SLASHNEXT

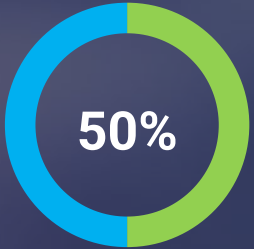
Secure Your Cloud Email + Mobile and Web Messaging Apps

HumanAI™ stops BEC, ransomware, credential phishing, smishing, account takeovers, phishing attacks and more

Humans — the most valuable, and vulnerable assets

82%

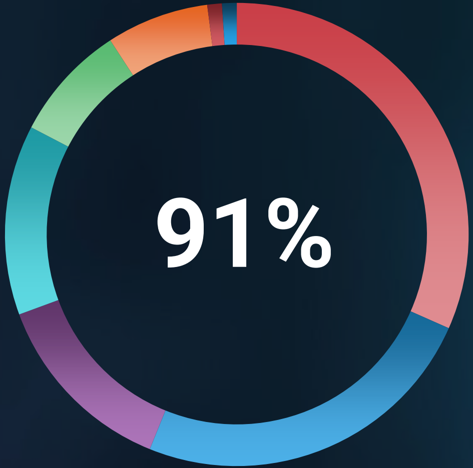
of successful breaches start with a human compromise in message apps



of attacks happen outside of email

twilio	SMS
cisco	Gmail
Uber	SMS

What Happens Next After Human Compromise?



of all attacks start with spear phishing

31% M365 Account Takeover

8% Wire Transfer

24% Ransomware

7% Data Theft

13% Installation of Malware

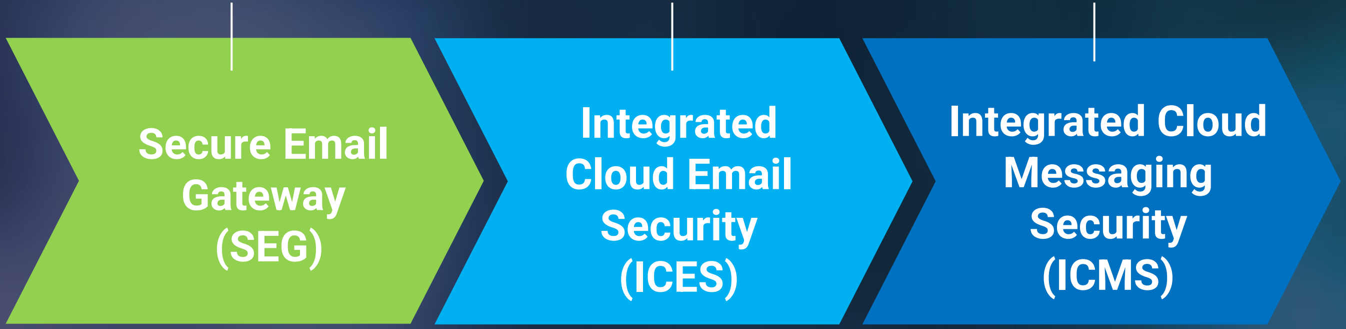
1% Cryptomining

13% Network Intrusion

1% Espionage

Legacy Email Security Fails to Stop Zero-hour Threats

Today’s advanced threats requires a solution that’s built from the ground up using HumanAI$^{\text{TM}}$



40% Will Move Off SEGs By 2023

Secure Email Gateway (SEG)

20% Growth In ICES By 2025

Integrated Cloud Email Security (ICES)

- Relationship graphs and contextual analysis
- Natural language processing
- Computer vision recognition
- Generative AI

