ForeScout CounterACT® Features and Benefits with HITRUST

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
3	01 Information Protection Program	05.b Information Security Coordination	An internal security information sharing mechanism exists to communicate nonconformities and lessons learned to senior management.	Implement and document information sharing mechanisms, such as forums, regular meetings, and incident response forms.	CounterACT provides notification actions.
6	01 Information Protection Program	00.a Information Security Management Program	Independent audits are conducted at least annually to determine whether the information protection program is approved by executive management, communicated to stakeholders, adequately resourced, conforms to relevant legislation or regulations and other business requirements, and is adjusted as needed to ensure the program continues to meet defined objectives.	Mandate annual audits of the ISMP to identify potential weaknesses and areas for improvement by assessing the program against industry standards.	CounterACT can assist by auditing open ports, programs and devices connected to the network.
7	01 Information Protection Program	02.a Roles and Responsibilities	Management identifies mobile computing requirements specific to BYOD usage, including identifying approved applications, eligibility requirements, privacy expectations, data wipe, and usage.	Update policies and procedures to incorporate: 1) expectations of privacy and the requirements for litigation, e-discovery, and legal holds with respect to mobile devices and 2) expectations regarding the loss of non-company data in the case a wipe of a mobile device is required. Furthermore, management should consider implementing the updated policies and procedures within the organization's environment.	CounterACT can classifiy and control endpoints, including corporate-owned, BYOD and guest hosts. Policies can be established to control how these devices access the network.
8	01 Information Protection Program	02.a Roles and Responsibilities	Non-employees are provided the organization's data privacy and security policy prior to accessing system resources and data.	Provide a link to privacy policies and applicable procedures/ policies on login screens. Design baseline requirement was met; no recommendations noted.	CounterACT Guest Registration allows access to your network without compromising your internal network security. Several guest registration options let you tailor the guest admission process to your organization's needs. Role-based access: CounterACT ensures that the right people with the right devices gain access to the right network resources.It leverages your existing directory where you assign roles to user identities.
10	01 Information Protection Program	05.b Information Security Coordination	Security activities (e.g., implementing controls, correcting non-conformities) are coordinated in advance and communicated across the entire organization.	"Increase documentation of security activities and implement a formal process for regularly communicating security activity.	CounterACT provides notification actions.
13	01 Information Protection Program	05.b Information Security Coordination	Security plans that meet applicable federal or best- practice requirements are developed for information systems that are periodically reviewed and communicated to relevant stakeholders.	Ensure that security plans for IT assets are regularly reviewed and are in line with industry best practices.	CounterACT supports the effective enforcement of portions of information security regulatory frameworks/guidelines.
14	01 Information Protection Program	00.a Information Security Management Program	The information protection program is formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met.	Develop an Information Security Management Program in order to guide security and privacy objectives, and provide management-level approval for security and privacy projects. This program should be reviewed on a regular basis to make sure it aligns with the organization's security and operational goals.	Elements of the Security Management Program can be implemented with CounterACT.
15	01 Information Protection Program	02.f Disciplinary Process	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures, including license, registration, and certification denial or revocation and other disciplinary actions, and notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated that identifies the individual sanctioned and the reason for the sanction.	Expand the procedures for non-compliance with Information Security policies to cover a wider variety of incidents and ensure that security violations are documented and analyzed. Ensure design baseline requirement is met.	CounterACT can help manage and monitor compliance of endpoints.
16	01 Information Protection Program	02.d Management Responsibilities	The organization ensures plans for security testing, training and monitoring activities are developed, implemented, maintained and reviewed for consistency with the risk management strategy and response priorities.	Revise the Security Awareness Training Program to ensure the inclusion of all relevant requirements relating to security testing, training and monitoring.	CounterACT can monitor services for compliance and automatically stop the process.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
17	01 Information Protection Program	00.a Information Security Management Program	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.	Define and implement an information protection program based on an industry-approved and accepted framework. Examples include, but are not limited to, HITRUST, NIST and ISO.	CounterACT takes care of several of the NIST elements. CounterACT directly impacts and supports these specific control areas documented in 800-53 rev4: • Access Control. Limits access to agency information systems to authorized users, processes administered on behalf of authorized users, or devices/ information systems, transactions and functions users are permitted to control. • Audit and Accountability. Enforces appropriate use policy for network and information systems. This also allows agencies to audit information system use and validate standards compliance by producing documents and reports. • Continuous Monitoring. Addresses management as well as operational and technical controls in information systems contained in the inventory of major information systems as required by NIST's Certification, Accreditation and Security Assessment control. • Configuration Management. Focuses on policies and procedures, change control, monitoring and configuration changes, configuration settings and access restrictions for configurations changes. • Identification and Authentication. Addresses device and host identification and authentication, authenticator management, feedback and cryptographic authentication. • Incident Response. Covers policies and procedures, incident handling, reporting and response assistance—including forensic services and automated tools. • Risk Assessment. Examines the creation of a Risk Assessment Policy and procedures to assess the potential impact of damage due to unauthorized access of information systems. Besides addressing potential risks, it focuses on software and hardware solutions that can mitigate risk by identifying and mitigating vulnerabilities. • System and Services Acquisition. Emphasizes trustworthy information systems and supply chain security. Public sector organizations must clearly and specifically express their information security requirements when working with commercial industry to acquire vital systems, components and services. • System and Communications Protection. Creates policies and procedures that reflect applicable federal laws, executive orders, directives, regulations, policies, standards and guidance that enforce monitoring and control communications at external and internal boundaries in the system. • System and Information Integrity. Examines policies and procedures in remediation of security flaws, generating security alerts and advisories. CounterACT also provides intrusion protection capabilities and orchestrates interoperability with other cyber-prevention tools and techniques, including protection against spyware.
19	01 Information Protection Program	05.a Management Commitment to Information Security	The organization's information protection and risk management programs, including the risk assessment process, are formally approved and are reviewed for effectiveness and updated annually.	Continue the development of the risk management policy, including procedures for risk treatment such as cost-benefit analysis, documented risk treatment, scheduled updates, and alignment with the HITRUST CSF.	CounterACT supports the effective enforcement of portions of information security regulatory frameworks/guidelines.
