ForeScout™

Solution Brief

Addressing FISMA Requirements with ForeScout CounterACT™

Federal Information Security Management Act Compliance (FISMA)

CounterACT Security Platform

The ForeScout CounterACT™ security platform provides real-time monitoring, control and policy-based remediation of managed, unmanaged and non-traditional devices to improve FISMA compliance. Here's how:

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor managed devices, Bring Your Own Devices (BYOD) and Internet of Things (IoT) endpoints

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints
- Improve compliance with industry mandates and regulations to include FISMA policies and practices

Orchestrate

- Share contextual insight with IT security and management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 (FISMA) to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security to administer the implementation of such policies and practices for information systems. ForeScout Technologies, Inc. offers uniquely effective network security technologies that can help you implement and enforce organizational policies—protecting vital information infrastructure without the need for significant management overhead as part of the overarching *Risk Management Framework (RMF)* used in today's federal security landscape.

How ForeScout Can Help

For federal agencies that are affected by FISMA, ForeScout CounterACT delivers the ability to achieve compliance as it pertains to monitoring, recording, controlling and reporting/auditing network access by devices. CounterACT can be deployed within an existing network infrastructure with no disruption of services and no need to re-architect the network or upgrade the switching fabric. The visibility and insight into network devices that it provides are critical for protecting network resources. Moreover, CounterACT can enforce network access control policies from any level of switch/network hierarchy, including the access layer, distribution layer and the core switch.

CounterACT's unique ability to control the environment provides a supporting role in the security stack of enterprise networks that helps to reduce the attack surface. CounterACT can enforce a wide variety of actions, providing any organization with the options they need to address FISMA RMF controls.

The orchestration with other key security tools that CounterACT provides is vitally important as more organizations look to integrate and automate their security responses. By enabling a wide array of tools to share contextual data and automate common workflows, CounterACT helps to standardize and make the compliance to controls a repeatable process.

FISMA Compliance Guidelines

The National Institute for Standards and Technology (NIST) provides specific requirements for information security in NIST Special Publication 800-53 rev 4.

CounterACT directly impacts and supports these specific areas in 800-53 rev4

Access Control (AC)
Organizations must limit the access to information systems to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Audit and Accountability (AU)
The Audit and Accountability (AU) control enforces appropriate use policy for network and information systems. It also enables agencies to audit usage of information systems and to validate compliance with standards by producing supporting documentation and reports.

Why Choose ForeScout for FISMA

- CounterACT is the solution that maps directly to 10 of 18 Control Families, and over 150 supporting controls
- CounterACT is the tool on the market that supports these controls in real time for explicit Continuous Diagnostics and Mitigation requirements

Continue Monitoring (CA)

The Certification, Accreditation and Security Assessments (CA) control addresses management, operational and technical controls in each information system contained in the inventory of major information systems.

Configuration Management (CM)

The Configuration Management (CM) control addresses policies and procedures, change control, monitoring of configuration changes, configuration settings, and access restrictions for configuration changes.

Identification and Authentication (IA)

The Identification and Authentication (IA) control addresses policies and procedures, device and host identification and authentication, authenticator management, feedback, and cryptographic authentication.

Incident Response (IR)

The Incident Response (IR) control addresses policies and procedures, incident handling, incident reporting, and incident response assistance, including forensic services and automated tools where applicable.

Risk Assessment (RA)

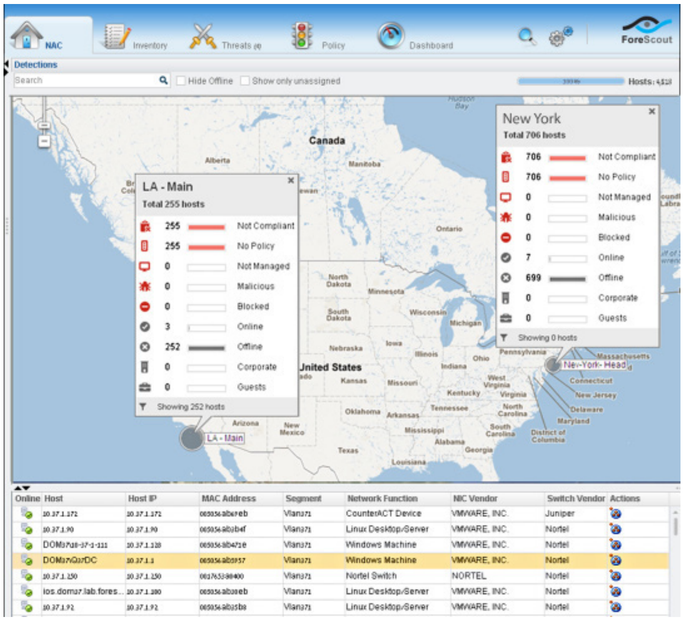
The Risk Assessment (RA) control addresses the creation of a Risk Assessment Policy and resulting procedures in order to assess the potential and magnitude of harm in the event of unauthorized access of information systems. In addition to the understanding of the potential risks, software and hardware solutions are implemented to help mitigate risk by identifying and addressing vulnerabilities.