Multi-Channel Starting 2022

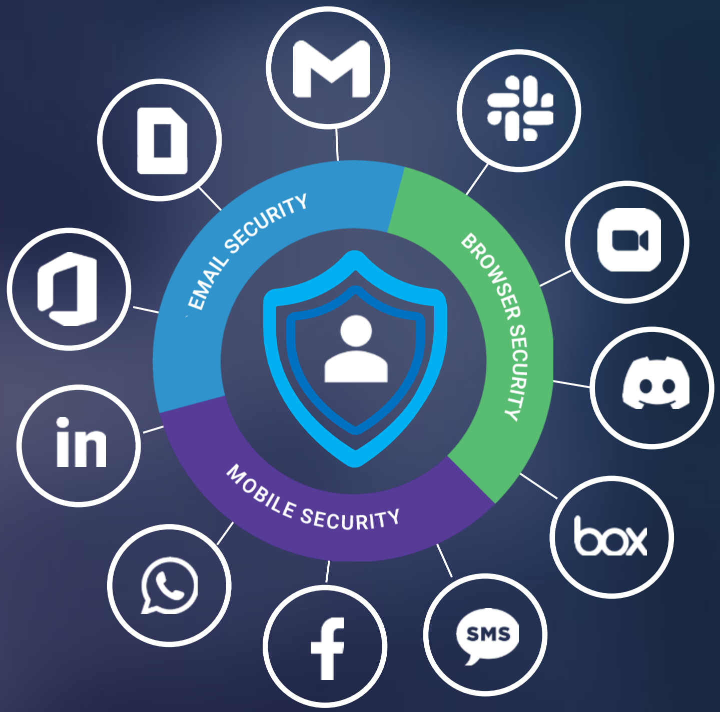
Integrated Cloud Messaging Security (ICMS)

- Email+ SMS/Mobile and web messaging apps

Gartner

SlashNext Integrated Cloud Messaging Security

HumanAI^{TM}

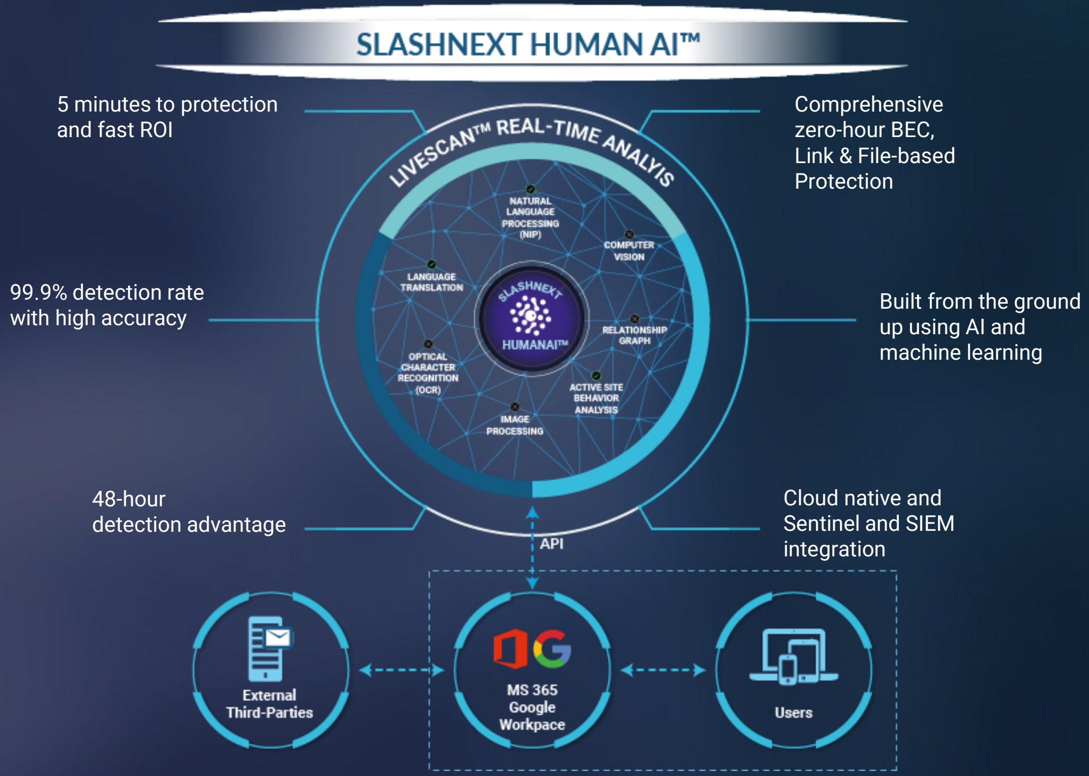


Stops the Human Threats That Matter

LINK-BASED THREATS	Credential Harvesting Spear-Phishing Scams/Fraud Smishing
ATTACHMENT-BASED THREATS	Malicious Attachments Ransomware/Malware Exploits
NATURAL LANGUAGE-BASED THREATS	Business Email Compromise (BEC) ATO and Supply Chain Business Text Compromise Business Message Compromise Insider Threats

