at bay

InsurSec
Rankings Report

Email + Remote Access

2025

An analysis of At-Bay claims + cybercrime data

Table of Contents

Introduction

For this year's InsurSec Rankings Report, we expanded our analysis beyond email solutions to include an investigation of risk associated with remote access tools. These two categories stand out because together they account for about 60% of all At-Bay insured claims in 2024. When excluding incidents caused by third-party compromises (like a SaaS provider hit by ransomware) or non-cyber events (incidents unrelated to external hacks), the number is even higher. About 90% of attacks against At-Bay insureds began with either email or remote access.

In a continuation of trends from previous years, cyberattackers have concentrated their focus on email and remote access tools because they share two characteristics that make them ideal jumping-off points for attacks: They're ubiquitous, and they're difficult to secure. Businesses are still struggling to keep VPN appliances secure, as they face a constant flow of new vulnerabilities. At the same time, generative AI has exposed how poorly many leading email security tools perform at catching sophisticated financial fraud.

About 90% of attacks against At-Bay insureds began with either email or remote access.

Most businesses can't simply stop using email or remote access tools, but the cyber risk associated with these tools varies widely. Thus, we believe that continuing to share our findings on the performance of these tools, and what we know about the evolving cyberthreat landscape, can help companies make better choices regarding their technology investments. The findings in this report represent an analysis of more than 100,000 policy years of At-Bay cyber claims data from 2021 through Q1 2025.

Key Findings

1

Email claims frequency increased 30% in 2024.

Claims from malicious email continue to see elevated frequency, jumping 30% in 2024 and 3.5X between 2021 and 2024. AI-powered email fraud became popular among attackers in 2023 and is driving a proliferation of email-based attacks. Q1 2025 claims frequency has begun to recede, potentially due to solutions and businesses catching up.

2

The manufacturing industry saw a 62% increase in email claims frequency YoY.

Manufacturing remains the most consistently targeted industry for email-based attacks, 3X more likely to incur an email claim than the lowest frequency industry (technology) in 2024.

3

Google workspace was the most secure email provider for the third year in a row.

Companies using Google Workspace saw the lowest email claims frequency on average. However, businesses using both Google and Microsoft 365 saw claims frequency increase year-over-year.

4

Email security solutions associated with worse outcomes overall.

The average claims frequency of all At-Bay customers with email security solutions saw a relative increase of 53% year-over-year. Nearly every email security solution was associated with higher email claims frequency, except Sophos which topped the rankings.

5

Organizations using VPN solutions by Cisco and Citrix were 6.8X more likely to fall victim to a ransomware attack.

Businesses using on-premise VPN solutions were correlated with 3.7X higher likelihood to be a victim of an attack compared to businesses using a cloud-based VPN or no VPN detected at all.

6

Managed detection and response (MDR) solutions were critical to preventing encryption, when properly configured and actively monitored.

Companies that suffered a computer intrusion from ransomware groups that appear to be targeting SonicWall devices successfully avoided the damaging effects of ransomware when intrusions were detected and blocked by their respective MDR providers.

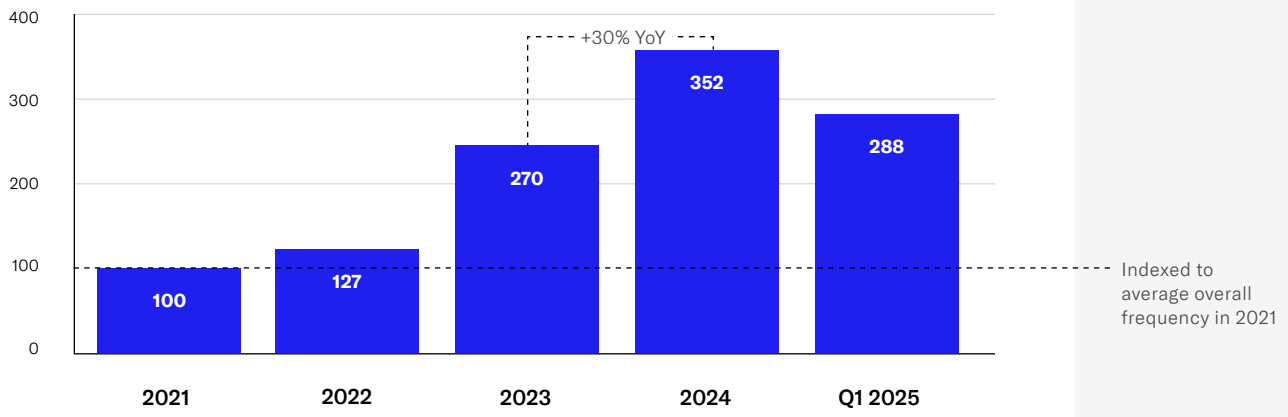
CHAPTER 1

The Email Claims Landscape

FIGURE 1

Email Claims Frequency Growing Steadily Since 2021, Receding in Q12025

Indexed Email Frequency by Year



Email attacks remain one of the fastest-growing and most persistent risks to businesses, with claims frequency increasing significantly since 2021. What began as a steady climb in 2022 accelerated dramatically as attackers began experimenting with generative AI. Claims more than doubled in 2023 and continued to rise another 30% in 2024, representing a 3.5X spike from 2021.

