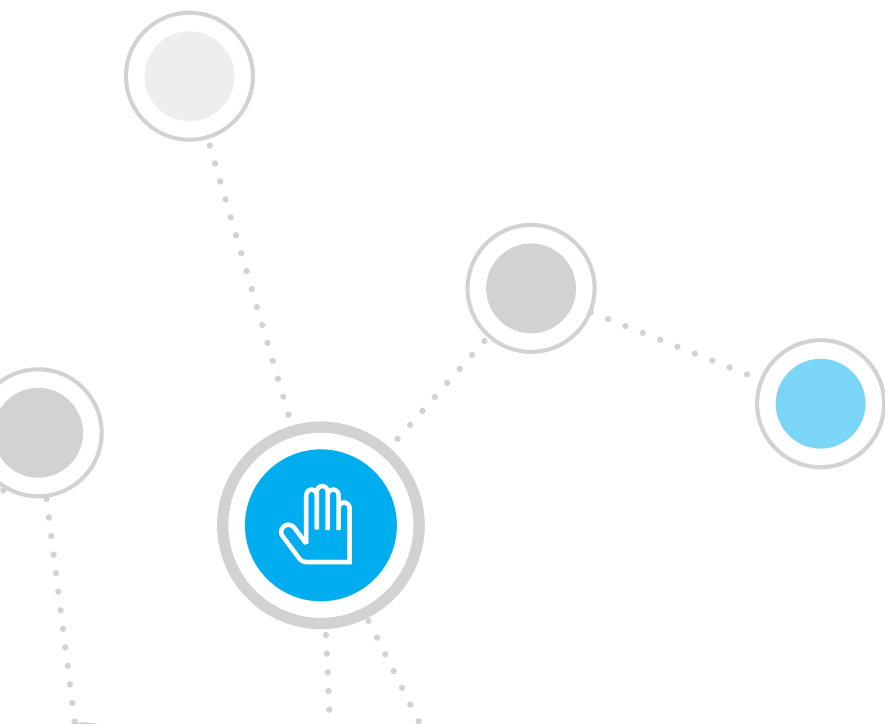




FORESCOUT

White Paper

The Fast Track to SANS Security: Implementing Critical Security Controls with ForeScout.



The Case for Standardized Security Controls

Organizations are struggling to more effectively secure their IT environments amid a torrent of cyberattacks and technical disruptions. Distributed, cloud-based hosting environments are making defensible perimeters a quaint anachronism. New mobile endpoints and the Internet of Things (IoT) continually extend the attack surface. Conventional security solutions are isolated in silos, and threat innovation accelerates powered by the profits of theft and blackmail.

In response, IT organizations are increasingly adopting security frameworks that prescribe and prioritize core sets of essential controls. A leading example is the Center for Internet Security's (CIS) Critical Security Controls (CSCs), a recommended set of actions for cybersecurity that provide specific ways to thwart the most common attacks.

The CSCs help organizations rapidly define the starting point for their defenses, direct scarce resources to actions with immediate and high-value payoff, then focus their attention on additional risk issues unique to their business. The first five controls are considered foundational cyber hygiene—basic things that every organization should do to create a strong defensive foundation. The remaining 15 controls address actions that should be prioritized based on an organization's environment and operations.

Because the CSCs derive from the most common attack patterns and are vetted across a very broad community of government and industry, they provide a practical basis for immediate high-value action.

The SANS Institute Advises: Simplify CSC Implementation with Endpoint Visibility and Control

While the CSCs are technology-agnostic, many observers have noted their frequent reference to endpoint visibility and control capabilities, and the contribution of security solutions that provide such functionality in expediting CSC implementation. Analysts at the SANS Institute specifically cite¹ the ability to automatically secure network resources from compromised endpoints as a common requirement of many controls.

¹ <https://www.sans.org/reading-room/whitepapers/access/protect-network-endpoint-critical-security-controls-37202>

The ForeScout Solution: Agentless Visibility, Control and Orchestration

ForeScout lets your IT organization see devices on your network, including non-traditional devices, the instant they connect. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among your existing security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout requires no installed software agents or previous device knowledge.

