4 Tenets to Address Advanced Email Security Threats

14 October 2024 - ID G00801182 - 18 min read

By: Satarupa Patnaik, Franz Hinner

Initiatives:Infrastructure Security

Email security remains critical due to evolving threats such as AI-generated phishing and credential theft. This research equips security and risk management leaders with essential strategies to build a robust email security strategy and effectively mitigate advanced attacks.

Overview

Key Findings

- Malicious actors leverage generative AI to create more convincing phishing emails and exploit new attack vectors like QR code phishing. These emails are difficult to detect as they evade traditional spam filters and trick users into unknowingly visiting phishing websites that lead to data breaches and fraud.
- Credential theft is now a common attack technique. For example, malicious actors redirect email recipients to fraudulent cloud-based software (SaaS) platforms like Microsoft 365, which impersonate legitimate SaaS services to steal login credentials.
- Many email security solution providers and clients primarily focus on inbound email security. However, significant threats such as sensitive data breaches due to misdirected emails, domain abuse and outbound phishing emails from compromised email accounts go unnoticed, causing compliance/legal issues and reputation damage to impacted organizations.
- Human errors account for 68% of all security breaches. Users often fall victim to phishing attacks, click malicious links and reuse weak passwords, unknowingly granting attackers access to sensitive information or to the organization.

Recommendations

- Invest in email security solutions that incorporate multiple AI/machine learning (ML) capabilities to identify AI-generated phishing and quishing attempts.
- Enforce multifactor authentication (MFA) and assess if your existing vendor has identity threat detection and response (ITDR) and the capabilities to identify impossible travel, credential theft attempts and identity-based attacks such as email account takeover.
- Invest in add-on solutions to enhance outbound email security and prevent accidental sharing of sensitive content in outbound emails, detect domain abuse and secure email content.
- Update security awareness training regularly to include information on the current threat landscape, the latest attack techniques and current anti-phishing preventative measures to ensure that all end users know their responsibility to keep the organization safe.

Introduction

Social engineering incidents, a common tactic in business email compromise (BEC) scams, had nearly doubled from 2022 to 2023 and still continue to be a common infection vector. [1] Phishing remains as one of the top causes of malware incidents, accounting for 31% of social engineering incidents. [2]

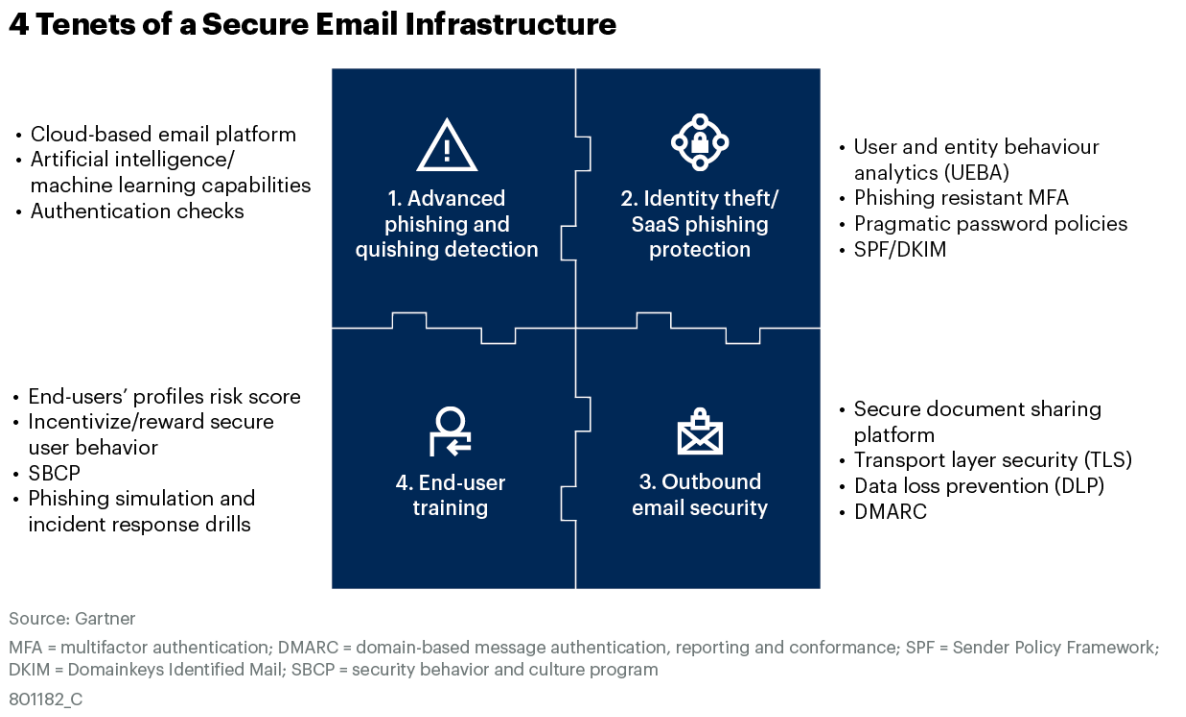
Despite significant investments in email security solutions, email remains a critical attack vector for malicious actors. As the threat landscape evolves, attackers constantly adapt their tactics, making it challenging for traditional email security controls to keep up. Native email security controls offered by significant providers often fail to stop these advanced threats. Attackers leverage social engineering techniques, spear-phishing emails targeting specific individuals and zero-day exploits (previously unknown vulnerabilities) to evade traditional filters.

