SLASHNEXT

Protect Employees from Malicious Phishing Sites

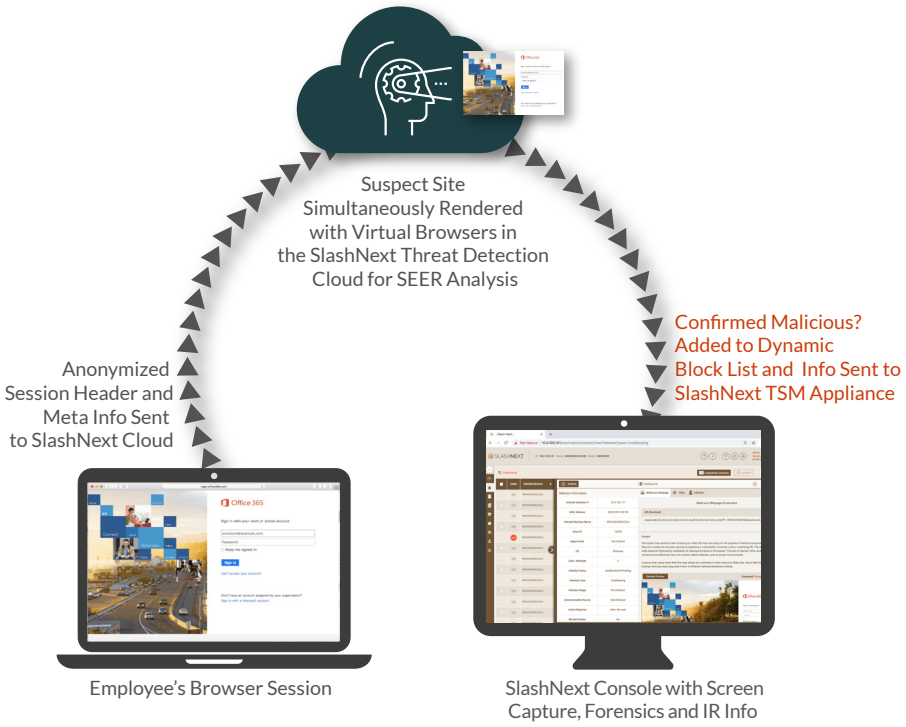
With Definitive Real-Time Phishing Site Detection

Close the Phishing Gap

Published industry reports show that over 90% of breaches start with phishing. With over 46,000 new phishing sites going live each day, and most disappearing within 4-8 hours, today's attacks move faster than static threat feeds and defenses can block them. SlashNext closes the gap with definitive real-time phishing site detection. Regardless of phishing attack vector (email, pop-ups, ads, search, social media, IM, etc.), SlashNext detects phishing sites the moment they are browsed, producing a dynamic block list for automated blocking by your URL filtration / blocking defenses. It's a whole new level of protection from the growing number of sophisticated zero-hour phishing threats on the Web.

How it Works

1. SlashNext monitors Internet traffic with an appliance that connects to a SPAN port. The SlashNext TSM appliance selects traffic for further analysis and sends anonymized session header and meta info to the SlashNext Threat Detection cloud for real-time analysis.
2. SlashNext renders suspect sites with virtual browsers in our purpose-built cloud. SlashNext SEER™ technology (Session Emulation & Environment Reconnaissance) inspects the site like a team of cybersecurity researchers using state-of-the-art text analysis, visual analysis, and active site interrogation.
3. SEER analysis features are fed into patent-pending progressive machine learning algorithms which deliver a single, definitive verdict: malicious or benign. There are no inconclusive risk probability scores and near-zero false positives.
4. Malicious URLs and domains are instantly added to a dynamic block list for your blocking infrastructure, typically firewalls, web proxies, or DNS. Incident information, including site screen capture, site artifacts, PCAP data, and more are instantly available in the local SlashNext console.



Key Features & Benefits

- Superior real-time phishing site detection via patent-pending SEER technology
- Definitive, binary detection: no inconclusive threat probability scores to research
- Works across all phishing attack vectors (email, pop-ups, ads, search, social media, IM, etc.),
- Detects phishing threats that evade URL inspection and domain reputation technologies
- Produces dynamic block list for existing blocking defenses (firewalls, web proxies, DNS)
- Near-zero false positives makes automated blocking feasible
- Zero-latency, out-of-band, cloud-powered threat detection with no PII sent to our cloud
- Malware callback detection to malicious C&C sites
- Detailed forensics, phishing site screen capture, and IR info to speed remediation
- Device and OS agnostic
- Easy 20-minute install, no tuning, instant threat detection and protection

More Powerful Phishing Protection

Better phishing detection means better protection, especially against the growing number of previously unknown zero-hour phishing threats on the Web. Slow moving threat feeds cannot keep pace with today's fast-moving threats, leaving organizations exposed. SlashNext SEER technology employs real-time Session Emulation and multiple forms of dynamic site analysis, including active site interrogation and progressive machine learning, to definitively and accurately detect malicious sites in real-time. High accuracy enables rapid and automated blocking by existing defenses, providing a whole new level of protection from sophisticated zero-hour phishing threats.

By contrast, other anti-phishing technologies rely primarily on URL inspection and domain reputation analysis, techniques which are easily evaded by sophisticated hackers. This not only causes them to miss phish, they are unable to deliver definitive phishing site detection, forcing additional threat research work onto IT security staff and delays in blocking malicious sites.

Security Without Disruption

SlashNext phishing site detection is cloud-powered and out-of-band, so it does not introduce any network latency. With seamless integration to existing blocking defenses, and near-zero false positives, automated blocking becomes feasible. Together with a simple 20-minute install and no tuning requirements, SlashNext phishing threat protection is immediate, non-disruptive, and effective.

> "SlashNext is the first advanced threat security product that we have bought to actually find issues our NextGen Firewall, Callback Attacks Prevention Tools, and Anti-Virus all missed"
>
> Raun Nohavitza
> VP of Information Technology, Centrify

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 feed management infrastructure.

With SlashNext, you can close the phishing gap with superior protection from today's—and tomorrow's—most advanced phishing threats on the Web.

Contact us today for info on a free gap analysis to easily test your existing defenses. Free trials also available.

SlashNext, Inc.
4301 Hacienda Drive, Pleasanton, CA 94588
1-800-930-6843 | info@slashnext.com | www.slashnext.com

SLASHNEXT