FORESCOUT

ForeScout Extended Module for Advanced Compliance

Improve endpoint security hygiene and automate configuration compliance

Any connected device on the network can be a launchpad for cyberattacks. With the exponential growth and proliferation of connected devices, weak endpoint defenses can easily be exploited and cause network breaches. Often, common attack vectors are not zero-day vulnerabilities as one would expect but, rather, misconfigurations of operating system and application settings and ineffective management of security updates. To reduce your security risk and exposure to cyberattacks, you need a scalable and automated approach for implementing security best practices and standards-based benchmarks on connected endpoints.

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 compliance posture

Control

- Notify end users, administrators or IT systems about compliance issues
- Conform with best practices, security benchmarks and industry mandates
- Restrict, block or quarantine non-compliant or compromised devices

Orchestrate

- Share contextual insights with IT security, risk and governance systems
- Automate common workflows, IT tasks and compliance processes
- Accelerate system-wide response to quickly mitigate risks and data breaches

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 of network-connected devices and whether they comply with your security standards. Most organizations are unaware of a significant percentage of endpoints on their network because they are:

- Unmanaged guest or Bring Your Own Device (BYOD) endpoints
- Devices with disabled or broken agents
- Transient devices undetected by periodic scans

As a result, organizations are often unaware of the additional attack surface and elevated risk that these devices represent.

Threat Landscape. According to industry reports[1], corporate-owned devices and servers are among the top enterprise assets targeted and breached by external attackers. These breaches—often caused by ineffective management of operating system and application configuration and updates—can cause legal exposure, reputation risk and financial harm to organizations. To protect against these cyberthreats, you need the ability to identify and fix configuration and compliance gaps when devices connect to the network, and to continuously monitor them thereafter.

Compliance Automation. Securing endpoints using best practices and security benchmarks published by standards organizations provides a critical cybersecurity foundation. Additionally, regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and others require organizations to secure individuals' personal, health and financial information. Without compliance automation tools and workflows, constrained IT staff and budgets face additional pressure, as failed audits can cause distractions and sidetrack pressing IT projects, as well as lead to legal exposure and additional costs.

[1] The Forrester Wave™: Endpoint Security Suites, Q4 2016

ForeScout Extended Module for Advanced Compliance

The ForeScout Extended Module for Advanced Compliance automates on-connect and continuous endpoint configuration assessment to comply with security benchmarks. This improves security hygiene and regulatory compliance by transforming a labor-intensive activity to one that that can be performed continuously on an enterprise-wide scale.

Standards organizations such as National Institute of Standards and Technology (NIST), Center for Internet Security (CIS) and Defense Information Systems Agency (DISA) publish benchmarks for security configurations for major operating systems and many applications. These provide best practices for endpoint configuration, vulnerability and security compliance for an effective cybersecurity program.

These endpoint security benchmarks are often published and shared in the Security Compliance Automation Protocol (SCAP) format. SCAP is a method for using commonly accepted standards to enable automated configuration and vulnerability assessment and provide security policy compliance metrics. Utilizing SCAP content can provide a highly productive environment for comprehensive compliance testing.

The Extended Module for Advanced Compliance supports the SCAP standard and enables you to leverage security benchmarks and content published in the SCAP format. This allows you to:

- Verify system security configuration settings
- Automate assessment and installation of application and OS updates
- Examine systems for signs of compromise
- Verify the state of a computer system against regulatory or other baselines
- Gather and aggregate assessment results for audit preparation

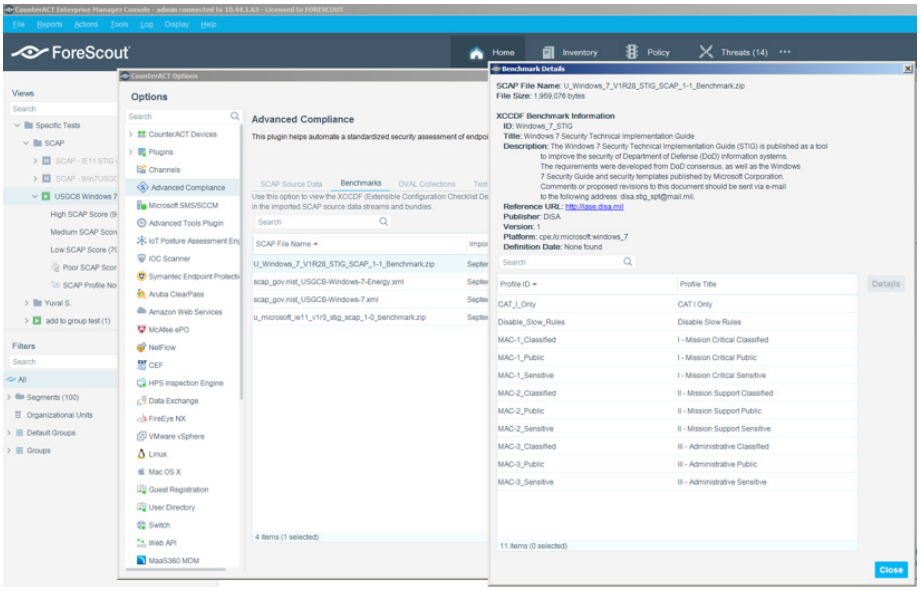

Figure 1: Verify system configuration compliance using SCAP security benchmarks.

Benefits

- Improve device hygiene for greater endpoint security
- Increase configuration compliance
- Reduce usage of outdated application versions
- Leverage credible, standards-based security benchmarks
- Streamline existing processes and automate compliance and remediation workflows

ForeScout Extended Modules

The ForeScout Extended Module for Advanced Compliance 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

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