

EXECUTIVE PAPER · INFRASTRUCTURE

Your VPN Appliance Is the Front Door

Firewalls, VPN gateways and file transfer servers have become the most exploited way into a company. Executives should run them as the highest-risk systems they own, with a patch clock, a watch on them, a retirement date, and a plan to replace remote access.

AUTHOR

Chris Watkins

SERVICE

Infrastructure

FOR

CEO, CFO, CTO, Board · 12 min read

AT A GLANCE

The problem. Verizon's 2025 breach report found that flaws in edge devices and VPNs made up 22% of the vulnerabilities exploited in breaches, up from 3% a year earlier. Mandiant found that the four vulnerabilities attackers exploited most in 2024 were all in edge devices, and three of them were attacked before a fix existed.

Why it persists. These boxes are bought as network equipment and run by small teams on maintenance windows. They cannot host the endpoint security software that protects servers and laptops, they keep few logs, and attackers have shown they can survive a patch or a reboot on them.

The recommendation. Keep a named inventory of every internet-facing device. Patch exploited flaws on them within 72 hours and hunt for compromise after every emergency fix. Send their logs somewhere they cannot be erased. Retire units that no longer receive updates. Set a dated plan to move remote access from appliance VPNs to access granted per user, per device and per application.

The Decision in Front of You

Every company that lets staff, contractors or partners connect from outside runs a few devices that sit on the internet and decide who gets in. They are VPN gateways, firewalls, load balancers, remote desktop gateways and managed file transfer servers. Most were bought as plumbing. Many are patched quarterly, if a change window opens.

The decision is whether to keep treating them as plumbing or to run them as the highest-risk systems you own. That means a patch clock measured in days, monitoring that assumes they will be breached, a retirement date for each unit, and a funded plan to reduce how much of the business sits behind a single appliance.

The stakes are concrete. When CISA ordered U.S. federal agencies to disconnect Ivanti VPN appliances in February 2024, the order gave them about two days, and reconnection required a factory reset, a rebuild and a reset of every credential the device had touched [8]. A company that faces the same event without a plan loses remote access for its workforce while the rebuild happens.

What's Happening

The edge became the main target

Verizon's 2025 Data Breach Investigations Report, covering November 2023 to October 2024 and about 12,200 confirmed breaches, found that edge devices and VPNs accounted for 22% of exploited vulnerabilities, against 3% in the prior period [3]. Organizations fully fixed only 54% of those edge flaws, with a median of 32 days to do it [3].

Mandiant's M-Trends 2025 reported exploits as the top way into networks in 2024, at about one intrusion in three [4]. The four vulnerabilities exploited most often were Palo Alto Networks' GlobalProtect flaw CVE-2024-3400, two Ivanti Connect Secure flaws, and a Fortinet management server flaw, all in edge devices [4]. Mandiant noted that three of the four were first exploited as zero-days, and that edge devices usually cannot run endpoint detection software, so intrusions through them go unseen [4].

The traffic data agrees. GreyNoise recorded 2.97 billion sessions against its sensors in the second half of 2025 and counted 16.7 million aimed at Palo Alto GlobalProtect alone [5]. More than half of the remote code execution attempts came from addresses it had never seen before, which defeats blocklists built on yesterday's attackers [5].

In February 2025 the cyber agencies of the United States, United Kingdom, Canada, Australia and New Zealand issued joint guidance on edge devices, one set for executives and one for practitioners, plus a specification telling manufacturers what logs their devices must keep [1][2].

Five cases from 2024 and 2025

Palo Alto PAN-OS, April 2024. Palo Alto disclosed CVE-2024-3400 on April 12, 2024, a command injection flaw in the GlobalProtect VPN feature rated 10.0, the maximum severity, that let an unauthenticated attacker run code as root on the firewall [6]. Exploitation dated back to at least March 26, and hotfixes arrived on April 14 [6][7]. The attacker copied firewall configuration files to a web folder and downloaded them, and planted a scheduled task to fetch further commands every minute [6]. For about two weeks the only defense was a mitigation, and the firewall itself was the compromised system.

