The Core MSP Email Security Guide

What Is Email Security?

90% of data breaches in 2023 started with an email[1] and your clients could be next. Phishing is the top attack vector for cybercriminals, with users receiving a sophisticated phishing attempt once a week that their current security misses.[2]

Email security is crucial in future-proofing your clients' business. It scans and filters incoming emails to block spam, phishing and malware. Email security also safeguards outbound emails with encryption and data loss prevention, making it a critical piece to a well-rounded security stack.

Components of Email Security

- **Advanced Phishing Security:** Identifies and blocks sophisticated emails that trick users into revealing sensitive information.
- **Antivirus and Zero-Hour Threat Protection:** Eliminates malware from emails before they reach your inbox.
- **Data Loss Protection:** Prevents sharing critical information without proper permissions.
- **Compliant Email Retention and Archiving:** Provides secure email storage methods required to meet legal and industry compliance.
- **Policy-Enforced Encryption:** Screens and encrypts emails based on preset rules, such as the presence of specific keywords or recipients.
- **Spam and Content Filtering:** Analyzes text and email contents to filter out commercial messages or potential malicious activity.
- **URL Scanning:** Rewrites and scans URLs in emails before allowing users to access the linked websites.
- **Attachment Defense:** Analyzes email attachments in a secure sandbox environment to detect and block malicious activity before delivery.

The Core MSP Email Security Guide

Why Does It Matter to My Business?

Email is the #1 vulnerability for phishing, business email compromise (BEC) and malware. With rapid advancements in AI and its growing use in cyberattacks, standard email security solutions and secure email gateways (SEGs) lack sophisticated protections to combat today's threats.

Without a dedicated email security solution, it's only a matter of time before a breach happens. Email security is also a key component for CIS Controls and essential for businesses seeking cyber insurance.

- Credential **phishing is up 703%** since 2024.[2]
- It takes less than **60 seconds** for users to fall for phishing emails.[3]
- **55.8%** of ransomware attacks target small businesses.[4]
- **1 in 5** organizations typically opt to pay the ransom.[4]
- At least **24 million** emails were tied to BEC attacks in 2024.[5]
- **$50,000** was the average transaction amount for BEC schemes in 2023.[3]
- AI-generated phishing messages had a **54%** greater click-through rate than human-written phishing emails at **12%**.[6]
- Lost business costs and breach expenses totaled a **record-breaking $2.8 million** in 2024.[7]
- **61%** of cybersecurity leaders are concerned about the use of AI in phishing campaigns.[8]

Upscaling Protection with API-Based Email Security

Out with the old and in with the future. Traditional SEGs? They're yesterday's news. Modern cloud platforms deliver traffic insights, enhance network adaptability and fortify protections. Integrated Cloud Email Security (ICES) taps into an API to directly connect with platforms like Microsoft 365 or Google Workspace, granting comprehensive email data access and real-time monitoring with ultimate flexibility. This means premium protection like:

- **Real-Time Monitoring:** Uncover insights into email flow and user habits.
- **Threat-Hunting Solutions:** Utilize advanced analysis to gain insights into cyberthreat behaviors.
- **Breach Prevention:** Enable early detection to stop breaches in their tracks.
- **Timely Protection:** Eliminate malicious links instantly.

API-based ICES delivers the eagle-eye insights and lightning-fast control clients need against today's sophisticated phishing, ransomware and BEC attacks. For MSPs, offering ICES isn't just smart—it establishes you as the go-to expert in modern defense.

The Core MSP Email Security Guide

How Do I Sell Email Security?

Email security is no longer a luxury—it's a must-have to protect sensitive data and avoid devastating breaches. Connect with your clients on the importance of email security and the real-world risks of going without it. For example, ransomware and extortion attacks **cost businesses a median of $46,000,** with some SMBs facing losses **soaring past $1.1 million.**[3]

Costs that great could sink a business or take years to recover from. Spark the conversation by asking these crucial questions about their current defenses

- How would you continue operations if ransomware locks down your email?
- If your email servers went down for over a week, how would that affect communication between your employees and customers?
- What is your recovery strategy and the potential fallout if phishing leads to a data breach?
- Many cyber insurance providers require specific email security. Do you have any of the five security measures in place: email security, multi-factor authentication (MFA), segmented backups, security awareness training or endpoint detection and response (EDR)?

Leveling with your clients will uncover other gaps in their security, offering you the opportunity to package and sell email security as part of a larger, multi-layered security approach.

Optimize Email Security and Grow with Pax8

Take control of your client's email security today. Work with Pax8 to deliver advanced solutions that block threats, protect data and build trust. Reduce your client's risk with our industry-leading vendors like Avanan, IRONSCALES and Proofpoint. We empower you to drive stronger, personalized business growth

Explore Pax8 security resources

Schedule a call

Sources:

1. 2024 Cofense Annual State of Email Security Report
2. SlashNext 2024 Phishing Intelligence Report
3. Verizon 2024 Data Breach Investigation Report
4. Hornetsecurity Q3 2024 Ransomware Attacks Survey
5. VIPRE Q3 2024 Email Threat Trends Report
6. Abnormal 2023 The State of Email Security In an AI-Powered World
7. IBM Cost of a Data Breach Report 2024
8. Egress Email Security Risk Report 2024