FORESCOUT

The Forescout Platform: Continuous Device Visibility for Real-Time Asset Management

COST & GOVERNANCE
• CFO/Finance
• Warranty & License
• Contracts & Legal
• Software Manager
• Logistics
SERVICE & SECURITY OPERATIONS
• CIO/CTO/Ops
• Service Manager
• Service Desk
• Incident Manager
• Change Board
• Field & Ops Staff

Figure 1: Consumers who need accurate real-time asset data.

> "By 2024, the number of enterprise internal and external hardware and software asset audit requests will increase by 100%, up from approximately two and a half to five requests annually."
>
> **— Gartner, April 2019[1]**

The Challenge: Knowing Your Assets

Effective asset management solutions are essential for managing the accounting, governance, maintenance and costs of an organization's assets. An accurate and contextually rich asset management database, typically a configuration management database (CMDB), is a necessary foundation for optimizing asset performance and availability as well as reducing costs and security risk. Given today's high-volume, sophisticated cyberattacks, it's essential to maintain real-time insight and governance of all IP-connected virtual and physical devices regardless of whether they are IT systems, operational technologies (OT) or Internet of Things (IoT) devices.

Without an automated way of maintaining real-time asset intelligence for all such devices, organizations can face high manual labor costs, reduced performance, potential downtime and risk of security breaches due to asset intelligence gaps. These dangerous gaps can be caused by data insight time delays, dependency on management agents to gather data, or incomplete, non-correlated data.

Without an automated way of maintaining real-time asset intelligence for all devices, organizations can face high manual labor costs, reduced performance, potential downtime and risk of security breaches due to asset intelligence gaps.

Asset, service, security and operations management business functions (see Fig. 1) all rely on accurate and current asset records. The systems that support these teams can have linked datasets that help to improve productivity and solution functionality. However, when the asset database source is not continuously refreshed as new assets join the network or configurations change, dependent systems are less effective. Typical asset databases are unable to continuously discover and collect data for all network-connected devices in real time, especially for agentless IoT and OT systems. To make matters worse, extensive manual labor is often deployed—usually with unrealistic expectations that these human interventions can close the information gap and maintain a trusted asset database. This creates a visibility gap where critical assets are literally unknown or unmanaged.

To close this visibility gap, many asset management solution vendors recommend integrating one or more third-party discovery technologies such as their own point-in-time discovery tool(s), Microsoft® System Center Configuration Manager (SCCM), Active Directory and other management systems, then combining the results into their asset database. This forces staff to sort through each discovery event stream, look for duplicates and resolve conflicting or inconsistent data before establishing a trusted baseline of assets. Even worse, this costly, thankless and error-prone process becomes out of date the instant it is completed.

Poor data input = ineffective business and security operations

Figure 2 illustrates the relationship between asset discovery and dependent systems, services and organizational functions. What's noteworthy is that incomplete asset discovery and visibility ultimately result in inaccurate data driving dependent services and functions.This highlights the domino effect of how incomplete asset intelligence reduces the effectiveness of managing, servicing and securing assets. Put simply, missing asset data makes the functions that rely on that data's accuracy—and, potentially, the assets themselves—far less effective. Poor data also opens doors to risk. Unaccounted for or unmanaged technology assets create vulnerable entry points for malicious actors, both inside and outside the organization, to exploit.

To address these problems, organizations need an automated solution that provides continuous visibility of all networked assets in real time, assesses their configuration properties in detail, monitors for changes and feeds accurate asset information to a multitude of dependent services and solutions. Forescout offers such a solution.

