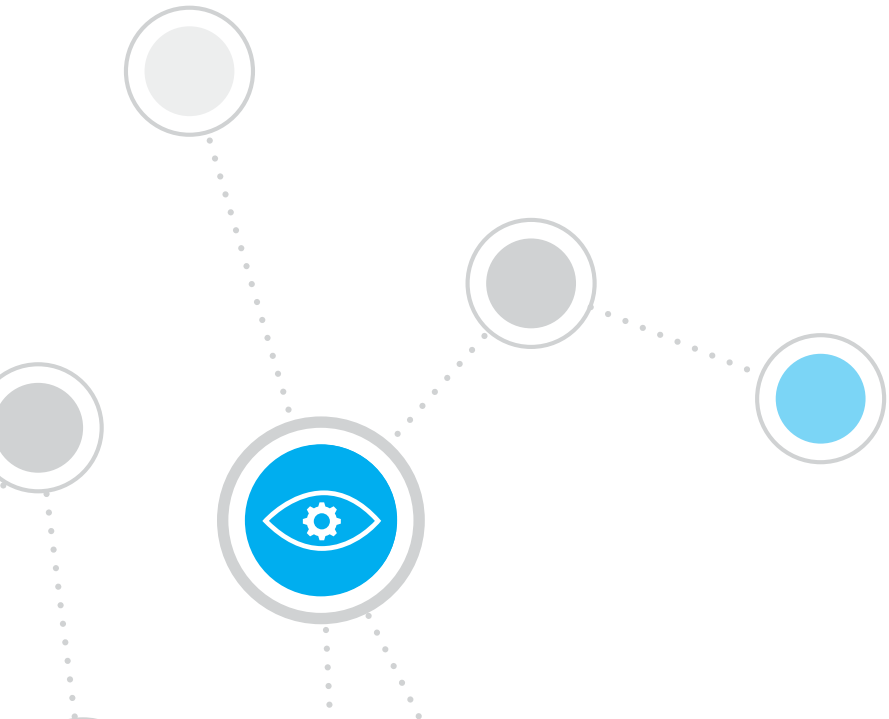
ForeScout

White Paper

ForeScout CounterACT®: Advanced Endpoint Visibility for ITAM and CMDB

"You Can't Manage What You Can't See!"



A Common Requirement and Challenge

IT asset management (ITAM) solutions are essential for automating IT accounting and governance tasks and for efficient management of asset costs. Configuration management database (CMDB) solutions are a necessity when it comes to obtaining a real-time view into the configuration, availability and functionality of the IT assets within an organization, and for tracking asset configuration items (CI's) and their attributes.

ITAM Consumers

- CFO / Finance
- Warranty & License
- Contracts & Legal
- Software Manager
- Logistics

CMDB Consumers

- CIO/CTO/Ops
- Service Manager
- Service Desk
- Incident Manager
- Change Board
- Field & Ops Staff

Figure 1: Key ITAM and CMDB consumers.

While ITAM and CMDB solutions differ in their objectives, they are both considered single sources of record for a multitude of data consumers (see Fig. 1). ITAM and CMDB solutions often have linked data sets that help to improve productivity and solution functionality. They also share a fundamental need for asset discovery and situational awareness. When ITAM and CMDB solutions are ineffective at automated asset discovery, costly (and often inaccurate) manual labor is required to close discovery gaps and maintain a trusted data set, especially given the constant change in today's dynamic, service-on-demand environment.

There is no getting around the fact that automated asset discovery and intelligence are necessities of modern business. But ITAM and CMDB solutions are plagued by the inability to see network-connected devices in real time due to legacy discovery methods that can't detect IP-addressed endpoints, and which produce gaps in asset visibility. As a best practice, many ITAM and CMDB solution vendors recommend integrating one or more third-party discovery technologies (System Center Configuration Manager, Active Directory, ITAM/CMDB discovery, etc.) and combining their results. However, this forces organizations to sort through each discovery event stream, looking for duplicate, conflicting and inconsistent data before establishing a trusted baseline of assets.

Invariably, after exhausting automated discovery techniques, organizations then attempt to eliminate the holes in their IT asset and configuration visibility through costly, manual true-up detection efforts. If there were an automated way to incorporate that data into the ITAM and CMDB solutions, it would help to resolve discovery issues and reduce or eliminate manual true-up efforts that, even when done right, have a short window before the information becomes outdated.

