The State of Phishing

In 2022, cybercriminals are moving with speed and at scale. Mobile phishing and credential harvesting are exploding, causing breaches in places once thought impenetrable. With billions of dollars, company reputations, and personally identifiable information at stake, advanced phishing protection is vital for all businesses.

EXECUTIVE SUMMARY

Since we last published our State of Phishing Report in 2021, some trends remain the same and much has changed. What is consistent is that phishing continues to explode. Hybrid work and the use of personal mobile devices for work continue to be a trend, and the bad actors are taking full advantage of the fact that many security technology vendors cannot keep up. What has changed is important.

Imagine the familiar metaphor of Whac-A-Mole when thinking about cybersecurity professionals trying to stop one phishing attack, only to see another new attack pop up someplace else. That metaphor no longer describes the state of phishing. Today the appropriate metaphor is The Matrix fight scene where Neo fights 195 Smiths at once, and the potential for Smith to morph and multiply is endless.

However, it's not all doom and gloom. This report demonstrates how phishing has changed through the lens of cybersecurity technology. We can only present the data in this report because technology is available to detect these trends and stop more threats. For example, at the end of 2021, we detected 50,000 malicious URLs daily, a 68% increase from the start of the year. Less than 12 months later, we detected 80,000 malicious URLs daily, which is another 61% increase. This equates to 255M phishing attacks detected in 2022. Certainly, there is an increase in phishing, and as cybersecurity tools improve, the industry is also detecting and stopping more attacks.

Finally, this report will dive into some of the most pervasive threats, including the shift to multi-channel phishing, sophisticated credential harvesting on email, and the massive increase in threats emanating from trusted services. With an 80% increase in threats from trusted services in 2022, we started to track these threats in a unique database in 2022.

IN THIS REPORT

- What big trends from 2021 continued in 2022, and what this likely means for the future
- Mobile, mobile, mobile — And other personal communication channel threats
- Email trends with Microsoft and ICES
- Threats menacing trusted services and the top 10 services hackers use for attacks
- Summary of key findings
- How an integrated, multi-channel security approach is needed

Report data and methodology: The report data is taken from a sample of threats detected by SlashNext security products. SlashNext analyzed over a billion link-based, malicious attachments and natural language threats scanned in email, mobile and browser channels over six months in 2022. The organizations in our sample ranged in size from 500 to 100,000 users. The organizations spanned a variety of industries in North America.

The threat data in the report is gathered using SlashNext's Two-Phase AI Detection, which uses virtual browsers, machine learning, and LiveScan™. This approach detects live and emerging zero-hour threats. Our cloud-based AI detection is preemptive with proactive threat hunting to detect phishing, scams, malware, and exploits, revealing approximately 700,000 attacks a day. Secondarily content is analyzed in real-time with LiveScan™ to reveal zero-hour threats automatically.

BIG TRENDS

People are the most vulnerable part of an organization when it comes to phishing, scams, and fraud. They are also the most unprotected across all communication channels. For hackers, phishing is the most effective and far-ranging tool to perpetrate cybersecurity breaches, including lucrative ransomware and data theft.

In 2021 we highlighted several high-profile breaches that started with phishing, and that trend continues. From pre-pandemic 2019 to post-pandemic 2022, phishing has increased consistently, with a 61% jump in malicious URLs from 2021 *(Exhibit 1)*. The jump in malicious URLs equates to 255M phishing attacks detected in 2022. 76% of the attacks found in 2022 were credential harvesting, which is still the number one cause of breaches, as demonstrated in the high-profile breaches in 2021 and again in 2022 with Twilio, Cisco, and Uber, all starting with credential theft.

