How Forescout Enables and Accelerates Alignment with TSA SD 2021-02

In July 2021, the Transportation Security Administration (TSA) released their second Security Directive (TSA SD 2021-02) which required pipeline owners and operators to implement cybersecurity practices to prevent operational disruption or system degradation. These rules are valid for one year or until July 26, 2022.

The Forescout platform provides, validates, or supports many of the capabilities required by TSA SD 2021-02, including:

SECTION	MEASURE	FORESCOUT CAPABILITIES	CONTROL TYPE
II.B.2.a	Apply multi factor authentication for non-service account.	The Forescout platform helps to ensure only approved accounts are configured in the local admin group and Remote access group of Windows machines (i.e., ensure no service accounts in local admin groups) and MFA is applied.	Supports
II.B.2.b.i	Identifying information and Operational Technology network inter-dependencies.	The Forescout platform passively models network communications to identify OT/IT/IOT inter-dependencies which are displayed in the form of a network map. A dedicated “threat scenario” can be simulated to identify whether there is undesired connectivity among network segments. In addition, it is possible to create self-learning anomaly detection profiles that first model normal network communications, and successively alerts if violations occur. Additionally, the Forescout platform provides a policy overlay and visualization tool of the traffic between assets including IT and OT. Data is ingested via netflow, SPAN, network taps or by integrating with the eyeInspect Command Center. Network communications and inter-dependencies can be visualized at the IP-to-IP level, as well as based on any attribute of a device (e.g., which device types communicate to which device types, which segments communicate to which segments, etc.).	Provides
II.B.2.b.ii	Implementing and maintaining capability for network physical and logical segmentation between Information and the Operational Technology systems sufficient to ensure the OT system can continue to operate even if the IT system is taken offline because it has been compromised.	The Forescout platform helps to ensure OT assets are NOT directly connected to the IT side (i.e., Dual Homed PCs in OT connecting directly to IT side bypassing firewall).	Validates

SECTION	MEASURE	FORESCOUT CAPABILITIES	CONTROL TYPE
II.B.2.b.iii	Defining a demilitarized zone and using firewall rules, physical separation, and other tools to eliminate unrestricted communication between the IT and OT systems.	The Forescout platform can layer a policy on top of the traffic to know what an approved traffic baseline is and integrate with firewalls to automatically segment assets to ensure zones and conduits are maintained.	Provides
II.B.2.b.iv	Organizing Operational Technology systems assets into logical zones, such as isolating unrelated sub-processes, by taking into account criticality, consequence, and operational necessity.	The Forescout platform passively, dynamically, and automatically generates a network map based on the Purdue model. This network map has filtering functionality which includes but is not limited to filtering specific network segments and/or user-defined sub-processes.	Provides
II.B.2.b.v	Monitoring and filtering traffic between networks of different trust levels, such as between the IT and the OT system, by defining appropriate communication conduits between the logical zones and deploying security controls to monitor and filter network traffic and communications between logical zones.	The Forescout platform can layer a policy on top of the traffic to know what an approved traffic baseline is and integrate with firewalls to automatically segment assets to ensure zones and conduits are maintained.	Provides
II.B.2.b.vi	Prohibiting OT system protocols from traversing the IT system unless expressly through an encrypted point-to-point tunnel.	The Forescout platform identifies intra-zone traffic within OT levels, OT communication protocols that traverse boundaries to the IT side, and any communication outside of approved policies to alert or block such traffic.	Validates
II.B.2.b.vii	Developing workarounds or manual controls to ensure industrial control system networks can be physically isolated when the IT system creates risk to the safe and reliable OT system processes.	NA	
II.B.2.c	Review and update log retention policies to ensure that they include policies and procedures for log management; include a secure log management infrastructure; and specify how long log data must be maintained, consistent with NIST standards.	The Forescout platform integrates directly with several market leading SIEM solutions, providing SYSLOG and CEF/LEEF/JSON formats. eyeInspect supports SYSLOG via UDP, TCP and TLS. • eyeInspect exports alerts flows, network event flows, and user activity flows • eyeInspect supports multiple parallel exporters • Logging is completely configurable from the user interface in terms of template and fields desired among the available fields. Additionally, the Forescout platform can send system, user, and policy action events to a central SIEM using syslog.	Supports
II.B.2.d.i	Identify malicious email traffic, spam and phishing emails an inhibit them from reaching end users.	NA	
II.B.2.d.ii	Prohibit ingress and egress of communications with known malicious IP addresses for IT systems and all OT systems with external connectivity.	The Forescout platform identifies known malicious IP addresses and leverages control capabilities for desired enforcement.	Provides
II.B.2.d.iii	Prevent users and devices from accessing malicious websites by implementing URL block lists and/or allow lists.	NA	
II.B.2.d.iv	Control access from the OT system to external internet access using an allow list.	The Forescout platform checks and establishes an approved behavior network pattern from OT environments to external Internet addresses (or any environment) and can alert or block if it is outside of approved policy rules.	Provides