Email continues to be the most common entry vector for attacks seen by At-Bay in 2024, with 43% of incidents initiated by a malicious email (Figure 2), according to our most recent InsurSec Report. The overwhelming majority of malicious emails that resulted in claims were related to financial fraud, with 83% of fraud attacks beginning with an email (Figure 3). Financial fraud incidents are costly. In 2024, the average amount of funds transferred in a fraud incident was $286K with the largest single transaction topping $5M.[1]

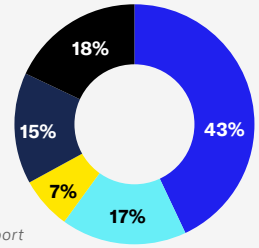
Initial data from the first quarter of 2025 shows email claims frequency declining to near-2023 levels, which may be due to solutions and businesses catching on to these tactics. We cover more on this in the next chapter.

[1] *The 2025 InsurSec Report, All Claims Edition*

FIGURE 2

Claims by Initial Entry Vector

2024

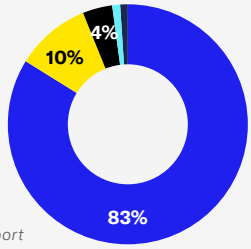


Source: 2025 InsurSec Report

FIGURE 3

Financial Fraud Claims by Entry Vector

2024



Source: 2025 InsurSec Report

Key

- Email
- Corporate System*
- Misc. Malicious Incidents
- Insured's Vendor or client
- Other

**VPN, RDP, or Remote Access Tools*

Email Claims Frequency by Company Annual Revenue

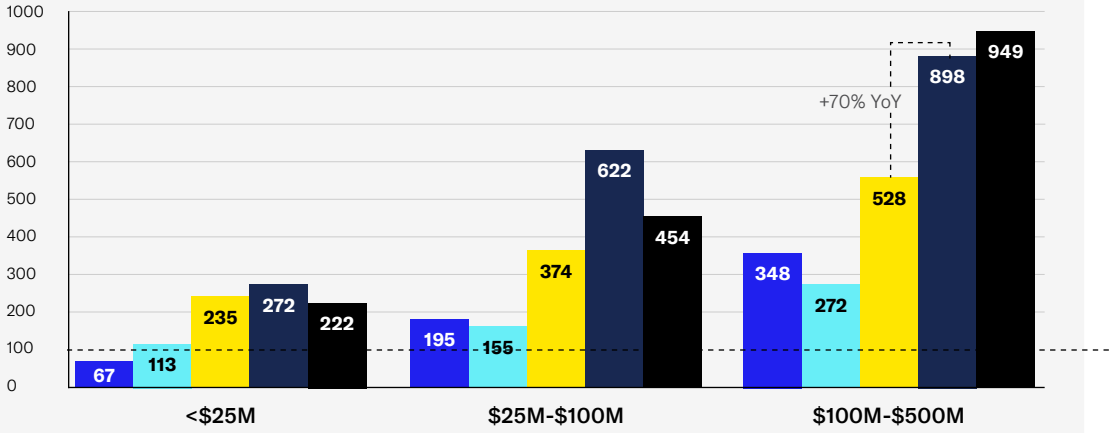
Our findings show that larger companies continue to face a disproportionately higher burden of email-related claims. In 2024, companies with revenue between $100M-$500M had more than 3X the claim frequency of those under $25M, with claims in the largest group rising 70% in a single year. Early 2025 data reinforces the trend.

Larger companies routinely execute bigger financial transactions, manage higher balances, and handle more payment volume, making them more attractive to attackers. Their broader vendor networks and complex organizational structures also introduce more points of weakness, providing attackers with anonymity and openings for interception. The steady rise in claims, especially at larger companies, suggests that attackers are deliberately concentrating efforts where the potential payoff is greatest.

FIGURE 4

The Largest Companies Saw a 70% Increase in Email Claims Frequency in 2024

Indexed Email Claims Frequency by Revenue Band



Key

- 2021
- 2022
- 2023
- 2024
- Q1 2025

Email Claims Frequency by Industry

Manufacturing has been one of the most consistently targeted industries for email-based claims, with frequency spiking over the past four years and increasing 62% in 2024 year-over-year. The sector's heavy reliance on global supply chains and the sheer volume of high-value invoices and cross-border transactions make it a natural target for fraudsters. Attackers are exploiting the pressure manufacturers face to process payments quickly, often across multiple time zones and languages. The persistence of legacy systems, lean IT budgets, and slower adoption of advanced email defenses further amplifies this risk.

Law firms also remain among the hardest-hit sectors. While 2024 showed a slight dip compared to 2023's peak, law firms still face steady pressure from attackers who know the industry manages client funds, settlements, and high-value corporate transactions under tight deadlines. The combination of large dollar amounts and trust-based communication practices continues to make law firms highly attractive targets.

Other industries have experienced more volatility. While retail has experienced increases year-over-year, claims frequency continues to be modest relative to the numbers seen in law firms and manufacturing. Meanwhile, finance, healthcare, professional services, and technology all saw spikes in 2023, but frequency has since receded.