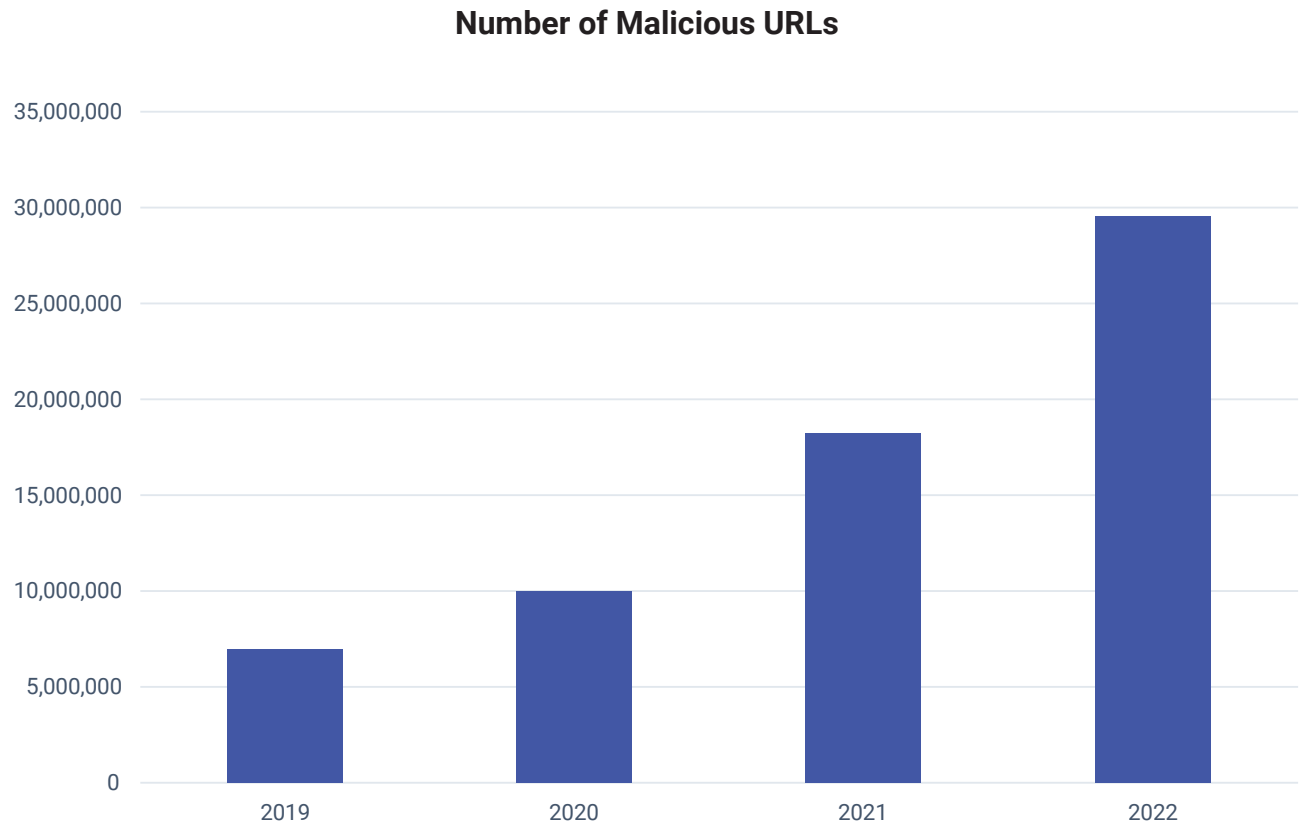


Exhibit 1: Malicious URLs from 2021 to 2022 has increased by 61%, equating to 255M phishing attacks detected in 2022.

Zero-Hour Threat Trends

The big standout trend in 2022 is the rise in zero-hour (never seen before) threats. 54% of threats detected by SlashNext in 2022 are zero-hour attacks, representing a 48% increase in zero-hour threats from the end of 2021 *(Exhibit 2)*. The increase in the numbers of zero-hour attacks being detected by threat intel vs. live scanning demonstrates how hackers are paying attention to what works and what gets stopped. The chart shows how hackers adapt and change tactics until they find success, highlighting the importance of having detection that can detect and mitigate evolving threats. These threats come from link-based attacks, malicious attachments, and natural language threats. Cybercriminals can send thousands of targeted spear phishing attacks using automation and machine learning to increase the likelihood of compromising a target by matching data to build detailed lists of targets to make each attack unique and customized to the victim to increase their success. This tactic enables the threat to bypass many threat detection engines for hours and sometimes days.

