# Palo Alto Networks and SafeBreach

### Benefits of the Integration

Together, Palo Alto Networks and SafeBreach help you:

- Ensure protection against threats by validating that Palo Alto Networks Panorama security controls are correctly deployed and optimally configured.
- Reduce the time it takes to detect, prevent, and respond to attacks.
- Minimize your overall attack surface by optimizing Panorama security controls based on real-life attack scenarios.

## The Challenge

Security operations teams understand how critical it is to maintain effective network security controls, in large part because configuration and policy drift can occur at any time. However, most security teams lack the tools to accurately and continuously test and visualize their security posture. SafeBreach provides continuous validation of security controls and rapid remediation for Palo Alto Networks Panorama™ network security management.

## SafeBreach

The integration of SafeBreach—the leading breach and attack simulation (BAS) solution—and Panorama enables security professionals to simulate attack methods against their deployed network security controls. Simulation results are correlated and enriched with network-related security data. This continuously validates an organization's security posture against cyberattacks and automates the combined processes of breach investigation, remediation, and prevention.

## Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls (NGFWs) 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.

Panorama manages Palo Alto Networks NGFWs. While some security deployments can often overload IT teams with complex security rules and data from multiple sources, Panorama offers easy-to-implement, centralized management features that provide insight into network-wide traffic and threats.

## Palo Alto Networks and SafeBreach

### Use Case No. 1: Validate Firewall Configurations and Policies

#### Challenge

Organizations cannot always tell if their configurations and policies are optimized to protect their networks.

#### Solution

SafeBreach's patented simulation technology and the most comprehensive Hacker's Playbook in the industry allow you to continually, safely test and report on the readiness of network infrastructure against real-life cyberattacks. You can simulate attack methods by threat groups; tactics, techniques, and procedures (TTPs); specific malware; or your own custom methods. The ability to visually display attack paths and security gaps makes it faster and easier to analyze, prioritize, and continuously improve your network security posture. SafeBreach enables security teams to:

- Automatically correlate simulation results against Panorama to quickly identify any configuration or policy gaps.
- Analyze which attack methods were stopped, prevented, detected, or missed.
- Identify network paths to quickly highlight where data can be exfiltrated from the organization.
- Align to the MITRE ATT&CK® framework and better evaluate overall organization readiness as well as security posture.

## Use Case No. 2: Prioritize and Remediate Vulnerabilities Identified by Simulated Attacks

### Challenge

Organizations can find it difficult to identify, much less prioritize and remediate, cybersecurity vulnerabilities.

### Solution

SafeBreach shares mitigation insights for network access and network inspection security controls and configurations with Panorama. As a result, security and network teams can holistically and effectively remediate their organization's critical exposures before attacks target them. Users can resolve numerous simulations simultaneously, using detailed mitigation data collected from Panorama.

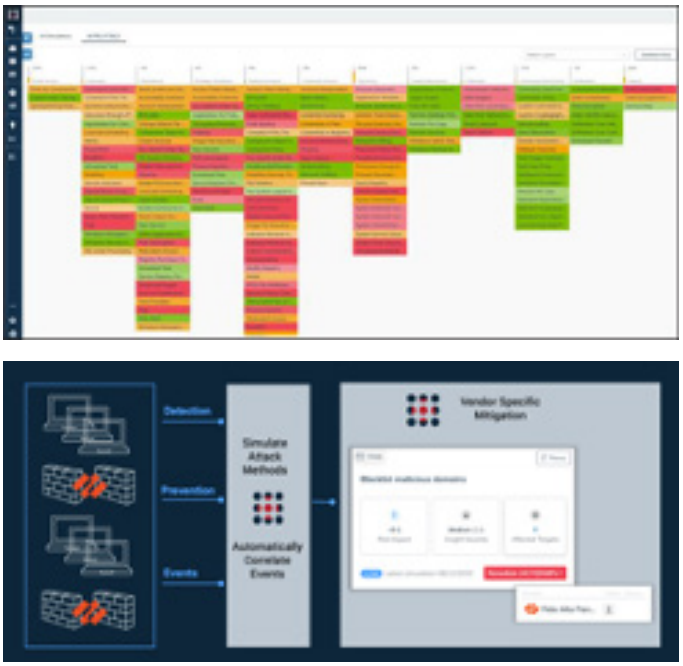


**Figure 1:** Palo Alto Networks and SafeBreach integration—use case 1

## About SafeBreach

SafeBreach simulates thousands of attack methods to provide a hacker's view of an organization's security posture, paint a picture of the security exposures to an enterprise and prioritize remediation efforts, securing against TTPs. SafeBreach Labs is dedicated to threat research from real- world investigation with the most extensive breach and attack methods in the industry with over 10,000 attack methods and growing. SafeBreach is privately held and is headquartered in Sunnyvale, California with an office in Tel Aviv, Israel.

For more information, visit www.safebreach.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.

paloalto NETWORKS

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