WHITE PAPER

SLASHNEXT SECURITY

SlashNext Cloud Email + Microsoft 365 = Complete Email Protection

How SlashNext AI Augments Microsoft 365 to Stop Zero-hour BEC Attacks and Advanced Phishing Threats.

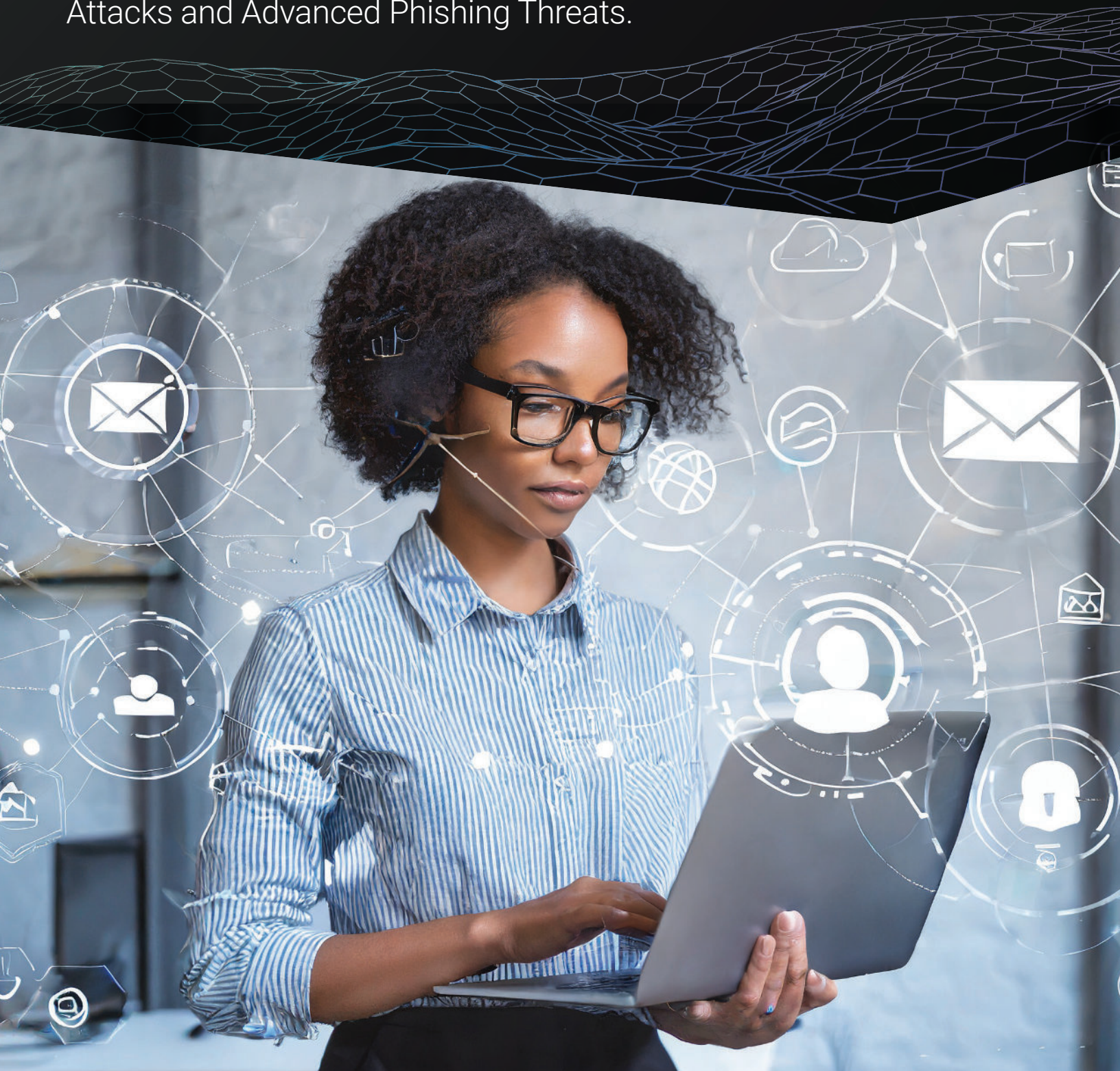


TABLE OF CONTENTS

INTRODUCTION

In today's digital landscape characterized by connectivity and remote collaboration, email is the lifeline for communication, and the prime vector for malicious actors seeking to exploit user vulnerabilities. Recognizing this, Microsoft has bolstered its email security arsenal with Defender for Office 365 (MDO), formerly known as Advanced Threat Protection (ATP), as an additional layer to Exchange Online Protection (EOP). While advanced features like Safe Links and Safe Attachments have rendered traditional secure email gateways less relevant and empowered Microsoft customers to transition away from them, the reality is that only by supplementing Microsoft with an additional AI-based email security solution can organizations achieve sufficient protection against BEC and advanced phishing attacks.

According to the 2023 FBI Internet Crime Report, in the past decade, organizations have lost $17 billion to Business Email Compromise (BEC) attacks alone, highlighting the staggering financial impact of these sophisticated attacks. Augmenting Microsoft with the right cloud email security services can significantly enhance an organization's email security posture and effectively mitigate evolving threats. Furthermore, attackers' expanding focus on adjacent messaging channels such as SMS, WhatsApp, Teams, and Slack highlights the need for a comprehensive security strategy that extends beyond email to safeguard all messaging channels effectively.

This paper reviews Microsoft's native email security capabilities and outlines compelling reasons for considering augmentation. Additionally, it offers practical guidance on selecting the most suitable cloud email security vendor, to effectively combat today's BEC and advanced phishing threats.

BEC and Advanced Phishing Are Big Business

- $2.9B in losses to BEC in 2023 with average of $137k per BEC incident
- 30% of social engineering threats are opened by employees
- 91% of successful cyber breaches start with a phishing attack

