CASE STUDY

SLASHNEXT

Large Toy Company Closes Multi-Channel Security Gaps

The Company

Large toy company closes security gaps in business and personal messaging channels outside of email. Adopts SlashNext integrated mobile security app and browser extension to stop zero-hour malicious phishing links, Smishing, business text compromise, exec impersonation and ransomware/malware file attacks.

Business Challenge

Despite use of a SEG, supplemental email security, Microsoft E5 (including defender for email and defender for endpoints, firewalls, proxies and next gen endpoint security, malicious threats were still getting through business and personal messaging channels commonly used by their users.

Current Challenges: Legacy Detection Missing Threats

The current security defenses were failing to address the shift to remote work on any device which left gaps in protection for people using the same devices for personal and professional use. Signature-based detection struggled to stop zero-hour threats - spear-phishing, Smishing, business text compromise (BTC), exec impersonation, HTML attachments, legitimate service compromise, rogue browser extensions. Bank fraud scams and other threats.

Solution: SlashNext Multi-Channel Mobile and Browser Protection

- Detects and stops broadest surface area of zero-hour user compromise threats across business/personal messaging channels
- Patented 2-phase cloud and on device AI detection of zero-hour threats
- Live, reinforced user awareness training of threats
- Great user on device (no proxy) use experience and guaranteed privacy of BYOD environments
- Fast mass-scale deployment using popular MDM/EUM tools and simple, zero-touch SaaS management

"SlashNext is the best layer of defense against malicious threats in personal and business messaging apps."

Global CISO

The Challenge

- Current security defenses were failing to address the shift to remote work on any device
- Signature-based detection struggled to stop zero-hour threats
- Despite use of a SEG, Microsoft E5 , malicious threats were still getting through business and personal messaging channels

The Solution

- SlashNext Multi-channel Mobile and Browser Protection

The Results

- Zero-hour Cloud and On-Device Protection
- Broadest Multi-channel Attack Surface Coverage
- 99.9% AI Detection, 1 in 1M FP Rate, 48 Hour Advantage

The Results

If the user encounters a phishing threat, there is a safe preview of malicious sites and helpful education about the threat type. Users now have an Improved experience without any reduction in productivity.

"SlashNext is the best layer of defense against malicious threats in personal and business messaging apps."

With a 99.07% detection rate and broad coverage, there has been a significant reduction in phishing incidents. The security administrators can easily deploy in minutes, manage groups, policies, users, and licenses. Advanced reporting and analytics features include filters to view data by threats, endpoints, and users for a full view across the enterprise.

About SlashNext

SlashNext protects the modern workforce from malicious messages across all digital channels. SlashNext Complete™ integrated cloud messaging security platform utilizes patented AI SEER™ technology with 99.9% accuracy to detect threats in real-time to prevent users from phishing, smishing, social engineering, ransomware, and malicious file downloads. Take advantage of SlashNext's Integrated Cloud Messaging Security for email, browser, mobile, and brand to protect your organization from data theft and financial fraud breaches today.

For more information, visit www.SlashNext.com

6701 Koll Center Parkway, Suite 250, Pleasanton CA 94566 | slashnext.com | info@slashnext.com | 800.930.8643
REV 092622