FORESCOUT

servicenow

Solution Brief

Absolute Asset Accountability and Security for Organizations Managing Industrial, Utilities and Critical Infrastructure Environments

Leverage Forescout and ServiceNow integration to streamline asset, risk and incident management.

Over

40%

of organizations are moving toward centralized OT security, either with increasing reliance on their IT infrastructure or an industrial SOC.[1]

Increased connectivity of industrial control systems (ICS) and operational technology (OT) networks has driven new efficiency gains in production, logistics, transportation and energy. However, with new connectivity comes new risk. Any connected device not continuously managed can represent a threat vector where cyber criminals and malware can infiltrate the network, having the potential to result in severe damage in environments where seconds of downtime can equal high dollars in losses or other perils. Both OT and IT cyber and risk stakeholders are trending toward a convergence model to address this reality and the challenges that come with it.

Challenges

These are some of the major challenges facing cyber and risk stakeholders today:

- Achieving and maintaining a detailed and accurate asset inventory
- Maintaining and enforcing regulatory and device compliance
- Identifying and containing compromised, unauthorized or blacklisted devices
- Detecting and rapidly remediating both cyber and operational risk
- Automating cybersecurity processes and incident response

Organizations cannot just rely on scheduled maintenance programs and procedures to ensure all connected devices are compliant and secure to prevent a cyberattack or regulatory fines. The goal is to continuously maintain asset accuracy, assess and respond to risk and enforce critical policies across all connected devices, regardless of where on the network. This can be particularly challenging for ICS/OT environments where downtime is too costly and most devices cannot accommodate a management agent.

The Solution: Forescout and ServiceNow Orchestration

Forescout, ServiceNow and their integration enables asset accountability and cybersecurity protection at enterprise-scale without compromising operational performance for mission-critical applications and processes.

Forescout provides continuous discovery, classification and rich contextual intelligence for all connected devices across your OT and IT networks. Additionally, Forescout offers network communication pattern insight among logical zones across your entire extended enterprise infrastructure. With this valuable insight and the ability to simulate new segmentation policies, you can fine-tune policies to drastically reduce your potential cyberattack surface and help ensure no undesirable communications exist across both OT and IT environments. Forescout also provides deep industrial asset insight and extensive threat monitoring to proactively combat OT risk. The Forescout solution leverages its real-time device and threat insight to automatically respond to threats, enforce device configurations and apply network access and segmentation policies with context-aware network and system actions that preserve operational uptime.

The ServiceNow® platform's configuration management database (CMDB) provides a single system of record that is the source data for ServiceNow's comprehensive asset, operations, service and security management solutions. With the CMDB, you can build logical representations of assets, services and the relationships between them that comprise the entire infrastructure of your organization. The more context the CMDB contains, the more effective asset, service, compliance and security management decisions can be made.

Forescout offers pre-built integration with ServiceNow that enables orchestrated workflows and information sharing between Forescout and ServiceNow. Forescout continually assesses devices as they connect and when properties change. Forescout can then automatically update, or create new, ServiceNow CMDB Configuration Item (CI) records, per policy, with real-time device and network context. Forescout can also automatically create ServiceNow IT or Security incident records as well as immediately respond to the incident with policy-driven network or system actions. Data is synchronized across Forescout and ServiceNow platforms for complete audit tracking of operational and security incidents.

Key Benefits

- Increase efficiency and accuracy by automating CMDB updates with real-time contextual asset intelligence for all connected OT and IT devices
- Proactively mitigate risk of cyber and operational incidents
- Reduce analyst workload and mean time to resolution (MTTR) by automating incident creation, prioritization and alert aggregation while synchronizing asset and incident data
- Automate policy enforcement, incident response and remediation workflows with context-aware actions across disparate network domains and device types without disrupting operations

Highlights

- Reduce manual asset inventory overhead with automated ServiceNow CMDB updates for all OT and IT assets
- Provide rich contextual device and network information for SOC optimization
- Streamline incident detection, record creation and resolution while maintaining real-time CMDB asset and incident record accuracy throughout the process
- Continuously enforce configuration and security policies based on both device and business context
- Automate network access control, segmentation and threat response without negatively affecting operations
- Dynamically secure OT and IT environments while leveraging existing network infrastructure and staff

Continuously maintain accurate asset intelligence

Automatically true-up the ServiceNow CMDB and add rich device context for the entire connected OT and IT asset landscape, including IoT and ICS, wired and wireless campus, data center and cloud devices. Parse 130+ industrial protocols to discover and manage rich properties like firmware, model, serial number and nested devices. Use this data to streamline configuration and compliance management, plus reduce inventory audit costs and manual overhead. Maintaining continuous asset accuracy, including contextual details, increases compliance and reduces risk without operational disruption.

