FORESCOUT

Addressing NIST Risk Management Framework Controls with ForeScout CounterACT®

National Institute of Standards and Technology 800 (53rev4 & 171)
Risk Management Framework and ForeScout CounterACT Control Mapping

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
AC-2	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.	3.1.1/3.1.2	Account Management	ForeScout CounterACT will perform a check of network devices and verify the following: • List network devices logged in with local logins. Local logins bypass the normal authentication process. • List 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 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. 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(Administrator) or root. To identify accounts with possible administration privileges run the following LDAP queries: Objects protected by AdminSDHolder: (admin account=1) Accounts that password does not expire: (&(object category)	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: 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.
AC-3	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.	3.1.1/3.1.2	Access Enforcement	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 Access Controls 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 CounterACT to provide the right action for each situation automatically, without the need for human involvement.	Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: 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.

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
AC-4	AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.	3.1.3	Information Flow Enforcement	ForeScout CounterACT 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].	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.
AC-7	AC-2, AC-9, AC-14, IA-5.	3.1.8	Unsuccessful Login Attempts	ForeScout CounterACT will monitor and report on unsuccessful login attempts * See AC-2 Account Management for linkage to LDAP query, and tracking login attempts (local or network)	This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.
AC-8		3.1.9	System use Notification	ForeScout CounterACT will perform a check of 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 check 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 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.	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
AC-14	CP-2, IA-2.	additional control	Permitted Actions without Identification or Authentication	ForeScout CounterACT will perform a check of network devices and verify the following: • List of the Windows, Linux and Macintosh network devices that are authorized to perform a network login. • List of the Windows, Linux and Macintosh network devices that are NOT authorized to perform a network login and match against any authentication events. • List 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	This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2.
AC-17	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.	3.1.1/3.1.2	Remote Access	ForeScout CounterACT will perform a check of network devices from the remote network segment and verify the following: • List VPN connections in the remote network segment and verify Windows, Linux and Macintosh network devices are CounterACT managed. • List unmanaged VPN connections in the remote network segment, send an email to the administrator and start SecureConnector. • List network devices that are NOT connected to the VPN and virtual firewall the connection.	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: 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.
AC-18	AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.	3.1.16	Wireless Access	ForeScout CounterACT will perform a check both network devices and network devices connecting via wireless network and verify the following: • List of the authorized wireless access points, authorized network devices and unauthorized network devices. • List of the wireless connections in the remote network segment and verify Windows, Linux and Macintosh network devices are CounterACT managed. • List of the unmanaged wireless connections in the remote network segment, send an email to the administrator and start SecureConnector. • List of the network devices that are connected via wireless and virtual firewall the connection.	Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
AC-19	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.	3.1.18	Access Control for Mobile Devices	ForeScout CounterACT will identify mobile devices, determine the specific type of mobile device, perform an inspection of authorized mobile devices and verify compliance of authorized mobile devices. • List 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 integration, CounterACT can inspect managed mobile devices for installed software and applications and compare with an authorized software list. • With MDM integration, CounterACT can inspect managed mobile devices for jailbroken / rooted devices. • With MDM integration, CounterACT can manage mobile devices for specific hardware profiles for mobile devices based upon locations deemed to be of significant risk.	A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: 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.
AU-7	AU-6	3.3.6	Audit Reduction and Report Generation	ForeScout CounterACT will identify that Windows devices have an existing event log and the log file is regularly updated. • As an example, we 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 the event log is currently updated.	Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6.
AU-12	AC-3, AU-2, AU-3, AU-6, AU-7.	3.3.1/3.3.2	Audit Generation	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.	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.
CA-7	CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4	additional control	Continuous Monitoring	ForeScout CounterACT helps ensure that the organization can analyze and determine security control implementations, helping to ensure a path for reviewing the frequency of continuous monitoring activities for cyber hygiene.	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. 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. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
CA-9	: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.	additional control	Internal System Connections	ForeScout CounterACT provides security compliance checks of systems prior to the establishment of the internal connection.	This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration. Related controls: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.
CM-2	CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.	3.4.1/3.4.2	Baseline Configuration	ForeScout CounterACT helps 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.	This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.
CM-3	CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.	3.4.3	Configuration Change Control	ForeScout CounterACT helps ensure that 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.	Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.
CM-6	AC-19, CM-2, CM-3, CM-7, SI-4	3.4.1/3.4.2	Configuration Management	ForeScout CounterACT is used to respond to unauthorized changes to [Assignment: organization-defined configuration settings].	Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
CM-7	AC-6, CM-2, RA-5, SA-5, SC-7.	3.4.6	Least Functionality	ForeScout CounterACT will identify applications, ports and processes/services on systems and compare via an authorized list of applications, ports and processes/services. 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]. <	Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.
CM-8	CM-2, CM-6, PM-5.	3.4.1/3.4.2	Information System Component Inventory	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]].	Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Related controls: CM-2, CM-6, PM-5.
CM-10	AC-17, CM-8, SC-7.	additional control	Software Usage Restrictions	ForeScout CounterACT helps 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 control the use of unauthorized distribution, display, performance, or reproduction of copyrighted work.	Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs. Related controls: AC-17, CM-8, SC-7.
CM-11	AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4	3.4.9	User-Installed Software	ForeScout CounterACT can be used to alerts [Assignment: organization-defined personnel or roles] when the unauthorized installation of software is detected.	"If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both. Related controls: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.
IA-3	AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.	additional control	Device Identification and Authentication	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. Network devices that are unauthorized will have limited network access.	Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.
IA-4	AC-2, IA-2, IA-3, IA-5, IA-8, SC-37	3.5.5	Identifier Management	ForeScout CounterACT will allow the organization manages 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)	Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
IA-8	AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.	additional control	Identification and Authentication (Non-Organizational Users)	ForeScout CounterACT **This control is satisfied by AC-2 - Account Management** CounterACT will perform a check of 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 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(Administrator) or root. To identify accounts with possible administration privileges run the following LDAP queries: Objects protected by AdminSDHolder: (adminCount=1) Accounts that password does not expire: (&(object category=user) (userAccountControl:1.2.840.113556.1.4.803:=65536) • List other network devices with logins CounterACT is not able to verify	Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.
IA-10	AU-6, SI-4.	additional control	Adaptive Identification and Authentication	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.	Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations when certain preestablished conditions or triggers occur, organizations can require selected individuals to provide additional authentication information. Another potential use for adaptive identification and authentication is to increase the strength of mechanism based on the number and/or types of records being accessed. Related controls: AU-6, SI-4.
IR-4	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.	3.6.1/3.6.2	Incident Handling	ForeScout CounterACT can be used to detect, contain, and mitigate the Incident for the organization. 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	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: 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.
IR-5	AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	3.6.1/3.6.2	Incident Monitoring	ForeScout CounterACT can be used to automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. This could include the network monitoring, physical access monitoring, and user/administrator reporting obtained by CounterACT	Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.
IR-6	IR-4, IR-5, IR-8.	3.6.1/3.6.2	Incident Reporting	ForeScout CounterACT has the capability to provide notification and reporting in a consistent and automated way. IR-6 (1) - The organization employs automated mechanisms to assist in the reporting of security incidents.	The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. 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. Related controls: IR-4, IR-5, IR-8.

