TRAVELERS

Q4 2025 CYBER THREAT REPORT

Attacks on VPNs Help Drive Ransomware Activity to New Highs

Table of Contents

Published by Travelers with contributions from:

Brad Roughan
AVP, Threat Intelligence – Cyber Risk Services, *Travelers*

Josh Doguet
Sr. Manager, Incident Response Intelligence, *Travelers*

Danial Ahmed
Sr. Manager, Cyber Risk Services, *Travelers*

Courtney Hassenfeldt
Cybersecurity Technologist, *Travelers*

John Lippe
Director, Cyber Claim Forensics, *Travelers*

Nicholas Kelley-Ossey
Sr. Director, Cybersecurity, *Travelers*

Alex Pinto
Sr. Director of Product Marketing – Cyber, *Travelers*

Executive Summary

After a slight increase in ransomware activity in Q3, 2025, the fourth quarter of 2025 eclipsed our historical benchmarks with 2,453 victims posted to leak sites, the highest quarterly total we have recorded since we began tracking in 2021. This represents a 48% increase from the previous quarter, as well as (coincidentally) a 48% increase over the same quarter in 2024.

The question we posed earlier this year – whether the ransomware ecosystem would reorganize after being disrupted by law enforcement actions – has been sufficiently answered. Unfortunately, that answer does not favor a lower risk outlook. Not only has the ecosystem reorganized, it has also consolidated around more efficient and aggressive operators, like Qilin, a group we'll take a closer look at in this report.

Meanwhile, the persistent trend of targeting virtual private network (VPN) technology as an attack vector continued from the third quarter. We'll spend much of this report going deeper into this category of technology, why it's become a popular target and how organizations can strengthen the defense of their networks while still allowing for remote access by employees.

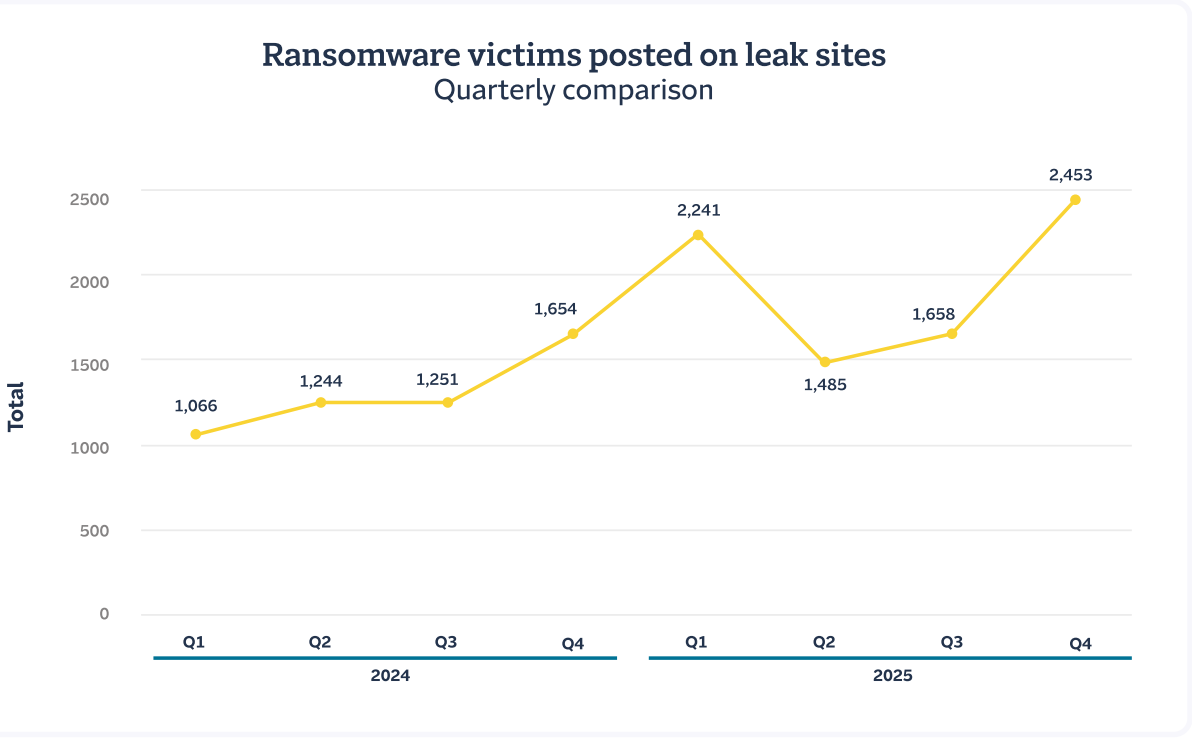
Increase in ransomware activity: 2,453 victims were posted to leak sites in Q4, making it the highest quarter on record and representing a 48% increase over Q3.

