PAUBOX

2025 REPORT

The Healthcare Email Security Report

Key insights from 180 email-related healthcare breaches

Table of contents

Executive summary

Between January 1, 2024, and January 31, 2025, 180 healthcare organizations reported email-related security breaches to the HHS Office for Civil Rights (OCR). Despite increased spending on email security solutions, these organizations still fell victim to cyberattacks—many due to limited security.

This report uncovers the root causes of these breaches and provides actionable recommendations to improve email security posture in the healthcare industry. Many organizations operate under a false sense of security, assuming that investing in premium solutions is enough. However, without proper implementation and enforcement of security protocols, they remain vulnerable.

OCR Director Melanie Fontes Rainer warns, "HIPAA-regulated entities need to be proactive in ensuring their compliance with the HIPAA Rules, and not wait for OCR to reveal long-standing HIPAA deficiencies."[1] The prevalence of breaches in 2024 underscores this warning: many healthcare organizations only realize their security gaps after a serious incident occurs.

The financial impact of these breaches extends beyond reputational damage. A Paubox survey found that nearly 70% of IT healthcare leaders estimate the consequence of a HIPAA violation would cost over $250,000, but according to IBM, the true average cost of a data breach in healthcare is $9.8 million[2]. Cases like Solara Medical Supplies' $9.76 million class action settlement[3] highlight how regulatory enforcement is escalating, putting organizations at greater financial risk.

> According to IBM, the true average cost of a data breach in healthcare is $9.8 million.

Methodology

This report is based on data collected from the HHS Office for Civil Rights (OCR) Breach Portal[4], commonly referred to as the Wall of Shame. It includes breaches reported between January 1, 2024, and January 31, 2025 that were categorized as email-related incidents. The analysis also incorporates:

MX record analysis: Reviewing mail exchanger records of breached organizations to determine their email security provider.

SPF and DMARC: Assessing whether the breached organizations had properly configured email authentication mechanisms.

Risk classification framework: Assigning organizations to High, Medium, or Low risk based on their security configurations.

Comparative analysis: Evaluating security postures across different email security providers, such as Microsoft 365, Proofpoint, and Google Workspace.

Email security by the numbers

180

healthcare organizations fell victim to email-related breaches in 2024

43.3%

of healthcare breaches were Microsoft 365

5%

of known phishing attacks are reported by employees

264%

increased surge of ransomware attacks on healthcare organizations

Understanding attack vectors: How email breaches happen

To better understand the nature of email breaches in healthcare, we examined the attack vectors used by cybercriminals. Below are the most common attack methods:

- **Phishing attacks:** Cybercriminals send deceptive emails[5] impersonating legitimate sources to trick employees into sharing credentials or downloading malware. According to a Paubox survey, IT leaders estimate only 5% of known phishing attacks are reporting by employees to their security teams.
- **Spoofing & impersonation:** Attackers impersonate or spoof executive email accounts to authorize fraudulent transactions or request sensitive data. Threat actors forge email headers to make messages appear as though they originate from trusted sources, bypassing weak security configurations.

> According to a Paubox survey, IT leaders estimate only 5% of known phishing attacks are reporting by employees to their security teams.

How spoofing works

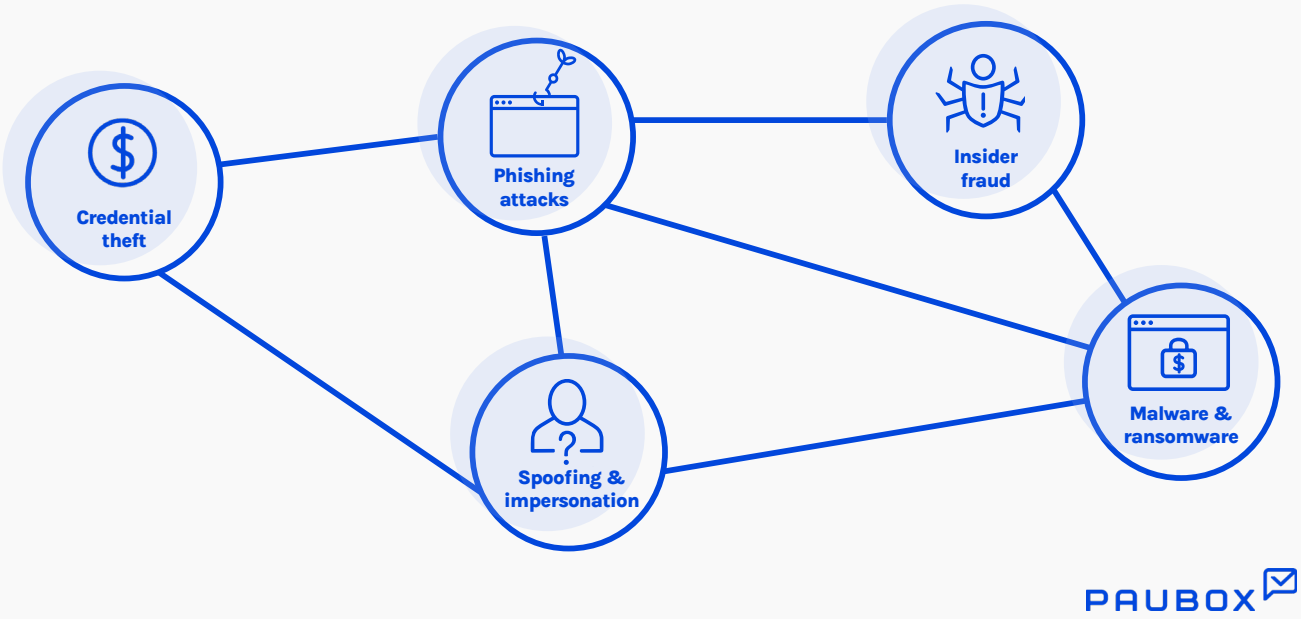
Attackers spoof executive email accounts to authorize fraudulent request

