Palo Alto Networks and Securonix

Security Analysis

Benefits of the Integration

- Accurately detect external and internal threats with SIEM and UEBA technologies that use patented machine learning algorithms.
- Enjoy rapid deployment and quick time to value with threat models delivered as out-of-the-box applications and built-in connectors.
- Leverage blazing-fast threat hunting using natural language search with Securonix Spotter.

The Challenge

Businesses of all sizes face an increasingly complex threat landscape and a shortage of cybersecurity professionals to deal with it. Cloud applications, the internet of things (IoT), and an increasingly diverse security vendor architecture only complicate the situation. With the limited security analyst resources available and the ever-changing threat landscape, organizations must use an integrated platform to keep up with threats.

Securonix Security Operations and Analytics Platform

The Securonix Security Operations and Analytics 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 burdens.

With a proven rapid time to value because of its analytics capability and cloud strategy, as well as its integrated security orchestration, automation, and response (SOAR) feature set, the Securonix Security Operations and Analytics Platform simplifies your cybersecurity operations, lowering the average time it takes to detect, respond to, and stop threats. With native support for thousands of third-party vendors and technology solutions, the Securonix platform simplifies security operations, events, escalation, and remediation. It easily scales from startups to global enterprises while providing the same fast security ROI as well as ongoing, transparent, and predictable cost.

Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere. Next-Generation Firewalls inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and Securonix

The integration between Palo Alto Networks Next-Generation Firewalls and the Securonix Security Operations and Analytics Platform combines powerful protection and threat detection with machine learning analytics. The Next-Generation Firewalls send critical activity data to Securonix for further analysis, allowing joint customers to correlate the rich data from their Next-Generation Firewalls with other third-party sources in the Securonix environment for advanced threat detection.

Use Case No. 1: Monitor Off-Network User Behavior

Challenge

Any activity outside your controlled network is in a blind spot. A user's day-to-day pattern of behavior on the secure network can look normal for their job role, but it's difficult to have the full context of their behaviors beyond your network.

Solution

By leveraging security log data from the Palo Alto Networks Next-Generation Firewalls, Securonix actively monitors users and their behavior across your systems, on or off the network, to gain deeper clarity into users' behavior with Securonix machine learning threat models.

Use Case No. 2: Better Utilize Analyst Skills

Challenge

Relying too much on manual response to threats detected by your security tools and security analysts reduces the productivity of your personnel and their ability to focus on proactive threat hunting.

Solution

Securonix security orchestration and response can run manual or automated playbooks that integrate with Palo Alto Networks Next-Generation Firewalls to query necessary firewall details as well as block ports, IP addresses, and URLs. Once threats are detected, Securonix can integrate across your existing security tools to respond to threats, freeing up your security professionals to focus on other high priorities.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics SaaS Cloud platform, Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

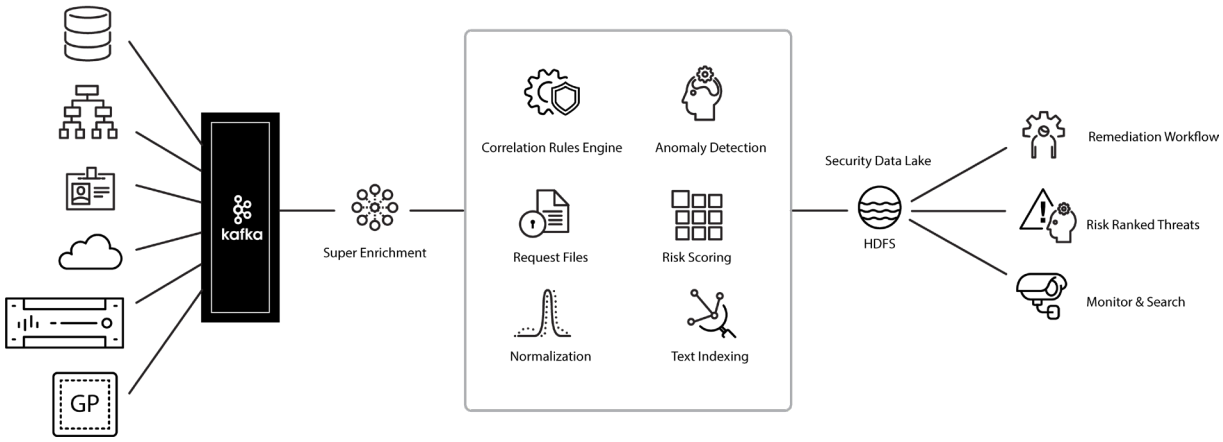

Figure 1: Palo Alto Networks and Securonix integration

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

securonix-tpb-042420