



# Palo Alto Networks and SafeBreach

## Benefits of the Integration

1. *Validate that Palo Alto Networks Panorama security controls are deployed correctly and configured optimally, ensuring protection against known threats.*
2. *Reduce the time to detect, prevent, and respond to attacks.*
3. *Reduce overall attack surface by optimizing Palo Alto Networks Panorama security controls based on real-life attack scenarios.*

## The Challenge

Security Operations teams understand how critical it is to maintain the effectiveness of their network security controls, in large part because configuration and policy drift can occur at any time. 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.

## SafeBreach

The integration of SafeBreach, the leading Breach and Attack Simulation (BAS) solution, and Palo Alto Networks® Security Operating Platform, which prevents successful cyberattacks through intelligent automation, enables security professionals to simulate attack methods against their deployed network security controls. The simulation results are correlated and enriched with network-related security data. This continuously validates an organization's security posture against cyber-attacks and automates the combined processes of breach investigation, remediation, and prevention.

## 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 SafeBreach

## Use Case No. 1

### Challenge

Validate next-gen firewall configurations and policies are set to best protect your enterprise.

### Solution

SafeBreach's patented simulation technology and the most comprehensive Hacker's Playbook in the industry allows you to continually and safely test and report on the readiness of network infrastructure against real-life cyber-attacks. You can simulate attack methods by threat groups, TTPs, specific malware or create your own attack method. The capability 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 and security posture

## Use Case No. 2

### Challenge

Easily prioritize and remediate all vulnerabilities and issues that are identified by simulated attacks.

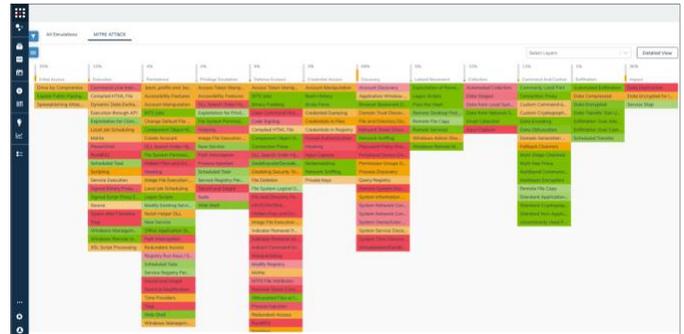
### Solution

SafeBreach mitigation insights for network access and network inspection security controls and configurations can be shared with Palo Alto Networks Panorama. As a result, security and network teams can holistically and effectively remediate the organization's critical exposures. Users can resolve numerous simulations simultaneously, using detailed mitigation data collected from Palo Alto Networks Panorama.

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](http://www.paloaltonetworks.com)



SafeBreach MITRE ATT&CK heat map of simulation results based on risk per tactics and techniques.

## 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](http://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 fore-front 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](http://www.paloaltonetworks.com).

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. panw-palo-alto-networks-and-xx-tb-022620