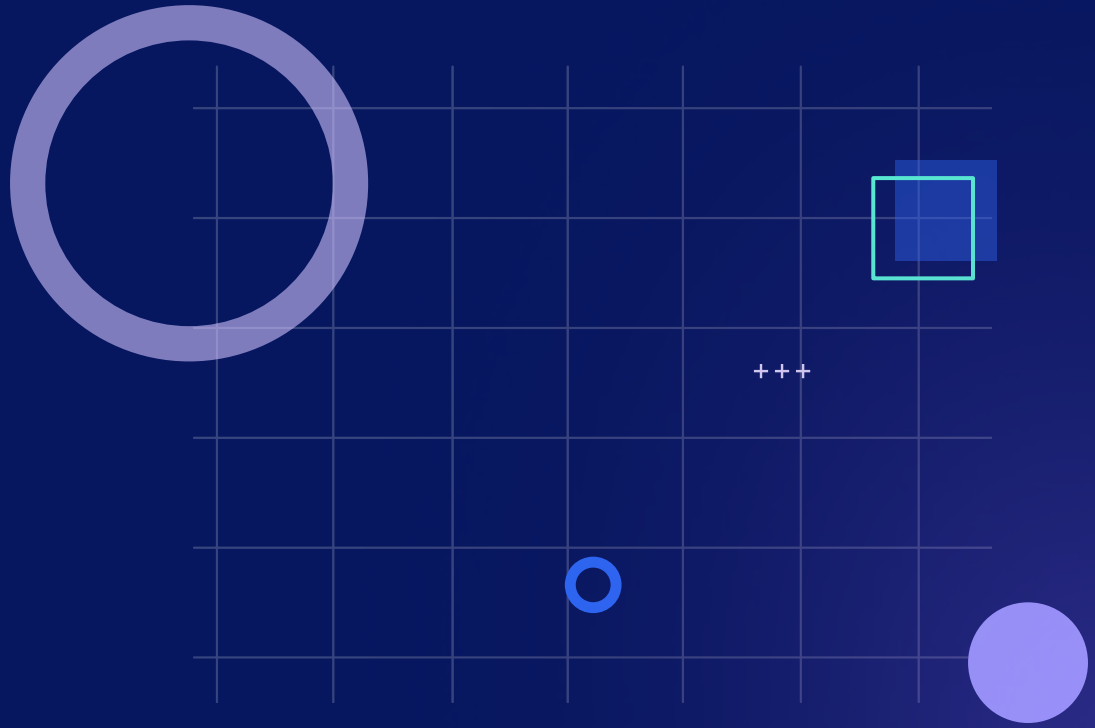
FORESCOUT

Remedio

Better Together

Better visibility,
more actionability



Joint Value Proposition

Forescout & Remedio share the view that strong security requires full asset visibility & automated remediation of compliance deviations. Integrating both solutions means:

- Stronger misconfiguration detection and response
- More host properties in Forescout to aid restriction, threat protection & policy refinement
- Automated access control, segmentation & compliance workflows (stopping lateral movement)
- Continuously assess all assets for compliance and compromise
- Immediately rollback changes

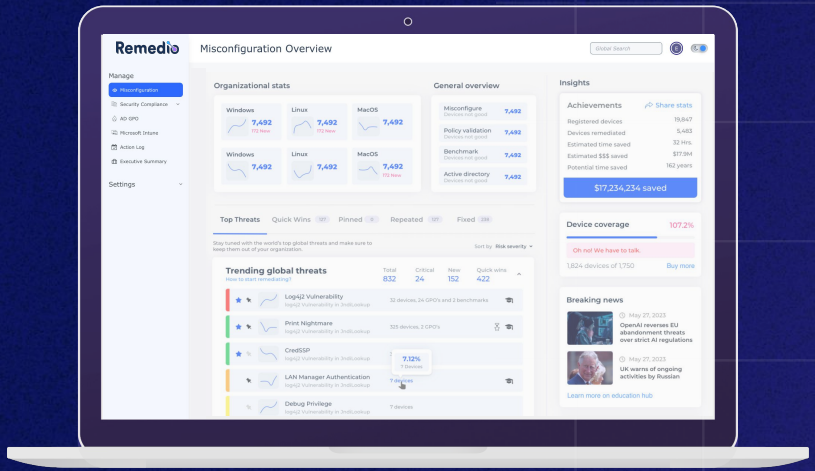
Automatic configuration risk detection and disruption-free remediation

Continuous inspection

Comprehensive visibility, ensure nothing is overlooked, monitor assets + AD/InTune/GPO.

Policy validation

Defining a policy does not guarantee it will be effective or enforced. Remedio does.



Dependency mapping

Understand change impact before you act. And if need be, rollback with a click.

Best practice benchmarking

Ease reporting , harden security, and ensure framework (NIST, CIS, MITRE, etc.) adherence.