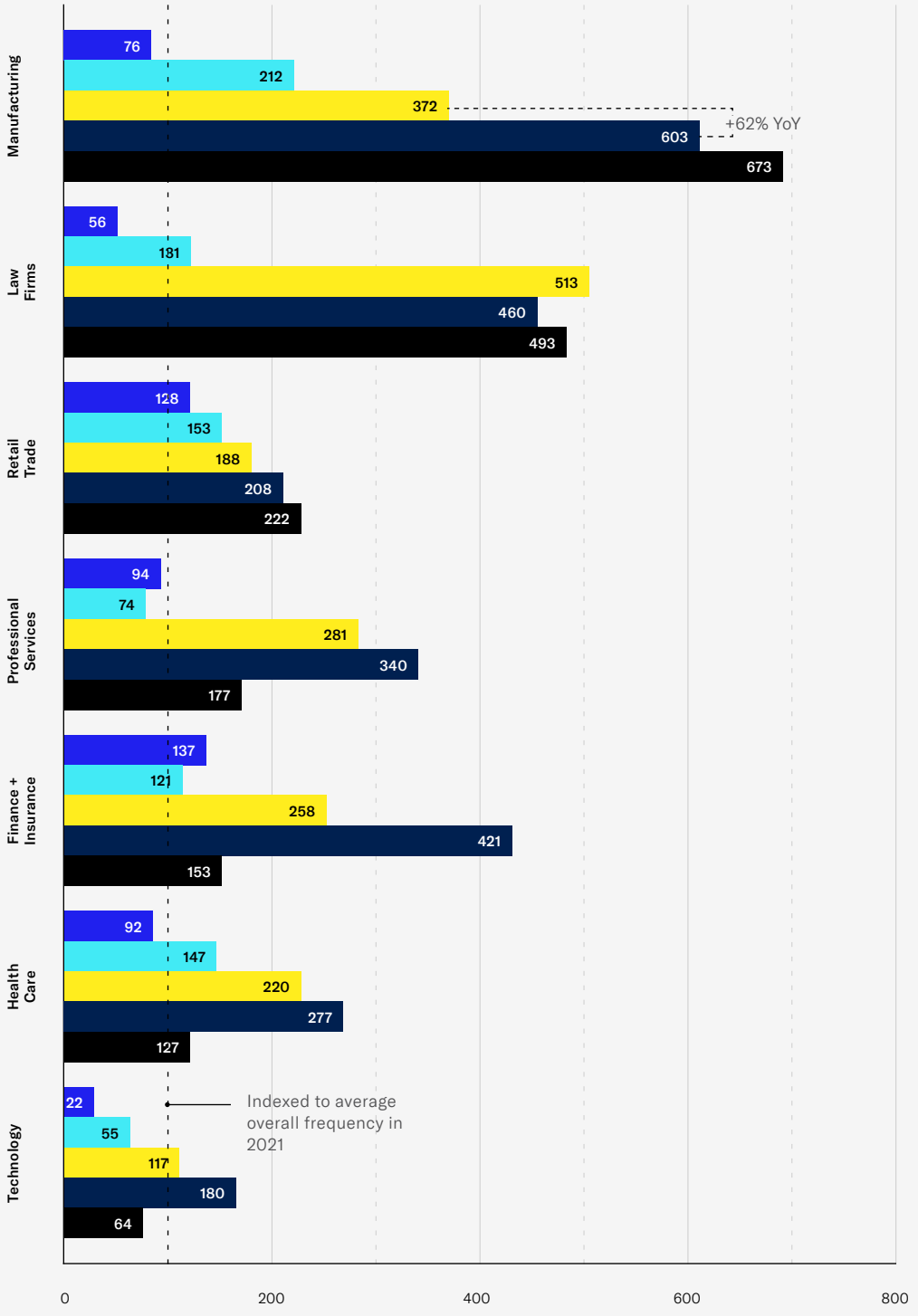
The data suggests attackers are becoming more selective, concentrating their efforts on industries where the opportunity for financial gain remains high and the barriers to successful fraud attempts are lower. Manufacturing's steady climb and law's enduring vulnerability highlight sectors where sustained investment in detection, prevention, and employee awareness is most urgently needed.

Manufacturing saw the highest email claims frequency in 2024, jumping 62% YoY

FIGURE 5

Manufacturing Email Claims Frequency Increased 62% in 2024

Indexed Email Claims Frequency by Industry



CHAPTER 2

Email Solutions and Security Rankings

The overall performance of all email solution providers in use among our insureds declined compared to previous years due to the prevalence of fraud attacks. Financial fraud continues to be the number one source of claims among At-Bay insureds, and the glut of attackers focusing on fraud is forcing a change in the requirements for securing email.

For another year, Google Workspace remained the most effective email provider at mitigating risk with stand-alone performance equivalent to some Secure Email Gateway (SEG) products. However, even they struggled to keep pace with emerging attacker tactics. Google Workspace businesses saw email claim frequency 3X year-over-year. Similarly, businesses employing Microsoft 365 saw email claims frequency worsen.

FIGURE 6

Google Workspace Customers Saw the Best Outcomes for the Third Year

Email Solutions Rankings by Claims Frequency

Email Solution	Email Claims Frequency (2023-Q1 2024)	Email Claims Frequency (2024-Q1 2025)
Google Workspace	0.053%	0.176% (+232%)
Microsoft 365	0.168%	0.278% (+65%)
Avg. Frequency for ALL	0.116%	0.247% (+113%)

**This year we excluded on-premise Microsoft Exchange from the rankings. Usage among our insureds has dropped significantly in recent years and Microsoft Exchange Server 2016 and 2019 have reached their End-of-Life (EOL) phase. We have more details in our Methodology.*

Email Security Solutions Rankings

To see which email security tools have kept pace with emerging attacker tactics, we once again analyzed claims and cybercrime data to compare the outcomes of businesses with email security solutions common among our insureds. This analysis included email-related claims where an email security solution was in place to calculate the normalized claims frequency.

Overall email claims frequency for customers using an email security solution increased in 2024. Not only that, nearly every email security tool we ranked fared worse in 2024 than the prior year. For customers using Mimecast, Intermedia, and Appriver, email claims frequency about doubled.

FIGURE 7

Most Email Security Solutions Associated with Worse Outcomes YoY

Email Security Solution Rankings by Claims Frequency

Email Security Solution	**Email Claims Frequency** (2023-Q1 2024)	**Email Claims Frequency** (2024-Q1 2025)
Sophos	0.189%	0.112% (-41%)
Proofpoint	0.104%	0.141% (+36%)
Mimecast	0.073%	0.143% (+96%)
Barracuda	0.148%	0.209% (+41%)
Intermedia	0.118%	0.270% (+129%)
Appriver	0.155%	0.286% (+84%)
Average Frequency of ALL At-Bay Customers with Email Security Solution	0.116%	0.177% (+53%)

Email security solutions have proven to be effective at blocking traditional email threats but are struggling to identify emails related to the modern, sophisticated, and often AI-powered fraud attacks that are becoming more common.

This shortfall became apparent during live testing we conducted in the summer of 2024. We evaluated a range of email security tools against threat tactics from actual fraud investigations our Response & Recovery team saw.

We were surprised to find that most email security tools we tested caught almost no fraud emails whatsoever. The few that worked well were the newest tools, built with AI from the start. This mattered because fraud emails often don't show obvious signs that traditional rule-based tools can detect.

The only email security solution that improved this year was Sophos, which jumped from last place in our previous report to first place. This may be due to an early investment in Natural Language Processing (NLP) capabilities that allowed them to be well-positioned against today's financial fraud tactics. However, similar to last year, the small sample size due to low market share should be taken into consideration for this data.

In general, the takeaway is this: Email security solutions were by and large caught off guard by the influx of modern email attacks, thus customers using these tools saw an increase in claims frequency across the board. Most solutions we researched have implemented more AI-based detection capabilities, and we suspect email-related claims frequencies for this cohort to improve.

It's important to note our data only covers Secure Email Gateway (SEG) products, since we have limited visibility into newer Integrated Cloud Email Security (ICES) tools. In the next section, we detail how this new generation of email solutions is being built to stop emerging email-based threats.

The Next Generation of Email Solutions

Unlike SEGs, ICES tools connect via API instead of rerouting email through mail exchanger records, which makes them harder for us to detect. We don't yet have enough claims data to measure their effectiveness the way we can with SEGs. However, we've run our own tests on ICES tools to see how well they stop common email attacks.

In those tests, we observed ICES tools effectively stopping certain types of attacks while legacy SEG-based email security solutions were challenged. Here are some examples:

SEG tools did not detect abuse of email to send sensitive data or fraud emails to external recipients.

This is important because many fraud scenarios start with an attacker compromising the email tenant of one victim organization and then using that access to send unauthorized (yet authentic) emails to a second victim organization. Detecting potential malicious activity in outgoing messages can help stop fraud incidents early in their lifecycle.

SEG tools failed to catch attackers inserting false content into active email threads, unless the injected content contained something clearly malicious, like a phishing link or malware.

They also missed other red flags, such as lookalike domains or spoofed addresses. In our tests we used several variations of this attack and the results were inconsistent. This is likely because SEGs have limited ability to track message context over time.

SEG tools miss malicious emails sent between users in the same company because they only scan messages that pass through them.

Internal emails often stay within the tenant, and unless configured otherwise, these messages bypass filtering by traditional security solutions. Attackers exploit this by using compromised accounts to send fraudulent requests, like payroll updates.

We share a specific fraud example, as well as the tools and capabilities required to prevent fraud from happening, in the next sections.

How Modern Fraud Happens

The most effective fraud emails today don't include phishing links or malicious attachments. They don't invite recipients to help members of the Nigerian royal family or invest in the latest meme cryptocurrency. Instead, fraud emails look like the mundane messages about payments owed and received that are trafficked ad nauseam by accounts payable departments.

We covered an example of what a modern fraud attack might look like in our last InsurSec Rankings Report, but it's worth repeating as we continue to see businesses fall victim to these tactics:

The Anatomy of an Email Fraud Attack

STEP 1

The Infiltration

An attacker uses stolen credentials to compromise a company's email system.

They search for information on business relationships and ongoing transactions.

STEP 2

The Setup

The attacker finds an invoice from a finance employee to a customer for a wire transfer payment.

