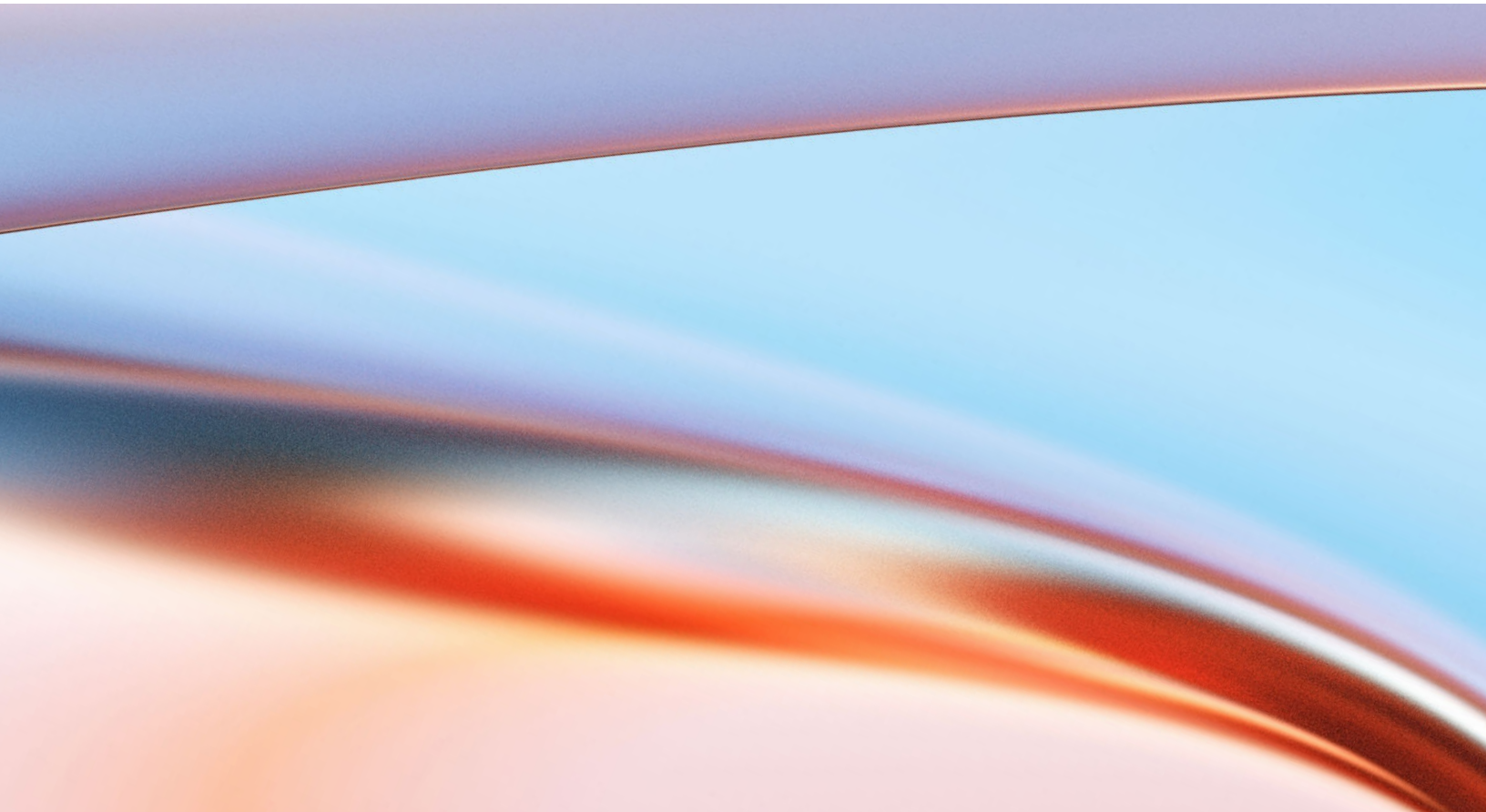
SONICWALL®

SONICWALL.COM

OBJECTION OVERRULED

The state of professional services cybersecurity in 2026.

