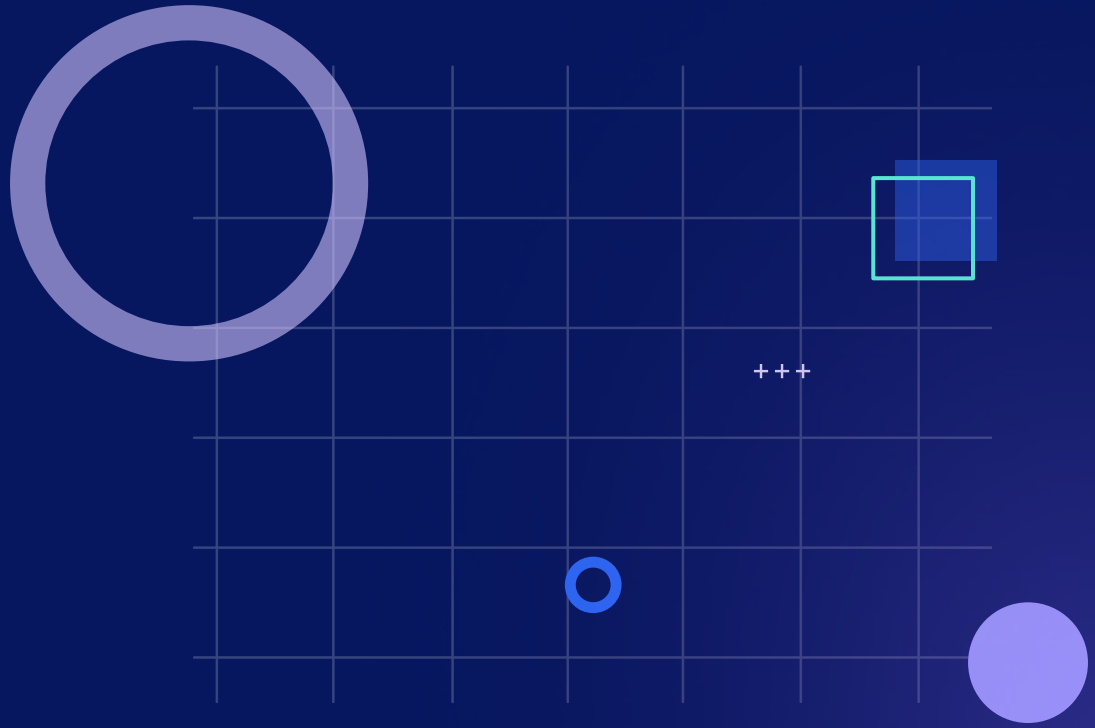
FORESCOUT

CYTPOL

Better Together

Better visibility,
more actionability



Joint Value Proposition

Forescout & GYTPOL 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

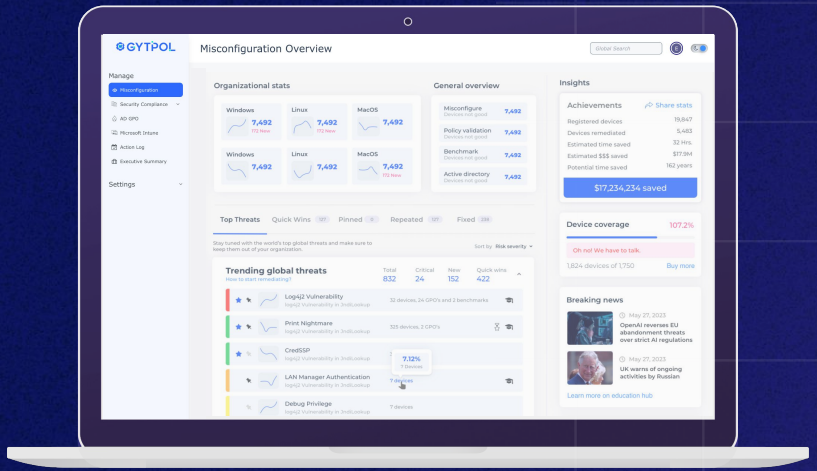
Automatic misconfiguration detection and risk-free remediation

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. GYTPOL 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.