They register a new domain that is a near-perfect match to the legitimate one (e.g., acme.co instead of acme.com).

STEP 3

The Impersonation

The attacker creates an email account with the new, lookalike domain.

They use the same name, address, and signature as the real employee to appear legitimate.

STEP 4

The Request

The attacker emails the customer who was invoiced to reroute the payment.

"So, sorry. We sent you an invoice with our old wiring instructions. Please use the new wire instructions below for your payment." The original email thread containing the invoice is appended at the bottom of the message to provide realism.

STEP 5

The Payout

This attacker has now broken into and hijacked an email conversation between two parties.

Unless the fraud is detected in time, they will likely receive the wired funds from the victim organization

Note that the company that erroneously transferred funds to the fraudster (in this case, the customer who was invoiced) did not suffer any kind of security failure on their email system or otherwise. This is the challenge of fraud detection today: There are few opportunities for victims to detect abnormal or malicious activity until it's too late.

How AI-Powered Email Solutions Catch Fraud

Because modern fraud messages rarely show clear signs that rules can catch, detection depends on spotting suspicious content and running deeper analysis. AI tools like large language models (LLMs) enhance this process by recognizing context-dependent signals and performing follow-up checks before flagging suspicious email activity. An AI-powered approach might include:

Language Pattern Identification:

An LLM compares the "voice" of a finance employee's past authentic messages with the suspect email. Mismatched tone and patterns, combined with a lookalike domain, indicate an attacker injecting into a thread and spoofing an employee.

Detecting Easy-to-Miss Artifacts:

LLMs can flag homoglyph tricks (e.g., "l" vs. "1") in addresses, URLs, or content. While these often fool rules-based detection and the human eye, an LLM's probability-driven sense of what "fits" in language makes such artifacts stand out.

Analysis in Context:

Attackers make subtle changes to email threads (phone numbers, signatures, headers) that seem harmless but raise flags in payment discussions. Unlike rule-based tools, LLMs read the whole conversation, using context to spot fraud.

Our earlier fraud example could be caught with rules, but most companies lack the talent to build and maintain them, and attackers shift tactics too fast. Our claims data shows these defenses often fail. AI-powered detection keeps pace with attackers, making fraud detection not only possible, but consistently reliable.

At-Bay Fraud Defense

At-Bay Stance Fraud Defense was built using real-world claims data to identify modern email-based fraud attempts that secure email gateways (SEGs) miss. Powered by AI, Fraud Defense integrates with Microsoft 365 and Google Workspace, sending real-time alerts to customers based on the latest fraud tactics we see in our claims data and loss reports every day. At-Bay Cyber and Tech E&O policyholders have access to Fraud Defense as part of their policy.

Learn more about Fraud Defense

Next Steps for Email Security

We expect this year's top three email security vendors to keep competing for the number one spot as their AI-based detection improves, and all will remain strong options. Still, businesses should look beyond tools to strengthen fraud resilience, especially by updating organizational responses to email threats in 2025.

In theory, tools that detect and alert on fraud emails should cover most risks. In practice, many companies still fall victim. Once a solid email security tool is in place, real resilience depends on communication.

First, employees must be retrained to trust email warnings.

In several of our 2024-2025 claims, tools correctly flagged fraud, but alerts were ignored. Years of training made workers expect obvious grammar errors, not today's AI-polished messages. Others distrust tools due to false positives. Either way, alerts must be taken seriously.

Second, incoming fraud emails should be treated as evidence of a targeted attack.

Employees should alert security teams immediately and, when relevant, collaborate with vendors and customers to uncover compromised systems, even if it's not their own.

Third, verifying messages by phone or in person before acting can stop most fraud attempts.

Pushback to this requirement is common, but with the average financial fraud loss at $268K, double-checking payments is smart business.

Finally, companies should assess whether their team or a managed service provider is equipped to track and analyze fraud threats.

If not, managed email security options are available.

MDR for Email

Businesses that deploy modern AI-powered email security solutions are better-positioned to identify and prevent email-related incidents from occurring, but implementation of these solutions is only the first step.
While effective, these tools can be noisy due to the volume of alerts they send, often overwhelming underresourced IT and security teams.

At-Bay MDR for Email combines enterprise-grade email security with 24/7 monitoring from security experts, taking on that homework by identifying the alerts that matter and remediating the issue.

Learn more about about MDR

CHAPTER 3

The Pitfalls of Remote Access

Remote access has been the most significant risk vector tracked by At-Bay for the past five years. In 2020, we reported that as many as 50% of ransomware attacks we saw that year originated from compromised RDP servers.[4]

At the time, we considered VPNs to be the safer alternative as they incorporated significantly more security features than other remote access tools and also were not the subject of significant attention from attackers. The gradual shift away from RDP among our insureds closed a door for attackers and by 2024 RDP was the entry vector for just 14% of ransomware cases.

Unfortunately, we now know that VPNs suffer from the same security shortcomings as RDP. The post-pandemic adoption of VPN solutions by businesses has created an unprecedented opportunity for attackers and subjected many companies to cyber risks far out of proportion to the value of the flexibility the VPN creates. In fact, based on our claims data, businesses with any kind of VPN fare worse than businesses where a VPN is not detected.

Our VPN rankings are different from our email security rankings. Since our data has shown that all VPNs increase a company's cyber risk of ransomware attack, we rank vendors based on how much risk they add, not how well they reduce it. This shows, using our claims data, which vendors make a company more likely to experience a claim.

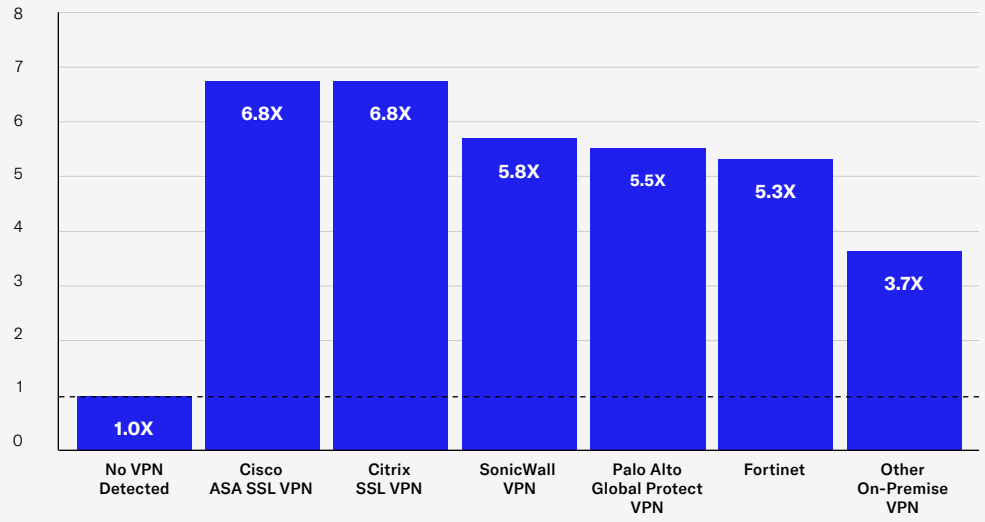
Organizations using VPN solutions by Cisco and Citrix were 6.8X more likely to fall victim to a ransomware attack.

[4] *Coveware: Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate*

FIGURE 8

Likelihood of a Business Using One of These VPNs to Fall Victim to an Attack

Indexed Ransomware Claims Frequency by On-Premise VPN, 2024-Q1 2025



Consistent with the findings from our 2024 InsurSec Report, SSL VPNs from Cisco and Citrix remain the two VPNs associated with the highest ransomware claim frequency. When compared to businesses without a VPN detected, organizations using Cisco or Citrix were 6.8X more likely to fall victim to an attack.

Additionally, businesses using an on-premise VPN of any kind were 3.7X more likely to fall victim to an attack than those using a cloud-based VPN or no VPN detected.

SonicWall VPN Update (Q3 2025)

The time frame for the VPN ranking above is January 2024 through Q1 2025. In Q3 of 2025, At-Bay's Response & Recovery Team observed a 300% increase in Akira ransomware cases compared to Q2, with average ransom demands 104% higher ($958K). Nearly all of these cases involved SonicWall devices. While the exact cause remains unclear, weak credentials, lack of automatic updates, and poor MFA/EDR coverage appear to be key factors.

Our analysis also revealed that Endpoint Detection and Response (EDR) alone was not enough to mitigate the damage. Over half of the victims had an EDR in place, and nearly all of them experienced full encryption. Early indicators show that one control, professionally managed EDR, successfully blocked or contained ransomware before it could cause damage, but only when properly configured and actively monitored.

Skyrocketing Remote Access Vulnerabilities

In 2024, 80% of ransomware attacks against At-Bay insureds had a remote access tool as their identified entry vector, and 83% of those cases involved a VPN device. The outsized risk of VPNs can be attributed to two factors inherent to VPN solutions.

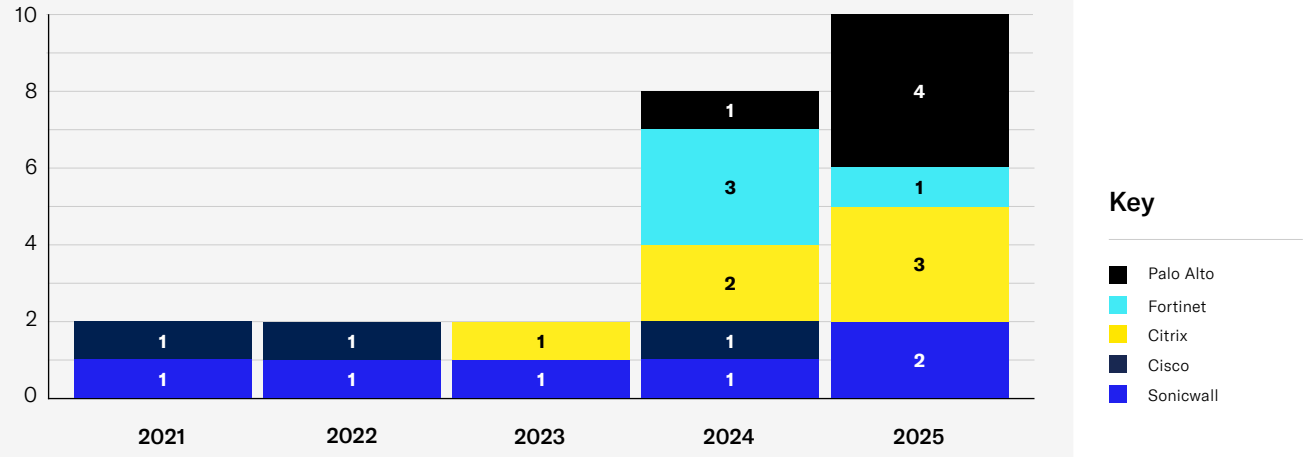
The first is straightforward: VPN tools provide attackers with a door into networks that would otherwise be inaccessible. The second risk with VPNs comes from the complexity of the devices that run them. Early VPNs were simple. They only handled VPN connections and were easier to secure. Over time, vendors began combining multiple functions (like firewall, router, proxy, and VPN) into a single device.

