SONICWALL®

SONICWALL.COM

CODE RED:

The state of healthcare cybersecurity in 2026.

Why the industry's attack rate never drops, and what to do about it.

Executive summary.

102,209

Malware hits per firewall (H1 2026): 4x the next-highest tracked vertical.

83%

83% Attack Retention. Intrusions persisted year-over-year: the highest retention of any tracked vertical.

10

Active ransomware families detected Jan–May 2026, including Gandcrab, Ryuk, and VHDLocker.

13.3 M

UltraVNC buffer overflow hits, remote desktop tools are the primary exploitation vector unique to this vertical.

243

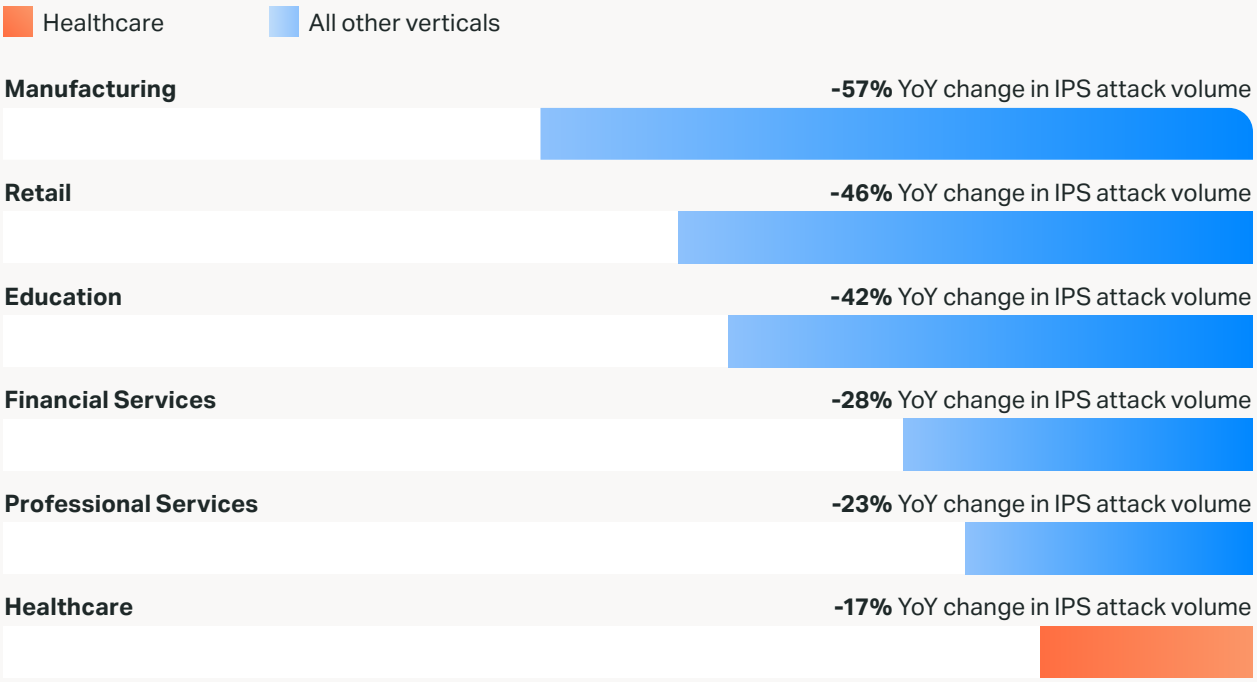
Unique attack methods targeting connected medical devices, IoT is healthcare's fastest-growing and hardest-to-patch exposure.

11.4 M

Apache Log4j2 hits tracked: clinical Java middleware still vulnerable 2.5 years after disclosure.

Healthcare is not just the most targeted vertical in SonicWall's 2026 telemetry; it's also the most persistently targeted. Attackers are targeting the healthcare industry more consistently than any other industry. While other industries saw IPS attack volumes decline between 17% and 56% year-over-year, healthcare barely moved at -16.9%. Attackers are not leaving. They're staying because the returns are too reliable and the defenses too predictable.

