GYTPOL Technical Overview

Proactively Secure Your IT Environment.
Continuously. Automatically.

GYTPOL

Introduction

Misconfigurations are one of the most overlooked yet critical threats to enterprise security. GYTPOL is an advanced security platform that identifies, validates, and remediates misconfigurations across endpoints, servers, and network infrastructure.

It delivers continuous visibility into your security posture, automatically enforces policy-based remediations, and ensures compliance without disrupting operations. With GYTPOL, organizations turn misconfiguration management into a proactive strength that improves security, reduces risk, and streamlines compliance.

Key Capabilities at a Glance

- Misconfiguration Detection
- Continuous Compliance Monitoring
- Active Directory Security Assessment (Low Privilege)
- GPO and Intune Policy Validation
- Custom Compliance and Benchmarking
- Auto Remediation with Safe Revert
- Lightweight Scan Execution (no 24/7 agents)
- Cross-Platform Coverage (Windows, Linux, macOS)
- Application Control
- Network Device Configuration Validation
- Integration with Leading IT and Security Tools
- SaaS and On-Premises Deployment Options

Platform Capabilities

1. Automated Detection and Remediation:

- Complete Security Posture Visibility: Continuously scans endpoints, servers, and networking devices to identify misconfigurations, policy violations, and risky deviations.
- Context-Aware Risk Scoring: Each misconfiguration is scored by business impact and technical severity, so teams can focus on the most critical issues first.
- Real-Time Monitoring: Detects configuration changes as they occur and prevents drift from secure baselines.
- Unauthorized Change Detection: Identifies unexpected or unauthorized configuration changes across your environment.
- Safe Revert for Every Change: Every remediation action includes a built-in revert option, allowing teams to safely roll back changes if needed. This ensures control and flexibility, even in automated environments.

2. Compliance Without Guesswork:

- Framework Coverage Out of the Box: Automatically maps your environment to leading compliance frameworks including CIS, NIST 800-53, NIST CSF, HIPAA, PCI-DSS, DORA, and Cyber Essentials.
- Gap Identification and Reporting: Highlights where your organization falls short and generates audit-ready reports.
- Continuous Enforcement: Ensures that configurations remain compliant, not just during audits but every day.

3. GPO and Intune Policy Validation:

- GPO Health Analysis: Identifies GPOs that are broken, misconfigured, or not linked properly.
- Advanced Policy Checks: Detects issues related to loopback, item-level targeting, GPP, and OU filtering.
- Reliable Enforcement: Applies secure settings even when GPOs fail, ensuring no endpoint is left exposed.
- Intune Device Validation: Highlights drift and gaps in policy enforcement across Intune-managed environments.

4. Custom Compliance Benchmarks:

- Policy Definition: Create and customize internal security and compliance policies tailored to your organization's needs.
- Automated Enforcement: GYTPOL continuously applies and maintains your custom policies across all devices.
- Drift Detection: Identifies and alerts on deviations from defined benchmarks in real time.
- Flexible Scope: Apply rules to specific devices, groups, or environments without affecting unrelated systems.

5. Active Directory Security Assessment:

- Runs with Low Privilege: Performs comprehensive AD assessments using low-level credentials. No need for Domain Admin rights or elevated permissions.
- Domain Risk Visibility: Identifies hidden risks such as outdated objects, misconfigured trusts, and policy conflicts.

6. Network Device Configuration Analysis:

- Covers Your Infrastructure: Analyzes routers, switches, and firewalls for misconfigurations that could expose your network.
- Device-Specific Guidance: Provides tailored remediation steps based on device model and vendor.
- Key Risk Detection: Detects use of default credentials, weak protocols, and other high-risk misconfigurations.

7. Intelligent Remediation and Auto-Healing:

- Automated Remediation: Fixes misconfigurations based on policies you control, without manual effort.
- Cross-Platform Remediation: Works across Windows, Linux, and macOS systems.
- Built-In Drift Prevention: Maintains secure configurations across updates, reboots, and user actions.
- Revert Option for Every Fix: Every remediation includes a one-click rollback to ensure safe recovery.
- Attack Surface Optimization: Understands how misconfigurations interact and recommends fixes that reduce overall exposure.

8. Application control:

- Policy-Based Restrictions: Define which applications are allowed or blocked based on organizational requirements.
- Risk and CVE Assessment: Evaluates applications against known vulnerabilities (CVEs) and risk scores to prioritize remediation.
- Automated Remediation: Removes / Un-install or disables non-compliant or vulnerable applications without manual intervention.
- Continuous Monitoring: Tracks application changes in real time to prevent policy drift and exposure.

9. Lightweight Architecture:

- No Persistent Agents: Uses native schedulers to operate quietly in the background.
- Minimal System Impact: Execution footprint is under 5MB, with negligible CPU or memory usage.
- Silent and Efficient: Runs once a day without disrupting users or system performance.

10. Seamless Ecosystem Integration:

- Easy Integrations: Connects with ServiceNow, Splunk, CrowdStrike, ForeScout, and other platforms.
- Automation Ready: Pushes alerts, status updates, and remediations into your existing SOC or ITSM tools.
- Open API: Enables full access to configuration data and reports for custom dashboards and scripts.

II. Flexible Deployment Options:

- SaaS or Self-Hosted: Choose the model that fits your security and compliance needs.
- Fast Time to Value: Setup is quick and simple, with no complex rollout or agent deployments.
- Scalable by Design: Easily supports thousands of endpoints and multi-tenant environments.

Why Customers Choose GYTPOL

- Detects and fixes misconfigurations automatically
- Maintains continuous compliance
- Keeps endpoints secure even when GPO fails
- Uses no agents and runs silently
- Provides a safe revert option for every action
- Works across platforms at enterprise scale