WHY AUGMENTING MICROSOFT 365 EMAIL SECURITY IS THE RIGHT CHOICE FOR TODAY'S THREAT LANDSCAPE

As organizations navigate the evolving landscape of email security challenges, it quickly becomes evident that relying solely on Microsoft's native security measures will leave them vulnerable to sophisticated attacks. While Microsoft's rule and signature-based detection technologies provide a strong baseline protection against low-effort, high-volume phishing attacks, they often lack adequate defense against BEC and advanced phishing threats.

A recent independent study of Cloud Email Security Vendors tested detection accuracy for BEC and advanced phishing threats, conducted by The Tolly Group, revealed Microsoft EOP and MDO missed 77% of BEC and advanced phishing threats. This sobering statistic highlights the need to augment Microsoft's security measures. API-based email security service, like SlashNext consistently identifies thousands of high-impact attacks a week for customers solely using Microsoft native protection. Highlighting that using Microsoft native protection alone will leave organizations vulnerable to executive impersonation, vendor invoice fraud, QRishing, and credential phishing. The potential ramifications of these missed attacks are significant, posing financial liability and harm to the targeted organizations.

In addition, the abuse of Generative AI tools has exacerbated this issue, enabling attackers to carry out BEC and advanced phishing attacks at unprecedented scale, ease and accuracy, making it increasingly difficult for Microsoft to keep up with the evolving threat landscape.

Independent Test Reveals Threat Types Most Missed by MS 365

- 77% — Percentage of BEC and advanced phishing attacks are missed by Microsoft EOP and MDO.
- 1,000+ — High impact emails that are missed by Microsoft 365 per week for average customer.
- 1,265% — increase in phishing emails since the launch of Generative AI.

SELECTING THE RIGHT SOLUTION FOR AUGMENTATION

The first step in determining the right augmentation solution is to understand the security features provided by Microsoft, in order to effectively identify the gaps and determine the specific enhancements needed to fortify your organization's defenses.