System and Services Acquisition (SA)

The System and Services Acquisition (SA) control addresses the emphasis on trustworthy information systems and supply chain security. It is essential that organizations have the capability to express their information security requirements with clarity and specificity in order to engage the information technology industry and obtain the systems, components, and services necessary for mission and business success.

System and Communications Protection (SC)

The System and Communication Protection (SC) control addresses the establishment of policy and procedures that reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance that enforce monitoring and controls communications at the external boundary of the system and at key internal boundaries within the system.



LA - Main
Total 255 hosts

255	Not Compliant
255	No Policy
0	Not Managed
0	Malicious
0	Blocked
3	Online
252	Offline
0	Corporate
0	Guests

Showing 252 hosts

New York
Total 706 hosts

706	Not Compliant
706	No Policy
0	Not Managed
0	Malicious
0	Blocked
7	Online
699	Offline
0	Corporate
0	Guests

Showing 0 hosts

Online	Host	Host IP	MAC Address	Segment	Network Function	NIC Vendor	Switch Vendor	Actions
	10.37.1.172	10.37.1.172	005056abereb	Vlan371	CounterACT Device	VMWARE, INC.	Juniper	
	10.37.1.90	10.37.1.90	005056ab3b4f	Vlan371	Linux Desktop/Server	VMWARE, INC.	Nortel	
	DOM37u8-37-1-111	10.37.1.128	005056ab471e	Vlan371	Windows Machine	VMWARE, INC.	Nortel	
	DOM37vQ37DC	10.37.1.1	005056ab3957	Vlan371	Windows Machine	VMWARE, INC.	Nortel	
	10.37.1.250	10.37.1.250	001765338400	Vlan371	Nortel Switch	NORTEL	Nortel	
	ios.dom37.lab.fores...	10.37.1.180	005056ab3eeb	Vlan371	Linux Desktop/Server	VMWARE, INC.	Nortel	
	10.37.1.92	10.37.1.92	005056ab35b8	Vlan371	Linux Desktop/Server	VMWARE, INC.	Nortel	

The ForeScout CounterACT security platform provides complete monitoring, recording, controlling and reporting/auditing of devices—both known and unknown—as they attempt to access the network.

System and Information Integrity (SI)

The System and Information Integrity (SI) control addresses policies and procedures, remediation of security flaws, security alerts and advisories, malicious code protection, intrusion detection and prevention tools and techniques, protection against spyware and other malicious code, and application and information integrity.

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
AC-2 **Account Management**	AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.	ForeScout CounterACT will perform a check of all network devices and verify the following: • List all network devices logged in with local logins. Local logins bypass the normal authentication process. • List all of the guest users logged in via CounterACT guest registration. • List the guest, anonymous and temporary users logged in by identifying LDAP group membership. • This rule will require external identification of guest, anonymous and temporary groups via the LDAP query: (object category=group) • List all of the administration and application accounts. • This will require inspection of the logged-in accounts and building a list of users. If an account naming standard is used, a regular expression for specific names can be created. This can be accomplished by identification of administration and application groups via the LDAP query: (object category=group). Additional LDAP queries that may help identify administrative accounts can check for a list of groups by: (object category=group) • In addition, this policy will check for administration accounts such as admin (Administrator) or root. To identify accounts with possible administration privileges, run the following LDAP queries: All objects protected by AdminSDHolder: (admin account=1) All accounts that password does not expire: (&(object category)
AC-3 **Access Enforcement**	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.	ForeScout CounterACT will use the defined logical access to information and system resources in accordance with applicable access control policies established by the organization. With CounterACT Network Access Controls (NAC), we establish a few areas of management needed to establish this policy: • Network device visibility and information - This must include device type user identity and role, device location, and its level of compliance with organizational security policies. • A flexible and granular policy engine combined with a range of control options - This includes the ability to configure the NAC product to provide the right action for each situation automatically, without the need for human involvement.
AC-4 **Information Flow Enforcement**	AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.	ForeScout Counter can enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: ForeScout CounterACT can enforce the flow based on organization-defined information flow control policies].
AC-7 **Unsuccessful Login Attempts**	AC-2, AC-9, AC-14, IA-5.	ForeScout CounterACT will monitor and report on unsuccessful login attempts. [* See AC-2 Account Management for linkage to LDAP query, and tracking all login attempts (local or network.)]

