreditation & security assessments*
- *Configuration management*
- *Identification & authentication*
- *Incident response*
- *Risk assessment*
- *System & communications protection*
- *System & information integrity*

One or more Deep Security protection modules are deployed to the server or virtual machine in a single Deep Security Agent. The Deep Security Agent is centrally managed across physical and virtual environments. Security Center experts produce updates to respond to the latest vulnerability threats and exploits. These security updates can be delivered automatically, or on demand, to achieve rapid and timely deployment to thousands of systems within minutes.

- **Intrusion detection and prevention system (IDS/IPS):** Advanced deep packet inspection shields vulnerabilities in operating systems and enterprise applications until they can be patched, achieving timely protection against known and zero-day attacks.
- **Web application protection:** Web application protection rules defend against SQL injection, cross-site scripting and other web application vulnerabilities—shielding these vulnerabilities until code fixes can be completed.
- **Application control:** Application control rules provide increased visibility into, or control over, the applications that are accessing the network. These rules can also be used to identify malicious software accessing the network, or to reduce the vulnerability exposure of servers.
- **Firewall:** An enterprise-grade, bi-directional and stateful firewall provides centralized management of server firewall policy, and includes pre-defined templates for common enterprise server types.
- **Integrity monitoring:** Monitoring critical operating system and application files (including files, directories, registry keys and values, etc.), the integrity monitoring software module detects malicious and unexpected changes to physical servers and virtual machines.
- **Log inspection:** Collecting and analyzing operating system and application logs for security events, log Inspection rules optimize the identification of important security events buried in multiple log entries. These events are forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving.

FISMA / NIST 800-53 REVISION 3 COMPLIANCE

Control	Description	How Deep Security Addresses this Control
Access Control		
AC-4	**Information Flow Enforcement—**The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	The Deep Security Agent incorporates a bi-directional stateful firewall that enforces the flow of data based on physical or logical addressing. The Agent also implements deep packet inspection on network traffic to detect and prevent unauthorized attacks and malware. Deep Security can also be used to create and manage sophisticated protection rules that allow and deny appropriate connections and alert on suspicious behavior with a minimum number of rules and maximum flexibility.
AC-5	**Separation of Duties—**Separate duties of individuals as necessary to prevent malevolent activity without collusion; documents separation of duties; and implements separation of duties through assigned information system access authorization.	The Deep Security Manager enables role-based access control (RBAC) and delegated administration to support separation of administrative duties with respect to creating, deploying, and auditing security policy and events that violate the policies.
AC-6	**Least Privilege—**The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	The Deep Security Agent incorporates a bi-directional stateful firewall that restricts network connections (ports, protocols, etc) based on organizational policy. The Deep Security Manager enables role-based access control (RBAC) and delegated administration to support the concept of least privilege and workflow of security response. Deep Security can also be used to create and manage sophisticated protection rules that allow and deny appropriate connections and alert on suspicious behavior with a minimum number of rules and maximum flexibility. Deep Security Log Inspection capabilities provide the ability to monitor and alert on important security events that could indicate suspicious activity. In addition, Deep Security Integrity Monitoring capabilities will detect and raise events whenever critical OS or application files are modified (i.e. Windows system files, Hosts file, registry, etc.)
AC-7	**Unsuccessful Login Attempts—**The information system enforces a limit of consecutive invalid access attempts by a user during a time period	Deep Security Log Inspection capabilities provide the ability to monitor and alert on important security events such as 'x' failed login attempts within 'y' time period providing administrators with visibility into unsuccessful login attempts.
AC-17	**Remote Access—**The organization authorizes, monitors, and controls all methods of remote access to the information system.	Deep Security offers controls for securing remote access including: • The ability to dynamically assign firewall rules based upon user location—for example, remote users will have a more stringent firewall policies assigned to reduce the attack surface • protection against bridging attacks (wired vs. wireless), • Enforcing usage of VPN connections for remote users, etc. All of the above capabilities are augmented with the IDS/IPS, Integrity Monitoring and Log Inspection capabilities provided by Deep Security to facilitate the monitoring and control of remote access methods.
AC-18	**Wireless Access Restrictions—**The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.	Deep Security offers controls for securing wireless mobile workers including: • The ability to dynamically assign firewall rules based upon user location—for example, remote users will have a more stringent firewall policies assigned to reduce the attack surface • Protection against bridging attacks (wired vs. wireless) • Enforcing usage of VPN connections for remote users, etc. All capabilities above are augmented with standard IDS/IPS, Integrity Monitoring and Log Inspection capabilities provided by Deep Security.