Why the sector's largest attack surface and broadest ransomware exposure demands a fundamentally different posture.



Executive summary.

3 Billion

Total IPS events in the first half of 2026: the largest absolute attack volume of any tracked vertical.

70M

Total ransomware hits: more than any other industry SonicWall tracks.

460

Organizations actively detecting ransomware campaigns: the broadest exposure of any vertical.

332M

SIPVicious combined hits in the first half of 2026: VoIP exploitation is the primary threat vector unique to this sector.

107M

Apache Log4j2 hits: document management and billing middleware still vulnerable 2.5 years after disclosure.

10

Active ransomware families including Filecoder, Gandcrab and Ryuk.

The largest attack surface in SonicWall's telemetry.

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 professional services, those doors are open by design. Law firms, accountancies, consulting practices, engineering firms, and managed service providers collectively host client portals, document management platforms, billing systems, and collaboration tools that are built to be accessible. That accessibility is the product, and it is also the vulnerability.

Professional services represent the largest attack surface in SonicWall's telemetry by absolute volume, generating 3 billion IPS events in the first half of 2026. This is not because professional services firms are uniquely insecure. It is because the sector is large, broadly distributed, and holds exactly what attackers want: client records, financial data, privileged communications, intellectual property, and in the case of MSPs, administrative access to the infrastructure of dozens of other organizations.

PROFESSIONAL SERVICES | H1 2026

3 billion

IPS EVENTS ACROSS LAW FIRMS, ACCOUNTANCIES, AND MSPS

Law firms
Client portals, document management

Accountancies
Billing and client ledger systems

Managed service providers
Administrative access to client infrastructure

VoIP Exploitation Exposure.

- 332M SIPVicious hits in the first half of 2026 (signatures ranked #3 and #6 by volume)
- Professional services is the only vertical where SIPVicious reaches this scale
- SIP exploitation provides call interception, fraud capability, and lateral movement opportunity
- Law firms and MSPs with exposed SIP endpoints are primary targets

An exposed SIP endpoint does not just enable call fraud. It provides a foothold into every system that shares network access with the phone infrastructure.

SONICWALL

The data attackers are actually after.

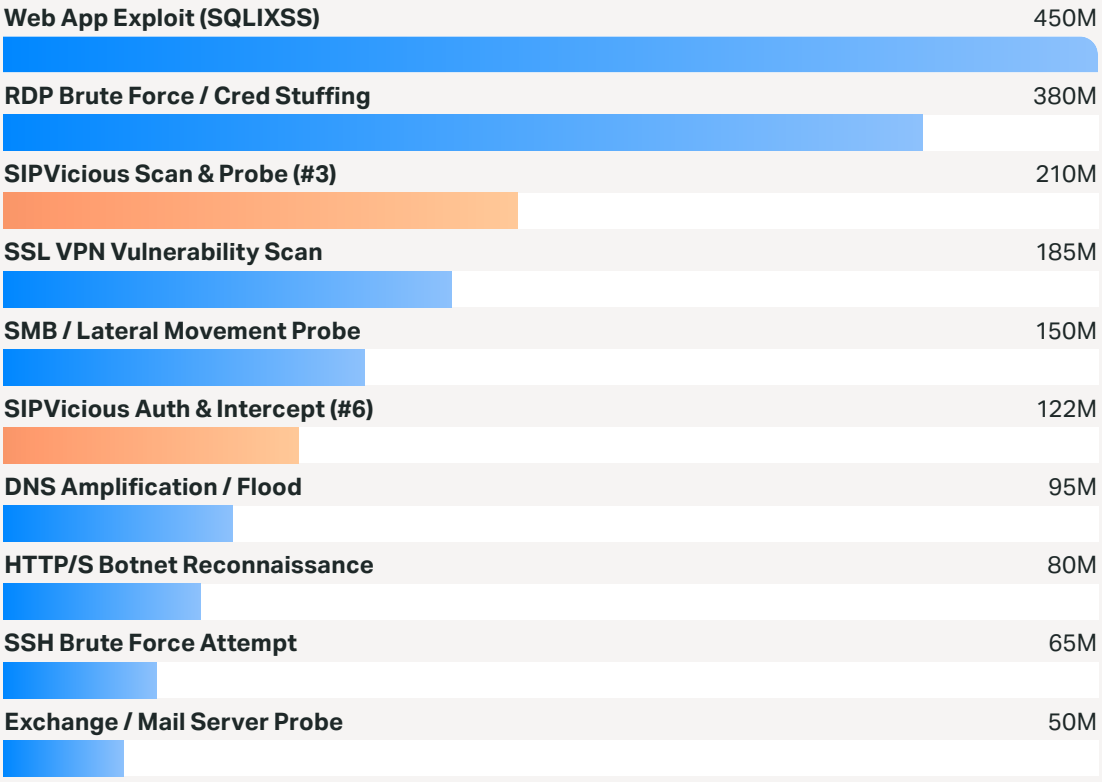
Professional services firms hold a category of data that is uniquely valuable: client records tied to active legal matters, financial transactions, privileged communications, and in the case of MSPs, administrative credentials for the networks of dozens of client organizations. This is not incidental data. It is data that carries legal, financial, and reputational leverage for the organizations it belongs to.

