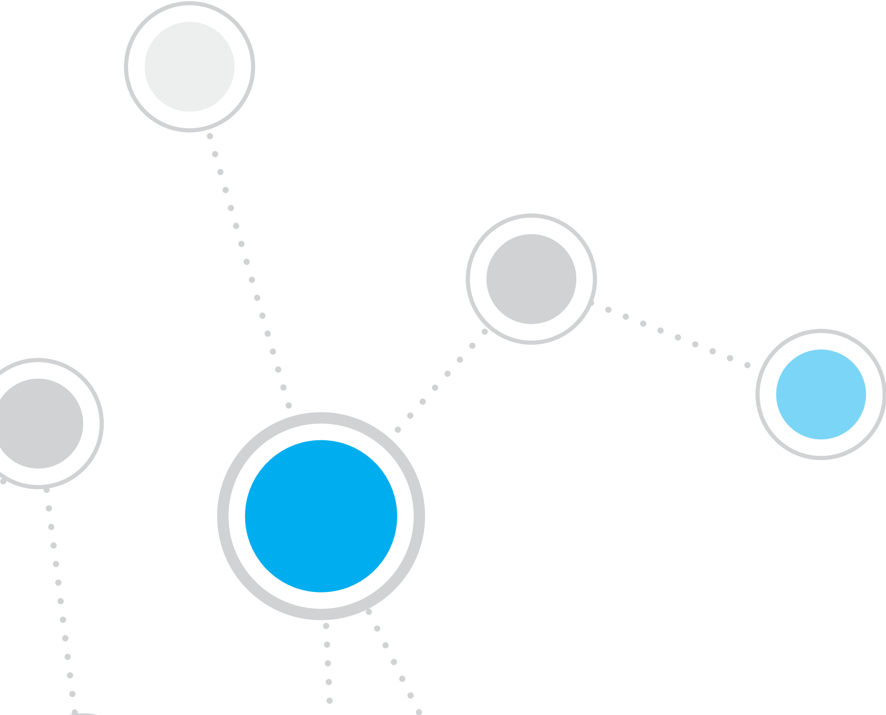
FORESCOUT

Tech Note

ForeScout CounterACT™ USB Detection and Blocking



Introduction

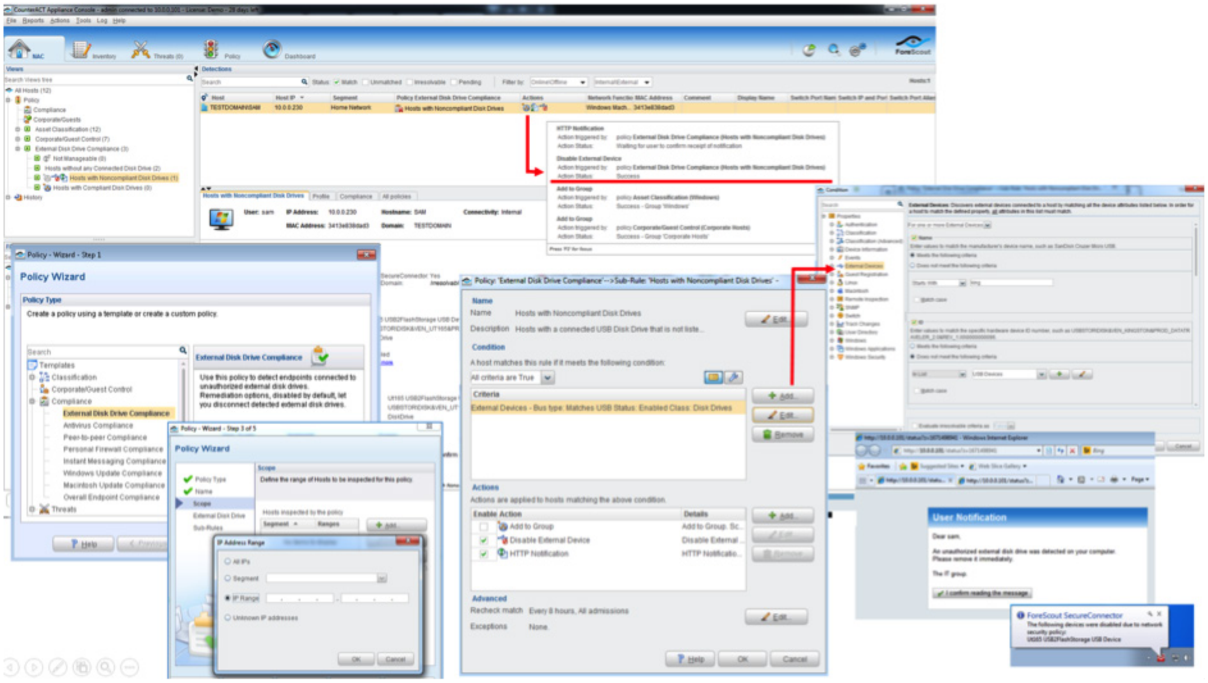
In November 2008, when a malware attack struck combat-zone computers and infiltrated the network, the U.S. military cracked down with a sudden ban on USB (Universal Serial Bus) devices. Banning the use of USBs made sharing information in the war theaters more difficult and reflected the severity of the intrusion and the threat from malware, which was potentially capable of even allowing an attacker to take remote control of a computer and extract confidential files and other information. Behind the scenes, ForeScout CounterACT™ was detecting and blocking USB drives from unauthorized network access, thus halting the spread of the malware and protecting military computers from further attack. With the growing threat of malware infiltration and cyberattacks—whether for espionage aimed at gathering military intelligence or for gaining illicit control of military networks and resources—the need to quickly detect and block unauthorized access to mission critical networks is paramount.