Spray and pray isn't happening anymore.

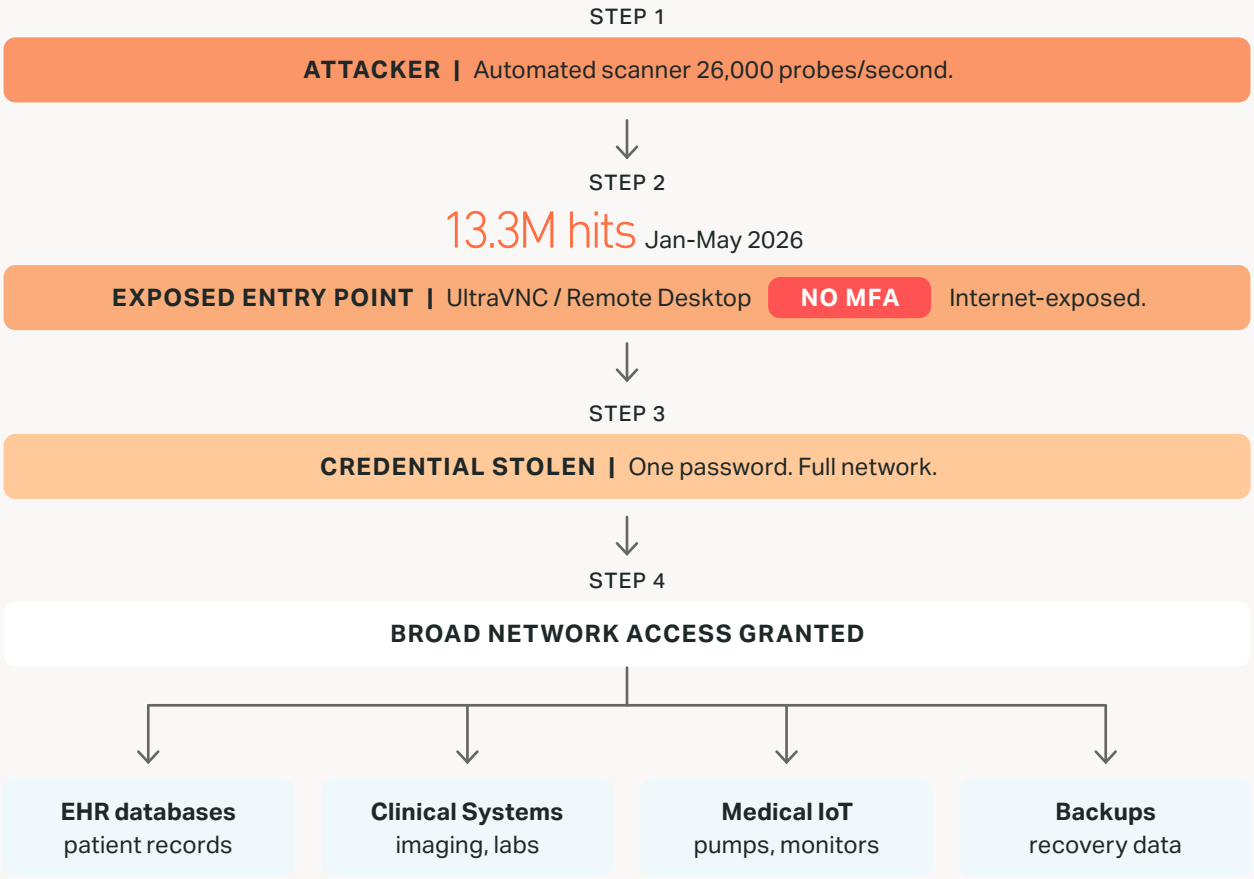


Sources: SonicWall 2026 YTD Vertical Threat Briefs: Jan-May 2026 vs Jan-May 2025

Remote access is the front door.