20	01 Information Protection Program	05.b Information Security Coordination	The organization's security lead meets with business area/ organizational unit security contacts on a monthly or near monthly basis.	Implement formally required regular meetings with business and operational areas. Design baseline requirement was met; no recommendations noted.	CounterACT supports the effective enforcement of portions of information security regulatory frameworks/guidelines.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
24	01 Information Protection Program	04.b Review of the Information Security Policy	The security policy reviews consider all appropriate elements that could impact the organization's risk profile.	Develop governmental policies and procedures which address how policies and other documentation could be reviewed and approved to ensure completeness. Criteria could include: i. The changing nature of the organization's operations and thus risk profile and risk management needs; ii. The changes made to the IT infrastructure of the organization, with the associated changes these bring to the organization's risk profile; iii. The changes identified in the external environment that similarly impact the organizations risk profile; iv. The latest controls, compliance and assurance requirements and arrangements of national bodies and of new legislation or regulation; v. The latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information; vi. The results of legal cases tested in courts that thereby establish or cancel precedents and established practices; and vii. The challenges and issues regarding the policy, as expressed to the organization by its staff, customers, partners, care givers, researchers, or governments, (e.g., privacy commissioners).	CounterACT supports the effective enforcement of portions of information security regulatory frameworks/guidelines.
26	02 Endpoint Protection	09.j Controls Against Malicious Code	Anti-malware is centrally managed and cannot be disabled by the users.	Ensure operating baseline is met. Ensure design baseline requirement was met.	CounterACT can check endpoints for compliance and provide automated responses such as remotely starting the service.
27	02 Endpoint Protection	09.j Controls Against Malicious Code	Audit logs of the scans are maintained.	Amend logging, monitoring and virus-scanning procedures to ensure that logs are properly created and maintained.	CounterACT can check endpoints for compliance and share that information with a SIEM system or send it to a syslog server.
28	02 Endpoint Protection	09.m Network Controls	File sharing is disabled on wireless-enabled devices.	Develop network protection policies and amend configuration standards to enforce the disabling of file sharing on wireless client devices.	CounterACT can monitor services for compliance and automatically stop the process.
29	02 Endpoint Protection	09.j Controls Against Malicious Code	Scans for malicious software are performed on boot and every 12 hours.	Amend policies and configurations for virus scanning applications to specify that scans should be taken at least every 12 hours.	CounterACT can check endpoints for compliance every 12 hours and is customizable for recheck.
30	02 Endpoint Protection	09.j Controls Against Malicious Code	User functionality, including user interface services (e.g., web services), are separated from information system management (e.g., database management systems) functionality.	Document the separation of user functionality from the information system management functionality.	CounterACT can classify endpoints and help an organization help segment the network.
33	03 Portable Media Security	09.o Management of Removable Media	The organization protects and controls media containing sensitive information during transport outside of controlled areas.	Ensure that a media log is kept which tracks any time that media is written to portable media and transported. Design baseline requirement was met; no recommendations noted.	While CounterACT does not facilitate tracking write operations to removable storage, it does provide for the ability to restrict access to external devices. Hospitals can use CounterACT to block access to non-approved external devices. Typically this functionality is deployed to block access to non-encrypted USB devices.
34	03 Portable Media Security	09.q Information Handling Procedures	The organization's security lead meets with business area/ organizational unit security contacts on a monthly or near monthly basis.	Perform a data inventory with regular updates that identifies the location of sensitive information, data owners, and encryption status for all inventoried information. Revise the encryption policy to require removable media encryption.	CounterACT provides for enforcement of removable media policies to shut down non-encrypted USB devices, for example.
35	04 Mobile Device Security	01.x Mobile Computing and Communications	The security policy reviews consider all appropriate elements that could impact the organization's risk profile.	Develop mobile device policies which specify security controls to be implemented, monitoring requirements, and details on the organizations BYOD policy.	CounterACT can help ensure mobile devices are enrolled in the enterprise mobilty management solution, or the captive portal can be used to trigger enrollment, helping ensure enrollment compliance.
36	04 Mobile Device Security	01.x Mobile Computing and Communications	Anti-malware is centrally managed and cannot be disabled by the users.	Revise the IT Asset Management Policy (IST-013) to incorporate references to the list and location of approved applications. Furthermore, healthcare providers should consider documenting how the organization manages phones and laptops from an asset inventory perspective.	CounterACT can provide real-time visibility into devices connected to the network and can send that data to a CMDB.
37	04 Mobile Device Security	01.y Teleworking	Audit logs of the scans are maintained.	Perform a risk evaluation of teleworking activities and acquiring additional insurance to address the potential impact of teleworking employees.	CounterACT posture assessment can be used to help ensure compliance testing, which may translate to reduced cost to transfer the risk to insurance.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
38	04 Mobile Device Security	01.x Mobile Computing and Communications	File sharing is disabled on wireless-enabled devices.	Develop mobile device policies which address security controls specific to requirements for sending devices to high-risk areas.	CounterACT can be used in conjunction with enterprise mobilty management solutions to adjust configuration based upon devices' connections or other conditions.
39	04 Mobile Device Security	01.y Teleworking	Scans for malicious software are performed on boot and every 12 hours.	Operations effectiveness requirements are met; no recommendations noted. Design baseline requirement was met; no recommendations noted.	CounterACT can help ensure security baselines are maintained on teleworking activities. It can automate remediation if devices or applications are found to be non-compliant.
40	04 Mobile Device Security	01.x Mobile Computing and Communications	User functionality, including user interface services (e.g., web services), are separated from information system management (e.g., database management systems) functionality.	Amend the policy and procedure documentation to align with the current practices in place within the organization.	CounterACT can verify that only approved devices are connected to wireless networks.
41	04 Mobile Device Security	01.x Mobile Computing and Communications	The organization protects and controls media containing sensitive information during transport outside of controlled areas.	Develop mobile device policies which identify how updates will be securely applied to all mobile devices.	CounterACT can provide posture assessment to validate minimum requirements and allow or disallow access based on the findings.
42	04 Mobile Device Security	01.x Mobile Computing and Communications	The organization shall ensure that mobile devices connecting to corporate networks, or storing and accessing company information, allow for remote wipe.	Update the current policy and procedure documentation to address a detailed process specific to remote patch management and ensure the latest available security-related patches are installed upon general release by the device manufacturer or carrier.	By integrating with popular mobile device management systems, wipe functionality can be automated based upon condition match; for example, when a user's AD account is deactivated, the mobile device is automatically wiped.
43	05 Wireless Security	09.m Network Controls	Firewalls are configured to deny or control any traffic from a wireless environment into the covered data environment.	Expand network protections documentation and procedures to require the use of authentication mechanisms, and to develop access control lists for remote access connections.	CounterACT can provide for dynamic segmentation via ACL, VLAN changes or virtual firewall.
44	05 Wireless Security	09.m Network Controls	Quarterly scans are performed to identify unauthorized wireless access points, and appropriate action is taken if any unauthorized access points are discovered.	Develop network protection policies and procedures that include standards for access point scanning and follow-up procedures as a result of the scans at least quarterly.	CounterACT provides continious visibility into devices that are connected to the network, both wired and wireless.