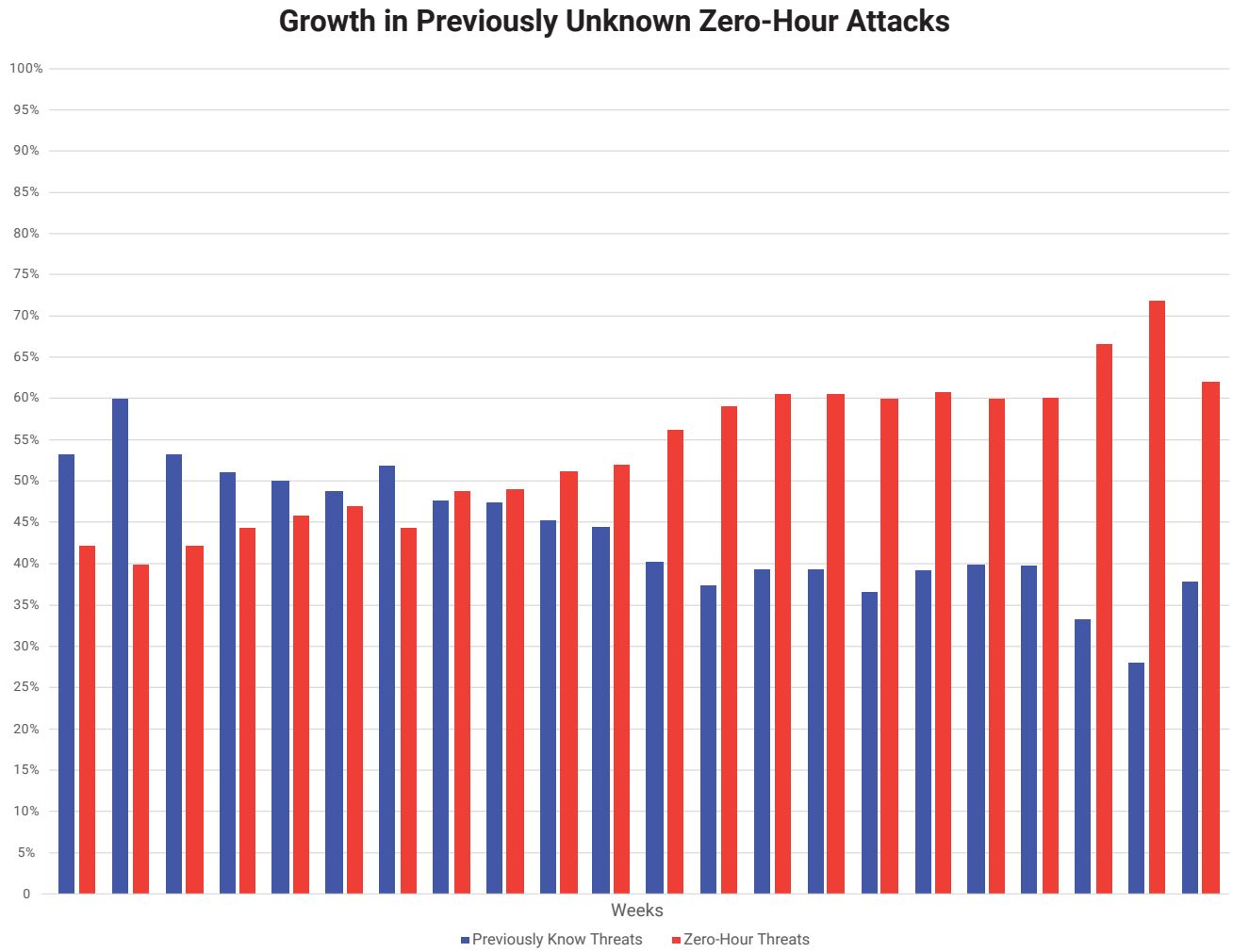


Exhibit 2: 54% of threats detected by SlashNext in 2022 are zero-hour, which is a 48% growth in zero-hour threats in 2022.