That leverage drives ransomware targeting. Professional services recorded 69.9 million ransomware hits in the first half of 2026, more than any other vertical. Ten ransomware families operated simultaneously against professional services networks: Filecoder dominated with 19.1 million hits across 113 organizations, while Gandcrab (11.9M) and Ryuk (10.5M) represent groups with documented enterprise targeting strategies. MalAgent (8.7M) and JScript (6.9M) complete a picture where both automated opportunism and human-operated targeted intrusion run in parallel.

The MSP dimension compounds this. An MSP breach is not one breach. It is potential access to every client environment the MSP manages. Ransomware groups understand this arithmetic. The presence of Ryuk and Sodinokibi in professional services environments is not coincidental. These are groups that specifically target organizations with administrative access to other organizations.

Top Attack Signatures in Professional Services H1 2026

SIPVICIOUS VOLP EXPLOITATION ACCOUNTS FOR 332M COMBINED HITS (#3 AND #6 SIGNATURES)



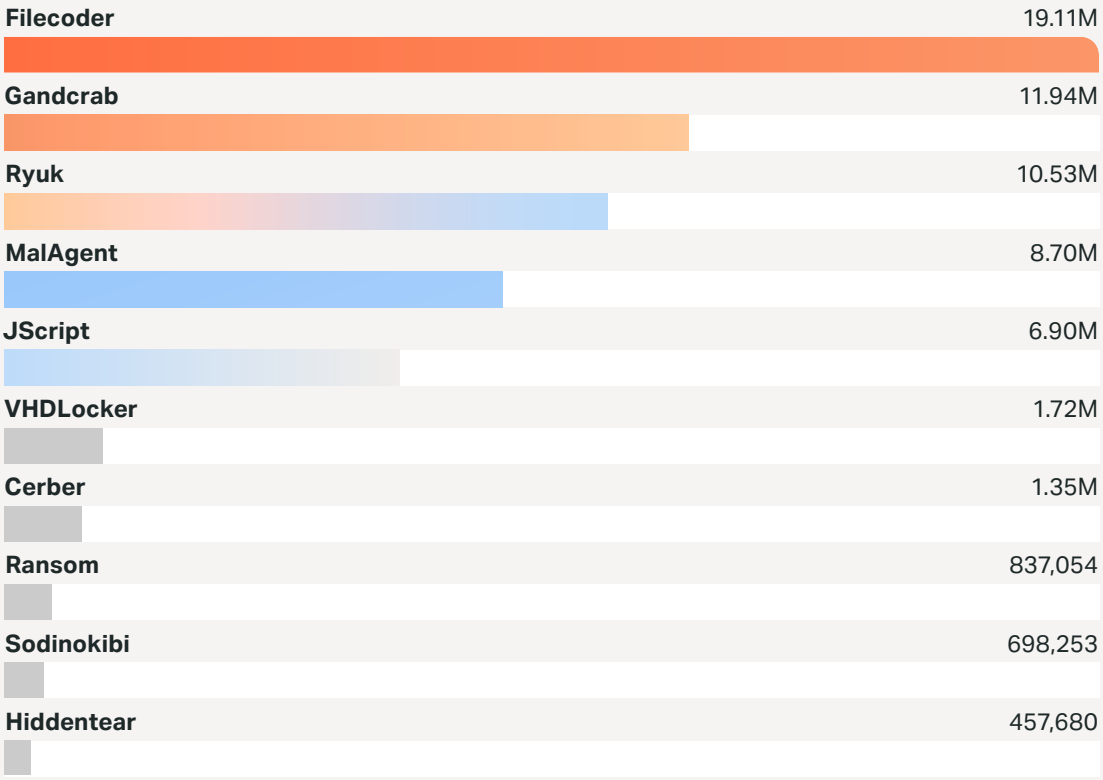
SIPVICIOUS IMPACT

332M Combined Hits
Rank #3: **210M hits**
Rank #6: **122M hits**
Primary Target:
Unprotected SIP Endpoints

SONICWALL

Ransomware Hits by Family FIRST HALF OF 2026

Top 10 active threat strains impacting 460 targeted organizations



WHY THIS MATTERS

Ten simultaneous ransomware families across 460 organizations is not spray-and-pray. It is a sector that multiple organized groups have independently determined offers reliable returns: high-value data, operational pressure to restore quickly, and clients whose interests create additional leverage.

STRATEGIC CONTEXT

10 active strains across 460 orgs

Targeted threat, not 'spray-and-pray'

Sector targeted for high-value data, restoration pressure & client leverage

SONICWALL®

Log4Shell is still generating 107 million hits.