Qilin dominates the threat landscape: With 551 victims in Q4, Qilin accounted for 22% of all ransomware attacks and more than doubled its Q3 activity following aggressive affiliate recruitment.

Attacks on VPNs continued: for the second quarter in a row, the major tactical story was attacks on VPN technology, particularly a category known as Secure Sockets Layer (SSL) VPN.

Ransomware Activity Accelerates to New Highs

The fourth quarter of 2025 marked an escalation in ransomware activity, as tracked by victim data posted on leak sites.* With 2,453 victims posted to leak sites, Q4 surpassed the total from the first quarter of 2025 (2,241 victims) to become the most active quarter in our historical dataset going back to 2021. This represents not just a continuation of the upward trend observed over a couple of years, but an acceleration.

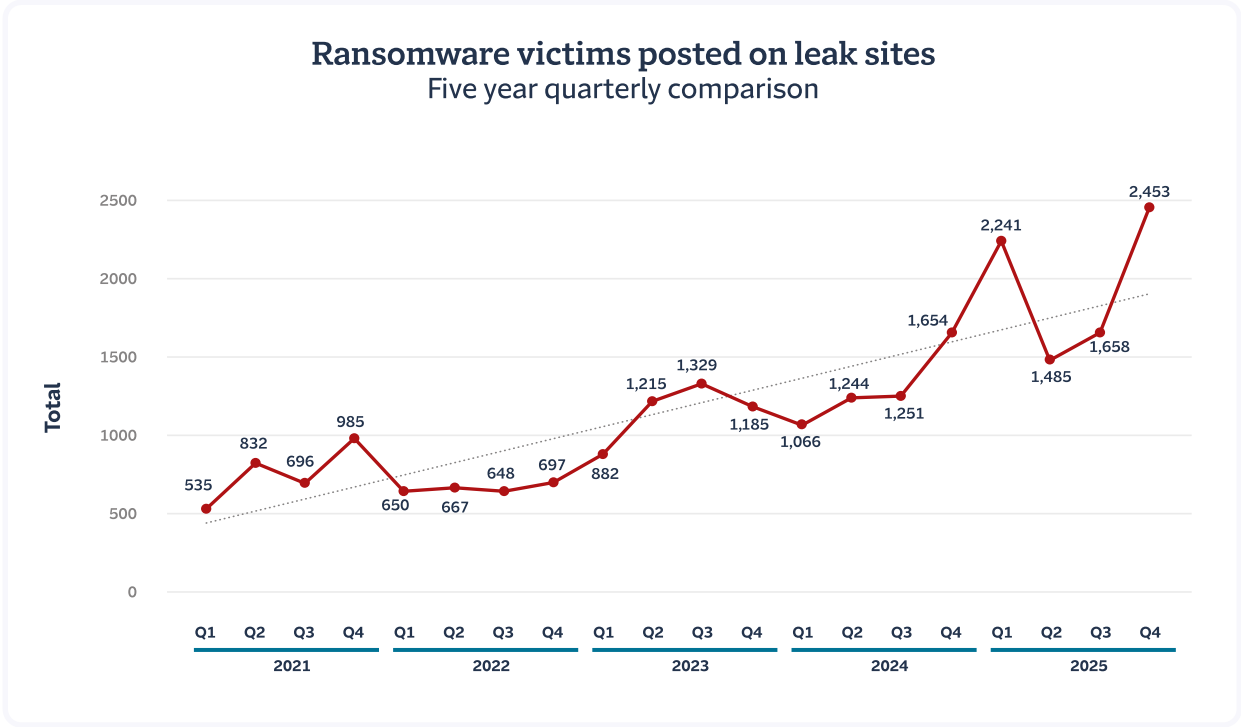


Looking at the full-year 2025 data, we observed 7,837 total victims, a 50% increase over 2024's total of 5,215 victims. This acceleration suggests that the ransomware ecosystem has not only recovered from law enforcement disruptions earlier in the year but has evolved to become more