FORESCOUT

Addressing the HITRUST CSF with ForeScout

Make HITRUST Common Security Framework Adoption a Reality with CounterACT®

Organizational Challenges

- Protect electronic information as mandated by HITRUST Common Security Framework
- Help ensure compliance with various healthcare requirements underlying HITRUST in an efficient and effective way
- Help ensure information protection through device, network and user access controls
- Streamline network access and information sharing for trusted contractors, partners and patients
- Secure information from traditional systems (PCs, laptops and servers) as well as BYOD and IoT

Technical Challenges

- Discover traditional, BYOD, medical IoT, rogue devices and non-medical IoT devices
- Control access to confidential and sensitive data
- Prevent infected or non-compliant devices from spreading malware or viruses across the network
- Defend against targeted attacks that can steal data or force network downtime
- Measure effectiveness of security controls and demonstrate compliance with HITRUST CSF

The HITRUST Common Security Framework (CSF) is a superset of security controls and requirements derived from multiple standards and regulations, as well as some that are unique to HITRUST. It was developed to provide a common framework that any healthcare or related organization can use to create, access, store or exchange protected health information. Since HITRUST CSF aggregates requirements from multiple standards and frameworks, it helps organizations achieve efficiency in meeting those requirements and takes a comprehensive approach to securing enterprise networks.

HITRUST incorporates requirements from HIPAA's Security Rule, the Payment Card Industry Data Security Standard (PCI DSS), the National Institute of Standards and Technology Risk Management Framework (NIST, RMF), the NIST Framework for Improving Critical Infrastructure Cybersecurity, relevant state-specific standards and various other standards.

These controls should be at the core of every healthcare entity's defense and/or architecture for protection of systems that are organizationally defined or established. ForeScout CounterACT® can be leveraged for this type of high-level, organization-wide control to secure healthcare networks and the protected healthcare information they contain.

Securing Healthcare Providers with ForeScout CounterACT

Many healthcare organizations today are unable to enforce cybersecurity policies across the enterprise, and, consequently, find it difficult to protect electronic health records. A key reason for this is the fact that devices that lack required security agents come and go from the network at will and are largely undetected by periodic, point-in-time vulnerability scans. Another reason is that many security systems work in silos and threats go undetected. This gap in security policy enforcement puts the entire network and the information it holds in jeopardy.

To make matters worse, Internet of Things (IoT) adoption is increasing network attack surfaces exponentially by opening up more entry points for stealing protected electronic health records.

In 2016, 450 Healthcare breach incidents were reported and 27 million records were breached.[1] Many healthcare organizations were victims of ransomware attacks and had to pay cybercriminals to get their data back.[2]

CounterACT can help prevent such attacks. It can be leveraged for organization-wide control to track devices and their users within legacy, new and highly technical network infrastructure without reengineering established networks or disrupting services. The CounterACT platform provides administrators with the critical ability to see and monitor myriad devices on the network in real time, from endpoints such as PCs, laptops, and printers, to IoT devices (including network-connected medical systems) and personally owned smartphones and tablets.

In addition to playing a critical role in securing devices and networks, the CounterACT platform can also orchestrate and enable a variety of security tools to share information and work together. This orchestration allows enterprises to integrate and automate their security responses while also helping to support compliance and standardization goals as well as preserving investments in existing security tools.

Delivering on various compliance standards within HITRUST presents organizations with a complex set of challenges from a people, process and technology point of view. By helping to enforce the HITRUST CSF, CounterACT helps healthcare organizations to comply with HIPAA, NIST, PCI and other regulatory standards.

Supporting HITRUST CSF Compliance

The following is a summary of how ForeScout CounterACT supports HITRUST CSF.

- **Information Security Management Program:** CounterACT enables creation of an information security management program by providing capabilities that enable an organization to keep track of—and secure—the devices, programs and open ports that are on a network. It also enables this type of program by allowing for orchestration of a system-wide threat response to remediate vulnerabilities and security incidents in the network.

  Related HITRUST Control References: (0.a) Information Security Management Program.

- **Access Control, Authorization and Authentication:** CounterACT enables implementation of policies and procedures to help ensure that members of an organization's workforce and related devices have appropriate access to protected electronic health records, and to prevent unauthorized workforce members and devices from obtaining access to protected electronic health records.

  When a device is attempting to connect to the network, CounterACT can identify the device type and location, user identity and role (employee, contractor, patient, guest), and level of compliance. It can even determine whether the device is owned by the organization or the user. Based on this information, CounterACT helps ensure that the right people with the right devices gain access to the right network resources. CounterACT also integrates with a variety of third-party authentication systems to help validate unique identities and users prior to their gaining role-based network access.