ForeScout CounterACT USB Detection/Blocking: How to implement it in your network

Using custom or predefined policies, CounterACT can detect or block unauthorized USB mass storage devices—such as memory sticks, external storage devices, smart phones and cameras—that are connected to Windows endpoints. It can also automatically notify Windows endpoint users that USB connections are not allowed. CounterACT's predefined External Disk Drive Compliance policy is offered as part of the easy-to-use policy wizard, which is accessible from the CounterACT console (see Figure 1).

Apply the CounterACT External Disk Drive Compliance template in three easy steps:

1. Add a policy using the External Disk Drive Compliance Template.
2. Define the policy scope and select Devices you want to apply this to (based on IP addresses and device names).
3. Set up conditions and actions for the device search.



Policy - Wizard - Step 1

Policy Wizard

Policy Type

Create a policy using a template or create a custom policy.

External Disk Drive Compliance

Use this policy to detect endpoints connected to unauthorized external disk drives. Remediation options, disabled by default, let you disconnect detected external disk drives.

Policy - Wizard - Step 3 of 5

Scope

Define the range of Hosts to be inspected for this policy

Policy: 'External Disk Drive Compliance'-->Sub-Rule: 'Hosts with Noncompliant Disk Drives' -

Name

Name: Hosts with Noncompliant Disk Drives

Description: Hosts with a connected USB Disk Drive that is not liste...

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
External Devices - Bus type: Matches USB Status: Enabled Class: Disk Drives

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
□	Add to Group	Add to Group: Bc...
☑	Disable External Device	Disable External ...
☑	HTTP Notification	HTTP Notificatio...

Advanced

Recheck match: Every 8 hours, All admissions

Exceptions: None

User Notification

Dear sam,

An unauthorized external disk drive was detected on your computer. Please remove it immediately.

The IT group.

✓ I confirm reading the message

ForeScout SecureConnector

The following devices were disabled due to network security policy:
U165 USB2FlashStorage USB Device

Figure 1: Enforcing External Disk Drive Compliance with ForeScout CounterACT predefined policy template.

ForeScout CounterACT: 3 Simple Steps to protect your network

1. **Identifies the endpoints and runs a check to determine whether or not the device (or user) is in compliance and authorized to access the protected resources.** CounterACT allows the IT manager to gain visibility of the network and detect multi-vendor and cross-platform devices without the need for an agent residing on the endpoint.
2. **Grants access IF the device is in compliance with the USB policies established for the network AND the person's (policy-based) role justifies their access.** CounterACT performs a comprehensive audit-and-report process that is transparent compliant end users. Using the pre-configured policies and reports provided in the External Disk Drive Detection and Blocking kit together with a few best practices, the IT manager is able to implement a USB-compliance network environment in just hours.
3. **Blocks access IF the device is out of compliance or the person does not have (policy-and-role-based) authorization to access the protected information.** If an access attempt is unauthorized, CounterACT automatically collapses data lines before the connection can take place. CounterACT is able to auto-remediate and bring the corporate network into compliance. The IT manager leverages this capability to enforce compliance, ensure role-based access, and keep authorized end users productive while protecting the production network and mission-critical data. Notifications are built in to alert the IT staff when an unauthorized attempt has taken place and the information is logged in a data store for later analysis. This provides the strong enforcement required to block unauthorized devices without causing major disruption to the network or organizational workflow process.