45	05 Wireless Security	09.m Network Controls	Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.	Develop network procedures which define how access points should be configured.	CounterACT can check for default login and SNMP credentials for network devices.
46	06 Configuration Management	06.g Compliance with Security Policies and Standards	Annual compliance reviews are conducted by security or audit individuals using manual or automated tools and, if non-compliance is found, appropriate action is taken.	Update security policies to ensure that detailed procedures are documented over the internal IT compliance assessment and IT security roadmap.	Technical controls can be enforced on various endpoints in the environment, helping to ensure compliance in real time.
47	06 Configuration Management	06.g Compliance with Security Policies and Standards	Automated compliance tools are used when possible.	Amend risk management policies and procedures to include compliance as a risk objective. Further, consider expanding the use of automated tools to support compliance objectives	Technical controls can be enforced on various endpoints in the environment, helping to ensure compliance in real time.
49	06 Configuration Management	10.h Control of Operational Software	The operating system shall have in place supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of their baseline.	Ensure that operating systems have antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of their baseline.	CounterACT can help ensure PC settings meet corporate baselines, including those for AV, firewall, DLP, encryption, etc., and can remediate or notify upon failure.
50	06 Configuration Management	06.g Compliance with Security Policies and Standards	The organization develops a continuous monitoring strategy and implements a continuous monitoring program.	Ensure continuous monitoring strategy is documented and implemented.	CounterACT is a real-time platform that provides continuous visibility, monitoring and control in the environment.
51	06 Configuration Management	10.h Control of Operational Software	The organization prevents program execution in accordance with the list of unauthorized (blacklisted) software programs and rules authorizing the terms and conditions of software program usage.	Amend the Asset Management Policy to reflect the role the healthcare provider plays in preventing the program execution in accordance with the list of unauthorized software programs and rules, and ensure that old versions of software are archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive or as dictated by MultiPlan's data retention policy.	CounterACT can be used to enforce blacklists for applications installed on Windows workstations and servers.
52	06 Configuration Management	06.g Compliance with Security Policies and Standards	The results and recommendations of the reviews are documented and approved by management.	Amend the Information Security Policy to formally document the process of reviewing and recommending program enhancements.	CounterACT supports the effective enforcement of portions of information security regulatory frameworks/guidelines.
53	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	A hardened configuration standard exists for all system components.	Implement procedures for the regular audit of configuration standards, both against the policy and against industry standards. Design baseline requirement was met; no recommendations noted.	CounterACT can be used to audit configurations against industry standards.
54	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	A technical vulnerability management program is in place to monitor, assess, rank, and remediate vulnerabilities identified in systems.	Develop a Threat and Vulnerability Management Program and Policy which mandates the use of mailing lists and other resources to help identify vulnerabilities and system weaknesses. The program should monitor, assess, rank, and remediate vulnerabilities identified in all systems.	CounterACT natively displays missing Windows patches.
55	07 Vulnerability Management	07.a Inventory of Assets	An inventory of assets is maintained.	Develop processes for auditing asset inventories which are documented and followed up on to ensure that issues that are identified are resolved. Expand policies and procedures to require that asset inventories include risk classifications and other details such as direct system owners and business use for each asset.	Real-time visibility of assets is provided out of the box with CounterACT.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
57	07 Vulnerability Management	10.b Input Data Validation	Applications that store, process or transmit covered information undergo automated application vulnerability testing by a qualified party on an annual basis.	Amend system development lifecycle policies and procedures to include regular vulnerability testing by a qualified party (internal or external), and ensure that application input validation testing occurs and is automated through use of tools or other non-manual methods.	CounterACT offers bi-directional workflows, real-time scanning and automated response with vulnerability assessment tools.
58	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	Internal and external vulnerability assessments of covered information systems and networked environments, including both network- and application-layer tests, are performed by a qualified individual on a quarterly basis or after significant changes.	Develop policies and procedures for threat and vulnerability management that mandate regular vulnerability assessments by a qualified vendor on both the network and application layer.	CounterACT enables automated incident response actions, including data access control or notification of the administrator of an incident. CounterACT works with ATD, SIEM, VA and other key threat detection systems to automate host and network controls.
59	07 Vulnerability Management	07.a Inventory of Assets	Inventories of IT assets are updated during installations, removals and system changes, with full physical inventories performed for capital assets (at least annually) and non-capital assets.	Expand the use of healthcare provider's asset management software to cover physical asset management. Develop policies and procedures for the maintenance, and update of asset inventories, including processes for verifying inventories through software, procurement and disposal at least annually.	With CounterACT, each device on the network is inventoried when it connects to the network, providing near real-time inventory of devices and their software.
60	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	Patches are tested and evaluated before they are installed.	Revise IST-019 to incorporate the requirement relating to pre-patch implementation testing prior to all patching instances. If no patch is available, apply other controls including: i. documentation of impact. ii. documented change approval by authorized parties. iii. functionality testing to verify that the change does not adversely impact the security of the system. iv. back-out procedures. v. turning off services or capabilities related to the vulnerability. vi. adapting or adding access controls (e.g., firewalls) at network borders (see 9.m). vii. increased monitoring to detect or prevent actual attacks. viii. raising awareness of the vulnerability.	CounterACT can be used to audit and establish that the correct versions of patches are installed.
62	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	Technical vulnerabilities are identified, evaluated for risk and corrected in a timely manner.	Revise the SDLC and patch management policies to incorporate references to the assessment/evaluation of risks relating to the technical vulnerabilities identified through the enumerated processes.	CounterACT monitors missing Microsoft patches. It can also work in conjunction with VA systems to enumerate systems and, if desired, take automated remediation action.
63	07 Vulnerability Management	07.a Inventory of Assets	The asset inventory also includes the owner of the information asset, categorizes the information asset according to criticality and information classification (see 07.d), and identifies protection requirements commensurate with the asset's categorization.	Implement additional functionality into Altiris and other asset-tracking tools to track asset ownership by unique individual, and to track item details such as level of criticality, business function, etc. Amend asset inventories to include asset ownership and levels of criticality.	CounterACT shows the logged-in user as well as information from authentication servers.
64	07 Vulnerability Management	07.a Inventory of Assets	The information lifecycle manages the secure use, transfer, exchange and disposal of IT-related assets.	Expand and develop IT lifecycle policies to further address the use and disposal of IT assets.	CounterACT supports the effective enforcement of portions of information security regulatory frameworks/guidelines.
65	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	The organization performs an annual enterprise security posture review.	Expand IT security policies to include annual enterprise security posture reviews and the use of automated monitoring mechanisms, and employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.	CounterACT checks systems for compliance in real time on an ongoing basis.
