SLASHNEXT

Microsoft 365 + Integrated Cloud Email Security

Transitioning from a Secure Email Gateway to Modern Architecture for the Modern Enterprise

TABLE OF CONTENTS

INTRODUCTION

Due to the demands of the modern workforce, there has been an exponential shift in the use of native cloud email protection capabilities, like Microsoft 365, in the last 12 months. This has led to an increase in the adoption of Integrated Cloud Email Security (ICES) solutions in place of Secure Email Gateways (SEG). According to Gartner, by 2023, 40% of all organizations will use native protection capabilities from cloud email providers rather than a SEG, and by 2025, 20% of anti-phishing solutions will be delivered through ICES via API integration, up from less than 5% today. [1]

The best way to ensure your email security solution will meet the demands of the modern workforce is to have protection that meets the demands of the new threat landscape, including:

- Full Defense in Depth approach to email security by supplementing Microsoft Defender for Office 365 (E5) with Integrated Cloud Email Security (ICES)
- Use of advanced detection techniques such as computer vision machine learning against advanced phishing threats and other highly targeted threats
- Delivers best-in-class zero-hour phishing protection to protect your Microsoft 365 cloud users
- Automate the response of suspicious emails using SIEM/SOAR integration to reduce overburdened IT security teams
- Multi-channel protection for threats in Email, SMS, Microsoft 365, LinkedIn, WhatsApp, Zoom, Box, and other messaging channels.

1. Gartner Market Guide for Email Security, 2021

WHAT EMAIL SECURITY TOOLS ARE REQUIRED AND THE ONES TO AVOID

Microsoft 365 Built-in Protection

According to Gartner, 70% of organizations use cloud email solutions, but complexity and security continue to concern organizations. Microsoft 365 has a high adoption rate which makes it a target for threat actors, so Microsoft continues to improve its built-in capabilities. At the core, Microsoft Exchange Online Protection (EOP) scans all inbound emails. The emails that are identified as malicious are quarantined and blocked. Good emails are delivered to users' mailboxes. Microsoft Defender for Office 365 provides additional protection for several important security capabilities, including several options to protect against known malware, phishing, and social engineering threats. (Exhibit 1)

Microsoft 365 Defender E3 and E5 protection

E3 + Defender for Office Plan 1	E5
Configuration, protection, and detection capabilities:	***All E3 + Defender for Office Plan 1 capabilities, plus: Automation, investigation, remediation, and education capabilities:***
• Safe Attachments • Safe Links • Safe Attachments for SharePoint, OneDrive, and Microsoft Teams • Anti-phishing protection in Defender for Office 365 • Real-time detections	• Threat Trackers • Threat Explorer • Automated investigation and response • Attack simulation training • Proactively hunt for threats with advanced hunting in Microsoft 365 Defender • Investigate incidents in Microsoft 365 Defender • Investigate alerts in Microsoft 365 Defender

Exhibit 1: *Microsoft E3 + Defender for Office Plan 1 and E5 protection provide several important security capabilities Source: Microsoft Defender for Office 365 security overview, microsoft.com*

While Microsoft's built-in security can detect and stop known threats, it struggles with zero-hour threats, spear-phishing, threats from trusted services, ransomware, and other complex phishing attacks.

Many Microsoft users have expressed dissatisfaction with built-in EOP and Defender for Office 365 and are looking for supplemental email security products to augment protection. With Microsoft's continued investments in email security, turning to secure email gateways for protection has decreased. According to Gartner, ICES with Microsoft is an option that many organizations have turned to.

SEG, Do You Really Need One?

Once a powerful solution to stop malicious emails from arriving in users' mailboxes, Secure Email Gateways (SEGs) legacy technology is not providing the modern real-time protection required to keep users safe. Now organizations are moving away from SEGs to Microsoft 365 and ICES.

The primary reason SEGs have become legacy protection can be attributed to two main reasons.

1. SEGs use reactive signature and domain-based detection, which can't keep up with today's phishing threats.
2. SEGs are built for the on-premise world, which prevents the implementation of a full defense-in-depth strategy for email security defense. In contrast, ICESs are built for the cloud and close the gaps in Microsoft 365 built-in security.

Let's take a look at these reasons in depth.