Sophisticated attacks can leave organizations vulnerable targets for future attacks such as identity thefts and lead to data breaches, financial losses and reputational harm.

While AI and behavioral analytics advancements are promising, a comprehensive approach is necessary to address technical vulnerabilities and human factors. This research explores the advanced threats in email security and offers actionable recommendations for organizations to build a robust email security infrastructure. This strategy goes beyond traditional perimeter defenses and incorporates four tenets for advanced threat protection: phishing and QR phishing (aka quishing) detection, identity theft protection, outbound email security, and user education (see Figure 1).

By understanding the limitations of current email security solutions and the latest threats, security and risk management (SRM) leaders can implement effective strategies to mitigate these risks and protect their organizations from email-borne attacks.

Figure 1: 4 Tenets of a Secure Email Infrastructure



Source: Gartner

MFA = multifactor authentication; DMARC = domain-based message authentication, reporting and conformance; SPF = Sender Policy Framework; DKIM = Domainkeys Identified Mail; SBCP = security behavior and culture program

801182_C

Gartner

Analysis

Invest in Email Security Solutions With Multiple AI/ML Capabilities

SRM leaders must evaluate their existing email security solutions and select/deploy solutions that incorporate AI/ML-based capabilities, such as:

- Natural language processing (NLP)

- Image processing
- Computer vision
- QR-code scanning
- Large language models (LLMs)
- Social graph (SG) analysis and
- Sender reputation/verification.

These capabilities help identify the subtle language cues and stylistic inconsistencies indicative of AI-generated phishing attempts and malicious URLs or fraudulent web login pages embedded in QR codes for quishing. Image processing also helps to identify fake company or brand logos used in email signatures. These solutions proactively block sophisticated phishing attempts that bypass traditional filters and reduce the risk of human error by automating the detection of AI-generated phishing and quishing emails. They also minimize business disruption and financial losses associated with these attacks.

Almost 70% of organizations today use cloud email solutions.[3]

Cloud-based solutions offer high scalability and better uptime due to defined service-level agreements from SaaS vendors. Furthermore, the scope of communication has expanded beyond email to other collaboration platforms, such as Microsoft's Teams, SharePoint and OneDrive, and Saleforce's Slack. Some email security tools may not protect these platforms. Hence, SRM leaders should supplement the native capabilities of their existing cloud email solutions with third-party security solutions to extend protection to all collaboration platforms. Organizations that continue to use on-premises email platforms should plan their transition to cloud-based email platforms, if possible, with built-in security features.

Authentication checks are a crucial part of advanced phishing detection. Utilizing domain-based message authentication, reporting and conformance (DMARC) as a first measure supporting AI/ML capabilities is an essential element of secure email infrastructure.

The selected email security solution should also have advanced integration capabilities such as bidirectional log ingestion with ITDR and endpoint security solutions, integration with third-party ticketing solutions and threat intelligence platforms to prepare for extended detection and response (XDR), security information and event management (SIEM) and security orchestration, automation and response (SOAR) migration.

For more details, refer to Tool: Vendor Identification for Email Security and Market Guide for Email Security.

Detecting and Protecting Against AI-Generated Phishing/Spear-Phishing Emails

Malicious actors leverage generative AI to create highly personalized and convincing phishing emails that mimic writing styles and even the voices of familiar senders. These emails evade traditional spam filters and trick users into revealing sensitive information or clicking malicious links.