66	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	The organization scans for vulnerabilities in the information system and hosted applications to determine the state of flaw remediation within every thirty (30) days (automatically) and again (manually or automatically) when new vulnerabilities potentially affecting the systems and networked environments are identified and reported.	Implement process to scan for vulnerabilities in the information system and hosted applications to determine the state of flaw remediation within every thirty (30) days.	CounterACT can be used in conjunction with vulnerablity assessment tools to automate response to vulnerabilities found in the environment.
67	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	The organization updates the list of information system vulnerabilities scanned within every thirty (30) days or when new vulnerabilities are identified and reported.	Develop and maintain a Threat and Vulnerability Management program which includes vulnerability scanning and vulnerability tracking and should include privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.	CounterACT can be used in conjunction with vulnerabilty asessment tools to automate response to vulnerabilities found in the environment.
68	07 Vulnerability Management	10.m Control of Technical Vulnerabilities	The technical vulnerability management program is evaluated on a quarterly basis.	Develop a Threat and Vulnerability Management policy which mandates evaluation on a quarterly basis to ensure its effectiveness and efficiency where systems of high risk are addressed first.	CounterACT can be used in conjunction with vulnerabilty assessment tools to automate response to vulnerabilities found in the environment.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
70	08 Network Protection	09.m Network Controls	A DMZ is established with all database(s), servers and other system components storing or processing covered information placed behind it to limit external network traffic to the internal network.	Document the existence of an established demilitarized zone, IP-based traffic restrictions, dynamic packet filtering, and strategic placement of servers and system components in an environment segregated from the DMZ.	CounterACT can help segment networks based on function, and work directly with firewall and ATD systems.
72	08 Network Protection	01.i Policy on the Use of Network Services	Authorized individuals are prohibited from using external information systems unless they can verify security controls are adequate and have an approved connection or processing agreement.	Expand access provisioning documentation to address the security review and analysis of information systems including ports, services and similar applications (e.g., protocols) necessary for business, and provide the rationale or identify compensating controls implemented for those protocols considered to be insecure.	While this requirement deals with documentation, it should be known that technical controls can be implemented around those policies with CounterACT.
73	08 Network Protection	01.n Network Connection Control	Exceptions to the traffic flow policy are documented with a supporting mission/business need and duration of that need, reviewed annually, and the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/ business need.	Develop policies and procedures for network procedures, including a network traffic flow policy and procedures for monitoring against that policy.	CounterACT can help segment networks based on function, and work directly with firewall and ATD systems.
76	08 Network Protection	09.m Network Controls	Firewalls restrict inbound and outbound traffic to the minimum necessary.	Expand network protections documentation and procedures to require the use of authentication mechanisms and to develop access control lists for remote access connections.	CounterACT can help segment networks based on function and work directly with firewall and ATD systems.
77	08 Network Protection	10.b Input Data Validation	For any public-facing web applications, the organization addresses new threats and vulnerabilities on an ongoing basis and ensures these applications are protected against known attacks by one of two methods.	Expand system development lifecycle guidance on the maintenance and vulnerability management, and ensure the vulnerability management process addresses new threats and vulnerabilities on an ongoing basis. Additionally, ensure the applications are protected against known attacks by either of the following methods: i. review applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; ii. install an automated technical solution that detects and prevents web-based attacks (e.g., a web-application firewall) in front of public-facing web applications, to continually check all traffic.	CounterACT can help segment networks based on function and work directly with firewall and ATD systems as well as repond automatically to threats.
78	08 Network Protection	01.n Network Connection Control	For each network access point or external telecommunication service's managed interface, network traffic is controlled in accordance with the organization's access control policy through firewall and other network-related restrictions.	Document practices for control of network access and other aspects related to external telecommunication services or other managed interfaces.	Network access control is a core function of CounterACT.
79	08 Network Protection	09.n Security of Network Services	Formal agreements with external information system providers include specific obligations for security and privacy.	Ensure contractual agreements with external providers include specific obligations for security and privacy.	CounterACT Guest Registration allows access to your network without compromising internal network security. Several guest registration options let you tailor the guest admission process to your organization's needs. Access is role-based: CounterACT help ensure that the right people with the right devices gain access to the right network resources.It leverages your existing directory where you assign roles to user identities.
81	08 Network Protection	09.m Network Controls	MAC address authentication and static IP addresses are implemented.	Develop network protections policies which document requirements for the use of MAC address authentication and static IPs.	Network access control is a core function of CounterACT.
82	08 Network Protection	01.m Segregation in Networks	Networks are segregated from production-level networks when migrating physical servers, applications or data to virtualized servers.	Document network security requirements with physical and logical segregation requirements.	CounterACT can help segment networks based on function and, with the virtual machine modules, can enforce segmentation in virtual environments.
83	08 Network Protection	09.m Network Controls	Organizations shall use secured and encrypted communication channels when migrating physical servers, applications or data to virtualized servers.	Ensure secured and encrypted communication channels are used when migrating physical servers, applications or data to virtualized servers.	CounterACT compliance/enforcement policies can be used to audit/ enforce encryption client status/configuration on Windows and Linux servers.
84	08 Network Protection	09.m Network Controls	Quarterly network scans are performed to identify unauthorized components/devices.	Perform quarterly network scans to identify unauthorized components/devices.	CounterACT enables automated incident response actions such as data access control or notification of the administrator of an incident. CounterACT works with ATD, SIEM, VA and other leading threat detection systems to automate host and network controls.
85	08 Network Protection	01.n Network Connection Control	Remote devices establishing a non-remote connection are not allowed to communicate with external (remote) resources.	Develop policies and procedures for provisioning and maintaining remote access. Specifically, through the use of VPN. VPN should be configured where access to Multiplan resources are through the VPN only and should not maintain simultaneous connections with non-MultiPlan resources/networks.	Network access control is a core function of CounterACT.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
86	08 Network Protection	01.n Network Routing Control	Requirements for network routing control are based on the access control policy, including positive source and destination checking mechanisms, such as firewall validation of source/destination addresses, and the hiding of internal directory services and IP addresses.	Develop network protection policies which cover the necessary protections on the network, including routing protocols and checking mechanisms for network traffic.	CounterACT can help segment networks based on function, and work directly with firewall and ATD systems.
87	08 Network Protection	01.n Network Routing Control	Routing controls are implemented through security gateways (e.g., firewalls) used between internal and external networks (e.g., the Internet and third-party networks).	Develop network protection policies that cover the necessary protections on the network, including firewalls and other security gateway devices.	CounterACT can help segment networks based on function and work directly with firewall and ATD systems.