Exchange Online Protection

At the core of Microsoft 365 security lies Exchange Online Protection (EOP), which serves as the first line of defense against email threats. According to Microsoft's own knowledgebase article, EOP focuses on preventing broad, volume-based and known attacks. Its security features are limited to:

- Connection management – blocks known spam from IP addresses with poor reputation.
- Malware scanning – quarantines known malware.
- Content filtering – identifies known phishing and spam.

In essence, EOP provides base-level email security capabilities using sender reputation and signatures.

Defender for Office 365 Plan 1

Microsoft Defender for Office 365 (MDO) P1, formerly known as Advanced Threat Protection (ATP), is part of the E5 license and is also available as an add-on purchase. While EOP protects against known attacks, MDO adds additional capability to protect email against zero-day threats. With MDO layered on top of EOP, organizations gain the following key security features:

- Safe Attachments – Malware scanning using a virtual environment.
- Safe Links - Checks for known malicious URLs when users click on links in emails.
- User impersonation – Prevents specific internal or external email addresses from being impersonated, using a manually created custom list.
- Domain impersonation - Prevents specific domains in the sender's email address from being impersonated, using a manually created custom list.
- Advanced Phishing Thresholds - Configure different actions based on confidence level of the phishing verdict. It does not increase the number of phishing emails detected.

While MDO's security features are more advanced than what base-level EOP provides, it is still largely signature and rule-based.

Key Criteria for Selection

In addressing the critical need for protection against BEC and advanced phishing threats, organizations should aim to achieve both budgetary and operational efficiencies by selecting a solution that complements Microsoft EOP and MDO. The goal is to enhance existing capabilities to achieve greater protection, without introducing security feature redundancy. The following are the key criteria for selecting the best solution:

- AI Native: Select an AI native solution that provides BEC Gen AI, natural language processing, computer vision, relationship graphs, and contextual analysis.
- Comprehensive Threat Vector Coverage: Choose a solution that offers zero-hour protection for all four threat vectors: BEC/plain-text, QRishing, link, and file-based threats.
- Zero-hour Threat Protection: Prioritize solutions with in-house technologies for zero-hour protection. Avoid vendors that rely on third-party intelligence feed updates for specific threat vectors, as this introduces delays in identifying and mitigating zero-hour attacks.
- Protects Adjacent Messaging Channels: Seek a solution that can also protect against phishing attacks delivered via SMS, WhatsApp, personal email, Teams, and other collaboration tools on mobile devices and computers. It's essential to recognize that executive impersonation attacks sometimes involve multi-channel tactics, with perpetrators leveraging SMS in later stages to fully compromise targets.
- Built for Microsoft: Select a solution that seamlessly integrates using Microsoft Graph API. API-based solutions ensure Microsoft EOP and MDO continue to function as designed. Avoid MX record-based Secure Email Gateways (SEGs) that may require disabling Microsoft security features for functional compatibility.
- Avoiding Feature Duplication: Maximize security budget efficiencies by ensuring that efforts to enhance email protection do not duplicate capabilities already provided by Microsoft. This includes avoiding the augmentation of Microsoft with SEGs, as it may lead to duplications in technology without providing additional protection and value.

One Last Thing: Generative AI Threats

Look for a solution equipped to combat BEC, and advanced phishing threats created by threat actors using generative AI tools. The solution should incorporate sophisticated AI technologies capable of predicting and mitigating BEC attacks orchestrated with the assistance of AI-generated tools.

SLASHEXT AI ENHANCES MICROSOFT 365

Top Decision Criteria

- Select a solution that is AI native, and purpose built to augment Microsoft 365 security for budgetary and operational efficiencies.
- Seek an AI solution that predicts and stops Gen AI threats as threat actors increasingly exploit Gen AI tools to orchestrate sophisticated BEC attacks.
- Choose a platform that protects email as well as adjacent messaging channels.
- Avoid vendors that rely on third-party intelligence feed updates for specific threat vectors, as this introduces delays in identifying and mitigating zero-hour attacks.

