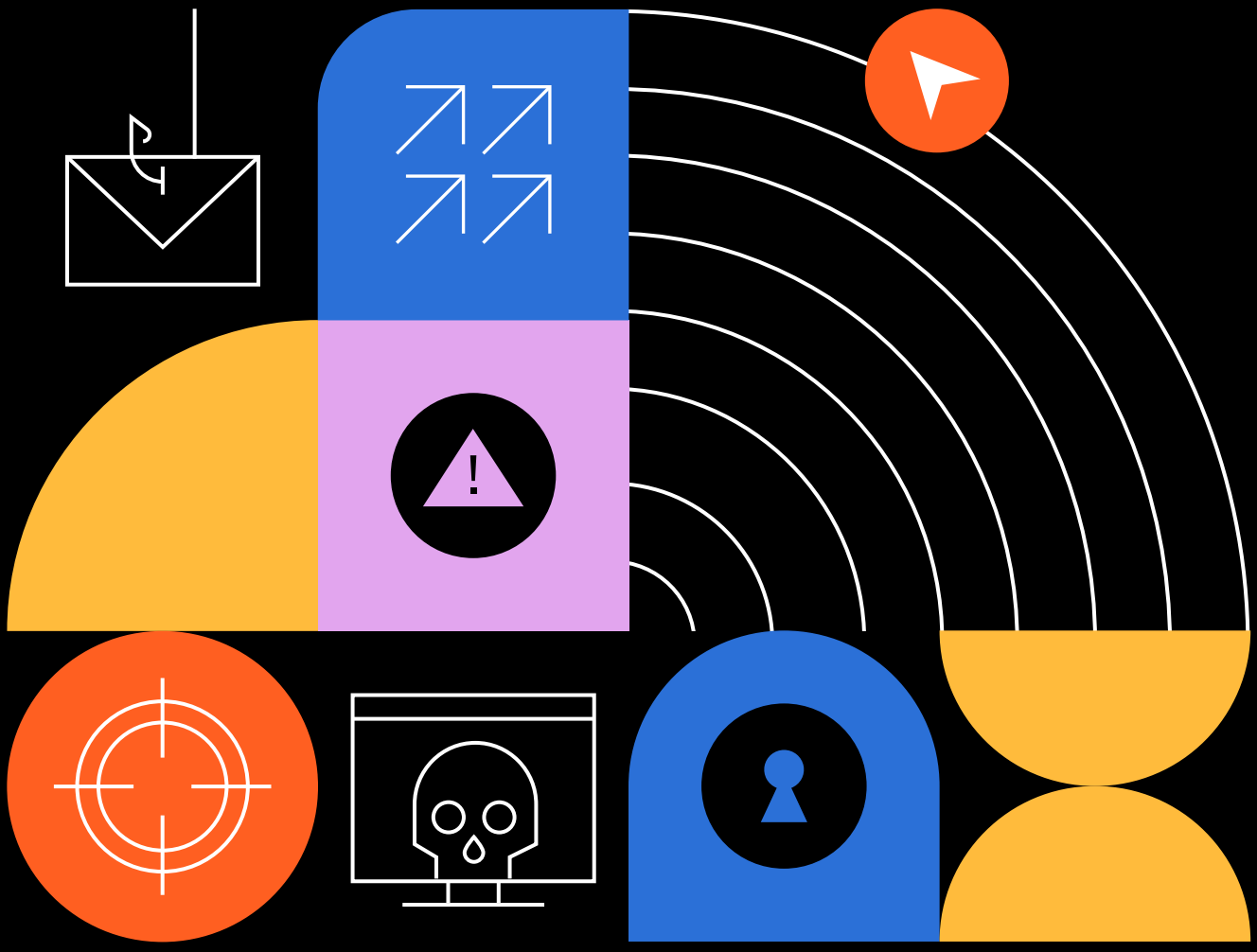
Coalition Security™

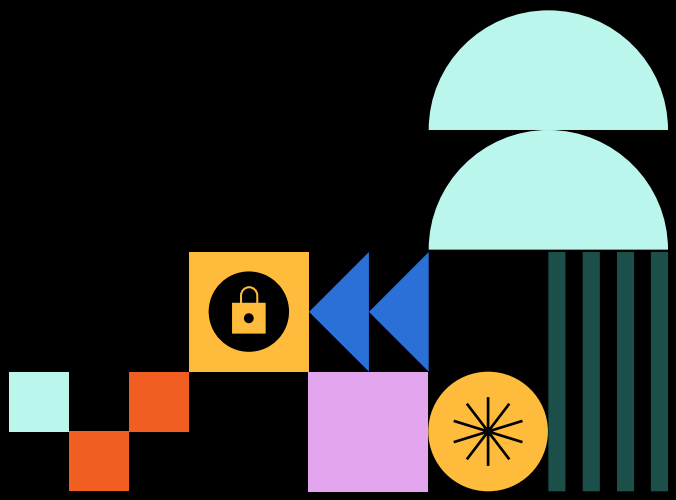
coalitioninc.com



Cyber Threat Index 2025

An examination of the ransomware playbook and how businesses can protect against common attack tactics

Table of Contents



Executive Summary

Business leaders tasked with securing digital infrastructure have likely heard about a dizzying array of attack types, software vulnerabilities, exposures, and misconfigurations.

However, there's a dearth of evidence-based strategies for cutting through the noise and focusing on what *actually* moves the security needle, especially for under-resourced small and midsize businesses (SMBs) that can only make a handful of security investments.

As part of Coalition's mission to protect the unprotected, the *Cyber Threat Index 2025* shares our expert analysis and insights into the ransomware playbook. Key findings include:

- The majority of ransomware claims started with threat actors compromising perimeter security appliances (58%) or remote desktop software (18%).
- Across all ransomware claims, the most common initial access vectors were stolen credentials (47%) and software exploits (29%).
- Exposed logins are an underappreciated driver of ransomware risk. Coalition detected over 5 million internet-exposed remote management solutions and tens of thousands of exposed login panels across the internet.
- Coalition forecasts more than 45,000 software vulnerabilities will be published in 2025.
- AI-driven risk prioritization can address notification fatigue. Coalition sent Zero-Day Alerts for just 0.15% of all vulnerabilities published in the first 10 months of 2024.
- Most proactive alerts sent by Coalition in 2024 concerned configuration issues, such as exposed login panels, exposed services, and risky technologies.

Coalition's security recommendations are calibrated using data from our 360-degree perspective on cyber risk. Our sources include digital forensics investigations, data collected from an internet-wide view from scanning every IPv4 address, proprietary AI models to analyze vulnerabilities and login panels, and actuarial evidence from cyber insurance claims.

About Coalition Security™

Coalition Security helps protect SMBs from the expanding universe of cyber threats. Our tools and services are built and managed by cybersecurity experts who can help spot, prevent, and respond to cyber threats before they impact businesses. With unique access to data from real-world risks and 90,000+ global policyholders, Coalition Security prioritizes threats based on their potential impact while providing security solutions that are tailored specifically for budget-conscious business leaders.

Introduction

While cyber attacks are an existential threat to organizations of all sizes, SMBs remain especially vulnerable to specific cyber attack types, such as ransomware. Cybersecurity concerns are a top threat for 60% of SMB owners, yet just 23% say they are very prepared to handle an attack.[1] Limited expertise and a lack of resources often leave these organizations struggling to navigate the increasingly complex cyber threat landscape.

The first two months of 2024 underscored the scale of the challenge. A series of zero-day vulnerabilities in Ivanti devices enabled both financially motivated criminals and nation-state actors to exploit businesses across various industries.[2] The Volexity researchers who first discovered the flaws reported the victims ranged "from small businesses to some of the largest organizations in the world."[3]

Weeks later, the ransomware attack on Change Healthcare, which processes payments and health information, upended thousands of healthcare organizations of all sizes.[4] The widespread event forced Change Healthcare's parent company to issue $2 billion in advance payments and prompted a congressional hearing.[5]

Despite the far-reaching impacts of both events, Coalition provided advanced notice about the underlying security issues, sending a Zero-Day Alert to vulnerable policyholders 50 days before the United States, United Kingdom, Australia, Canada and New Zealand issued a joint warning about threat actors exploiting the Ivanti vulnerabilities.

Meanwhile, the Change Healthcare incident exploited an exposed Citrix login panel without multi-factor authentication (MFA), a security risk Coalition has required businesses to address in order to purchase cyber insurance since 2021. Early warnings like these are especially critical for SMBs, which often lack the in-house expertise to independently detect and respond to emerging threats.