88	08 Network Protection	01.m Segregation in Networks	Security gateways (e.g., firewalls)--capable of enforcing security policies, configurable to filter traffic between domains, and blocking unauthorized access--are used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet) including DMZs, and enforce access control policies for each of the domains.	Document network security requirements and procedures, including requirements for firewalls, IPS/IDS, and logging requirements.	CounterACT can help segment networks based on function and can work directly with firewall and ATD systems.
89	08 Network Protection	09.m Network Controls	Technical tools such as an IDS are implemented and operating on the network perimeter and other key points to identify vulnerabilities and mitigate threats, and are updated on a regular basis.	Develop network protection policies which document and provide guidance on the use of an Intrusion Detection System and vulnerability scans.	CounterACT has a built-in signatureless intrusion detection system.
90	08 Network Protection	01.n Network Connection Control	The ability of users to connect to the internal network is restricted using a deny-by-default and allow-by-exception policy at managed interfaces according to the access control policy and the requirements of clinical and business applications.	Develop network access protections, including access controls for deny-by-default and allow-by-exception requirements.	Network access control is a core function of CounterACT.
92	08 Network Protection	01.i Policy on the Use of Network Services	The organization determines who is allowed access to specific networks and network services and specifies the means of access allowed, including specific ports, protocols and services along with the rationale--or identifies implemented compensating controls--for them to be non-secure.	Develop/formalize and document procedures for managing network access. Procedures must specify who is allowed access to specific networks and network services and the means of access allowed, including specific ports, protocols and services along with the rationale—or identify implemented compensating controls—for them to be secure.	The policies for managing network access are input into the CounterACT policies and can be maintained and enforced.
94	08 Network Protection	01.i Policy on the Use of Network Services	The organization identifies and manages the external information systems that may be used by employees and other workforce members.	Develop a list of all approved information systems and leverage the Altiris asset management system that is currently in place to enforce application use restrictions.	CounterACT can be used to enforce the current version/ configuration being used.
95	08 Network Protection	01.i Policy on the Use of Network Services	The organization specifies the networks and network services to which users are authorized access.	Expand access provisioning documentation to address the policies and procedures regarding the provisioning of access to the network.	Access control is a core function of CounterACT.
96	08 Network Protection	09.m Network Controls	The organization uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection that, at a minimum, use shared information (i.e., MAC or IP address) and access controls lists to control remote network access.	Perform regular reviews of wireless configurations to verify that security requirements are maintained. Ensure that requirements for authentication on the network are clearly documented.	CounterACT supports 802.1X to perform authentication. It is differentiated from other products by not requiring 802.1X, as it can be a challenge for some to implement. CounterACT integrates with existing network devices and can assess endpoint hygiene using an agentless approach. Alerts, controls and reports can be performed with the information CounterACT gathers on the endpoint device. Being agentless is important, especially with non-traditional endpoints such as IoT devices (IP cameras, medical devices, printers, etc).
97	08 Network Protection	09.m Network Controls	The organization uses at least 2 DNS servers located on different subnets, which are geographically separated and perform different roles (internal and external) to eliminate single points of failure and enhance redundancy.	Document network protection procedures with requirements for DNS servers to be physically separated, logically segregated, and segregated based on their roles (internal or external).	CounterACT can provide network segmentation.
98	08 Network Protection	09.m Network Controls	The organization utilizes firewalls from at least 2 different vendors that employ stateful packet inspection (also known as dynamic packet filtering).	Document network protection policies and procedures with requirements for multiple firewalls and dynamic packet filtering to reduce the possibility of compromising the entire network.	CounterACT can help with restriction actions and automate response with ATD and firewall systems.
99	08 Network Protection	01.m Segregation in Networks	The organization's network is logically and physically segmented with a defined security perimeter and a graduated set of controls, including subnetworks for publicly accessible system components that are logically separated from the internal network based on organizational requirements; and traffic is controlled based on functionality required and classification of the data/systems based on a risk assessment and their respective security requirements.	Formally document the current network security requirements with physical and logical segregation requirements noted.	CounterACT can help segment networks based on function and can work directly with firewall and advanced threat detection (ATD) systems.
100	08 Network Protection	01.w Sensitive System Isolation	The sensitivity of applications/systems is explicitly identified and documented by the application/system owner.	Expand the healthcare provider's asset inventory system that is currently being used to include system sensitivity with approval from the system owner.	CounterACT can provide endpoint security event, device and user data to the healthcare provider's CMDB.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
101	08 Network Protection	01.w Sensitive System Isolation	Unless the risk is identified and accepted by the data owner, sensitive systems shall be isolated (physically or logically) from non-sensitive applications/systems.	Develop network protection policies which require the separation of sensitive systems from non-sensitive applications on the network.	CounterACT can automatically isolate hosts based on a security event such as non-compliance.
102	09 Transmission Protection	10.f Policy on the Use of Cryptographic Controls	Encryption is used to protect covered information on mobile/removable media and across communication lines based on pre-determined criteria.	Implement mandatory encryption standards for all removable media and mobile devices. Design baseline requirement was met; no recommendations noted.	CounterACT can detect unapproved USB device types and enforce control such as a disconnect on the USB. It can limit access to approved USB-encypted drives and can also integrate with MobileIron and AirWatch to provide alert and control functions on mobile devices that do not have enterprise mobility management agents installed for device encryption.
103	09 Transmission Protection	10.f Policy on the Use of Cryptographic Controls	Key management is implemented based on specific roles and responsibilities and in consideration of national and international regulations, restrictions and issues.	Update policy and procedure documentation to reflect key management specific to national and international regulations and issues (where applicable), as well as perform an assessment at least annually to ensure that key management policies are in line with applicable standards.	CounterACT supports the effective enforcement of portions of information security regulatory frameworks/guidelines.
104	09 Transmission Protection	10.g Key Management	Keys are limited to a period of time not to exceed one year.	Amend encryption policies and procedures to require that all encryption keys have a documented and enforced life span after which they cannot be used. The maximum life span should be one year in order to reduce the likelihood of compromise, activation, and deactivation.	CounterACT can be used to enforce the correct version of encryption software and help ensure the proper configuration is used on managed Windows/Mac/Linux machines.
107	09 Transmission Protection	09.s Information Exchange Policies and Procedures	The organization formally addresses multiple safeguards before allowing the use of information systems for information exchange.	Develop policies and procedures that document the multiple safeguards used to protect the exchange of information.	CounterACT can run compliance checks on endpoints to determine if they are approved corporate assets, and that they comply with security standards before allowing them to connect to the corporate network. It does not require an agent or 802.1X, so it can be quickly deployed and provide immediate value. CounterACT can be used to enforce mobile device compliance via integration with MDM/EMM products.