efficient and coordinated in its current incarnation. It also shows that the spike we reported in the first quarter of 2025 was not an aberration, and in fact may end up looking more like an inflection point.

*Data shared on leak sites provides a proxy for overall ransomware activity. A victim's information will typically be posted if the victim has refused to pay a ransom. This means that the data should be viewed as a fraction of overall activity, but one that can provide a longitudinal comparison of activity over longer time frames.

A longer view: ransomware since 2021

With another full year of data available, it's an appropriate time to take a longer view back and compare where we are today. In fact, the addition of data from 2025 gives us a **full five-year view** of ransomware leak site data.



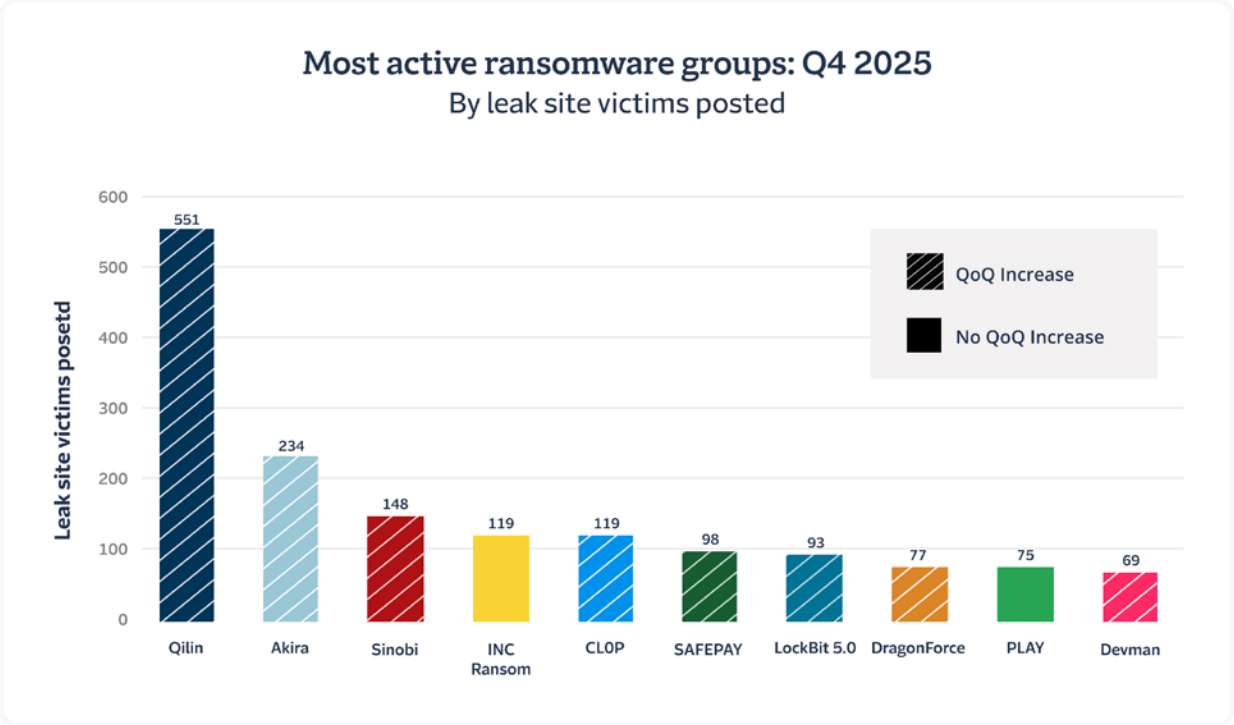
It shouldn't be a surprise to longtime readers that the trend line for ransomware activity has steadily increased over a half-decade span. This has been one of the most frequently referenced storylines in these reports: while there are fluctuations quarter to quarter, the general trend is toward increasing activity.

