XYPRO®
Mission Critical Security

XYGATE SecurityOne®

Ransomware Protection, Compliance Automation, and Zero Trust Security for HPE Nonstop

Overview

XYGATE SecurityOne (XS1) is a unified security platform for HPE Nonstop systems that combines ransomware detection, compliance automation, and Zero Trust enforcement in a single cyber resilience solution. XS1 continuously monitors system activity, detects advanced threats, enforces policy controls, and delivers contextualized alerts to help you protect critical assets, meet regulatory requirements, and harden your environment—without complexity or blind spots.

Ransomware Detection

XS1 focuses on behaviors, not signatures—identifying unauthorized modifications, suspicious access patterns, and stealthy "low-and-slow" campaigns that mimic legitimate activity. By establishing baselines and system behavior, it exposes anomalies aligned with Zero Trust principles and flags threats early.

Key Features

- **Ransomware & malware detection** based on behavior, not signatures
- **File Integrity Monitoring (FIM)** for PCI DSS and critical data protection
- **Zero Trust access controls** with least privilege and anomaly detection
- **Real-time monitoring** with contextual alerts
- **Monitoring for CLIMs (Cluster I/O Module) and Windows consoles**
- **Flexible deployment:** cloud, on-premises, or virtual

Key Benefits

- **Protects HPE Nonstop** From modern ransomware attacks
- **Automates and simplifies compliance reporting**
- **Reduces Mean Time to Detect (MTTD)** and respond to threats
- **Reduces SIEM costs** by lowering data volume up to 90%
- **Boosts security teams' productivity** with contextual alerts
- **Streamlines forensic investigations** with full evidence trails
- **Delivers complete visibility** into system, user, and network behavior
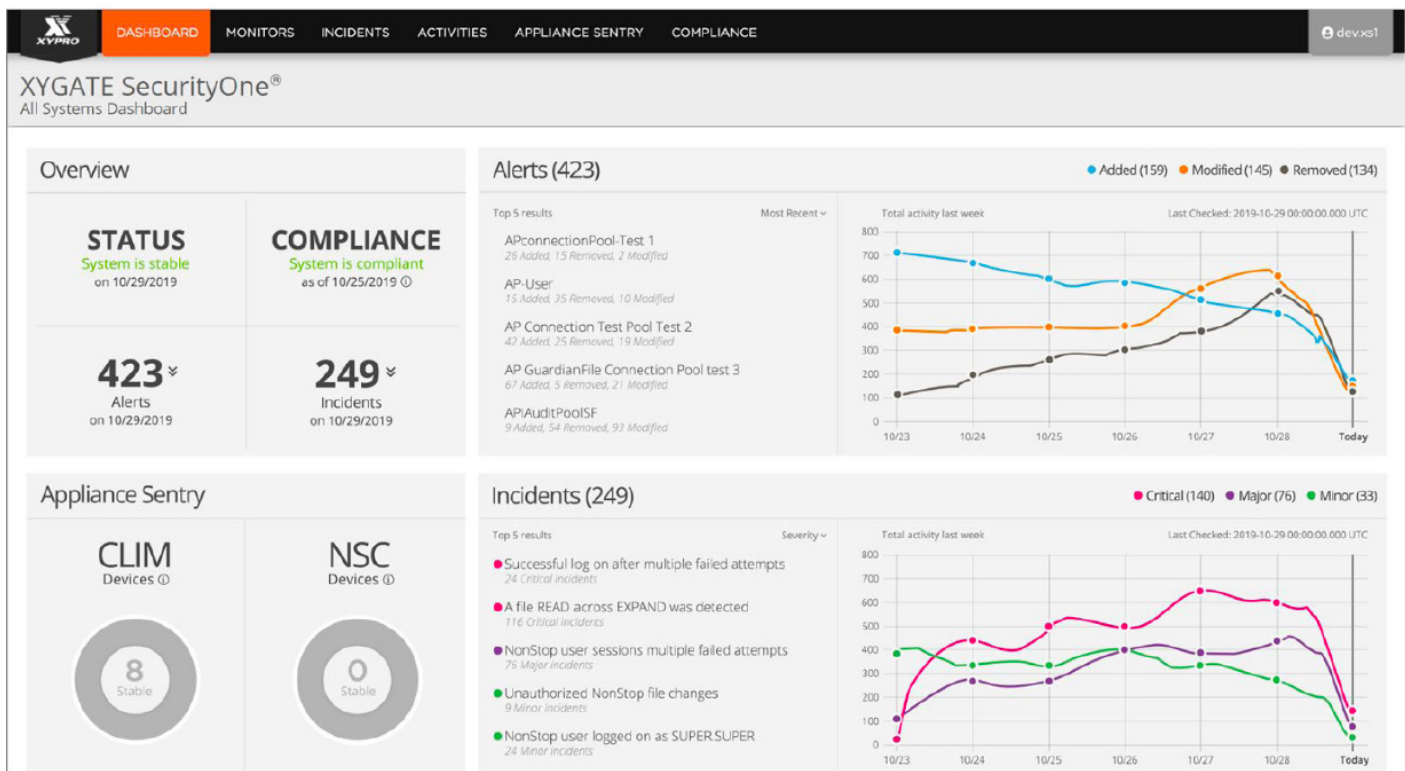
Compliance Automation