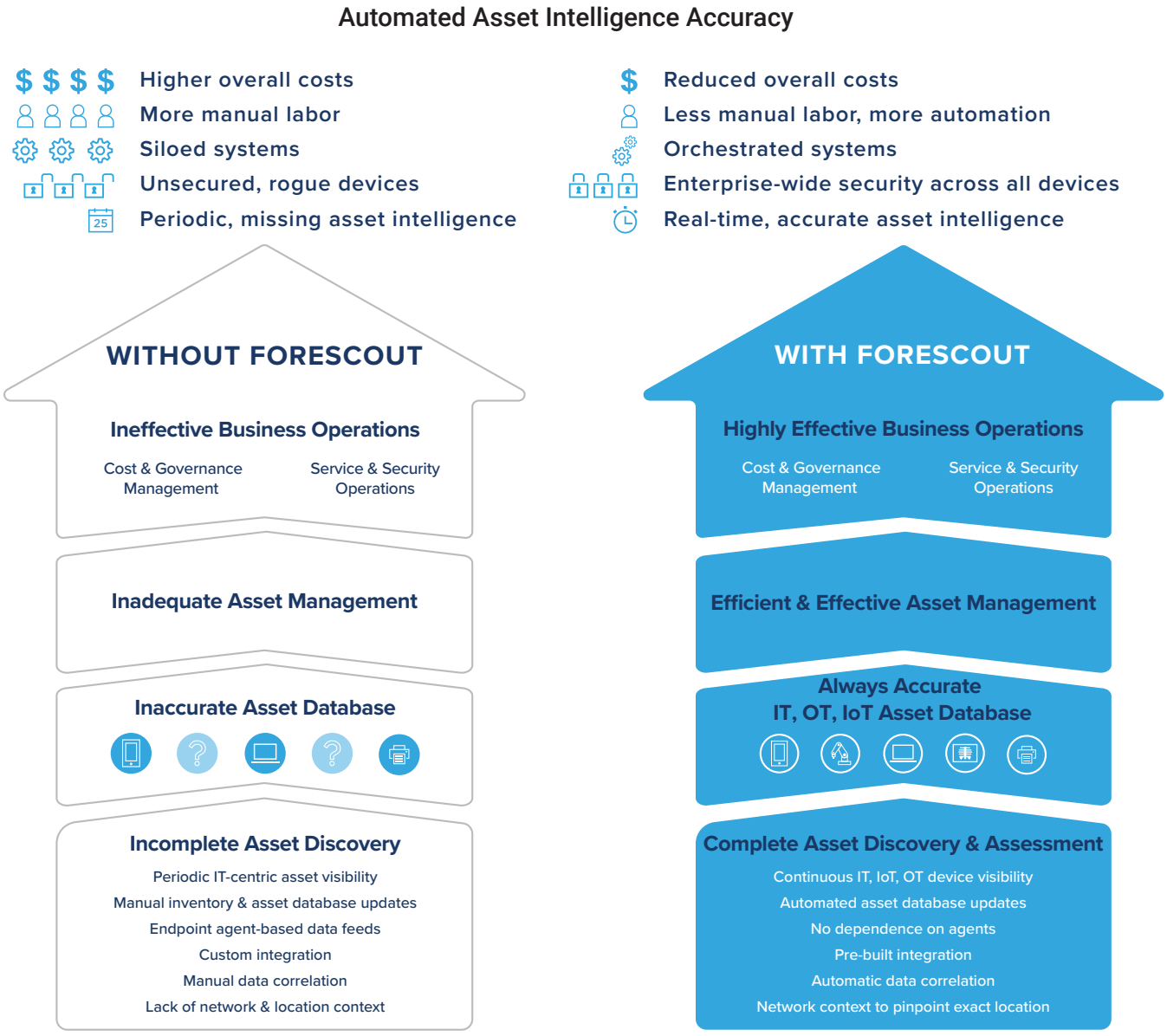

Figure 2: The Forescout platform automates asset data collection to improve efficiency, accuracy and situational awareness.

The Forescout Solution

Providing real-time asset management of all IP-connected devices is essential in today's fluid and dynamic business environment. The Forescout platform's ability to provide real-time, accurate asset intelligence across device types, organizational units and functions delivers significant business value by:

Avoiding manual, error-prone and expensive inventory processes: The Forescout platform can streamline and automate an accurate asset database/CMDB and eliminate infrequent, time-consuming manual inventorying—the cost of which can easily exceed $1 million per year for medium-sized networks.

Helping ensure and demonstrate compliance: Real-time contextual updates to the asset database/CMDB ensure a single source of truth for accurate asset intelligence, governance, security operations management and reporting. Policy-driven remediation also demonstrates compliance.

Boosting operational efficiency: In addition to feeding the CMDB with real-time asset intelligence, the Forescout integration with ServiceNow also enables organizations to automatically create an IT or security incident record, automate remediation/workflows and create a complete audit trail that is synchronized with the asset record.

Accelerating incident response: The Forescout platform provides IT service and security operations teams with rich device context to prioritize and remediate issues, as well as an automated means to restrict or block the network access of noncompliant or compromised devices. Policy-driven remediation actions can be triggered automatically by either Forescout or ServiceNow.