Server thinks request is genuine and sends message to victim

Recipient believes email is legitimate and falls victim to request

PAUBOX

Most common vector attacks



- **Credential theft:** Hackers use leaked or stolen login credentials to gain unauthorized access to email systems, often due to weak or reused passwords. The Warby Parker breach, which compromised nearly 200,000 patients' data through credential stuffing attacks[6], acts as an example of these risks.
- **Malware & ransomware:** Attackers distribute malicious software through email attachments or links, encrypting files and demanding ransom for decryption keys.
- **Insider fraud:** More than half of insider fraud incidents within the healthcare sector involve the theft of customer data, according to Carnegie Mellon University Software Engineering Institute (CMU SEI)[8]. Employees with access to patient information remain a significant risk factor in breaches.

Insight

Since 2018, ransomware attacks on healthcare organizations have surged by 264%, according to the OCR.[7]

Each of these attack vectors exploits poor security configurations and user vulnerabilities, highlighting the need for robust authentication and threat detection mechanisms.

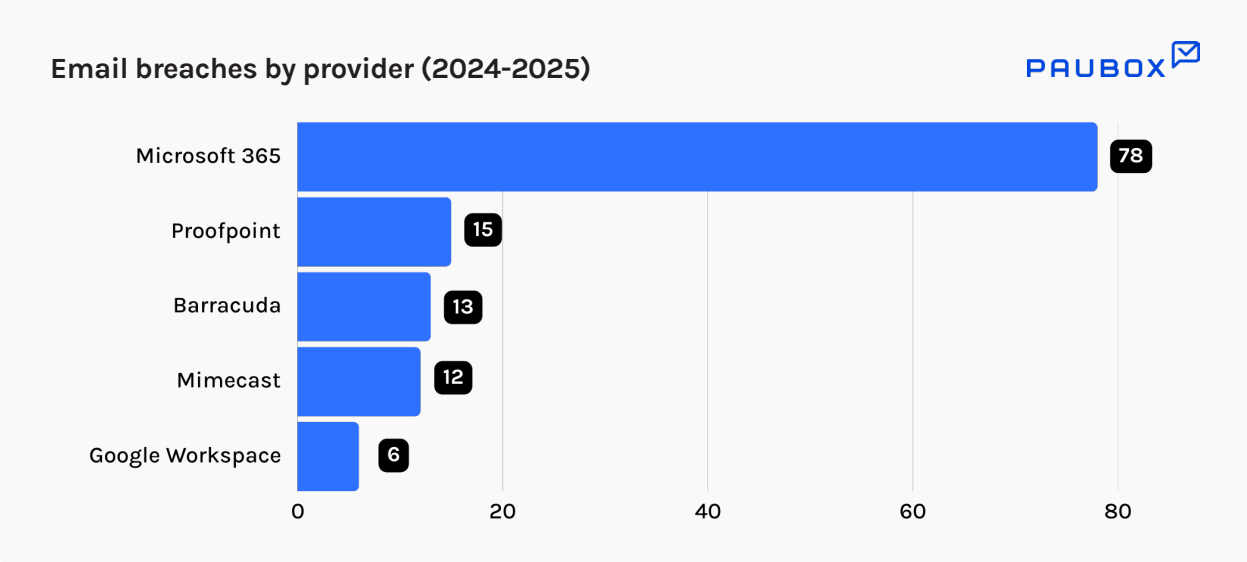
Healthcare's email crisis

Understanding the breach landscape

Email remains the primary communication tool in healthcare, yet it is also the weakest security link. In 2024 alone, 180 healthcare organizations fell victim to email-related breaches, exposing thousands of sensitive patient records. These incidents highlight the growing need for robust email security policies.