Apache Log4j2 RCE (Log4Shell) ranks seventh by volume in professional services with 107 million hits across the sector — 2.5 years after the vulnerability was publicly disclosed and emergency-patched across the industry. Professional services firms typically run Java-based middleware stacks for document management, billing, case management, and client relationship platforms. These systems are operationally critical, deeply integrated, and difficult to patch without scheduled downtime that disrupts billable activity.

The patching calculus is well understood. Taking a client billing system offline for maintenance has an immediate, measurable cost. The residual risk of an unpatched Log4j instance feels abstract by comparison — until it is not. Attackers have internalized this calculation and continue to probe for it. 107 million hits represents sustained, systematic exploitation of that gap.

Log4Shell is joined in the professional services threat landscape by a broader web application attack surface. Directory traversal, malformed request probes, and remote code execution signatures account for 72% of all IPS volume in the sector. Professional services firms host client portals, extranet platforms, and SaaS integrations that attract automated scanning at scale. The web application perimeter is broad and, in many firms, insufficiently monitored.

107M

LOG4SHELL HITS, 7TH BY VOLUME

2.5 yrs

SINCE PUBLIC DISCLOSURE AND PATCH

What protection looks like in practice.

The professional services sector has an access problem. Client portals, remote work platforms, VoIP infrastructure, and MSP management tools all require external access by design. The traditional response — VPN-based broad network access — turns every one of those access points into a potential full-network breach. A stolen credential for a client portal should not become a path to billing systems, document stores, or in the case of an MSP, client environments.