Integration Use Cases

GYTPOL reports device misconfigurations and compliance to Forescout.

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

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

Device Information

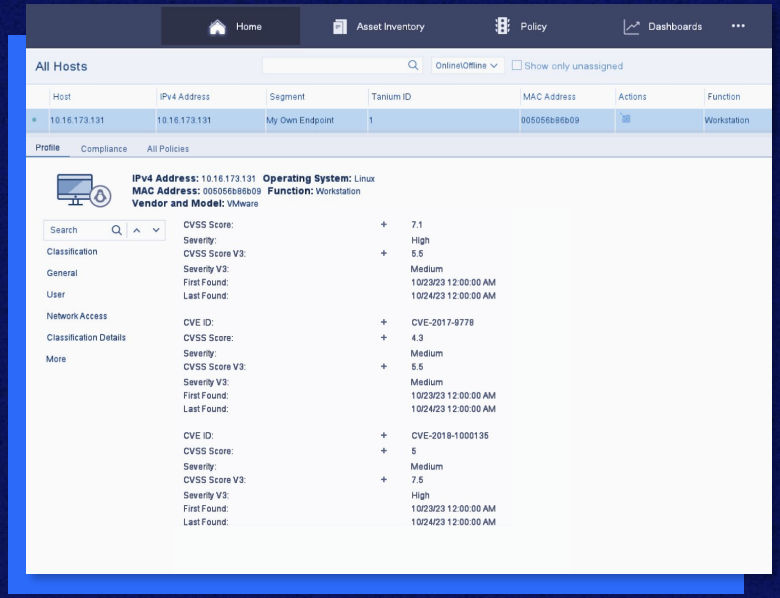
Enrichment powered by GYTPOL

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...



Agent Enablement

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

Forescout validates

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

- Upon connection
- Continuously

Forescout initiates

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

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

Together, we optimize

Security for endpoint and network policy compliance via...

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

Automated Network Policy

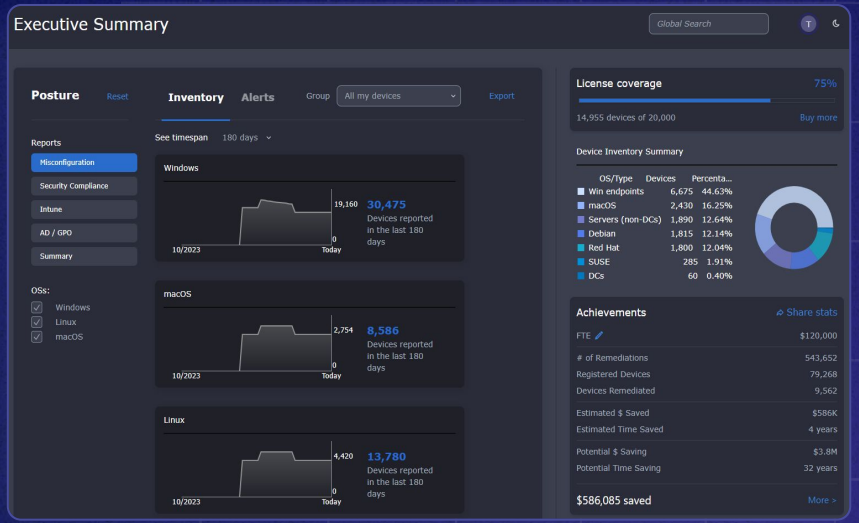
React to misconfigurations and compliance requirements with Forescout policy-driven network controls. Respond to threats with automated network access and segmentation policies.

Create targeted Forescout policies
Utilizing both GYTPOL and Forescout data.