SlashNext Integrated Cloud Email Security

Cloud native zero-hour protection for Microsoft 365 users



5 minutes to protection and fast ROI

99.9% detection rate with high accuracy

48-hour detection advantage

Comprehensive zero-hour BEC, Link & File-based Protection

Built from the ground up using AI and machine learning

Cloud native and Sentinel and SIEM integration

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^{TM} 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

HumanAI$^{\text{TM}}$ Zero-hour Protection

Stops 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

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

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

Computer Vision Recognition
Live Scan$^{\text{TM}}$ inspect URL in real-time for any visual deviations such as image and layouts to detect credential phishing webpage

File Attachment Inspection
Live Scan$^{\text{TM}}$ analyze attachments social engineering traits and malicious codes to stop ransomware

Sender Impersonation Analysis
evaluates header details and email authentication results to stop impersonation attacks

BEC Generative AI

Stopping tomorrow’s threats today

AI/ML Facts

AI/ML sucess and effectiveness depends on the ability to continuously learn to improve over time

Original Email

I have written you multiple times to remind you that you owed us $3325.32. Unfortunately, the invoice sent on August 1st is more than 14 days late. If you have lost or deleted the original invoice, here is a copy. Please send the payment immediately.

BEC Generative AI – sample clone

To make you aware, you owe us a total of $3325.32. In case you misplaced the original invoice sent on 08/01, I have included a copy here for your convenience. To the best of your ability, kindly pay the money as soon as you can.

SlashNext BEC Generative AI

Extract topic, intent, emotions and style of a malicious email, and exhaust all possible ways a human can write a similar email (semantical clones). Providing a rich data set for ML training, testing and runtime predictions

Stronger Together with SlashNext ICES

Zero-hour Protection With HumanAI^{TM}

Microsoft

- Sender blocklist contains known bad IPs and domains
- Email authentication reviews DMARC, SPF & DKIM auth results
- Safe Links rewritten URLs against known URL threat DB at time-of-click
- Safe Attachments sandbox files for malicious codes

✓ Cloud native & purpose built for Microsoft

✓ Zero-hour BEC protection

✓ Zero-hour credential phishing & link protection

✓ Zero-hour ransomware and file protection

✓ Spam and newsletter detection

✓ Comprehensive defense in depth protection with MS API integration

✓ 48-hour detection advantage

✓ Explainable threat insight for seamless investigation and response

✓ Security analytics integration w/ Microsoft Sentinel

✓ 360° protection across email, SMS/Mobile and browser

SLASHNEXT

- **Relationship and contextual analysis** detect unusual communication cadence and conversation style
- **Natural language process** detects topic, tone, emotion, intent, and manipulation triggers associated with BEC
- **BEC Generative AI** clones latest threats for ML training and detection
- **Live Scan^{TM} Computer Vision** inspect webpages for visual deviations
- **Live Scan^{TM} file inspection** scans for social engineering traits and malicious codes

Use Case – Replace SEG with ICES

180K

Mailboxes

Best Zero-Hour Link, File and BEC Detection

Ease of Implementation, Management and Controls

$2M Annual Saving

”The beauty of SlashNext is in the simplicity of the solution and their ability to detect and stop the most zero-hour email threats in our highly regulated environment.” Global 200 CISO

Why SlashNext?

We stop zero-hour attacks

- ✓ Best BEC, Link and File-based Detection
- ✓ Fast ROI and Time to Value
- ✓ +SMS/Mobile & Browser Protection
- ✓ Guaranteed User Privacy