115	11 Access Control	01.t Session Time-out	A time-out system (e.g., a screen saver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to re-establish authenticated access; or, if the system cannot be modified, a limited form of time-out that clears the screen but does not close down the application or network sessions is used.	Ensure that configurations are set within the environment per the documented policies and procedures. Ensure policy and procedure documentation is aligned with the current practices that are being executed.	CounterACT is used by healthcare orginizations to validate that systems requiring screen saver time-out policies are in place, as well as to handle excluded devices such as digital signage.
117	11 Access Control	01.a Access Control Policy	Access controls are consistently managed for all systems and applications in networked and distributed environments based on the classification of and risks to the information stored, processed, or transmitted.	Amend the data classification policy to align with risk assessments for data types. (i.e., restricting provisioning based on sensitivity of data).	Network access control is a core function of CounterACT.
118	11 Access Control	01.v Information Access Restriction	Access rights from an application to other applications are controlled.	Ensure access rights from an application to other applications are controlled.	CounterACT can be configured to detect traffic from one endpoint to another or a range of network IPs. Once traffic is detected, CounterACT can alert or perform control actions.
120	11 Access Control	06.e Prevention of Misuse of Information Assets	Computer login banners are displayed outlining the terms and conditions of access and must be accepted before access is granted.	Amend information security policies to add login banners stating that the computer in use is private, and post monitoring, privacy, and security notices along with user acceptance of terms before access is granted.	CounterACT can display a captive portal before the user can access the network. This is typically used for Bring Your Own Device (BYOD) or Guest access.
122	11 Access Control	01.v Information Access Restriction	Covered information is encrypted when stored in non-secure areas and, if not encrypted at rest, the organization must document its rationale.	Expand the data classification and encryption policy to include requirements that any non-encrypted information in non-secure areas be documented with rationale.	CounterACT helps detect blindspots in your DLP agent deployment. It can verify whether the DLP agent is installed, running and up to date. If any of the policy is failing, CounterACT can alert and automate enforcement of compliance/remediation/control actions.
129	11 Access Control	01.a Access Control Policy	Logical and physical access control rules and rights for each user or group of users for each application are considered together and clearly defined in standard user access profiles (e.g., roles) based on need-to-know, need-to-share, least privilege and other relevant requirements.	Develop standardized user profiles for different user groups and migrate existing and new accounts into those user profiles. Exceptions should be approved and documented.	CounterACT integrates with LDAP and AD to leverage the groups and can therefore provide access and controls to network resources. For example, account group users can be move to a VLAN or printers connected to switch ports can have an ACL that only allows access to print servers and network management servers.
131	11 Access Control	01.j User Authentication for External Connections	Network equipment is checked for unanticipated dial-up capabilities.	Develop consistent documentation for network protection procedures, including configuration standards and network monitoring for equipment for all elements of the network.	CounterACT uses SNMP and Nmap to help detect misconfigurations of network devices. SNMP is used to determine if the correct network management is configured and Nmap can help detect unsecure open ports or services such as telnet and HTTP.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
132	11 Access Control	01.v Information Access Restriction	Outputs from application systems handling covered information are limited to the minimum necessary and sent only to authorized terminals/locations.	Expand the data classification policy and associated procedures to specify that covered information can only travel to specified locations. Requirements could include: i. controll access rights to other applications according to applicable access control policies; ii. ensure that outputs from application systems handling covered information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations; and iii. periodic reviews of such outputs to ensure that redundant information is removed.	CounterACT can be configured to detect traffic from one endpoint to another or a range of network IP addresses. Once traffic is detected, CounterACT can send alerts or perform control actions.
133	11 Access Control	01.j User Authentication for External Connections	Remote access by vendors and business partners (e.g., for remote maintenance) is disabled/deactivated when not in use.	Develop and document formal protocols related to managing vendor access to assist with ensuring vendor and business partner access is deactivated consistently.	The policies for managing vendor and business partner network access are input into the CounterACT policies and can be maintained and enforced.
134	11 Access Control	01.j User Authentication for External Connections	Remote administration sessions are authorized, encrypted, and employ increased security measures.	Expand remote access policies and procedures to specifically identify increased security standards for remote administration and access activities.	CounterACT can be used to apply restrictions based on device posture.
136	11 Access Control	01.a Access Control Policy	The access authorization process addresses requests for access, changes to access, removal of access, and emergency access.	Operational Effectiveness: Implement emergency access procedures and regular reviews of the access process to ensure access is only granted using approved channels. Expand the Information security policy and access provisioning policy to address standard access profiles and the provisioning of emergency access.	The policies for managing network access are input into the CounterACT policies and can be maintained and enforced.
137	11 Access Control	09.ab Monitoring System Use	Unauthorized remote access connections to the organization's network and information systems are monitored and reviewed at least quarterly, and appropriate action is taken when unauthorized connections are discovered.	Expand monitoring and remote access policies and procedures to ensure that unauthorized remote access connections to the organization's network and information systems are monitored and reviewed at least quarterly, and appropriate action is taken when unauthorized connections are discovered.	CounterACT can use a port SPAN on the remote access point/ VPN concentrator to see the traffic flow. It can integrate VPN endpoints by IP and provide the same endpoint visibility as if endpoints are on your local network and provide control using our Virtual Firewall (TCP reset and ICMP unreachable on traffic flow). It can also disconnect VPN sessions on certain products.
146	12 Audit Logging & Monitoring	09.ab Monitoring System Use	Alerts are generated for technical personnel to analyze and investigate suspicious activity or suspected violations.	Verify alerts are generated by all systems to enable technical personnel to analyze and investigate suspicious activity or suspected violations, and ensure manual reviews of system audit records are performed randomly on demand, and no less than once every thirty (30) days.	CounterACT can send alerts to administrators related to suspicious activity such as failed authentications, MAC spoofing, etc.
149	12 Audit Logging & Monitoring	09.aa Audit Logging	Audit logs are maintained for management activities, system and application startup/shutdown/errors, file changes, and security policy changes.	Expand audit-logging capabilities to address the capture of system errors and changes to policies such as: i. server alerts and error messages; ii. user log-on and log-off (successful or unsuccessful); iii. all system administration activities; iv. modification of privileges and access; v. Start up and shut down; vi. application modifications; vii. application alerts and error messages; viii. configuration changes; ix. account creation, modification, or deletion; x. file creation and deletion; xi. read access to sensitive information; xii. modification to sensitive information; and xiii. printing sensitive information.	CounterACT can maintain endpoint/host logs.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
152	12 Audit Logging & Monitoring	09.aa Audit Logging	Auditing is always available while the system is active and tracks key events, success/failed data access, system security configuration changes, privileged or utility use, any alarms raised, activation and de-activation of protection systems (e.g., AV and IDS), identification and authentication mechanisms, and creation and deletion of system-level objects.	Expand logging procedures to cover all systems and a wider range of functionalities, such as: i. dates, times, and details of key events (e.g., log-on and log-off); ii. records of successful and rejected system access attempts; iii. records of successful and rejected data and other resource access attempts; iv. changes to system configuration and procedures for managing configuration changes; v. use of privileges; vi. use of system utilities and applications; vii. files accessed and the kind of access; viii. network addresses and protocols; ix. alarms raised by the access control system; and x. activation and de-activation of protection systems, including anti-virus systems and intrusion detection systems, and identification and authentication mechanisms. xi. creation and deletion of system-level objects.	CounterACT provides monitoring of endpoint state changes, and can take appropriate configured actions such as logging the event, sending syslog to third-party vendors, notifying administrators, etc.