SEG Signature and Domain-Based Detection Can't Keep Up

Today, having a SEG provides little to no value and only adds complexity to your email security. When SEGs first gained popularity, it was universally agreed that Microsoft security lacked the technology to stop email threats. However, Microsoft has improved, and now using a SEG creates more redundancy than offering value. SEGs use similar, overlapping technologies as Microsoft's built-in security, including URL rewriting and file attachment sandboxing for advanced threat protection.

These technologies are powered by distinct intelligence networks and are effective at stopping known threats and spray-and-pray phishing campaigns since both use reactive signature-based detection techniques. As threat actors innovate relentlessly to refine their phishing techniques, SEG technologies can't keep pace, which is why advanced detection techniques such as computer vision machine learning are required to detect advanced phishing threats and other highly targeted threats.

SEG's Prevent Implementing a Defense-in-Depth Strategy

SEG architecture sits in front of Microsoft's built-in security and requires organizations to disable critical Microsoft security features to prevent disruption to inbound email delivery. This is important because it blinds Microsoft to incoming threats, and blocking phishing emails based on the original sender's IP reputation is impossible since all incoming emails arrive from the SEG's IP address. Furthermore, SEGs change certain indicators in the email header, reducing the malicious signals that can be acted on by Microsoft.

An unfortunate consequence of using a SEG is an increased attack surface. Since SEGs require a public DNS MX record change, adversaries now have a roadmap to customize phishing campaigns for testing and reconnaissance before launching the attacks and increasing the success rate.

Finally, SEGs also introduce an additional point of failure. Since SEGs are a mail transfer agent with security features, if there is a service outage, it will introduce email delays or, worse, complete email failure for the organization.

ICES has closed the gaps in Microsoft 365 native security, enabling a full defense-in-depth approach

When Microsoft 365 built-in security offering was much smaller, it made sense to bypass/replace it with SEG technology. Still, you cannot apply a robust defense-in-depth approach today as SEGs require disabling Microsoft security features. Today SEG solutions have too much redundancy with Microsoft 365 E3/E5 solution, including sender IP reputation, email authentication, and URL rewriting.

ICES solutions use AI, including behavior analysis, natural language processing, and computer vision, to detect communication anomalies and close the gaps in Microsoft's built-in security offering with important threat payloads, including spear-phishing, BEC, and account takeover, to name a few.

Integrated Cloud Email Supplements (ICES)

As previously mentioned, Microsoft's built-in security has improved, yet threat actors have become more sophisticated. The attack surface has expanded to multiple channels, plus email threats are coming from compromised websites that are difficult to detect. Ransomware-as-a-service gangs use credential harvesting through email as an entry point. Email security solutions must have modern, more advanced detection technology to combat these threats. Just in time—In walks the ICECs.

ICES solutions are built for the cloud by offering seamless cloud-native integrations with Microsoft. It integrates using Microsoft Graph API and "sits" behind Microsoft to stop attacks missed by Defender for Office 365. Using AI, including behavior analysis, natural language processing, and computer vision to detect communication anomalies, closes the gaps in Microsoft's built-in security offering. Most importantly, they augment Microsoft's built-in protection to provide protection for sophisticated threat payloads.

ICES solutions with behavioral-based technology that uses machine learning to detect advanced phishing threats offer an advantage over SEGs and other signature-based solutions. As threat actors continuously change tactics to launch advanced phishing

campaigns, the AI-based ICES solutions leverage machine learning algorithms to automate analyses at a significantly larger scale and far faster speed than traditional URL inspection and domain reputation. The result is the detection of known and unknown phishing threats is proactive and stopped before they can impact users.

When looking at ICES to augment Microsoft 365 built-in protection to make sure it will meet the demands of the modern threat landscape with:

- Delivers high efficacy for best-in-class zero-hour phishing protection and a full defense-in-depth approach to email security
- AI-based detection for advanced phishing and other highly targeted threats, such as business email compromise, ransomware, impersonation, and account takeovers
- Multi-channel protection for Email, SMS, Microsoft Teams, Sharepoint, OneDrive, LinkedIn, WhatsApp, Zoom, and other messaging channels
- Real-time awareness training
- SIEM/SOAR integration to simplify the reporting

A Cautionary Tale: Credential Harvesting Took Down a Pipeline

The Colonial Pipeline breach will stay in our minds for a long time. It disrupted the airline industry, created panic, long lines at the pump, and triggered a government investigation.

