

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

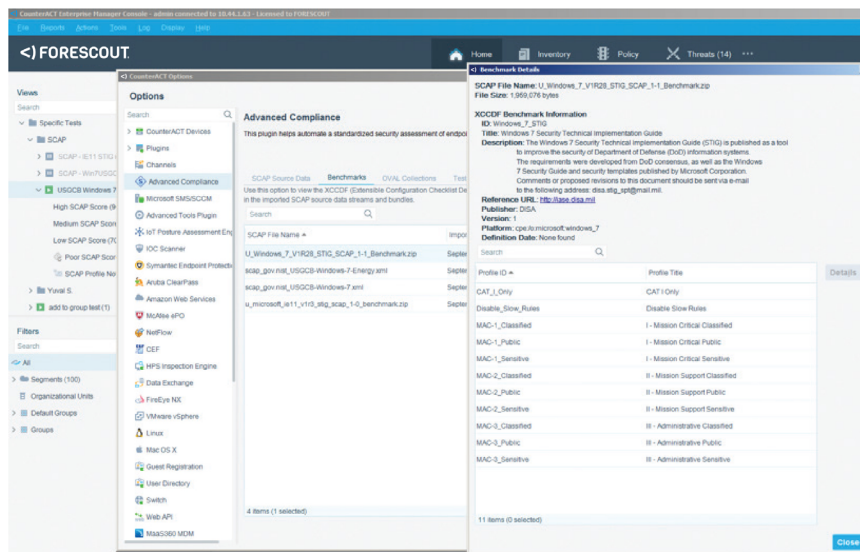
The Forescout solution can enhance security and help organizations comply with security audits by generating and emailing a detailed report of any endpoint that fails to meet a defined compliance level for any given SCAP benchmark. Equally important, the solution can quarantine all endpoints that fall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



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](https://forescout.com)

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 05_20