Zero Trust Network Access addresses this at the architecture level. Access is granted to specific applications, not to the network behind them. Identity and device posture are verified continuously, not just at login. A compromised credential from a phishing attack or credential-stuffing campaign no longer unlocks the environment. It unlocks a single application, with no lateral path beyond it.

For MSPs, the stakes are higher. SonicWall Cloud Secure Edge applies the same Zero Trust principles to multi-tenant managed environments, allowing MSPs to enforce application-level access controls across client environments without granting broad network trust. A credential compromise at the MSP level does not cascade into client environments.

A stolen credential should not unlock the client file.

THE OLD MODEL | VPN

- One credential verified at the perimeter
- Broad network access granted — client files, billing, communications
- Never re-verified
- Lateral movement: unrestricted

THE ZERO TRUST MODEL

- Identity and device posture verified continuously
- Application-level access only
- Client data access scoped by policy
- Lateral movement: blocked

Zero Trust in practice: a legal industry case study.

XimpleIT, a Colorado-based MSP specializing in legal industry clients, deployed SonicWall Cloud Secure Edge across its law firm customer base after a client breach caused by an unpatched legacy VPN. The incident exposed a gap common across the sector: as legal work moved to cloud-based applications and hybrid environments, the underlying access architecture had not kept pace. Legacy VPN access gave attackers a single point of entry and, once inside, no further enforcement, segmentation, or visibility into where a compromised credential had traveled.

By replacing that model with Cloud Secure Edge, XimpleIT now verifies both user identity and device posture before granting access, eliminating implicit trust and preventing lateral movement across client environments. For a vertical built on privileged communications and client records, that shift from broad network trust to application-level, continuously verified access is precisely the architecture change this brief recommends.

> "Having somebody, a real person, who checks in regularly, provides assistance implementing new solutions, and helps us win deals is a big differentiator. That is rare. SonicWall gives us the platform and the partnership to walk into a law firm and tell them, with confidence, that their data is protected, not just monitored."
>
> **JUAN SERNA, FOUNDER AND IT DIRECTOR, XIMPLEIT**

WHY THIS MATTERS

The legal sector's exposure is not hypothetical. It took one unpatched VPN and one breach to force the shift this brief recommends across all of professional services, and Zero Trust architecture closed exactly the gap this data shows attackers are exploiting.

ACTIONABLE RECOMMENDATIONS

Five actions to take now.

1

HARDEN SIP INFRASTRUCTURE AND RESTRICT EXPOSED ENDPOINTS

Block SIP ports 5060 and 5061 where VoIP is not required on public-facing interfaces. Enforce SIP digest authentication on all endpoints. Audit any VoIP infrastructure with internet exposure and move to session border controllers with proper authentication enforcement. 332 million exploitation attempts indicate this is not a theoretical risk.

2

REMEDIATE LOG4J ACROSS ALL JAVA-BASED MIDDLEWARE

Inventory every Java-based system in the environment — document management, billing, case management, client portals — and patch or isolate on a defined schedule. Where patching is not immediately feasible, deploy WAF rules and network-level isolation as interim controls. 107 million hits means attackers are not waiting for the next maintenance window.

3

REPLACE BROAD VPN ACCESS WITH APPLICATION-LEVEL ZERO TRUST

A stolen credential in a professional services environment should not grant access to client files, billing records, or privileged communications. Application-level Zero Trust enforces least-privilege access per application and eliminates lateral movement paths that VPN architectures leave open by design.

4

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

Ten simultaneous ransomware families across 460 organizations indicates the sector is broadly targeted with both automated and human-operated campaigns. Immutable, offline backups are non-negotiable. Pair with endpoint detection and response that supports behavioral detection and automatic rollback to limit dwell time and blast radius.

5

APPLY ZERO TRUST TO MSP CLIENT ENVIRONMENT ACCESS

An MSP breach is not one breach. Enforce application-level access controls on all managed client environments. Administrative access to client infrastructure should require continuous identity verification, device posture checks, and should be scoped to specific systems rather than granted at the network level.

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.

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

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