The ForeScout solution includes two components:

- **ForeScout CounterACT**, an agentless security appliance (physical or virtual) that dynamically identifies and evaluates network endpoints and applications the instant they connect to your network. CounterACT quickly determines the user, owner and operating system, as well as device configuration, software, services, patch state and the presence of security agents, then it provides remediation, control and continuous monitoring of these devices.
- **ForeScout Base and Extended Modules** leverage the capabilities of the ForeScout ControlFabric* Architecture to provide CounterACT with unprecedented interoperability, integration and multivendor security orchestration capabilities. Modules support more than 70 third-party solutions*.

This paper examines in detail how ForeScout solutions can simplify and expedite a successful CSC implementation.

CSC 1: Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

How ForeScout helps make it happen

Real-time asset intelligence collection - As devices connect to your network, CounterACT collects a very broad range of asset data as a basis for granting or denying access. These data include:

- The type of device, including its 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, VoIP phone, security or manufacturing system, medical or point-of-sale device
- The identity of the connecting user, allowing you to distinguish between employee, partner, contractor and guest devices
- Whether the device is owned by the organization or the user
- Where the device is connecting, and the connection type (wired, wireless, virtual private network)

 Who are you?	 Who owns your device?	 What type of device?	 Where/how are you connecting?	 What is the device hygiene?
<ul style="list-style-type: none"> • Employee • Partner • Contractor • Guest 	<ul style="list-style-type: none"> • Corporate • BYOD • Rogue 	<ul style="list-style-type: none"> • Windows, Mac • iOS, Android • VM • Non-user devices, IoT 	<ul style="list-style-type: none"> • Switch/Port/PoE • Wireless/Controller • VPN • IP, MAC • VLAN 	<ul style="list-style-type: none"> • Configuration • Software • Services • Patches • Security Agent

- The device's IP address, MAC address, switch port, SSID and VLAN

Figure 1: Device data acquired by CounterACT.

Comprehensive asset data integration - These data are assembled through an unusually broad array of acquisition methods, including:

- Polling tables in switches, access points and controllers for a list of connected devices
- Registering to receive SNMP traps from switching and wireless infrastructure whenever a device connects
- Monitoring 802.1X requests coming into CounterACT's built-in RADIUS server or an external instance
- Monitoring DHCP requests to detect when a new device requests an IP address
- Monitoring network traffic via SPAN ports to glean information from banners, HTTP and other traffic
- Conducting NMAP scans for additional information on operating systems, services, processes, applications, etc. running on an endpoint
- Using domain credentials to actively inspect and interrogate endpoints
- Analyzing NetFlow data to discover IP addresses not captured otherwise and performing passive fingerprinting
- Importing external customer data such as a set of MAC addresses maintained in an FTP server or an LDAP server
- Using our optional SecureConnector to inspect and interrogate certain types of mobile and personally-owned devices

This asset information is compiled and correlated to provide the basis for automated access provisioning, allowing CounterACT to grant, deny or restrict a device's access to network resources according to device state and security policy.

CSC 2: Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

How ForeScout helps make it happen

Comprehensive software discovery and assessment – When CounterACT inspects a device, it creates an inventory of software that is installed and running on the system. It then compares that inventory to a whitelist of approved software versions or a blacklist of prohibited ones, and approves, denies or restricts access based on the result. This evaluation can also generate alerts, repair tickets and reports, and initiate remediation actions. CounterACT can also tie into third-party systems for software lifecycle management.

Applications	Operating System	Security Agents
Installed	OS Type	Anti-malware/DLP agents
Running	Version number	Patch management agents
Version number	Patch level	Encryption agents
Registry settings	Services and processes installed or running	Firewall status
File sizes	Registry	Configuration
	File names, dates, sizes	

Figure 2: Types of device software data acquired by CounterACT.