Ivanti Connect Secure and MITRE, 2024 and 2025. In January 2024 a nation-state actor exploited two Ivanti Connect Secure zero-days, hijacked sessions to get past multi-factor authentication, and moved from MITRE's research network into its VMware infrastructure [9][10]. MITRE, which maintains the ATT&CK framework that defenders use to describe attacks, published the intrusion so others would understand that a mature security program can still be breached through its VPN [10]. CISA's directive for agencies required disconnection, factory reset, rebuild and credential rotation before any Ivanti device returned to service [8]. A year later, on January 8, 2025, Ivanti disclosed another unauthenticated remote code execution flaw in the same product line, already exploited [11]. The lesson is that one product can produce repeated emergencies, and each one costs a rebuild.

Cisco ASA, September 2025. CISA's Emergency Directive 25-03 ordered federal agencies to collect forensic data from Cisco ASA firewalls, patch them, and permanently disconnect any whose support ended by September 30, 2025 [12]. The attacker, linked by Cisco to the ArcaneDoor campaign first seen in 2024, modified the device's read-only memory so the implant survived reboots and software upgrades [12]. CISA's April 2026 update states that patching does not necessarily remove an attacker and that some models need a full power-off reset [12].

CitrixBleed 2, June and July 2025. CVE-2025-5777 let an unauthenticated attacker read memory from Citrix NetScaler gateways, and public exploits showed it could steal session tokens [13]. GreyNoise saw targeted exploitation from June 23, almost two weeks before public exploit code appeared on July 4 [14]. CISA added it to its Known Exploited Vulnerabilities catalog on July 10 and gave agencies one day to fix it [13]. On July 17 the Dutch Public Prosecution Service disconnected its internal systems from the internet after a warning from the national cyber center about Citrix vulnerabilities. Six days later the justice minister told parliament the service was still offline, staff could log in only at office locations and had no email, and parts could stay offline for weeks [15]. The national cyber center urged every NetScaler customer to investigate for misuse even after updating [15].

Fortinet FortiGate, April 2025. Fortinet disclosed that attackers who had exploited older FortiOS flaws left a symbolic link in a file system area that updates do not clear, keeping read-only access to patched devices [16]. The Shadowserver Foundation counted more than 14,000 affected devices [16].

The pattern is older than these cases. In 2023 the Cl0p group exploited a flaw in the MOVEit file transfer product, and by June 2024 Emsisoft counted 2,773 organizations and about 95.8 million individuals affected [17].

SIDEBAR: WHY A PATCH DOES NOT END THE INCIDENT

In three of the cases above, a fixed device could still be compromised: Cisco's implant in read-only memory, Fortinet's symbolic link, and Citrix session tokens stolen before the patch [12][15][16]. CISA's Ivanti instructions required a factory reset and new credentials for this reason [8]. Treat every emergency patch on an edge device as the start of an investigation.

Why the Usual Approach Fails

Edge devices sit between two teams. The network team owns the hardware and treats firmware updates as change-controlled events that need downtime. The security team owns vulnerability scanning and usually sees servers and laptops first. Neither owns the question of whether the VPN gateway has been compromised.

The tools that protect the rest of the estate do not reach these boxes. They run closed operating systems from the vendor. Endpoint detection agents cannot be installed, so the most capable monitoring a company owns is blind to them [4]. Local logs are small, rotate quickly, and are the first

thing an attacker on the device can alter.

Patching on a monthly or quarterly cycle misses the attack window. Verizon's median of 32 days to fix edge flaws compares with attackers who started before disclosure in the Palo Alto, Ivanti and Citrix cases [3][6][11][14].