  As part of decision making as to whether to grant or deny access, CounterACT can collect additional data that includes the device's operating system (Windows®, Macintosh®, Linux®, iOS® or Android™), whether the device is physical or virtual, and whether it's a non-user device such as a printer, Voice over Internet Protocol (VoIP) phone, security or manufacturing system, or medical or point-of-sale device. It can also determine where the device is connecting as well as the connection type (wired, wireless, Virtual Private Network) and the device's IP address, Media Access Control (MAC) address, switch port, Service Set Identifier (SSID) and Virtual Local Area Network (VLAN).

  For managed devices, CounterACT can identify the users currently logged in and their account types. It compares this data with policies for the device and user. If discrepancies are found, CounterACT can restrict or deny access.

  CounterACT supports 802.1X to perform authentication. It is differentiated from other products by not requiring 802.1X, as this protocol can be a challenge for some to implement. CounterACT integrates with existing network devices and can assess endpoint hygiene using an agentless approach.

  Being agentless is important, especially with regard to non-traditional endpoints such as IoT devices (IP cameras, medical devices, printers, sensors, etc.) since many of them cannot host third-party security agents, run outdated or unsupported operating systems, cannot be patched and often lack even the most basic security features.

  To limit the risk of unauthorized or unintentional modification of information systems, CounterACT supports spreading permissions across multiple administrators.

  Related HITRUST Control References: (01.a) Access Control Policy, (01.b) Authorized Access to Information Systems, (01.i) Policy on the Use of Network Services, (01.j) User Authentication for External Connections, (01.k) Equipment Identification in Networks, (01.v) Information Access Control, (07.b) Ownership of Assets.

- **Endpoint Protection:** CounterACT is a physical or virtual agentless security appliance that can dynamically identify and evaluate network endpoints and applications the instant they connect to a network without requiring agents or prior knowledge of a device. CounterACT can quickly determine device configuration, software, services, patch state and the presence of security agents for compliance with security policy. It can also conduct similar evaluations of network devices and network-based security infrastructure.

  Next, it can provide remediation, control and continuous monitoring of devices. If a scan finds that a device's operating system or key applications are missing critical patches, CounterACT can trigger an update by the patch management system. When repairs are complete, CounterACT can restore authorized access. If the device is non-compliant, CounterACT can deny access or quarantine it for remediation.

  CounterACT can initiate an immediate vulnerability assessment (VA) of new network devices using its own scanning capabilities or those of a partner solution. CounterACT enables establishment, implementation, and active management

(tracks, reports on and corrects) of the security configuration of laptops, servers and workstations using a rigorous configuration management and change-control process in order to prevent attackers from exploiting vulnerable services and settings.

CounterACT can also be used to validate that systems requiring screensaver time-out policies are in place, as well as to handle excluded devices such as digital signage.

Related HITRUST Control References: (07.a) Inventory of Assets, (01.k) Equipment Identification in Networks, (01.t) Session Time-out, (011.a) Reporting Information Security Events.

- **Network Protection:** CounterACT enables implementation of network security policies and procedures, change control, monitoring and configuration changes, and access restrictions. It can provide for continuous visibility into devices that are connected to the network, both wired and wireless.

  CounterACT can provide for dynamic segmentation via Access Control List (ACL), VLAN or virtual firewall. This dynamic network segmentation capability is the basis for creation and modification of policies and procedures that enable segregation of network access so as to prevent lateral movement of attacks. This also helps contain protected electronic health information within a subgroup in an organization, protecting it from unauthorized access by the larger organization. Isolating healthcare clearing house functions is an example of this segmentation. Employees can be dynamically assigned to VLANs that are appropriate for their roles. An example of this is allowing only network administrators to access network infrastructure.

  When a device requests a network connection, CounterACT's initial scan can identify the type of connection and restrict or deny access if the endpoint posture is compromised.

  Related HITRUST Control References: (01.i) Policy on the Use of Network Services, (01.j) User Authentication for External Connections, (01.m) Segregation in Networks, (01.n) Network Connection Control, (01.v) Information Access Control, (01.w) Sensitive System Isolation, (06.c) Protection of Organizational Records, (09.c) Segregation of Duties, (09.m) Network Controls.

