FORESCOUT

CIS Critical Security Controls Forescout IT-OT Converged Value

CIS Critical Controls (CSC) v7		
Basic 6		
Control #	Description	Forescout IT-OT Converged Value
1 **Inventory and Control of Hardware Assets**	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.	**Real-time asset intelligence collection:** Forescout is the leader in device visibility and control. The company offers a unified IT-OT platform that performs a thorough inventory of device information across the extended enterprise network, including campus, data center, cloud, OT and IoT environments. Forescout 8.1 includes expanded coverage to identify more than 500 OS versions and over 5,000 device vendors and models. **Access control:** Automated access provisioning allows the Forescout platform to grant, deny or restrict a device's access to network resources according to device state and security policy. **Passive technology and extensive classification for OT networks:** Thorough device inventory using our patented deep packet inspection technology and other non-intrusive methods reduces operational disruption. New deep packet inspection of over 100 IT and OT protocols to auto-classify thousands of industrial automation devices across manufacturing, energy, oil and gas, utilities, mining and critical infrastructure. **Medical IoT classification:** Healthcare device classification for over 350 medical technology vendors, including the Global Top 20. **Multi-factor risk scoring:** Prioritize mitigation actions for high-risk misconfigured, vulnerable or non-compliant devices.
2 **Inventory and Control of Software Assets**	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.	**IT software inventory:** When the Forescout platform 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. The Forescout platform can also integrate with third-party systems for software lifecycle management. **OT networks:** Selective scanning technology, specifically for OT, can track Windows patches and applications on the OT network.

CIS Critical Controls (CSC) v7		
Basic 6		
Control #	Description	Forescout IT-OT Converged Value
3 **Continuous Vulnerability Management**	Continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate and minimize the window of opportunity for attackers.	**Forescout 8.1 adds OT and ICS vulnerability assessment to existing Windows vulnerability assessment capabilities, providing insight into the high-risk devices on your network.** **Blocking and remediating vulnerable devices:** The Forescout platform can identify, remediate, block or isolate vulnerable/compromised devices. It can initiate an immediate vulnerability assessment of new network devices using its own scanning capabilities or those of a partner solution such as Qualys, Tenable or Rapid7. If a device is missing a critical patch, the Forescout platform can trigger an update by the patch management system. After remediating the device, the Forescout platform can restore authorized access. **Extensive OT vulnerability capabilities:** The Forescout platform continuously assesses industrial control system (ICS) device vulnerabilities in our Common Vulnerabilities and Exposures (CVE) database and can provide continuous vulnerability updates. Our industrial threat library (ITL) has 2,100+ ICS-specific behavioral checks and 3,000+ indicators of compromise (IOCs} to identify network and system level vulnerabilities.
4 **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.	**Automated user and privilege validation:** For managed devices, the Forescout platform 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, the Forescout platform can deny or restrict access. It can track both IT and OT network logins to monitor the behavior of employees, maintenance users and other third parties.

CIS Critical Controls (CSC) v7		
Basic 6		
Control #	Description	Forescout IT-OT Converged Value
5 **Secure Configuration of 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.	Effective configuration management requires detailed information on all IT, IoT and OT devices. The Forescout platform tracks numerous configuration elements of IT and ICS devices such as vendor, firmware, modules, host versions, patches and applications. **Automated, policy-based device control:** Once the platform 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. **Monitor and manage existing security agents:** One of Forescout's strengths is its platform's 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, data loss prevention (DLP) and patch management to increase the effectiveness of your existing tools. Forescout's eyeExtend products allow tight orchestration of security workflows and processes between Forescout and third-party security solutions.
6 **Maintenance Monitoring & Analysis of Audit Logs**	Collect, manage and analyze audit logs of events that could help detect, understand or recover from an attack.	**Endpoint logging policy enforcement:** If security event logging is part of an organization's endpoint policy, the Forescout platform can support enforcement. When a device requests network access, the platform'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 noncompliant, the Forescout solution can deny access or quarantine it for remediation.

