AREA 1

FORTINET

AREA 1 SECURITY AND FORTINET SOLUTION BRIEF

Defeat phishing attacks with a preemptive and comprehensive solution

Fortify Network Defenses and Stop Phishing Attacks

Close the Phishing Security Gap.

Area 1 Security plus Fortinet:

- Deploy and integrate in minutes
- Protects 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
- Automated updates facilitate security orchestration

Even the best conventional security defenses are proving unable to stop phishing attacks, which still cause 95 percent of cybersecurity-related data breaches and financial loss. The fact that the attacks are often multi-vector, hitting email, web, and network traffic, makes finding and defending against them all the more challenging and complex. And because the attacks are dynamic, launching and shutting down phishing sites and payloads within hours, defenses often lack the timely threat insight that's vital to effective protection.

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 web page. Once the victim's device is infected, a hacker can gain access to their network 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 in advance of a planned attack. After setting up a phishing site, hackers launch and shut down their attacks in a matter of hours. The dynamic nature of phishing sites makes legacy security defenses less effective, since those defenses mostly rely on threat intelligence extracted from active, launched attacks.

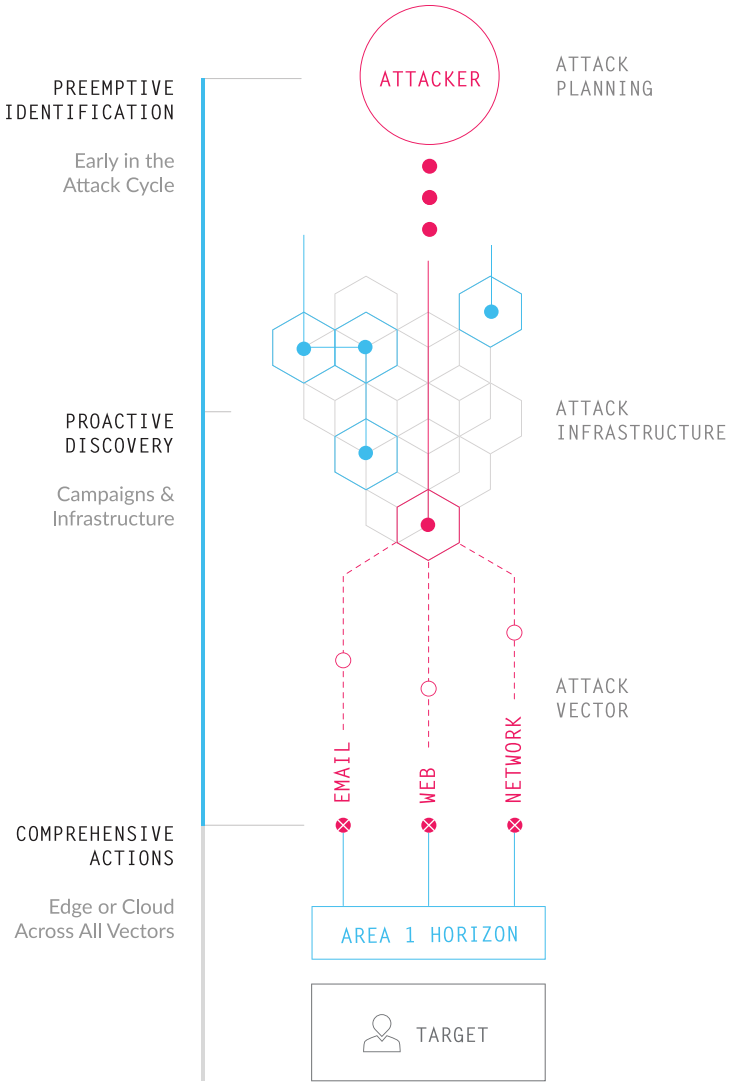
EARLY VISIBILITY INTO PHISHING SITES AND CAMPAIGNS

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 to prepare for launching an attack—can provide the early visibility and threat indicators necessary to protect from impending attacks. Arming email, web, and network cyberdefenses 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 communication, and data exfiltration to external sites. With early visibility into phishing sites and payloads before attacks launch, security defenses can prevent cyber breaches.

AREA 1 HORIZON™ ANTI-PHISHING SERVICE

Area 1 Security's anti-phishing cloud service 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, Area 1 Security is the only security provider that offers early visibility into phishing sites, malware payloads, and compromised servers in advance of the 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.



FORTIGATE AND AREA 1 HORIZON INTEGRATION STRENGTHENS PHISHING DEFENSE

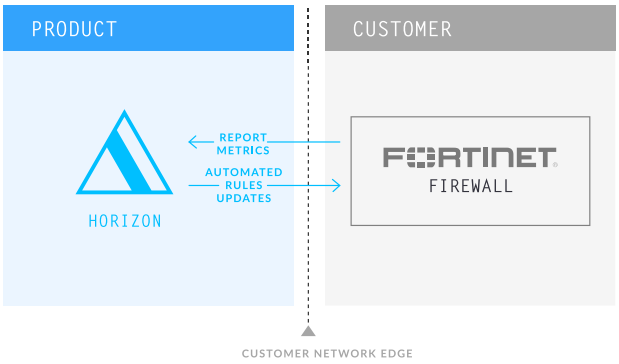
Fortinet FortiGate firewalls integrate with the Area 1 Horizon anti-phishing service to enhance network and web defenses and protect customers from targeted phishing attacks.

The Area 1 Horizon service integrates quickly and easily with Fortinet's firewalls, updating them automatically with emerging phishing infrastructure and campaign indicators to enable advanced, effective protection from targeted attacks.

This combined solution results in superior FortiGate detection and blocking of web-based and network-based phishing activity. It prevents access to, and downloads from malicious phishing sites and stops attacker lateral movement through victim networks, preventing phishing command-and-control communication and data exfiltration.

AREA 1 HORIZON: FORTINET FIREWALL INTEGRATION

Fortify Firewall Phishing Protection, Easy Deployment



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 FORTINET

The Fortinet FortiGate network security platform provides high performance, layered security services and granular visibility for end-to-end protection across the entire enterprise network. Innovative security processor (SPU) technology delivers high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine to help protect against malware hiding in SSL/TLS encrypted traffic. The platform also leverages global threat intelligence to protect individual customers, by using Fortinet's FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.