Among the affected organizations, Microsoft 365 emerged as the most breached email security provider, accounting for 43.3% of all incidents (78 organizations). This is followed by Proofpoint (12.8%), Barracuda Networks (7.2%), Mimecast (6.7%), and Google Workspace (3.3%). While Microsoft 365 offers built-in security measures, misconfigurations and lack of enforcement have left many organizations vulnerable to attacks.

> Barracuda, Mimecast, and Proofpoint account for 26.7% of breaches in 2024.

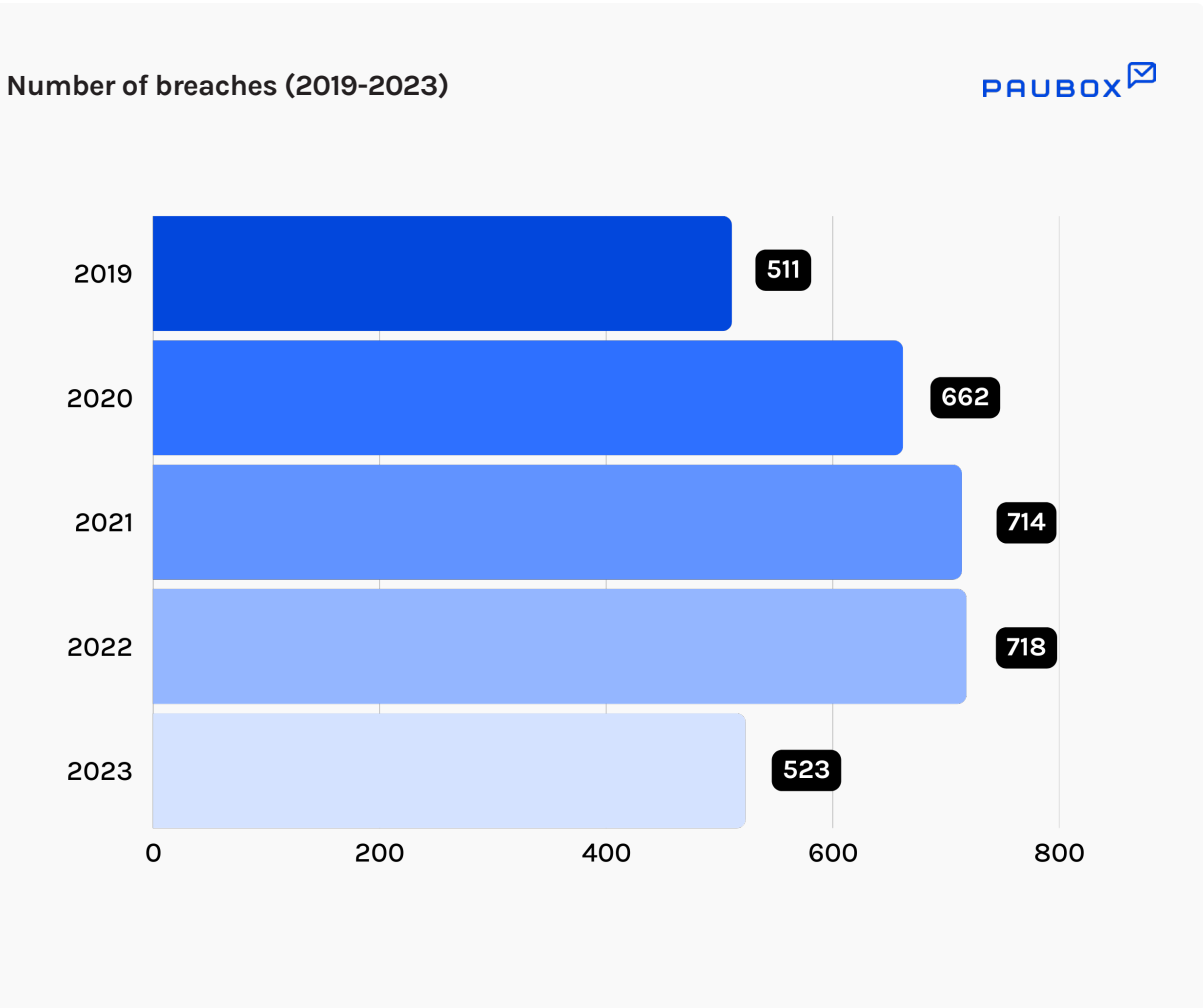


Rising cybersecurity spending isn't stopping breaches

According to Moody's, "Cybersecurity spending rose by 70%, over the past four years."[9] Cybersecurity as part of overall technology budgets rose by 50% from 2019 to 2023 in the healthcare sector alone.