But with the addition of 2025 data, it doesn't take more than a moment's glance to grasp that something has changed. The figures from Q1 and Q4 2025 were significant departures from the quarters preceding them, to a degree that makes the ebbs and flows of activity in previous years look gradual by comparison.

Not only is the quarter-to-quarter volatility higher – so is the total amount of activity. Looking at the total numbers by year, 2025 saw 50% more victims posted than the previous year, 70% more than 2023, and nearly 3 times more than 2022.

Several threat actor groups drove the spike in activity

Several groups contributed to the rise in activity in Q4, some of which were minimally active – or not active at all – in the previous quarter.



It's typical for threat actor groups to cycle in and out of active patterns. We recently reported, for instance, on the CL0P group's pattern of short but dramatic bursts of activity bookending long periods of dormancy. While CL0P's pattern is one of the more exaggerated examples, it's representative of the fact that some groups will spend extended periods of time surveilling and researching, only re-engaging with active exploits once they've found a promising strategy.

Because of these cycles, we've historically observed that for every group that has an active quarter, another drops off the map. That's how we've ended up with relatively stable quarter-to-quarter activity levels for long stretches of time, like those seen in the five-year view in the previous section. What's notable about this past quarter was that several well-known groups (or the current incarnations of legacy groups) saw increased activity simultaneously. Akira, Sinobi, CL0P and others were significantly more active than they were in the previous quarter.

The biggest increase, though, came from a group that was already at or near the most active all year.

Deep Dive: Qilin Group

The most active group in the quarter was also the one with the largest quarter-over-quarter increase in activity: Qilin.

Security researchers first identified the group that would become Qilin on cybercrime forums in 2022. The group was part of a then-new trend of ransomware-as-a-service (RaaS) operations, where developers provide ransomware tools and infrastructure to "affiliates" who carry out the attacks in exchange for a cut of ransom payments.

As it expanded operations, a distinct feature of the group's attacks was the regular use of double-extortion: both encrypting data (the traditional ransomware tactic) as well as stealing data and threatening to leak it unless ransom is paid. By 2024, Qilin was frequently appearing in our quarterly roundups of the most active leak site operators, though it remained a mid-tier player rather than a high-volume threat.

> A distinct feature of the group's attacks was the regular use of double-extortion: both encrypting data (the traditional ransomware tactic) as well as stealing data and threatening to leak it unless ransom is paid.

2025: Affiliate surge

That changed this year. The dissolution of ransomware-as-a-service group RansomHub (an event you can read about in our Q2 2025 report), left its many ransomware affiliates without a primary RaaS partner. Qilin has proven to be the largest beneficiary of the sudden availability of experienced ransomware groups – even more so than Akira, a group that led a coordinated campaign of attacks in the third quarter of 2025.

Researchers point to several characteristics that led to Qilin's success in recruiting affiliates: the technical attributes of its software, its affiliate-friendly revenue sharing agreements and support capabilities that go beyond just providing software tools. Unfortunately, that success comes at significant expense to legitimate organizations. Last quarter, Qilin posted 551 victims to leak sites. Construction firms and government organizations in the U.S. were its most frequent targets, but the group has also targeted hospitals, health clinics and other nonprofits – the kinds of organizations that some ransomware groups have refrained from targeting in the past. Absent law enforcement action, we don't foresee a slowdown in the activity of this criminal group.

How SSL VPN Became the Leading Attack Vector

Beginning in August 2025, the Akira group launched a coordinated campaign of attacks targeting under-secured access points of VPN solutions being used by organizations to provide remote access to their systems.