Control	Description	How Deep Security Addresses this Control
AC-19	**Access Control for Portable and Mobile—Devices.** The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.	Deep Security offers controls for securing mobile workers including: • The ability to dynamically assign firewall rules based upon user location—for example, remote users will have a more stringent firewall policies assigned to reduce the attack surface • Protection against bridging attacks (wired vs. wireless), • Enforcing usage of VPN connections for remote users, etc. All of the above capabilities are augmented with the standard Deep Security IDS/IPS, Integrity Monitoring and Log Inspection capabilities.
Audit and Accountability		
AU-2	**Auditable Events—**The information system generates audit records for events.	The Deep Security Log Inspection module provides the ability to monitor and alert on important security events that could indicate suspicious activity. In addition, the Deep Security Agent will log Firewall, IDS/IPS, and Integrity Monitoring events and generate alerts based upon the security policy assigned. Alerts can be delivered via various mechanisms such as email, SNMP, as well as through the Manager interface.
AU-3	**Content of Audit Records—**The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	Deep Security Agent and Deep Security Manager event logs contain very granular network information about the event, including the event type, sources of events and can even capture the complete contents of the packet. The Manager also logs all important internal system events such as administrator logins and system errors.
AU-4	**Audit Storage Capacity—**The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	The events and logs are spooled locally at each Deep Security Agent and sent to the Deep Security Manager on a scheduled heartbeat. The size of the local spool is configurable and the Manager is limited only by the available disk space assigned to the database.
AU-5	**Response to Audit Processing Failures—**Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	Deep Security has several mechanisms to respond to audit processing failures. It will alert when disk space is low or as Agents go offline. It will then overwrite the oldest logs as needed so that the most recent events are available. The Agent will enforce protection even if it cannot generate events.
AU-6	**Audit Monitoring, Analysis, and Reporting—**The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.	Deep Security provides a number of features which assist with audit monitoring, analysis, and reporting such as customizable dashboards, alerting, and reporting. In addition the Deep Security Log Inspection module makes it possible to identify important security events buried in operating system and application logs. It forwards this valuable event information via syslog to a centralized log server or SIEM for further analysis. Deep Security also supports integration with industry leading SIEM vendors such as ArcSight, RSA Security, Q1 Labs, Intellitactics, Log Logic, NetIQ and more.
AU-7	**Audit Reduction and Report Generation—**The information system provides an audit reduction and report generation capability.	The Deep Security Manager has several out-of-box reports that can be scheduled or produced on demand. Reports can be automatically delivered via email and can be restricted based on role-based administrative access. In addition, event information can be exported for further analysis.
AU-8	**Time Stamps—**The information system provides time stamps for use in audit record generation.	All alerts and logs are time stamped.