The root cause was credential stealing phishing that exposed a password for an employee VPN account for network access. The employee likely used the same password for the VPN in another location. Hackers are phishing humans in email, SMS, web, social, gaming, collaboration apps, and search.

There is much to learn from the Colonial Pipeline breach, but mostly it's a wake-up call about the importance of phishing. While ransomware is the end of the attack chain, phishing is at the start.

Stop phishing and stop 95% of ransomware.

WHAT MAKES SLASHNEXT UNIQUELY QUALIFIED TO ACHIEVE COMPLETE DEFENSE-IN-DEPTH EMAIL SECURITY

SlashNext technology is unique from other ICES solutions by delivering powerful layers of protection. SlashNext's patented SEER™(Session Emulation and Environment Reconnaissance) technology with Live Scanning and AI database blocks phishing threats missed by Microsoft 365, SEG ATPs, and identity graph technologies with a proven 99.9% detection rate and 1 in 1 million false positives for true zero-hour phishing protection.

SlashNext's Patented Technology Approach

The unique approach is multi-layered with global cloud and in-channel detection techniques to see through evasion tactics to accurately detect phishing attacks, even on compromised websites and trusted services, resulting in a 99.9% detection rate with very low false positives.

- The global AI-based detection cloud detection uses a broad intelligence gathering network and powerful behavioral learning, natural language processing, and computer vision. This enables SlashNext to detect phishing threats up to 48 hours before they show up on VirusTotal and other threat databases resulting in tens of thousands of new threats added daily, with thousands not available elsewhere.
- SlashNext LiveScan offers real-time scanning of suspicious phishing threats that are not in the database, offering true zero-hour detection before they reach users with 99.9 % accuracy.
- Phishing Attachment Protection can see through Microsoft Office, Adobe, and HTML attachment to detect malicious content, multiple URL redirects / forwards, and other types of URL obfuscation.

The Best Protection Where It's Needed the Most

BEC is a problem, and most organizations have had some type of BEC incident. However, the most successful form of BEC comes from legitimate account takeovers, which start with credential harvesting attacks. In addition, 60% of ransomware-related breaches result from direct downloads using stolen credentials, according to Verizon DBIR 2022. In a recent report by Cofense, Microsoft missed 62% of credential harvesting attacks while only missing 6% of BEC. (Exhibit 2)

Percentage of Threats Missed by Microsoft Defender and SEGs

SEG	BEC (Business Email Compromise)	Malware	Credential
Barracuda	4%	20%	**67%**
Cisco	11%	10%	**55%**
FortiNet	3%	4%	**74%**
Microsoft Defender for O365	4%	6%	**62%**
Microsoft EOP	2%	3%	**67%**
Mimecast	12%	9%	**57%**
Proopoint	6%	19%	**51%**
Symantec	4%	19%	**55%**
TrendMicro	3%	18%	**42%**

Exhibit 2: Microsoft missed 62% of credential harvesting attacks while only missing 6% of BEC. Source: 2021 Cofense Annual State of Phishing Report

Powerful Protection and Fast ROI

SlashNext integrates with Microsoft 365 Security for immediate, powerfully accurate cloud email protection. While other ICES solutions require baselining, including reading all employee contacts, email history, and attachments, which is intrusive and can take hours and days to complete.

SlashNext enables organizations quickly achieve complete email security:

- Integration to protection in 5 minutes with unintrusive deployment using the Microsoft Graph API for immediate protection
- Data is never stored on a disk to ensure zero loss of PII
- Real-time scanning, detection, and removal of zero-hour threats before they reach users. 99.9% accuracy, 1 in 1 million false-positive rates, and 48-hour time to detection advantage.
- Advanced search and unified security analytics enable security professionals to pinpoint threats by user and type across email, web, and mobile channels—extensible REST API integrations for leading SIEMs and SOARs, including abuse inbox management playbook.

