DATA SHEET

SLASHNEXT

Integrated Cloud Email Security

Modern cloud email security, with the only generative AI-powered technology, stops sophisticated email attacks like BEC, credential stealing, ransomware, and malware threats to reduce the risk of a data breach.

Powerful, Simple, Secure, Fast ROI

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 BEC and 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 protections cannot safeguards against rapidly evolving phishing tactics. 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.

SlashNext's Generative HumanAI™, the industry's first artificial intelligence solution that uses generative AI to defend against advanced business email compromise (BEC), supply chain attacks, executive impersonation, and financial fraud. SlashNext now has the most comprehensive cloud email protection against link-based, attachment-based, and natural language-based BEC attacks.

With SlashNext's cloud email security continuously detects and remediate threats missed by Microsoft Defender, ATPs with 99.9% detection rate and 1 in 1M FPs. SlashNext Generative HumanAI anticipates vast numbers of potential AI-generated BEC threats by using AI data augmentation and cloning technologies to assess a core threat and then spawn thousands of other versions of that same core threat, which enables the system to train itself on possible variations.

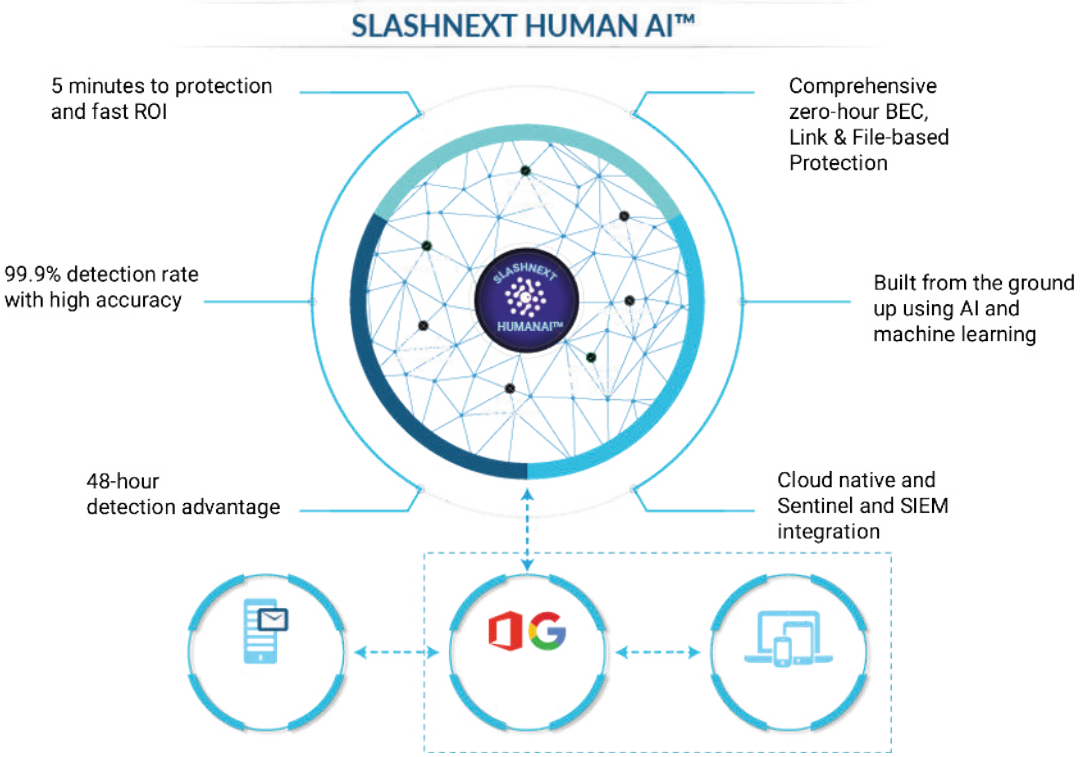
The unique differentiation of HumanAI is its ability to spot how threat actors play off human emotions, such tone, style, intent and motvies. SlashNext Generative HumanAI simulates those same human emotions and behaviors in its detection process.

Threat actors can now leverage widely available AI tools to aid their attack efforts, like ChatGPT, which can have profound security ramifications to organizations. Threat actors are weaponizing these tools to rapidly target users with tailored malware and BEC attacks. SlashNext Generative HumanAI anticipates the use of these new threat tactics and provides the only effective countermeasure to stop them today. 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.

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.

Continuous Real-Time Detection and LiveScan Stop Threats Missed by Microsoft Defender



5-Minutes to Protection

Cloud native integration with Microsoft 365 Graph API. Purpose built to provide zero-hour protection for Microsoft Defender for Office 365 users

Comprehensive Defense-in-Depth Strategy

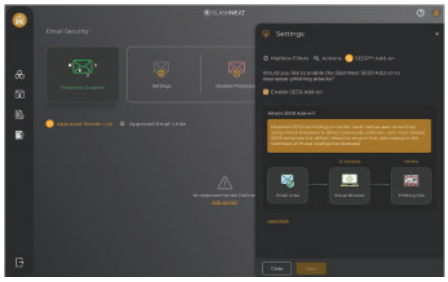
SlashNext ICES blocks complete spectrum of zero-hour BEC, wire fraud, credential phishing, and ransomware attacks, supplementing MS Safe Attachments & Safe Links

HumanAI™ Zero-hour Detection

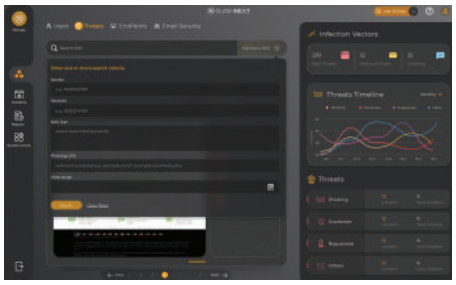
Zero-hour multi-phase analysis using relationship graphs, natural language processing, and computer vision recognition to stop and remediate threats with a 99.9% detection rate, and 1 in 1M FPs