FISMA / NIST 800-53 REVISION 3 COMPLIANCE

Control	Description	How Deep Security Addresses this Control
AU-9	**Protection of Audit Information—**The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	The delivery of events to the Deep Security Manager is authenticated and encrypted using certificates and SSL encryption. Data at rest in the database is password protected. Deep Security Agent Log Inspection may also be used to forward important security events from operating system and application logs to a centralized logging server to prevent local tampering. Deep Security Manager enables role-based access control (RBAC) and delegated administration to support separation of administrative duties to a limited subset of privileged users.
AU-11	**Audit Record Retention—**The organization retains audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Deep Security supports integration with SIEM solutions for long term archival of security event information. In addition, the Deep Security Manager can store audit logs and events for an indefinite amount of time, limited only by the available disk space of the database server. Native database tools can be used to back up and archive data as appropriate.
AU-11	**Audit Generation—**The information system: provides audit record generation capability for the list of auditable events defined in AU-2; allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and, generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	Deep Security Agent and Deep Security Manager event logs contain very granular network information about the event, including the event type, sources of events and can even capture the complete contents of the packet. The Manager also logs all important internal system events such as administrator logins and system errors. The Deep Security Manager enables role-based access control (RBAC) and delegated administration to support separation of administrative duties to a limited subset of privileged users. Deep Security supports integration with SIEM solutions for long term archival of security event information. In addition, the Deep Security Manager can store audit logs and events for an indefinite amount of time, limited only by the available disk space of the database server. Native database tools can be used to back up and archive data as appropriate.
Certification, Accreditation, and Security Assessments Policies and Procedures		
CA-1	**Assessment Policies and Procedures—** The organization develops, disseminates, and reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	Deep Security is the first host intrusion prevention system to achieve Common Criteria certification for Evaluation Assurance Level 3 Augmented (EAL 3+), and it has achieved this certification across more platforms (Microsoft® Windows®, Solaris™, and Linux) than any other host-based intrusion prevention product. The report is available at http://www.commoncriteriaportal.org/files/epfiles/20080505_thirdbrigade-cert-e.pdf
CA-3	**Information System Connections—** Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; documents, for each connection, the interface characteristics, security requirements, and nature of the information communicated; and monitors the information system connections on an ongoing basis verifying enforcement of security requirements	The Deep Security Agent incorporates a bi-directional stateful firewall that enforces sophisticated protection rules that allow and deny appropriate connections and alert on suspicious behavior with a minimum number of rules and maximum flexibility. The Agent also implements deep packet inspection on network traffic to detect and prevent unauthorized attacks and malware.

Control	Description	How Deep Security Addresses this Control
CA-7	**Continuous Monitoring—**The organization monitors the security controls in the information system on an ongoing basis	The Deep Security Agent supports continuous monitoring using multiple techniques including: • Firewall policy enforcement and alerting • IDS/IPS for the detection and prevention of attacks • Automated scanning and recommendation capabilities that can be used to assign IDS/IPS, Integrity Monitoring, and Log Inspection rules based upon the current profile of the system being protected • Integrity Monitoring to detect and alert on changes to critical OS and application files • Log Inspection to forward important security events buried in OS and application log files for further analysis and action • The Deep Security Manager supports dashboards, alerting, and reporting to provide visibility into important security events.
Configuration Management		
CM-2	**Baseline Configuration—**The organization develops, documents and maintains under configuration control, a current baseline configuration of the information system.	Deep Security provides out-of-box security profiles that can be used to specify configurations for unique server functions (e.g., a DNS, Web, or database server), and restrict or prevent access to services and protocols. Deep Security also supports the ability to schedule automatic scans of host systems—one time only, daily, weekly, and so forth—offering recommendations on the appropriate security rules to protect these hosts. The solution's security profiles contain the configuration policy. Role-based access-control capabilities support separation of administrative duties with respect to creating, deploying, and auditing policy and events that violate the policies. The deployment of new security rules can be completely automated so that downloading and installing new security rules to the appropriate systems occur without administrative intervention.
CM-3	**Configuration Change Control—**The organization authorizes, documents, and controls changes to the information system	Deep Security provides administrators with the ability to monitor and audit changes to the information system via Integrity Monitoring capabilities. The Deep Security Integrity Monitoring module provides the ability to monitor critical operating system files, registry keys and values, and application files for changes and generate alerts on detected changes. This level of visibility and reporting into changes occurring on information systems is critical from an audit perspective.
CM-5	**Access Restrictions for Change—**The organization defines, documents, approves and enforces physical and logical access restrictions associated with changes to the information system	Deep Security provides administrators with the ability to monitor and audit changes to the information system via Integrity Monitoring capabilities. The Deep Security Integrity Monitoring module provides the ability to monitor critical operating system files, registry keys and values, and application files for changes and generate alerts on detected changes. Delegated administration and workflow of incident response provide increased visibility and control over changes to the information system.
CM-6	**Configuration Settings—**Establishes and documents mandatory configuration settings for information technology products employed within the information system using security configuration checklists that reflect the most restrictive mode consistent with operational requirements; monitors and controls changes to the configuration settings in accordance with organizational policies and procedures	Deep Security provides administrators with the ability to monitor and audit changes to the information system via Integrity Monitoring capabilities. The Deep Security Integrity Monitoring module provides the ability to monitor critical operating system files, registry keys and values, and application files for changes and generate alerts on detected changes. Delegated administration and workflow of incident response provide increased visibility and control over changes to the configuration settings.

