FORESCOUT

Forescout eyeExtend

for Advanced Compliance®

Simplify endpoint configuration management and compliance enforcement

Zero-day attacks get a lot of attention—with good reason. To break into the network and steal sensitive data, many of these threats take advantage of misconfigured operating systems and software, as well as missing security updates. They can be particularly damaging because PCI DSS, HIPAA and other industry and government regulations require organizations to secure systems that contain sensitive information—with potential legal exposure and steep fines for those that don't. Standards organizations such as the National Institute of Standards and Technology (NIST) publish operating system and application configuration benchmarks in the Security Compliance Automation Protocol (SCAP) to help enterprises run endpoint compliance testing. However, organizations remain challenged by the proliferation of BYOD, transient and guest systems that ultimately go undetected and un-benchmarked, leaving security configuration holes that can be easily exploited.

Forescout eyeExtend for Advanced Compliance fills enterprise security and compliance gaps with automated on-connect and continuous endpoint detection and SCAP-enabled configuration testing against relevant regulations. The solution can also notify administrators and automate network access control by quarantining or limiting network access of devices when test results don't meet preconfigured thresholds.

Challenges

- Detecting and monitoring all network-connected managed and unmanaged devices across campus, data center, cloud and OT networks
- Ensuring all devices are properly configured and updated at all times in compliance with industry mandates and security best practices
- Reducing IT and security staffs' manual workload of managing device hygiene and compliance
- Preventing misconfigured devices from accessing the network and creating security gaps that can be easily exploited

The Compliance Solution

Forescout eyeExtend for Advanced Compliance automates on-connect and continuous endpoint configuration assessment to comply with industry regulations and transform a slow, manual, labor-intensive process into one that can be performed continuously on an enterprise scale.

Forescout eyeExtend for Advanced Compliance can leverage any security benchmark and content published in the SCAP standard. It slashes compliance and security risk by detecting any device connecting to the network. It runs a preconfigured set of configuration benchmarks and isolates or limits network access until results are

eyeExtend

Benefits

- Enhance security hygiene and regulatory compliance
- Simplify compliance auditing, assessment and analysis with customizable compliance thresholds and reporting geared to compliance audits
- Reduce risk by preventing or limiting network access until all benchmarks have run and vulnerabilities eliminated
- Automate remediation in cases of exceeded thresholds or indicators of compromise

Highlights

- Real time discovery, classification and assessment of endpoint systems without requiring agents
- On-connect, SCAP-enabled endpoint configuration assessment to comply with security mandates
- Continuous endpoint configuration benchmarking
- Notification to network administrators or security officers of configuration issues so they can take action
- Restrict, block or quarantine noncompliant or compromised devices
- Set benchmark performance thresholds for results analysis and automated remediation workflows
- Automate vulnerability response and mitigation in response to benchmark results

satisfactory or vulnerabilities have been remediated—all without the need for agents. The Forescout platform lets you preconfigure compliance thresholds for results analysis, automated notification of IT administrators and triggering of remediation workflows.

Organizations can also use the Forescout platform to run configuration benchmarks continually on all Windows network devices, either according to a preconfigured schedule or when an event takes place, such as a system reconnecting to the network. It continuously inspects devices for compliance with enterprise policies and indicators of compromise. Also, if a device is compromised or falls out of compliance, the Forescout solution can quarantine or limit network access and orchestrate remediation processes automatically to help increase security operations efficiency while reducing business risk in real time.

In summary, Forescout eyeExtend for Advanced Compliance helps you streamline and improve configuration management and compliance enforcement for all Windows network endpoints.

Use Cases

Continuous Configuration Management

The Forescout platform helps organizations comply with relevant regulatory requirements and security best practices by continuously discovering and running SCAP-enabled configuration benchmarks on every Windows device connecting to the network. It can also confirm that all Windows endpoints remain compliant while they are on the network by running benchmarks automatically on a schedule or in response to an event.