CIS Critical Controls (CSC) v7		
Foundational		
Control #	Description	Forescout IT-OT Converged Value
7 **Email and Web Browser Protections**	Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.	**Client configuration policy enforcement:** When a device requests a network connection, Forescout's inventory and security assessment capabilities identify each browser and email client installed on the device and check its security configuration. Depending on your policy, this scan can include application version, patch status, scripting languages enabled and other potential vulnerabilities. When the Forescout platform finds an application that's out of compliance, it can deny or restrict access, or terminate the app. It can also trigger a vulnerability scan or patch update. On an ICS network, Forescout can monitor vulnerable protocols such as HTTP.
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.	**Malware defense in the OT environment:** Our protocol checks are a first line of defense against malware, as malware often exploits protocol vulnerabilities to spread. Forescout's industrial threat library (ITL) also has built-in checks to detect malware upon deployment. A learned ICS network communication model provides a basis for anomaly detection, and our continuous OT network monitoring uses this to detect threats and deliver alerts to a central management platform in real time. We release scripts when needed to detect specific indicators or behaviors and support centralized updates and distribution of selected threat intel and indicators of compromise in Structured Threat Information eXpression (STIX) format to help guarantee timely updates of available malware indicators. After ingestion of new threat intel or IOCs, our forensic time machine allows users to search network logs to determine if these new IOCs were seen on the ICS network in the past. Our solution also provides seamless integration with malware analysis facilities and security workflows. **Antimalware policy enforcement for desktops:** The Forescout platform 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, antispyware, 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. Noncompliant devices can be denied access or isolated on a secure network segment for remediation. **Network-based threat detection solutions:** The Forescout platform brings the visibility, control and enforcement capabilities of Forescout to third-party security solutions, including leading advanced threat detection (ATD) platforms. When notified of an infected endpoint by a network-based ATD solution, the Forescout platform can immediately quarantine that device and initiate a managed remediation using threat details provided by the ATD system. When repairs are complete, the Forescout solution can restore appropriate access and scan other endpoints for the same compromise indicators. **Threat Intelligence Ingestion:** Automated threat intelligence ingestion provides rapid and continuous protection against cyberthreats. This function allows users of the Forescout OT solution to continuously adapt and modernize their security posture against malware, as well as other cyberthreats. **Contextual analysis and correlation of alerts:** This capability manages and prioritizes known threats and alerts for users to quickly evaluate and correlate with other alerts elsewhere in the network.

CIS Critical Controls (CSC) v7		
Foundational		
Control #	Description	Forescout IT-OT Converged Value
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.	The Forescout platform has a broad arsenal of tools to detect and manage inappropriate use of ports and services on networked devices. **Define and enforce your policy:** On an ICS network, the Forescout platform can create both network and protocol baselines to help ensure all communications happening within the control system are known and approved. If a communication or protocol message is outside of approved baselines, an alert and packet capture (PCAP) are immediately created for fast detection, response and recovery. On an IT network, the Forescout platform 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 noncompliant devices and issue a user notification or remediation alert. **Out-of-the-box MAC spoofing detection:** The Forescout platform's new patent-pending rogue device detection can identify and stop impersonators using MAC address spoofing techniques. **Deep packet inspection:** These capabilities allow control at syntax level (packets) and semantic level (anomaly detection and ITL). The Forescout platform tracks usage of ports and protocols and changes and keeps a complete network change log. In addition, our active component for OT can scan selected hosts for all open ports. Our Industrial Threat Library (ITL) features more than 2,100+ behavioral-based indicators highlighting specific ICS threats and anomalies. The ITL indicators include both cyber and operational threats and anomalies to provide additional business value.
10 Data Recovery Capabilities	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	**Endpoint data protection confirmation:** If host-based backup protection is part of your endpoint security strategy, the Forescout platform can help ensure your chosen software is installed, correctly configured and operational. Connecting devices can be evaluated as part of the platform's access inspection, and non-conforming hosts can be quarantined or removed from the network until repaired.
11 Secure Configuration of 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.	**Network configuration policy enforcement:** In addition to scanning connecting endpoints to assess their configuration and inventory installed services, the Forescout platform can also conduct similar evaluations of network devices and network-based security infrastructure. Heterogeneous support allows the Forescout solution to interrogate firewalls, servers, switches and routers—even in mixed environments that include switches from multiple vendors. It can alert on noncompliant devices and quarantine them for remediation.