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
RA-5	CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2	3.11.2/3.11.3	Vulnerability Scanning	ForeScout CounterACT will Integration with 3rd part scanners to conduct 3rd Party vulnerability scanning. CounterACT can be automated to conducting automated vulnerability scans on the information system and hosted applications once they are connected to the network. (Just in time scanning - When device are online they should be scanned)	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. 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. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.
SA-18	PE-3, SA-12, SI-7.	additional control	Tamper Resistance and Detection	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]	Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use. Related controls: PE-3, SA-12, SI-7.
SC-7	AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.	3.13.1/3.13.2	Boundary Protection	ForeScout CounterACT will identify users that are authorized to access the boundary and create a policy to add they 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.	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.
SC-25	SC-30	additional control	Thin Nodes	ForeScout CounterACT identifies systems that are potential thin clients via network vendor and other characteristics. • CounterACT will identify Un-managed thin clients and authentication events. • CounterACT will identify Un-managed thin clients	The deployment of information system components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber attacks. Related control: SC-30.
SC-26	SC-30, SC-44, SI-3, SI-4.	additional control	Honey pots	ForeScout CounterACT will identify systems that are attempting to scan the network, and build a model of threats and establishing a mark or host to be used in the attacks of the network. • 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	A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function. Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed. Related controls: SC-30, SC-44, SI-3, SI-4.

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
SC-27	SC-29	additional control	Operating System-Independent Applications	ForeScout CounterACT will identify system as Operating System-Independent Applications	Platforms are combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both. Platform-independent applications are applications that run on multiple platforms. Such applications promote portability and reconstitution on different platforms, increasing the availability of critical functions within organizations while information systems with specific operating systems are under attack. Related control: SC-29.
SC-30	SC-26, SC-29, SI-14	additional control	Concealment and Misdirection	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)	Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis. Related controls: SC-26, SC-29, SI-14.
SI-2	CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.	3.14.1/3.14.2/ 3.14.3	Flaw Remediation	ForeScout CounterACT will identify systems that have SCCM registration, Anti-Virus compliance and Windows patch compliance. • CounterACT will identify if a client is registered with SCCM • CounterACT will identify Anti-Virus compliance including specific Anti-Virus is running and definitions are up to date • CounterACT will identify Windows Patch Compliance.	Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.
SI-3	CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.	3.14.1/3.14.2/ 3.14.3	Malicious Code Protection	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 solutions via the Advanced Threat Detection Integration Module. Patented deterministic methodology (ActiveResponse) helps ensure detection of "zero-day" threats from self propagating malicious code as well as internal espionage and/or sophisticated hackers.	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

800-53rev4	800-53rev4 related/ supported controls	800-171	Control Name	ForeScout CounterACT Control Mapping	Guidance to Control Compliance
SI-4	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	3.14.6/3.14.7	Information System Monitoring	ForeScout CounterACT will support the IOC model to find and support the 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.	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. 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). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: 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.
SI-7	SA-12, SC-8, SC-13, SI-3.	additional control	Software, Firmware, and Information Integrity	ForeScout CounterACT will work to help ensure that Software security and version controls. 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].	Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284