At the time of our last report, this had contributed significantly to the overall attack picture for the third quarter, with more than 50% of Travelers' ransomware claims during August and September attributed to attacks on just one SSL VPN technology.

Now, after another three months have passed, the tactic has only gained momentum. It has always been one of the several most common methods of gaining initial access, but after Akira's campaign, other groups, including Qilin, have placed a much heavier focus on SSL VPN as an attack vector.

To learn about how prevalent these attacks have become, our team studied a subset of Travelers cyber claims (those that required incident response efforts) over the past two years.

> We found that from August through the end of 2025, 85% of the claims studied were attributed to VPN exploitation as the initial access vector, and 70% targeted products from a single SSL VPN provider.

We found that from **August through the end of 2025, 85% of the claims studied were attributed to VPN exploitation** as the initial access vector, and **70% targeted products from a single SSL VPN provider.**

Across the full year 2025, the study showed VPNs were used as the method of initial access in 44% of ransomware and system intrusion claims, up from 36% in 2024. When including other types of external remote services, the figure climbs to 52%.

While the study is not a perfect representation of Travelers claims overall, the high degree of concentration around one type of exploit is striking. No other method of initial access exceeds 8% of the total in the past two years.

What makes SSL VPN a target?

To understand why attackers focus on this technology, it helps to understand the differences between how remote access is granted through different technologies and implementations. **If you'd benefit from a quick primer on VPN technology, scroll to the next page for our Briefing on the topic first**. Otherwise, we'll jump into some technical analysis.

SSL VPN solutions are popular because they couple easy access for end users with the flexibility for IT departments to scale up quickly as their companies grow. They allow for less-centralized management of company devices and easier deployment of bring-your-own-device (BYOD) programs. That ease comes at the expense of increased risk, however. While traditional Internet Protocol Security (IPsec) VPN solutions prioritize device-bound and network-level security, the fact that SSL VPN is based on internet protocols means the attack surface is wider: there are simply more ways a malicious actor could potentially gain access or cause damage.

Let's walk through the steps of a few common methods of gaining initial access that reveal the options attackers have in exploiting the technology.

Pre-authorization exploitation:

1. Attacker uses widely available tools to scan the internet for SSL VPN gateways. Attackers will know the hallmarks of gateways that are less likely to be secure.
2. Attacker attempts to exploit a known vulnerability in the software. If the VPN has not been patched, the attacker may be able to remotely execute code that allows for unauthorized access to the network without needing credentials, and in some cases to bypass multifactor authentication (MFA).

Brute-force attack:

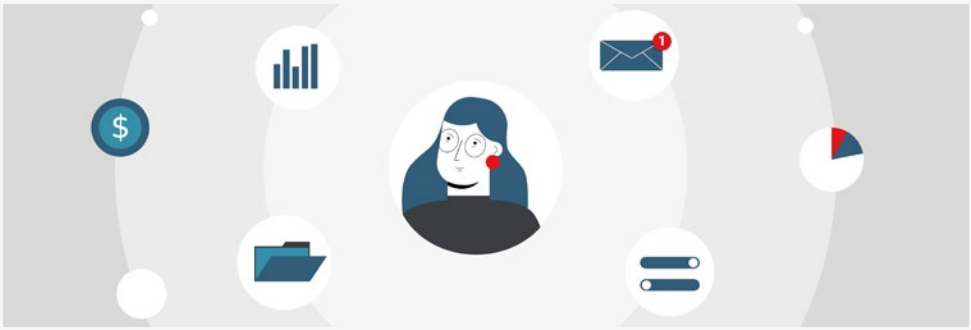
1. Attacker uses widely available tools to scan the internet for SSL VPN gateways. Attackers will know the hallmarks of gateways that are less likely to be secure.
2. If no vulnerability exists to exploit, the attacker can run software that attempts thousands of possible password combinations. It's not uncommon for a VPN endpoint to have default credentials (such as the username "admin") in place.
3. In cases where MFA is enabled on the account, the attacker will attempt to bypass MFA. This may allow them to circumvent some basic MFA implementations (such as delivery of a passcode through a text via SMS).