Empowering smarter decision-making: The Forescout platform facilitates accurate asset intelligence that is the basis for strategic decision-making and policy creation as companies plan and implement digital transformation initiatives. Also, the comprehensive visibility into networked assets that the platform provides leads to enhanced asset lifecycle management while also helping executives to better understand business risks and make more informed decisions.

Cutting costs: By accurately tracking installed software, the Forescout platform helps organizations comply with licensing agreements, reduce penalties and reassign unused software licenses. In addition, it can reduce operational costs and help avoid noncompliance and associated fines by improving the security posture of devices by automatically enforcing configuration and endpoint security tool requirements.

How Forescout does it

The Forescout platform serves as the foundation that fosters an accurate source of asset intelligence that business, IT and security operations solutions and teams can depend on to be more effective. With the convergence of IT and OT networks, it is increasingly important to cohesively inventory, classify and assess both environments to more fully understand and address enterprise-wide risk.

The Forescout platform uses a combination of agentless methods to discover every IP-connected physical and virtual device on the extended enterprise network. Its technology- and vendor-agnostic approach is not dependent on data from any individual network architecture. Forescout also automatically classifies and continually assesses devices using passive-only profiling techniques that don't disrupt critical business processes or introduce operational risk. By being able to apply deep packet inspection of over 100 IT and OT protocols, Forescout gains real-time contextual insight across virtual and physical devices of all types including:

- Traditional IT endpoints, including mobile devices
- Data center
- IoT and OT/Industrial Control Systems (ICS)
- Physical and software-defined networking infrastructure

Valuable in-depth contextual information is collected, such as device type, manufacturer, OS configuration, applications installed, patch state, network location, currently logged-in users and more. With this information, a detailed asset inventory and baseline of "normal" network communications is established in the Forescout platform's real-time asset repository for immediate analysis, policy-enforcement and access control. Forescout can also automatically share this rich real-time information with other platforms, such as the ServiceNow platform CMDB, to enhance the effectiveness of downstream applications that depend on a CMDB for accurate, complete asset intelligence. For more information on how Forescout sees and assesses all devices, visit www.forescout.com/eyesight.

The Forescout platform can also use its real-time, rich asset intelligence to automatically apply granular policy-driven controls to continuously enforce configuration, security and access requirements. Forescout offers a broad array of host and network-based controls that can help streamline asset management, service and security operations by automating workflows using real-time asset intelligence. For more information on Forescout control capabilities visit www.forescout.com/eyecontrol.