SECTION	MEASURE	FORESCOUT CAPABILITIES	CONTROL TYPE
II.B.2.d.v	Investigate any communication between the OT system and an outside system that deviates from the identified baseline of communications and ensure it is necessary for operations.	The Forescout platform automatically learns and establishes rich contextual asset information, including but not limited to communication baselines while alerting, blocking or taking action if deviations are identified.	Provides
II.B.2.e	Set AV/anti-malware programs to conduct weekly scans, with on-access and on-demand scans, of IT and OT systems and other network assets using current signatures.	The Forescout platform helps to ensure AV is installed, running, and up to date on endpoints, including attempts at automatically starting or updating AV.	Validates
II.B.2.f.i	Implementing software analytics that allow Owner/Operators to rapidly determine which host sourced each DNS query.	The Forescout platform includes the ability to provide a variety network logs. Specific to DNS, Forescout parses DNS queries and responses and can provide which host sourced the query.	Provides
II.B.2.f.ii	Maintaining a current list of domains that are frequently visited or searched for by legitimate users within their systems that are not already included in commercially available top one million domain lists.	The Forescout platform logs attempted and successful name resolution requests within the monitored networks, by default keeping up to 30 days of history (configurable). This can be used to look up visited domains by network users, for awareness or forensic analysis. Furthermore, eyeInspect includes a database of known malicious IPs and domains, regularly updated, and alerts in real-time if a device attempts to connect to these IPs/domains. When the list of IPs and domains is updated, eyeInspect offers the options to automatically scan its log history and report if a newly learned malicious domain was used in the past, i.e., it supports retroactive analysis of malicious behavior and infections.	Supports
II.B.2.f.iii	Developing and/or updating policies and procedures requiring investigation of the reputation of the domains that are only rarely queried for and/or accessed by legitimate users within their organization, to determine if the communication with these domains carries an inappropriate level of risk to the organization.	The Forescout platform blacklisted domain database is updated regularly; additionally, rarely queried domain names can be investigated using the eyeInspect network baselining functionality.	Supports
II.B.2.g.i	For operating systems, applications, drivers, and firmware, on IT systems, software updates and patches must be tested and applied within a certain time of update and patch availability.	The Forescout platform provides an extensive list of software and versions installed on the endpoint. Easy to search and isolate unapproved versions. The Forescout platform verifies whether Microsoft patches are up to date or missing.	Supports
II.B.2.g.ii	For operating systems, applications, drivers, and firmware, on OT systems, software updates and patches must be tested within a specified timeframe of update and patch availability and implemented within a specified time frame of testing validation. Patches not implemented must be included on a cumulative list that includes operational and other risk-based considerations justifying the determination not apply the patch.	The Forescout platform includes firmware version information for OT devices, and maintains a host changelog, as well as asset baselining capability to easily report on devices which are out-of-compliance.	Supports
II.B.2.h.i	If using MS Office, fully disable macro use and user-based approval across the organization for MS Office products using Group Policy. Macros determined necessary for business functionality may be enabled on a case-by-case basis only after implementing additional host-based security controls and network monitoring.	The Forescout platform checks registry settings to help ensure the macro setting is disabled.	Validates
II.B.2.h.ii	Apply application allow-listing to IT and OT systems and then implement software restriction policies, or other controls providing the same security benefits, to prevent unauthorized programs from executing.	The Forescout platform provides an extensive list of software and versions installed. Policies could be written to identify endpoints with unapproved software.	Validates

SECTION	MEASURE	FORESCOUT CAPABILITIES	CONTROL TYPE
II.B.2.h.iii	If not already incorporated into the system-change management, update application allow-listing no less frequently than quarterly to remove applications no longer in use.	The Forescout platform can provide an extensive list of software and versions installed. This is easy to search and isolate unapproved versions.	Validates
II.B.2.h.iv	Monitor and/or block connections from known malicious command and control servers (such as Tor exit nodes, and other anonymization services) to IP addresses and ports for which external connections are not expected (such as ports other than VPN network gateways, mail ports, or web ports).	The Forescout platform maintains and regularly updates a database of known malicious IP addresses. Additionally, this list is fully customizable. Control can be initiated through the Forescout platform if desired.	Provides
II.B.2.h.v	Implement Security, Orchestration, Automation and Response as applicable. If the owner/operator determines these capabilities are not applicable, they must document which aspects of the system to not apply the capability and the justification for excluding these operations.	The Forescout platform can take control actions based on policy datapoints learned natively or through integrations with other tools. In addition, eyeExtend Connect can work with a 3rd party SOAR tool to take instructions from it to initiate control actions such as port block or VLAN change.	Supports
II.B.2.h.vi	Require implementation of signatures to detect and/or block connection from post-exploitation tools.	The Forescout platform maintains, and regularly updates a database of signatures for threat detection and can utilize the Forescout platform for enforcement. This list is fully customizable. Control would be initiated through the Forescout platform if desired.	Provides
II.C.1	Owner/Operator must develop and adopt a cyber contingency and response plan to reduce the risk of operational disruption.	The Forescout platform can block/segment infected endpoints like a kill-switch in the event of an emergency, giving control back to administrators to reduce the impact of the event and maintaining control from a central location without needing feet on the ground.	Supports

Control Type Description

Provides: provides information you provide directly to auditor or feeds data into an artifact

Validates: can be used to prove whether another control(s) is present and/or working

Supports: feeds info into another system or processes which serve the requirements

FORESCOUT
Active Defense for the Enterprise of Things™

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

Intl. + 1.408.213.3191
Support +1.708.237.6591