Coalition does not possess clairvoyance or any other mystical powers. Instead, we know threat actors follow a playbook that repeatedly exploits the same types of security issues, and the following is an examination of just that.

[1] *US Chamber of Commerce, Small Business Index*
[2] *TechTarget, Ivanti vulnerabilities explained: Everything you need to know*
[3] *Volexity, Ivanti Connect Secure VPN Exploitation Goes Global*
[4] *US Senate Committee on Finance, Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group's Response*
[5] *Reuters, UnitedHealth says advanced over $2 bln in payments to providers*

Introduction

The Cyber Threat Index 2025 examines the ransomware playbook along multiple dimensions:

1. Which attack vectors are exploited to gain access to networks and deploy ransomware
2. The most common misconfigurations and vulnerabilities that expose organizations to attack vectors used in ransomware events
3. How businesses should prioritize and remediate these security issues

This report focuses on ransomware because its impact extends far beyond initial victims. Ransomware attacks disrupt supply chains, violate privacy rights, and undermine societal resilience. The cascading impacts of these events have led governments in Europe,[6] the US,[7] Canada,[8] and other regions to declare ransomware a critical national security issue. By sharing actionable intelligence, we aim to equip businesses of all sizes (especially SMBs) with the necessary tools to stay secure and build resilience in a rapidly evolving threat environment.

[6] European Union, EU Statement – UN Security Council: Briefing on Threats Posed by Ransomware Attacks against Hospitals and Other Healthcare
[7] World Economic Forum, US announces National Cybersecurity Strategy
[8] Government of Canada, National Cyber Threat Assessment

SECTION 1

Ransomware Initial Access Vectors

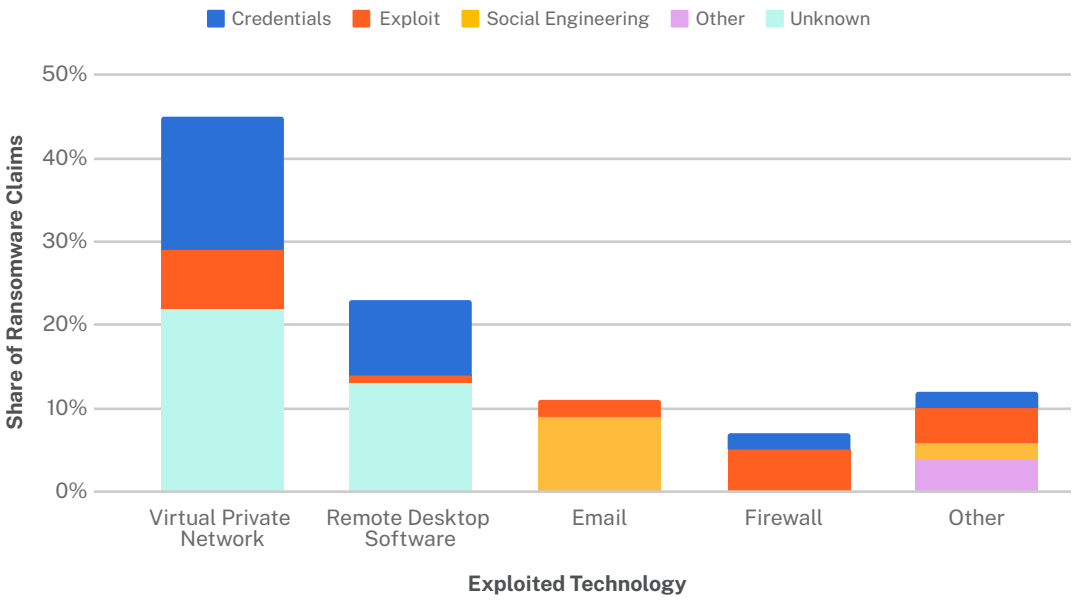
An initial access vector (IAV) describes how threat actors gain access to a network. Coalition analyzed ransomware claims to understand two aspects of the IAV, namely the technology (what was accessed) and the attack vector (how it was compromised).

Technologies exploited in ransomware attacks

Virtual private networks (VPNs) and firewalls were the first and fourth most commonly exploited technologies used for initial access (Figure 1.1). A firewall, for example, controls connections by blocking network addresses associated with malicious activity. Meanwhile, a VPN is designed to provide authenticated users with elevated access to internal systems.

Vendors such as Fortinet®, Cisco®, SonicWall®, and Palo Alto Networks® build the most commonly compromised products, which fall under a more general category of perimeter security appliances. These devices are often built into an organization's physical networking infrastructure, typically offering both VPN and firewall functionality.

Known Initial Access Vectors for Ransomware Claims *(Figure 1.1)*



Remote desktop software was the second-most commonly exploited technology. These products provide a remote user with cursor-level control over a system, which can be useful for IT support to resolve issues without requiring physical access to a PC. However, the same functionality allows threat actors to conduct malicious activity, such as downloading and deploying ransomware code, which was the case in almost a quarter (23%) of the incidents in our sample.

Remote Desktop Protocol (RDP), developed and maintained by Microsoft, was compromised in almost 80% of the incidents in this category. RDP is most commonly enabled using native software built into Microsoft systems, such as via Remote Terminal Services on Windows servers or in the settings of Windows Enterprise and Pro operating systems. The other incidents in this category impacted remote desktop products, like ConnectWise's ScreenConnect and AnyDesk's remote desktop software.

Email was the third-most commonly exploited technology. Microsoft Exchange was the only specific email product mentioned in the forensics investigations. The remaining technologies, including cloud services like Amazon Web Services (AWS), web browsers, and web servers, were less frequently exploited.

Ransomware attack vectors

Compromised credentials were the most common attack vector, representing almost half (47%) of known IAVs in ransomware incidents. Such attacks typically targeted RDP and VPNs,[9] which provide threat actors with privileged access to internal systems and networks.

Investigators observed brute-force password guessing in just under half (42%) of these incidents. This approach was visible in activity logs that show thousands of unsuccessful authentication attempts shortly before compromise.

In contrast, investigators cannot always confidently identify how credentials that were not brute-forced were compromised. When threat actors steal credentials via phishing or infostealing malware, they make a single attempt to log in, just like a legitimate user. Even when brute-force guessing was used, Coalition Incident Response[10] found that VPNs were often not configured with sufficient activity logs to make this determination.

Software exploits were the second-most common known IAV. Exploits typically take advantage of a vulnerable system, ranging in complexity from simple commands that exploit a single vulnerability to advanced espionage software that chains together multiple vulnerabilities.

"Compromised credentials were the most common attack vector, representing almost half (47%) of known IAVs in ransomware incidents."

[9] *Using compromised credentials to exploit email is known as a business email compromise, the most common cyber insurance claim. However, it is not typically monetized by demanding a ransom. Instead, threat actors typically use the inbox to make fraudulent payment requests, or as a launchpad for further compromise.*

[10] *Coalition Incident Response services are provided by Coalition Incident Response, Inc., a wholly owned affiliate of Coalition, Inc.*

Ransomware attacks exploited vulnerabilities in various products: multi-purpose networking devices from Ivanti, Fortinet, and Cisco, Microsoft's Exchange Email Server, and even open-source Linux web servers.

Software exploits are distinct from a malware payload, the software that is installed after initial compromise. For example, the same ransomware payload — the software that encrypts a victim's data — can be installed after gaining access via software exploit or stolen credentials.

Social engineering was the third-most common IAV, typically involving email to communicate with victims. Investigations identified multiple incidents that involved tactics like:

- Manipulating employees into installing remote access technology and providing access to a threat actor
- Tricking employees into clicking a malicious link that installed malware on the device
- Impersonating legitimate software so employees inadvertently installed malware
- Phishing employees into revealing credentials

Notably, all of these attacks exploited the human factor. The remaining attack vectors included attackers exploiting misconfigured AWS environments, using Google advertisements for a drive-by-download attack, and supply chain attacks.

RANSOMWARE OUTLOOK

Studying IAVs reveals clear themes in the ransomware playbook:

- Targeting perimeter security appliances or RDP (58% and 18% of ransomware events)
- Compromising credentials to gain privileged access (47% of known IAVs)
- Using software exploits to deliver malware or extract data (27% of known IAVs)

Businesses with large security budgets might be able to use this information to hire security experts to map these attack vectors to vulnerabilities and misconfigurations in the defender's network. However, many SMBs lack the budget to do so and need guidance on which misconfigurations and vulnerabilities threat actors are exploiting in the wild. We address this problem in the next section.