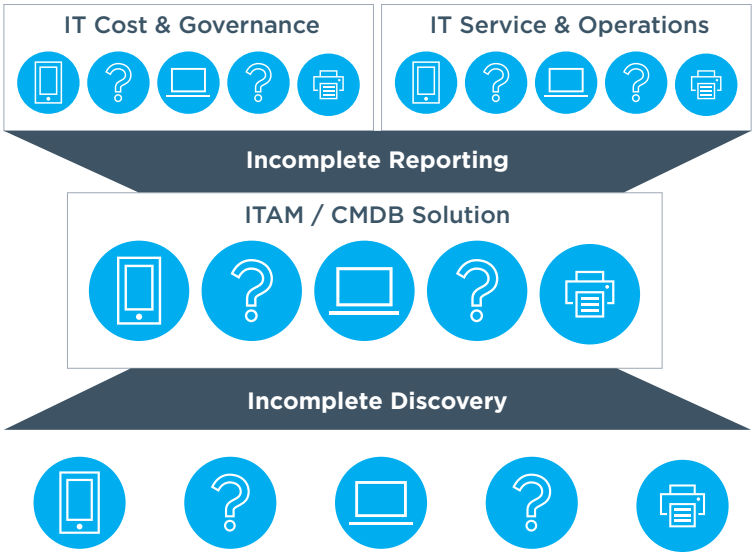


Figure 2: Poor asset visibility impairs other services.

Poor Data Input = Poor Data Output

Figure 2 illustrates the relationships between ITAM and CMDB solutions and some of the dependent teams and organization functions. Incomplete asset visibility within ITAM and CMDB solutions results in incomplete data being fed to those dependent IT services. This presents a domino effect, as incomplete data reduces the effectiveness of the IT Cost and Service Operations that depend on ITAM and CMDB solutions. Missing IT asset data drives inaccurate or incomplete reporting to support teams, and weakens integration points into technologies and solutions that rely on that data. In turn, a poorly functioning asset discovery solution creates headaches for finance and support organizations that are forced to use solutions with incomplete or inaccurate endpoint data.

To address these problems, organizations need a solution that provides visibility of IP-addressable assets on their network in real time, monitors IT asset and CI attributes consistently, and feeds accurate asset information to a multitude of dependent services and solutions.

The ForeScout CounterACT Solution

ForeScout CounterACT® takes a vendor-agnostic approach to detecting connected devices on an organization's network in real time and without the need for installed agents. CounterACT integrates with network switches, routers, wireless appliances and security components, thereby helping to consolidate asset discovery and detection to draw a more in-depth and accurate picture of connected and connecting IT assets. CounterACT then detects and presents rich contextual data to operations staff or a third-party tool for consumption. CounterACT can detect changes to endpoints in real time, and can assess transient assets as they enter and leave the network. In addition to collecting IT asset data and conducting endpoint hygiene, ForeScout is capable of automating daily tasks that can help with improving an organization's operational efficiency and effectiveness. Finally, ForeScout Extended Modules allow organizations to orchestrate simple, common, closed-loop processes with ITAM and other complementary IT services such as configuration management, patch management and event management.

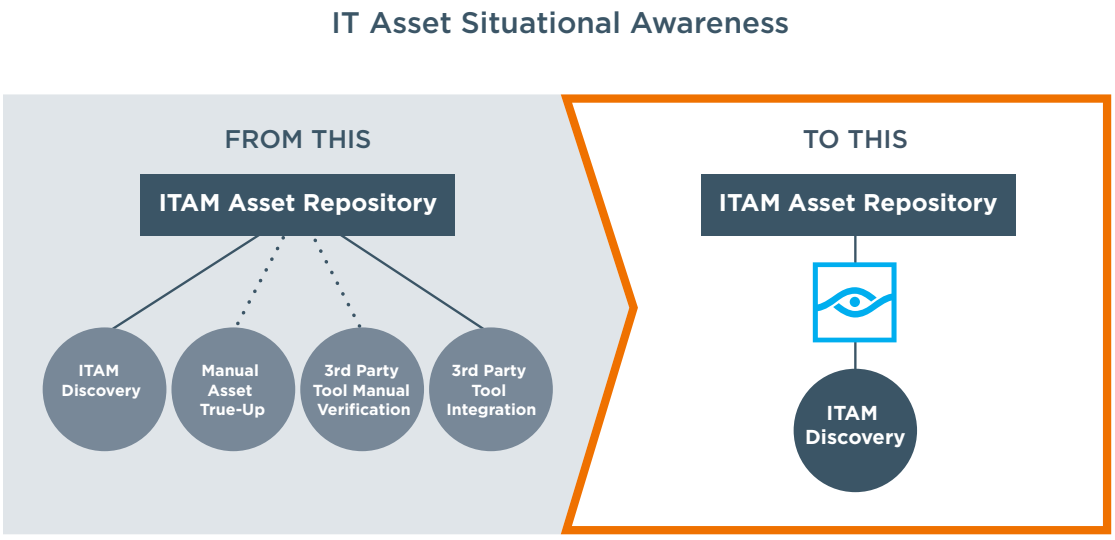


Figure 3: ForeScout CounterACT simplifies asset data feed to improve accuracy and situational awareness.

ForeScout Solution: Asset Visibility, Control and Workflow Orchestration

A unique attribute of ForeScout CounterACT is its ability to identify a vast array of devices on the network—even those without secure management agents. This allows CounterACT to identify infrastructure components, physical/virtual systems, managed PCs, smartphones, unmanaged Bring Your Own Device (BYOD), Internet of Things (IoT) devices, Operational Technologies (OT) and rogue endpoints. Specifically regarding managed IP-enabled IT assets on a network, it identifies them and develops a rich, real-time contextual database that includes their configurations, attributes and other specific information. Moreover, CounterACT can validate that antivirus and other host-based security applications are installed, running and updated.

