DATA SHEET

SLASHNEXT

Network Phishing Intelligence

Anywhere Zero-Hour Protection Against the Broadest Range of Phishing Threats Accessible Through Cloud APIs, DNS RPZ, and TIP Integrations

Boost Network Security Controls

Use live threat intelligence to turn existing network security controls into a real-time, multi-vector phishing defense. Enterprise DNS, proxies, and firewall infrastructure can operationalize SlashNext phishing domain and C2 threat intelligence to disrupt phishing attacks at the network edge. Accessible through cloud APIs, DNS RPZ, and TIP integrations. No additional hardware or software needed.

Tens of Thousands of Sophisticated, Fast-Moving Threats Go Live Everyday

Phishing has become the number one security threat to business and consumers alike. The phishing attacks have grown in both sophistication and attack vector, moving beyond email to mobile, Web, SMS, collaboration, gaming and social networking services. SlashNext Network Phishing Intelligence enables organizations to better understand and protect themselves from zero-hour phishing and social engineering threats on the web. Through multiple sources, SlashNext proactively inspects millions of suspicious URLs daily. Unlike other anti-phishing technologies, SlashNext patent-pending SEER™ technology uses virtual browsers to dynamically inspect page contents and server behavior to detect tens of thousands of new phishing URLs per day with extreme accuracy.

Together with fully automated URL re-checking and retirement, security teams get the most comprehensive, real-time phishing threat intelligence available.

Comprehensive Network Phishing Threat Intelligence

Unlike other anti-phishing technologies and threat feeds, SlashNext Network Phishing Intelligence covers all six major categories of phishing and social engineering threats.

Credential Stealing
Fake log-in pages

Rogue Software
Rogue apps & extensions

Scareware
Fake virus alerts

Social Engineering Scams
Credit card fraud

Phishing Exploits
Weaponized documents, etc.

THE SLASHNEXT ADVANTAGE

- **Anywhere, Anytime Protection:** 24/7 phishing protection, both inside and outside of the network perimeter
- **Broadest Range of Protection:** Protecting web, SMS, social, mobile, search, and collaboration/messaging Tools by detecting credential stealing, rogue browser extensions, and more
- **Real-Time:** 1B internet transactions & 7M URLs URLs, domains, and IPs analyzed daily,
- **Unparalleled Accuracy:** Industry highest detection rate at 99.07% and 1 in 1 million false positives
- **SEER Technology:** Patented behavioral phishing detection technology uses millions of virtual browsers to detect unknown phishing sites and SMS with unmatched accuracy
- **Preemptive:** Global, Proactive threat hunting provides advance visibility of threats
- **Easily Accessible:** Web API access to threat data in multiple machine-readable formats
- • **SlashNext Expertise:** Threat research specialists focused on modern phishing threat defense.

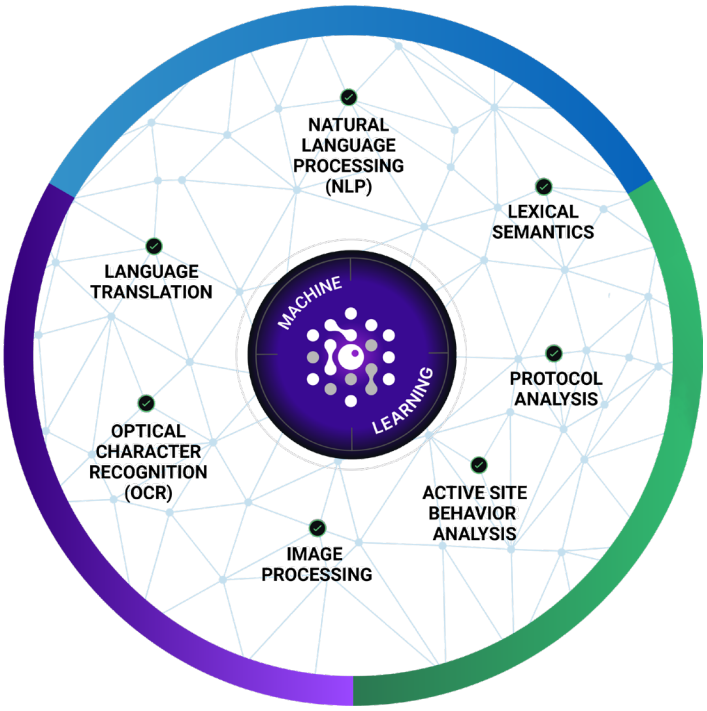
Deployment Flexibility

Rapid deployment with pre-built integrations with leading TIP, DNS, and NextGen Firewall vendors for rapid, automated deployment. As a cloud-powered, API-based service, SlashNext Network Phishing Intelligence can be ingested and operationalized by existing DNS, proxies, and firewall infrastructure via DNS RPZ.

Harness the Power of Real-Time with SEER™ Technology

SlashNext's patented behavioral phishing detection technology uses millions of virtual browsers to detect unknown threats with unmatched accuracy. SEER™ (Session Emulation and Environment Reconnaissance) is a scalable, cloud-based threat detection technology that uses computer vision, NLP, and OCR, to dynamically inspect page contents and server behavior. Sophisticated machine learning algorithms and virtual browsers perform rich analysis to accurately detect zero-hour phishing threats and numerous enrichment artifacts.

This unique combination of techniques sees through evasion tactics and accurately detects phishing pages, even those hosted on compromised websites and legitimate infrastructure. It also follows through on all URL re-directs and performs run-time analysis on the final page of multi-stage threats.



About SlashNext

SlashNext is the phishing authority and leading the fight, together with its partners, to protect the world's internet users from phishing anywhere. SlashNext end-to-end phishing protection services utilize our patented SEER technology to detect zero-hour phishing threats by performing dynamic run-time analysis on billions of URLs a day through virtual browsers and machine learning. Take advantage of SlashNext's services using mobile apps, browser extensions, and APIs that integrate with leading mobile endpoint management and IR tools.

SlashNext is headquartered in Silicon Valley and backed by top-tier venture capital firms. For more information, visit www.SlashNext.com

Request a demo today at www.slashnext.com/request-a-demo

6701 Koll Center Parkway, Suite 250, Pleasanton CA 94566 | slashnext.com | info@slashnext.com | 800.930.8643
REV 092420