REPORT

SLASHNEXT

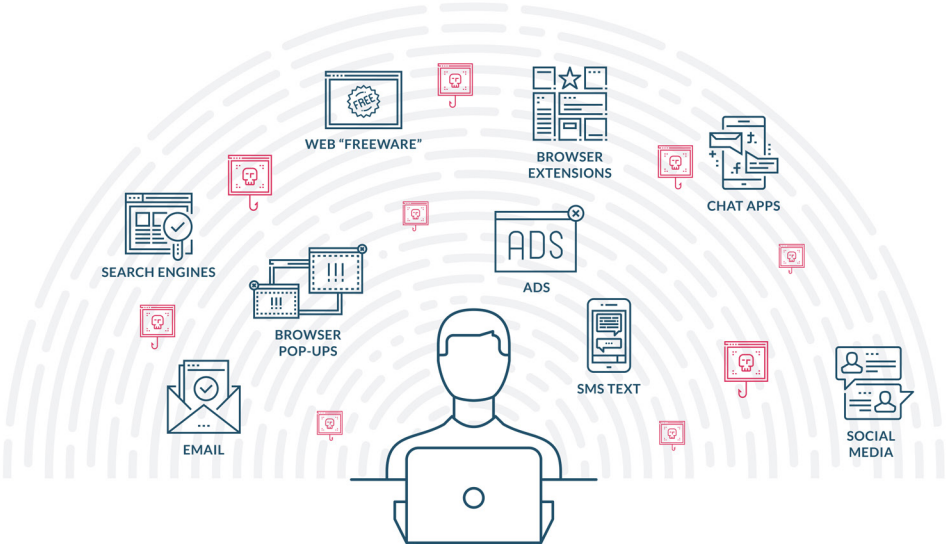
# Defending Against Zero-Hour Phishing Threats with AI Phishing Defense

## THE NEW PHISHING LANDSCAPE

Malware was once a prominent threat to internet users. Phishing was present, but it was not the number one threat action, as it is today. Phishing is favored because when it comes to infiltrating an organization's assets, personal data phishing has become the first choice for bad actors. Threat actors are going after the human attack surface with new kinds of phishing and social engineering techniques, tactics, and procedures.

While credential-stealing delivered via email remains popular, new phishing categories using new attack vectors are evading existing multi-level security controls. The classical phishing paradigm was you'll get an email with a link to a fake log-in page. That is no longer the case—There are multiple phishing threat types, and they are spread beyond email to mobile, SMS, social, collaboration, and search services.

## EMAIL PHISHING PROTECTION NO LONGER ENOUGH



## EXECUTIVE SUMMARY

Today's threat actors are leveraging advanced phishing techniques, while businesses are still using legacy phishing protection, which relies on domain reputation, URL inspection, and resource-heavy human forensics. The only way to effectively stop the dramatic rise in phishing attacks is to move beyond legacy phishing detection, to 2.0 AI-driven dynamic run-time analysis. SlashNext exclusively focuses on 2.0 AI phishing detection by inspecting billions of URLs at cloud speed and scale, employing simulations that overcome sophisticated evasive techniques. By leveraging natural language processing, computer vision, and behavioral analysis, SlashNext detects and blocks threats hours and sometimes days before vendors using old phishing techniques.

SlashNext Browser and Mobile AI Phishing Defense offer anywhere, anytime zero-hour protection against the broadest range of phishing threats. A simple, intuitive user experience blocks threats, alerts users with a warning page, and offers a safe preview with information about the threat.

Additional key features and benefits:

- Broadest Range of Protection: Protects against attacks on corporate and personal email, SMS, social media, messaging, and collaboration platforms by detecting credential stealing, rogue browser extensions, and more.
- Lightweight App & Extension: Negligible impact on battery consumption and device performance.
- No Personal Identifiable Information (PII) or Privacy Risks: No network traffic or personally identifiable information leaves the device, so PII and user privacy remain secure.
- Real-Time Training: Simultaneously detects, blocks, and educates at the point of click to reinforce training and remind users about real threats.