FISMA / NIST 800-53 REVISION 3 COMPLIANCE

Control	Description	How Deep Security Addresses this Control
CM-7	**Least Functionality—**The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services.	The Deep Security Agent enforces remote access to each host based on organizational policy. This can include stateful packet filtering, blocking spoofed addresses, restricting or allowing specified protocols, and blocking malware.
Identification and Authorization		
IA-3	**Device Identification and Authentication—** The information system identifies and authenticates specific devices before establishing a connection.	The Deep Security Agent incorporates a stateful firewall that enables communications to be restricted or allowed based on MAC and IP addresses.
IA-7	**Cryptographic Module Authentication—** The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	Deep Security implements the OpenSSL module and is certified FIPS 140-2 compliant. The certificate is available at this link: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt642.pdf
Incident Response		
IR-4	**Incident Handling—**The organization implements an incident handling capability for security incidents that includes preparation, detections and analysis, containment, eradication and recovery.	Deep Security provides comprehensive protection using multiple techniques to support Incident Handling requirements, enabling: • Firewall policy enforcement and alerting • IDS/IPS for detection and prevention of attacks • Automated scanning and recommendation capabilities that can be used to assign IDS/IPS, Integrity Monitoring, and Log Inspection rules based upon the current profile of the system being protected • Integrity Monitoring to detect and alert on changes to critical OS and application files • Log Inspection to forward important security events buried in OS and application log files for further analysis and action The Deep Security Manager supports dashboards, alerting, and reporting to provide visibility into important security events and support Incident Handling efforts. Deep Security Manager also integrates with existing security information and event management systems to enhance incident response and process automation.
IR-5	**Incident Monitoring—**The organization tracks and documents information system security incidents on an ongoing basis.	The Deep Security Manager tracks, reports and alerts on security incidents. These alerts are visible in the interface or can be delivered via email or SNMP to the relevant administrator.
Risk Assessment		
RA-3	**Risk Assessment—**The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).	Deep Security supports the risk assessment process in a number of ways. First, its recommendation capabilities allow agencies to periodically identify and alert administrators of vulnerabilities on systems for which a mitigation option exists. Secondly, it provides the ability to prioritize events based on risk by enabling ranking of systems by assigning consequence values for system assets and the ranking events based on both this value and the severity score of the vulnerability. Event prioritization and consequence ranking are done on an ongoing basis. System evaluation and security recommendation scanning can be performed on an administrator-defined schedule.

FISMA / NIST 800-53 REVISION 3 COMPLIANCE

Control	Description	How Deep Security Addresses this Control
RA-5	**Vulnerability Scanning—**The organization scans for vulnerabilities, employs vulnerability scanning tools and techniques, analyzes legitimate vulnerability scan reports, remediates legitimate vulnerabilities and share information obtained from the vulnerability scanning process with designated personnel throughout the organization.	The Deep Security "recommendation scan" feature scans the host in order to determine installed software and associated vulnerabilities. Deep Security remediates legitimate vulnerabilities found using vulnerability scanning tools on both commercial and custom enterprise and web applications. It detects and prevents attacks that target data and applications, including activity from malicious code. Deep Security alerts personnel the moment an attack has been attempted, and provides detailed logging of the event for audit purposes. For commercial applications which contain known vulnerabilities targeted by malicious code, Deep Security virtual patching capabilities protect systems and data until vendor patches can be deployed. Web application protection rules defend against SQL injection attacks, cross-site scripting attacks, and other Web application vulnerabilities, and shield these vulnerabilities until code fixes can be completed.
System and Communications Protection		
SC-5	**Denial of Service Protection—**The information system protects against or limits the effects of denial of service attacks.	The Deep Security Agent firewall protects against many forms of network-based Denial of Service attacks including SYN floods and ACK storm. Deep packet inspection protects against malware attacks by blocking the network traffic containing the malicious packets.
SC-7	**Boundary Protection—**The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	The Deep Security Agent firewall monitors and controls communications at the host itself (internal boundary). The Deep Security Agent incorporates a bi-directional stateful firewall that enforces the flow of data based on physical or logical addressing. The Agent also implements deep packet inspection on network traffic to detect and prevent unauthorized attacks and malware. Deep Security can also be used to create and manage sophisticated protection rules that allow and deny appropriate connections and alert on suspicious behavior with a minimum number of rules and maximum flexibility.
SC-10	**Network Disconnect—**The information system terminates a network connection at the end of a session or after a period of inactivity.	The Deep Security Agent monitors the duration of each TCP-based communication session and drops the session after a designated duration, but does not monitor application level timeouts.
SC-30	**Virtualization Techniques—**The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations	The Deep Security solution enables consistent and comprehensive security mechanisms across physical, virtualized and cloud computing servers with security protection that is validated to Common Criteria Evaluation Assessment Level 3 Augmented (CC EAL 3+). Deep Security supports VMware, Citrix and Microsoft virtualization platforms.
System and Information Integrity		
SI-2	**Flaw Remediation—**Identifies, reports and corrects information system flaws.	Deep Security complements secure coding initiatives with strong detection and prevention of attacks against technical flaws and vulnerabilities: ▪ **Detection**—Even if an application is not susceptible to a specific attack, it is important to identify attackers before they find other potential vulnerabilities. ▪ **Protection**—Deep Security shields web application vulnerabilities, preventing security breaches until the underlying flaws can be addressed. Deep Security systematically monitors a wide range of vulnerability research sources to identify and deliver new deep packet inspection (DPI) rules to customers. The deployment of new security rules can be completely automated so that downloading and installing new security rules to the appropriate systems occur without administrative intervention. Deep Security also supports the ability to schedule automatic scans of host systems—one time only, daily, weekly, and so forth—offering recommendations on the appropriate security rules to protect these hosts.

