MARCH 31, 2026 GENERAL, THREAT INTELLIGENCE

FROM THREAT REPORT TO PROTECT REPORT: WHAT THE 2026 SONICWALL CYBER PROTECT REPORT MEANS FOR SMBS AND THE PARTNERS WHO PROTECT THEM

by Michael Crean

Shifting from threat tracking to protection outcomes, the 2026 Cyber Protect Report reveals why SMBs remain exposed and how partners can close the gap.

Every year, SonicWall publishes its annual research to help partners and their customers understand the threat landscape. This year, we did something different.

We asked a harder question: instead of cataloging what attackers are doing, what if we focused on what actually keeps businesses protected? The result is the 2026 SonicWall Cyber Protect Report, a deliberate reframing of our annual research around protection outcomes and a stark look at why so many organizations are still losing ground despite significant security investment.

What we found wasn't surprising to our teams in the field. But it should be a wake-up call for every small- to mid-sized business (SMB) and every MSP who protects them.

THE THREAT LANDSCAPE IS GETTING MORE PRECISE, NOT JUST BIGGER

Before we get to the "why," it helps to understand what the data is telling us about the "what."

High and medium severity attacks surged 20.8% to 13.15 billion hits, meaning that while overall volume held steady, the attacks that actually matter increased sharply. Attackers aren't swinging more often. They're *connecting* more often.

A few other numbers worth sitting with:

- Automated bots generate more than 36,000 vulnerability scans per second, making up more than half of all internet traffic. For SMBs, the question isn't whether they'll be scanned. It's whether they'll be found vulnerable when they are.
- IoT attacks rose 11% to 609.9 million hits, peaking in December in line with continued botnet activity. Every unsecured camera, router, or connected device on an SMB network is a potential foothold.
- And then there's Log4j. Four years after its public disclosure, it still generated 824.9 million IPS hits in 2025. Old vulnerabilities don't retire. Attackers keep using them because organizations keep leaving them unpatched.
- Finally, ransomware fell 33.9% overall, but that headline obscures a more troubling reality. Ransomware was present in 88% of SMB breaches in 2025, compared to just 39% at large enterprises.

THE SEVEN DEADLY SINS OF CYBERSECURITY

Here's what our researchers kept coming back to while analyzing breach investigations, security assessments and incident reviews: the organizations that suffered most weren't victims of sophisticated, novel attacks. They were victims of gaps they already knew about or should have.

We've named these the Seven Deadly Sins. Not because they're obscure, but because they're not. They're operational failures hiding in plain sight.

Sin 1: Ignoring the Fundamentals - Identity, cloud and credential compromise account for 85% of actionable security alerts. The attacker's preferred front door isn't a zero-day. It's a stolen password walking through an unguarded entrance. The fundamentals aren't hard to fix. They're hard to sustain.

Sin 2: False Confidence - Ransomware was present in 88% of SMB breaches last year. The "we're too small to be a target" assumption isn't just wrong. It's dangerous. And it's not the only trap: 80% of IT leaders claim they can contain an incident in under eight hours, while IBM data shows attackers dwell undetected for an average of 181 days. Those two numbers cannot both be true.

Sin 3: Overexposed Access - 48% of breaches involved compromised VPN credentials as the initial access vector. Once inside a flat network, attackers don't need sophisticated tools. They just need time. Average lateral movement occurs within 48 minutes of initial compromise. In the fastest observed cases, full propagation took 18 minutes.

Sin 4: Reactive Security Posture - The average breach goes undetected for 181 days. With 44% of alerts going uninvestigated due to alert fatigue and talent constraints, attackers aren't waiting to be found. Without 24/7 monitoring and proactive threat hunting, they don't have to.

Sin 5: Cost-Driven Security Decisions - A single SMB breach can exceed $4.91 million in downtime and recovery. Organizations with incident response plans save an average of $1.23 million per breach. Cheap security isn't cheap. It's just cheap upfront.

