XYGATE® SecurityOne®

PATENTED

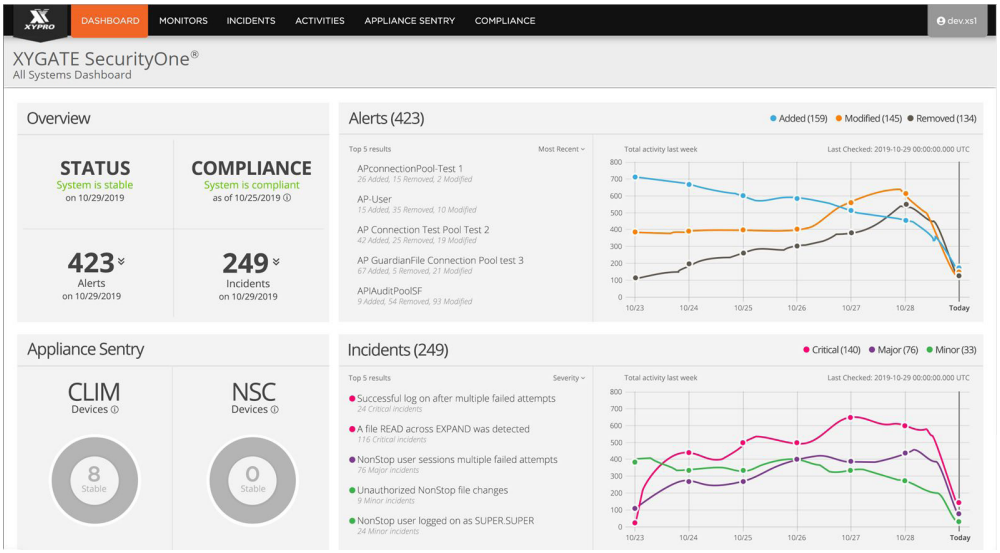
Ransomware Protection and Compliance Automation

KEY BENEFITS

- Protect against ransomware and malware
- Automate Compliance Reporting
- Improve Security Staff Productivity
- ***NEW*** Deploy in the Cloud, On-premise or as a Virtual Appliance

KEY FEATURES

- File and System Integrity Monitor
- Real-Time Threat Detection and Alerting
- Appliance Monitor for NonStop CLIMs and Windows Console
- Modern Browser Interface
- Simplified Forensic Investigations
- Analyze Keystroke Patterns to provide contextual insights
- ***NEW*** Integration with ETI-NET Backbox
- Visibility into System, Network and User Activity
- User Behavior Profiling



Ransomware Protection

XYGATE SecurityOne® (XS1) is a cutting-edge ransomware protection, zero trust security, and compliance automation platform for HPE NonStop Systems. XS1 provides real-time detection of ransomware-specific Indicators of Compromise and suspicious activity, enabling immediate response to potential threats. Leveraging patented contextualization technology, XS1 gathers and analyzes data from multiple sources, using advanced security intelligence algorithms to correlate events and provide a comprehensive security incident view. This empowers security teams to proactively identify and address security events before they escalate into breaches, ensuring continuous compliance and enhanced cyber resilience.

Reduce Mean Time to Detection

Security teams require enhanced visibility and proactive data analysis to accelerate detection and response times, preventing potentially catastrophic ransomware breaches.

Currently, the mean time to detect a cybersecurity incident is ***over 200 days***, due to reliance on manual detection and investigation methods. Attackers exploit this delay by disguising their actions as normal user behavior, enabling them to move undetected through systems. Faster detection is critical for disrupting these hidden threats before they cause significant damage.

PCI DSS 4.0 Compliance

XS1 automates PCI DSS 4.0 compliance, reducing the complexity and manual effort typically required to meet regulatory standards. XS1 continuously monitors your environment, identifying and alerting on compliance gaps in real time. With built-in reporting and automated evidence collection, XS1 ensures that your organization stays compliant with the latest PCI DSS requirements, including advanced controls for data protection and threat detection.

The value of XS1 lies in its ability to simplify compliance management, reduce audit preparation time, and minimize the risk of costly non-compliance penalties.

XYPRO
Mission Critical Security

XYGATE®
SecurityOne®

Ransomware Protection and Compliance Automation

> “We took a look at every possible NonStop risk management solution for our compliance needs and XYGATE SecurityOne was by far above-and-beyond the others.”
>
> -Global CISO

File Integrity Monitoring

File integrity monitoring (FIM) is a crucial aspect of maintaining PCI DSS compliance and protecting critical data from unauthorized changes. XS1 continuously monitors file systems for any unauthorized modifications, additions, or deletions, ensuring that security teams are alerted to potential threats in real-time. This proactive monitoring helps detect both insider threats and external attacks aimed at manipulating sensitive files.

By incorporating FIM into its comprehensive security platform, XS1 ensures that organizations meet PCI DSS requirements for monitoring critical system files. The platform not only identifies unauthorized changes but also correlates these events with other security data, providing a holistic view of potential threats and ensuring compliance with PCI mandates. This automated approach to file integrity monitoring reduces manual oversight, streamlines audit processes, and strengthens overall cybersecurity resilience.

Zero Trust Security

In a Zero Trust security framework, Low & Slow attacks pose a unique challenge by mimicking legitimate behavior with minimal activity, allowing them to bypass traditional security measures without violating system policies. XYGATE SecurityOne is designed to identify these subtle threats by detecting specific event patterns and analyzing their context, revealing suspicious activities that traditional solutions might overlook.

Through continuous profiling of user behavior and anomaly detection, XYGATE SecurityOne can identify compromised accounts. For example, if a system administrator’s behavior significantly deviates from established norms, it may indicate malicious activity or a compromised account. User behavior baselines are established based on roles or by analyzing typical activity patterns, ensuring security teams can respond to potential threats in real time while aligning with the principles of Zero Trust security.

SIEM Integration

Many organizations view SIEMs such as Splunk and others as the ultimate solution for threat detection and alerts. However, SIEMs are only as effective as the data they receive—simply put, they can't detect what they don’t know. XS1 collects data from logs, agents, and unique sources specific to XYPRO that are not available to SIEMs. By forwarding XS1-generated incidents to a SIEM, organizations can significantly enhance the quality of SIEM analysis.

Most SIEM vendors charge based on the volume of data ingested, but XS1 is licensed per system rather than by event volume. Since XS1 sends already-contextualized incidents, it transmits far fewer events, which can reduce SIEM license fees. For example, 10 HPE NonStop events sent directly to a SIEM would result in 10 event charges. By processing those events through XS1, a single, contextualized incident is forwarded, potentially reducing SIEM license fees by 90% for NonStop events.

XYPRO Mission Critical Security

XYPRO Headquarters
4100 Guardian St., Suite 100
Simi Valley, California 93063 USA

XYPRO.com

USA / Canada:	+1 805 583 2874
Asia Pacific:	+61 3 9008 4283
EMEA:	+44 207 099 4176
Ibero América:	+52 55 4170 8281
Japan:	0066 33 821682