156	12 Audit Logging & Monitoring	09.ab Monitoring System Use	Automated systems support near real-time analysis and alerting of events (e.g., malicious code, potential intrusions) and integrate intrusion detection into access and flow control mechanisms.	Expand the capacity for automatic alerting and analysis of all systems to ensure the employment of automated mechanisms to integrate the audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	CounterACT has an open API and platform to allow for automation between current network devices (system, router, wireless controller) and security software. We currently integrate with over 70 tools from leading companies, including FireEye, Palo Alto Networks, Rapid7, Nexus, Splunk, McAfee and VMware. Full list: https://www.forescout.com/partners/technology-partner-program/
157	12 Audit Logging & Monitoring	09.c Segregation of Duties	The number of individuals responsible for administering access is limited to the minimum necessary based upon each user's role and responsibilities, and these individuals cannot access audit functions related to these controls.	Amend the policies to incorporate references and practices relating to the principle of least privilege (limited to the minimum necessary based upon each user's role and responsibilities, and a prohibition on these individuals accessing audit functions related to these controls). Additionally, the amended policies should include assurances that the development, testing, quality assurance and production functions are separated among multiple individuals/ groups.	CounterACT supports spreading permissions across multiple administrators.
158	12 Audit Logging & Monitoring	09.c Segregation of Duties	Job descriptions define duties and responsibilities that support the separation of duties across multiple users.	Amend the job descriptions to ensure they define duties and responsibilities that support the separation of duties across multiple users. Additionally, incompatible duties shall be segregated across multiple users to minimize the opportunity for misuse or fraud; and, in cases where conflicting duties must be assigned to a single user, activity logging and log reviews by an independent party shall be required.	CounterACT supports spreading permissions across multiple administrators.
160	12 Audit Logging & Monitoring	09.ab Monitoring System Use	Monitoring includes inbound and outbound communications and file integrity monitoring.	Develop network protection procedures which include plans for the monitoring of inbound and outbound network activity for anomalous activity, as well as change detection .	CounterACT can be configured to detect anomalous activities and tie them to device type. For example, IP cameras, printers and medical devices are allowed to communicate with an internal server, but if they start to communicate with external resources, CounterACT can send alerts and provide network controls to isolate or block that specific traffic or all traffic.
161	12 Audit Logging & Monitoring	09.ab Monitoring System Use	Monitoring includes privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.	Further develop monitoring procedures to address the usage of privileged access and provision higher monitoring requirements for privileged accounts, thus ensuring that privileged operations are monitored for: i. the use of privileged accounts (e.g., supervisor, root, administrator); ii. the system start-up and stop; and iii. I/O device attachment/detachment.	CounterACT can provide visibility as well as control for mananged endpoints. It can determine if a privileged account is being used and either perform control actions (VLAN isolation, port ACL, etc.) or alert staff of activity. It can also detect the moment a device connects and disconnects from the network. Custom scripts can be use to determine system start-up and last shutdown. Detection and control of external devices is supported as well.
162	12 Audit Logging & Monitoring	09.c Segregation of Duties	No single person is able to access, modify or use information systems without authorization or detection.	Perform regular audit accounts to verify that no generic or shared accounts exist. Design baseline requirement was met; no recommendations noted.	CounterACT authenticates the user on a restricted segment (based on VLAN or ACL), and only once the user is authenticated successfully is appropriate authorization provisioned.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
164	12 Audit Logging & Monitoring	09.c Segregation of Duties	Separation of duties is used to limit the risk of unauthorized or unintentional modification of information and systems.	Develop procedures to facilitate separation of duties across the organization to limit the risk of unauthorized or unintentional modification of information systems; or, as an alternative, utilize dual controls to limit the risk of unauthorized or unintentional modification of information and systems.	CounterACT supports spreading permissions across multiple administrators.
166	12 Audit Logging & Monitoring	09.ab Monitoring System Use	The information system is able to automatically process audit records for events of interest based on selectable criteria.	Expand the capacity for automatic alerting and analysis of all systems in an effort to facilitate near real-time analysis of events and maintenance of an audit log to track prohibited sources and services.	CounterACT logs are searchable and events of interest can be sent to SIEM and other security platforms for long-term archiving and reporting.
167	12 Audit Logging & Monitoring	09.ab Monitoring System Use	The organization analyzes and correlates audit records across different repositories and correlates this information with input from non-technical sources.	Analyze and correlate audit records across different repositories and correlate with input information from non-technical sources to enhance organization-wide situational awareness.	CounterACT logs are searchable and events of interest can be sent to SIEM and other security platforms for long-term archiving and reporting.
168	12 Audit Logging & Monitoring	06.e Prevention of Misuse of Information Assets	The organization provides notice that the employee's actions may be monitored, and that the employee consents to such monitoring.	Develop separate processes for employees to acknowledge monitoring outside the acknowledgment of policies during training. Design baseline requirement was met; no recommendations noted.	CounterACT can send email, HTTP notification or balloon notification to employees.
170	12 Audit Logging & Monitoring	09.af Clock Synchronization	The organization's system clocks are synchronized to an agreed-upon, authoritative real-time standard (e.g., daylight savings time) and synchronized daily and at system boot.	Develop configuration documentation to address how time is provisioned across user devices and the network environment and define MultiPlan's requirement to synchronize all system clocks and times where a computer or communications device has the capability to operate a real-time clock.	CounterACT allows you to write custom scripts to be deployed on the endpoints to set the clocks as per requirements.
173	13 Education, Training and Awareness	06.e Prevention of Misuse of Information Assets	Employees and contractors are informed in writing (e.g., when they sign rules of behavior or an acceptable use agreement) that violations of security policies will result in sanctions or disciplinary action (see 02.f).	Expand training requirements to cover contractors and therefore capture their consent to acceptable use policies.	CounterACT can include acceptable use policies with confirmation of receipt via captive portal during the guest/BYOD/corporate device network access process.