SECTION 2

Internet-Exposed Logins

To exploit compromised credentials, attackers need access to a login interface. We use the term **exposed logins** to describe a login interface that can be accessed from the open internet.

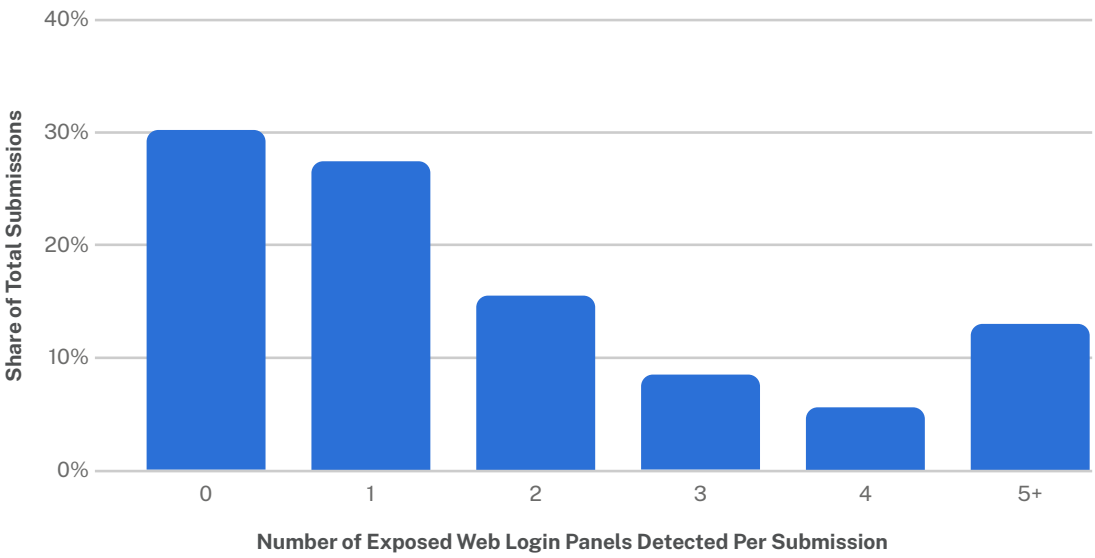
Email is a familiar example of an exposed login. Anyone with an internet connection can navigate to office365.company.com, input stolen credentials, and gain access to sensitive emails. This login can be restricted by only allowing access to users connected to the corporate network, though doing so creates friction for remote workers who would need to connect by VPN to access their email inbox.

Web login interfaces, also known as **panels**, allow employees to access internal systems from a web browser. This might allow the employee to access a VPN, upload identity documents to HR, submit receipts and invoices to finance, and access industry-specific systems, like patient portals in healthcare.

Most businesses (65%+) had at least one internet-exposed web login panel at the time of applying for cyber insurance (Figure 2.1). These panels were identified by an AI system built by Coalition, trained to detect the visual patterns of web login panels.[11] We use the AI system to detect panels on the websites of businesses that submit applications for cyber insurance.

The detected panels span email, VPN, finance, human resources, and more. We detected at least five web panels on 15% of these submissions. Seven businesses were found to have at least 100 exposed web login panels.

Exposed Web Login Panels *(Figure 2.1)*



[11] *To identify the exposed web logins associated with a given company, Coalition built a generalized web panel detection system that uses a list of domains as input, screenshots webpages for subdomains, and runs an image classifier that predicts if the screenshot contains a login page.*

A minority of businesses had no exposed web login panels that could be detected, possibly because access was restricted to connections from the corporate network. Another explanation is that companies with a small digital footprint do not need any login functionality.

Panels are not interchangeable from a security perspective. A threat actor logging into an exposed email inbox is a security compromise — the most common cyber insurance claim, in fact.[12] However, a business email compromise event does not allow a threat actor to deploy ransomware.

Businesses that want to reduce their exposure to ransomware should focus on the riskiest exposed logins. Ransomware events are far more likely to begin with compromised credentials used to access RDP or perimeter security appliances, typically VPNs (see Figure 1.1).

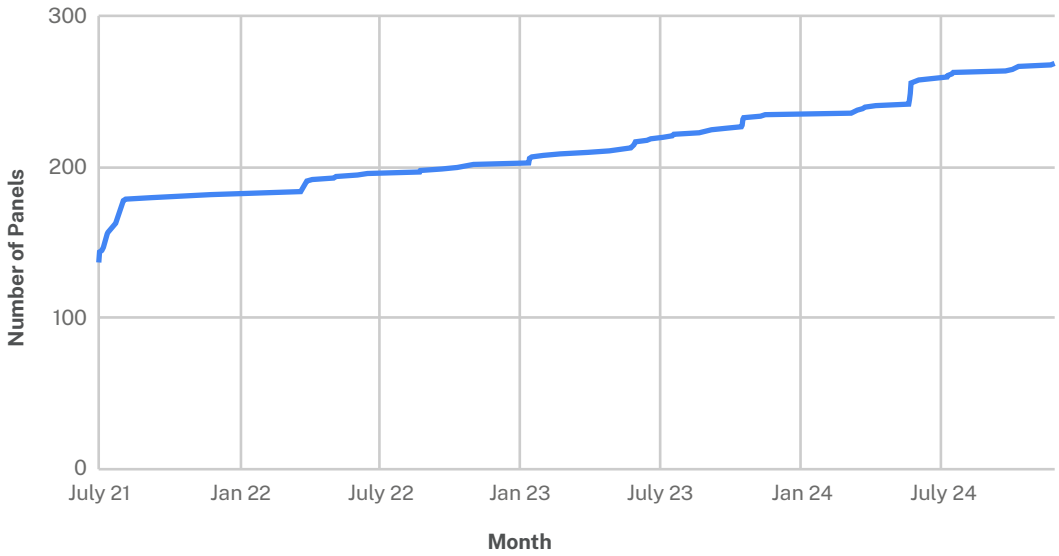
Risky panels

Businesses often use web panels to access and manage perimeter security appliances.

Coalition first started detecting panels in January 2021 and made securing certain panels a requirement for buying cyber insurance in July 2021. In June 2023, the US Cybersecurity and Infrastructure Security Agency (CISA) ordered federal agencies to either remove certain administrative panels from the internet or add additional mitigations.[13]

Since July 2021, Coalition has added 132 more web panel contingencies (Figure 2.2). These panels create risk: Organizations with an exposed web panel were three times more likely to suffer a cyber incident.[14] However, not all panels are the same.

Coalition Web Panel Contingency Rules *(Figure 2.2)*



[12] *Coalition, 2024 Cyber Claims Report: Mid-year Update*
[13] *US Cybersecurity and Infrastructure Security Agency, BOD 23-02: Implementation Guidance for Mitigating the Risk from Internet-Exposed Management Interfaces*
[14] *Coalition, 2024 Cyber Claims Report*

Administrative panels help manage perimeter security appliances by allowing IT administrators, for example, to add firewall rules via a web browser. This is particularly useful to SMBs outsourcing IT management to a third-party provider that does not have local access to devices.

The most common administrative panel was used to manage Microsoft Exchange (Figure 2.3). The three most commonly detected VPN admin panels were associated with products made by Cisco, SonicWall, and Palo Alto Networks — all vendors whose products were exploited as ransomware IAVs.

Using compromised admin credentials to access one of these panels may allow attackers to disable or bypass security features. Coalition typically recommends that policyholders restrict external network access and update the firmware of the underlying device.

Top 10 Panels Detected by Coalition *(Figure 2.3)*

VENDOR	PRODUCT TYPE	SHARE OF PANEL DETECTIONS (%)
Cisco	VPN+	10.1
Sonicwall	VPN	9.1
Microsoft	Email	7.6
PaloAlto Networks	VPN+	6.6
Fortinet	VPN+	6.5
Citrix	VPN	5.7
Citrix	Gateway	5.3
Microsoft	Email Admin	3.7
VMware	Virtual OS	3.5
Open-Source	VPN	3.2

VPN panels are also used to provide employees with VPN access. Web login panels can be used to establish a VPN connection from within a web browser. For example, all of the VPNs in Figure 2.3 can be configured to do so by enabling Secure Sockets Layer (SSL) VPN functionality.

Even when users need to install dedicated VPN software, panels are often used for password management, including credential reset. This functionality is attractive to SMBs that cannot afford to run a 24/7 help desk to help with credential reset. However, it also allows threat actors to test whether credentials bought from the dark web are valid or brute-force guess credentials.

Citrix Panels

Misconfigured Citrix panels caused over $1 billion in losses in 2024, likely more than any single common vulnerability and exposure (CVE). We know this because a single incident resulted in at least $1.6 billion in losses.[15]

Change Healthcare suffered a ransomware incident in February 2024. The CEO's testimony before Congress revealed that attackers gained access via a Citrix web panel with stolen credentials, exploiting the lack of MFA.[16] The threat actor was able to pivot through the network, exfiltrate data, deploy ransomware, and encrypt business systems.

The impact of the resulting outage rippled through the healthcare sector. An estimated 80% of physician groups reported losing revenue from unpaid claims, and 85% had committed additional staff time and resources to complete revenue cycle tasks.[17]

Numerous businesses relied on Change Healthcare to process payments, ranging from hospitals to pharmacies to insurers. The event impacted over 20% of Coalition's healthcare policyholders with more than $100 million in revenue, highlighting how supply-chain incidents can lead to outsized losses.

The Change Healthcare attack was noteworthy for Coalition: not because of losses, but because we had warned about the risks associated with Citrix panels since January 2021. If Change Healthcare had applied for Coalition cyber insurance, we would have issued a Citrix panel contingency — and if it had fixed the issue by enforcing MFA, the US healthcare industry may have avoided the incident altogether.

"Misconfigured Citrix panels caused over $1 billion in losses in 2024, likely more than any single common vulnerability and exposure (CVE)."

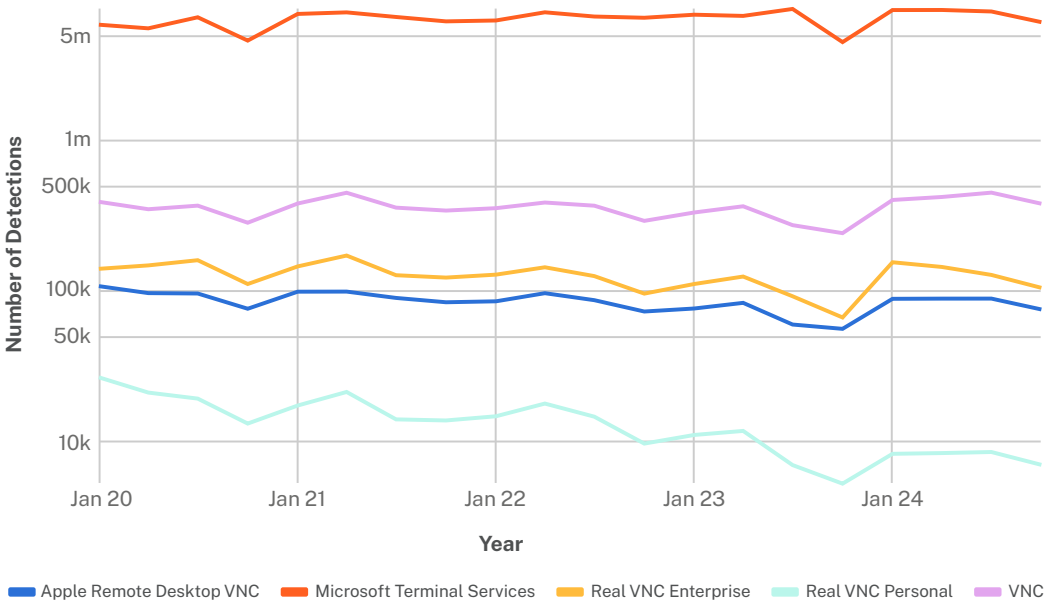
[15] *Cybersecurity Dive, UnitedHealth expects up to $1.6B hit from Change cyberattack this year*
[16] *CSO, Authentication failure blamed for Change Healthcare ransomware attack*
[17] *American Medical Association, Change Healthcare cyberattack*

Remote Desktop Protocol

If a system exposes RDP, then a connection can be initiated from any IP address. A successfully authenticated user can then issue remote commands on the exposed system.

To enable RDP, many organizations use Microsoft's Terminal Services, a component that comes pre-installed in Windows servers. Over 5 million systems expose Microsoft Terminal Services to the internet (Figure 2.4).

Internet-Exposed Remote Management Technologies *(Figure 2.4)*



The simplest way to expose RDP to the internet is to enable traffic through Port 3389 and open RDP, thereby allowing authentication attempts to be submitted from any IP address. This configuration is vulnerable to attackers who scan the internet for exposed RDP, attempting brute-force attacks if RDP is directly exposed.

Given the challenges in implementing MFA in such a setup, many defenders opt to use technologies like RDWeb and Remote Desktop Gateway instead, which make MFA more easily enabled. The latter approach can also require the party initiating the connection to presenta certificate.

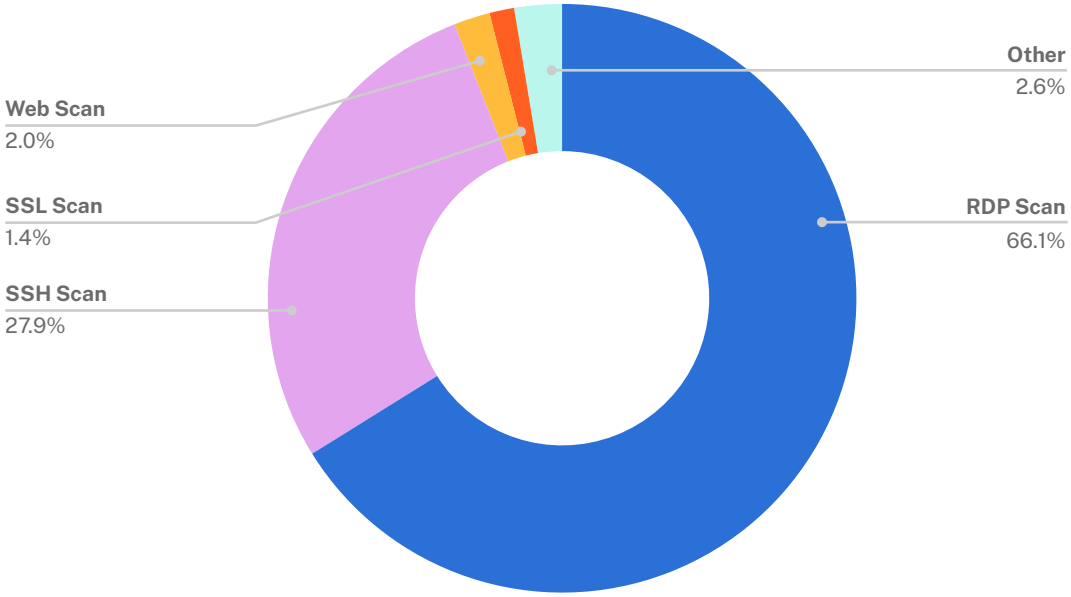
HONEYPOTS

Coalition gathers security insights via a global honeypot network, a collection of fake devices that listen to internet activity. With no legitimate business reason for anyone to connect to our honeypots, we can assume the entities that attempt to connect are collecting reconnaissance about vulnerabilities. A small percentage of these actors (like Coalition) are scanning the internet for defensive purposes, but many more are threat actors seeking targets.

Such security features may appear to mitigate ransomware risk, especially for SMBs that lack security expertise. However, Coalition's experience is that attackers are so determined that these security features are insufficient for the risk associated with RDP.

Attackers' outsized interest in RDP can be seen in honeypot traffic, which is dominated by inbound RDP requests. Scans for RDP represented almost 70% of Coalition honeypot activity in 2024 (Figure 2.5).

Inbound Honeypot Connections by Protocol *(Figure 2.5)*



EXPOSED LOGINS SUMMARY

Internet-exposed logins are an underrated driver of ransomware. We observe:

- Most businesses (65%+) have at least one internet-exposed web login panel.
- Over 5 million systems expose Microsoft Terminal Services to the internet.
- Admin panels used to configure network devices represent one-fifth of the 15 most common exposed risky panels.

This exposure explains how stolen credentials represent 47% of known ransomware initial access vectors.

Logins need to be secured with a risk-based approach. Admin panels and RDP should not be accessible from the open internet. Meanwhile, VPN panels can remain exposed if MFA is enabled and the device's firmware is up-to-date.

