PALO ALTO NETWORKS AND AREA 1

Preemptive, Comprehensive Protection from Phishing Attacks

Benefits of the Integration

The combined Area 1 Security and Palo Alto Networks offering:

- Deploys an integrated solution in minutes.
- Protect across all attack vectors—network, web, and email traffic.
- Stops web-based phishing, such as credential harvest and dropper attacks.
- Thwarts network phishing activity, including attacker lateral movement, command-and-control traffic, and data exfiltration.
- Facilitates security orchestration with automated MineMeld updates.

Phishing attacks, reportedly used in 91% of successful data breaches,[1] continue to evade security defenses. Detecting and protecting from these attacks is complicated by the fact that the attacks are often multi-vector, meaning that they impact email, web, and network traffic. Further complicating defense, these attacks are dynamic—hackers often launch and shut down phishing sites and payloads in a matter of hours to evade detection.

Phishing Attack Vectors

Attacks often start by tricking a victim into unknowingly downloading malware that is hidden in an email file attachment or on a webpage. Once the victim's device is infected, a hacker can gain access to connected networks and systems. From there, the attacker can establish communication with external phishing sites to exfiltrate data and download more malware, further infecting systems to achieve their malicious objectives. To protect from attacks, organizations need phishing security solutions that can detect and block threats across all attack vectors, including email, web, and network.

Phishing Sites and Campaigns Are Dynamic

When executing phishing campaigns, hackers often first compromise trusted websites and email servers or establish imposter websites and email accounts, weeks or even months before a planned attack. After setting up a phishing site, hackers launch and shut down attacks in a matter of hours. The dynamic nature of phishing sites makes legacy security defenses—which mostly rely on threat intelligence extracted from active, launched attacks—less effective.

Early Visibility into Phishing Sites and Campaigns

To protect from phishing attacks, cybersecurity solutions, including email, web, and network defenses, need early insight into phishing sites before campaigns launch and attacks are active. Fortifying defenses with security technology that hunts for malicious sites before attacks launch during the weeks and months hackers are establishing or compromising websites in preparation of launching an attack, can provide the early visibility and threat indicators necessary to protect from impending attacks. Arming email, web, and network cyber defenses with early insight into phishing sites and payloads enables these defenses to more effectively detect and block phishing email, malicious web downloads, attacker movement through your network, command-and-control (C2) communication, and data exfiltration to external sites. With early visibility to phishing sites and payloads before attacks launch, security defenses can prevent cyber breaches.

1. "The Ultimate List Of Cyber Security Statistics For 2019," PurpleSec, accessed December 18, 2019, https://purplesec.us/resources/cyber-security-statistics.

Area 1 Horizon Anti-Phishing Service

Area 1 Security offers an anti-phishing cloud service that stops email, web, and network phishing attacks that other security technologies miss. Area 1's innovative technology crawls the web continuously and proactively, discovering phishing campaigns and infrastructure before attacks launch. On average, we detect malicious sites and payloads a full 24 days before industry benchmarks.

By proactively hunting for new phishing infrastructure as it's set up, Area 1 Security has early visibility into phishing sites, payloads, malware, and compromised servers before campaigns launch. The resulting insight and threat information powers the Area 1 Horizon™ anti-phishing service to detect and block phishing threats that other security technologies miss. The service is easy to deploy and integrates with existing email, web, and network security infrastructure to provide an added layer of anti-phishing protection that effectively stops attacks.

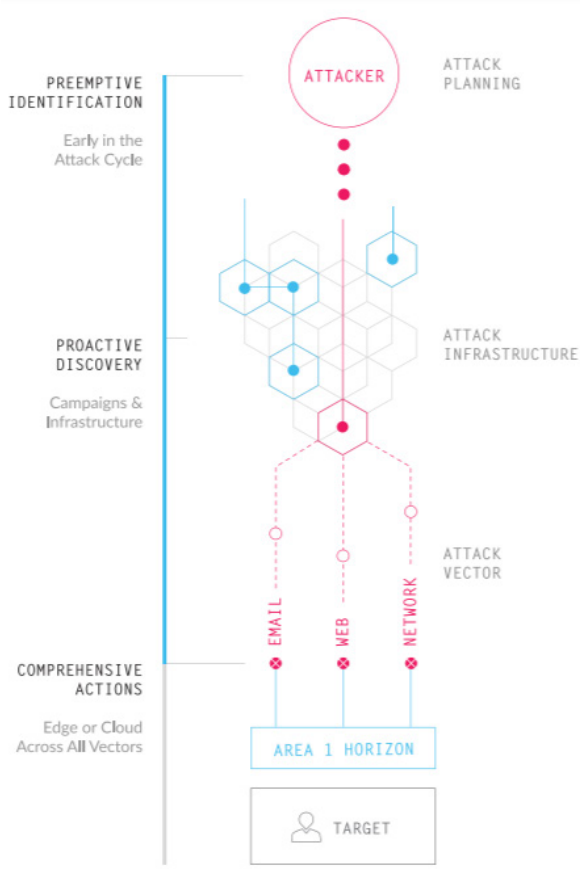

Figure 1: Area 1 Horizon in your infrastructure

Palo Alto Networks

The Palo Alto Networks Security Operating Platform® prevents successful cyberattacks through intelligent automation. It combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle.

Area 1 Security and Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls integrate with the Area 1 Horizon anti-phishing service to fortify network defenses and protect against targeted phishing attacks. The service automatically updates Palo Alto Networks firewalls and Dynamic Block Lists in Panorama™ network security management with emerging phishing site and campaign indicators to enable more effective protection from targeted attacks. The combined solution results in better detection and blocking of web-based phishing activity, such as preventing access to and downloads from previously unknown phishing sites. The combination also fortifies detection and prevention of network phishing activity including attacker lateral movement through victim networks, phishing, command-and-control traffic, and data exfiltration. The Area 1 service also integrates with Palo Alto Networks MineMeld™ threat intelligence syndication engine to provide security operations center (SOC) teams with enhanced visibility of phishing attack activity. Automated phishing detection and rule set updates to MineMeld facilitate efficient response and analytics for SOC teams.

About Area 1 Security

Backed by top-tier investors, Area 1 Security is led by security and data analytics experts from NSA, USCYBERCOM, Cisco/IronPort and FireEye, who realized the pressing need for a proactive solution to targeted phishing attacks. Area 1 Security is working with organizations that implement the most sophisticated security infrastructures. These companies include F500 banks, insurance providers, retail organizations, and health care providers. Our mission is to preempt and stop targeted phishing attacks at their very outset and significantly improve the customer's cybersecurity posture. To learn more, please visit www.area1security.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.

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

palo-alto-networks-and-area1-tpb-122319