This led to today's Next Generation Firewalls (NGFWs), which can replace an entire stack of older servers, and became widely adopted when remote work exploded. But while powerful, these devices are very complex, and many customers don't fully understand how to use or secure them. The result is that NGFWs create a very large attack surface, which attackers are actively taking advantage of.

Since 2020, a huge number of serious security problems have been found in these devices, with discoveries of high or critical severity (i.e., likely to be the entry vector for a computer intrusion) vulnerabilities related to the riskiest remote access vendors used by At-Bay insureds skyrocketing in 2024 and 2025.

FIGURE 9

High or Critical Severity Vulnerabilities Confirmed Exploited by Vendor



Source: National Vulnerability Database; nvda.nist.gov

[6] *The 2025 InsurSec Report, At-Bay*

If we expand our criteria to examine vulnerabilities of all severity levels (not just high or critical), just one vendor, Fortinet, has more than 500 vulnerabilities listed in the National Vulnerability Database for the period from 2020-2025.

Still, the number of vulnerabilities doesn't automatically mean a product is unsafe if it's well maintained. What concerns us more is what this trend suggests: Attackers may already know about flaws that defenders don't, and even more exploitable issues are likely to surface in the future.

The recent volume of cases related to SonicWall is a perfect example of this. While we're analyzing these incidents in detail to try to determine what changed starting in July of 2025, the possibility that attackers are leveraging an as-yet unknown zero-day vulnerability can't be ruled out. What we have seen in our research is that in the event of a breach, immediate identification and containment are critical.

CASE STUDY

At-Bay MDR Contains and Remediates Threat in 25 Minutes

A manufacturing company avoided a potential claim when At-Bay MDR for Endpoint flagged a high-severity alert. A threat actor was attempting to gain control of a system that belonged to the client's employee.

At-Bay's MDR team immediately began an investigation and discovered the root cause of the attempt was part of a sophisticated malware campaign. Within minutes, At-Bay MDR identified and deleted all instances of the malicious script and blocked malicious domains identified as part of the attack's infrastructure.

Within 25 minutes, the threat had been identified, contained, and remediated.

At-Bay MDR combines enterprise-grade technology with 24/7 monitoring and remediation by security experts. According to our claims data, 90% of claims could have been prevented by At-Bay MDR.

Learn more about MDR

Next Steps for Remote Access

Remote access is complicated and risky, but most companies can't do without it. In the two years since At-Bay began publicly sharing our perspective on the relative risk of VPN devices, the most effective guidance we offer to our insureds is unfortunately not a straightforward solution:

Properly Configure and Monitor VPNs

VPNs can be operated safely if fully patched, configured to minimize attack surface, fully integrated with MFA, and closely monitored by competent professionals, but this is beyond the capabilities of most companies. The better path forward is to stop using VPNs and migrate to modern remote access tools where required.

Move to a Secure Access Service Edge Tool

Businesses using mostly cloud services can move to Secure Access Service Edge (SASE) tools, which reduce VPN risks and add stronger security across both cloud services and legacy systems. Because SASE requires users to connect to a cloud service before accessing other resources, there's no exposed "front door" like a VPN appliance. This shift has helped companies avoid many of the ransomware attacks hitting others.

A major benefit of SASE is centralized maintenance: vendors patch their cloud once, instantly protecting all customers. While SASE tools can have vulnerabilities, they're typically in client software that outsiders can't directly reach, making them far less attractive than exposed VPN appliances. In our claims data, companies using SASE are largely absent from victim lists, and we've seen no evidence of SASE as a root cause in claims from 2020–2025.

Consider an MDR Service

If a transition to SASE is untenable, companies should strongly consider an MDR service for monitoring connections coming into their environment through remote access tools. While MDR does not eliminate the risk of an attacker gaining initial access, it plays a critical role in limiting the damage that can follow.

MDR provides continuous, 24x7 professional monitoring to quickly identify suspicious activity, contain intrusions to limit damage. In this way, MDR serves as a vital last line of defense by helping ensure that a single compromise does not turn into a full-scale breach or business disaster.

CHAPTER 4

Conclusion

This report highlights a cyber landscape defined by accelerating change, where the pace of evolving threats is increasingly outstripping traditional defenses. Email and remote access tools remain the dominant entry points for attacks, but the nature of these threats is rapidly shifting. AI-powered fraud, sophisticated ransomware, and vulnerabilities in VPN appliances demonstrate that falling behind on security innovation is no longer a minor risk, it is a major business vulnerability. Organizations that fail to keep pace with these developments expose themselves to rapidly increasing financial, operational, and reputational damage.