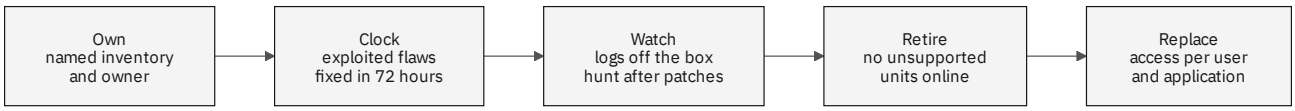
Unsupported units stay in service because they still pass traffic. CISA's February 2026 directive BOD 26-02 states that unsupported edge devices face exploits for newly found flaws that will never be fixed, and cites widespread campaigns against them [18].

Finally, the VPN model itself grants broad access. A traditional VPN puts the remote user on the internal network, so a stolen session or a compromised gateway reaches far more than one application. CISA, the FBI and partner agencies said in 2024 that VPNs are prone to vulnerabilities and misconfiguration, and urged organizations to move toward zero trust designs that grant access per application [19].

The Framework: Own, Clock, Watch, Retire, Replace

Run the edge as a separate control with five parts. Each has an owner and a number that leadership sees monthly.

Exhibit 1. Five controls for internet-facing devices, each with an owner and a measure



Source: author's framework, drawing on the Five Eyes edge device guidance [1][2], CISA ED 25-03 and BOD 26-02 [12][18], and CISA network access guidance [19].

Own. List every device reachable from the internet: model, software version, end-of-support date, the business services behind it, and a named owner. Include devices that vendors or managed service providers run for you. BOD 26-02 gives federal agencies three months for their first inventory and requires continuous discovery within two years [18].

Clock. Subscribe to the vendor's advisories and to CISA's Known Exploited Vulnerabilities catalog, which lists flaws confirmed as attacked [20]. When an edge device's flaw appears there, the fix or the vendor's mitigation goes in within 72 hours, outside the normal change calendar. CISA gave agencies one day for CitrixBleed 2 and 48 hours for later Cisco firewall updates [12][13]. Pre-approve the emergency change so nobody waits for a meeting.

Watch. Send device logs to a system the device cannot alter, and alert on new administrator accounts, configuration exports and logins from unusual places. After every emergency patch, run the vendor's integrity tool, look for indicators the advisories list, and revoke active sessions. The Five Eyes guidance asks manufacturers for forensic logging for this reason [2].

Retire. Any device past its end-of-support date comes off the internet on a dated plan. BOD 26-02 gives agencies 12 months to remove devices already unsupported and 18 months to replace all identified ones [18]. A private company can use the same deadlines.

Replace. Write a two- to three-year plan to move remote access from appliance VPNs to identity-based access, often sold as zero trust network access or secure service edge. Users then reach one application at a time after the system checks who they are and the state of their device [19].

What the patch clock buys

Exhibit 2. Shortening the patch window cuts known-exploited exposure by about 90%

Measure	Typical practice	With a 72-hour clock
Exploited edge flaws per year (assumed)	6	6
Days from fix release to install	32 (Verizon 2025 median [3])	3
Days exposed to a known, exploited flaw per year	192	18
Hunt for compromise after each patch	Rarely	Every time

Source: author's illustrative estimate. Assumes six exploited flaws a year across the edge estate, each patched after the stated delay, with exposure counted from fix release. Zero-day exposure before a fix exists is not reduced by patching speed, which is why the Watch control follows every patch.

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of running the edge as a top-risk control

Area	Cost or risk	Mitigation
Emergency patching	Out-of-hours work and brief outages of remote access	Run gateways in pairs so one can be patched while the other carries traffic
Log collection	Storage and analyst time for high-volume firewall logs	Keep authentication and administration events in full; sample traffic logs
Hardware refresh	Replacing unsupported units is capital spend that buys no new feature	Price it against a forced rebuild under a directive like ED 24-01 [8]
Identity-based access	Licenses, application onboarding, and a migration of one to three years	Move contractors and high-risk applications first; keep a small VPN for legacy protocols
Vendor concentration	A new access platform becomes the next critical dependency	Require the provider's logs, test its outage plan, and keep emergency access paths
When this is wrong	A small business with no internet-facing devices, running on SaaS with single sign-on and device checks, has little edge to manage	Put the effort into identity controls and the SaaS provider's security settings