Types of Vulnerabilities & Misconfigurations Covered

- General
- App & Internet Features
- Privilege Escalation
- SSH
- SMB and Sharing
- Databases
- Web Servers
- Credentials
- Obsolete Software
- Remote Code Execution
- Lateral Movement
- Domain Controllers - Security
- Legacy Protocols

Integration Use Cases

Remedio reports device misconfigurations and compliance to Forescout.

FORESCOUT verifies that a Remedio agent is installed on every device / triggers workflows to install if missing.

FORESCOUT reacts to Remedio-detected policy deviations with network controls (i.e. applies automated NAC & segmentation policies)

Device Information

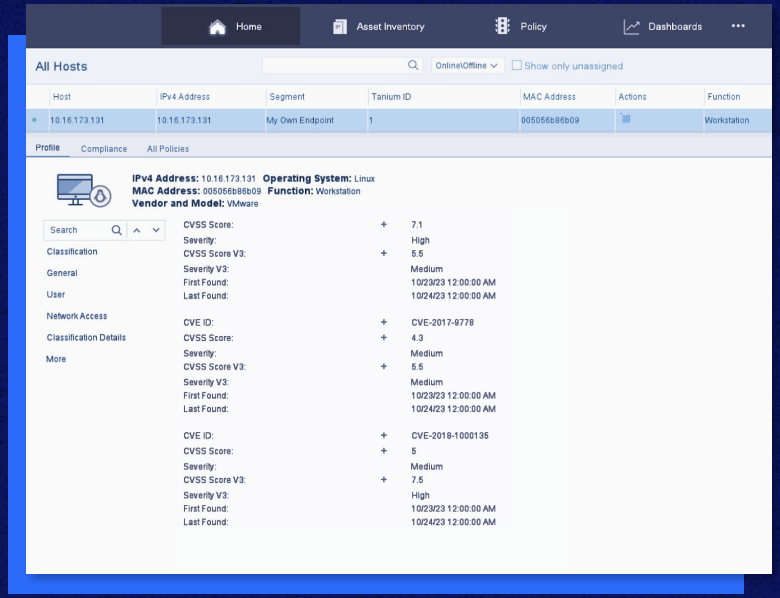
Enrichment powered by Remedio

More devices

- Corporate IT, Cloud, BYOD, guest, IoT, OT
- Managed & unmanaged
- Transient & stationary
- On & off premise
- Wireless, wired, remote/VPN/SASE access

More information per device

- Detailed system configuration info
- OS and app misconfigurations
- Device adherence to control standards (CIS1, CIS2, STIG)
- Unique asset identifiers
- Number of Critical, Medium, and Low severity items
- And much more...



Sensor Enablement

For corporate user, data center, and cloud assets — covering managed and unmanaged devices

Forescout validates

That all corporate IT devices have Remedio agent (scheduler) installed, running & up-to-date...

- Upon connection
- Continuously

Forescout initiates

Automatic user notification and remediation of non-compliant devices...

- Utilizing Remedio where present
- Where absent, triggering installation & onboarding workflows

Together, we optimize

Security for endpoint and network policy compliance via...

- Remedio context-awareness & secure configuration assurance
- Forescout network controls

Automated Network Policy

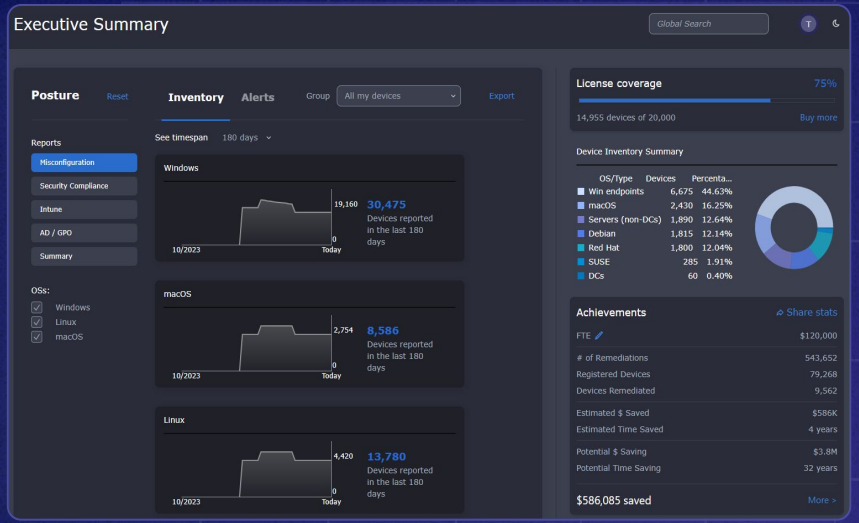
React to misconfigurations and compliance requirements with Forescout policy-driven network controls. Respond to threats with automated network access and segmentation policies.

