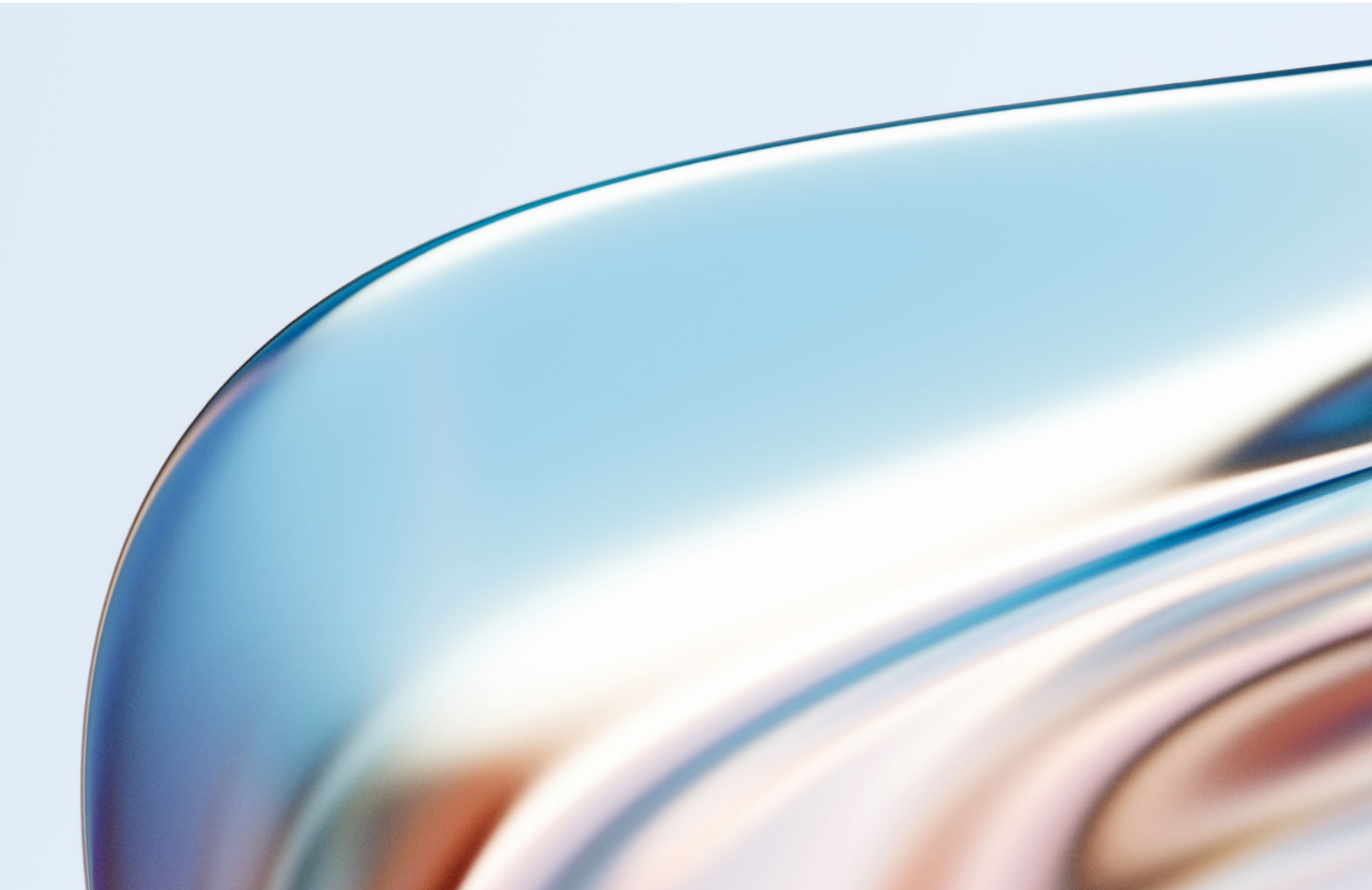
SONICWALL®

SONICWALL.COM

BREAKING POINT

The state of manufacturing cybersecurity in 2026.

The convergence of IT and operational technology is creating an attack surface that threat actors have learned to exploit with precision.



Executive summary.

61,743

IPS hits per device in the first half of 2026: third highest of any tracked vertical.

43M

Hikvision IP Camera Command Injection hits: the single largest IoT attack signature across any industry SonicWall tracks.

10

Active ransomware families in H1 2026, including Zhen, Filecoder and VHDLocker.

29.7M

Total ransomware hits in the first half of 2026.

262

Unique IoT attack signatures detected across manufacturing networks.

539

Devices detecting SCADA attack attempts: the highest of any tracked vertical.