Credential exploit:

1. Attacker purchases leaked credentials from a dark web marketplace.
2. Attacker locates a VPN gateway likely associated with the credentials.
3. Assuming MFA is enabled on the account, the attacker will deploy a technique to bypass MFA. This may allow them to circumvent some basic MFA implementations (such as delivery of a passcode through a text via SMS).

With any of these initial access attempts completed, the attacker has options. They can likely move laterally within the network. They may attempt to expand their own access by provisioning an account with admin-level permissions. They may seek data to exfiltrate and use in an extortion scheme. They may be able to conceal their activity on the network for a period of days, weeks or even months; or they may deploy ransomware right away.

Note that one of the key elements in each of these attack patterns is the ability for the attacker to locate and access the VPN gateway – something that's made possible by the SSL VPN's nature of being exposed to the internet.



Briefing: How Does a VPN Work?

A VPN is a familiar, everyday piece of technology for millions of workers. And like many of the technologies that underpin corporate IT, its functionality is invisible: at most, end users briefly interact with a login credential interface to begin a session and move on.

Now that VPNs are the focus of sustained cyberattack activity, it's a good time to learn what's *actually happening* behind our screens when we use them. This will help us to better understand the risks VPNs can pose, and what steps are needed to improve security. For that, some definitions are in order.

What is a Virtual Private Network?

Many users know what VPN stands for, but few have to think about what those words mean in the context of this technology. Let's break it down.

- **A VPN is *Virtual***, meaning no physical cables are used in the process of connecting the endpoint (your computer) to the server.
- **A VPN is *Private***, meaning it provides a connection between a device and another device or network that no one else on the internet can see into.
- **A VPN is a *Network***, because whenever you establish a persistent connection from one device to another (or to a collection of devices), this inherently fits the definition of a computer network.

Each part of the acronym is critical to the core functionality offered: It's an encrypted (private) connection allowing your computer to connect (network) from nearly any location, irrespective of proximity to company servers (virtual).

Types of VPNs

Once you go beyond that basic definition, VPN turns into a family of technology solutions rather than a single product. There are three main categories, with sub-categories within each. Understanding their differences is key. The type of VPN used at your organization has much to do with the degree and type of risk your organization is up against in today's threat environment.

1. **A site-to-site VPN** is typically employed by large organizations to enable a persistent private network connection between one physical location and another, such as a headquarters and a branch office.
2. **VPN applications / hosted VPN services** allow a device to connect to a private network through an application that can be downloaded through a web browser or mobile app store. These accessible, low-cost services are marketed to individual consumers as a way of concealing their web activity.
3. **Remote access VPN / client-to-site VPN:** This category blends some of the flexibility of a consumer VPN application with the defined structure of a site-to-site VPN. They are relatively easy to set up at a large scale for an organization, but security is dependent upon the specifics of how that is done. There are two sub-categories.
    A. **Internet Protocol Security VPN (IPSec VPN)** secures data by encrypting and authenticating each piece of that data between two endpoints. Think of this as the traditional VPN solution most organizations have used historically. It requires that an application be configured on the client device, and a piece of networking equipment, such as a firewall, be configured to accept the client connection.
    B. **Secure Socket Layer Virtual Private Network (SSL VPN)** uses web browser-based protocols to create a secure connection that provides remote access to applications or a network. SSL VPNs use Hypertext Transfer Protocol Secure (HTTPS), which is the same technology most websites use. An end user of this type of VPN will often use their normal web browser to navigate to a specific webpage to enter credentials and initiate the SSL VPN connection.

Why are SSL VPNs more often targeted by attackers than other VPN implementations?

SSL VPN solutions (as well as those based on Transport Layer Security, or TLS, which is the successor to SSL – those terms are sometimes used interchangeably in this context) provide ease of access and flexibility, which inherently increases risk. The attack surface is wider on an SSL VPN, meaning there are more ways a malicious actor could potentially gain access or cause damage. Traditional IPsec VPN solutions prioritize strong, device-bound and network-level security, making them more suitable for high-security environments.

