SLASHNEXT SECURITY

CAL POLY

AI-Powered Email Monitoring Enables SOC Students To Improve Campus Security

Our advanced AI technology protects against zero-hour spear phishing, BEC, smishing, and other socially engineered attacks in email, SMS, Slack, Teams, and other messaging apps.

Cal Poly State University Embraces Gen AI for Cloud Email+ Security

Educational institutions, particularly university campuses, are a favorite target for cybercriminals because of the large distracted populations, multiple vendor relationships and research facilities make them vulnerable to threats like BEC, QR phishing, and other advanced threats.

Cal Poly's SOC was drowning in these types of threats. Seventy-five percent of the student SOC team's time was spent on abuse inbox analysis. The remaining time was spent on addressing SIEM alerts and other tasks.

After deploying SlashNext Cloud Email Security they saw an 80% reduction in the malicious emails being reported to the security team in the first 24 hours. SlashNext monitors 6,500 faculty and staff inboxes, and in the first week analyzed over a million emails, detected 434 zero-hour link attacks, and 271 BEC emails targeting the highest levels of campus leadership. The reduction of abuse email management, allows Cal Poly to assigns projects to students, including:

Security KPI Tracking Using Splunk: Tracking response of SOC analysts to measure response and resolution time.

Ingest CIS Threat Intelligence into Splunk: Enhances security posture with proactive alerts around identified threats.

Management of Palo Alto IP/Domain Block Lists: Simplifies and automates adding IPs or domains to firewall's block list.

HIBP Automation: Monitors for addresses in data breaches and automates notification to impacted users reducing process time from 15 minutes to one minute.

AWS Security Alerts: Identify high-risk AWS activity, providing invaluable visibility of campus-wide AWS activity and potential incidents.

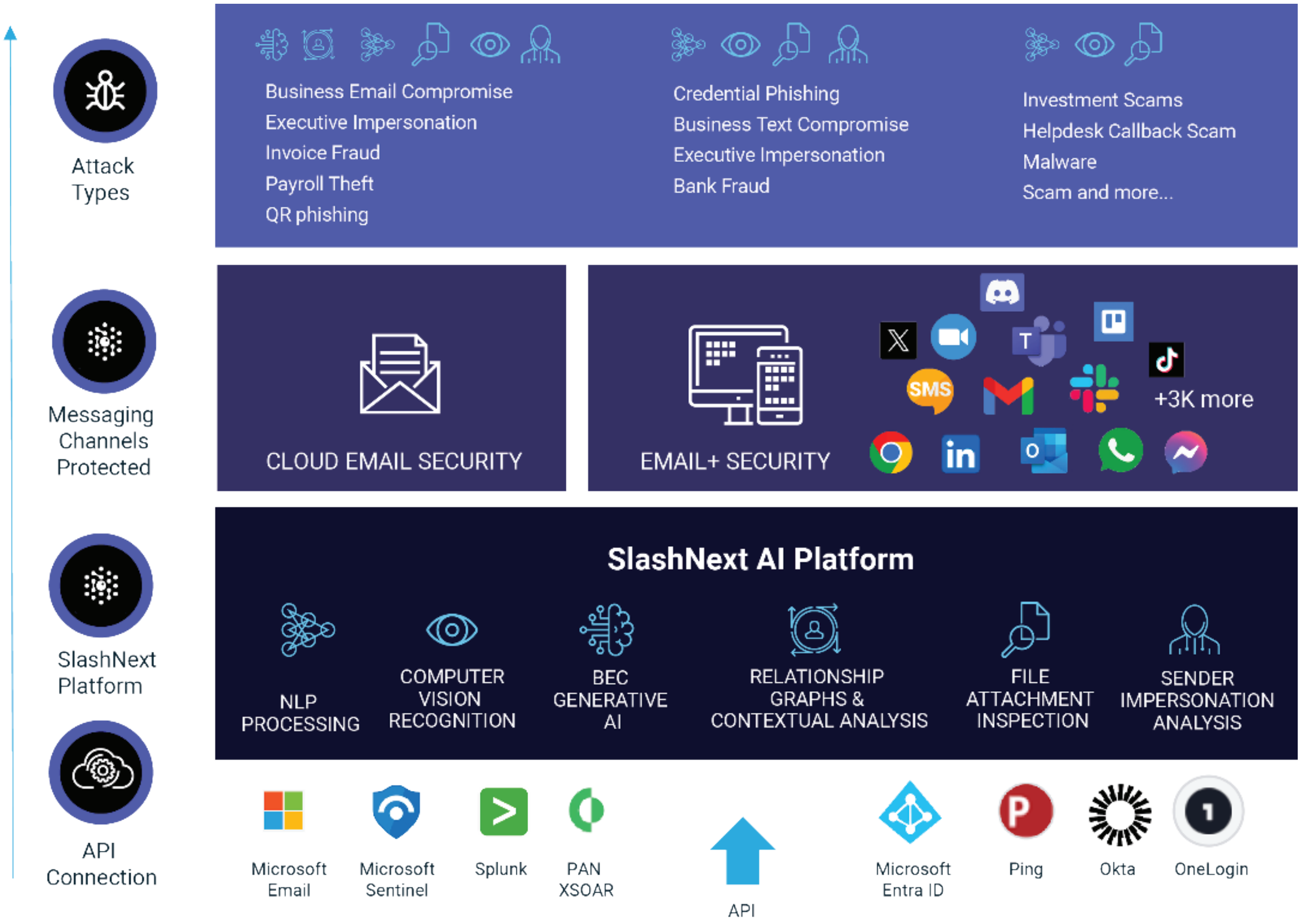
Next Gen AI Cloud Email+ Security

Email is still the primary tool for communication, and it's a rich target for cybercriminals seeking to exploit user vulnerabilities. Generative AI has exacerbated this issue, enabling attackers to launch BEC and advanced phishing attacks like executive impersonation, invoice fraud, and QR phishing with unprecedented scale and ease. In addition, attackers are expanding to adjacent communication channels such as SMS, Teams, and Slack.

SlashNext's advanced AI platform is purpose built to anticipate and stop the vast numbers of sophisticated threats. The service delivers industry leading 99.9% detection rate and 1 in 1 million false positive rate 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 wih a 48-hour detection advantage to stop zero-hour threats
- Increased SecOps and user productivity from using a solution with the highest detections and the lowest false positives rates
- 360° protection with threat protection across all messaging channels: in email, mobile and web

SlashNext's Gen AI-powered Cloud Email Security platform integrates natively with Microsoft using its Graph API. It is purpose built to predict and stop business email compromise and advanced phishing threats missed by Defender for Office 365.



The **SlashNext AI Security** platform includes:

- **Cloud Email Security:** Next Gen AI detects BEC and advanced phishing threats for inbound, outbound, and internal emails, with 48-hour 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.

Learn more at https://slashnext.com

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