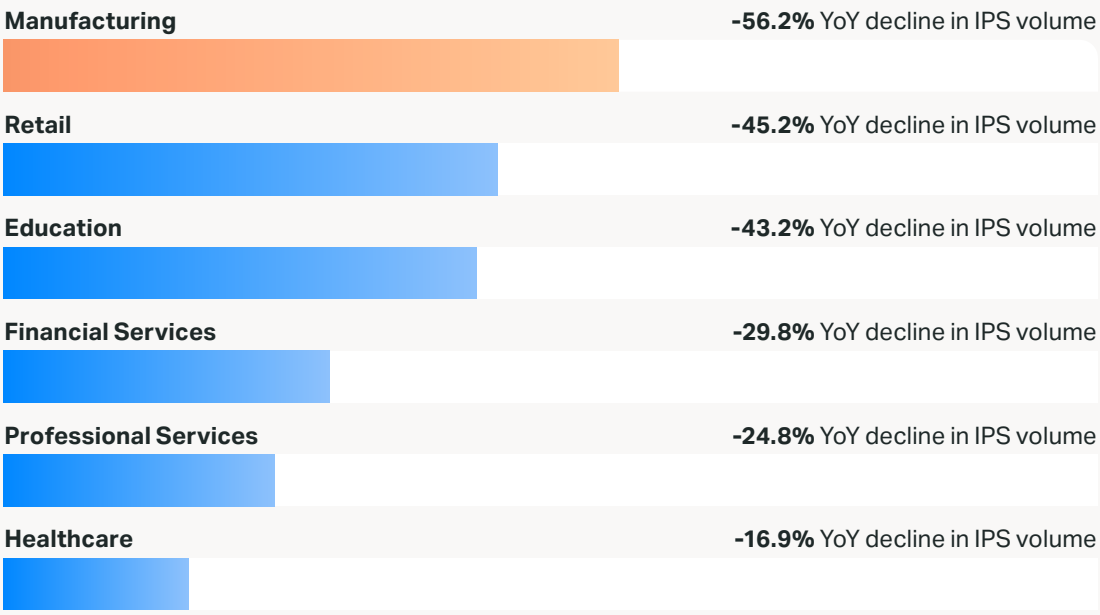
The unlocked doors attackers are still walking through.

Every year, attacks look more sophisticated. In some ways, they are. AI has made them faster, cleaner and harder to spot at a glance. But the underlying methods have not changed. Attackers are still walking through the same unlocked doors.

In manufacturing, those entry points are physical. From IP cameras monitoring production lines and building automation systems managing HVAC and access controls, to industrial equipment connected directly to corporate networks for maintenance—every single connection was built for operational efficiency. And yet each one represents a potential vulnerability. Manufacturing saw a 56.2% year-over-year (YoY) decline in IPS volume in the first half of 2026, the steepest of any tracked vertical. But volume decline does not mean reduced risk. It means attackers are becoming more selective. The absolute volume remains significant at 474 million events. And as more operational technology connects to IT infrastructure, the attack surface is expanding, not contracting.

YoY IPS Volume Change by Vertical

H1 2026 vs H1 2025



WHY THIS MATTERS

Manufacturing's IPS volume decline is the steepest of any vertical, but its Internet of Things (IoT) attack surface is the largest. Fewer, more targeted attacks on a growing connected device footprint is not an improvement in posture.

An open door to the factory floor: how IP cameras became manufacturing's biggest IoT threat.

The Hikvision IP Camera Command Injection signature generated 43 million hits in the first half of 2026. It is the single largest IoT attack signature across any industry SonicWall tracks. Manufacturing relies heavily on IP cameras for production line monitoring, warehouse oversight and facility security. These cameras are networked, they run embedded operating systems and they are rarely updated on a predictable cycle.

The Hikvision command injection vulnerability (CVE-2021-36260) was disclosed in 2021. Five years later, it remains the third-highest volume attack signature in manufacturing. Legacy vulnerabilities do not expire. When the devices that carry them cannot be patched on a standard cycle and share network access with production systems, they remain permanently available to automated scanning tools.

IoT attacks are the second-largest attack category in manufacturing by volume, generating 46.2 million hits. More than half of manufacturing networks detected IoT exploitation in the first half of 2026, across 262 unique attack signatures. The variety of signatures reflects the variety of connected devices: IP cameras, industrial sensors, building automation systems and other connected equipment. Each device category has its own vulnerability profile. Each represents a separate entry point.

Manufacturing IoT Exposure

43M

Hikvision hits in the first half of 2026, **the largest IoT signature across any vertical**

262

unique IoT attack signatures detected

#2

IoT attacks are the #2 attack category by volume

CVE 2021

CVE-2021-36260 was disclosed in 2021 and still actively being exploited in 2026

WHY THIS MATTERS

These devices cannot be patched on a standard cycle, share network access with production systems, and run embedded operating systems that were never designed with enterprise security in mind.