Attackers target SSL VPN solutions because they have constant exposure to the internet, meaning they are easy to find with an internet scanning tool – and because organizations often lag in patching them. The attacks typically follow a repeatable playbook rather than exploiting a newly discovered vulnerability, as portrayed in this Travelers video.

It's important to note that SSL VPN solutions are not inherently insecure, but they do face more and different threat vectors in real-world deployments. To secure them properly requires architectural decisions around defense-in-depth, segmentation and aggressive patch management.

5 steps to make remote access less risky

As we noted in our Briefing, SSL VPNs aren't *inherently risky*. It's just that the way they are implemented in the real world – on the internet – introduces an array of factors that increase their attack surface. That's a challenge, but it also means organizations can take steps to reduce risk without overhauling their entire network infrastructure.

That being said, the best practice may be to implement a Zero Trust Network Access (ZTNA) solution, which includes a host of improvements over VPN solutions such as the ability to intelligently assess each incoming request and only allow access to a limited portion of the network as needed.

But a transition to ZTNA isn't realistic for every organization, especially if the organization wants to act quickly in the face of increased VPN attacks. The following are five ways businesses can harden existing SSL VPN usage to reduce the risk of an attack.

1. Harden authentication, going beyond simple MFA

At the authentication stage, organizations must **require MFA on all VPN gateways**, if they do not already. They should also move beyond the simplest MFA implementations, such as the delivery of a passcode through a text (SMS) message to the user's phone, and instead require a more secure version of MFA. An authenticator app or hardware key in place of SMS can prevent some MFA bypass techniques like SIM swapping or certain man-in-the-middle attacks.

Additionally, businesses should consider adding a layer of security by introducing **certificate-based verification** to the MFA process, making it a "third factor" after a password and a one-time code. A practical approach to introducing device certificates involves a user first providing traditional credentials like a username and password, then completing an MFA step (such as using a hardware-based token or an authentication app), and finally, the device itself presenting its certificate to the authentication server for validation.

These measures can significantly reduce the likelihood of unauthorized access in situations where credentials are leaked or brute forced.

2. Introduce RBAC and device assessment

Role-based access control (RBAC) policies enable organizations to get closer to a zero-trust model without fully replacing existing solutions. This means abandoning the widespread practice of granting broad network access to all authenticated users, and instead defining access based on job functions and business requirements. Access does not have to be tailored to each individual – groupings of roles are often sufficient to control access.

For especially sensitive resources, time-based access restrictions can complement an RBAC policy. This might include allowing access to certain resources only during defined business hours and capping sessions with an automatic timeout for idle connections to minimize exposure windows.

Similarly, device posture assessment capabilities should be integrated into the access workflow, automatically verifying that connecting devices meet established security baselines before granting network access. This includes validation of operating system patch levels, antivirus status and disk encryption compliance.

For contractor and third-party access scenarios, organizations should establish separate VPN pools with enhanced restrictions and time-limited account provisioning.

3. Enhance network architecture

Upgrading VPN security can also include a network segmentation strategy that isolates VPN users on a dedicated network (known as a virtual local access network or VLAN) with strict firewall rules governing lateral movement. On top of broad segmentation into VLANs, additional micro-segmentation policies can create barriers between network resources, preventing compromised VPN sessions from escalating. This architectural approach ensures that even if a threat actor gains initial access, they would have limited opportunities to expand their foothold within the organization's infrastructure.

4. Monitoring, maintenance and strategic evolution

Comprehensive logging and monitoring frameworks form the foundation of effective VPN security operations. The key, though, is integrating that data with a Security Information and Event Management (SIEM) platform to enable real-time threat detection and response.

With this arrangement, organizations can implement automated alerting for things like geographic anomalies, unusual access patterns and failed authentication attempts, while maintaining logs to support incident investigations and compliance requirements. Regular security assessments, including annual external penetration tests and quarterly internal reviews, ensure that VPN configurations remain aligned.