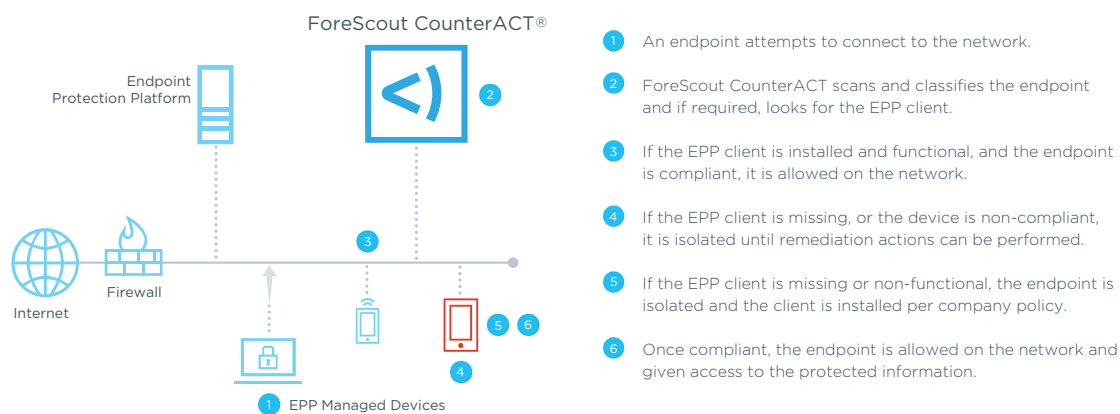


Figure 3: CounterACT initiating agent re-installation on a managed device.

For example, if CounterACT's endpoint scan identifies a managed device, but finds the required endpoint protection platform (EPP) client is missing or inoperative, it can restrict the device's network access and notify the EPP system to restart or reinstall the client. When the remediation is complete, ForeScout restores authorized access.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement and actively manage (track, report on and correct) 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.

How ForeScout helps make it happen

Automated, policy-based device control – Once 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. Minor violations might result in a warning message sent to the end-user. Employees and contractors who bring their own devices can be redirected to an automated onboarding portal. Serious violations could result in actions such as blocking or quarantining the device. For CounterACT-managed devices, policies can be built that can set certain security configuration.

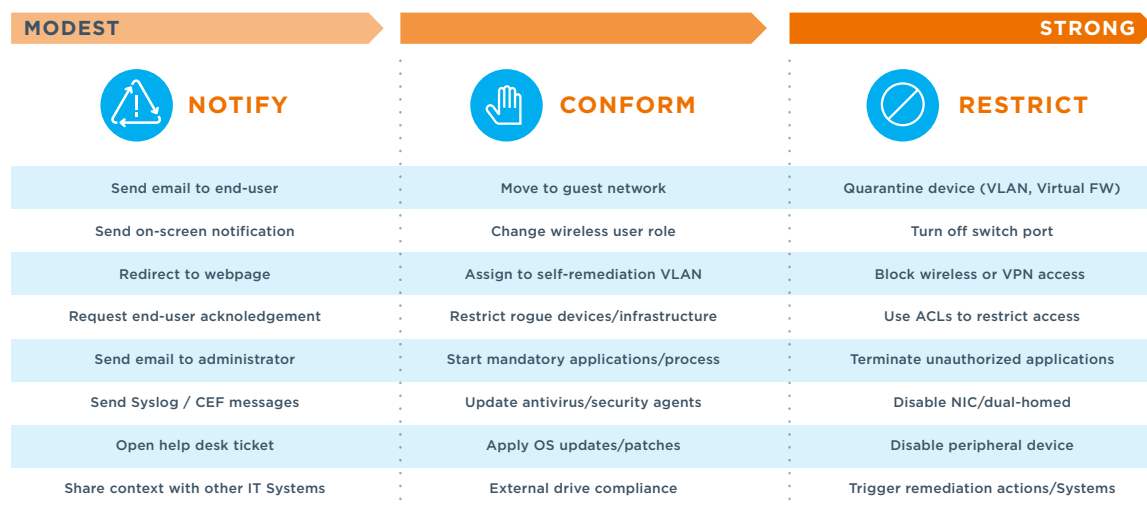


Figure 4: Types of device control actions available in CounterACT.

Monitor and manage existing security agents – One of CounterACT’s strengths is its ability to help ensure that your existing agent-based security controls are working. It can install, update, restart and reconfigure various security and management agents such as malware detection, encryption, firewall, DLP and patch management to increase the effectiveness of your existing tools. ForeScout Extended Modules allow tight orchestration of security workflows and processes between CounterACT and third-party security solutions.

CSC 4: Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate and minimize the window of opportunity for attackers.

How ForeScout helps make it happen

Granular access policies - CounterACT's enforcement policies can be tuned based on device, user, resource request and configuration or host-based protection violation scenarios.