Additionally, ForeScout CounterACT also provides post connection monitoring to network connections remain compliant and produces reports for audits, control and more.

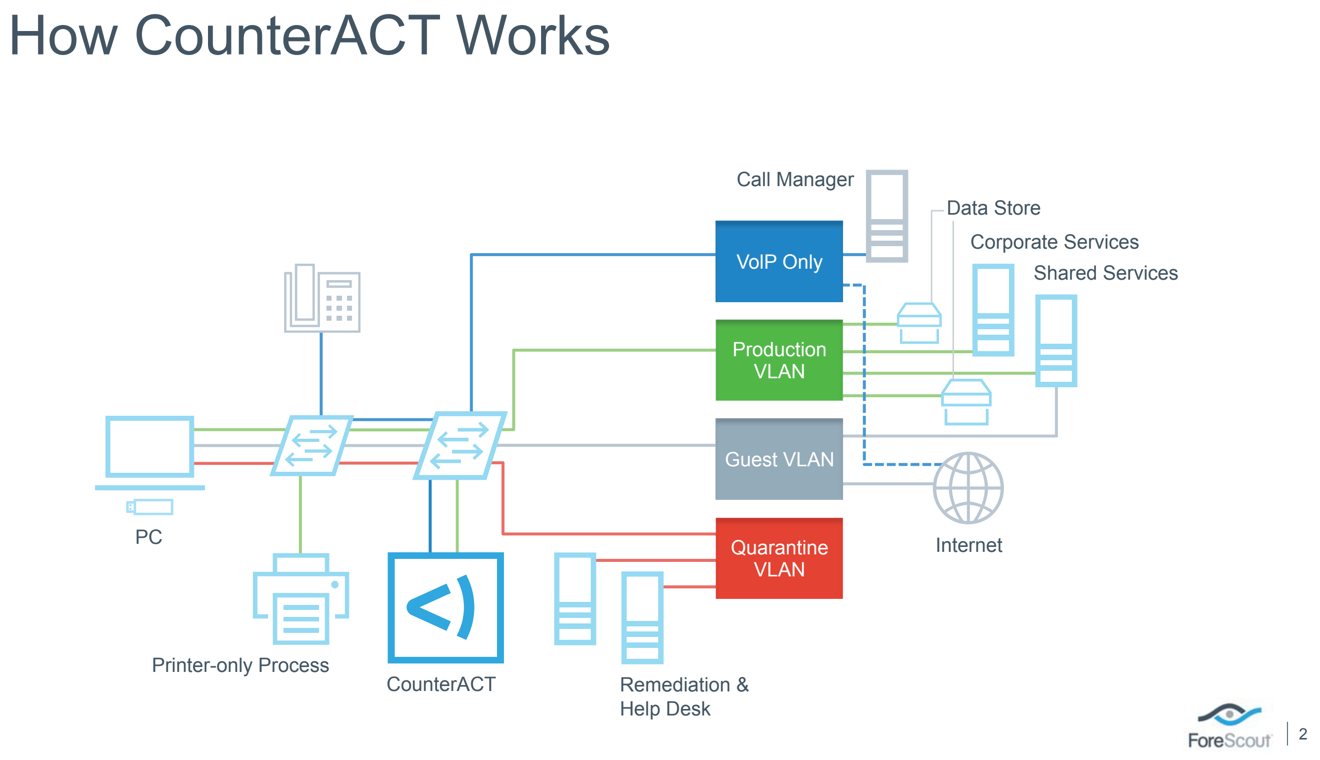


Figure 2: How ForeScout CounterACT works.

Learn more at
www.ForeScout.com

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
Fax 1.408.371.2284

About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of October 2015, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions.