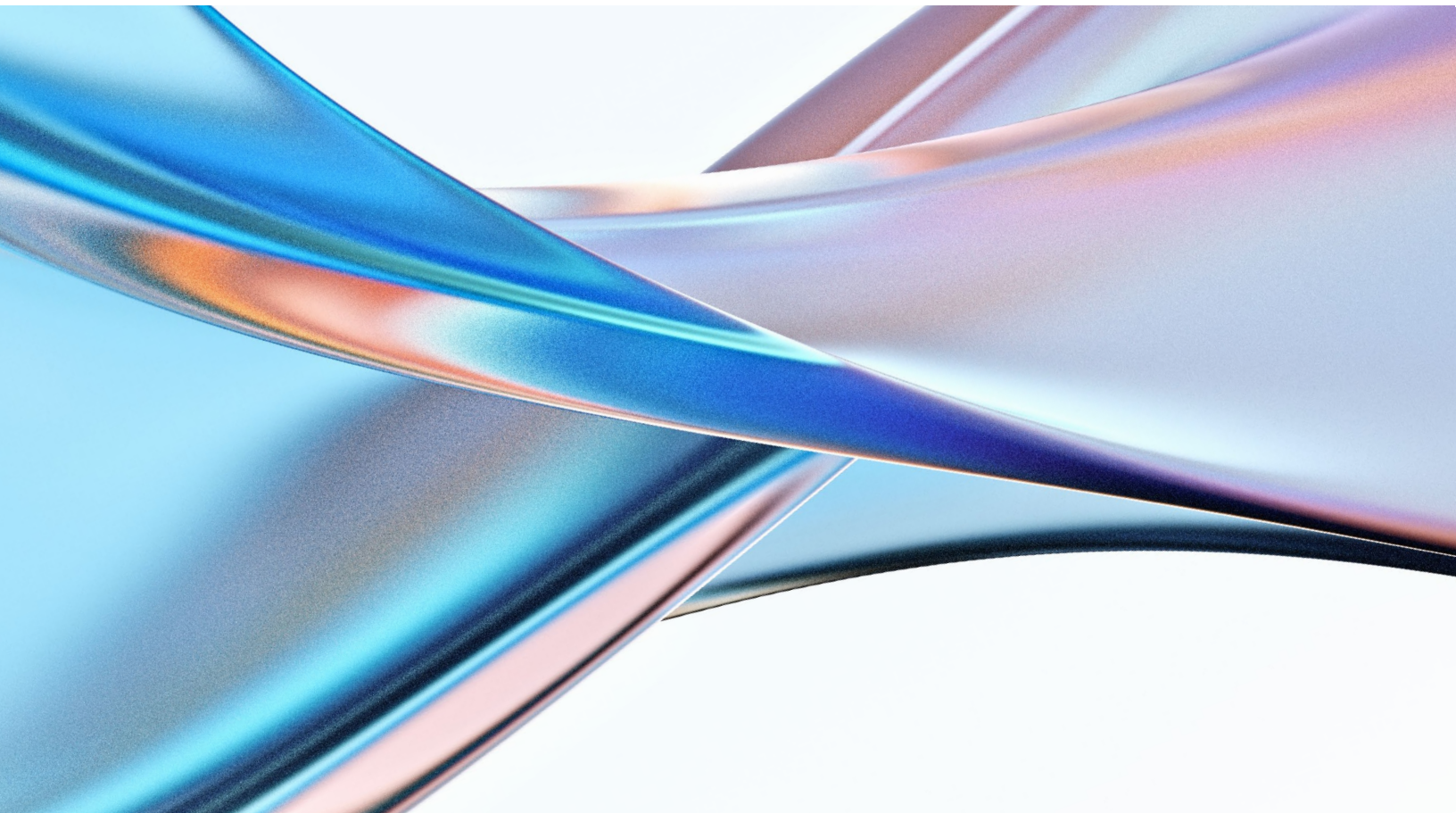
SONICWALL®

SONICWALL.COM

OVERDRAWN

# The state of financial services cybersecurity in 2026.

Why the sector's highest per-device attack intensity demands a different defense posture.



# Executive summary.

## 132,378

Hits per firewall: Financial Services is hit by cyberattacks more than twice as often as the average industry, more than any other sector we track.

## 39,341

Malware hits per firewall: second only to healthcare in per-device intensity.

## 10

Active ransomware families detected Jan–May 2026, including Filecoder, MalAgent and Sodinokibi/REvil.

## 42 M

Over 40M attacks concentrated on unpatched, end-of-life systems still running inside financial institutions.

## 35.6 M

Apache Log4j2 hits tracked: Java-heavy payment and banking middleware still vulnerable 2.5 years after disclosure.

## 747

Firewalls still detecting Heartbleed (OpenSSL CVE-2014-0160) — twelve years after initial disclosure.

INTRUSION PREVENTION

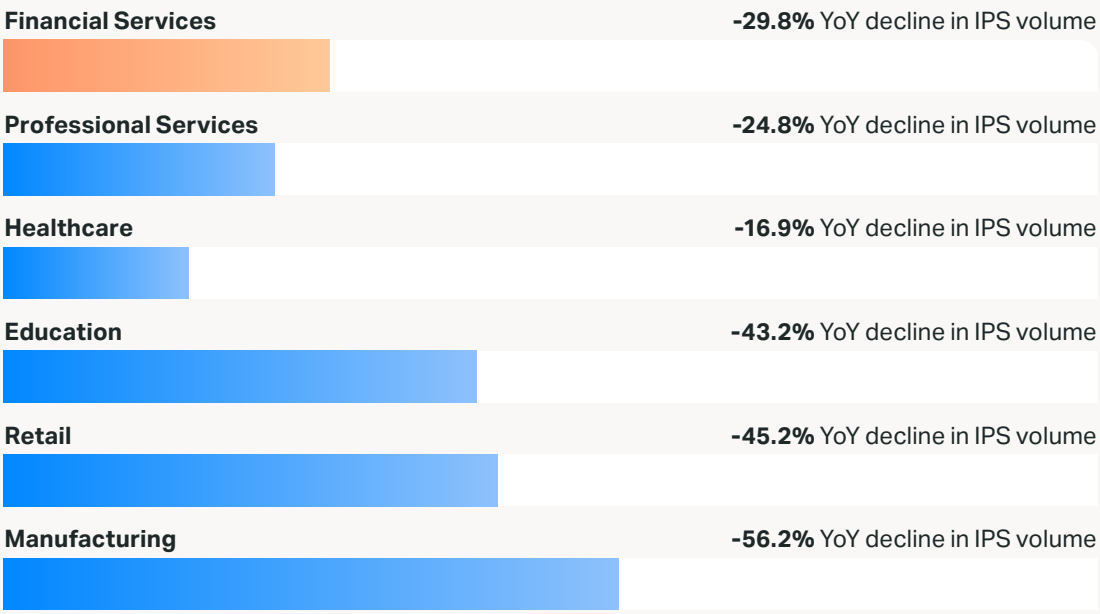
# The most intense attack surface per device.

In the first half of 2026, financial services firms faced more cyberattack attempts per organization than any other industry SonicWall tracks. More than double the average across all tracked sectors.

Overall attack volumes are falling across every industry as attackers grow more selective, trading quantity for precision. Financial services followed that trend, but the drop was smaller than elsewhere. Attackers are not walking away from this sector. They are simply becoming more deliberate about how they hit it, focusing effort where the payoff is highest rather than casting a wide net.

## YoY IPS Volume Change by Vertical

1H 2026 vs 2025




WHY THIS MATTERS

Financial Services declined 29.8% year over year (YoY), sitting between Healthcare (–16.9%) and the broader pack, reflecting sustained attacker interest despite improved defenses.



Learn more about Cloud Secure Edge

SONICWALL®

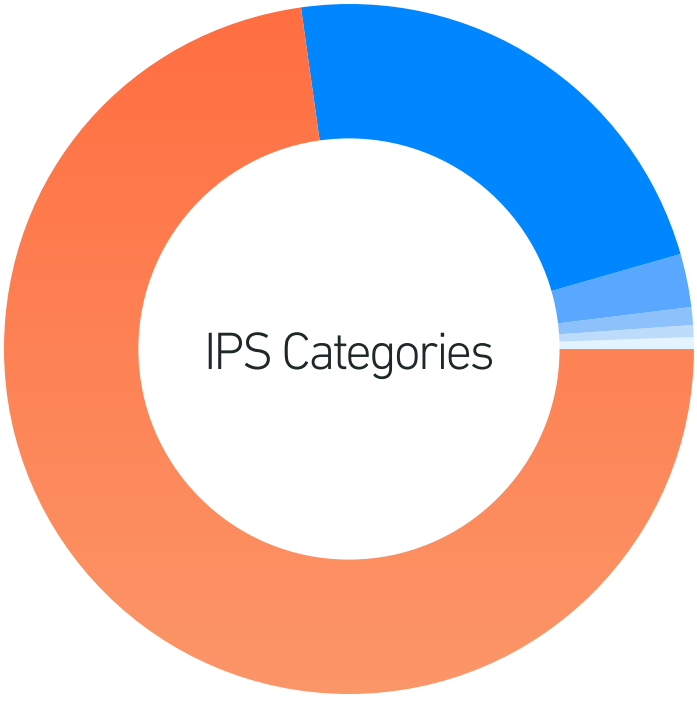
# IPS Top 10 by volume.

| # | SIGNATURE | CATEGORY | HITS | FIREWALLS |
|---|---|---|---|---|
| 1 | Web Application Malformed Request URI 7 | WEB-ATTACKS | **68,137,891** | 200 |
| 2 | GoodTech Telnet Server Buffer Overflow 1 | MISC | **42,153,814** | 5 |
| 3 | Apache Log4j2 JNDI Log Messages RCE | MISC | **35,586,995** | 892 |
| 4 | Web Application Directory Traversal 7 | WEB-ATTACKS | **26,058,605** | 484 |
| 5 | Web Application Directory Traversal 20 | WEB-ATTACKS | **20,306,752** | 1,228 |
| 6 | Web Application Malformed Request URI 6 | WEB-ATTACKS | **18,003,177** | 473 |
| 7 | Web Application Directory Traversal 8 | WEB-ATTACKS | **16,880,499** | 380 |
| 8 | Web Application Directory Traversal 36 | WEB-ATTACKS | **12,614,060** | 245 |
| 9 | Web Application Directory Traversal 5 | WEB-ATTACKS | **11,609,088** | 234 |
| 10 | Web Application Directory Traversal 1 | WEB-ATTACKS | **7,972,909** | 880 |

# IPS Attack Category Breakdown

| | |
|---|---|
| web attacks | 72.9% |
| misc | 22.7% |
| exploit kit | ~2.5% |
| SUSP traffic | ~1.0% |
| IoT attacks | ~0.5% |
| PL VULNS | ~0.4% |

WEB-ATTACKS dominate at 73% of IPS volume (257.8M hits), but the MISC category is elevated by the GoodTech Telnet anomaly. IoT-ATTACKS affect 1,185 firewalls—a broader footprint than the raw hit count suggests.






Learn more about Cloud Secure Edge

SONICWALL

# Three outstanding debts the financial industry keeps carrying.

## 01. Legacy Infrastructure: The GoodTech Telnet Anomaly

The GoodTech Telnet Server Buffer Overflow signature generated 42.2 million hits, an extreme concentration that has no equivalent in any other tracked vertical. A handful of financial-sector devices with exposed Telnet services are generating detection volumes comparable to an entire fleet elsewhere. These devices almost certainly represent legacy core banking or payment infrastructure that pre-dates modern security best practices. These legacy systems have a serious problem: they send usernames and passwords across the network in plain text. Anyone intercepting the connection can read them directly. Worse, the type of attack being used here can give an intruder full remote control of the machine. These are not isolated back-office servers. They sit next to the systems that process payments and hold transaction records.

This is not a low-level warning to log and revisit. It requires immediate investigation.

## 02. Log4Shell and Heartbleed: Unpatched Legacy at Scale

Apache Log4j2 RCE (Log4Shell) is the #3 threat by volume with 35.6 million hits across financial firewalls, more than two years after the vulnerability was publicly disclosed and emergency-patched across the industry. Java-heavy middleware stacks common in financial services (payment processors, core banking APIs, fraud detection engines) continue to run unpatched instances at scale. OpenSSL Heartbleed ranks seventh by breadth as firewalls continue to receive active probes twelve years after its 2014 disclosure. Both findings point to the same structural problem: the software patching cycle inside financial institutions does not keep pace with vulnerability timelines, because the cost of taking critical systems offline for patching is perceived as higher than the residual risk. Attackers have learned this calculation and continue to exploit it.

