SLASHNEXT

Targeted Phishing Defense

Defend Against Spear Phishing Attacks Targeting Your Organization

SlashNext Targeted Phishing Defense enables organizations to better defend against previously unknown and targeted attacks involving spear phishing and APTs. With the industry's first definitive real-time phishing site detection and real-time phishing threat intelligence, organizations can automatically detect targeted, zero-hour phishing threats and block attacks that are evading existing security controls.

With SlashNext Targeted Phishing Defense, organizations get a whole new level of protection from the growing number of more sophisticated, targeted phishing threats, regardless of phishing attack vector—email, pop-ups, ads, search, social media, IM, rogue apps, and more.

BETTER DETECTION = BETTER PROTECTION

With more sophisticated phishing attacks, better detection enables better protection. SlashNext closes the gap on targeted zero-hour phishing threats using a unique combination of technologies:

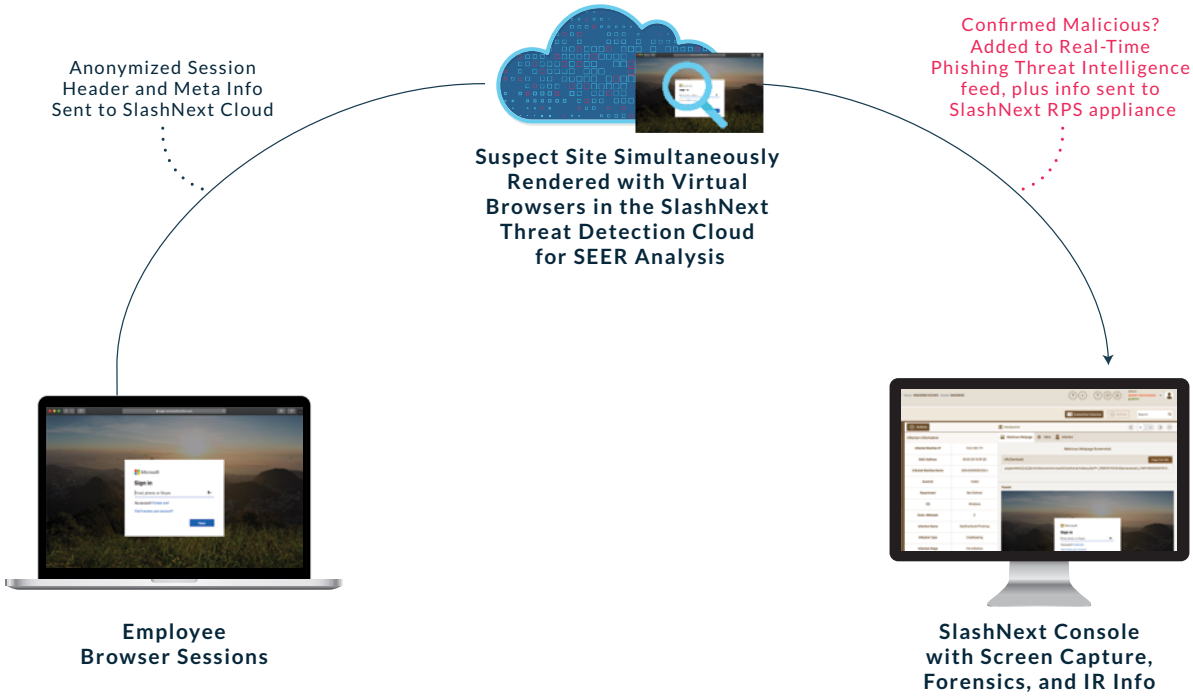
- Real-time webpage scanning (via an on-prem appliance) together with out-of-band threat detection in the SlashNext SEER™ cloud
- SEER technology. SEER (Session Emulation and Environment Reconnaissance) uses virtual browsers in a purpose-built cloud to inspect page contents and perform active site behavioral analysis. With machine learning, SEER accurately detects phishing threats missed by URL inspection and domain reputation methods
- Preemptive threat hunting and SlashNext global sensor network fuel SlashNext Real-Time Threat Intelligence, enabling organizations to stay ahead of threats and operationalize a dynamic blacklist of URLs, domains, and IPs for enhanced phishing protection

PHISHING CALLBACKS (C2S) DETECTION

SlashNext Targeted Phishing Defense analyzes Internet-bound traffic to identify communications with malicious C2 servers. Phishing attacks often aim to steal user login credentials or compromise users' machines with malware. Increasingly, threat actors are using harder-to-detect rogue browser extensions or in-memory browser spyware to access systems and exfiltrate data. SlashNext catches phishing callbacks to C2s and provides detailed info on compromised machines and C2 specifics including IP, geo info, and more.

THE SLASHNEXT ADVANTAGE

- Accurate, real-time detection of targeted phishing threats
- Works across all phishing attack vectors (email, pop-ups, ads, search, social media, IM, rogue apps, etc.)
- SEER technology—detects malicious sites that evade URL inspection and domain reputation analysis methods
- Definitive detection with near-zero false positives
- Zero-latency, out-of-band, cloud-powered threat detection with no PII sent to our cloud
- Detects phishing C2 callbacks
- Detailed forensics, phishing site screen capture, and IR info to speed remediation
- SlashNext Real-Time Phishing Intelligence provides industry's broadest, most up-to-the-minute intelligence of zero-hour phishing threats
- Device and OS agnostic
- Easy 20-minute install, no tuning, instant threat detection



HOW IT WORKS

- SlashNext monitors Internet traffic with a Real-Time Page Scanning (RPS) appliance that connects to a SPAN port. The appliance selects traffic for further analysis and sends anonymized session header and meta info to the SlashNext threat detection cloud for real-time SEER™ analysis.
- Suspicious pages are rendered with virtual browsers in the SlashNext threat detection cloud. SlashNext SEER technology (Session Emulation & Environment Reconnaissance) inspects the site using advanced computer vision, OCR, NLP, and active site behavior analysis.
- SEER analysis features are fed into machine learning algorithms which deliver a single, accurate, definitive verdict: malicious or benign. There are no inconclusive threat risk scores and near-zero false positives.
- Malicious URLs, domains, IPs, and IOC metadata are sent to the appliance and viewable in the local SlashNext console. They are also added to the global SlashNext Real-Time Phishing Threat Intelligence feed, which can be accessed via Web APIs for automated ingestion by security infrastructure.

FASTER INCIDENT RESPONSE

SlashNext complements its superior phishing site detection with detailed incident and IR information. The SlashNext management console provides detailed forensics data, including:

- Full session PCAPs
- Phishing lure page screen capture
- Description of the phishing page, including detected intent and behavior
- Phishing lure page website artifacts, including source code and image files recorded at the moment of live interaction

Detailed threat information is presented in an easy to understand, interactive format that enables rapid event triage and remediation. Screen captures can be used for employee phishing awareness training. Detailed forensics not only speeds incident response, it makes SlashNext suitable for larger firms as well as those that do not yet have advanced SIEM or threat intelligence management infrastructure.

4301 Hacienda Drive, Pleasanton, CA 94588 | slashnext.com | info@slashnext.com | 800.930.6843