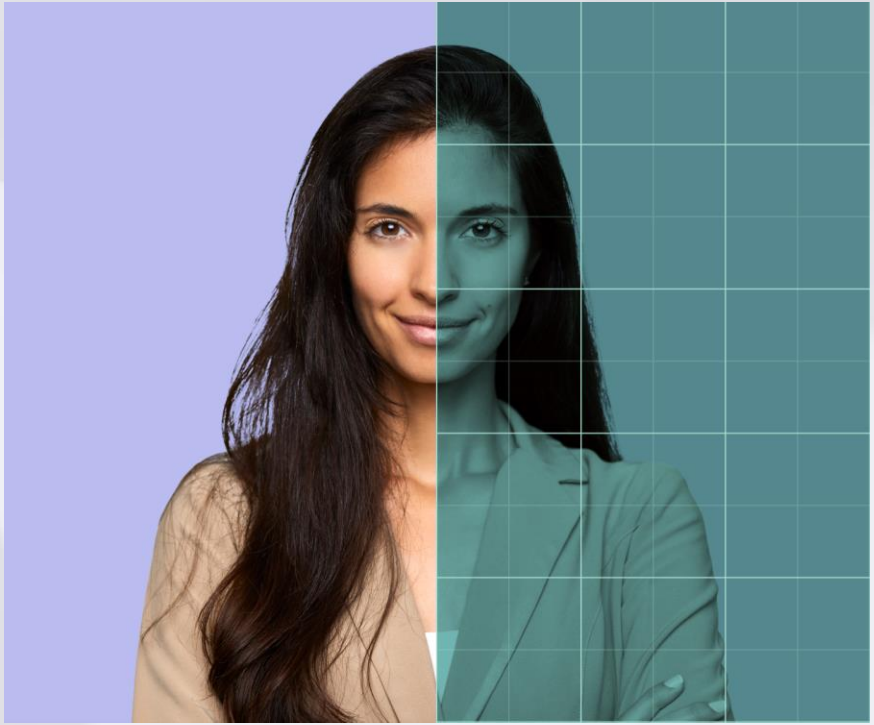
Abnormal

The Future of Email Security



Maiwand Youssofzay / Country Manager - ASEAN

Abnormal

Our Background

- Cloud email security platform that leverages behavioral data science to stop email attacks
- Purpose-built for large deployments
- Customer obsessed: As per Gartner Peer Insights, 100% of our customers are willing to recommend us and have given us a rating of 4.9 out of 5
- Microsoft Strategic Partnership

Our Team DNA

Top Security Companies:

proofpoint.

paloalto NETWORKS

Carbon Black.

+

Top AI/ML Companies:

Google

amazon

Johnson & Johnson

MetLife

GAP

FOX

MassMutual

MARRIOTT VACATIONS WORLDWIDE

AVERY DENNISON

PG&E

MOLSON COORS beverage company

xerox

ADT

stryker

WD Western Digital

MATTEL

Abnormal + Microsoft Partnership

"Abnormal Security augments native Microsoft security services to protect our customers from advanced socially-engineered attacks while also reducing security stack complexity and improving SOC efficiency"

Member of
Microsoft Intelligent Security Association
Microsoft

Members are top experts in the cybersecurity industry with a goal of improving customer security

https://www.microsoft.com/en-us/security/business/intelligent-security-association

✓

Microsoft Preferred Solution

Preferred solutions are selected by a team of Microsoft experts and are published by Microsoft partners with deep, proven expertise and capabilities to address specific