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap for the edge

Window	Actions	Owner	Milestone
First 30 days	Inventory every internet-facing device with version, support date and owner. Check each against the KEV catalog. Pre-approve emergency changes for edge devices.	CIO with network lead	Inventory signed off; zero KEV-listed flaws open on edge devices; emergency change process published
First 90 days	Forward edge logs to a central system with alerts on admin and configuration events. Write a post-patch hunt checklist per vendor. Pair single gateways.	Security operations lead	100% of edge devices logging off-box; first hunt run within 72 hours of an advisory
First 90 days	List every unsupported unit and set a removal date. Choose the remote access target design and first user group.	CTO with procurement	Retirement schedule approved and funded; access design decision recorded
First 365 days	Remove all unsupported edge units. Move contractors and the most sensitive applications to identity-based access. Report edge metrics monthly.	CTO with CISO	Zero unsupported devices online; exploited edge flaws fixed within 72 hours 95% of the time; first user groups off the VPN

Source: author's recommendation, timelines informed by CISA BOD 26-02 [18].

SIDEBAR: RANSOMWARE THROUGH THE VPN

In July 2025 Arctic Wolf reported a surge of Akira ransomware intrusions that began with logins to SonicWall SSL VPNs, some on fully patched devices, with a short interval between VPN access and encryption [21]. Researchers advised considering disabling the VPN service until the cause was known [21]. A company that can switch remote users to another access path for a week has an option that a single-gateway company lacks.

Questions to Ask Your Team

1. How many devices do we expose to the internet, who owns each one, and when does vendor support end?
2. How long did we take to patch our edge devices after each of the last three emergency advisories?
3. After we patched, did anyone check whether the device had already been compromised?
4. Where do our firewall and VPN logs go, and could an attacker on the device delete them?
5. Which of our edge units are past end of support, and what is the removal date for each?

6. If we had to disconnect our VPN for a week, how would staff and contractors work?
7. What share of our remote users could reach their applications without being placed on the internal network?

Closing

Attackers now come in through the devices built to keep them out, often before a fix exists, and sometimes stay after it is installed. Run your VPN gateways, firewalls and file transfer servers as the highest-risk systems you own. Give each one an owner, patch exploited flaws within 72 hours, hunt after every emergency fix, keep logs off the box, and remove units that no longer receive updates. Then fund the move to identity-based access so the next gateway flaw opens one application instead of the whole network.

Sources

[1] Cybersecurity and Infrastructure Security Agency. "CISA and Partners ASD's ACSC, CCCS, NCSC-UK, and Other International and US Organizations Release Guidance on Edge Devices." Alert. 2025. https://cisa.gov/news-events/alerts/2025/02/04/cisa-partners-asds-acsc-cccs-ncsc-uk-and-other-international-and-us-organizations-release-guidance.

[2] National Cyber Security Centre (New Zealand). "Joint guidance: Security for edge devices." 2025. https://www.ncsc.govt.nz/protect-your-organisation/joint-guidance-security-for-edge-devices/.

[3] Tenable. "Cybersecurity Snapshot: Verizon DBIR: Zero-Day Vulnerability Exploits Surge, VPN and Edge Devices Targeted." Coverage of the Verizon 2025 Data Breach Investigations Report. 2025. https://www.tenable.com/blog/cybersecurity-snapshot-verizon-dbir-zeroday-vulnerability-exploits-surge-vpn-edge-device-04-25-2025.

[4] CyberScoop. "Mandiant M-Trends 2025." Coverage of Mandiant's M-Trends 2025 report. 2025. https://cyberscoop.com/mandiant-m-trends-2025/.