Report and Quarantine Noncompliant Endpoints

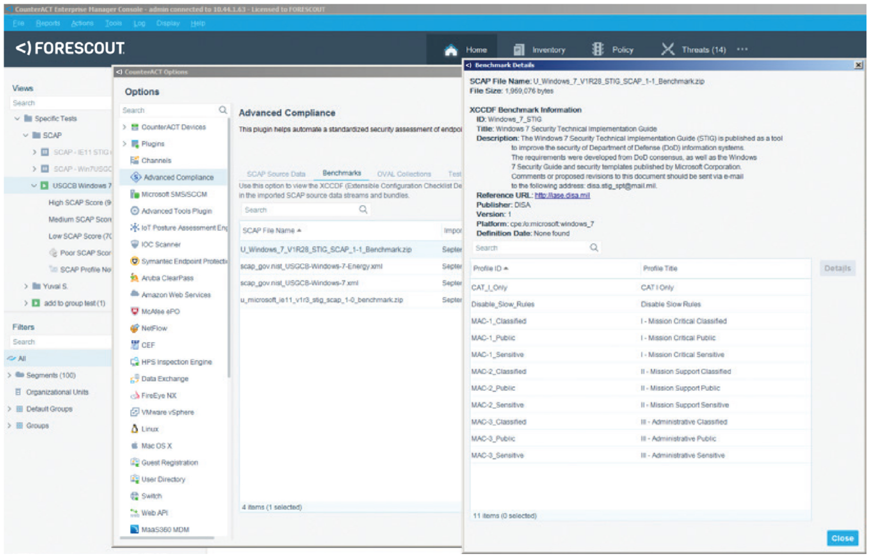
The Forescout solution can enhance security and help organizations comply with security audits by generating and emailing a detailed report of any endpoint that fails to meet a defined compliance level for any given SCAP benchmark. Equally important, the solution can quarantine all endpoints that fall below a preconfigured minimum compliance level.

Measure Compliance Levels Against Known Benchmarks

IT can assess the overall state of compliance by using the Forescout platform to report on compliance of all Windows endpoints for a given benchmark. The platform can then drill down on any compliance rules of interest for a more in-depth understanding of endpoint compliance.

Generate Standard Security Compliance Reports

Information security officers can use eyeExtend for Advanced Compliance to generate detailed reports in the standard Asset Report Format (ARF), either individually or on an ongoing basis, according to a preconfigured schedule. Users can define a target server for the placement of reports for audits and automated submission to external ARF-compliant applications.



Advanced Compliance

This plugin helps automate a standardized security assessment of endpoi

Use this option to view the XCCDF (Extensible Configuration Checklist De in the imported SCAP source data streams and bundles.

SCAP File Name ▲	Impor
U_Windows_7_V1R28_STIG_SCAP_1-1_Benchmark.zip	Septer
scap_gov.nist_USGCB-Windows-7-Energy.xml	Septer
scap_gov.nist_USGCB-Windows-7.xml	Septer
u_microsoft_ie11_v1r3_stig_scap_1-0_benchmark.zip	Septer

4 items (1 selected)

SCAP File Name: U_Windows_7_V1R28_STIG_SCAP_1-1_Benchmark.zip
File Size: 1,969,076 bytes

XCCDF Benchmark Information
ID: Windows_7_STIG
Title: Windows 7 Security Technical Implementation Guide
Description: The Windows 7 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed from DoD consensus, as well as the Windows 7 Security Guide and security templates published by Microsoft Corporation. Comments or proposed revisions to this document should be sent via e-mail to the following address: disa.stig_spt@mail.mil.
Reference URL: http://iase.disa.mil
Publisher: DISA
Version: 1
Platform: cpe:/o:microsoft:windows_7
Definition Date: None found

Profile ID ▲	Profile Title
CAT_I_Only	CAT I Only
Disable_Slow_Rules	Disable Slow Rules
MAC-1_Classified	I - Mission Critical Classified
MAC-1_Public	I - Mission Critical Public
MAC-1_Sensitive	I - Mission Critical Sensitive
MAC-2_Classified	II - Mission Support Classified
MAC-2_Public	II - Mission Support Public
MAC-2_Sensitive	II - Mission Support Sensitive
MAC-3_Classified	III - Administrative Classified
MAC-3_Public	III - Administrative Public
MAC-3_Sensitive	III - Administrative Sensitive

11 items (0 selected)

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