SECURONIX™ | CISCO

SOLUTION BRIEF

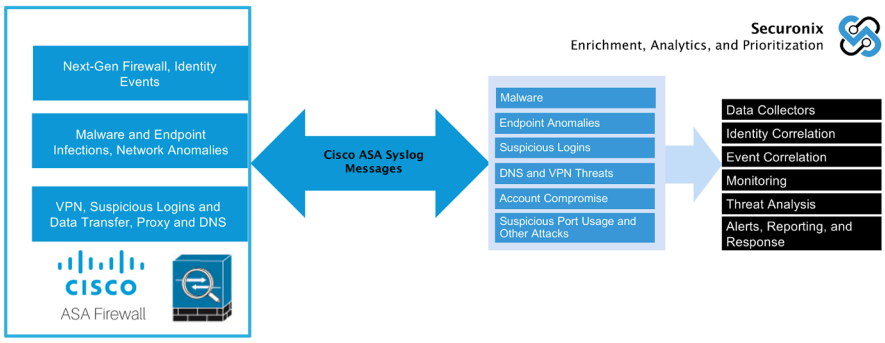
Application, Network, and Endpoint Visibility and Protection with Securonix and Cisco ASA

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.

A next-generation firewall (NGFW), Cisco ASA software is the core operating system that powers the Cisco ASA family of security devices. It delivers enterprise-class firewall and VPN capabilities and integrates with Cisco Intrusion Prevention System (IPS), Cisco Cloud Web Security (formerly ScanSafe), Cisco Identity Services Engine (ISE), and Cisco TrustSec for comprehensive security solutions that meet continuously evolving security needs.

When integrated, the Securonix platform receives Cisco ASA security events, enriches them with user and entity behavior analytics, and delivers that security context to the security operations center (SOC) analyst. Furthermore, Securonix Security Orchestration and Response (SOAR) empowers SOC analysts to quickly respond to threats.



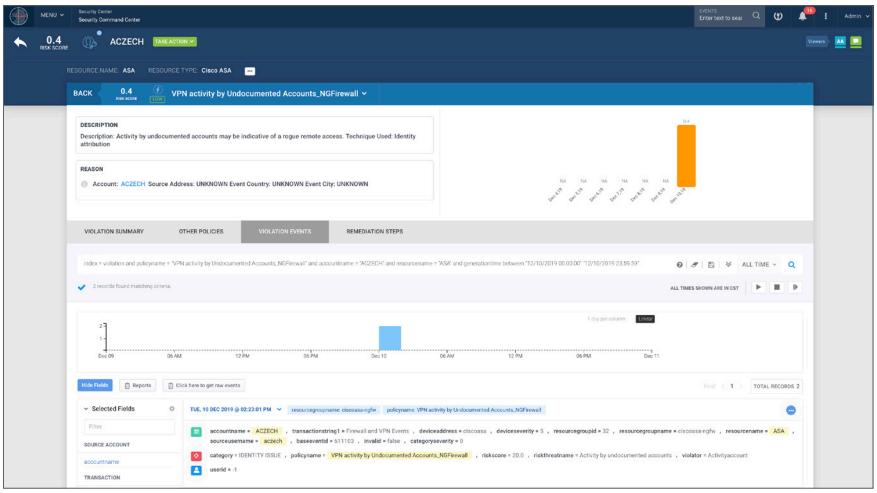
Solution Benefits

- Integrate Cisco ASA NGFW alerts to identify threats to your network security.
- Gain visibility and insight into user activity across your environment.
- Securonix analyzes a series of events over time using threat chain models in order to surface the highest risk events beyond the most recent incident.
- Automate incident response and reduce mean time to respond with access to real-time actionable intelligence.
- Multi-attack monitoring coverage, utilizing detailed syslog processing for comprehensive security.
- Enrich data with additional context from on-premises data sources and other applications for threat modeling.
- MITRE ATT&CK compliance with threat chain methodology that is in line with MITRE's own staged threat framework.

Multi-Attack Event Coverage

The Securonix platform captures events from multiple Cisco ASA modules. This includes VPN and NGFW events such as repeated failed logins, account sharing, high vulnerability count, and data sharing over FTP/SMB ports, as well as other possible indicators of compromise (IOC) such as rare server traffic and rare port usage. It also captures file-based events such as rare file type usage as well as network traffic events such as traffic to new or rare domains and beaconing attempts.

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



Context-Driven Threat Modelling

The Securonix platform adds useful information to all ingested Cisco ASA events. Each event is linked to related events that occur elsewhere within the enterprise environment, creating a consolidated threat model that identifies a threat as it evolves through various threat stages. The platform allows you to take actions at each stage to mitigate, prevent, or remediate as appropriate, and also provides recommended actions when 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. The platform dashboard provides a bird's eye view of the current environment status, while an easy to access event search widget allows you to quickly access additional event information from the first page.

How it Works

- Cisco ASA delivers real-time, continuous threat analysis. It protects, blocks, and remediates malware and cybersecurity threats.
- Securonix integrates Cisco ASA alerts along with other environmental alerts, adding context and correlating user behavior.
- Using threat chain modelling, Securonix brings to light the highest risk events in your organization.

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