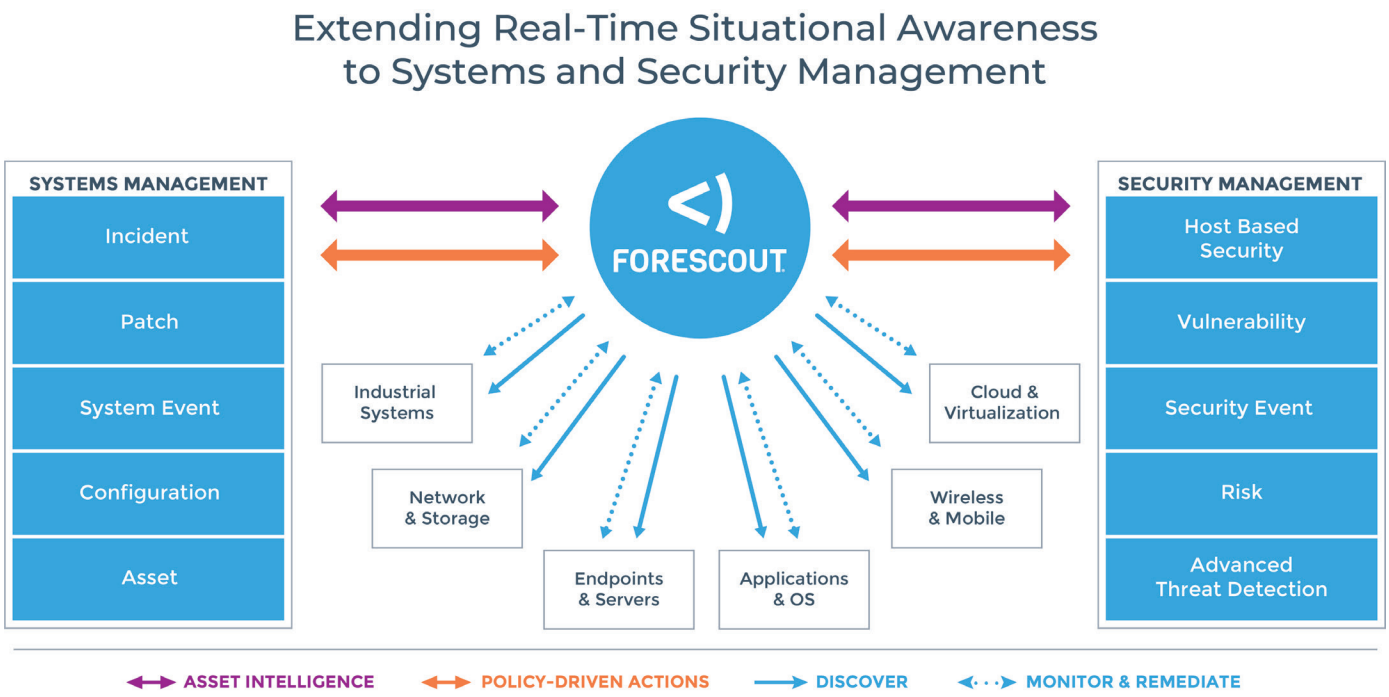

Figure 3: The Forescout platform can discover assets on the network and feed this information to numerous third-party systems and help streamline management operations.

Extending Visibility and Control to Streamline Asset and Security Operations

The Forescout platform, combined with Forescout eyeExtend products and Base Modules, allows organizations to gain comprehensive visibility and orchestrate closed-loop processes with critical asset and security services to increase efficiency and effectiveness.

With over 40 Base Modules,* the Forescout platform provides native integration with leading IT and OT network switches, routers, wireless appliances, firewalls, VPN concentrators and data center and cloud solution providers—thereby helping to consolidate asset discovery and draw a more in-depth and accurate picture of connected assets.

Forescout eyeExtend solutions provide bi-directional orchestration with leading management and security tools, leveraging the Forescout platform's real-time visibility and control to further streamline asset and security management processes. For more information, visit www.forescout.com/eyeextend.

Forescout eyeExtend for ServiceNow®

Forescout eyeExtend for ServiceNow enables bi-directional integration of the Forescout platform with ServiceNow solutions: ServiceNow platform CMDB, IT Service Manager (ITSM) and Security Operations.

The integration orchestrates information sharing and workflows driven by a single-source-of-truth for enterprise-wide asset intelligence using the ServiceNow platform CMDB. The database is automatically updated by the Forescout platform and used across multiple use cases.

This allows organizations to better manage assets, enforce configuration and security policies, quickly respond to incidents or breaches, and make more informed decisions.

The Forescout-ServiceNow integration also greatly improves efficiency and effectiveness by automating portions of IT service and security operations. For example, ServiceNow IT and Security Incident records/tickets can automatically be created via Forescout as policy violations and compromised devices are detected.

Through Forescout eyeExtend for ServiceNow, ServiceNow can also direct the Forescout platform to take policy-driven actions that accelerate remediation of service and security incidents such as patch updates, restarting services and blocking or isolating noncompliant/compromised devices on the network. Once remediation is complete, eyeExtend for ServiceNow updates the CMDB with the new state and allows access according to policy. Organizations thereby achieve closed-loop processes and accurate incident lifecycle reporting.

Forescout is Transforming Asset, Service and Security Management

The Forescout platform is a unique, invaluable tool for bringing greater efficiency and accuracy to asset, service and security solutions. It enables organizations to maintain an accurate view of network-connected assets and provides the ability to track movement of devices and facilitate remediation actions against noncompliant or compromised devices. By delivering in-depth asset visibility in real-time, the Forescout platform makes it possible to automate simple tasks and complex processes with policy-based precision and control.

Forescout is helping 3,300 customers in over 80 countries* to reduce risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance, and increase security operations productivity. Specifically, regarding security and asset/systems management, the Forescout platform is delivering value through absolute device visibility and our infrastructure-agnostic approach to asset discovery and automation. There is nothing else like it on the market today.

> "You have to be compliant; it's not a choice. For a network the size of ours, the man-hours to do so manually cost well over $1 million, and the cost of a breach can go through the roof."
>
> **— Phil Bates, Chief Information Security Officer, State of Utah**

*As of December 31, 2018

***Notes**

1 Gartner Research Note: Reduce Audit Costs and Risks With a Comprehensive IT Asset Management Strategy, April 2019

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