"Overall, issuers say they devoted a median of 8% of their technology budgets to cybersecurity in the survey, up from 5% in 2019. The increase is likely a response to rapid digitalization and an accompanying rise in cyber risk in recent years. A shift to remote work during the COVID-19 pandemic has also broadened issuers' digital footprints and opened new channels for cyberattacks."

> Cybersecurity as part of overall technology budgets rose by 50% from 2019 to 2023 in the healthcare sector alone



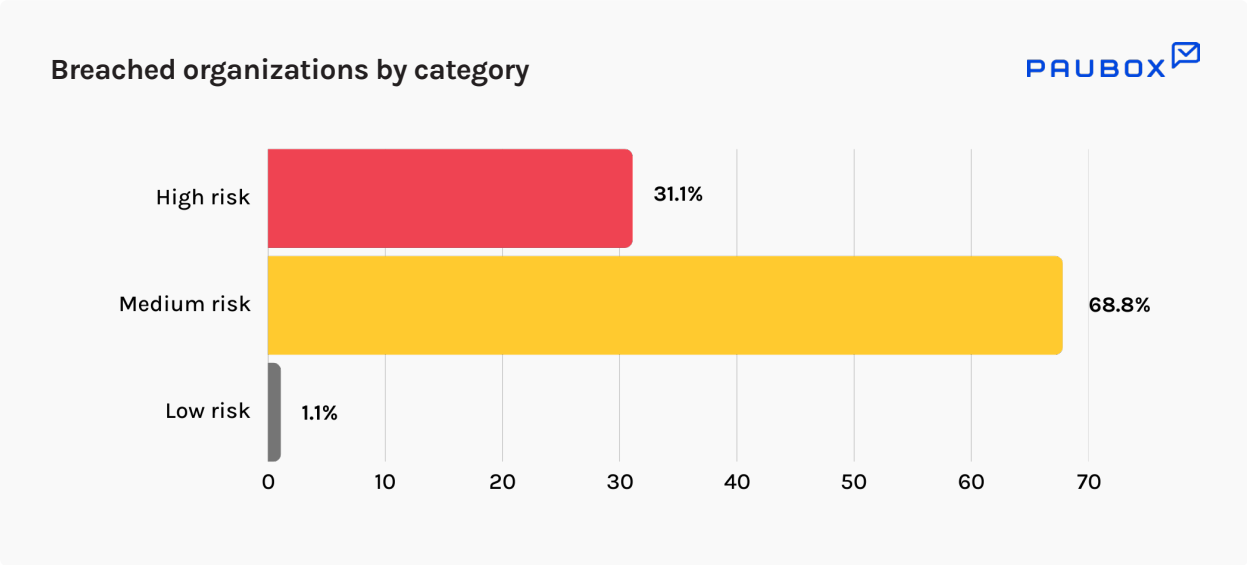
The Microsoft 365 paradox: Market leader in breaches

Breach risks by the numbers

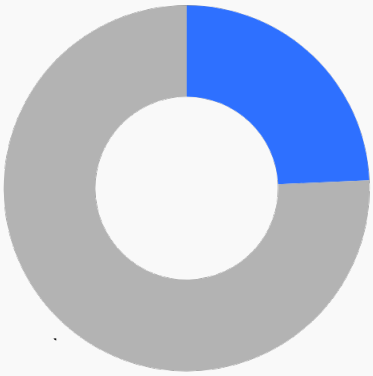
Despite the increase in cybersecurity spending, email is still at high risk. 31.1% of breached organizations were categorized as High Risk, meaning they had multiple security gaps that exposed them to major cybersecurity threats. The majority, 67.8%, fell into the Medium Risk category, indicating partial security measures that still left vulnerabilities open for exploitation. Only 1.1% of organizations were classified as Low Risk, suggesting that few organizations have fully optimized their email security posture.

The alarming reality

Even organizations that invest in security tools are not immune to breaches. A Paubox survey showed that despite advancements in technology, only 27% of IT leaders feel confident about avoiding breaches in 2025, signaling a critical gap in current strategies. Without proper implementation, configuration, and continuous monitoring, these security measures offer a false sense of protection rather than real security.



Breakdown of breached Microsoft 365 users



24.3% were classified as "High-risk"

37.2% had DMARC in "monitor-only" mode

27% of IT leaders feel confident about avoiding breaches in 2025

A false sense of security in healthcare email

Microsoft 365 dominates the business email landscape, particularly in the healthcare sector. However, its widespread adoption also makes it a major target for cybercriminals.

- Microsoft 365 accounted for 43.3% of healthcare email breaches.
- While Microsoft offers security tools, many healthcare organizations fail to configure them properly.
- 37.2% of breached Microsoft 365 — effectively allowing phishing attacks to go undetected.
- 24.4% of Microsoft 365 users were classified as 'High Risk' despite paying for E5 security licenses.