According to the Verizon 2024 Data Breach Investigations Report, phishing and pretexting were the most common cause of data breaches, accounting for 73% of breaches. [2] IBM estimates the average cost of a business data breach to be $4.24 million in 2023. [4]

Phishing attacks that compromise credentials and steal data can cause companies to incur significant financial losses, damage an organization's reputation, erode customer trust and disrupt business operations.

Traditional spam filters with reputation- and signature-based detection and anti-malware solutions cannot accurately identify these attacks. AI capabilities such as NLP, LLM, SG analysis and sender reputation/verification help detect these advanced phishing attacks. These capabilities examine details such as the receiver's communication history to understand if the recipient has ever interacted with the sender in the past. They also compare the sender's writing style, patterns and keywords with the language models in their databases to assess the associated risk and provide risk/threat scores before declaring the emails malicious, potentially malicious or suspicious. Some email security solutions also add a context-aware banner to all emails from outside the organization to alert users in real time to be cautious when dealing with emails.

SG analysis also examines the entire communications network and rank-scoring of different nodes to evaluate the likelihood of two communicants crossing paths. In some cases, it can be context-aware of roles within those networks.

Detecting and Protecting Against Quishing Attacks

The rising popularity of QR codes has created a new attack vector for phishing scams. Attackers embed malicious URLs within QR codes placed in emails. When users scan the code with their smartphones, they are unknowingly directed to phishing websites designed to steal login credentials or distribute malware.

A report by Barracuda highlights that around one in 20 mailboxes were targeted with malicious QR codes in the last quarter of 2023. [5] Since many users access work email on their phones, successful QR code phishing attacks can compromise corporate credentials and grant attackers access to sensitive company data.

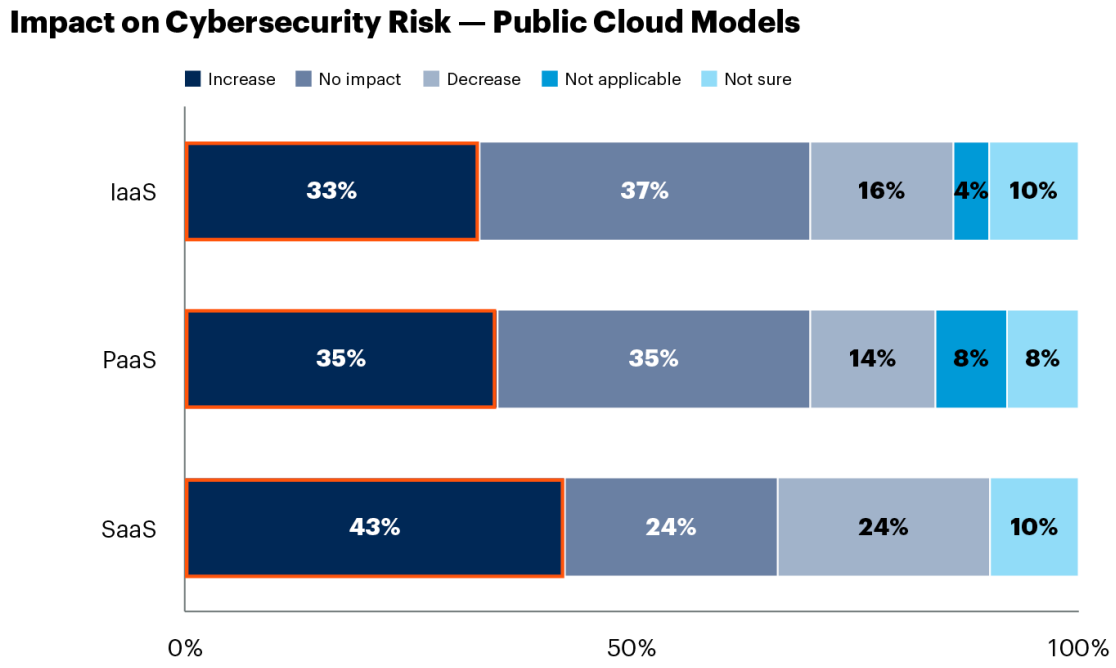
QR codes are often contained in the body of the email and are not attached as URLs or documents. Hence, file-based scanning and anti-phishing solutions often fail to decode or identify URLs embedded in QR codes effectively. However, AI capabilities such as image processing and computer vision can address this gap. By analyzing elements like the URL and other subtle hints, such as webpage and dialogue box dimensions, texts used, login prompts and background images, these technologies can detect fraudulent login pages. Also, URL scanning and rewriting help identify the subtle cues that can indicate machine-generated text and fraudulent webpages in the emails and prevent attacks.