CIS Critical Controls (CSC) v7		
Foundational		
Control #	Description	Forescout IT-OT Converged Value
12 **Boundary Defense**	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	Forescout's learned communication model allows you to analyze cross-network flows and detect anomalies in communications. Interactive network maps provide visualization of network communication and flows. Automatic role assignment also helps to control information flows. **Enforcing remote device and connection security:** When a remote device requests a network connection, the Forescout platform'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:** The Forescout platform 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.
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.	Forescout helps to secure sensitive information by analyzing communication flows and looking for specific data exfiltration techniques such as DNS tunneling. The platform can help ensure that host-based DLP software is properly installed, patched and functional. Improperly configured devices can be quarantined or removed for remediation.
14 **Controlled Access Based on the 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.	Forescout provides capabilities that are essential in managing user access to networks that have been segmented to protect resources of varying sensitivity. the Forescout platform's initial device scan automatically determines user identity. On an ICS network, the platform can track network logins to monitor behavior. It can implement a complete role-based access control system which can be integrated with the organization's LDAP/Active Directory so that every user has identity, accountability and access to only the resources they need. 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 Forescout 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 onboarding:** When an employee tries to access enterprise resources with a personal device, the Forescout platform 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:** The Forescout platform 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. **Monitor for dangerous activities on an ICS network:** User activity such as restart, firmware updates and writes can be tracked to send alerts and reduce downtime.

CIS Critical Controls (CSC) v7		
Foundational		
Control #	**Description**	**Forescout IT-OT Converged Value**
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.	**Wireless endpoint compliance:** The Forescout platform can help ensure that wireless user devices are compliant right down to the wireless client. Compliance checks validate correct security configurations and documented users, detect unauthorized peer-to-peer (P2P) apps or enabled peripheral networks, and confirm that access is granted only as appropriate for the device state and user authorization. **Wireless infrastructure inventory and rogue device detection:** The Forescout platform 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.
16 Account Monitoring and Control	Actively manage the lifecycle of system and application accounts — their creation, use, dormancy and deletion — in order to minimize opportunities for attackers to leverage them.	**Managing session duration:** The Forescout platform supports guest and contractor network access in which time durations for expiration of their user credentials can be set. It can also verify screen locks on systems meet company policies. Forescout 8.1 includes new capabilities such as visibility into Cisco ACI, Microsoft Azure and Belden industrial switching environments, extending coverage across data center, cloud and OT networks to provide organizations the line of sight they need across IT and OT domains. Multi-cloud visibility now includes Microsoft Azure, adding to existing capabilities for AWS and VMware.
Organizational		
19 Incident Response & 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.	The Forescout platform helps you define an effective incident response program. It provides a visual map of the network that can be used during an incident to visualize the threat and its spread through the network, allowing rapid threat containment. **Packet capture for forensics:** Alerts provide rich contextual information about the source, nature and target of a threat, along with detailed packet capture related to the threat. **Track endpoint state for forensic reference:** In the event of an incident, 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 the Forescout platform builds through its own device inspections and through its integrations with the other management and security technologies in your environment. **Extended capabilities:** Responders benefit from an API to perform threat hunting and quickly search the network for advanced threat indicators. Contextual alert information can be forwarded to SIEMs and/or correlation engines to initiate appropriate response plans or actions, and the network and protocol baselines generated can be used in a recovery situation to help ensure devices and applications are once again operating as expected. Forescout 8.1 now integrates with ServiceNow ITSM and Security Operations products to automate and accelerate incident response.

* Control #'s 17, 18, and 20 are not applicable for 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