The capabilities of CounterACT comes with an array of optional integrations. ForeScout Extended Modules provide interoperability, integration and security orchestration support for various third-party security management products. These Extended Modules allow organizations to eliminate the need for traditional discovery solutions and can help reduce or eliminate manual true-up exercises. ForeScout CounterACT can help simplify an organizations asset data feed, while improving its accuracy.

As Figure 3 illustrates, organizations often leverage multiple data sources to develop an in-depth picture of their existing IT assets.

CounterACT's asset discovery and situational awareness approach has the ability to discover assets on the network and feed this information to a wide range of third-party systems and services, including ITAM, configuration, security, ticketing and reporting. CounterACT uses a wide array of detection methods to bring about real-time visibility that lets IT personnel identify managed, unmanaged, transient, IoT and rogue devices, including physical, virtual and mobile systems. The list below summarizes the detection methods CounterACT uses to identify the endpoints on the network and their attributes.

- Interrogate ARP and CAM table on network devices
- NAT device detection
- Listen for SNMP traps from network infrastructure
- Scan the network IP range and fingerprint OS type
- Passively listen to network traffic on span port
- Watch DHCP authentication
- Proxy DNS requests from DHCP community
- NetBIOS scan
- LDAP query for "Member of"
- Endpoint-based interrogation of host settings that includes looking for hypervisors

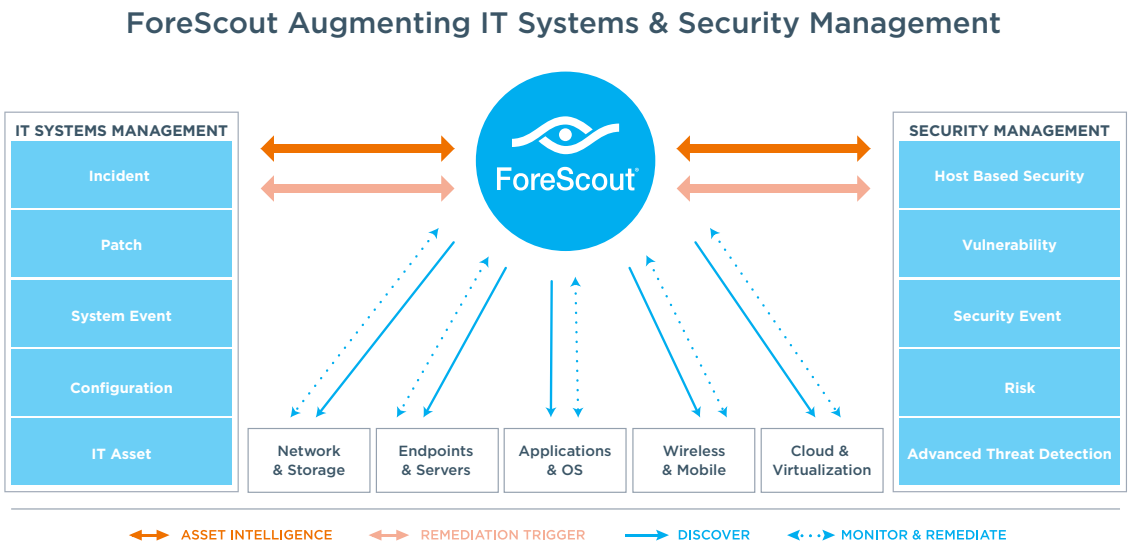


Figure 4: The ForeScout platform unifies visibility, automation and control across IT infrastructure and security management solutions.

By delivering in-depth asset visibility in real time, ForeScout CounterACT empowers organizations to automate simple tasks and complex processes with policy-based precision and control. ForeScout delivers value to more than 2,500 organizations* worldwide in both security and IT systems management through our vendor-agnostic approach to asset discovery and automation. In addition to providing advanced asset visibility, CounterACT detects configurations and provides situational awareness that can be shared with many solutions throughout the organization. As CounterACT detects a device on the network, it collects in-depth endpoint attributes, including hardware and OS configuration, software and currently logged-in users, then feeds that information to various third-party solutions, improving their endpoint visibility.

Summary

ForeScout CounterACT is a unique, invaluable tool for organizations that value the efficiency and accuracy of ITAM and CMDB solutions. Any organization seeking to enhance enterprise IT security management efforts should evaluate this agentless visibility, control and workflow orchestration platform.

Acronym Glossary:

ARP (Address Resolution Protocol)

CAM (Content Addressable Memory)

DNS (Domain Name Server)

DHCP (Dynamic Host Configuration Protocol)

LDAP (Lightweight Directory Access Protocol)

NetBIOS (Network Basic Input/Output System)

SNMP (Simple Network Management Protocol)

Learn more at
www.ForeScout.com

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

About ForeScout

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of June 30, 2017 more than 2,500 customers in over 70 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide response. Learn how at www.forescout.com.

*As of June 30, 2017