Sometimes the URLs embedded in the QR codes are initially nonmalicious so they can pass the email security solutions and be delivered to the end user's mailbox. Then, the links are redirected to malicious websites after the email is delivered to the end user. In such cases, click-time protection, URL rewriting/blocking and clawback capability help to remove the email from all mailboxes and keep end users safe.

Protect Against Identity Theft and SaaS Phishing

In the 2023 Gartner Cloud Security Governance Survey, 33% of participants stated that infrastructure as a service (IaaS) increased cybersecurity risk. Thirty-five percent of participants stated that platform as a service (PaaS) increased cybersecurity risk, while 43% stated the same for SaaS (see Figure 2). The survey also found that organizations are most concerned about cybersecurity incidents related to unauthorized external access and data theft due to public cloud usage. [6]

Figure 2: Impact on Cybersecurity Risk — Public Cloud Models



n = 51, IT and business leaders who have visibility into cloud security governance

Q: How have each of these public cloud models impacted your cybersecurity risk over the past 12 months?
Source: 2023 Gartner Cloud Security Governance Survey
IaaS: infrastructure as a service; PaaS: platform as a service; SaaS: software as a service
Note: The total may not sum to 100% due to rounding,
807512_C

Gartner

SRM leaders should adopt a layered security approach by utilizing phishing-resistant MFA and assess if their email security solution has identity protection and response capabilities for preventing and detecting sophisticated threats such as credential phishing emails.

To quickly identify spoofing and identity theft/impersonation, domain alignment using Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) is used to authenticate the sender's identity. SPF and DKIM allow domain owners to enforce policies on handling emails that fail authentication checks, thereby enhancing sender reputation and improving the deliverability of legitimate emails.

Enforce MFA for all SaaS applications to add an extra layer of security beyond login credentials. MFA helps strengthen the security posture of your organization and optimize user experience. While any MFA type (such as app-based authentication, SMS or voice) is always better than no MFA, they are still vulnerable to certain threats such as phishing attacks. The Cybersecurity & Infrastructure Security Agency (CISA) strongly urges all organizations to implement phishing-resistant MFA (which is the most secure form of MFA) as part of applying zero-trust principles. [7] Phishing-resistant MFA is considered to be a potentially better standard for MFA and is also resistant to push bombing, Signaling System 7 (SS7), and SIM swap attacks. For more details on the types of MFA, see Market Guide for User Authentication.

SRM leaders should set password policies that prevent users from reusing old passwords, common/repeated words, simple phrases such as qwerty and abcd, the user's birth date and name, and the organization's name. Ensure that your password policy is set to accept only complex phrases in upper- and lowercase combined with numbers and special characters.

Some email security vendors also provide native ITDR capabilities or integrate them with third-party solutions. These capabilities include identity log ingestion, internal account protection and geolocation tagging capabilities to identify impossible travel- and identity-based attacks such as account takeover (ATO) emails. They also help detect log-on requests and correlate with URL reputation to identify fraudulent login pages. These capabilities are commonly called user and entity behavior analytics (UEBA).

For more advanced threats such as EvilProxy attacks, where attackers can steal session cookies to bypass MFA protections, SRM leaders must prepare for incident remediation and fortify security by implementing a multilayered approach. EvilProxy is also used for identity phishing to get initial access and bypass MFA for ATO attacks on platforms such as Microsoft 365, Google and GitHub, which can potentially lead to future supply chain attacks.

SRM leaders must implement the following measures as a part of a multilayered approach to detect and prevent EvilProxy attacks:

- Detect EvilProxy by URL analysis to prevent phishing-as-a-service (PhaaS) attacks on email and cloud accounts.
- Use hardware security keys for MFA when possible, as they are more resistant to interception.