Explainable Attack Insights

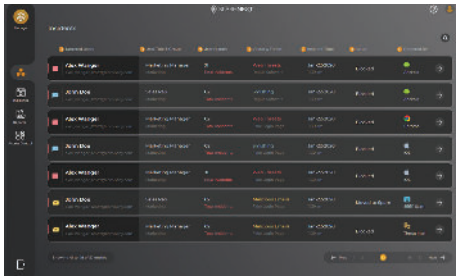
Visual illustration clearly and thoroughly explains the reason why emails are classified as malicious



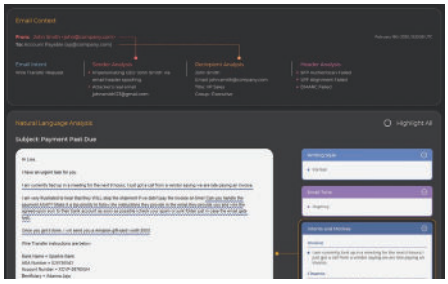
Deploy Through API



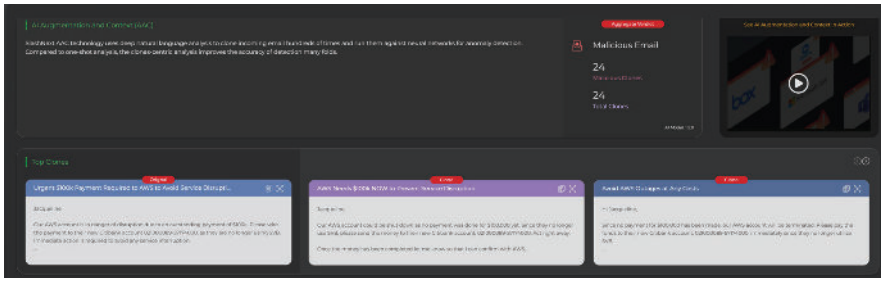
Unified Security Analysis



Real-Time Search



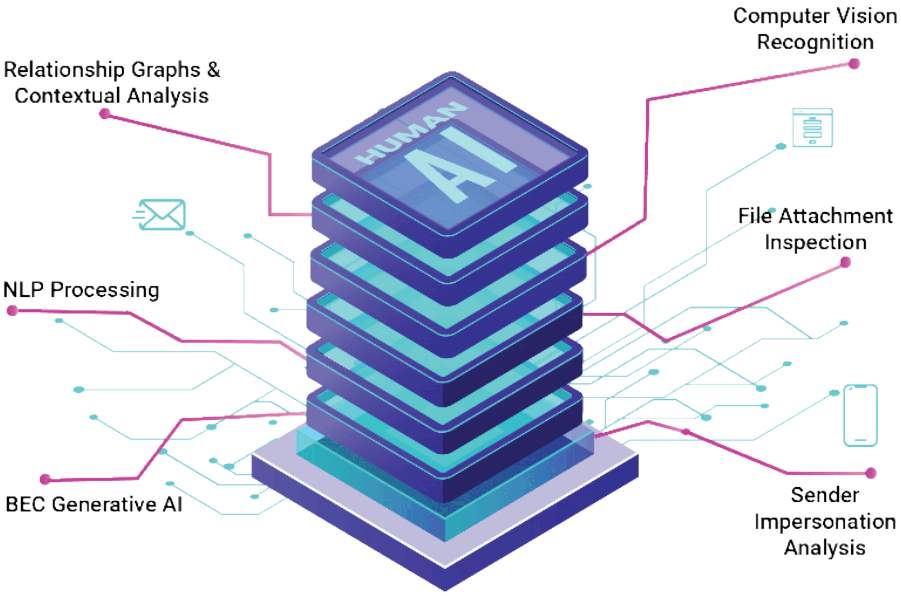
BEC Generative AI Threats Insights



BEC Generative AI Created Clones

Harness the Power of SlashNext Generative HumanAI™

Stop 65% more zero-hour threats – BEC, links and files



Relationship Graphs & Contextual Analysis
A baseline of known-good communication patterns and writing styles of employees and suppliers to detect unusual communication cadence and conversation style

BEC Generative AI
Auto generates new BEC variants from today's threat to stop tomorrow's attacks

Computer Vision Recognition
Live ScanTM inspect URL in real-time for any visual deviations such as image and layouts to detect credential phishing webpage

NLP Processing
Analyzes text in email body and attachment for topic, tone and emotion, intent, and manipulation triggers associated with social engineering tactics

File Attachment Inspection
Live ScanTM analyze attachments social engineering traits and malicious codes to stop ransomware

Sender Impersonation Analysis
Evaluates header details and email authentication results to stop impersonation attack.

SlashNext's patented behavioral phishing detection technology uses millions of virtual browsers to detect unknown threats with unmatched accuracy. SlashNext HumanAI technology is specifically trained to stop zero-hour BEC, account takeover, credential theft attacks using generative AI, relationship graph, contextual analysis, natural language processing, and computer vision.

These are the key ingredients needed to proactively stop zero-hour attacks.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 protects the modern workforce from malicious messages across all digital channels. SlashNext Complete™ integrated cloud messaging security platform utilizes patented HumanAITM technology with 99.9% accuracy to detect threats in real-time to stop zero-hour threats in email, mobile, and web Messaging Apps across M365, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Teams, and others messaging channels. Take advantage of SlashNext's Integrated Cloud Messaging Security for email, browser, and mobile to protect your organization from data theft and financial fraud breaches today.

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

REV 042023