To stay ahead, businesses must adopt a proactive approach, integrating modern, AI-enhanced security solutions with disciplined oversight, continuous monitoring, and rigorous employee training.

Managed EDR and MDR solutions have proven especially effective at preventing encryption and intrusion, while AI-driven email security tools can identify fraud attempts that would evade traditional detection. Emerging managed email security solutions provide an additional layer of protection for resource-strapped businesses.

Partnering with an InsurSec company that leverages real-world loss data to inform security decisions can provide the crucial insights and managed solutions necessary to stay ahead of evolving threats, prioritize investments in security controls, and reduce business risk in this dynamic environment. In a landscape where the speed of cyber risk is only accelerating, maintaining alignment with the latest security intelligence is not optional, it is essential. Businesses that fail to keep up will face mounting exposure, while those that proactively integrate data-driven insights into their security strategy can significantly reduce risk and preserve operational resilience.

Methodology

At-Bay's analysis is based on claims information from 2021 through the first quarter of 2025. Incidents reviewed included those related to email claims, financial fraud, remote access, and ransomware.

By analyzing actual claims data, the At-Bay Research team set out to answer these questions:

1. How are attacks changing?

2. How do outcomes associated with specific solutions and security solutions differ?

3. How do remote access solutions change the risk profile of a company?

This data was collected from At-Bay policyholders during initial underwriting, throughout the policy year, as well as when their claims were processed by our team in the wake of an incident.

Email Analysis + Rankings

To establish the set of "Email Security Solutions" that were worth investigating, we identified more than a dozen providers that were prevalent enough within our customer population to warrant further analysis. For the selected solutions, our researchers established a normalized claims frequency to identify potential correlations with incident occurrences. After further analysis, six email security solutions were considered prevalent enough to provide statistically significant results. The same was done for the "Email Solution" category.

This year, we've excluded on-premise Microsoft Exchange from the rankings for two reasons:

1. Usage of Microsoft Exchange Server has plummeted among our insureds in recent years due in no small part to our efforts to inform them of the extremely high level of risk that this solution posed for their technology environment.

2. On October 14, 2025, Microsoft Exchange Server 2016 and 2019 will reach their End-of-Life (EOL) and no longer receive security updates, bug fixes, or technical support from Microsoft. Our recommendation to organizations still using on-premises Exchange 2016

or 2019 servers is to migrate to Microsoft 365 to avoid significant security vulnerabilities and compliance issues. Adopting the successor to Exchange Server 2019, Exchange Server Subscription Edition, may also be an option. However, At-Bay currently has no information about the security performance of this product due to it being released in July 2025 and therefore can't recommend it.

By identifying the solutions that have a high or low claims frequency compared to the average, we believe that we can assess the relative effectiveness of email security solutions in mitigating the risk of security incidents stemming from email usage.

We infer that insureds with email security solutions that have fewer email claims are more effective at mitigating email risk. The same goes for the customers who didn't have an email security solution in place, that the relative claims frequency is indicative of the effectiveness of the native security capabilities that come built-in for today's email solutions.

Remote Access Analysis and Rankings

Our data has shown the use of any on-premise VPN increases a company's cyber risk of ransomware attack. For this analysis we analyzed which vendors are associated with a company more likely to experience a claim.

To be clear, our claims data does not point to these products being directly responsible for every claim. While on-premise VPNs may not be the initial attack vector in particular incidents, companies using them have a much higher rate of attacks. This could be because of other on-premises systems, or because cybercriminals target these companies knowing that they have an old technology stack.

A Note About Our Revenue Bands

While At-Bay helps place insurance for business with up to $5B in revenue, and these insureds are included in the data, labeling the largest revenue band group "100M-500M" more accurately captures the size of risk represented.

Contributors

Adam Tyra
CISO for Customers

Ayelet Kutner
Chief Technology Officer

Chin Chang
Senior Manager, Risk Analytics

Laurie Iacono
Director, Threat Intelligence

Michael Lowe
Head of Marketing

Ronit Suzan
Product Specialist

Samantha Wong
Risk Analyst

About At-Bay + InsurSec Report

At-Bay is the InsurSec provider for the digital age, helping businesses mitigate cyber risk and avoid incidents by continuously analyzing data from security scans and collecting cyber threat intelligence and the relevant details of security incidents reported by insureds. Because we can correlate information about a significant number of real-world incidents with data about the victim's technology environment before the incident occurred, this enables us to reliably identify trends and relationships that other companies and security vendors cannot. We're able to clearly identify security controls that mitigate risk, differentiate them from security controls that don't mitigate risk, and prove our case with empirical data from actual incidents where those security controls were in place.

Our goal is to share our findings on the respective impacts of a range of security controls with the public at large. We believe we can use facts and evidence to cut through the noise of a crowded cybersecurity marketplace and enable organizations to deploy scarce cybersecurity resources for maximum impact. We regularly develop and share a slate of statistically provable leading practices for security that can be readily consumed by organizations regardless of headcount or the size of their security budget.