XS1 maps controls, monitors for gaps continuously, and automates evidence capture and reporting. This shortens audit preparation, reduces manual effort, and lowers the risk of non-compliance across evolving PCI DSS requirements.

Zero Trust Security

The platform continuously profiles user activity and correlates deviations from role or historical baselines. Privileged mis use and lateral movement are ide ntified quickly, enabling decisive act ion when behavior changes.

File Integrity Monitoring

XS1's File Integrity Monitoring (FIM) safeguards PCI DSS compliance and protects critical data by continuously scanning file systems for unauthorized changes, additions, or deletions. Security teams are alerted in real time, enabling rapid response to both insider threats and external attacks targeting sensitive files.

By integrating FIM into its unified security platform, XS1 not only detects unauthorized changes but also correlates them with other security events for a complete view of potential threats. This automated, standards-based approach meets PCI DSS requirements for monitoring critical system files, reduces manual oversight, streamlines audits, and strengthens overall cyber resilience.

www.xypro.com

SIEM Optimization & Integration

On HPE Nonstop, Zero Trust means no request is trusted automatically—every request must be verified. XS1 enforces this by checking each access attempt in real time against user role, behavior, and data sensitivity, ensuring users only get the access they need. For high-risk actions, it can require extra approval, block sensitive tools, or limit access paths. If risk increases mid-session, XS1 can instantly quarantine, block, or end access—delivering active control, not just passive monitoring.

XS1 also reduces standing privileges by granting just-in-time access and restricting lateral movement. All privileged sessions can be monitored down to keystrokes, ensuring full accountability. Security teams get clear, SIEM-ready incidents tied to policies, providing solid evidence for PCI DSS and Zero Trust compliance.

Make your SIEM smarter – send it signals, not noise.

Beyond access control, XS1 makes your SIEM smarter and more cost efficient by acting as a Nonstop-native analytics layer. Instead of flooding Splunk or other SIEMs with thousands of raw events, XS1 collects and correlates unique Nonstop telemetry—file changes, privileged activity, console data, XYGATE events—and outputs enriched, deduplicated incidents. This reduces noise, speeds investigations, and provides higher-fidelity detections.

Organizations typically see up to a 90% reduction in SIEM ingestion volume, which directly lowers costs while improving visibility and detection accuracy. Integration is straightforward (syslog/CEF/JSON/HTTPS), and incidents arrive audit-ready, ensuring your SIEM remains the system of record.

Choose the Best Bundle

Bundle	Included Solutions
Suite +	XYGATE Access Control, XYGATE Object Security, XYGATE Compliance PRO, Compliance Bundle
Compliance	FIM Bundle, XYGATE Compliance PRO
FIM	Intellligent File and System Integrity Monitoring

"We evaluated every Nonstop security solution—and XYGATE SecurityOne was in a league of its own—Global CISO, Fortune 500 Enterprise"

Contact Information

✉ sales@xypro.com   🌐 www.xypro.com

XYPRO®
Mission Critical Security