SECTION 3

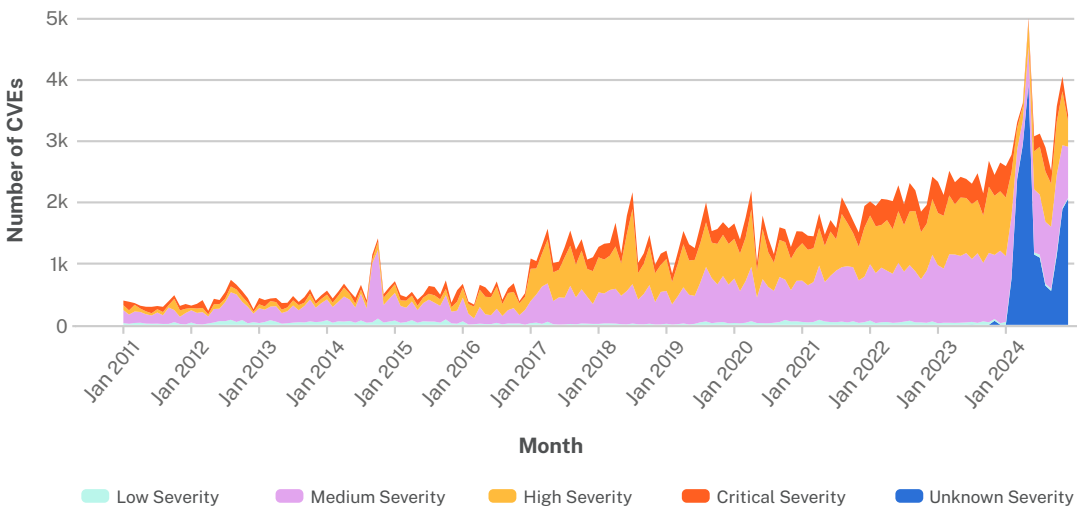
Vulnerabilities

Just over 40,000 vulnerabilities were published in 2024, a 38% increase on 2023.[18] Threat actors were able to choose from over 3,000 new vulnerabilities every month, which helps explain why software exploits were the second-most frequent IAV in Coalition ransomware claims.

Curious developments played out alongside the continued growth in Common Vulnerabilities and Exposures (CVEs) (Figure 3.1). A dramatic spike in vulnerabilities in April and May — over 5,000 vulnerabilities published in May alone — coincided with a breakdown in the system of classification. Most vulnerabilities were classified as "unknown severity," rather than low, medium, high, or critical.

This created a problem for SMBs: Not only were there a record number of vulnerabilities to triage, but the (admittedly flawed) system to enrich the data was disrupted. Despite coinciding, these two phenomena have different causes.

Monthly Volume of CVEs, 2011-2024 *(Figure 3.1)*



The disruption in severity classification results from a political problem. The US National Institute of Standards and Technology (NIST), the federal agency tasked with enrichment, stopped enriching vulnerabilities in February 2024. NIST instead began working to establish a "new consortium" to manage the process.[19]

[18] *Coalition focuses on vulnerabilities published in the National Vulnerability Database (NVD), which collates vulnerabilities impacting all global software and hardware products. New vulnerabilities are assigned a CVE identifier, whether discovered via exploitation in the wild or defensive research. Private repositories exist with additional vulnerabilities, though the most important vulnerabilities are likely to end up in the NVD.*
[19] *Infosecurity Magazine, NIST National Vulnerability Database Disruption Sees CVE Enrichment on Hold*

A new consortium was announced in March,[20] but there was no enrichment for most of the vulnerabilities published in May. As of October 2024, a significant number of unenriched vulnerabilities remained. Yet, the lack of enrichment does not explain the vulnerability surge in May. If anything, the disruption should have prevented vulnerabilities from being added to the National Vulnerability Database (NVD).

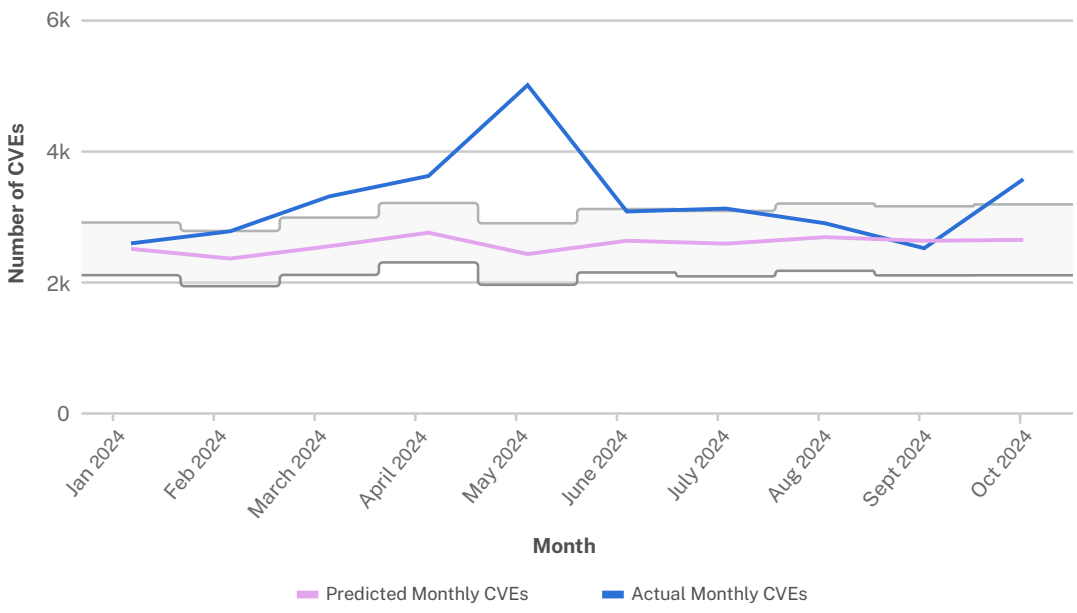
The surge in published vulnerabilities was caused by a handful of CVE Numbering Authorities (CNAs), the software companies and other third parties trusted to maintain the NVD. More and more actors have been given these powers to deal with the increasing volume of software products and, therefore, vulnerabilities. While this has broadly been successful, it has also led to idiosyncratic behavior.

In February 2024, an open-source project, the Linux Kernel, was made a CNA. The project argued that the Linux Kernel — the operating system component that interfaces between hardware and software — was so crucial to security that every bug represented a security vulnerability.

This broad definition resulted in the Linux Kernel issuing over 1,100 vulnerabilities in May.[21] For comparison, only 2,400 vulnerabilities were published in May 2023 across all global software and hardware products.

A similar, though less dramatic, story can be seen with other CNAs. Wordfence issued 474 vulnerabilities in May 2024, compared to 35 in May 2023. Similarly, TrendMicro's Zero Day Initiative issued almost 800 CVEs in May. Together, the vulnerabilities published by three CNAs account for the increase over the number of vulnerabilities Coalition predicted for May in the *Cyber Threat Index 2024* report (Figure 3.2).

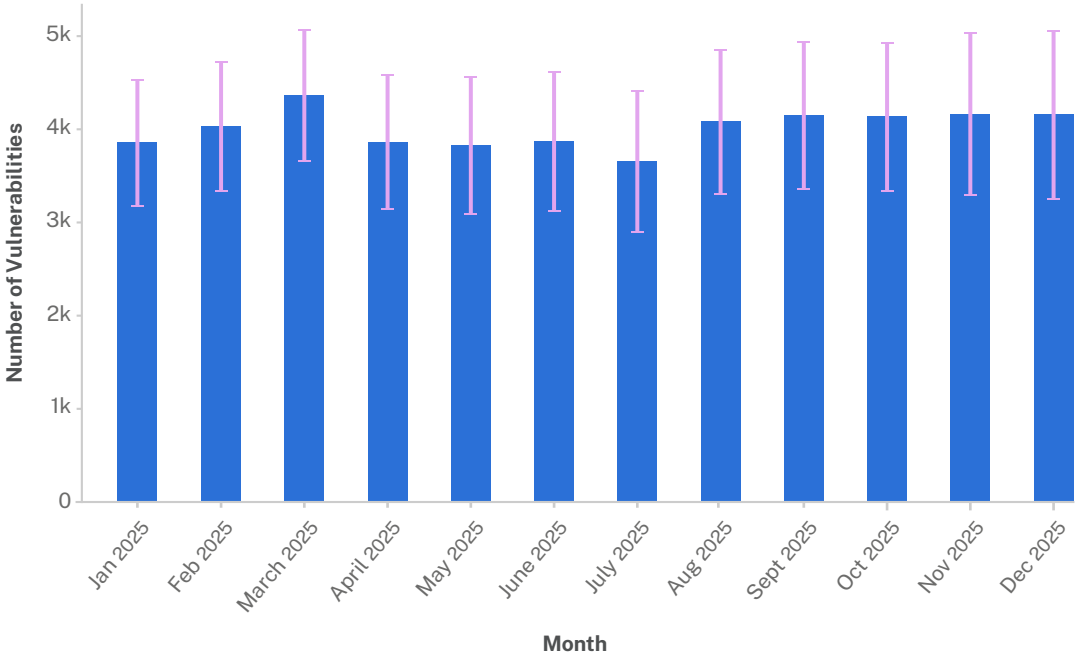
2024 CVEs: Actual vs. Predicted *(Figure 3.2)*



[20] *Infosecurity Magazine, NIST Unveils New Consortium to Operate National Vulnerability Database*
[21] *Risky Biz News: The Linux CNA mess you didn't know about*

Looking forward, Coalition forecasts over 45,000 vulnerabilities in 2025 (Figure 3.3), a 15% increase on the first 10 months of 2024. Notably, the enrichment issues complicate our forecast for 2025 because we do not have 2024 data disaggregated by severity. Regardless of the precise number, thousands of vulnerabilities will be published each month in 2025. SMBs lack both the resources to patch a high number of vulnerabilities — requiring dedicated IT staff and testing infrastructure — as well as the experience to focus on the most pressing vulnerabilities.