 User Communications	 Applications/OS	 Security Agents	 Peripherals	 Network Action
<ul style="list-style-type: none"> • Self-remediation <ul style="list-style-type: none"> - Send email - Send to web page - Communicate policies • Open help desk ticket 	<ul style="list-style-type: none"> • Update application • Configure Registry • Start required application • Stop blacklisted or legacy application • Trigger external remediation system 	<ul style="list-style-type: none"> • Install agent • Start agent • Update agent • Update configuration • Trigger external remediation service 	<ul style="list-style-type: none"> • Alert administrator • Alert user about non-compliance • Disable peripheral • Disable USB ports 	<ul style="list-style-type: none"> • VLAN Assignment • ACL Assignment • Virtual Firewall • Switch port block • WLAN role

Figure 5: Some of the risk mitigation and remediation actions available in CounterACT.

Blocking and remediating vulnerable devices - CounterACT can identify, remediate, block or isolate vulnerable and compromised nodes. It can also initiate an immediate vulnerability assessment (VA) of new network devices using its own scanning capabilities or those of a partner solution such as Qualys, Tenable or Rapid7.

If the scan finds that the operating system or key applications are missing critical patches, ForeScout can trigger an update by the patch management system. When repairs are complete, CounterACT can restore authorized access. This bi-directional exchange of the device's status and policy-based automation of remediation procedures occurs without the need for manual intervention.

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

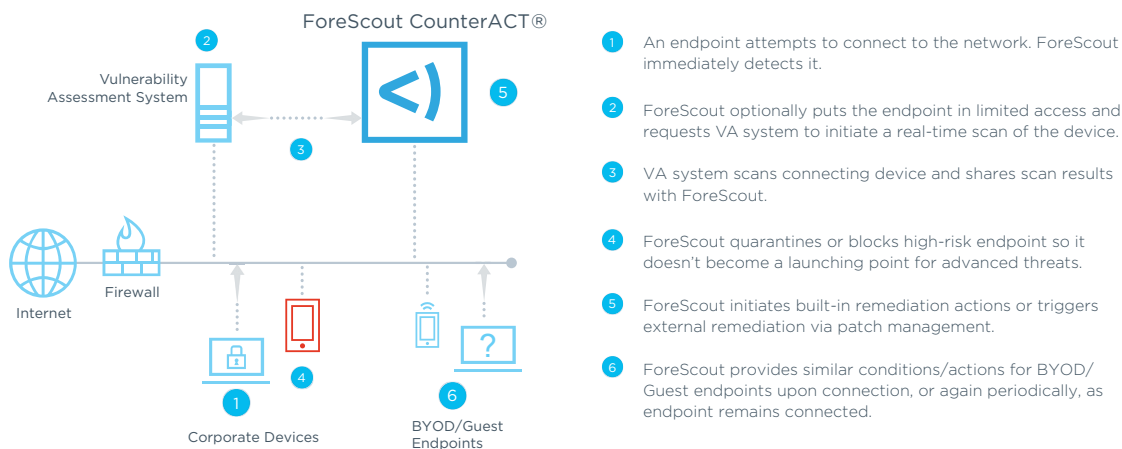


Figure 6: Triggering a vulnerability assessment and software patch update through multivendor orchestration.

CSC-5: Controlled Use of Administrative Privileges

The processes and tools used to track, control, prevent and correct the use, assignment and configuration of administrative privileges on computers, networks and applications.

How ForeScout helps make it happen

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

CSC 6: Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage and analyze audit logs of events that could help detect, understand or recover from an attack.

How ForeScout helps make it happen

Endpoint logging policy enforcement – If security event logging is part of an organization’s endpoint policy, CounterACT can support enforcement. When a device requests network access, ForeScout’s initial inspection can determine whether logging is enabled and how it is configured, including the chosen location for log storage. If the device is non-compliant, CounterACT can deny access or quarantine it for remediation.

CSC 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

How ForeScout helps make it happen

Client configuration policy enforcement – When a device requests a network connection, CounterACT's inventory and security assessment identifies each browser and email client installed on the device and checks its security configuration. Depending on your policy, this scan can include application version, patch status, scripting languages enabled and other potential vulnerabilities. If CounterACT finds an application out of compliance, it can deny or restrict access, or terminate the app. It can also trigger a vulnerability scan or patch update.

