FORESCOUT

## Highlights

### See

- Discover devices as they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Assess device hygiene and continuously monitor security posture

### Control

- Notify end users, service desk personnel or IT systems about security issues
- Conform with policies, industry mandates and best practices
- Restrict, block or quarantine non-compliant or compromised devices

### Orchestrate

- Share device properties, configuration information and network context with ServiceNow
- Validate and true-up your asset repository to establish a trusted baseline of assets
- Verify requisite device configuration and software updates and facilitate remediation actions

# ForeScout Extended Module for ServiceNow®

## Automate asset discovery, improve asset compliance and boost IT service efficiency

If you're storing your asset information in multiple unlinked repositories using disparate asset discovery techniques, you're not alone. Not only can this waste valuable time doing manual true-ups and creating a unified data set, it often leads to substandard decision-making based on inconsistent data. Real-time asset discovery and monitoring is an essential part of any successful IT asset management program, as it can help your organization establish a trusted data set, improve asset compliance and make informed business decisions.

## The Challenges

**Visibility.** Serious attempts to manage security risk must start with knowing who and what is on your network, including visibility into the configuration and compliance of network-connected devices. Most organizations are unaware of a significant percentage of endpoints on their network because they are:

- Unmanaged guests or Bring-Your-Own-Device (BYOD) endpoints
- Internet of Things (IoT) devices
- Devices with disabled or broken agents
- Transient devices, undetected by periodic scans

As a result, organizations are often unaware of their complete asset inventory and overall compliance posture.

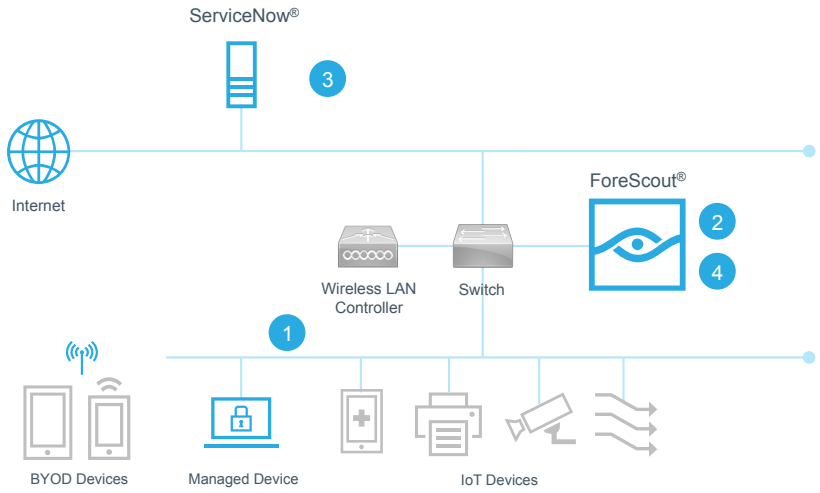
**Automated Asset Intelligence.** With the proliferation of devices on today's networks and a highly mobile and transient workforce, IT teams are constantly challenged to track devices and their configuration as they enter or leave the network. Organizations must rely on manual processes to manage assets and sort through data sets with duplicate, conflicting or inconsistent data in an attempt to establish a trusted baseline of assets, and retire or remediate devices as required.

**IT Governance and Services.** Incomplete asset information reduces the effectiveness of IT governance and service operations that depend on configuration management database (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, lack of a single-source asset repository or trusted baseline of assets creates headaches for finance and support organizations that are forced to use solutions with incomplete or inaccurate endpoint data.

## How it Works

ForeScout CounterACT® is a network security solution that gives you the unique ability to see devices, including non-traditional devices, as they connect to the network. CounterACT provides policy-based assessment, monitoring and precise automated control of these devices.

1. ForeScout CounterACT discovers and classifies various types of devices as they connect to the network
2. The ForeScout Extended Module shares device properties, configuration information and network context with ServiceNow
3. ServiceNow adds or updates this information in the CMDB to true-up existing asset repository
4. CounterACT can import CMDB properties from ServiceNow to be used in its inventory and policies




## ForeScout Extended Modules

The ForeScout Extended Module for ServiceNow is an add-on module for ForeScout CounterACT that is sold and licensed separately. It is one of many ForeScout Modules that enable CounterACT to exchange information, automate multivendor workflows and accelerate system-wide response.

For details on our licensing policy, see www.forescout.com/licensing

Learn more at
**www.ForeScout.com**

The ForeScout Extended Module for ServiceNow® leverages CounterACT's real-time visibility and provides up-to-date device properties, classification, configuration and network context to ServiceNow. This enables you to get a current view of networked assets, track their movement and remediate or retire these assets as required. As a result, you can make informed decisions by leveraging an accurate single-source-of-truth asset repository, avoid manual, time-consuming and error-prone processes and optimize IT governance and service operations.

ForeScout CounterACT discovers and classifies various types of devices as they connect to the network whether they are traditional IT-managed laptops and servers, mobile devices, switching and wireless infrastructure, printers or networked IoT devices. The Extended Module provides pre-defined policy templates to synchronize discovered assets, their properties and associated network context with ServiceNow. It includes a certified app available in the ServiceNow store to prioritize and automatically merge asset records in the ServiceNow CMDB.

The Extended Module for ServiceNow also allows you to define CMDB properties that can be brought over to enrich the device inventory and policies within CounterACT. This enables you to continuously monitor or track changes in virtual or physical devices within the ServiceNow asset repository, apply granular policies within CounterACT and maintain an accurate single source of truth for better decision-making. Additionally, as devices enter or leave the network, CounterACT continuously monitors these changes and keeps the ServiceNow CMDB current and up to date.

ForeScout can also help you prepare for audits, inventory software usage and verify license compliance. It can scan your network and help true-up and track asset information in ServiceNow. In addition, you can verify whether software updates delivered to managed devices are applied error-free and update the ServiceNow CMDB. If requisite updates are not applied, CounterACT can quarantine the device and initiate policy-based remediation actions.

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