SECURONIX™ | CISCO

SOLUTION BRIEF

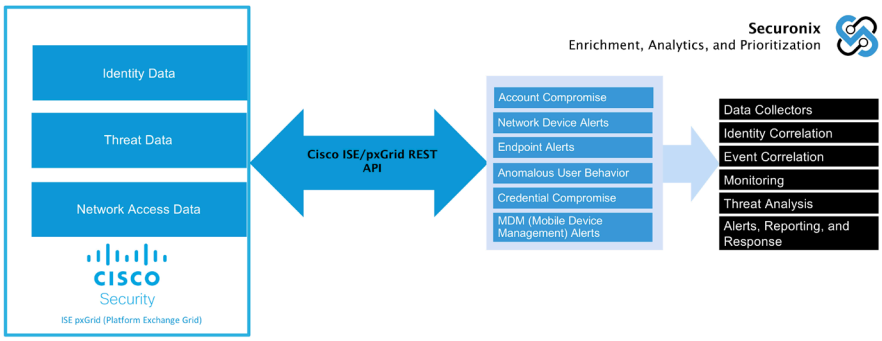
Integrated Security Visibility with Securonix and Cisco pxGrid

The cybersecurity landscape has become more complex. Hackers continue to innovate, and business technologies continue to generate increasing amounts of data. This makes legacy security monitoring solutions obsolete as they struggle with an inability to scale and weak rule-based threat detection techniques.

The Securonix platform delivers unlimited scale, powered by advanced analytics, behavior detection, threat modeling, and machine learning. It increases your security through improved visibility, actionability, and security posture, while reducing management and analyst burden.

With the Cisco Platform Exchange Grid (pxGrid), multiple security products share data and work together. This open, scalable, and Internet Engineering Task Force (IETF) standards-driven platform helps to automate security event integration across multiple products.

Integrating the Securonix platform and Cisco ISE pxGrid forms a powerful, centralized security solution. Securonix leverages Cisco pxGrid's cross-platform network security events for identity, threat, and access behavior analytics. Securonix further enriches network security events with machine learning analytics, identifies policy violations, and empowers your security operations team to take automated or manual threat response actions.



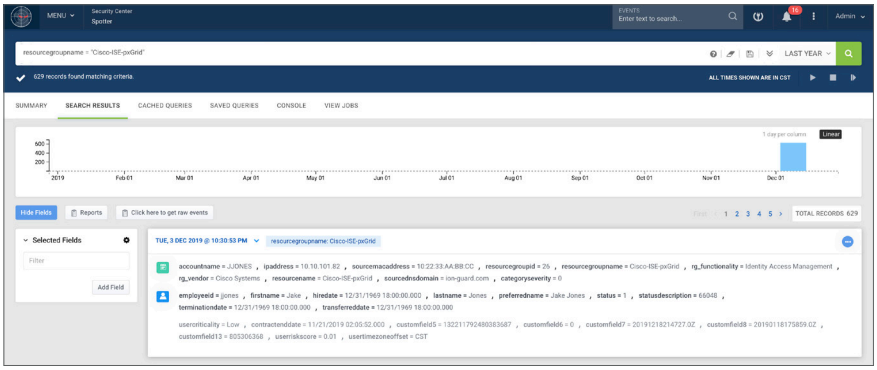
Solution Benefits

- Integrate alerts from Cisco pxGrid's cross-platform network security event identification.
- Gain visibility and insight into user activity across your environment.
- Securonix analyzes a series of events over time using threat chain models to surface the highest risk events.
- Automate incident response and reduce mean time to respond with access to real-time actionable intelligence.
- Multi-attack monitoring coverage, utilizing detailed event processing for comprehensive security.
- Enrich data with additional context from on-premises data sources and other applications for threat modeling.

Better Attack Understanding With Multi-Source Alerts

The Securonix platform captures events from Cisco pxGrid, utilizing the pxGrid REST API to ingest events from endpoints, MDM solutions, network devices as well as other integrated security alerts. Post capture, these events are correlated and identified according to their source, enabling better attack understanding.

With comprehensive event coverage, Securonix integrates the complete range of threat information from the Cisco pxGrid platform, utilizing the information for both threat identification and context definition, as well as creating threat models using existing threat events.



Securonix Spotter search with Cisco ISE pxGrid

Context-Driven Threat Modelling

The Securonix platform adds useful information to all ingested ISE pxGrid events. Each event is linked to other related events that may have occurred elsewhere within the enterprise environment, creating a consolidated threat model that tracks a threat as it evolves through various threat stages. The platform allows actions to be taken to mitigate, prevent, or remediate threats as appropriate, and provides recommendations where possible.

Focus on Visibility and Information Access

Besides tracking threats, a key benefit of the Securonix platform is the detailed visibility into every aspect of enterprise security provided by the web interface. The dashboard provides a bird's eye view of current environment status, while an easy to access event search widget allows quick event access from the first page.

How it Works

- Cisco pxGrid enables cross-platform collaboration to monitor network access, threat detection, and enforce access.
- Securonix behavior analytics enriches Cisco pxGrid events and baselines normal behavior patterns in your user data in order to detect account misuse and anomalous behaviors.
- Using threat chain modelling, Securonix brings to light the highest risk events in your organization.
- The Securonix intelligent orchestration engine centralizes operations by streamlining incident response and automation.

About Cisco

Cisco security products work together to deliver effective network security, incident response, and heightened IT productivity through automation. Our security innovations protect customers, employees, and brands by providing highly secure firewalls, web, and email services. Simplifying the complexity of network security, keep your business more secure, and make IT more productive with Cisco security services and solutions. For more information visit www.cisco.com.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000