XYGATE® SecurityOne®

PATENTED

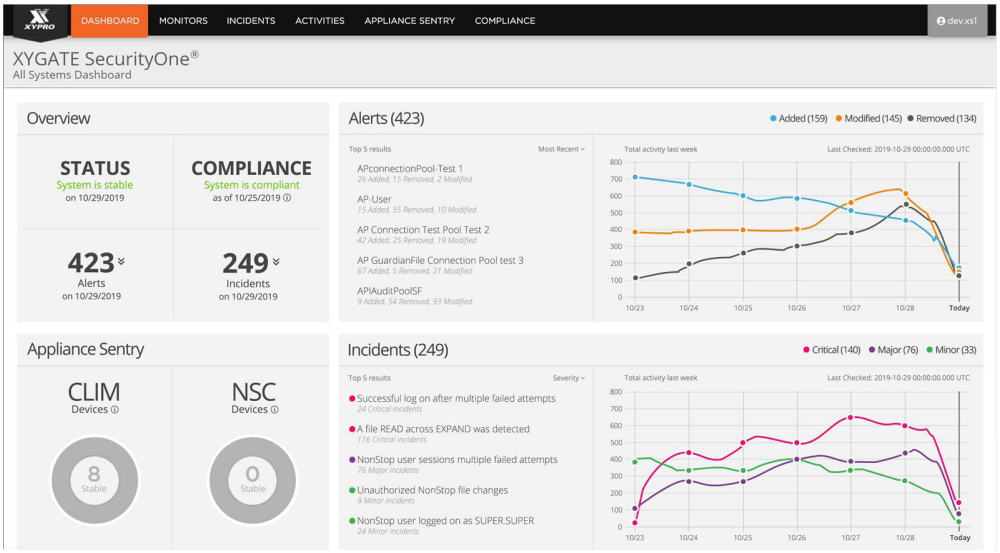
Risk Management & Threat Detection

KEY BENEFITS

- Reduce Incident Costs by 80%
- Simplify Compliance Reporting
- Improve Security Staff Productivity
- Save Money on SIEM License Fees

KEY FEATURES

- File and System Integrity Monitor
- Real-Time Threat Detection and Alerting
- Appliance Monitor for NonStop CLIMs and Windows Console
- Contextualized and Prioritized Incidents
- Modern Browser Interface
- Automated PCI DSS Compliance Management and Reporting
- Simplified Forensic Investigations
- Interpret Keystroke Activity for Context
- *NEW* Integrate Multiple NonStop and Linux Event Sources
- Visibility into System, Network and User Activity
- User Behavior Profiling



NonStop Security Analytics

XYGATE SecurityOne® is a next-generation risk management and security analytics platform for the HPE Integrity NonStop Server. XS1 actively detects NonStop specific Indicators of Compromise and alerts on suspicious activity in real time.

Our patented contextualization technology gathers data from multiple disparate sources and uses specialized security intelligence algorithms to correlate, contextualize and analyze events to display a detailed security incident picture in real time. Security operators can detect actionable security events before they become a breach.

Reduce Mean Time to Detection

Security teams need greater visibility and proactive analysis of their data for faster detection and response times to avoid a catastrophic security breach.

The mean time to detect a cyber security incident is currently over 180 days. This is mostly due to manual detection and discovery methods used to investigate security incidents. Attackers know that blending in their activities as innocuous user behavior is great camouflage as they move around the system.

Multi-Platform Risk Management

XYGATE SecurityOne integrates NonStop, Linux, Windows and other application data sources to paint a complete picture of the security environment. With summary/detail dashboards and an easy to use browser interface, XYGATE SecurityOne manages security configurations, measures and enforces compliance and policies on a global level, takes the guesswork out of audit and forensic investigations and much more.

This combination of system hardening, user profiling, application security and threat intelligence greatly reduces the likeliness of costly post-breach data recovery actions.

XYPRO
Mission Critical Security

XYGATE® SecurityOne®

Risk Management & Threat Detection

> "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

Detecting the Low and Slow

Low & Slow attacks utilize low volumes of activity that appear legitimate. By not violating system security policies, they pass undetected, flying below the radar of traditional detection strategies and solutions.

XYGATE SecurityOne detects specific event patterns and evaluates their context to identify suspicious activity that current solutions are not geared to detect. By identifying anomalous behavior, XYGATE SecurityOne is able to "profile" and alert on compromised accounts. Acceptable user behavior can be determined based on roles or measured by profiling activity. For example, if one system administrator's behavior is significantly different to all other administrators, it may be that person is performing malicious activity or their account has been compromised.

It's Not That SIEMple

Many organizations believe SIEMs are the ultimate authority on security threat detection and alerts. The reality is SIEMs are only as intelligent as their input. In short, SIEMs don't know what they don't know.

XS1 consumes data via logs, agents and other sources unique to XYPRO and not available to SIEMs. XS1 generated incidents can be forwarded to SIEMs, improving the quality of their analysis.

Most SIEM vendors base license fees on the volume of data they consume. XS1 is licensed per server rather than event volume. Because XS1 is sending the SIEM already-contextualized events, it sends far fewer. Hence, the use of XS1 can reduce your SIEM license fees.

For example, 10 HPE NonStop events forwarded to a SIEM result in a 10-event SIEM fee. Those same 10 events processed first by XS1, will generate a single, contextualized Incident that forwards to the SIEM. This example would result in a 90% cost savings on SIEM license fees associated with 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