Microsoft AI INNER CIRCLE

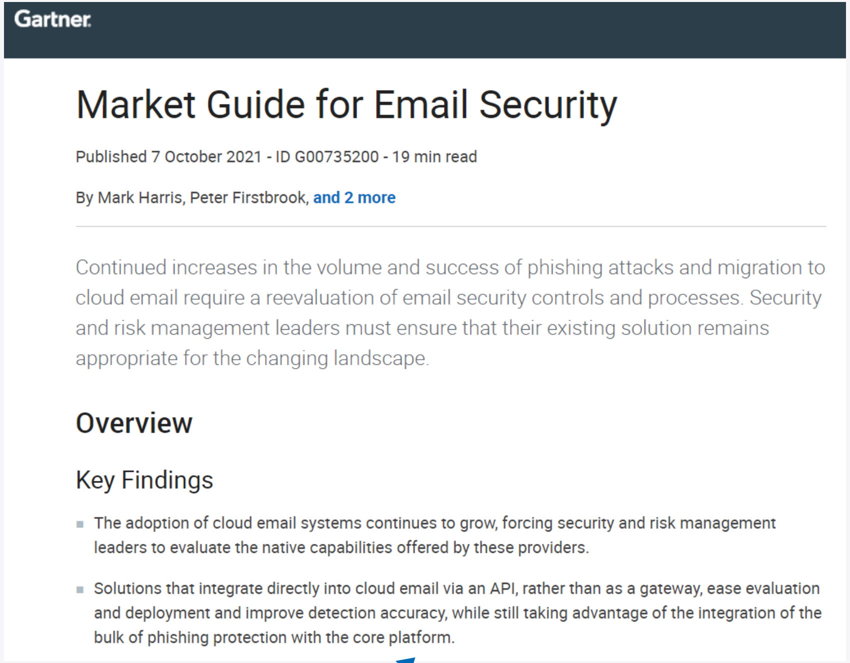
Members with unique expertise in the ability to drive business transformation using the power of AI and Data

2022 Partner of the Year Winner

2022 Microsoft Security Excellence Awards Finalist

Learn more at abnormalsecurity.com/microsoft-partnership

Gartner Market Review - Oct 2021



Gartner

Market Guide for Email Security

Published 7 October 2021 - ID G00735200 - 19 min read

By Mark Harris, Peter Firstbrook, and 2 more

Continued increases in the volume and success of phishing attacks and migration to cloud email require a reevaluation of email security controls and processes. Security and risk management leaders must ensure that their existing solution remains appropriate for the changing landscape.

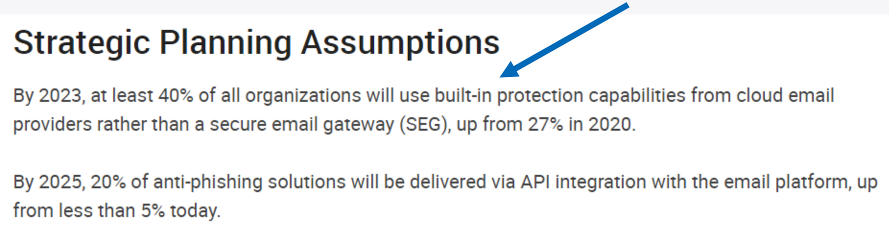
Overview

Key Findings

- The adoption of cloud email systems continues to grow, forcing security and risk management leaders to evaluate the native capabilities offered by these providers.
- Solutions that integrate directly into cloud email via an API, rather than as a gateway, ease evaluation and deployment and improve detection accuracy, while still taking advantage of the integration of the bulk of phishing protection with the core platform.

Improved detection accuracy

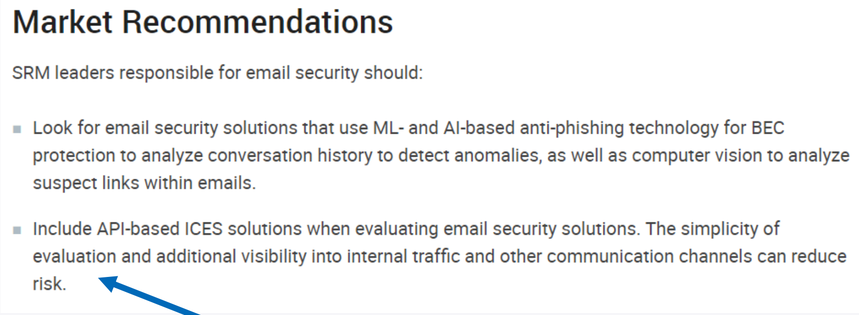
SEG use down
API use up



Strategic Planning Assumptions

By 2023, at least 40% of all organizations will use built-in protection capabilities from cloud email providers rather than a secure email gateway (SEG), up from 27% in 2020.

By 2025, 20% of anti-phishing solutions will be delivered via API integration with the email platform, up from less than 5% today.



Market Recommendations

SRM leaders responsible for email security should:

- Look for email security solutions that use ML- and AI-based anti-phishing technology for BEC protection to analyze conversation history to detect anomalies, as well as computer vision to analyze suspect links within emails.
- Include API-based ICES solutions when evaluating email security solutions. The simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk.

Simplicity of evaluation