The paradox is that many organizations invest in Microsoft 365's security features but neglect to properly configure critical settings, leaving their systems vulnerable.

Key takeaway

Organizations need to layer solutions like Paubox on top of email providers like Microsoft 365 to maintain compliance.

Security gaps that led to breaches

Email security misconfigurations: A preventable crisis

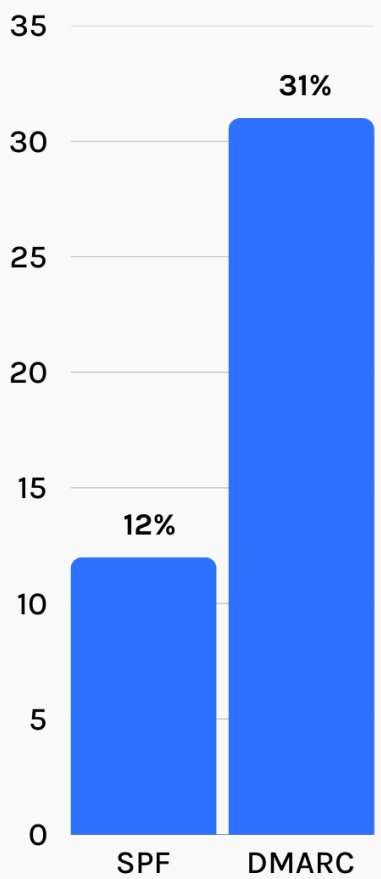
Most breaches in healthcare email systems stem from basic security. A lack of essential protections opens the door to phishing, spoofing, and ransomware attacks.

- **SPF (Sender Policy Framework) issues:** 12.2% lacked SPF records altogether. 40% had weak ‘soft SPF’ configurations, making it easier for attackers to spoof emails.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance) issues:** 30.6% lacked DMARC records. 34.4% had DMARC in ‘monitor-only’ mode, which allows spoofing attempts to continue unchecked.

Insight

Healthcare organizations are failing to implement basic security policies, leaving them exposed to avoidable threats.

Common security misfigurations by percentage



From inbox to breach

Real-world consequences of poor email security

In 2024, HHS OCR announced a settlement with Solara Medical Supplies[10], a distributor of diabetes management products. Solara reported a breach in 2019 after a phishing attack allowed unauthorized access to eight employee email accounts.

The result:

- Over 114,000 patient records compromised
- OCR settlement totaling $3 million
- Class action lawsuit settlement totaling $9.76 million
- Severe reputational damage and loss of patient trust

Similar cases appear frequently on the OCR Wall of Shame, proving that lax email security has real-world consequences. OCR Director Melanie Fontes Rainer pointed out that, “Patients must be able to trust that sensitive, health information in their files is protected to preserve their trust in the patient-doctor relationship and ensure they get the care they need.”[11]

> “Patients must be able to trust that sensitive, health information in their files is protected to preserve their trust in the patient-doctor relationship and ensure they get the care they need.”
>
> **Melanie Fontes Rainer,** OCR Director

Insight

Proper email security is not just a best practice—it’s a legal and financial necessity.

Future outlook

Where healthcare email security is headed

"The increasing frequency and sophistication of cyberattacks in the health care sector pose a direct and significant threat to patient safety," said HHS Deputy Secretary Andrea Palm.[12] "These attacks endanger patients by exposing vulnerabilities in our health care system, degrading patient trust, disrupting patient care, diverting patients, and delaying medical procedures." Based on the trends identified in this report, we predict the following developments:

- **Increased attacks on cloud-based email systems:** As Microsoft 365 and other cloud-based solutions dominate, attackers will develop more sophisticated techniques to exploit misconfigurations and bypass existing security measures.
- **Adoption of AI-driven phishing attacks:** Cybercriminals will leverage AI-generated phishing emails to craft more convincing social engineering attacks. "Attackers are leveraging AI to craft highly convincing voice or video messages and emails to enable fraud schemes against individuals and businesses alike," said FBI Special Agent in Charge Robert Tripp.[13]
- **Mandated email security standards:** More healthcare organizations will be required to enforce DMARC, and SPF, shifting from optional security measures to mandatory compliance.
- **Escalating healthcare cybersecurity investment:** Organizations will need to allocate more resources to defend against increasingly sophisticated cyber threats. CareM Direct of Information Technology, Ryan Winchester added, "Small businesses, especially those without an IT background, are at huge risk

> "The increasing frequency and sophistication of cyberattacks in the health care sector pose a direct and significant threat to patient safety,
>
> **Andrea Palm,** HHS Deputy Secretary

Email trend security predictions for 2025

1. **Increased attacks on cloud-based email systems**
   Attackers will develop techniques to exploit misconfigurations and bypass existing security measures.