The UltraVNC buffer overflow signature generated 13.3 million hits in the first five months of 2026, a finding unique to healthcare's top ten. No other vertical sees remote desktop exploitation at this scale. And the reason is structural: healthcare organizations depend on remote management tools to support distributed clinical environments, telemedicine platforms and third-party vendor access to medical equipment. When those tools are internet-exposed without Multi-Factor Authentication (MFA) or network-level controls, they become the most predictable entry point in any healthcare network.

VPN-based access compounds the risk. Once credentials are validated, broad network access is granted, and from there, the path to clinical systems, Electronic Health Record (EHR) databases and connected devices is rarely restricted. A stolen set of remote-access credentials does not just unlock one application. It unlocks the whole environment.



A stolen remote-access credential does not unlock one application, it unlocks the environment.

Medical IoT creates an unmanaged attack surface.

The healthcare vertical detected Internet of Things (IoT) exploitation across 243 unique attack signatures. Connected infusion pumps, patient monitors, imaging systems and building automation devices create an attack surface that expands faster than security teams can govern it. These devices typically cannot run endpoint agents, rarely receive patches on a predictable cycle and often share network segments with clinical systems that process protected health information.

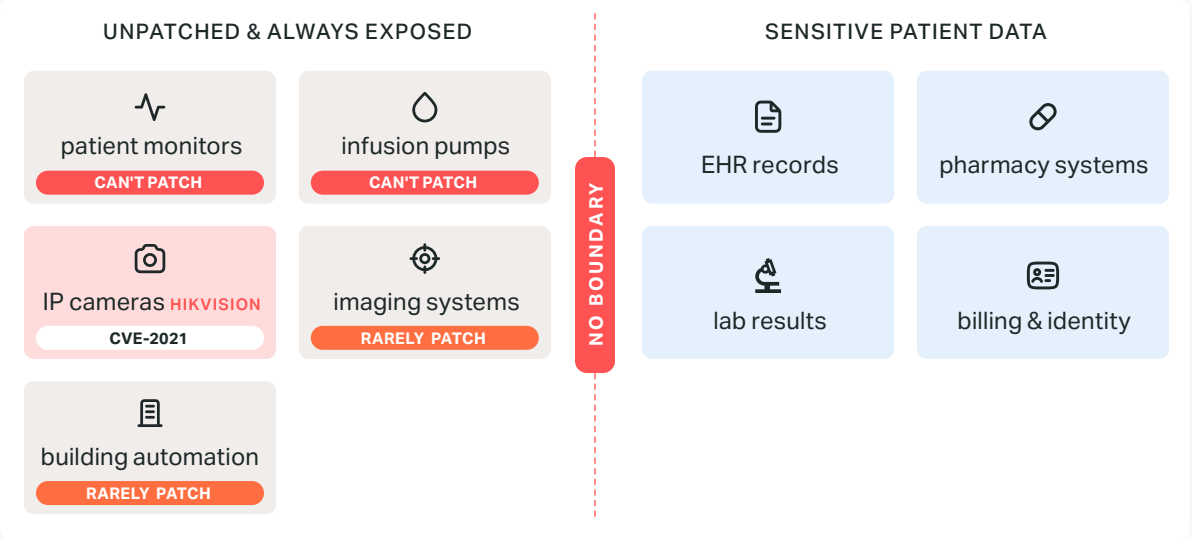
The Hikvision Command Injection vulnerability (CVE-2021-36260) (a flaw from 2021) continues to generate millions of hits annually across healthcare environments. Legacy vulnerabilities do not expire. When the devices that carry them cannot be patched or replaced on an enterprise cycle, they remain permanently available to automated scanning tools.

HEALTHCARE NETWORK EXPOSURE

These devices cannot run security software, are rarely patched, and share the same network as patient records.

243
unique attach methods against medical devices

5 yrs
CVE-2021-36260 open and still exploited



CVE-2021-36260 | HIKVISION COMMAND INJECTION | STILL ACTIVE

Replacing VPN is a deployment problem, not a planning problem.

VPN-based broad network access is the architectural flaw that turns a single stolen credential into a full network breach. The fix of providing application-level Zero Trust access that verifies identity and device posture continuously, rather than granting network trust at login, is well understood. What slows deployment in multi-location healthcare environments is not the technology. It is the absence of a repeatable process for standing it up across facilities that open on compressed timelines.