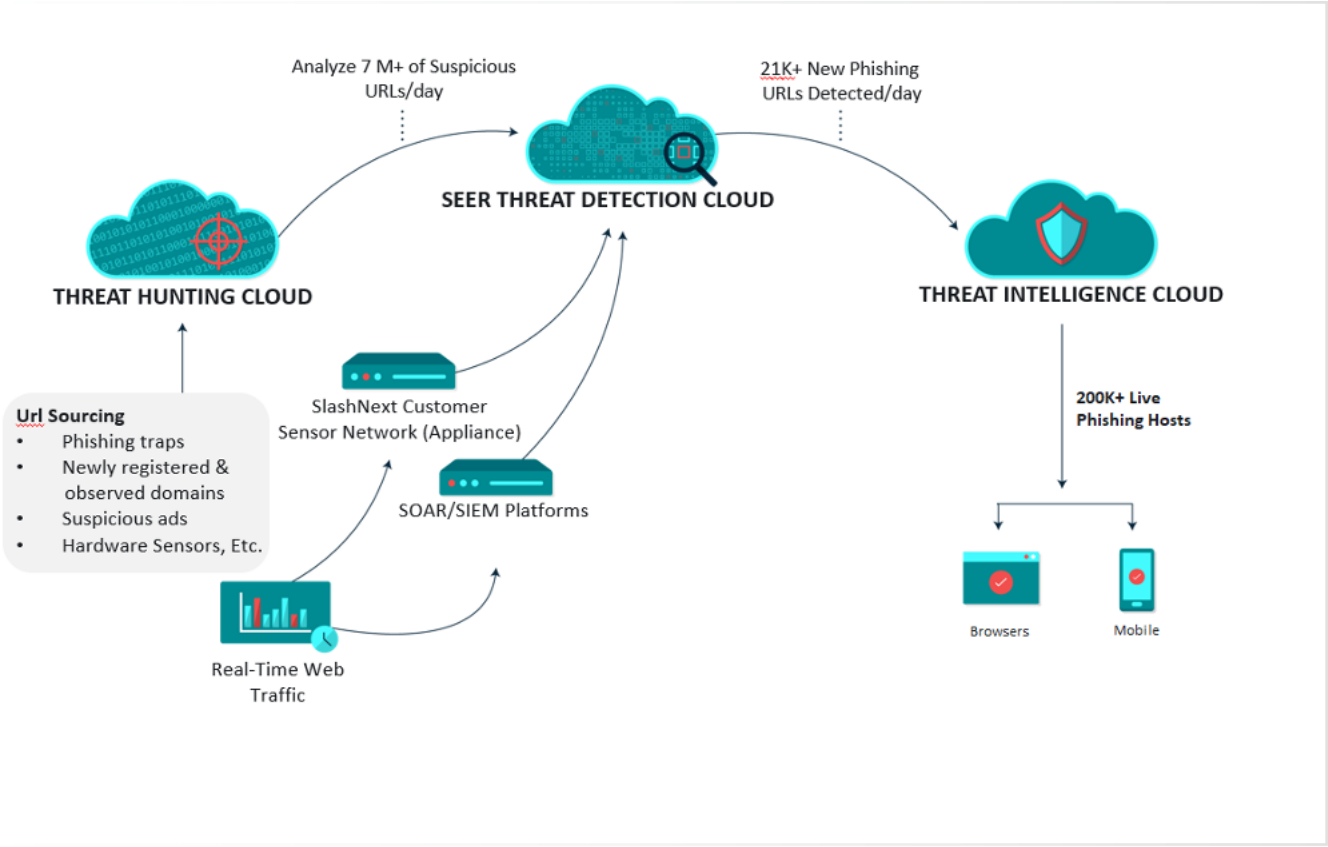
Easy Deployment and Management: Easily deployed and managed with leading UEM and Single Sign-On (SSO) solutions or SlashNext's Endpoint Management System for complete, real-time visibility to phishing attacks across the user base.

**2.0 AI PHISHING DEFENSE**: World's Largest Phishing Intelligence Network

Bad actors have become sophisticated, employees can't spot the fakes, and traditional defenses that rely on domain reputation and blacklists are not enough. It's not surprising that Verizon's 2020 Data Breach Incident Report found that over 90% of breaches involve phishing. A new next-generation 2.0 AI phishing defense approach is required.

