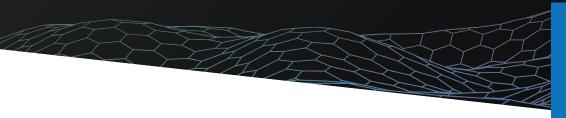
# SLASHNEXT

# **Cloud Email Security Risk Assessment**

Identify Threats in Microsoft 365 Email



In the face of increasing cyberattack frequency and financial repercussions, organizations require a seasoned cybersecurity partner that ensures cyber readiness and offers a complete defense in depth strategy.

SlashNext helps organization assess where your current security defenses stand today, what threats are missed, and how you can improve your security readiness by plugging into SlashNext Generative AI in observability mode.

Powerful layers of analysis using relationship graph, contextual analysis, NLP, computer vision and Generative AI to detect:

Advanced BEC detection including executive compromise, invoice/payment fraud and vendor email compromise

File Attachment Inspection to detect malicious file payloads

**Zero-hour link protection** with preemptive sourcing and real-time scans

SlashNext detects threats in real time with 99.9% accuracy and 1 in 1 million false positive rate. Our risk assessment is tailored to provide a deeper understanding of your risk exposure and insights into the discovery and containment of attack entering your organization.



## SET IN 15 MINUTES OR LESS

One-click integration. Requires no help from your team.



### ZERO RISK TO YOUR EMAIL INFRASTRUCTURE

Read-only solution. Will not take action on malicious findings , but provide alerts.



RECEIVE A CUSTOMIZED REPORT

Receive a risk report with summaries of the findings and a risk score.

#### Get a Customized Email Security Risk Assessment

The customized report provides a clear and insightful view of your organization's email security. Our goal is to offer data-driven insights to make informed decisions, fortify your cybersecurity measures, and ensure your organization's protection.

#### Actionable Insights on Attack Types, Payload, Intent and Techniques

Impersonated a	ttacks ref	er to att	acks in w	hich the
sending display	name is	manipul	ated to ap	pear a
one of your em	ployees.	This tab	le will be	blank i
impersonation	attacks	did no	t occur	in the
	1			

Impersonation Attacks



			. 17	personisted	Vens
800					
400 -	-	-	-		ł
200					I

The information in this chart hows the number of employee names used in impersonation attacks. This table will be blank if impersonation attacks did

Impersonated Users

not occur in the reporting period.

formation in ti	his table are the employed	es that are most free	quently impersonated.	
Signlay Name	Small	Orpartment	Titala	Threat Court
uiqi Chen	naiqi@company.com	Finance	Hanager Accounts	432
feliess Carrior	mellea@company.com	Finance	Assistant Manager Accounts	421
runklin Tovantz	franklingtcompany.com	Sales	Sales Manager	395
yan Roslansky	Iyan@company.com	Finance	Senior Manager Accounts	364
anial Shaparo	dariet@company.com	Sales	Sales Specialist	345
ışılar Barden	taylor@company.com	Sales.	Sales Engineering	338
ari Srinivasan	harigeompany.com	Finance	Chief Finance Officer	302
arries Party	James@company.com	Finance	Finance Manager	235
esiar Cruz	onarthcompany.com	Sales-	Sales Operations Manaper	185

#### **Comprehensive Summary of the Impact on Your Organization**



Eighty-two percent of successful breaches start with a human compromise threat, like business email compromise and credential theft, which leads to ransomware, malware, data exfiltration, and financial fraud. SlashNext stops BEC, text scams, credential theft, and other types of zero-hour phishing across email, mobile, and collaboration apps, including Microsoft 365, Teams, Slack, LinkedIn, and WhatsApp. SlashNext's Generative AI leverages a combination of relationship graph, contextual analysis, computer vision, natural language processing, and generative AI to detect threats in real-time with 99.9% accuracy.

#### Schedule a risk assessment at www.slashnext.com/risk-assessment/