Zero-hour threats are designed to make the biggest impact before security controls detect and block them. These methods are particularly effective for delivering credential stealing attacks. Of the zero-hour attacks detected, 76% were spear phishing credential harvesting. Credential harvesting starts the attack chain for ransomware, data exfiltration, and cyber espionage. The top three most frequently detected zero-hour threats are credential harvesting (by a landslide), followed by social engineering scams, malware, ransomware, and exploits.

Top Three Zero-Hour Threats		
1	Credential harvesting	76%
2	Scams	15%
3	Malware, ransomware, and exploits	1%

Exhibit 3: Of the zero-hour attacks detected, 76% were spear phishing credential harvesting.

The increase in zero-hour threats is also impacting industries differently. The healthcare industry receives more zero-hour threats than other industries with 86% all threats detected falling into the zero-hour spear phishing attack category vs. previously known threats *(Exhibit 4)*.

Top Five Industries Targeted the Most By Zero-Hour Threats	
1	Healthcare
2	Professional and Scientific Services
3	Information Technology
4	Construction and Engineering
5	Finance and Insurance

Exhibit 4: Industries receiving more zero-hour spear phishing attacks.

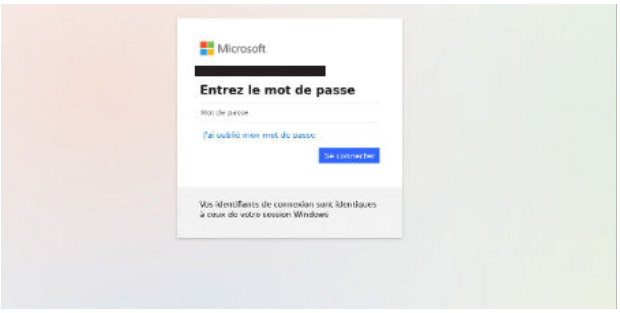
The 61% increase in phishing and the rise of zero-hour credential harvesting attacks is a powerful combination. Security controls should include AI-based technology that preemptively hunts threats and the ability to scan for threats in real-time. While training is important, training alone cannot stop the speed, scale, and sophistication of zero-hour threats. Without this technology, users and organizations are at great risk of suffering a breach. Once a user's credentials are compromised, the threat is further mobilized and can be catastrophic to the enterprise. Breaches are tremendously costly. It's not just the loss of critical business or customer data; there's a risk of loss of IP, shareholder value, lawsuits, financial payouts, and more. These are just a few consequences a company can face when their employees fall victim to these attacks.