Create targeted Forescout policies
Utilizing both Remedio and Forescout data.

Use Forescout as central policy decision point
Triggered by real-time Remedio & Forescout data.

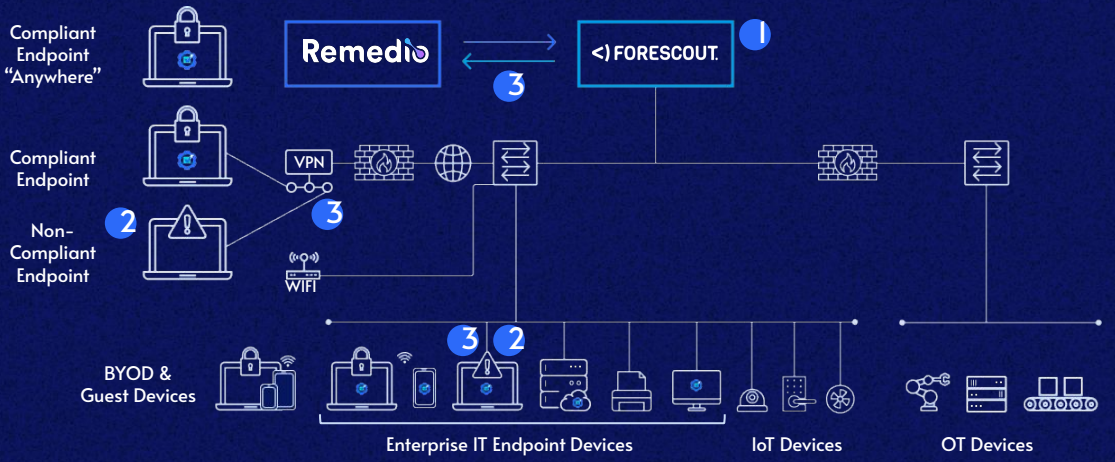
Optimize policy enforcement & threat response
By leveraging Forescout automation with multiple layers of heterogeneous enforcement points.

Increase compliance while reducing workload
Automation of policy-driven actions.



How The Integration Works

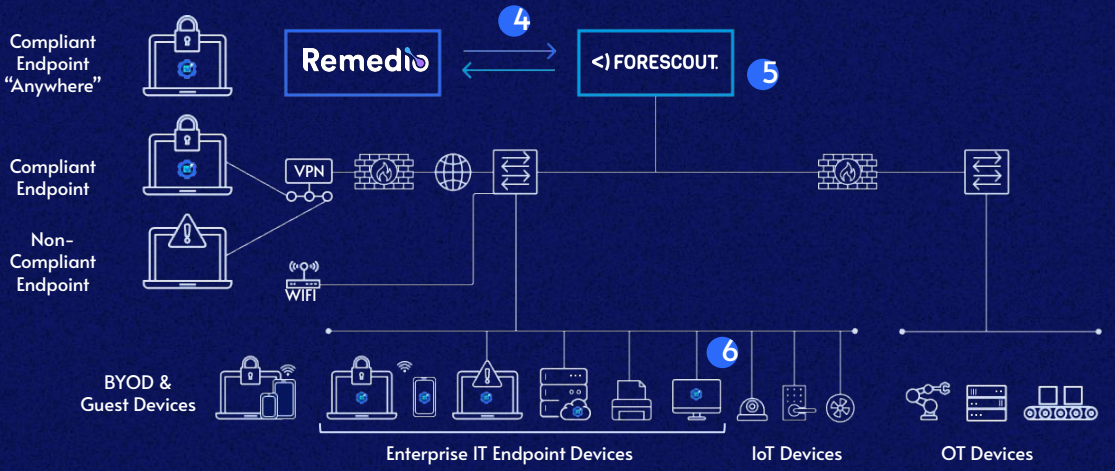
Automate real-time, asset intelligence and security governance to increase operational resilience, asset protection and threat defense at enterprise scale



1. Forescout discovers, identifies and assesses all connected assets/devices
2. Forescout detects non-compliant devices that need the Remedio scheduler
3. Forescout facilitates remediation via Remedio, installing the scheduler and restricting network access as needed

How The Integration Works

Automate real-time, asset intelligence and security governance to increase operational resilience, asset protection and threat defense at enterprise scale



4 Remedio feeds Forescout managed endpoint data, including those off-network, for unified visibility and management

5 Forescout utilizes combined real-time asset intelligence to enforce network access, segmentation, and threat response policies

6 Remedio detects changes to endpoint compliance and triggers Forescout to take network-based action

Key Benefits

Reduce response and resolve times (MTTR) for security issues

Shrink the attack surface — locking down risks related to misconfigurations and policy deviations

Enhance security and compliance governance — automating policies between endpoints and network layer

Accelerate adoption of Zero Trust Architecture (ZTA) to meet mandates and compliance.