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
AC-8 **System Use Notification**		ForeScout CounterACT will perform a check of all managed network devices and verify the following: • Perform a registry key value check of Windows® based on registry setting of operating types • Perform a Linux® File check for /etc/ssh/sshd_welcome or /etc/issue which displays the login banner. NOTE: This will only check for Command Line logins and will not display a banner for any KDE or GUI Linux logins. • Perform a Macintosh® File check for /Library/Security/PolicyBanner.txt or /Library/Security/PolicyBanner.rtf which will display the login banner. CounterACT will perform a check of all systems that do not have a system use banner and perform a virtual firewall, limiting access only to CounterACT until the notification is approved. • This policy should only be run on end user systems which are defined in IP Range of the Scope. • To prevent inadvertent blocking of systems, this policy will only trigger during an authentication event.
AC-14 **Permitted Actions without Identification or Authentication**	CP-2, IA-2.	ForeScout CounterACT will perform a check of all network devices and verify the following: • List all of the Windows, Linux and Macintosh network devices that are authorized to perform a network login. • List all of the Windows, Linux and Macintosh network devices that are NOT authorized to perform a network login and match against any authentication events. • List all of the network devices that are NOT authorized authentication events and match against any authentication events. • List remaining network devices that connected to the network.
AC-17 **Remote Access**	AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.	ForeScout CounterACT will perform a check of network devices from the remote network segment and verify the following: • List all of the VPN connections in the remote network segment and verify Windows, Linux and Macintosh network devices are CounterACT-managed. • List all of the unmanaged VPN connections in the remote network segment, send an email to the administrator and start SecureConnector. • List all of the network devices that are NOT connected to the VPN, and virtual firewall the connection.

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
AC-18 **Wireless Access**	AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.	ForeScout CounterACT will perform a check of both wired and wireless devices connecting to the network and verify the following: • List all of the authorized wireless access points, authorized network devices and unauthorized network devices. • List all of the wireless connections in the remote network segment and verify Windows, Linux and Macintosh network devices are CounterACT-managed. • List all of the unmanaged wireless connections in the remote network segment, send an email to the administrator and start SecureConnector. • List all of the network devices that are connected via wireless, and virtual firewall the connection.
AC-19 **Access Control for Mobile Devices**	AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.	ForeScout CounterACT will identify all mobile devices, determine the specific type of mobile device, perform an inspection of authorized mobile devices and verify compliance of authorized mobile devices. • List all of the mobile devices and types of mobile devices connected to the wireless network - CounterACT can limit connection to the network based on device type, MAC address or Mobile Device Management (MDM) membership. • With MDM, CounterACT can inspect managed mobile devices for installed software and applications and compare with an authorized software list. • With MDM, CounterACT can inspect managed mobile devices for jailbroken/rooted devices. • With MDM, CounterACT can manage mobile devices for specific hardware profiles for mobile devices based upon locations deemed to be of significant risk.
AU-7 **Audit Reduction and Report Generation**	AU-6	ForeScout CounterACT will ensure that all Windows devices have an existing event log and the log file is regularly updated. • As an example, it will look for Windows Server 2008/Vista/7 systems. CounterACT will monitor -- %SystemRoot%\System32\winevt\Logs\System.evtx • CounterACT will check for date/timestamp of the file System.evtx for any updates within the last hour to verify that the event log is currently updated.
AU-12 **Audit Generation**	AC-3, AU-2, AU-3, AU-6, AU-7.	ForeScout CounterACT will generate audit logs (syslog) and can monitor syslog sent to it for reporting and audit generation. CounterACT is not a long-term storage solution for audit logs.
CA-7 **Continuous Monitoring**	CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4	ForeScout CounterACT enables the organization to analyze and determine the level of security control implementations, ensuring a path for reviewing the frequency of continuous monitoring activities for cyber hygiene.