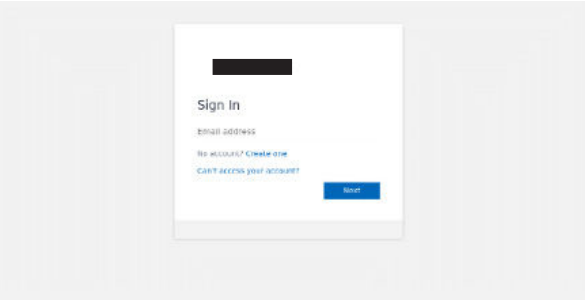
Rise of Multi-Channel Threats

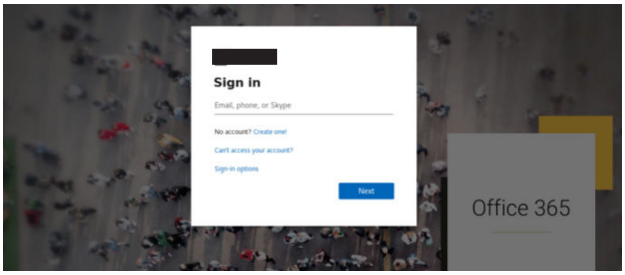
Multi-channel phishing is fast becoming the preferred way for cybercriminals to deliver successful attacks because they know the gaps in cyber defenses. While organizations focus on protecting email from phishing and malware, they often overlook security defenses for other channels. They are leaving other communication channels vulnerable to cybercriminals, allowing a clear path to target high-value users.

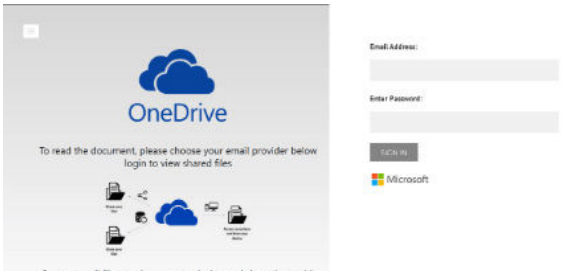
The modern workforce is hybrid and increasingly using personal devices to access business applications, requiring cybersecurity leaders to focus on multi-channel security. Cybercriminals are capitalizing on digital channels that aid the productivity of remote workers, like SMS/Text, Slack, LinkedIn, 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.

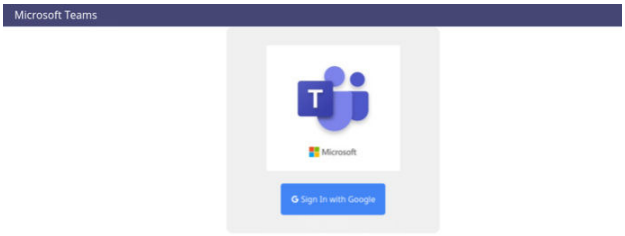
A growing multi-channel trend observed by SlashNext is cybercriminals sending spear phishing attacks, impersonating coworkers through WhatsApp and SMS to send URLs masquerading as MS Teams invites to harvest Microsoft 365 credentials. The benign invite contains a malicious URL that takes the user to a landing page to log in to the meeting and asks them to enter their Microsoft 365 credentials, and just like that, a user has given up their credentials *(Exhibit 5)*.

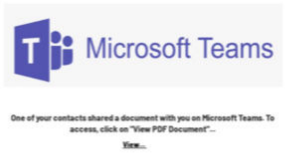


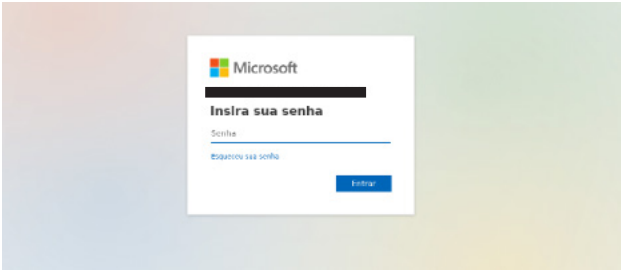












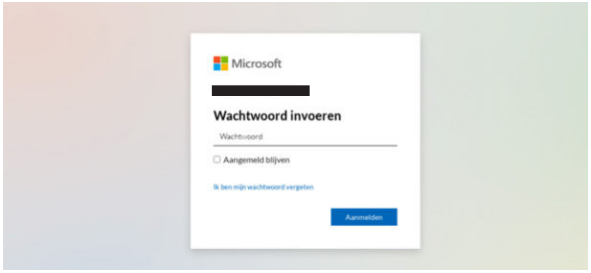


Exhibit 5: Global examples of spear phishing attacks to harvest Microsoft 365 credentials.