2. **Mandated email security standards**
   More healthcare organizations will be required to enforce DMARC and SPF.

3. **Adoption of AI-driven phishing attacks**
   Cybercriminals will leverage AI-generated phishing emails to craft convincing social engineering attacks.

4. **Escalating healthcare cybersecurity investment**
   Organizations will need to allocate more resources to defend against increasingly sophisticated cyber threats

PAUBOX

when it comes to cybersecurity. Many rely on outdated or consumer-grade technology, leaving their networks vulnerable. Unsecured home Wi-Fi, outdated IoT devices, and unpatched software only add to the problem. Healthcare organizations need to evaluate everything connected to their network and invest accordingly to secure it."

> "Healthcare organizations need to evaluate everything connected to their network and invest accordingly to secure it."
>
> **Ryan Winchester,** Director of IT

Addressing concerns with risk analysis

According to OCR, required measures are mandatory, while addressable ones offer flexibility based on risk. If an addressable measure is deemed necessary, it must be implemented. If not, the organization must document its reasoning and apply an alternative solution. Decisions should be based on risk analysis, existing security, and costs. Failure to properly assess or document these choices can still lead to penalties.

"An accurate and thorough risk analysis is foundational to both HIPAA Security Rule compliance and protecting health information from cyberattacks," said Fontes Rainer.[17] "Failure to conduct

Increased regulatory pressure

HIPAA is increasing email security requirements to protect against cyber threats. According to the new HIPAA Security Rule NPRM[14], "the proposed rule would modify the HIPAA Security Rule to require health plans, health care clearinghouses, and most health care providers, and their business associates to better protect individuals' electronic protected health information against both external and internal threats." Recent settlements[15] suggest enforcement efforts are escalating.

Senators Wyden and Warner also introduced[16] the Health Infrastructure Security and Accountability Act (HISAA) in an effort to bring the patchwork of healthcare data security standards under one minimum umbrella and to require healthcare organizations to remain on top of software systems and cybersecurity standards.

a risk analysis leaves health care entities exposed to future hacking and ransomware attacks. OCR urges health care entities to take the necessary steps to reduce risks and vulnerabilities and safeguard protected health information."

With increased regulatory scrutiny, organizations must justify their security decisions, especially when choosing alternatives to addressable specifications. OCR has made it clear that poorly

> "An accurate and thorough risk analysis is foundational to both HIPAA Security Rule compliance and protecting health information from cyberattacks."
>
> **Fontes Rainer**

implemented compliance measures will not be tolerated. To stay ahead of these threats, healthcare IT leaders must shift from a reactive security approach to a proactive one, ensuring their email security configurations meet best-in-class standards.

"The data shows that even the most established email security tools are just a starting point in protecting patient data. To stay compliant, organizations must continuously evaulate their implementations. That can mean adding in additional layers of defense", said Paubox Chief Compliance Officer, Rick Kuwahara.

The solution

HIPAA compliant solutions for any organization

The data is clear: paying for premium security solutions is not enough if organizations fail to implement basic security measures. Healthcare IT leaders must move beyond compliance checkboxes and leverage email security solutions that provide freedom from human error.

Paubox stops inbound and outbound email threats that lead to costly data beaches and HIPAA violations. Our patented email, text, and marketing solutions let healthcare organizations send encrypted HIPAA compliant emails directly to the recipient's inbox – no portals or passcodes necessary. The best part is that our solution integrates with your existing email platform and is set up in minutes.

> "No amount of training can completely eliminate human error, so businesses must have safeguards in place."
>
> **Ryan Winchester,** Director of IT

Eliminate the risk of human error

Other solutions require employees to manually encrypt emails, increasing the risk of human error. Paubox encrypts every email by default. Winchester shared, "No amount of training can completely eliminate human error, so businesses must have safeguards in place."

Easy to send, easy to receive

Paubox works with your existing email, like Microsoft 365, Microsoft Exchange, and Google Workspace. There are no extra steps to send or receive an email. HIPAA compliant emails are read directly in the recipients' inboxes, and responses land directly in yours.

Protect your organization from security threats

ExecProtect, our patented inbound email security solution, safeguards against executive impersonation, catching malicious emails before they arrive in your inbox. Data loss prevention ensures sensitive company information isn't leaked outside the organization.