CSC 8: Malware Defenses

Control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective action.

How ForeScout helps make it happen

Anti-malware policy enforcement – CounterACT helps ensure that host-based antimalware defenses are installed, up-to-date, correctly configured and operational. It can verify the presence and status of antivirus, antispymware, personal firewall and intrusion prevention tools. It can check key device settings to see that content from external devices won't run automatically, such as data execution prevention and address space layout randomization. Non-compliant devices can be denied access or isolated on a secure network segment for remediation.

Integration with network-based threat detection solutions – ForeScout Extended Modules bring the visibility, control and enforcement capabilities of CounterACT to third-party security solutions, including leading advanced threat detection (ATD) platforms. When notified of an infected endpoint by a network-based ATD solution, CounterACT can immediately quarantine that device and initiate a managed remediation using threat details provided by the ATD system. When repairs are complete, CounterACT can restore appropriate access and scan other endpoints for the same compromise indicators.

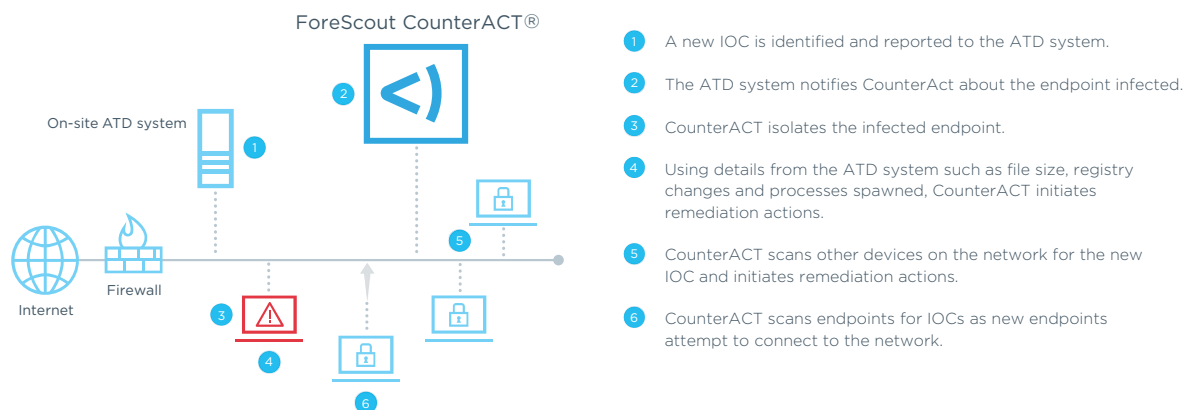


Figure 7: CounterACT integration with network-based advanced threat defenses.

CSC 9: Limitation and Control of Network Ports, Protocols and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability available to attackers.

How ForeScout helps make it happen

Device configuration policy enforcement – CounterACT can identify open ports, active protocols and running services, and compare that inventory with configuration policy for that host. It can deny or restrict access for non-compliant devices and issue a user notification or remediation alert.

CSC 10: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

How ForeScout helps make it happen

Endpoint data protection confirmation – If host-based backup protection is part of your endpoint security strategy, CounterACT can help make sure your chosen 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.

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers and Switches

Establish, implement and actively manage (track, report on and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

How ForeScout helps make it happen

Network configuration policy enforcement - Just as CounterACT scans connecting endpoints to assess their configuration and inventory installed services, it can also conduct similar evaluations of network devices and network-based security infrastructure. Heterogeneous support allows CounterACT to interrogate firewalls, servers, switches and routers—even in mixed environments that include switches from multiple vendors. It can alert on non-compliant devices and quarantine them for remediation.

CSC 12: Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

How ForeScout helps make it happen

Broad integration with third-party security solutions - CounterACT works with many third-party security systems such as SIEMs, advance threat detection systems and endpoint protection platforms. When CounterACT receives a threat message from these systems, based on policy and threat severity, CounterACT can limit the network access of that device. CounterACT also has detection capability for malicious network activities.

Enforcing remote device and connection security - When a remote device requests a network connection, CounterACT's initial scan can identify the type of connection and deny or restrict access if the endpoint posture is compromised. At the same time, it can evaluate the device configuration, installed software and patch levels for compliance with security policy.