Fornida's engagement with ExaltHealth, a five-hospital rehabilitation chain with eight more in planning, produced a model for solving that problem operationally. After the first two hospital openings exposed the gaps in ad hoc IT buildouts, including an EDR deployment audit that found 40% of endpoints unprotected despite active licensing, Fornida embedded Zero Trust Network Access into a standardized opening playbook. ZTNA now ships pre-configured with every new facility's equipment package. Legacy VPN is retired facility-by-facility as the rollout proceeds. The transition does not require a network rebuild or a single coordinated cutover. It requires a repeatable process.

FORNIDA + ZERO TRUST: WHAT CHANGES AT THE ARCHITECTURE LEVEL

- Vendor and clinician remote access scoped to specific applications, not the network
- Identity and device posture verified continuously, not only at login
- A compromised credential no longer grants lateral access to EHR systems, clinical devices, or administrative infrastructure
- Legacy SSL-VPN retired per facility as the standard playbook rolls forward

5

Operating hospitals: one CTO covering all IT, compliance, and clinical tech operations.

4

Vendor systems touched by a single nurse support ticket: EMR, insurance gateway, pharmacy, patient monitoring.

8+

Facilities in planning, each one a new expansion project that must open on time.

100%

EDR coverage achieved after audit revealed 40% of endpoints were unprotected

Ransomware targeting Is deliberate, not opportunistic.

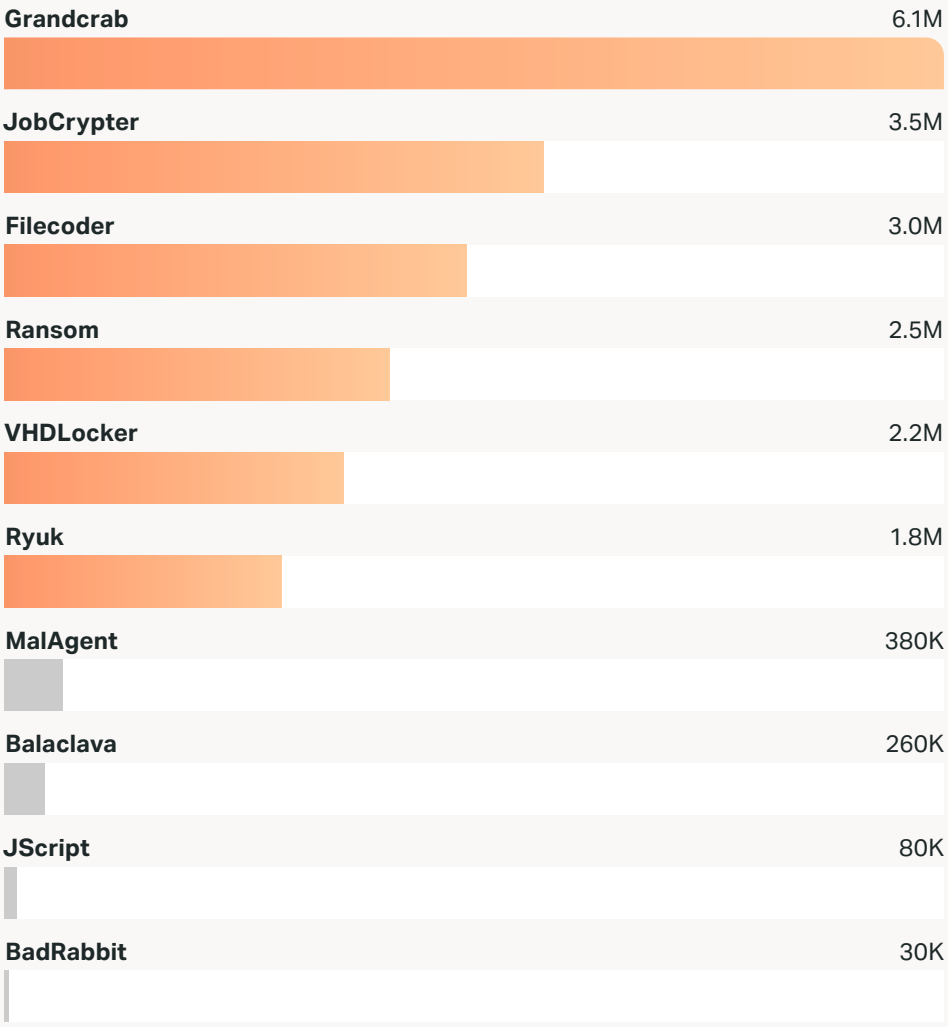
Healthcare's ransomware landscape in the first half of 2026 includes ten active families, more than any other vertical. Gandcrab (6.1M hits), JobCrypter (3.5M), Filecoder (3.0M), VHDLocker (2.2M) and Ryuk (1.8M) are all active simultaneously. This is not spray-and-pray opportunism. The presence of multiple distinct ransomware groups operating concurrently against a single vertical reflects a deliberate targeting strategy driven by a simple calculation: healthcare organizations cannot absorb extended downtime, and they are significantly more likely to pay.