Sources

[1] "HHS Office for Civil Rights Settles with L.A. Care Health Plan Over Potential HIPAA Security Rule Violations", public3.pagefreezer.com

[2] "Cost of a Data Breach Report 2024", ibm.com

[3] "Solara Medical Supplies To Pay $3m To Settle Cyber Violations", hmenews.com

[4] U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, ocrportal.hhs.gov

[5] "What is a phishing attack?", paubox.com

[6] "HHS Office for Civil Rights Imposes a $1,500,000 Civil Money Penalty Against Warby Parker in HIPAA Cyber-security Hacking Investigation", hhs.gov

[7] "HHS Office for Civil Rights Settles Ransomware Cybersecurity Investigation under HIPAA Security Rule for $250,000", public3.pagefreezer.com

[8] "Insider Threats in Healthcare (Part 7 of 9: Insider Threats Across Industry Sectors)", insights.sei.cmu.edu

[9] "Cyber budgets increase, executive overview improves, but challenges lurk under the surface," moodys.com

[10] "Solara Medical Supplies, LLC Resolution Agreement and Corrective Action Plan", www.hhs.gov

[11] "HHS Office for Civil Rights Settles with Holy Redeemer Family Medicine Over Disclosure of Patient's Protected Health Information, Including Reproductive Health Information", public3.pagefreezer.com

[12] "HIPAA Security Rule NPRM", www.hhs.gov

[13] "FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence", www.fbi.gov

[14] "HIPAA Security Rule NPRM", www.hhs.gov

[15] "Solara Medical Supplies To Pay $3m To Settle Cyber Violations", hmenews.com

[16] "HIPAA Gets a Potential Counterpart in HISAA", natlawreview.com

[17] "HHS Office for Civil Rights Settles 9th Ransomware Investigation with Virtual Private Network Solutions", public3.pagefreezer.com

PAUBOX EMAIL SUITE

Send email as normal, but HIPAA compliant

- Setup in 15 minutes
- HITRUST certified since 2019
- No portals, no passwords
- Top rated U.S. support

Start for free

"2025 will be the year of highly convincing phishing emails. With AI's rapid advancement, cybercriminals can scrape social media and craft personalized emails designed to steal identities and money. That's why we need companies like Paubox to leverage AI for defense–because even one mistake can have serious consequences."

PAUBOX

RYAN WINCHESTER, Paubox customer
Heritage Management Services

KEY INSIGHTS

2025 Healthcare Email Security Report

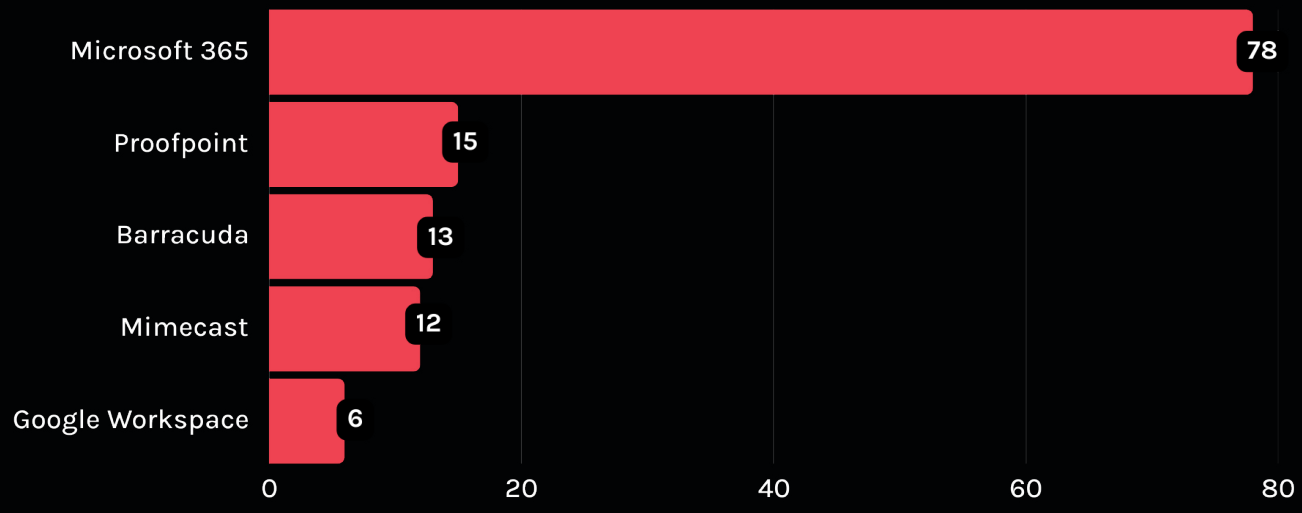
PAUBOX

"To stay compliant, it's crucial to continuously evaluate your implementations to keep up with evolving threats.