Apply dynamic segmentation without affecting operations

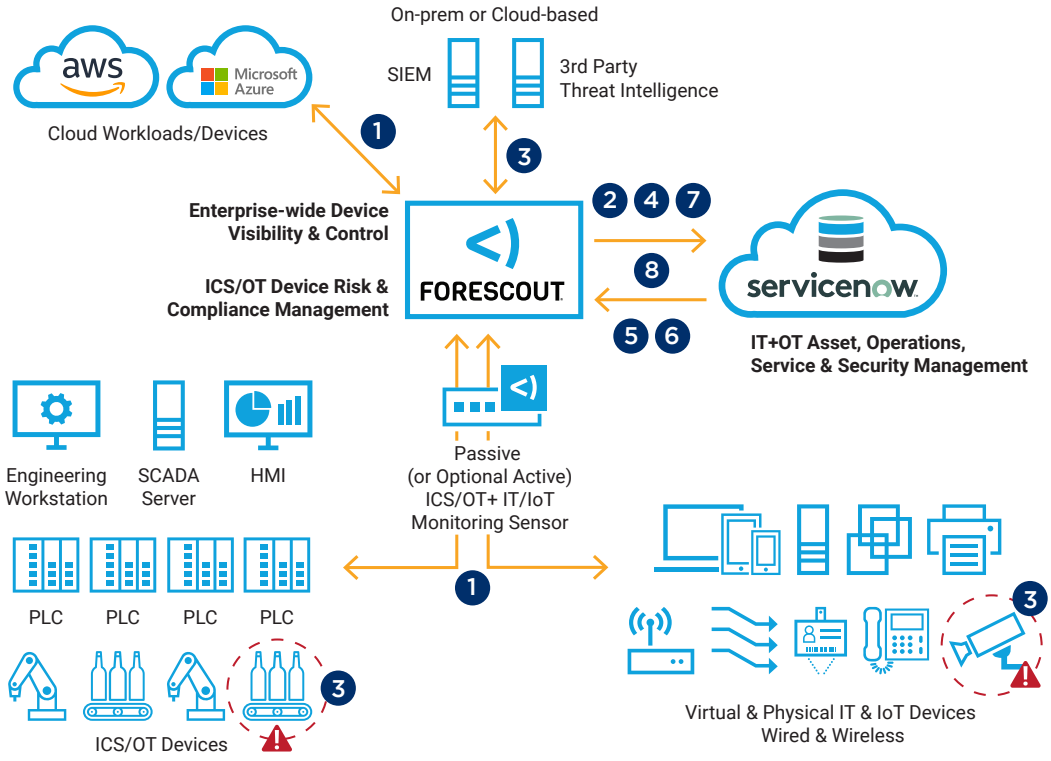
Leverage rich asset insight to optimize network security operations and heterogeneous network management by supporting common industrial scenarios, grouping assets by logical business applications, and visualizing the communication patterns among the logical asset groups to detect segmentation policy violations or concerns. Fine tune policies with simulation before implementation. Automatically control network access and enforce segmentation with context-aware, policy-driven network actions that maintain operational uptime. Cohesively enforcing network access and segmentation policies across heterogeneous networks dramatically reduces the cyberattack surface.

Automate incident detection, record creation, prioritization and response workflows

Automatically create ServiceNow IT Service or Security Incidents per policy. Trigger incident creation upon detection of device non-compliance or threats as determined by Forescout's device posture assessment, comprehensive OT threat library and/or other integrated third-party threat intelligence sources. Forescout can help Identify and prioritize industrial threats with impact-based risk scoring, including but not limited to:

- Failure of critical devices
- Unstable process values
- Incorrect process measurements
- Switch, firewall and device misconfiguration/noncompliance
- Malware and zero-day attacks
- Network vulnerabilities and CVEs
- Undesired network access and data flows

The Forescout platform can also automatically respond to ServiceNow incidents with context-aware, policy-driven actions to immediately contain threats or initiate remediation without affecting critical operations. Throughout the process, accurate information on the state of device properties is synchronized between Forescout and ServiceNow platforms.



Forescout-ServiceNow Workflows

1. Forescout continually discovers, classifies and assesses all connected devices.
2. Forescout automatically updates or creates a new ServiceNow CMDB CI record.
3. Upon assessment, if Forescout detects a threat based on Forescout or third-party intelligence, Forescout takes policy-driven actions to mitigate.
4. Forescout automatically creates a ServiceNow Security or IT incident with base incident and affected device information.
5. ServiceNow ingests information from Forescout and updates Forescout with additional incident information.
6. ServiceNow can also trigger Forescout to facilitate remediation per policy.
7. Forescout updates ServiceNow CMDB CI records with new device state as it changes providing results of mitigation and remediation actions.
8. Data is synchronized across Forescout and ServiceNow platforms for audit tracking accuracy.

Conclusion

ServiceNow is the leader in providing enterprise-scale digital workflows that unlock productivity. Forescout is the leader in enterprise-wide device visibility, control and threat defense across IT, OT and IoT. The combination of ServiceNow and Forescout increases operational efficiency, streamlines enterprise risk and compliance management and reduces MTTR with a foundation of continuous asset accuracy, policy enforcement and audit traceability for all devices in the connected enterprise.

TAKE A TEST DRIVE

[1] SANS State of OT/ICS Cybersecurity Survey, 2019 https://www.forescout.com/platform/operational-technology/2019-SANS-state-of-OT-ICS-cybersecurity-survey/

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

Learn more at Forescout.com