Sin 6: Reliance on Legacy Access Models - VPN CVEs grew 82.5%, with 60% rated high or critical. Yet VPNs remain the default for most SMBs, authenticating once and then trusting everything after. Attackers don't need to break through the perimeter. They just need valid credentials.

Sin 7: Chasing Hype Over Execution - The average enterprise runs 45 security tools. Nearly half of security professionals spend more time maintaining them than defending against attacks. AI is a powerful force multiplier, but it multiplies what's already there, and in environments where the fundamentals are broken, it has nothing to work with.

WHAT THIS MEANS IF YOU'RE AN SMB

The good news is that most of these gaps are fixable without a major budget overhaul. They don't require ripping out existing infrastructure or buying the latest platform. They require intentional action, applied consistently.

Enforce MFA on every account with no exceptions. Establish a patch process that treats internet-facing systems as urgent. Audit admin privileges and remove access that can't be justified by current role. Segment your network so a single compromised credential can't reach everything. Test your backups. Run a tabletop exercise. Know what your tools are actually covering.

None of this is new. That's the point. The organizations that are most exposed aren't missing technology. They're missing follow-through.

WHAT THIS MEANS IF YOU'RE AN MSP OR MSSP

The 2026 Cyber Protect Report is designed with partners in mind. The Seven Deadly Sins framework gives MSPs and MSSPs a clear, business-language structure for conversations with SMB decision-makers who don't think in terms of CVEs and alert queues, but who absolutely understand downtime, missed payroll and reputational damage.

Use this data to elevate your conversations. The gap between what SMB leaders believe about their security posture and what's actually true is one of the most consistent findings in breach investigations. Helping your customers close that gap through honest assessment, validated controls, and proactive monitoring is where your value as a trusted partner is most clearly demonstrated.

SonicWall's portfolio is built to help you do exactly that. SonicSentry MXDR delivers 24/7 SOC and NOC-backed managed detection and response. Cloud Secure Edge (CSE) replaces legacy VPN architecture with identity-first, application-level access. And SonicPlatform unifies management across the entire environment so partners have the visibility to stay ahead of what's coming.

These Seven Deadly Sins aren't a condemnation. They're a road map, and a conversation starter that turns security from a line item into a business priority.

PROTECTION IS THE POINT

Cybersecurity isn't abstract. It's about making sure a business can pay its employees on time, serve its customers without interruption and grow without fear. For the SMBs that represent 99% of U.S. businesses and nearly half of private sector employment, the stakes couldn't be higher.

The 2026 SonicWall Cyber Protect Report exists because we believe partners deliver the best security outcomes, and because we believe SMBs deserve the same level of protection as the enterprises they supply, serve and support.

Download the full report today and see what protection looks like when the fundamentals are finally covered.

SHARE THIS ARTICLE

AN ARTICLE BY

Michael Crean

EXECUTIVE VICE PRESIDENT, MANAGED SECURITY SERVICES

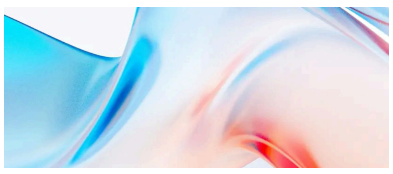
Michael Crean currently leads the Managed Security Services team at SonicWall, where he came aboard following SonicWall's acquisition of leading MSSP Solutions Granted Inc. Crean, a U.S. Army combat veteran, founded Solutions Granted Inc. in 2001. He saw the need to bridge the gap between IT and IS with solid security offerings and strong, cost-effective solutions. His relentless commitment to providing security that met corporate goals and compliance standards caused immediate growth; at the time of its acquisition, Solutions Granted provided managed security offerings to thousands of customers worldwide. He is now helping to empower MSP partners with managed detection and response (MDR) and other solutions.

RELATED ARTICLES

MARCH 26, 2026

Partner Power News - March 2026: Outcomes. Acceleration. Opportunity.

Read More



MARCH 18, 2026

Your Immune System Doesn't Wait. Neither Should Your Security.

Read More