To successfully predict and protect users from phishing attacks, you must start with visibility. SlashNext global intelligence network provides insight into over 1 billion internet transactions and 7 million URLs inspections daily, using virtual browsers and AI. The source of intelligence includes:

- **Spam Email and SMS Traps** - Extensive honeypot network collecting suspicious emails and text
- **Suspicious Ad Networks** - Click redirect chain collecting suspicious ads
- **Hardware sensors** - Suspicious web links extracted from live web traffic
- **Domains and certification logs** - Newly registered domains and https certificates feeds are analyzed
- **Passive DNS** – Newly registered and observed domains are extracted from crawl throughs of suspicious IPs

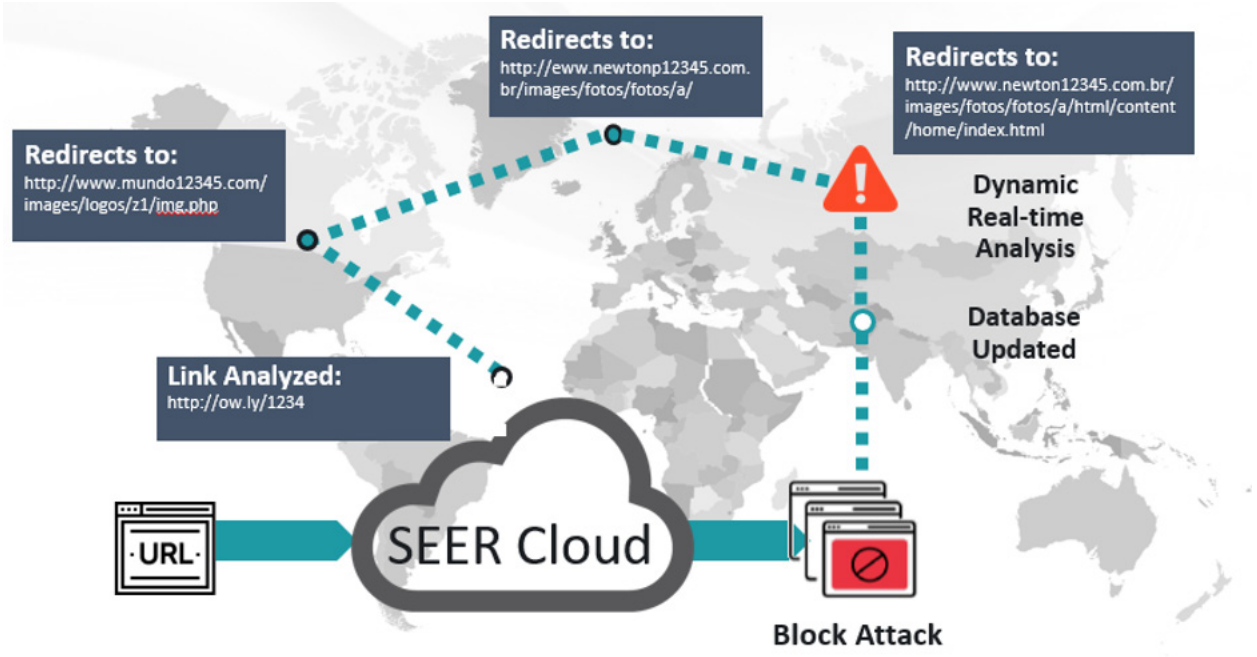


## OVERCOMING INSPECTION BLOCKING

Many sophisticated attack pages apply defensive and offensive techniques to block inspection by security vendors. These techniques include:

- **CAPTCHA** – SlashNext "injects" itself behind the CAPTCHA to access of the attack page
- **Access Control by IP** – SlashNext uses dynamic residential IP addresses, to mimic end-user browsing profile when the webpage is unreachable by using co-location IPs
- **URL Redirection** – SlashNext follows all URL redirections to analyze the destination webpage
- **Using Shared Infrastructure** – SlashNext applies a zero-trust-approach and applies the same scanning technologies to all webpages
-

