SLASHNEXT

Email Detection and Response

Detect and remove targeted spear phishing, social engineering, rogueware, scam, bank fraud and data exploit threats that easily evade your Microsoft 365 email security defenses.

Powerful, Simple, Secure, Fast ROI

Now organizations can leverage SlashNext's award-winning AI threat detection to securely detect and remove targeted spear-phishing and other human threats that easily evade email security defenses.

Current email defenses, including Microsoft 365 built-in security, miss up to 65% of targeted spear phishing, social engineering, business email compromise (BEC), and other malicious digital user attacks launched from legitimate, trusted sites. Targeted, well-crafted spear-phishing continues to rise dramatically in an environment where cybercriminals use automation and AI to increase the likelihood of compromising a target. The once-reliable security strategies of Secure Email Gateways (SEGs), proxy/SASE, and endpoint anti-phishing protections are no longer adequate safeguards against rapidly evolving phishing tactics. For instance, spear-phishing delivered through legitimate cloud services can bypass traditional cybersecurity solutions. Since these attacks focus on a person, not the technology, success rates are higher, providing the attacker a lower-cost entry point into an organization.

With SlashNext's new AI-based email detection and response, organizations can detect these targeted attacks with pinpoint accuracy and remove them from individual infected user inboxes with one click. Leverage SlashNext's patented SEERTM AI to detect and remove attacks that easily evade relationship graphs, URL rewriting, and sandbox email security technologies.

Minutes to Instant Detection and Response
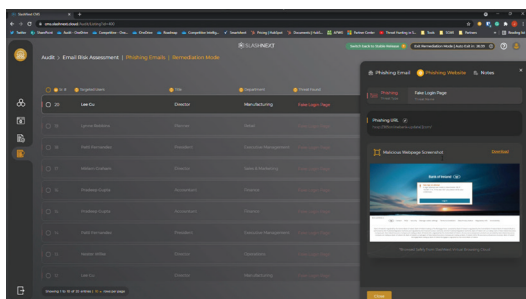
Review threats, high risk users and forensics
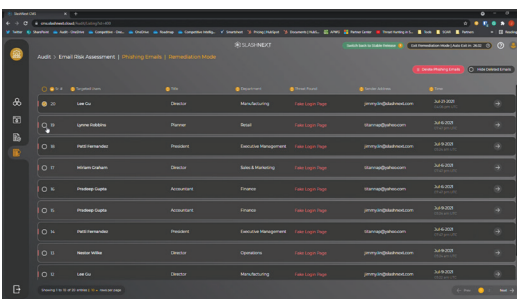
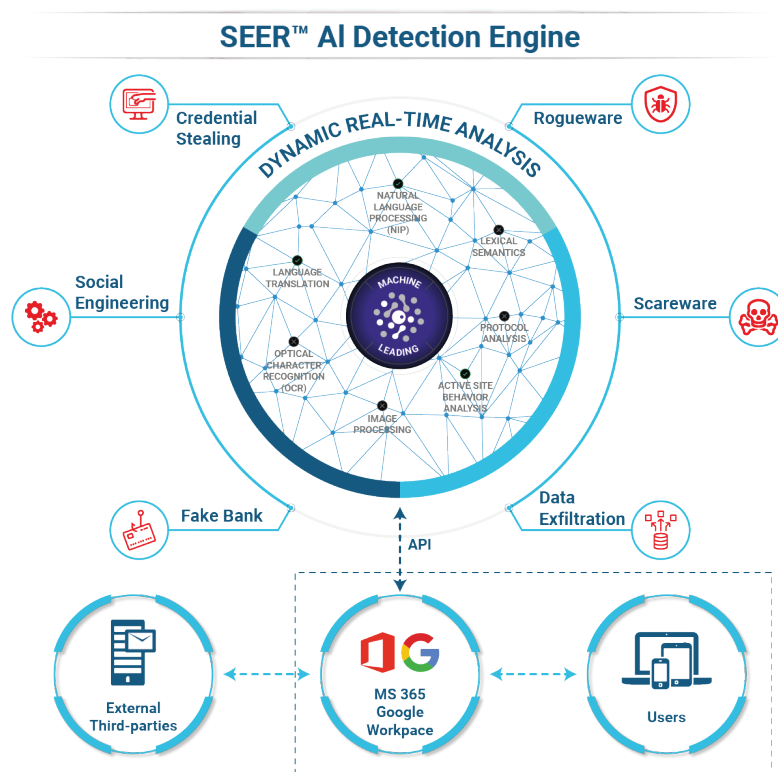
Select all or specific emails for instant deletion

THE SLASHNEXT ADVANTAGE

- **Powerful**
  Unparalleled, 99.99% zero-hour detection and one in 1 million false positive rate provides confidence in remediation.

- **Simple**
  Instant detection of spear phishing and other threats. Respond immediately by user, group or company-wide to any threat identified.

- **Secure**
  As a SaaS-based trusted and verified partner of Microsoft it takes five minutes to instant detection by securely authenticating to the Microsoft Graph API using OAuth.

- **Fast ROI**
  Dramatically reduce the time it takes to remove the threats missed by a Microsoft 365. Security teams, on average spend three to five minutes per incident, so payback period is in weeks.

- **Full Visibility**
  Elegant cloud management console enables simple deployment, management, and advanced reporting across threats, users, and devices.

Harness the Power of Real-Time with SEER™ AI

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.

SEER™ AI Detection Engine

DYNAMIC REAL-TIME ANALYSIS

- Credential Stealing
- Rogueware
- Social Engineering
- Scareware
- Fake Bank
- Data Exfiltration

MACHINE LEARNING

- NATURAL LANGUAGE PROCESSING (NlP)
- LEXICAL SEMANTICS
- LANGUAGE TRANSLATION
- PROTOCOL ANALYSIS
- OPTICAL CHARACTER RECOGNITION (OCR)
- ACTIVE SITE BEHAVIOR ANALYSIS
- IMAGE PROCESSING

API

- External Third-parties
- MS 365 Google Workpace
- Users

Take the /Next Phish Challenge to See How SlashNext Finds Threats Missed by SEG, Proxy and Endpoints

SlashNext is confident that your current security tools are missing up to 65% of the most dangerous threats and will prove it to you. Take the complimentary challenge by running the Microsoft 365 vulnerability assessment, doing a free trial of the SlashNext 360 defense-as-a-service, or simply put a suspicious URL in the /Next phish scanner missed by your secure email gateways, proxy, or endpoint service. **TAKE THE CHALLENGE at www.slashnext.com/assessment-take-the-challenge/**

About SlashNext

SlashNext is the authority on spear-phishing and human hacking, leading the fight together with its partners to protect the world's internet users from targeted phishing anywhere. SlashNext 360° Defense Service utilizes our patented AI SEERTM 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 phishing defense services using mobile apps, browser extensions, and APIs that integrate with leading mobile endpoint management and IR services.