Forecasted Vulnerabilities in 2025 *(Figure 3.3)*



"Looking forward, Coalition forecasts over 45,000 vulnerabilities in 2025 (Figure 3.3), a 15% increase on the first 10 months of 2024."

Risky vulnerabilities

In 2024, vulnerabilities with the following characteristics were exploited in various ransomware attacks and should be considered high risk for businesses:

1. Discovered as zero days being exploited in the wild
2. Affecting perimeter security appliances that provide access to sensitive systems
3. Requiring no user interaction or authentication to gain remote code execution, elevate privileges, or extract data

Ivanti

In January 2024, Ivanti announced two vulnerabilities, originally detected by Volexity,[22] as zero days that were being exploited in the wild. This satisfies the first characteristic.

The vulnerabilities affect certain versions of Ivanti's Connect Secure VPN, Neurons zero-trust access, and Policy Secure network access control products.[23] All products are designed to be exposed to the internet, which satisfies the second characteristic.

Attackers combined these two vulnerabilities to install web shells, which enable ongoing access to the compromised devices that could be used to deploy ransomware or extract sensitive data. Exploiting the vulnerabilities did not require authentication or user interaction, thereby satisfying the third characteristic.

These vulnerabilities are so powerful that multiple threat actors were detected exploiting them, including "China-nexus espionage groups" as well as ransomware actors.[24] This led CISA to issue an emergency directive requiring federal agencies to "implement vendor mitigation guidance."[25] However, attackers managed to work around Ivanti's Integrity Checker Tool.

CISA issued another emergency directive to federal agencies, which essentially assumed devices were compromised.[26] The advisory recommended not only patching affected Ivanti products, but also disconnecting the devices from the internet. In the wake of these vulnerabilities, Ivanti's CEO announced a new commitment to security, which involved embracing Secure by Design.[27]

CISA issued another cybersecurity advisory about the same three Ivanti products in January 2025.[28] Ivanti's reporting suggests these new vulnerabilities meet the criteria above.[29] The vulnerabilities allow an unauthenticated, remote attacker to run code on these devices, which allows threat actors to install web shells.[30] However, Ivanti is not unique in announcing these kinds of vulnerabilities.

"These vulnerabilities are so powerful that multiple threat actors were detected exploiting them, including 'China-nexus espionage groups' as well as ransomware actors."

[22] *Volexity, Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN*
[23] *TechTarget, Ivanti vulnerabilities explained: Everything you need to know*
[24] *The Record, Volt Typhoon and 4 other groups targeting US energy and defense sectors through Ivanti bugs*
[25] *US Cybersecurity and Infrastructure Security Agency, Emergency Directive Requiring Federal Agencies to Mitigate Ivanti Connect Secure and Policy Secure Vulnerabilities*
[26] *US Cybersecurity and Infrastructure Security Agency, Supplemental Direction V1: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*
[27] *Ivanti, Our Commitment to Security*
[28] *US Cybersecurity and Infrastructure Security Agency, Ivanti Releases Security Updates for Connect Secure, Policy Secure, and ZTA Gateways*
[29] *Ivanti, Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-0282, CVE-2025-0283)*
[30] *Mandiant, Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation*

Palo Alto Networks

In April 2024, Volexity detected zero-day exploitation of a vulnerability in Palo Alto Networks' Pan OS, upon which various products run.[31] Only firewalls configured to enable remote access via the GlobalProtect gateway or panel were vulnerable. Weaponization allowed remote attackers to run arbitrary code on the device and install a reverse shell, which was used to pivot into the victim's network — an illustrative example of a firewall vulnerability as an initial access vector.

Fortinet

In October 2024, Fortinet announced a vulnerability with "missing authentication for [a] critical function" in FortiManager, a product used by network administrators to manage Fortinet devices.[32] The vulnerability was discovered by Mandiant as a zero day that was being exploited in the wild,[33] allowing remote attackers to send specially crafted commands to remotely install code or extract data, such as "IPs, credentials, and configurations of the managed devices" like VPNs and firewalls.[34]

Citrix

Although the specific CVE identifiers are new, the same kinds of vulnerabilities were exploited in 2023. For example, CISA reported that threat actors were exploiting CVE-2023-3519 to gain unauthenticated remote code execution in Citrix's perimeter security appliances, namely ADC and NetScaler Gateway.[35] This vulnerability allowed attackers to install a web shell in an externally accessible device, then move laterally across the network — a story that should now be familiar.

VULNERABILITY OUTLOOK

The rate at which vulnerabilities are published is accelerating, driven by a mixture of more software products, more threat activity, and also more CNAs that can publish vulnerabilities.

Based on these trends, Coalition anticipates over 45,000 vulnerabilities will be published in 2025, a rate of nearly 4,000 per month. Staying ahead of these vulnerabilities sounds like a daunting task for under-resourced SMBs. However, only a fraction of these vulnerabilities are exploited in the wild. Defenders just need to find the right strategy for focusing on the highest-risk software vulnerabilities.

[31] *Volexity, Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)*
[32] *Fortinet, Missing authentication in fgfmsd*
[33] *Mandiant, Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)*
[34] *National Cyber Security Centre, Exploitation of vulnerability affecting Fortinet FortiManager*
[35] *US Cybersecurity and Infrastructure Security Agency, Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells*

SECTION 4

Outreach

The surge in vulnerabilities in 2024 has underscored the need for speed and efficiency in alerting businesses, particularly SMBs, to emerging cyber threats. While cybersecurity vendors have traditionally handled these alerts, cyber insurance providers are now stepping in proactively, leveraging a deep alignment with risk management and unique threat insights to address the challenge directly.

Effectively managing cyber risk at scale demands sharp cybersecurity expertise, automation-driven processes, and seamless coordination — all while remaining cognizant of alert fatigue and constrained resources. The manual notification methods that once sufficed are now inadequate in keeping businesses informed and protected.

Zero-Day Alerts

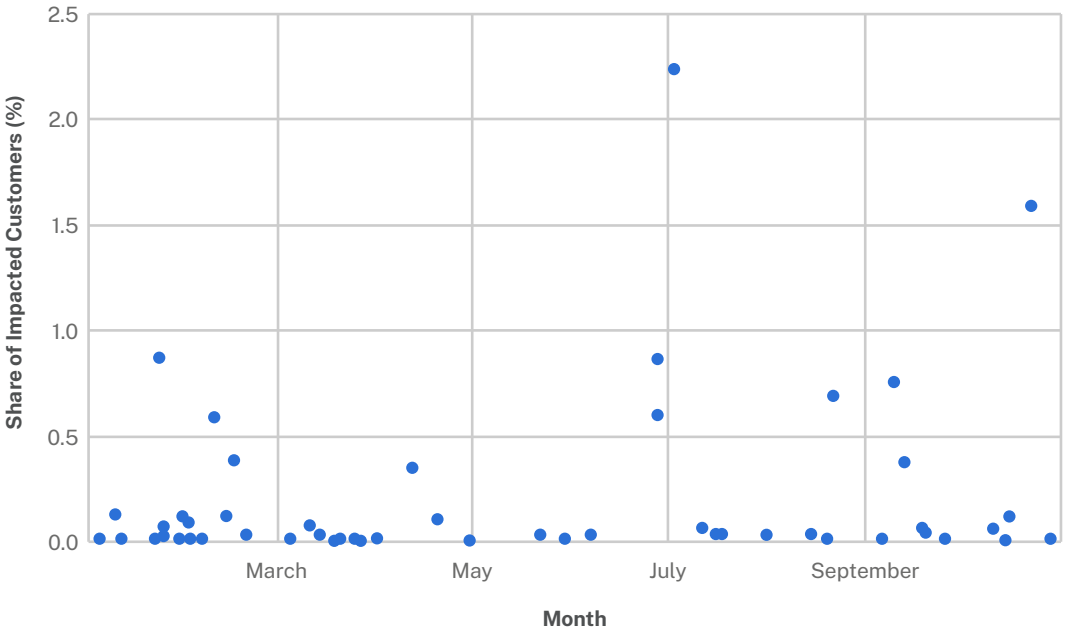
Coalition sends Zero-Day Alerts (ZDAs) when a new vulnerability is discovered and is either actively being exploited by threat actors or exploitation is imminent. Vulnerability discovery and potential exploitation is always a race against time as ransomware gangs try to compromise as many systems as possible before defenders can apply the patch. Such notifications need to be sent immediately.