Control	Description	How Deep Security Addresses this Control
SI-3	**Malicious Code Protection—**The information system implements malicious code protection.	Deep Security detects and prevents attacks that target data and applications, including activity from malicious code. Deep Security alerts personnel the moment an attack has been attempted, and provides detailed logging of the event for audit purposes. For commercial applications which contain known vulnerabilities targeted by malicious code, Deep Security virtual patching capabilities protect systems and data until vendor patches can be deployed. Deep Security systematically monitors a wide range of vulnerability research sources to identify and deliver new deep packet inspection (DPI) rules to customers. The deployment of new security rules can be completely automated so that downloading and installing new security rules to the appropriate systems occur without administrative intervention. Deep Security also supports the ability to schedule automatic scans of host systems—one time only, daily, weekly, and so forth—offering recommendations on the appropriate security rules to protect these hosts. Web application protection rules defend against SQL injection attacks, cross-site scripting attacks, and other Web application vulnerabilities, and shield these vulnerabilities until code fixes can be completed.
SI-4	**Information System Monitoring Tools and Techniques—**The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	The Deep Security Agent collects and analyzes operating system and application logs for security events. Log Inspection rules optimize the identification of important security events buried in multiple log entries. These events are forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. Reports can be scheduled to run automatically and alerts can be delivered via SNMP or email, in addition to visibility from the Deep Security Manager console.
SI-5	**Security Alerts, Advisories and Directives—**The organization receives, generates, and disseminates security alerts and implements security directives in accordance with established time frames.	Deep Security provides alerts that are integral to a security incident response plan. And because it can prevent attacks as well, Deep Security reduces the number of incidents requiring a response. The solution's integration with leading SIEM vendors enables a consolidated view of security incidents. Monitoring the integrity of critical system and application files such as executables, configuration and parameter files, and log and audit files—it includes support for alerting, dashboards, and reporting on events raised. Deep Security enables collection of important security events from operating system and application log files, including the ability to forward all events—or only events relevant—to centralized logging servers or SIEMs via syslog in real time, in addition to sending these events to the Deep Security Manager.
SI-6	**Security Functionality Verification—**The information system verifies the correct operation of security when anomalies are discovered.	The Deep Security Manager monitors the Agents to ensure that it is in constant communication and creates an alert if an Agent terminates communication for any reason.
SI-7	**Software and Information Integrity—**The information system detects and protects against unauthorized changes to software and information.	The Deep Security Integrity Monitoring module provides the ability to monitor critical operating system files, registry keys and values, and application files for changes and generate alerts on detected changes. These events are sent to the Deep Security Manager which supports dashboards, alerts, and reporting. In addition, these events can also be sent to a SIEM for additional correlation and analysis.

For more information please call **+1-877-21-TREND** or visit us at: **www.trendmicro.com/go/enterprise**