[5] GreyNoise Intelligence. "2026 GreyNoise State of the Edge Report: Where Attacks Concentrate, Defenses Fall Short." 2026. https://www.greynoise.io/blog/2026-greynoise-state-of-the-edge-report-where-attacks-concentrate-defenses-fall-short.

[6] Palo Alto Networks Unit 42. "Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400." 2024. https://unit42.paloaltonetworks.com/cve-2024-3400/.

[7] The Hacker News. "Hackers Deploy Python Backdoor in Palo Alto Zero-Day Attack." 2024. https://thehackernews.com/2024/04/hackers-deploy-python-backdoor-in-palo.html.

[8] Cybersecurity and Infrastructure Security Agency. "Supplemental Direction V1: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities." 2024. https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure.

[9] Help Net Security. "MITRE breached by nation-state threat actor via Ivanti zero-days." 2024. https://www.helpnetsecurity.com/2024/04/22/mitre-breached/.

[10] Crumpton, L., and Clancy, C. (MITRE). "Advanced Cyber Threats Impact Even the Most Prepared." 2024. https://medium.com/mitre-engenuity/advanced-cyber-threats-impact-even-the-most-prepared-56444e980dc8.

[11] Rapid7. "CVE-2025-0282: Ivanti Connect Secure zero-day exploited in the wild." 2025. https://www.rapid7.com/blog/post/2025/01/08/etr-cve-2025-0282-ivanti-connect-secure-zero-day-exploited-in-the-wild/.

[12] Cybersecurity and Infrastructure Security Agency. "ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices." Emergency Directive 25-03, as updated by V1. 2025, 2026. https://cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices.

[13] BleepingComputer. "CISA tags Citrix Bleed 2 as exploited, gives agencies a day to patch." 2025. https://www.bleepingcomputer.com/news/security/cisa-tags-citrix-bleed-2-as-exploited-gives-agencies-a-day-to-patch/.

[14] GreyNoise Intelligence. "Exploitation of CitrixBleed 2 (CVE-2025-5777) Before Public PoC." 2025. https://www.greynoise.io/blog/exploitation-citrixbleed-2-cve-2025-5777-before-public-poc.

[15] Minister van Justitie en Veiligheid. "Voortgang informatiebeveiliging Openbaar Ministerie." Kamerstuk 26 643, nr. 1377, Tweede Kamer der Staten-Generaal. 2025. https://zoek.officielebekendmakingen.nl/kst-26643-1377.pdf.

[16] Cybersecurity Dive. "14K Fortinet devices compromised in new attack method." 2025. https://www.cybersecuritydive.com/news/14k-fortinet-devices-compromised-new-attack-method/745259/.

[17] Emsisoft. "Unpacking the MOVEit Breach: Statistics and Analysis." 2024. https://emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

[18] Cybersecurity and Infrastructure Security Agency. "BOD 26-02: Mitigating Risk From End-of-Support Edge Devices." Binding Operational Directive 26-02. 2026. https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices. Deadlines as reported by BleepingComputer, "CISA orders federal agencies to replace end-of-life edge devices." 2026. https://bleepingcomputer.com/news/security/cisa-orders-federal-agencies-to-replace-end-of-life-edge-devices.

[19] Cybersecurity and Infrastructure Security Agency, FBI, and partners. "Modern Approaches to Network Access Security." 2024. https://cisa.gov/resources-tools/resources/modern-approaches-network-access-security. VPN findings as summarized by SecurityWeek, "US, Allies Publish Network Access Security Guidance." 2024. https://www.securityweek.com/us-allies-publish-network-access-security-guidance/.

[20] Cybersecurity and Infrastructure Security Agency. "Known Exploited Vulnerabilities Catalog." https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

[21] The Hacker News. "Akira Ransomware Exploits SonicWall SSL VPN in Likely Zero-Day Attacks." Coverage of Arctic Wolf Labs research. 2025. https://thehackernews.com/2025/08/akira-ransomware-exploits-sonicwall.html.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.