174	13 Education, Training and Awareness	02.e Information Security Awareness, Education, and Training	Employees and contractors receive documented initial (as part of their onboarding within 60 days of hire), annual and ongoing training on their roles related to security and privacy.	Implement role-based training for roles with high cybersecurity or privacy risk. Track role-based training within the same system and with the same requirements as standardized training. Expand training procedures to cover contractors and ensure that they are aware of security and privacy policies.	CounterACT can assist with the distribution of training material via captive portal and email.
182	14 Third-Party Assurance	05.k Addressing Security in Third-Party Agreements	A standard agreement with third parties is defined and includes the required security controls in accordance with the organization's security policies.	Ensure that additional policy requirements for transfer of subcontractor personnel, IT installations/maintenance, penalties, and issues escalation are monitored, managed and implemented in accordance with documented policies. Add additional details to the standard MSA and FA-02 which cover the transfer of subcontractor personnel, IT installation and maintenance responsibilities, penalties for non-compliance and the escalation process for issues encountered.	CounterACT can use a dissolvable agent to check endpoint security compliance while the contractor is trying to get on the network.
183	14 Third-Party Assurance	05.i Identification of Risks Related to External Parties	Access granted to external parties is limited to the minimum necessary and granted only for the duration required.	Implement standardized requirements for vendor accounts, including duration maximums and access limits, and update policies and procedures to address updates to vendor control functions. Also, document requirements for vendor access.	Employees can use a CounterACT-sponsored portal to provision network access to a guest/contractor before their visit. Access can be granted for the duration entered in the sponsor portal. Access can also be terminated from the sponsor portal.
184	14 Third-Party Assurance	05.i Identification of Risks Related to External Parties	Access to the organization's information and systems by external parties is not permitted until due diligence has been conducted, the appropriate controls have been implemented, and a contract/agreement reflecting the security requirements is signed acknowledging they understand and accept their obligations.	Expand policies and procedures for third-party due diligence to include requirements that vendors be evaluated specific to security control requirements and prior to access being granted on the systems.	CounterACT can provide visibility and enforcement of the written policy regarding network access. Approved devices can be allowed access and rogue devices can be isolated or staff can be alerted about out-of-policy activity. CounterACT provides Guest/Contractor/BYOD registration/onboarding based on defined security policies by an organization, which means network access is controlled based on security policies and compliance.
202	15 Incident Management	11.a Reporting Information Security Events	All employees, contractors and other third-party users receive mandatory incident-response training to ensure they are aware of their responsibilities to report any information security events as quickly as possible, the procedure for reporting information security events and the point(s) of contact.	Incorporate training for reporting security and IT incidents into the general employee training in order to reduce the delays when reporting. Design baseline requirement was met; no recommendations noted.	CounterACT can create awareness by sending periodic emails, HTTP notification or balloon notification to help ensure that employees, contractors and other third-party users receive the appropriate training.
204	15 Incident Management	11.c Responsibilities and Procedures	Following an incident, audit trails and evidence are collected and secured, system and data access controlled, emergency actions documented, actions reported to management, system and control integrity confirmed with minimal delay, and stakeholders notified immediately when a safe and secure environment has been restored.	Amend Security Incident Response procedures to include additional details and procedures for how incidents are resolved and how responsible parties should be contacted.	CounterACT stores data for up to a week for audit trails and collecting evidence. CounterACT enables automated incident response actions such as data access control or notification of the administrator of an incident, etc. CounterACT works with ATD, SIEM, VA and other leading threat detection systems to automate host and network controls.

#	Domain	CSF Control	HITRUST CSF Requirement Statement	Recommendation	How ForeScout CounterACT® helps:
206	15 Incident Management	11.c Responsibilities and Procedures	Incidents are promptly reported to the appropriate authorities and outside parties (e.g., FedCIRC, CERT/CC).	Perform tests to verify the ability of the organization to comply with reporting requirements. Design baseline requirement was met; no recommendations noted.	CounterACT can send an email to authorities based on incidents reported by CounterACT or third-party security systems to CounterACT.
207	15 Incident Management	11.a D94	Intrusion detection/information protection system (IDS/IPS) alerts are utilized for reporting information security events.	Develop and amend procedures for network protection and monitoring to include the use of IPS/IDS technologies and monitoring/alerting based on IPS and IDS.	CounterACT includes an insider threat protection system for the purpose of identifying and blocking rogue port scans, email worms, service attacks and other malicious traffic.
211	15 Incident Management	11.c Responsibilities and Procedures	The incident response plan is communicated to the appropriate individuals throughout the organization.	Include incident response plans in documentation that is acknowledged by employees. Further, include incident response as a regular training topic. Design baseline requirement was met; no recommendations noted.	CounterACT can send an email or notification to employees. It can also send a reminder through HTTP or balloon notification to help ensure employees read the incident response plan.
213	15 Incident Management	11.a Reporting Information Security Events	The organization shall implement an insider threat program that includes a cross-discipline insider threat incident-handling team.	Develop an insider threat program in coordination with the threat and vulnerability management program.	CounterACT includes an insider threat protection system for the purpose of identifying and blocking rogue port scans, email worms, service attacks and other malicious traffic.
228	17 Risk Management	03.b Performing Risk Assessments	The organization performs risk assessments in a consistent way and at planned intervals, or when there are major changes to the organization's environment, and reviews the risk assessment results annually.	Continue development and implementation of risk management policy and practices, and align these practices with HITRUST baseline requirements.	CounterACT can continuously monitor and enforce endpoint compliance as stipulated by various regulatory requirements.
240	18 Physical & Environmental Security	08.b Physical Entry Controls	Inventories of physical access devices are performed every 90 days.	Expand automatic asset inventories to include physical security assets (e.g., cameras and badge reads), or implement a manual process to inventory those assets at a minimum of every 90 days.	CounterACT device discovery and classification can assist with an accurate count of physical devices on the network. For example, CounterACT can classify security cameras and badge readers on the network.
256	19 Data Protection & Privacy	06.d Data Protection and Privacy of Covered Information	The organization implements technical means to ensure covered information is stored in organization-specified locations.	Expand data classification policies and asset inventory capabilities to identify the systems where different types of sensitive data can be stored.	CounterACT can provide assistance in the enforcement of data storage policies.
257	19 Data Protection & Privacy	06.d Data Protection and Privacy of Covered Information	The organization specifies where covered information can be stored.	Expand data classification, encryption policies and system inventory capabilities to address exactly where and how covered information can be stored.	CounterACT can provide assistance in the enforcement of data storage policies.

About ForeScout

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of September 30, 2016 more than 2,200 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions. **See** devices. **Control** them. **Orchestrate** systemwide response. Learn how at www.forescout.com.

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

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