MULTIPLE GROUPS. SIMULTANEOUS CAMPAIGNS. HEALTHCARE IS A DELIBERATE TARGET.

10
active ransomware families: more than any other vertical

16.6M
total ransomware hits, Jan-May 2026

RANSOMWARE HITS BY FAMILY (JAN-MAY 2026)



WHY THIS MATTERS

Spray-and-pray ransomware hits one or two families. Ten concurrent families signals multiple organised groups who have independently concluded the same thing; healthcare organisations cannot afford downtime, and they pay.

SOC POV

"In healthcare breach investigations, remote access is almost always the entry point. The tool, whether VNC, RDP or a vendor management platform, was working as intended. The problem is, it was exposed to the internet with no additional authentication layer and connected directly to clinical systems. Once an attacker is in through that door, the medical devices on the same network segment give them options that do not exist in other industries. We consistently find that the question is not how the attacker got in, it is why nothing was in place to limit where they could go."

What protection looks like in practice.

The answer isn't removing remote access; healthcare can't operate without it. The answer is replacing implicit trust with continuously verified access. SonicWall Cloud Secure Edge (CSE) applies Zero Trust principles to every access request, regardless of whether the user is a clinician connecting from home, a vendor technician accessing medical equipment or an administrator managing a distributed facility network. Rather than granting broad network access the moment credentials are verified, CSE grants application-level access only, and continuously re-verifies identity and device posture throughout the session. A compromised remote-access credential no longer means a compromised network.

A COMPROMISED CREDENTIAL SHOULD NOT MEAN A COMPROMISED NETWORK.

The shift from implicit trust to continuously verified access.

THE OLD MODEL | VPN

One credential verified

- Broad network access granted
- Never re-verified
- Lateral movement: unrestricted

everything

THE ZERO TRUST MODEL

Identity + device verified

- Application-level access only
- Continuously re-verified
- Lateral movement: blocked

only what's needed

Four actions to take now.

1

RESTRICT REMOTE DESKTOP TOOLS

Limit UltraVNC and RDP to internal VLANs, Require MFA on all remote access, no exceptions for vendor accounts or break-glass credentials.

2

SEGMENT MEDICAL LOT DEVICES

Place connected medical devices on dedicated network segments isolated from clinical systems. Assume these devices cannot be patched and build controls around that reality.

3

REPLACE VPN WITH APPLICATION-LEVEL ZERO TRUST ACCESS

Broad VPN turns one stolen credential into a total-network breach. Application-level Zero Trust enforces least-privilege access per application and limits lateral movement.

4

ADDRESS LEGACY VULNERABILITY EXPOSURE NOW

Log4Shell (11.4M hits) and Hikvision CVE-2021-36260 are still generating millions of detections. Inventory clinical middleware and IoT firmware: patch or isolate on a defined schedule.

Cloud Secure Edge: sonicwall.com/products/cloud-secure-edge

SONICWALL

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®