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
CA-9 **Internal System Connections**	AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.	ForeScout CounterACT provides security compliance checks of systems prior to the establishment of the internal connection.
CM-2 **Baseline Configuration**	CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.	ForeScout CounterACT will be used to ensure the real-time notification and validation to the required up-to-date, complete, accurate, and readily available baseline configuration for devices seen within the enterprise. CM-2(7) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.
CM-3 **Configuration Change Control**	CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.	ForeScout CounterACT can ensure there are automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base via remediation controls within CounterACT. *CM-3 (3) The information system implements [Assignment: organization-defined security responses] automatically if baseline configurations are changed in an unauthorized manner.
CM-6 **Configuration Management**	AC-19, CM-2, CM-3, CM-7, SI-4	ForeScout CounterACT is used to respond to unauthorized changes. [Assignment: organization-defined configuration settings].
CM-7 **Least Functionality**	AC-6, CM-2, RA-5, SA-5, SC-7.	ForeScout CounterACT will identify applications, ports and processes/services on each system and compare via an authorized list of applications, ports and processes/services. All unmatched systems will be recorded as a violation. CM-7 (1) CM-7 (2) The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].
CM-8 **Information System Component Inventory**	CM-2, CM-6, PM-5.	ForeScout CounterACT has a built-in inventory of current system information that is available via HTTP connection to CounterACT. In addition, an inventory report can be built and emailed to an email account. CM-8 (3) The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and (b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].
CM-10 **Software Usage Restrictions**	AC-17, CM-8, SC-7.	ForeScout CounterACT will ensure the proper usage restrictions. This includes the organization software and associated documentation in accordance with contract agreements and copyright laws. CounterACT can also be used to control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
CM-11 **User-Installed Software**	AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4	ForeScout CounterACT can be used for alerts [Assignment: organization-defined personnel or roles] when the unauthorized installation of software is detected.

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
IA-3 **Device Identification and Authentication**	AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.	ForeScout CounterACT will receive inputs from AC-14 Permitted Actions without Identification or Authorization, AC-17 Remote Access, AC-18 Wireless Access and AC-19 Access Control for Mobile Devices. All network devices that are unauthorized will have limited network access.
IA-4 **Identifier Management**	AC-2, IA-2, IA-3, IA-5, IA-8, SC-37	ForeScout CounterACT can allow the organization to manage information system identifiers by Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier (Plugin Integration to NGFW and DEX will allow for deeper integrations going forward)
IA-8 **Identification and Authentication (Non-Organizational Users)**	AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.	ForeScout CounterACT will perform a check of all network devices and verify the following: • List network devices logged in with local logins. Local logins bypass the normal authentication process. • List the guest users logged in via CounterACT guest registration. • List the guest, anonymous and temporary users logged in by identifying LDAP group membership. • List all of the administration and application accounts. This will require inspection of the logged- in accounts and building a list of users. If an account naming standard is used, a regular expression for specific names can be created. In addition, this can also be accomplished by identification of administration and application groups via the LDAP query: (object category=group). Additional LDAP queries that may help identify administrative accounts. This can be checked by an LDAP query for a list of groups by: (object category=group). In addition, this policy will check for administration accounts such as admin or root. To identify accounts with possible administration privileges, run the following LDAP queries: All objects protected by AdminSDHolder: (adminCount=1) All accounts that password does not expire: (&(object category=user)(userAccountControl:1.2.840.113556.1.4.803:=65536) • List all other network devices with logins CounterACT is not able to verify
IA-10 **Adaptive Identification and Authentication**	AU-6, SI-4.	ForeScout CounterACT can be used to provide the organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] With CounterACT we can see the state of users and network locations for service utilized and duration of access.