Organizations often inquire which approach is superior: Microsoft EOP and MDO's rule and policy-based system or our Cloud Email Security service powered by SlashNext AI. The answer lies in recognizing the distinct roles each plays in protecting your users. While Microsoft's native email security effectively mitigates high volume "spray and pray" phishing campaigns, our Next-Gen AI Email Security is purposefully engineered to combat targeted BEC and advanced phishing threats. By combining forces with Microsoft, the combination delivers a comprehensive email security strategy tailored to safeguard your organization.

The SlashNext AI Security platform is described in the following sections.

BEC Gen AI

Aptly termed "Using Gen AI to fight Gen AI," BEC Gen AI generates all possible variants of a BEC email while preserving the original message's topic, emotion, and intent. This innovative capability enables the prediction of new BEC patterns and serves as a proactive measure to predict and stop future BEC attacks.

Natural Language Processing and Parallel Prediction

Employed to analyze the language used within emails, comprehending the topic, emotion, and intent to detect suspicious calls to action. Additionally, Parallel Prediction enhances the effectiveness of NLP in identifying BEC emails by offering a secondary opportunity for analysis. In cases where the initial scan fails to identify malicious intent, this iterative process evaluates email variants generated by BEC Gen AI, reducing the risk of false negatives and enhancing overall accuracy.

Relationship Graphs and Contextual Analysis

Dynamically analyzes historical and current data to develop a comprehensive understanding of your employees' communication styles, language patterns, behavior, and relationships with both internal colleagues and external senders. By leveraging this contextual awareness, SlashNext AI can detect deviations from known good communication patterns between senders and receivers, which are often indicative of phishing and impersonation attempts.

Computer Vision

Computer Vision technology utilizes sophisticated algorithms to scrutinize visual elements within webpages, including layouts, logos, and textual content. This meticulous analysis enables the detection of subtle anomalies that may signal attempts at credential harvesting, scamming, or the presence of malicious websites. This comprehensive analysis is applied to email links and email attachments.

Virtual Browsers

Virtual Browsers technology acts as a preprocessing step by simulating a web browser environment to open email links, files, and URLs extracted from QR codes. This enables subsequent computer vision analysis to accurately identify potential threats such as credential harvesting and malicious webpages. Moreover, Virtual Browsers technology allows the service to circumvent defensive measures like CAPTCHA, ensuring thorough inspection of webpages and files.

API Architecture

Unlike traditional secure email gateways, SlashNext seamlessly integrates with Microsoft using its Graph APIs, ensuring quick deployment without disrupting mail flow. This API architecture allows our

platform to provide a defense-in-depth approach alongside Microsoft's native email security capabilities, offering comprehensive protection against the widest range of threats.

SlashNext is a member of the Microsoft Intelligent Security Association (MISA) and partners with Microsoft in various ways, actively developing integration capabilities, including API Integration:

- To sync historical email data.
- To sync users and groups.
- To provide single sign-on.
- With Sentinel for advanced email analytics.

Business and AI Threat Insights

SlashNext offers comprehensive visibility into all detected threats across email and other messaging channels. Through intuitive dashboards and executive summary reports, security teams can easily access information about high-impact security events. These insights enable security teams to enhance the overall security hygiene of their email platform and provide valuable data for assessing the return on investment (ROI) of our Next Gen AI Email Security service.