MOBILE, MOBILE, MOBILE

And Other Personal Communication Channel Threats

SlashNext recorded a 50% increase in attacks on mobile devices, with scams and credential theft at the top of the list of payloads. Security professionals expressed little concern over smishing and mobile attacks before high-profile breaches, including those at Uber, Twilio and Cloudflare made global headlines. Now mobile phishing attacks are on the rise, with 83% of organizations reporting mobile device threats growing more quickly than other device threats, according to Verizon Mobile Security Index 2022.

Three high-profile breaches in 2022 at Uber, Twilio, and Cloudflare, demonstrate the rise in SMS phishing attacks to successfully harvest credentials at the start of the attack chain to perpetrate a breach. These attacks were well-planned and executed. They are hard to identify by users, meaning organizations can't rely on employee training to stop SMS and other communication channel attacks.

Most threats on mobile start with SMS text messaging. Scams and spear phishing delivered through SMS text are credential stealing, malware, and exploits. These attacks are customized specifically for mobile delivery and designed to only work for Mobile iOS or Android. What makes them most dangerous is that most mobile devices do not have SMS phishing protection to block these attacks. *(Exhibit 6)*.

Exhibit 6: Example of malicious SMS attacks on mobile

EMAIL TRENDS- ICES AND MICROSOFT EOP

According to Gartner, 70% of organizations use cloud email solutions, but they are concerned about complexity and security 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 and is very good at detecting spam at 99%. Emails that Microsoft believes to be good are delivered to users' mailboxes. However, they do not have a good track record with sophisticated zero-hour threats, including BEC, Account Takeover, and supply chain attacks.

SlashNext data shows that 22% of malicious threats get through Microsoft EOP, which can leave a 20,000 user inboxes organization with as many as 500,000 emails a day entering the organization that could be targeting users with phishing, malware, exploits, and social engineering threats. In order to maintain effective security controls across the organization, supplemental email security is required.

THREATS MENACING TRUSTED SERVICES

One-third, 32%, of all threats detected are by SlashNext in 2022 are hosted on trusted services including Microsoft, AWS, and Google to name a few. Phishing and malware threats hide behind trusted services as part of the evolution of hackers using trusted domains to host their attacks.

Trusted domains are used to give attackers more anonymity. It's hard for users to identify these types of attacks, and taking down this malicious content is often more complex, which gives hackers more time to perpetrate these attacks.

In 2022, SlashNext detected many phishing threats hosted on ipfs.io, Cloudflare-ipfs.com, and other vendors. We feel it's important to call out that these attacks are part of the evolution of hackers using trusted domains to host their phishing attacks because they are hard to detect, and we have seen breaches this year using ipsf. The benefit of using these types of trusted domains is that they are very hard to detect with reputation-based threat detection and will not be flagged by security vendors immediately. Hence, hackers choose to use trusted ipsf gateways.

Trusted domains are used for various phishing attacks, not just ipfs, but ipfs may make takedown of the phishing content more complex, especially if they use a botnet to host content.

The Top Services Hackers Used For Attacks

IPSF
Digital Ocean
Amazon AWS
Fleek
Siasky.net
Google
Microsoft
Evernote
GoDaddy
Weebly
Adobe
Box
Shopify

The Most Impersonated Global Brands

Microsoft
Google
DocuSign
Adobe
DropBox
Stripe
Box
ADP
Facebook
Instagram
WhatsApp
PayPal
Discord
Apple
Bank of America
Amazon
Wells Fargo
Netflix

SUMMARY OF KEY FINDINGS

The results in the report highlight how people work today has exposed them to more cyberattacks, adding to the threats facing organizations. The increase in phishing, over 300% since 2019, is not as significant as how the techniques and methods have evolved. There are three key findings that, in our opinion, demonstrate a shift in cybercriminals' tactics that should inform organizations on where to focus security priorities.