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
IR-4 **Incident Handling**	AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	ForeScout CounterACT can be used to detect, contain, and mitigate incidents. Examples IR-4(5) - The organization implements a configurable capability to automatically disable the information system if [Assignment: organization-defined security violations] are detected. IR-4(9) - The organization employs [Assignment: organization-defined dynamic response capabilities] to effectively respond to security incidents
IR-5 **Incident Monitoring**	AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	ForeScout CounterACT can be used to automate mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. This can include network monitoring, physical access monitoring, and user/administrator reporting obtained by CounterACT.
IR-6 **Incident Reporting**	IR-4, IR-5, IR-8.	ForeScout CounterACT has the capability to ensure notification and reporting in a consistent and automated way, specifically in accordance with IR-6 (1), which stipulates that the organization must employ automated mechanisms to assist in the reporting of security incidents.
RA-5 **Vulnerability Scanning**	CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2	ForeScout CounterACT can provide integration with third-party scanners to conduct third-party vulnerability scanning. CounterACT can be automated to conduct automated vulnerability scans on the information system and hosted applications once they are connected to the network.
SA-18 **Tamper Resistance and Detection**	PE-3, SA-12, SI-7.	ForeScout CounterACT will provide the ability to provide the inspection of devices connecting to the network Seeing the device components and hardware on the device. SA-18 (2) - The organization inspects [Assignment: organization-defined information systems, system components, or devices]
SC-7 **Boundary Protection**	AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.	ForeScout CounterACT will identify users that are authorized to access the boundary and create a policy to add their systems as authorized boundary systems. Otherwise, the organization would identify systems authorized to connect to the boundary, right click the host and manually Add to Group --> NIST RMF - Authorized Boundary systems. • CounterACT will detect network traffic to the Boundary systems as defined by CounterACT segment. • Authorized boundary systems will have any alternate network interface cards (i.e., wireless) disabled. • Unauthorized access to boundary systems will have a virtual firewall applied to prevent communication.
SC-25 **Thin Nodes**	SC-30	ForeScout CounterACT will identify systems that are potential thin clients via network vendor and other characteristics. • CounterACT will identify all unmanaged thin clients and authentication events • CounterACT will identify all unmanaged thin clients

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
SC-26 **Honey Pots**	SC-30, SC-44, SI-3, SI-4.	ForeScout CounterACT will identify systems that are attempting to scan the network and build a model of threats and establish a mark or host to be used in the event of attacks. • Probe Count: The number of probes a host performs before CounterACT tracks the host with a mark • After the probe count threshold has passed, the host is calculated by CounterACT as a probing host and has performed a network scan • Customize naming conventions used in your network environment o [Makes CounterACT marks more realistic • Naming options o Mark Names: Reflects naming conventions used for host and user names in network o Lists of Names: Similar to host and user names used in your network
SC-27 **Operating System-Independent Applications**	SC-29	ForeScout CounterACT will identify system as Operating System-Independent Applications
SC-30 **Concealment and Misdirection**	SC-26, SC-29, SI-14	ForeScout CounterACT will identify system as Operating System-Independent Applications
SC-30 **Concealment and Misdirection**	SC-26, SC-29, SI-14	ForeScout CounterACT will identify systems that are attempting to connect on the same physical port, including virtual devices. • CounterACT will identify two network hosts with one being a VOIP device • CounterACT will identify two or more hosts connecting to the same port with virtual machines • CounterACT will identify two or more hosts connecting to the same port (NAT)
SI-2 **Flaw Remediation**	CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.	ForeScout CounterACT will identify systems that have SCCM registration, antivirus compliance and Windows patch compliance. • CounterACT will identify if a client is registered with SCCM • CounterACT will identify antivirus compliance, including if and when specific antivirus software is running and definitions are up to date • CounterACT will identify Windows patch compliance
SI-3 **Malicious Code Protection**	CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.	ForeScout CounterACT will help in the identification of systems that have malicious code by looking for md5, dlls, files, applications, and services. CounterACT also supports other third-party security solutions via the Advanced Threat Detection Integration Module. Patented deterministic methodology (ActiveResponse™) ensures detection of zero-day threats from self-propagating malicious code as well as internal espionage and/or sophisticated hackers.

800-53rev4	800-53rev4 related/supported controls	ForeScout Solution & Response to Control
SI-4 **Information System Monitoring**	AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7	ForeScout CounterACT will support the IOC model to find and support detection intrusions. Example: SI-4 (3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
SI-7 **Software, Firmware, and Information Integrity**	SA-12, SC-8, SC-13, SI-3.	ForeScout CounterACT will work to ensure that software security and version controls are up to date. Examples: SI-7(2) - The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification. SA-7 (3) - The organization employs centrally managed integrity verification tools. SI-7 (5) The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered. SI-7(8) - The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [Selection (one or more): generates an audit record; alerts current user; alerts [Assignment: organization-defined personnel or roles]

ForeScout™

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Toll-Free (US) 1.866.377.8771
Tel (Intl) 1.408.213.3191
Support 1.708.237.6591
Fax 1.408.371.2284

Copyright © 2015. All rights reserved. Privacy policy. ForeScout Technologies, Inc. is a privately held Delaware corporation. ForeScout, the ForeScout logo, ControlFabric, CounterACT Edge, ActiveResponse and CounterACT are trademarks or registered trademarks of ForeScout. Other names mentioned may be trademarks of their respective owners. **Version 12_15**