- Enable conditional access policies and impossible travel restrictions for cloud accounts to detect suspicious login attempts.
- Implement robust logging and monitoring systems to quickly detect and investigate suspicious account activities.
- Adopt a zero-trust security model, requiring continuous authentication and authorization for all users and devices. For more details, see How to Build a Zero Trust Architecture.
- Invest in specific solutions to detect insider threats and perform hygiene checks on all user accounts, such as UEBA solutions for ATO, to reduce dwell time and speed up incident response. Most email security vendors also offer these as add-on solutions.
- Implement strong network segmentation to limit lateral movement in case of a breach.
- Implement robust web application firewalls (WAFs) and API security measures to protect against reverse proxy attacks.
- Implement sandboxing technologies to inspect messages in-depth and identify malicious URL redirect patterns and EvilProxy frameworks.

Invest in Add-On Solutions to Enhance Outbound Email Security

Some modern email security solutions have AI-based email screening capabilities to identify sensitive content and misspelled recipient names and generate context-aware banners to alert users and reduce human error. These warning banners also help to educate end users in real time and improve user awareness. However, more is needed to substantially reduce the human risk factor associated with outbound emails especially when sent from compromised email accounts. Hence, SRM leaders must invest in add-on solutions to improve outbound email security.

Invest in DLP Solution

To further reduce the risk of human errors, SRM leaders should invest in DLP solutions to alert users and prohibit them from attaching or texting confidential information over email. They should ensure that the DLP policies extend to other collaboration platforms such as Teams, Slack and SharePoint to prevent data leakage and breaches. Implement DLP solutions within the cloud email environment to prevent sensitive data from being accidentally or maliciously sent externally.

SRM leaders must also define a DLP strategy that aligns with the organization's established data security governance program. See the Market Guide for Data Loss Prevention to understand and adopt risk-based adaptive data protection techniques to strengthen the organization's data security.

Use Document Sharing Platforms

While email remains a standard communication tool, attaching large files can be risky from a security and data protection standpoint. Avoid sending sensitive information via email whenever possible and leverage secure document-sharing platforms for confidential files as a more secure alternative for collaboration and data transfer.

SRM leaders should choose solutions that offer granular levels of access control and complete encryption to protect data during transit and at rest. These platforms can be cloud-first such as Google Workspace and OneDrive or locally synchronized such as Box and Dropbox.

Invest in DMARC Services

SRM leaders should further invest in DMARC solutions for strong governance and authentication for their email domains to improve email security posture.

DMARC is the combination of SPF and DKIM protocols. It guards the organization against domain impersonation attacks and exact domain name spoofing. DMARC comes with its own challenges to deploy, configure and continuously monitor the solution depending on the size of the organization and the number of domains. For more information, see Implement DMARC to Prevent Business Email Compromise.

SPF records can be difficult to maintain and break if messages are forwarded. Certificate management and key rotation are issues for DKIM and Brand Indicators for Message Identification (BIMI). An email that fails DKIM due to rotated/reused or expired key or software issues will also fail the authentication required for BIMI, and the BIMI logo will not be displayed. Similarly, forwarded emails with modified contents also fail DKIM and SPF checks, leading to BIMI failures. DMARC reporting and monitoring services help resolve many of these issues and save project managers time.

Implement End-to-End Encryption by Using TLS to Secure Sensitive Communications

When email was designed in the 1970s, it lacked end-to-end encryption, and messages were exposed throughout their journey until email providers adopted Transport Layer Security (TLS). TLS protects the data during transit by securing the communication channels between email clients and email servers. However, older systems and devices might not support the latest versions of TLS, making them vulnerable.

Email encryption solutions have been available for a long time, but have only been adopted by about 40% of organizations due to usability issues.[3]

Secure email gateways (SEGs) commonly include encryption, but the usability differs greatly. SRM leaders must ensure that all emails are encrypted using TLS 1.2+. If necessary, additional levels of encryption (that is, content encryption in the user's inbox) should be the incumbent SEG filter or Microsoft Exchange/Google Workspace capability.

Many email data protection (EDP) vendors support Pretty Good Privacy (PGP) and/or Secure Multipurpose Internet Mail Exchange (S/MIME) encryption in their native configurations or as plug-ins. However, it is not advised to utilize these solutions unless there is a business justification or compliance-based requirement. These protocols are old and not scalable, and certificate management for email encryption is also cumbersome. To learn more about PGP and S/MIME, refer to Note 1.