One Last Thing: Email+

The modern workforce is hybrid and increasingly using personal devices to access business applications, requiring cybersecurity leaders to focus on multi-channel security. Cybercriminals are capitalizing on digital channels that aid in the productivity of remote workers, like SMS/Text, Slack, LinkedIn, Zoom, Microsoft Teams, Google Meet, and WhatsApp. These channels are less protected and provide an easy way to trick users, steal credentials, and ultimately exfiltrate data from an organization. It's common for email executive impersonation attacks to initiate in email and subsequently transition to SMS in later stages to compromise users. SlashNext's Email+ platform detects, predicts and stops zero-hour social engineering threats in over 3K+ email, mobile and browser messaging apps

SlashNext Next-Gen AI Email Security Includes:

- API-based Cloud Email Security: Next Gen AI detects BEC and advanced phishing threats for inbound, outbound, and internal emails, with 48hr detection advantage.
- Comprehensive Threat Coverage: Uniquely trained AI classifiers identify all forms of BEC, social engineering and advanced phishing threats with accuracy and precision.
- AI Threat Insight: Delivers advanced security analytics, offering comprehensive insights into the rationale behind AI's classification of threats.
- Spam/BulkMail: Automatically detects and removes unsolicited bulk emails from user inboxes to improve employee productivity and reduce SecOps hours spent on abuse inbox management.
- Email+ Security: Extends protection to adjacent channels, such as SMS, Slack, Zoom, Teams, Gmail and other messaging apps on mobile devices and computers.
- Unified Administration Console: A single pane of glass for deployment, configuration, and reporting.
- API Integration Ecosystem: Seamlessly ingest advanced security events into Microsoft Sentinel, Splunk, or any SIEM solution.

MAXIMIZE EFFICACY, PRODUCTIVITY, AND ROI

Budgetary and operational efficiencies will be realized when selecting a solution that offers AI native technology, and is purpose built to augment Microsoft 365. SlashNext's Cloud Email Security's native AI technology delivers the highest efficacy and stops threats before they ever reach users resulting in maximum productivity and return on investment.

Maximum Efficacy

SlashNext's Cloud Email Security's advanced AI platform is purpose built to anticipate and stop the vast numbers of sophisticated BEC threats, phishing, and ransomware. The service delivers industry leading 99.9% detection rate and 1 in 1 million false positive rates by utilizing Gen AI, natural language parallel prediction, computer vision, relationship graphs, and contextual analysis for:

- Broad threat coverage due to large and diverse LLMs
- Highest accuracy and a 48-hour detection advantage to stop sophisticated zero-hour threats.
- 360° protection with threat protection across all messaging channels: in email, mobile and web.

SlashNext's Cloud Email Security's advanced AI platform increases SecOps and user productivity because the highest detections and the lowest false positives rates reduces the number of emails that reach users resulting in the reduction of time spend researching and remediating threats by SOC teams.

Maximum Productivity and ROI

A large-scale phishing campaign against a large enterprise could result in 20,000 emails hit an organization systems. Even if only 5% of the users report the emails, it could result in the handling of up to a 1,000 emails. The remainder of the time is spent addressing SIEM incidents, security tool alerts and other tasks. Within 24 hours of deploying SlashNext Cloud Email Security users , malicious emails flagged by SlashNext and not even being reported to the security team saving a significant amount of time. SlashNext stopped attacks before they are delivered into user's inboxes, reducing abuse email reviews by nearly 80% saving an average of 6,000 SecOps hours saved annually allowing the security team to dive into the other tasks critical to organizations security posture.

In evaluating the ROI of our product, it is instrumental to look at its impact through a multifaceted lens, including user productivity, potential risk of loss, and the optimization of SOC resources.

Starting with user productivity, our product significantly reduces the interruption caused by phishing and other malicious emails. An illustrative example of this is when, within 24 hours of deployment in a large enterprise, our solution drastically cut down the need for employee intervention in reporting suspicious emails. In a scenario where an organization could receive 20,000 malicious emails from a phishing campaign, the efficiency of preemptive filtering becomes evident, allowing employees to remain focused on their primary responsibilities without the distraction of security concerns.

