SONICWALL

Cyber Threats on the Rise

How Zero Trust Secures Your Business

The Modern Threat Landscape

259%
Ransomware Spike

Ransomware spike in LATAM, contributing to a dramatic rise in attack volume across the Americas—NOAM saw an **8% increase**

452%
Surge in SSRF Attacks

1 in 3
Cyber Insurance Claims Involve BEC

198M
Healthcare records **hit by ransomware in 2024**

AI helps attackers scale phishing, scan for vulnerabilities, and bypass outdated defenses faster than ever.

Top Attack Vectors

Business Email Compromise (BEC)
Impersonated emails trick staff into wiring money or revealing credentials.

Mobile and BYOD Attacks
Phishing via QR codes, fake apps, or "MFA fatigue" on personal devices.

Privilege Escalation
Attackers use **built-in OS tools** (e.g., **PowerShell**) to gain admin rights undetected.

Malware and Ransomware
Locks or steals data; **demands ransom** to restore operations.

SSRF (Server-Side Request Forgery)
Forces web apps to call internal systems, **bypassing perimeter security**.

38% of exploited Microsoft vulnerabilities in 2024 allowed privilege escalation.

Zero Trust Addresses Modern Threats

Verify Everyone
Continuous checks on user identity, device posture, and real-time risk.

Limit Lateral Movement
Segmentation ensures that a single breach can't spread network-wide.

Real-Time Monitoring
Suspicious activity triggers instant alerts or automated blocks.

The Benefits

Stop BEC and Malware
Strong MFA and device verification keep attackers out.

Contain Ransomware
Segmentation isolates compromised endpoints, halting spread.

Prevent SSRF Exploits
App-level controls let only valid requests reach internal services.

Secure BYOD
Conditional access ensures unpatched or risky devices can't log in.

Key Steps to Start

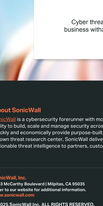
Map Out Critical Assets
Know what you must protect first.

Enable MFA and Posture Checks
Only healthy devices + verified users get in.

Segment Your Network
Don't let attackers roam if one machine is hit.

Use Real-Time Threat Intelligence
Leverage SonicWall's cloud analytics to spot emerging attacks instantly.

How SonicWall Cloud Secure Edge Tackles These Threats



User and Device Verification
Enforces continuous user and device verification before granting access.

Least-Privilege Access Policies,
Applies least-privilege access policies, reducing attack surface and lateral movement opportunities.

Real-Time Threat Intelligence
Blocks malicious websites, phishing pages and risky domains using real-time threat intelligence.

Web Usage Policies
Enforces web usage policies to reduce risk from high-risk web traffic.

Ready to Learn More?

Explore SonicWall Cloud Secure Edge

Download Our Whitepaper on Zero Trust essentials

> Cyber threats aren't slowing down—protect your business witha Zero Trust model that keeps attackers locked out.

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