Update Security Awareness Training Regularly

According to Verizon's 2024 Data Breach Investigations Report, 68% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering. [2] The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities. [2] According to the Federal Trade Commission (FTC), around 490,000 impersonation scams were reported last year in the U.S. The losses due to these scams exceeded $1.1 billion. [8]

This human fallibility has been a constant companion to email, a vulnerability exploited by bad actors throughout its history. While it is impossible to eradicate the human error element entirely, it can be reduced to some extent. SRM leaders need to adopt the following measures to identify phishing attempts, practice password hygiene and report suspicious activity:

- **Implement secure behavior and culture program (SBCP):** Security awareness training alone will not be enough to reduce the risks caused by human activities. Leverage the Gartner PIPE Framework to guide your execution of an SBCP to foster and embed new, more secure practices and behaviors that help minimize avoidable cybersecurity risks. Use behavior-centric, outcome-driven metrics to demonstrate that the SBCP is working. See CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework for more details.

- **Incentivize/reward secure user behavior:** Introduce security awareness quiz programs and other interactive sessions to engage end users. Use rewards to encourage participation. This will motivate end users to be more vigilant and report threats such as social engineering attempts and phishing emails.

- **Curate training for end users based on their roles, user behavior and the threat landscape:** Email security also relies on secure behavior and practices by all end users. Many email security solutions now have their users' profile risk scores on their UIs. Categorize all end users based on their profile's risk score and job roles. Curate security awareness training for each group based on their scores and roles. Include real-life examples or use cases in your security awareness training sessions. Real-time embedded nudges, such as context-aware banners, header references, word highlights in emails and malicious URL blocking with warning messages, can notify users of suspicious email elements and link to relevant training. This direct linkage to relevant training modules helps in real-time user education.Given the modern threat landscape, conducting QR code security awareness training is advised. SRM leaders should ensure that the organization develops and delivers security awareness training using real-world traffic that has been neutered and specifically focused on new threats such as quishing scams. Train employees to be wary of QR codes embedded in emails, especially from unknown senders, and only scan QR codes from trusted sources. If you need to analyze the URL, manually type the URL encoded in the QR code into a web browser instead of clicking on the scanned embedded link.Secure practices empower employees to identify and avoid QR code phishing attempts. They reduce the risk of employees unknowingly compromising their credentials or infecting devices with malware and protect sensitive business data from unauthorized access.

- **Organize phishing simulation campaigns and incident response (IR) drills:** Do this regularly to test employees' responses and ensure that all end users and internal security operations center (SOC) teams know their roles and responsibilities in mitigating threats. Also, it is important not to benchmark your business's simulation failure rates with your peers as every organization has a unique security posture, employees, and different types and frequencies of phishing simulation. This creates unnecessary pressure on the organization to meet certain standards while shifting its focus from the actual outcome: improving the security posture and employees' learning.

Evidence

[1] 2023 Data Breach Investigations Report, Verizon.

[2] 2024 Data Breach Investigations Report, Verizon.

[3] Market Guide for Email Security

[4] Cost of a Data Breach Report 2024, IBM.

[5] Top Email Threats and Trends, Barracuda.

[6] **2023 Gartner Cloud Security Governance Survey.** This survey aimed to understand more about cloud security governance — adoption, challenges, owners and risks. The survey was conducted from 8 through 21 August 2023. Fifty-one IT and business leaders participated from Gartner's Research Circle, a Gartner-managed panel, who have visibility into cloud security governance. Survey respondents were from North America (n = 16), EMEA (n = 24), Asia/Pacific (n = 8) and Latin America (n = 3).

[7] Implementing Phishing-Resistant MFA, Cybersecurity & Infrastructure Security Agency.

[8] FTC: Americans Lost $1.1 Billion to Impersonation Scams in 2023, Bleeping Computer.

[9] Difference between PGP and S/MIME, JavaTpoint.

Note 1: What Is PGP and S/MIME?

PGP is used for end-to-end encryption of email contents and has better encryption capabilities than S/MIME. S/MIME provides both end-to-end encryption of email contents and digital signatures for authentication. S/MIME is more commonly adopted by business organizations as it is less expensive than PGP. S/MIME can process multimedia emails, whereas PGP can only process plain text emails. S/MIME also offers data security features such as message integrity, authentication and nonrepudiation. [9]

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Tool: Vendor Identification for Email Security

Market Guide for Email Security

Voice of the Customer for Email Security

Innovation Insight on Security Behavior and Culture Program Capabilities

How to Protect Organizations Against Business Email Compromise Phishing

Implement DMARC to Prevent Business Email Compromise