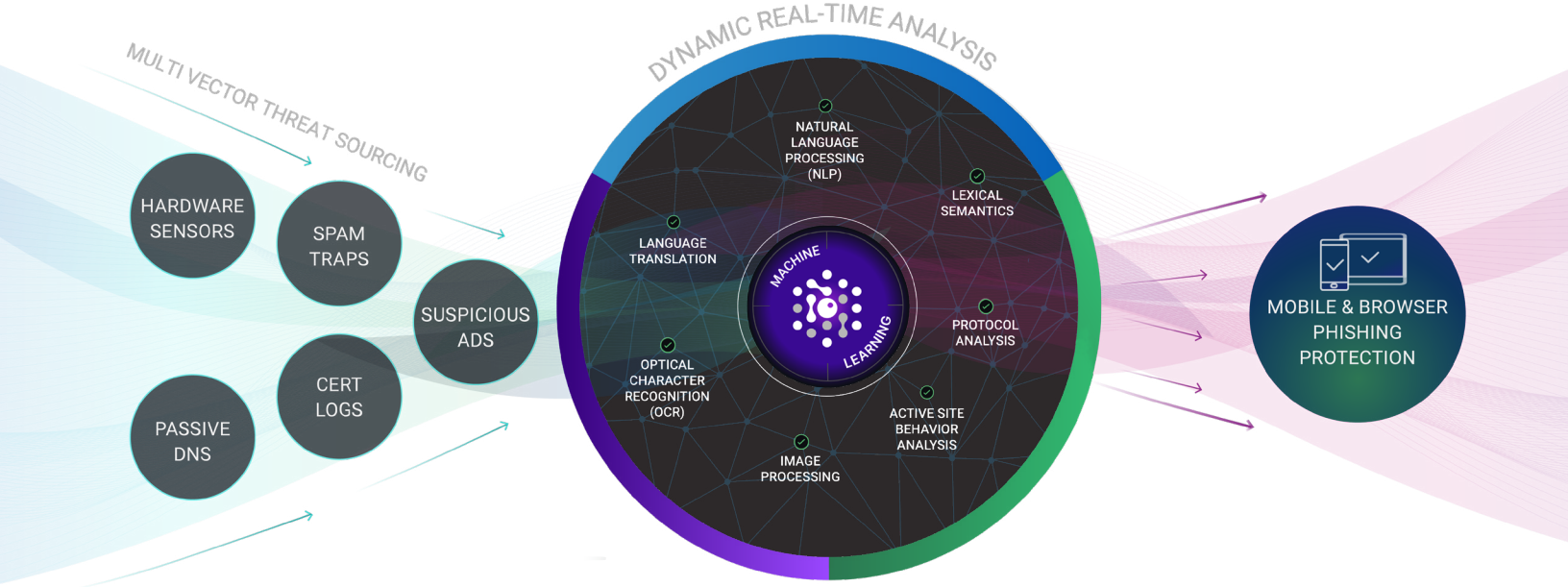
### SLASHNEXT FOLLOWS URL REDIRECTIONS



## VIRTUAL BROWSER AND PROGRESSIVE MACHINE LEARNING

Most of the industry is using domain and URL reputation techniques to identify phishing webpages. That approach is often not accurate or fast enough to detect new and fast-moving phishing attacks. SlashNext's patented Session Emulation and Environment Reconnaissance™ (SEER) detection technology are purpose-built for phishing detection and it centers on the behavioral analysis of the content. A URL is loaded into a virtual browser session and fully rendered, enabling our technology to see the webpage as it is intended by the target user. SEER then analyzes the webpage content using computer vision, natural language processing, and other machine learning classifiers to see exactly how it looks and understand the context of the page. SEER has viewed billions of websites that have been written historically for phishing or for benign purposes. And just like a security education company that trains employees, our machine learning classifiers are trained to recognize a phishing site.

Progressive learning, a new form of machine learning invented by SlashNext, uses Artificial Intelligence (AI) techniques to emulate human cognitive reasoning and allow the system to learn and respond accurately without the need for human intervention. Classifiers are initially trained and tested using a training dataset, but as the classifier starts to lose its accuracy in production, instead of a human stepping in to retrain the classifier, an AI layer accomplishes that task. Or said another way, the AI layer allows the progressive learning machine to use dynamic features. This patented innovation allows the system to learn from its environment at runtime and become incrementally more accurate in its future detections without any human interaction. The core inspiration for progressive learning came from malware researchers. Using progressive learning we replicate the analytical reasoning process that a malware researcher goes through when manually analyzing a potential threat. Human researchers combine intuition, cognitive thinking, natural language analysis, and various other discovery methods to understand new, unknown threats. At SlashNext we have succeeded in automating the thought process and techniques of some of the world's best cyber researchers and codified this knowledge into a cloud-based progressive learning AI.





6701 Koll Center Parkway, Suite 250 Pleasanton, CA 94566 | slashnext.com | info@slashnext.com | 800.930.6843