- 50% increase in mobile phishing threats
- 54% rise in zero-hour threats with a 78% focus on delivering well-crafted zero-hour spear phishing attacks
- Increase in threats hosted on trusted services, including Microsoft, AWS, and Google

With the 50% increase in mobile phishing threats and organizations citing a rise in mobile threats (Verizon MSI), the trend will most certainly continue. Add in the Twilio and Uber breaches, and it's clear organizations are not fully covered in mobile. There are 6.5 billion mobile devices globally, and most are not managed devices. Many use the same devices for work and personal use, combine that with remote work, and millions of users regularly work outside traditional security defenses. Making a mobile security plan to protect against SMS and text phishing, where most of the threats start, is a good defense against breaches. Adding mobile protection for Microsoft Teams, Zoom, LinkedIn, Slack, Telegram, and WhatsApp will ensure that an organization is ready for the growth in mobile attacks.

The 54% rise in zero-hour threats with a 78% focus on delivering well-crafted zero-hour spear phishing attacks is the leading factor in the success of phishing attacks and ransomware. Automation has made delivering these targeted phishing attacks at scale a fast and easy endeavor for bad actors. Their technology is sophisticated and can quickly detect if an attack was detected, and they can quickly change techniques to ensure higher success. Security controls should include phishing defense that can detect threats preemptively and also in real-time to stop never seen before threats quickly. Stopping the attack chain is critical because once credentials are harvested, a major breach can happen in hours.

Threats hosted on trusted services will continue to grow because it's a successful technique to avoid detection. These threats are hard to detect quickly with reputation-based and relationship graph technologies. Once the threat is detected, it can be hard to take down, which gives hackers even more time to keep these attacks live.

HOW AN INTEGRATED, MULTI-CHANNEL SECURITY APPROACH IS NEEDED

SlashNext Integrated Cloud Messaging Security provides zero-hour AI-based protection for threats in email, mobile, and web messaging apps – Outlook, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Teams, 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 integrate into email, mobile, and browsers to block 99.9% of zero-hour phishing threats before they reach users. Hence, organizations will become much safer from the most prolific rise in cybercrime in recent years.

Extremely Accurate Two-Phase AI Detection

SlashNext exclusively focuses on Integrated Cloud Messaging Security by inspecting billions of URLs at cloud scale with virtual browsers to overcome sophisticated evasion techniques. With patented two-phase AI detection at scale to detect the most evasive zero-hour threats using virtual browsers, machine learning, and LiveScan™ to stop account takeover, credential harvesting, ransomware, malware, and exploits.

The SlashNext Advantage is Your Advantage

- **Preemptive:** Global, proactive threat hunting provides advanced visibility, detection, and protection from emerging threats
- **Real-Time:** Real-time, automated scanning provides more effective protection from zero-hour threats
- **Quick and Accurate:** 48-hour detection advantage with a 99.9% detection rate and 1 in 1 million false positives
- **Overcomes Evasion Tactics:** Overcomes evasive techniques like Captcha & IP restrictions, URL obfuscation, and attacks using compromised websites and trusted services.
- **Multi-Channel Protection:** Protect corporate email to personal mailboxes, web and mobile threats on MS365, SharePoint, Zoom, SMS, LinkedIn, WhatsApp, and other messaging channels
- **Multi-Payload Protection:** Stop account takeover, credential harvesting, BEC, ransomware, malware, exploits, social engineering, and advanced zero-hour attacks.
- **Integrated Cloud Security:** Protection for email, mobile, web, and brand protection.
- **Fast Deployment:** Works out of the box in 5 minutes

About SlashNext

SlashNext protects the modern workforce from malicious messages across all digital channels. SlashNext Complete™ integrated cloud messaging security platform utilizes patented 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, What'sApp, 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.

Contact Us

6701 Koll Center Parkway, Suite 250
Pleasanton CA 9456694588

Contact Sales 1(800) 930-8643

Request a Demo https://www.slashnext.com/request-a-demo/