## 03. Ransomware: Concentrated, Financially Motivated, Modern

Financial Services recorded 9.2 million ransomware hits, with ten active families operating simultaneously. Filecoder dominates with 5.2 million hits, suggesting a small number of persistently infected environments generating high-volume traffic. The presence of Sodinokibi/REvil and Prometheus alongside older families is significant: these are groups with documented financial-sector targeting strategies and the operational discipline to move laterally through complex enterprise environments. The concentration on financial firewalls indicates targeted intrusion rather than broad campaign exposure.



Learn more about Cloud Secure Edge

MALWARE (GAV)

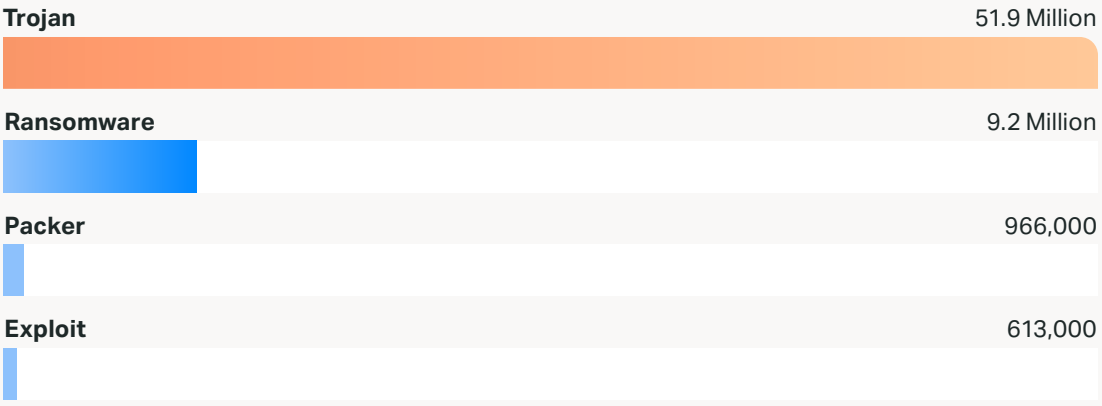
# Malware intensity second only to healthcare.

In the first half of 2026, financial services firms detected 62.8 million instances of malicious software attempting to run on their networks.

The vast majority was not the kind designed to destroy files or shut systems down. It was the quieter, more dangerous kind: software built to steal login credentials and maintain a hidden foothold inside the network for future use. That is a deliberate choice by attackers. In financial services, silent and persistent access is worth more than visible disruption.

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.