Enforcing unmanaged device security - CounterACT can also help defend the local perimeter against improper access or inadvertent threat transfer by contractors and partners. Third-party devices can be automatically assessed for configuration and security posture as they request network access, and access can be granted, denied or restricted based on the results.

CSC 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

How ForeScout helps make it happen

Enforcing data security software policy - If host-based data loss prevention (DLP) software is part of your standard endpoint configuration, CounterACT can help ensure compliance. When a device requests access to the network, CounterACT's inspection scan can confirm that the proper application is installed, patched and functional. Scheduled scans can monitor the device population and improperly configured devices can be quarantined or removed from the network for remediation.

CSC 14: Controlled Access Based on Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (for example, information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

How ForeScout helps make it happen

CounterACT provides capabilities that are essential in managing user access to networks that have been segmented to protect resources of varying sensitivity. Its initial device scan automatically determines user identity, and it integrates with multiple sources of user authorization. These features help ensure that corporate and employee-owned devices get appropriate network access. They also facilitate automated on-boarding processes that greatly enhance security while eliminating manual administration. Examples of CounterACT controlled access include:

- **Dynamic assignment to network segments** - Employees can be dynamically assigned to VLANs that are appropriate for their roles. An example of this would be allowing only network administrators to access the networking infrastructure.
- **Automated bring your own device (BYOD) onboarding** - When an employee tries to access enterprise resources with a personal device, CounterACT can automatically identify the device, assess its configuration and security state, authenticate the user and grant the appropriate level of access.
- **Flexible guest access automation** - CounterACT can automatically register guest users via wireless hot spots and self-serve or sponsor portals. The guest's device is assessed for security issues and access is granted based on the rights requested by the internal sponsor. Access can be limited by various means, including time-of-day controls, connection type and device-specific restrictions.

CSC 15: Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points and wireless client systems.

How ForeScout helps make it happen

Wireless endpoint compliance - CounterACT can help ensure that wireless user devices are compliant right down to the wireless client, with correct security configurations, documented users, no unauthorized peer-to-peer (P2P) apps or peripheral networks enabled, and access granted only as appropriate for the device state and user authorization.

Wireless infrastructure inventory and rogue device detection - CounterACT can inventory and evaluate wireless network devices, validating that authorized network components are correctly configured and that rogue access points with wired network infrastructure connections are discovered.

CSC 16: Account Monitoring and Control

Actively manage the life cycle of system and application accounts — their creation, use, dormancy and deletion — in order to minimize opportunities for attackers to leverage them.

How ForeScout helps make it happen

Managing session duration - CounterACT supports guest and contractor network access in which time durations for expiration of their user credentials can be set. CounterACT can also verify screen locks on systems meet company policies.

CSC 19: Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (for example, plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence and restoring the integrity of the network and systems.

How ForeScout helps make it happen

Track endpoint state for forensic reference - In the event of an incident, responders will 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 the other management and security technologies in your environment.

Streamline Your CSC Build-Out with ForeScout

Automated endpoint visibility and control is a consistent theme in the Critical Security Controls. Without the ability to see and manage the diverse and growing population of devices that access your network resources, securing them is impossible. ForeScout solutions for agentless network visibility and control give you those capabilities, providing many CSC requirements out of the box.

To learn more about how ForeScout solutions can speed and simplify CSC implementation in your environment, come to www.forescout.com and request a no-strings solution demonstration.

Acronym Glossary:

Dynamic Host Configuration Protocol (DHCP)

File Transfer Protocol (FTP)

HyperText Transfer Protocol (HTTP)

Internet Protocol (IP)

Lightweight Directory Access Protocol (LDAP)

Media Access Control (MAC) address

Network Mapper (Nmap)

Remote Authentication Dial-In User Service (RADIUS)

Service Set Identifier (SSID)

Simple Network Management Protocol (SNMP)

Switch Port Analyzer (SPAN)

Virtual Local Area Network (VLAN)

Voice over Internet Protocol (VoIP)

Learn more at
www.ForeScout.com



FORESCOUT

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

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

About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of January 2016, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions.

*As of January 2016

© 2019 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners. **Version 01_19**