In such cases, we recommend immediately applying a patch if it is made available by the vendor and is feasible to implement on short notice. If testing is required, then we recommend mitigations like putting the system behind a firewall until the patch can be applied.

However, under-resourced SMBs cannot be expected to immediately mitigate thousands of vulnerabilities announced each month. Sending a notification for all vulnerabilities would inevitably result in notification fatigue. Prioritization means that we sent an average of just 5.5 ZDAs each month in 2024 (Figure 4.1).

"Effectively managing cyber risk at scale demands sharp cybersecurity expertise, automation-driven processes, and seamless coordination — all while remaining cognizant of alert fatigue and constrained resources."

Zero-Day Alerts 2024 *(Figure 4.1)*



To further reduce the decision burden on businesses, we scan policyholders to identify which are affected by each vulnerability. All but two ZDAs had less than 1,000 recipients (Figure 4.1). In fact, the median number of recipients was just 29. Vulnerabilities are often only present on specific versions of a software system and can only be exploited if the system is configured in a certain way.

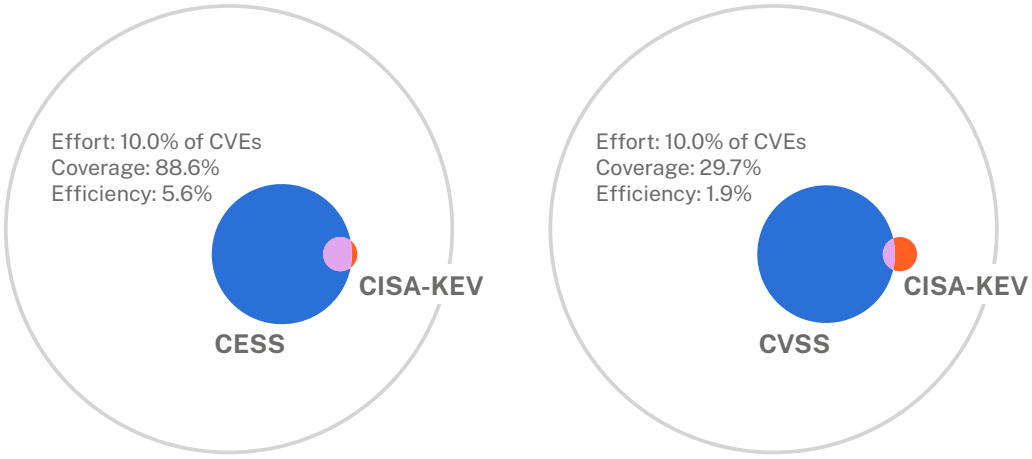
This combination of prioritizing vulnerabilities and paying attention to the details of exploitation means that less than 0.05% of policyholders are notified about the typical ZDA. In fact, the vast majority (over 90%) of policyholders did not receive a single ZDA in 2024.

Coalition keeps the notification burden low by prioritizing high-risk vulnerabilities, a process using a mixture of AI, honeypots, and human judgment. AI and human judgment rely on threat actors following the same playbook, even if the technical details of the vulnerability are different in each ransomware campaign. This typically involves exploiting perimeter security appliances. We trained the Coalition Exploit Scoring System (Coalition ESS) to identify these patterns in the exploitation of vulnerabilities. The model predicts how likely a vulnerability will be exploited based on inherent characteristics and social media chatter.

We use Coalition ESS to triage thousands of potential vulnerabilities released each month that might warrant notification. Then, a human reviews the specific details of a vulnerability to determine whether a notification is necessary.

Comparing our predictions to the Common Vulnerability Scoring System (CVSS) severity from the NVD, Coalition ESS would recommend patching almost 90% of known-exploited vulnerabilities, whereas CVSS would cover less than 30% for the same amount of effort (Figure 4.2). This evaluation assumes CISA can perfectly identify which vulnerabilities we should notify policyholders about.[36]

How Coalition ESS and CVSS Cover CISA KEV *(Figure 4.2)*



Coalition Control® Security Findings

Coalition does not expect all security issues to be addressed as urgently as ZDAs. Acknowledging the trade-off between urgency and notification fatigue, our security findings are displayed in Coalition Control®, our unified cyber risk management platform. We also send a monthly digest email of outstanding issues to policyholders.

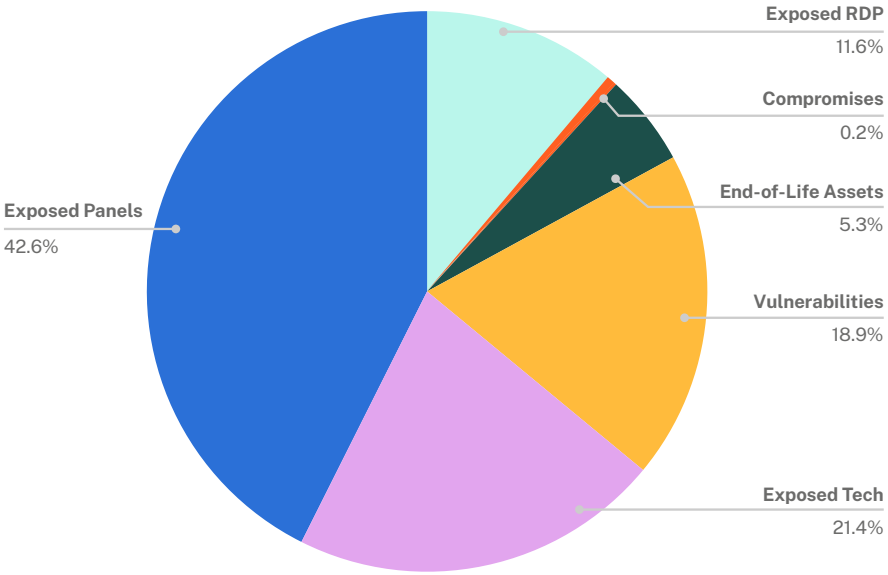
In the first 10 months of 2024, Coalition notified policyholders about tens of thousands of security findings via digest emails. The most common security finding was sent to just under 5% of policyholders. However, the typical issue impacted a small fraction, with just 0.05% of policyholders being notified about the median security issue.

[36] *In reality, CISA's KEV list is not perfect for the purposes of cyber insurance. CISA considers targets that we do not typically insure. For example, CISA cares about vulnerabilities in mobile operating systems that are used by intelligence agencies to target high-value individuals like journalists or politicians. Coalition policyholders are unlikely to be targeted in the same way. CISA's KEV list also captures a binary yes-no on exploitation. Cyber insurance providers are interested in the extent to which a vulnerability is exploited, with mass exploitation by ransomware gangs being far more costly than a single incident.*

Internet-exposed login panels were the most frequent security finding weighted by exposed policyholders (Figure 4.3). Our mitigation advice depends on the type of panel. Admin panels can be used to change configuration settings for network devices, and even to push malicious software out to devices. We recommend removing admin panels from the public internet, by restricting access to pre-approved network addresses.

However, employee VPN panels need to be accessible from the open internet so that employees can log in from random remote locations, such as a foreign hotel's network while traveling. We typically recommend these panels are secured by enabling MFA and updating the firmware of the underlying networking device.