SlashNext + Microsoft Defender = Complete Email Security

SlashNext SEER™ AI detection engine integrates via API Microsoft and intercepts email before it reaches the user's inbox. Built specifically to stop zero-hour attacks missed by Microsoft Email Security. The chart below shows how SlashNext and Microsoft work together and eliminate the need for a SEG solution like Proofpoint. (Exhibit 3)

SlashNext + Microsoft E5 Together Eliminates the Need for Secure Email Gateways

		proofpoint.	Microsoft E5	SLASHNEXT Complete™	Complete Protection
Secure Email Gateway	Mail Routing and Policy	YES	YES	NO	✔
Zero-Hour Malware Protection	Malware Attachments	YES	YES	YES	✔
	URL Protection	NO	NO	YES	✔
	Teams, SharePoint, OneDrive	NO	YES	YES	✔
Zero-Hour Phishing Protection	Spear Phishing	NO	NO	YES	✔
	External Phishing	YES	YES	YES	✔
	Internal Phishing	NO	YES	YES	✔
	RealTime Awareness Training	NO	NO	YES	✔
	Encrypted Email Protection	NO	NO	YES	✔
Zero-Hour Social Engineering Protection	BEC Executive Impersonation	YES	YES	2H 2022	✔
	BEC Invoice Fraud	YES	YES	YES	✔
Defense-in-Depth URL Analysis	Intelligence Database	YES	YES	YES	✔
	Real Time URL Scan	NO	NO	YES	✔
Outbound Security	Email DLP	YES	YES	NO	✔
Multi-Payload Phishing Protection	Credential Stealing	YES	YES	YES	✔
	Trusted Service Compromise	NO	NO	YES	✔
	Rogueware	NO	NO	YES	✔
	Account Takeover, Supply Chain Attacks	YES	YES	YES	✔
	Smishing/Business Text Compromise	NO	NO	YES	✔
Multi-Channel Phishing Protection	Corporate Mailboxes	YES	YES	YES	✔
	Personal Mailboxes	NO	NO	YES	✔
	Mobile	NO	NO	YES	✔
	Social	NO	NO	YES	✔
	Collaboration/Messaging	NO	NO	YES	✔
SOAR	Incident Response	YES	YES	YES	✔
	Reports and Threat Intelligence	YES	YES	YES	✔
	Brand Protection	YES	NO	YES	✔
FAST ROI	Microsoft Graphic API Integration	NO	N/A	YES	✔
	Out-of-Box Immediate Protection	NO	YES	YES	✔

Performance Stats and Customer Reference

The rise of well-crafted spear phishing is the leading factor in the success of phishing attacks and ransomware. Spear-phishing delivered through trusted cloud services bypass traditional cybersecurity solutions at an alarming rate. In the first half of 2022, SlashNext reported that 80% of phishing emails detected had URLs hosted on trusted services. Threat actors are using tactics like HTML attachments that sandboxing technologies cannot detect. And 69% of emails stopped by SlashNext were zero-hour phishing attempts stopped using our LiveScan™ technology.

80%
of emails with phishing URLs hosted on Trusted Services

69%
of emails contain zero-hour phishing URLs blocked by Live Scan™

22%
of emails with HTML phishing attachments

"SlashNext Email Protection has essentially stopped our employees from interacting with live phishing threats," said John Menezes, Stratejm CEO. This extra layer of protection around our company's people protects them from malicious email and keeps our organization safe from ransomware attacks, account takeovers, financial fraud, and more."

Additional customer references available upon request.

Multi-Channel Phishing Protection for the Modern Workforce with SlashNext Complete™

How people work today has exposed users to cyberattacks, adding to the threats facing organizations. Using multiple devices for work and personal use to communicate and collaborate, combined with the reality of remote work, means millions are regularly working outside traditional security defenses. This means phishing threats – already at record numbers – continue to rise across multiple channels, including Microsoft Teams, Zoom, LinkedIn, SMS/Text, Slack, Telegram, WhatsApp, and others.

Organizations can access a full protection suite through SlashNext Complete™ for multi-channel protection across email, browser, mobile, and API. SlashNext Email Protection and the SlashNext Complete solution work with existing security – including SEGs, endpoint security tools, and Microsoft security built into Microsoft 365. By blocking 99.9% of zero-hour phishing threats before they reach a company's people – through email or another digital channel – the organization becomes much safer from the most prolific rise in cybercrime in recent years.

ABOUT SLASHNEXT

SlashNext protects the modern workforce from phishing and human hacking across all digital channels. SlashNext Complete™ utilizes our patented AI 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 phishing defense services for email, browser, mobile, and APIs that integrate with leading mobile endpoint management and IR services.

CONTACT US

6701 KOLL CENTER PARKWAY, SUITE 250
PLEASANTON CA 9456694588

CONTACT SALES 1(800) 930-8643

START A FREE TRIAL HTTPS://WWW.SLASHNEXT.COM/FREE-TRIAL-REQUEST/