## Malware (GAV) by category.






Learn more about Cloud Secure Edge

SONICWALL®

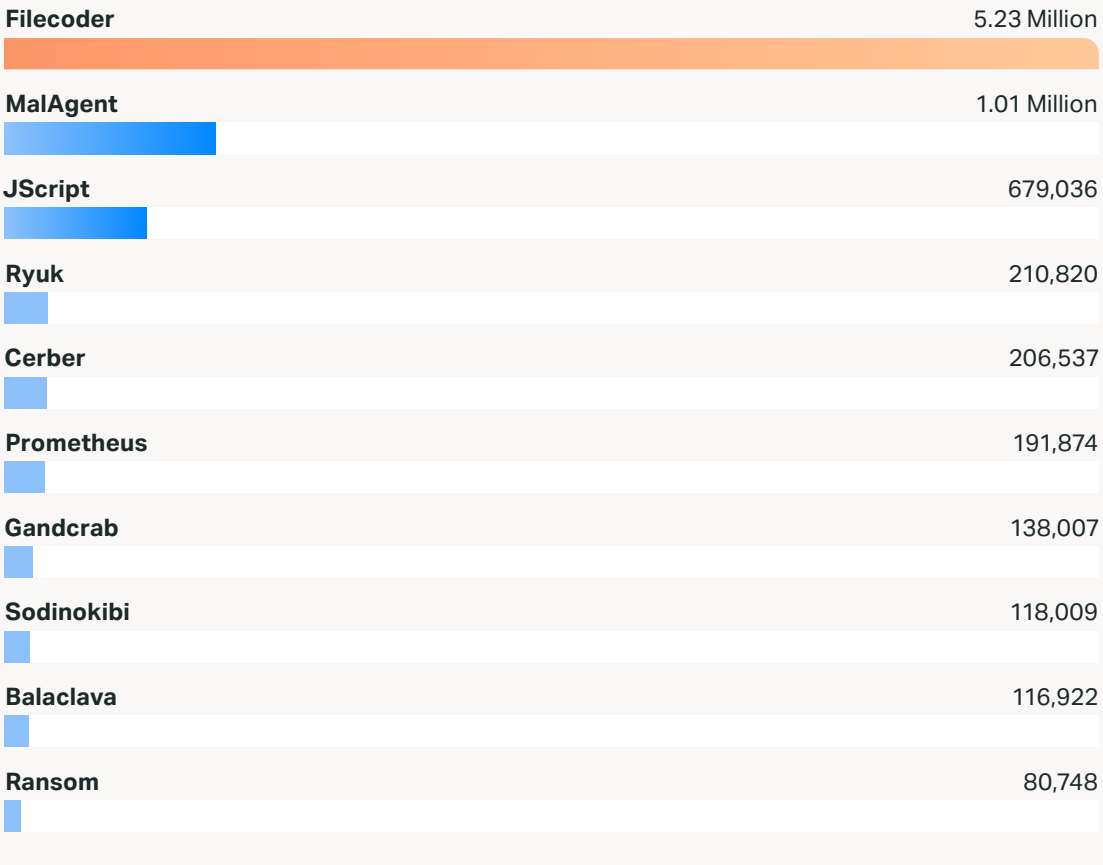
RANSOMWARE

# Ten active families, narrow footprint, deliberate targeting.

The coexistence of ten ransomware families in a single vertical is not random. Each group has independently concluded that financial services organizations offer a superior return: high-value data, significant pressure to restore operations quickly and regulatory consequences that create additional leverage. The Filecoder dominance (5.2M hits, 11 FWs) combined with modern groups such as Sodinokibi/REvil and Prometheus characterizes a landscape where both automated opportunism and human-operated targeted campaigns are running simultaneously.

## Ransomware hits by family

1H 2026




Filecoder accounts for 57% of total ransomware hits, concentrated on 11 devices. Sodinokibi/REvil and Prometheus represent modern, financially motivated threat actors specifically targeting this sector.



Learn more about Cloud Secure Edge

SONICWALL

ACTIONABLE RECOMMENDATIONS

# Five actions to take now.

1

### REPLACE BROAD NETWORK ACCESS WITH ZERO TRUST

Most security breaches do not stop at the front door. Once an attacker is inside a financial services network, traditional access controls rarely limit where they can go. A stolen credential does not just unlock one system. It unlocks the environment. Zero Trust changes that. A compromised credential no longer means a compromised network.

2

### AUDIT AND DECOMMISSION EXPOSED TELNET SERVICES IMMEDIATELY

The GoodTech Telnet anomaly represents an active critical exposure. Identify all Telnet-enabled devices, isolate them from payment and transaction infrastructure, and schedule immediate decommission or migration to SSH-based management.

3

### PRIORITIZE LOG4J REMEDIATION ACROSS JAVA-BASED FINANCIAL MIDDLEWARE

Log4Shell continues to generate millions of hits. Inventory all Java-based systems (payment processors, core banking APIs, fraud detection engine) and patch or isolate on a defined schedule. Where patching is not operationally feasible, deploy WAF rules and network-level isolation.

4

### AUDIT TLS ENDPOINTS FOR HEARTBLEED EXPOSURE

Financial firewalls are still receiving active Heartbleed probes 12 years after CVE-2014-0160 disclosure. Conduct a full TLS endpoint audit, replace any legacy OpenSSL instances below 1.0.1g, and rotate any certificates issued on vulnerable infrastructure.

5

### IMPLEMENT OFFLINE, AIR-GAPPED BACKUPS AND EDR WITH RANSOMWARE ROLLBACK

Ten concurrent ransomware families — including Sodinokibi/Revil — indicates targeted intrusion capability. Immutable, offline backups are non-negotiable. Pair with EDR that supports behavioral detection and automatic rollback to limit dwell time and blast radius.



Learn more about 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®