When corporate access leads straight to the machine floor.

Manufacturing has the highest Supervisory Control and Data Acquisition (SCADA) attack detection rate of any vertical SonicWall tracks. Across 18 unique SCADA attack signatures, networks are detecting active exploitation attempts against industrial control systems. These are not generic web attacks, rather they are targeted probes against the operational technology that runs production lines, manages facility systems and controls physical processes.

The risk compounds as corporate IT networks and operational technology networks share infrastructure and access paths. This is increasingly common. Remote monitoring, predictive maintenance and Enterprise Resource Planning (ERP) integration all create pathways between systems that were historically isolated. A compromised business credential can become a path to operational systems. A stolen login for a procurement application raises a question: what else can that credential reach? In many manufacturing environments, the answer is more than it should be.

Ransomware groups have recognized this. Ten families were active against manufacturing networks in the first half of 2026. The Zhen ransomware family generated 22.2 million hits concentrated on a very small number of devices, the pattern of a single active outbreak rather than a broad campaign. Filecoder (2.87M), VHDLocker (2.61M), and Ryuk (1.05M) represent the broader landscape: a mix of opportunistic and targeted campaigns, each calculated to exploit an industry that cannot afford to stop production.

SCADA Exposure

539	18	Highest
devices detecting SCADA attack attempts	unique SCADA attack signatures detected	SCADA attack exposure of any tracked vertical

Ransomware hits by family

H1 2026

Zhen	**Filecoder**	**VHDLocker**	**Ryuk**
22,248,955	2,870,208	2,611,570	1,050,886
JobCrypter	**MalAgent**	**Gandcrab**	**JScript**
478,203	141,829	141,218	72,094

WHY THIS MATTERS

Extreme volume concentration on two devices is an active incident, not a statistic. Zhen detections at this scale require immediate investigation regardless of how long they have been generating alerts.

The Zero Trust blueprint: architectural isolation for industrial systems.

The architectural problem in manufacturing is the same one found across every sector that has connected operational systems to corporate infrastructure: access designed for convenience, not security. VPN-based remote access grants broad network access the moment credentials are validated. Manufacturing environments depend on operational technology (OT) — the systems that control physical equipment, production lines and industrial processes — alongside traditional IT infrastructure. In environments where the two share the same network, a compromised business credential can reach systems that control physical processes.

Zero Trust changes the architecture, not just the policy. Application-level access means a credential grants access to a specific system, not the network behind it. Continuous identity and device verification means a session valid at login is not automatically valid for operational systems. A stolen credential no longer means a compromised production floor.

Overall, malware detections are down significantly compared to last year, but that is largely a reflection of better detection tools, not fewer attacks. The threat has not shrunk. It has just become harder to see.

A compromised credential should not reach the production floor.

THE OLD MODEL | VPN

- One credential verified at the perimeter
- Broad network access granted
- Corporate and OT networks accessible
- Lateral movement: unrestricted

THE ZERO TRUST MODEL

- Identity and device posture verified continuously
- Application-level access only
- OT systems isolated by policy
- Lateral movement: blocked

ACTIONABLE RECOMMENDATIONS

Five actions to take now.

1

REPLACE VPN-BASED REMOTE ACCESS WITH ZERO TRUST

Apply application-level Zero Trust access to all remote connections to manufacturing environments, including vendor and maintenance access to production systems. A stolen credential should not reach the production floor.

2

AUDIT AND UPDATE IP CAMERA FIRMWARE ACROSS ALL FACILITIES

The Hikvision command injection vulnerability is five years old and still generating 43 million exploitation attempts. Identify all affected devices, apply available firmware patches and place unpatched devices on isolated network segments with no path to production or corporate systems.

3

INVESTIGATE ZHEN RANSOMWARE DETECTIONS IMMEDIATELY

Volume concentration of 22.2 million hits on two devices indicates active infection. Initiate incident response procedures. Do not treat this as a background detection to be reviewed at the next scheduled assessment.

4

ENFORCE STRICT IT/OT NETWORK SEGMENTATION

Production systems, SCADA controllers and industrial equipment should not share network access paths with corporate IT infrastructure. Enforce boundaries that cannot be traversed without explicit policy authorization, and treat any access to OT systems as a privileged session requiring continuous verification.

5

EXTEND LOG4J REMEDIATION TO OPERATIONAL TECHNOLOGY MANAGEMENT SYSTEMS

Apache Log4j2 generated 13.8 million hits across manufacturing networks in the first half of 2026. Inventory all Java-based operational management and ERP systems and patch or isolate on a defined schedule. Where patching is not operationally feasible, deploy WAF rules and network-level isolation.

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®