A key element of these regular reviews is patching. As we've seen with the recent campaigns targeting unpatched VPNs, there's a significant gap in patch management at many organizations. (Some of the vulnerabilities exploited recently had been announced, along with a patch, a full year earlier.)

A patch management process should prioritize VPN infrastructure. The process should require that critical security updates be applied within 72 hours of release, and businesses should implement monthly maintenance cycles to address non-critical vulnerabilities.

5. Upgrade

Even if replacing an existing SSL VPN solution is not feasible to do quickly, it should be on the longer-term roadmap. Organizations should evaluate modern security-focused VPN providers that offer advanced integration capabilities with contemporary authentication and monitoring tools. For new deployments or infrastructure modernization initiatives, ZTNA solutions should be strongly considered, as they provide application-level access control, enhanced visibility, cloud-native scalability and a fundamentally reduced attack surface compared to traditional VPN architectures.

Impact Alerts: Q4 2025

A selection of vulnerabilities gathered by the Travelers Threat Intelligence team. Travelers issued Threat Alerts to policyholders directly impacted by these vulnerabilities.

A vulnerability in Oracle E-Business Suite, CVE-2025-61882, was heavily exploited in October 2025 and led to widespread extortion events. Exploitation started as early as August 2025, and an emergency patch was issued by Oracle on October 4. The group primarily seen targeting this exploit was CL0P. Exploitation of this vulnerability is in line with previous CL0P activity of widespread exploitation prior to public disclosure of the vulnerability.

Also in October, an unauthenticated remote code execution vulnerability was identified in Microsoft's Windows Server Update Services (WSUS) and recorded as CVE-2025-59287. Researchers identified active exploitation day of release. While specific threat actors have not been identified publicly, reports show that the vulnerability was exploited by ransomware groups and advanced threat actors. The time frame in which this was exploited underscores the importance of staying on top of threats and having the ability to patch quickly in serious cases.

A vulnerability in WatchGuard Firebox was identified on December 19 and recorded as CVE-2025-14733. The vulnerability can allow a remote unauthenticated attacker to execute arbitrary code. VPN devices continue to be prime targets for threat actors, in this case researchers identified over 100,000 exposed and unpatched devices two days after the vulnerability was released. The vulnerability was identified as being actively exploited at time of release.

A vulnerability in MongoDB referred to as "MongoBleed" was released on December 28 and tracked as CVE-2025-14847. It is a vulnerability that allows unauthenticated remote attackers to read "uninitialized server memory, potentially leaking database credentials, API keys, session tokens and sensitive personal data." The vulnerability was identified as being actively exploited soon after release, but the details of the actors exploiting have not been publicly reported.

Conclusion

The results from the fourth quarter of 2025 demonstrate that the ransomware ecosystem has evolved to be more efficient and coordinated than it was prior to recent law enforcement action. With 2,453 victims posted to leak sites – the highest quarterly total on record – and aggressive groups like Qilin having recruited skilled affiliate groups to carry out attacks with its tools, the risk outlook remains elevated.

Aside from following general security practices like those shown below, organizations should be especially focused on securing their remote access technologies, like VPNs. With such a large share of recent attacks focusing on these technologies as a vector for access to systems, organizations should strongly consider shifting to a ZTNA solution for remote access, and in the meantime take steps to secure existing VPNs.

Recommendations from the Travelers Cyber Risk Services Team

To mitigate these risks, organizations should adopt a strong cyber prevention program, including the following recommendations detailing the top security investments with the greatest return on investment.

These recommendations will help increase the bar required for ransomware actors to successfully carry out an attack on an organization.

They include:

- Implement phishing-resistant MFA for all remote access and email.
- Run an effective vulnerability management program to quickly patch critical vulnerabilities in edge devices, such as virtual private networks (VPNs).
- Ensure you have reliable backups and have a resilient disaster recovery and business continuity plan.
- Run endpoint detection and response (EDR) solutions with 24x7 active monitoring.

travelers.com

One Tower Square
Hartford, CT 06183

Travelers analysis was made possible with supporting data from eCrime.ch.