DATA SHEET

SLASHNEXT

Real-Time Threat Observability

Identify Threats in Microsoft 365 Email and in Weblogs with Microsoft Sentinel

Overview

See where your current security defenses stand today, what threats are missed, and how you can improve your security readiness by plugging into SlashNext HumanAI™, a combination of computer vision, natural language processing, and behavioral contextualization that detects malicious URLs, BEC, malware and exploits in real-time. By detecting threats in real time with 99.9% accuracy, we help organizations detect and prevent threats before they become a breach.

SlashNext offers Real-Time Threat Observability Assessments designed to identify threats evading your current defenses. SlashNext offers two Observability Assessments for comprehensive insights into how threats are reaching your employees and how employees might be interacting with these threats.

1. Real-time Observability Assessment for M365 Email
2. Real-time Observability Assessment of URLs for Microsoft Sentinel

These assessments are designed to provide real-value, with detailed insights into companies' risk exposure for email and web usage.

Real-time Threat Observability for M365 Email

Microsoft 365 Email with Defender for Office is not designed to detect or prevent advanced attacks found in natural-language BEC, links and/or attachments.

- Set-up is easy. Install in five minutes with one-click integration and will not require valuable security team time
- Implement the read-only solution with no impact to your existing email infrastructure or mail flow
- Will not take any action on the emails it finds to be malicious, but will alert you of the findings through a management console
- At the end of the Observability period receive a risk report with summarizes the of the findings and arisk score

Real-time Threat Observability for URLs with Microsoft

Firewalls, network proxies and AV solutions are not designed to detect or prevent advanced attacks found in spear phishing, smishing or other advanced link attacks.

- Stream web logs from network proxies directly into Microsoft Sentinel which integrates with SlashNext Web Log Assessment
- Identifies threats that your users are actively interacting and engaging with which may lead to Credential Harvesting, Ransomware and other malicious

RISK REPORT RESULTS

Receive insights into email and web threats evading current security defenses.

NUMBER OF EMAILS THREATS

Number and percentage of threats found

TYPES OF EMAILS THREAT

BEC, Credential Harvesting, Ransomware, Fraud, ATO

SUCCESSFUL THREATS ATTACKS

Identify the number of advanced attacks that users engaged with in your environment including spear phishing, smishing or other advanced attacks.

TYPES OF USERS EXPOSED

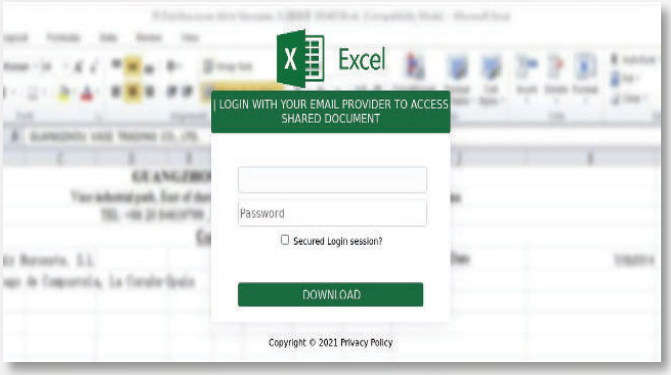
Number of users exposed, including high-risk users

THREAT SCORE

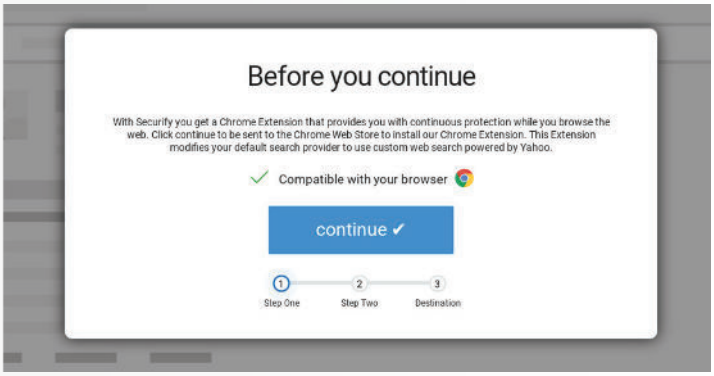
Understand the risk to your organization as compared to the industry

It Only Takes One

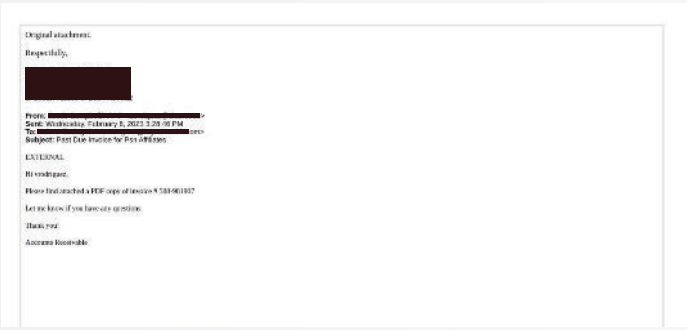
Credential Stealing Phishing



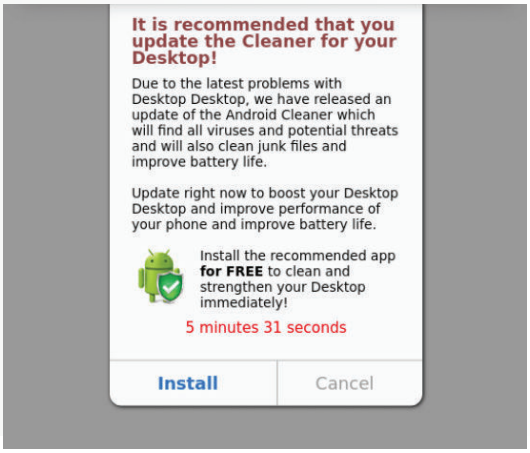
Malware and Exploits



Business Email Compromise



Scams



82% of successful breaches start with a human compromise threat, includes ransomware, malware, data exfiltration and financial fraud. SlashNext protects the modern workforce from malicious messages across all digital channels. SlashNext's patented HumanAI™, a combination of computer vision, natural language processing, and behavioral contextualization, detects threats in real time with 99.9% accuracy. SlashNext Complete™ integrated cloud messaging security platform stops zero-hour threats in email, mobile, and web messaging apps across M365, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Teams, and other messaging apps to detect and prevent threats before they become a breach.

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