Coalition Control Security Findings in 2024 (Figure 4.3)



Exposed tech is a broad category that covers various products and services that are associated with elevated risk when exposed to the internet. Commonly exposed services include:

- Telnet, an ancient protocol used to administer servers that doesn't use encryption
- Microsoft's Remote Procedure Call (RPC) that bad actors can use to remotely extract credentials and even execute commands on machines in a network
- Open Git repositories, which store software code

Commonly exposed devices include various Fortinet and Ivanti products, along with other perimeter security appliances. While these devices cannot be entirely disconnected from the internet — you can't put the VPN behind the VPN — elevated risk is still associated with login functionality, which creates exposure to stolen credentials. These devices also frequently have high-severity vulnerabilities. CISA regularly issues public notices that attackers are actively exploiting vulnerabilities in such systems.[37]

[37] *US Cybersecurity and Infrastructure Security Agency, Known Exploited Vulnerabilities Catalog*

Exposed RDP is a subset of exposed devices and assets that we break out because it is so high risk. Whereas we accept VPNs can be exposed to the internet if MFA is enabled, we do not recommend RDP should be accessible over the open internet under any circumstances.

Consider that RDP was the IAV in almost one-fifth of ransomware claims, even though we require insurance applicants to remove RDP from the internet. Threat actors are scanning for RDP at such a high cadence that leaving RDP exposed is risky, even for a few hours or days.

Vulnerabilities are the third-most common category of security findings. These so-called "n-day" vulnerabilities have been known to the public for days, sometimes even months and years. In contrast, Coalition ZDAs concern vulnerabilities that were just discovered. Nevertheless, n-day vulnerabilities carry significant risk, not least because threat actors have had time to develop exploit code. We typically advise installing the patch or removing the system from the open internet if a patch cannot be applied.

End-of-life (EOL) systems represent an example of a system where patches cannot be applied. A system reaches EOL when the vendor no longer ships security updates. Despite this, EOL assets represented 3% of our security findings (Figure 4.3). This means organizations are exposing EOL assets, typically Windows Web or Email Servers, to the open internet.

Compromises concerning assets with active malware infections, represented just 0.3% of our security findings in 2024. Our recommendation is to remediate the infection, offering active support if the policyholder cannot do so.

OUTREACH SUMMARY

Security outreach must carefully balance urgency and notification fatigue. When it comes to emerging risks, Coalition issued a ZDA for less than 0.2% of the vulnerabilities published in 2024, with the typical alert sent to around 30 recipients.

Policyholders can use our Coalition Control® platform to track exposure to security risks:

- Exposed panels, services, and devices represent the majority (76%) of security issues, with exposed RDP representing 15% of these
- Unpatched vulnerabilities (19%) and EOL assets (5%) create risk
- Just 0.2% of the issues concerned active infections detected via threat intelligence

SECTION 5

Protecting businesses against the ransomware playbook

Ransomware can have devastating impacts on an individual business, and its impacts can cascade far beyond the initial victim. When aggregated across an economy, ransomware represents a national security problem. Yet, ransomware attacks are rarely innovative. Most incidents follow a playbook that can be studied by defenders — the task of the *Cyber Threat Index 2025*.

Our analysis of ransomware IAVs revealed three main routes:

1. Stolen credentials inputted into exposed login interfaces, mainly VPN panels and RDP
2. Software exploits, typically used to compromise perimeter security appliances
3. Social engineering that takes advantage of poor security awareness

These vectors can also be used to deepen compromise by moving laterally through a network.

The status quo of the software industry leaves under-resourced SMBs with the responsibility to secure their networks. There is no simple way forward, given that businesses cannot remove all login interfaces, software, and internet connectivity. The decision burden will worsen with a forecast of over 45,000 vulnerabilities published in 2025.

Coalition believes greater accountability — with the insurance industry leading the change in forthcoming initiatives — will lead vendors to take more responsibility for securing their software products. However, this structural shift will take time.

In the short term, defenders must focus on the riskiest security issues to reduce the likelihood of a breach. The basic blueprint is:

1. Monitor your attack surface to detect exposed login panels, services, and more
2. Patch emergent zero-day vulnerabilities in internet-facing technology
3. Educate employees about common social engineering tactics
4. Implement 24/7 monitoring of systems and networks, with rapid response procedures

We recognize that SMBs need the most support in doing so, which is why Coalition offers various services to support policyholders with securing their networks.

Coalition Security™

Cyber experts invested in your security

Coalition Security can help protect SMBs from the expanding universe of cyber threats. Our tools and services are built and managed by cybersecurity experts who can help you spot, prevent, and respond to cyber threats before they impact your bottom line.

With unique access to data from real-world risks and 90,000+ global policyholders, we're able to prioritize threats based on potential impact while providing security solutions that are tailored specifically for budget-conscious business leaders.[38]

Coalition Control

Proactively detect, assess, and mitigate threats with a unified cyber risk management platform that continuously monitors your attack surface for hundreds of security issues. Our prioritized action plans and on-demand guidance help you allocate resources where they matter most.

Coalition Security Awareness Training

Boost your employees' cyber knowledge with engaging, cost-effective courses and interactive exercises to deliver memorable training. Improve cyber awareness, educate on compliance best practices, and prevent employees from falling for phishing scams.

Coalition Managed Detection and Response (MDR)

Stop and mitigate attacks with 24/7 endpoint monitoring and unlimited remediation. Our vigilant team of cyber experts leverages industry-leading endpoint detection and response tools to detect signs of compromise and accelerate response on your behalf.

Coalition Incident Response

Access digital forensics and incident response expertise, ready to assist you at the first sign of an incident to limit damage. Available to all Coalition policyholders, our incident response experts respond quickly and decisively and can help you get back up and running fast.

To learn more about Coalition Security, visit coalitioninc.com/security.

[38] *Coalition Security Services, Coalition MDR, and Coalition SAT services are provided by Coalition Incident Response, Inc., a wholly owned affiliate of Coalition, Inc.*

Methodology

The *Cyber Threat Index 2025* includes data from a range of sources collected from January 1, 2024, to October 31, 2024. This includes Coalition's proprietary data from our claims survey, scanning engine, Coalition ESS, honeypots, and notification campaign logs.

Claims survey

Coalition policyholders can receive post-breach support from Coalition Incident Response (CIR)[39] and various external law and digital forensics and incident response firms from Coalition's panel. To improve the claims feedback loop, Coalition asks incident responders to submit details via a survey. The responses filled out for ransomware claims were used to create Figure 1.1.

This analysis faces limitations. Forensics is an imperfect science, even in the physical world. It is even harder in the digital world, where threat actors actively work to destroy evidence, such as by deleting logs. As a result, one-third of the investigations did not confidently identify an IAV. There are also differences between how investigators fill out the survey; some do not include enough detail for a post-hoc determination of the IAV in our analysis.

Scanning the internet

Coalition continuously scans the entire IPv4 space and parts of the IPv6 multiple ports per month. Our scanning engine first starts a round of TCP-SYN scanning across all IP addresses, followed by service identification and protocol enrichment scanning depending on the port or service being scanned. Our scanning infrastructure is geo-distributed across multiple countries and providers and uses custom task distribution and scanning modules built in-house.

Figure 2.4 was created using this "global" scanning data, for which the majority of addresses are not owned by policyholders. However, Coalition policyholders receive a deeper and more frequent scan, which collects additional information, such as panel information, via dedicated modules. This data was used to create Figure 2.1 and Figure 2.3.

[39] *Coalition Incident Response services provided through Coalition's wholly owned affiliate are offered to policyholders as an option via our incident response firm panel.*

Vulnerability scoring

Coalition ESS scores all of the CVEs found in the NVD. The current version uses various features, including CVSS information, vendor and product information, social media chatter, and security advisories. This information was used to create Figures 3.1–3.3 and Figure 4.2.

Honeypots

Coalition has an extensive network of honeypots that are geo-distributed across multiple locations and providers. These sensors act as machines that appear unprotected against multiple known vulnerabilities or appear to be running outdated software and appliances. Running these honeypots gives us an idea of what is being scanned on the internet and how attackers are leveraging and exploiting security concerns, including vulnerabilities, to execute their attacks. This data was used to create Figure 2.5.

Zero-Day Alerts and security findings

Coalition sends security risk notifications to policyholders via various channels. ZDAs are sent as soon as we have detected a business is vulnerable to a high-risk CVE. Logs of our ZDA communications were used to create Figure 4.1. To calculate the percentage of policyholders notified, we divided by the number of policyholders at the end of the observation window rather than normalizing by the number of policyholders at the time the notification was sent. This slightly underestimates estimates early in the observation window.

In addition, Coalition Control sends a monthly digest of unresolved security risks to each policyholder. The security issues identified in this digest were used to create Figure 4.3. Most are detected via scanning engine, although the “compromise” category is detected by ingesting threat intelligence feeds.

Coalition Security™

coalitioninc.com/security

44 MONTGOMERY STREET, SUITE 4210
SAN FRANCISCO, CA 94104