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

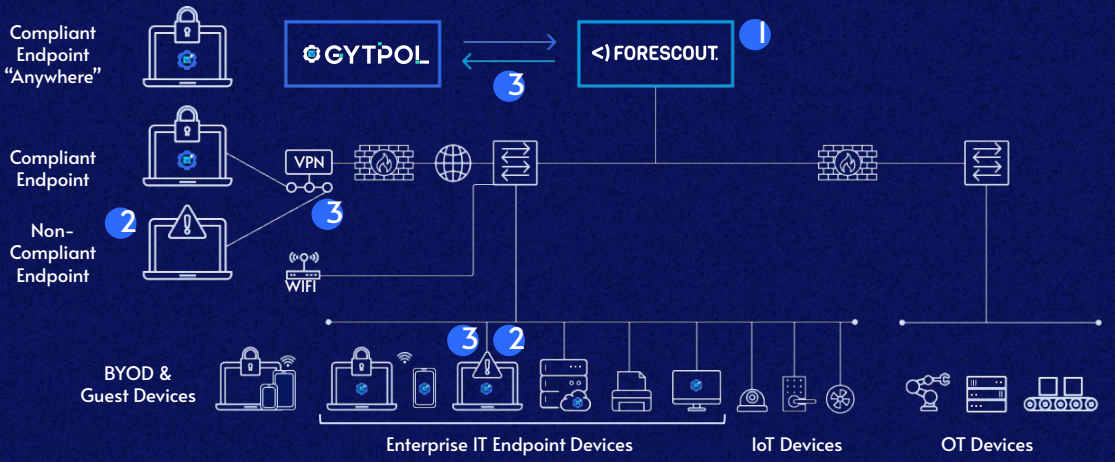
Optimize policy enforcement & threat response
By leveraging Forescout automation with multiple layers of heterogeneous enforcement points.

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



How The Integration Works

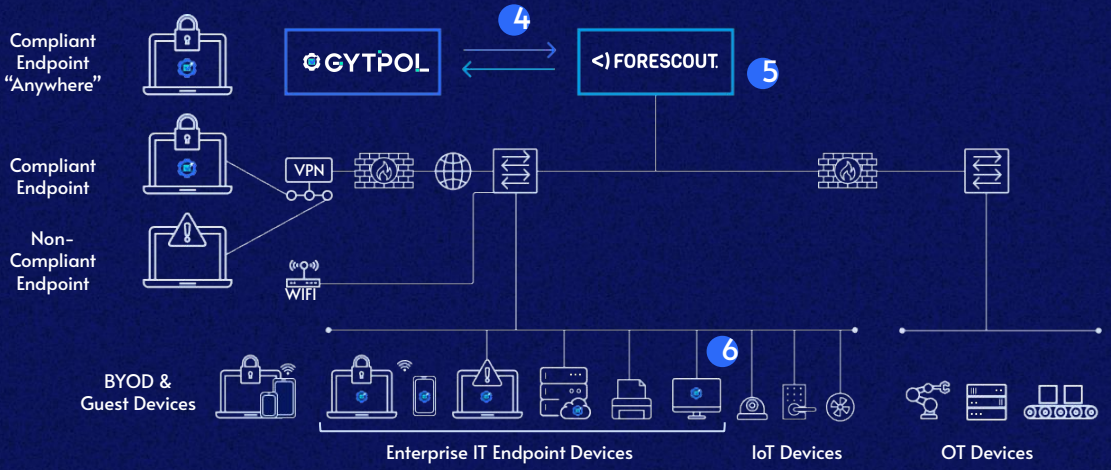
Automate real-time, asset intelligence and security governance to increase operational resilience, asset protection and threat defense at enterprise scale



1. Forescout discovers, identifies and assesses all connected assets/devices
2. Forescout detects non-compliant devices that need the GYTPOL scheduler
3. Forescout facilitates remediation with GYTPOL to install the scheduler and limit network access until compliant

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 GYTPOL feeds Forescout managed endpoint data, including those off-network, for unified view and to apply policies against

5 Forescout utilizes combined real-time asset intelligence to enforce network access, segmentation and threat / non-compliance response policies to mitigate risk

6 GYTPOL endpoint compliance change triggers Forescout policy 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.