– Rick Kuwahara, Paubox Chief Compliance Officer

180 healthcare organizations fell victim to email-related breaches in 2024

Email breaches by provider



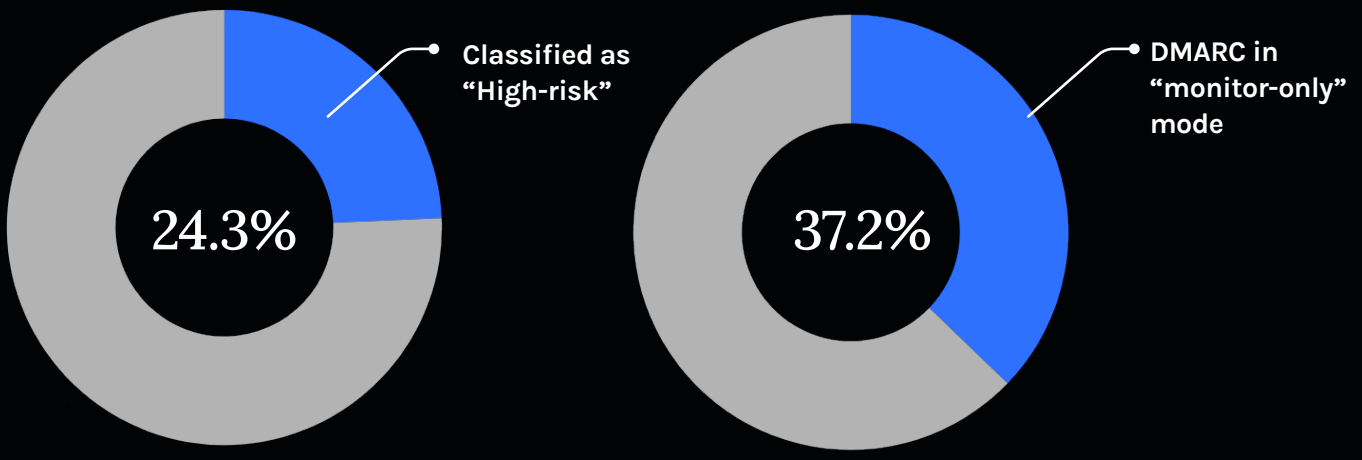
Insight

Proper email security is not just a best practice—it's a legal and financial necessity.

PAUBOX

Microsoft 365 accounted for 43.3% of healthcare email breaches in 2024.

Breakdown of Microsoft 365 breaches



Only 5% of known phishing attacks are reported by employees

Insight

Organizations need to layer solutions like Paubox on top of email providers like Microsoft 365 to maintain compliance

PAUBOX

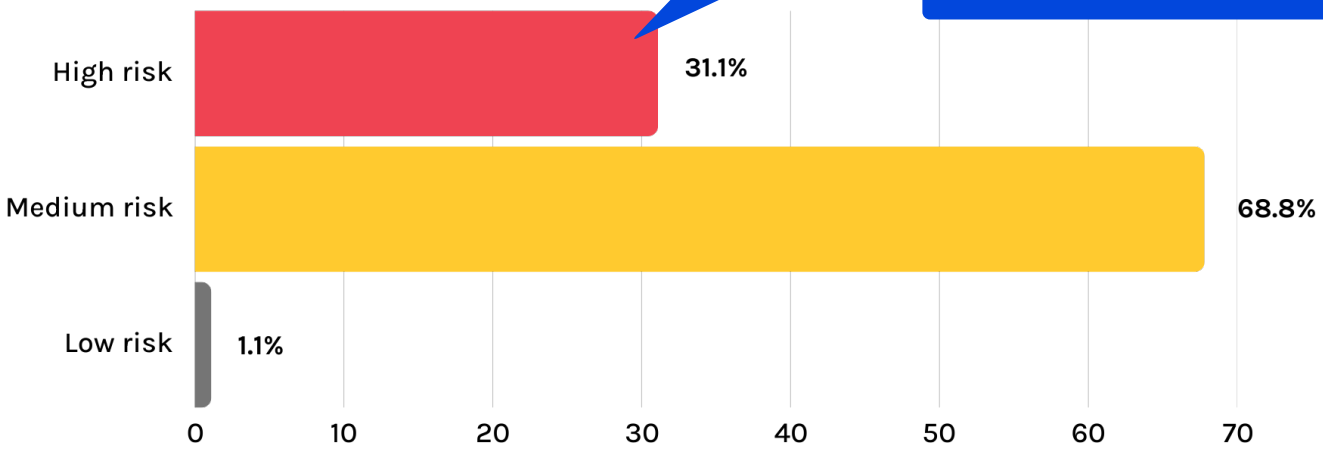
According to IBM, the true average cost of a data breach in healthcare is $9.8 million.

Cybersecurity as part of overall technology budgets rose by 50% from 2019 to 2023 in the healthcare sector alone.

31.1%

of breached organizations had multiple security gaps that exposed them to major cybersecurity threats.

Breakdown of Microsoft 365 breaches



PAUBOX