When considering the potential risk of loss, the importance of early and effective threat interception cannot be overstated. By stopping attacks before they reach user inboxes, our technology not only prevents the immediate threats but also significantly lowers the chance of successful breaches. This preemptive action is crucial in averting financial and reputational damage that can arise from security

incidents.

Lastly, the benefit of reduced SOC resource allocation is quantified through significant savings in operational hours. By automating the threat detection and neutralization process, our product frees up SecOps teams to concentrate on more strategic tasks. For instance, in an example scenario, the deployment of our solution resulted in nearly 80% reduction in abuse email reviews, translating to an impressive 6,000 hours saved annually for SecOps teams. This time savings allows for a more effective allocation of resources towards enhancing the organization's overall security posture.

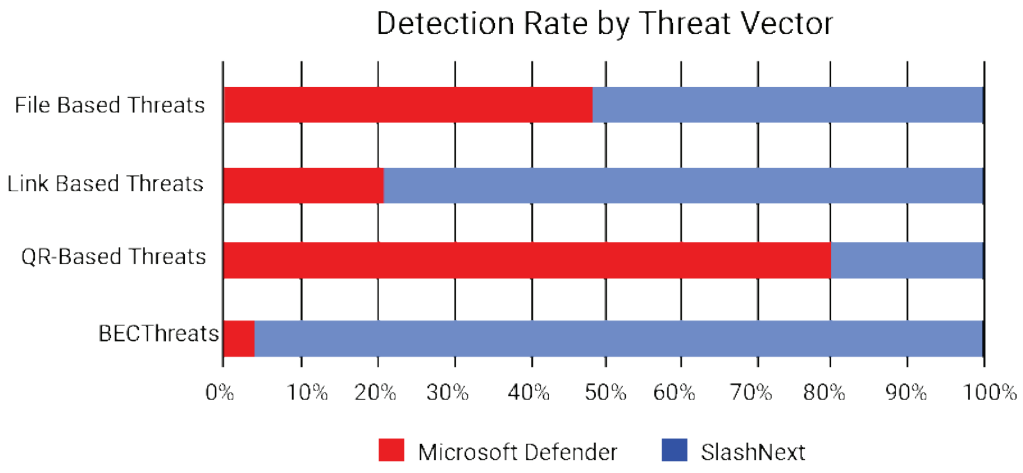
Through this lens, the example of handling a large-scale phishing campaign vividly illustrates the broader impacts of our product on enhancing operational efficiency, reducing risk, and optimizing resource allocation, underpinning the comprehensive value proposition of our solution.

Conclusion

Microsoft alone cannot address the complexities of today's BEC and advanced phishing threats. SlashNext's Next Gen AI Email+ Security offers a fundamentally different approach, leveraging cutting-edge artificial intelligence to detect and mitigate sophisticated attacks in email, SMS, Slack, Teams, and other messaging apps. With the average cost of a BEC incident is $137K and organization can save $3.35M annually by mitigating BEC threat risk with SlashNext.

As mentioned earlier, a recent independent study, conducted by The Tolly Group revealed Microsoft EOP and MDO missed 77% of BEC and advanced phishing threats . This statistic is further corroborated by what SlashNext see their customer base and prospect trials. SlashNext's API-based email security service consistently identifies thousands of high-impact attacks each week for customers solely using Microsoft native protection, including executive impersonation, vendor invoice fraud, QRishing, and credential phishing. The potential ramifications of these missed attacks are significant, posing financial liability and harm to the targeted organizations.

Microsoft Defender + Slashnext are Better Together on Advanced Threats



Tolly Study Testing of 300 Advanced Threats, March 2024

About SlashNext

SlashNext protects the modern workforce from malicious messages across all messaging channels. SlashNext Complete™ integrated cloud messaging security platform uses patented generative AI 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 many 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.

For more information, visit www.SlashNext.com

Schedule a customized email risk assessment at https://slashnext.com/risk-assessment

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

REV 240321-000