- **Third-Party Assurance:** CounterACT can help ensure that the right people with the right devices gain access to the right network resources. It does this by streamlining network access and information sharing for trusted contractors, partners, patients and vendors. Employees and contractors who bring their own devices can be redirected to an automated onboarding portal.

  CounterACT guest registration can allow access to networks without compromising internal network security. Several guest registration options enable tailoring the guest admission process to the organization's needs. CounterACT can use a dissolvable agent to check endpoint security compliance while contractors or guests are trying to access the network. It leverages existing directories to obtain user identities.

  Related HITRUST Control References: (05.i) Identification of Risks Related to External Parties, (0.5j) Addressing Security When Dealing with Customers, (05.k) Addressing Security in Third-Party Agreements.

- **Data Protection and Privacy:** CounterACT enables implementation of policies and procedures to protect electronic protected health information from improper alteration and destruction by limiting access to healthcare information systems to authorized users and devices. It can actively manage (inventories, tracks and corrects) all hardware devices on the network and their location so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

  CounterACT can also protect data from inappropriate third-party modifications by facilitating streamlined network access and information sharing for trusted contractors, partners, patients and vendors.

  Related HITRUST Control References: (06.d) Data Protection and Privacy of Covered Information.

- **Mobile Device Security:** CounterACT has the ability to see mobile devices the instant they connect to the network. CounterACT communicates bi-directionally with Enterprise Mobility Management (EMM) systems, which allows it to query for device attributes such as device enrollment or non-compliance. When used in conjunction with EMM systems, CounterACT also enables policy-based access rules regardless of the device type.

  CounterACT works with ForeScout ControlFabric® Architecture to orchestrate information sharing and automate operation among disparate security and IT management tools. By integrating with an EMM system, remote "wipe" functionality can be automated based upon condition match. For example, when a user's account is deactivated, the mobile device is automatically wiped.

  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.

  Related HITRUST Control References: (01.x) Mobile Computing and Communications, (01.y) Teleworking.

- **Portable Media and Device Security:** To support a host-based backup protection security strategy, CounterACT can help ensure that relevant third-party protection software is installed, correctly configured and operational. Connecting

devices can be evaluated as part of CounterACT's access inspection, and non-conforming hosts can be quarantined or removed from the network until repaired. CounterACT can also identify open ports, active protocols, and services currently running, and compare that inventory with configuration policies for that host. It can also restrict or deny access for non-compliant devices and issue a user notification or remediation alert. Healthcare organizations can use CounterACT to block unapproved external devices from network access. Typically, this functionality is deployed to block unencrypted USB devices.

Related HITRUST Control References: (01.l) Remote Diagnostic and Configuration Port Protection.

- **Configuration Management:** CounterACT can actively manage (inventories, tracks and corrects) software on the network so that only authorized software is installed and executed while unauthorized and unmanaged software is discovered and prevented from installation or execution.

  CounterACT can also install, update, re-start and re-configure various security and management agents such as those responsible for malware detection, encryption, firewall, DLP and patch management to enable data encryption and protection.

  If a CounterACT scan finds that the operating system or key applications are missing critical patches, it can trigger an update by the patch management system. When repairs are complete, CounterACT can restore authorized access.

  Related HITRUST Control References: (06.g) Compliance with Security Policies and Standards, (10.h) Control of Operational Software.

- **Incident Management:** If CounterACT discovers a security problem on an endpoint, its sophisticated policy manager can automatically execute a range of responses depending on the severity of the problem. It can also prevent infected or non-compliant devices from spreading malware or viruses across the network by sending alerts to administrators, putting infected devices in quarantine and repairing them. When repairs are complete, CounterACT can restore appropriate access and scan other endpoints for the same Indicators of Compromise (IOCs).

  CounterACT extends its incident management capabilities by integrating with leading third-party Advanced Threat Detection (ATD) and Next Generation Firewall (NGFW) systems to detect and automate threat response. For example, it can work with ATD systems to detect advanced threats and IOCs, identify potentially compromised endpoints and take corrective actions, including isolating compromised endpoints to prevent lateral threat propagation, preventing other infected endpoints from connecting to the network and providing additional endpoint context (user, device, applications, location) for effective incident response.

  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.

  CounterACT also enables integration with third-party Security Information and Event Management (SIEM) systems to provide real-time information, including data about managed (company-owned) and unmanaged IoT and rogue devices, as well as Bring Your Own Device (BYOD) and mobile systems, as they connect to the network. The SIEM can correlate this information with real-time information provided from other sources. Through this correlation, it can identify the threats that pose the greatest risk. Also, when used in conjunction with existing SIEMs, CounterACT can provide automation of daily tasks while providing a dynamic threat detection approach to security that helps to ensure compliance and reduces the attack surface.

  CounterACT's remediation capabilities can be further extended with scripts that run on non-compliant hosts to fix violations. 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.

  Related HITRUST Control References: (09.j) Controls Against Malicious Code, (09.m) Network Controls, (11.a) Reporting Information Security Events.

- **Audit Logging and Monitoring:** CounterACT enables enforcement of an appropriate use policy for network and information systems by implementing procedures to enable reviewing of information system activity, such as audit logs, access reports and security incident tracking reports. When a device requests network access, the CounterACT platform's initial inspection can determine whether logging is enabled and how it is configured, including the chosen location for log storage.

  When an incident occurs, responders can analyze logs and other data collected on the endpoint's activities, security status, access records, patch level, installed applications and other information to provide context to the event, and to determine appropriate incident-response activities, including remediation and follow-up. This data can be found in the real-time contextual database of endpoint state and activity that CounterACT builds through its own device inspections, and through its integrations with other management and security technologies.

  CounterACT has an open API and platform to allow for automation between current network devices (systems, routers, wireless controllers) and security software. CounterACT can integrate with more than 70 tools* from leading companies, including FireEye, Palo Alto Networks, Rapid7, Nexus, Splunk, McAfee, VMware and others. A current list of supported vendors can be found here: https://www.forescout.com/partners/technology-partner-program/

CounterACT can notify leading SIEM systems of endpoint system changes, the presence and activity of endpoint security agents, and logging applications and services. The SIEM's correlation engine can elevate the priority of an identified threat based on the type of threat reported and the severity of the threat based on other issues that have been reported. The SIEM console can provide continuous monitoring and support mitigation of enterprise-wide threats that can originate from non-compliant endpoints by department or organization. The SIEM can also generate compliance reports for the entire organization or by business unit in order to meet regulatory requirements.

Related HITRUST Control References: (09.s) Information Exchange Policies and Procedures: Encryption, (09.aa) Audit Logging, (09.ab) Monitoring System Use, (09.ae) Fault Logging.

- **Transmission Security:** CounterACT enables creation of policies and procedures that reflect required standards and guidance that enforce monitoring and control communications at external and internal boundaries in the system. CounterACT can be used to enforce the correct version of encryption software and help ensure the proper configuration is used on managed Windows, Mac or Linux systems. It can also run compliance checks on endpoints to determine if they are approved corporate assets and whether they comply with security standards before allowing them to connect to the corporate network and start information exchange.

  Related HITRUST Control References: (10.f) Policy on the Use of Cryptographic Controls, (10.g) Key Management.

- **Risk Management:** CounterACT can be used to audit configurations against industry standards and take corrective action for violations. It can also work in conjunction with Vulnerability Assessment (VA) systems to evaluate systems and, if desired, take automated remediation action.

  Related HITRUST Control References: (03.b) Performing Risk Assessments, (10.m) Control of Technical Vulnerabilities.

- **Physical and Environmental Protection:** CounterACT device discovery and classification can assist with an accurate count of physical devices on the network and classify them. The security team can then ensure proper physical protection for each of those devices.

  Related HITRUST Control References: (08.b) Physical Entry Controls.

A more detailed description of HITRUST CSF compliance support that maps the ForeScout CounterACT platform's capabilities to the framework's requirements can be found here: https://www.forescout.com/company/resources/forescout-counteract-features-benefits-hitrust/

CounterACT Security Platform

The ForeScout CounterACT security platform can provide real-time monitoring control and policy-based remediation of managed, unmanaged and non-traditional devices to support your HITRUST CSF compliance efforts. Here's how:

See. Detects devices the instant they connect to the network without requiring agents. Profiles and classifies devices, users, applications and operating systems. Continuously monitors managed devices as well as BYOD and IoT endpoints.

Control. Allows, limits or denies network access based on device posture and security policies. Assesses and remediates malicious or high-risk endpoints. Assists with improving compliance with industry mandates and regulations, including HITRUST standards.

Orchestrate. Shares contextual insights and data with IT security and management systems. Automates common workflows, IT tasks and security processes across systems. Accelerates system-wide response to quickly mitigate risks and data breaches.

FORESCOUT

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

[1] http://www.beckershospitalreview.com/Healthcare-information-technology/2016-averaged-1-healthcare-data-breach-per-day.html
[2] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
* As of December 31, 2016.