SONICWALL®

WHITE PAPER

Critical Security Threats and the Need for ZTNA

How Evolving Cyberattacks Demand a Zero Trust Approach

Table of Contents

SONICWALL®

1

Executive Summary

Cyber threats have become more **frequent** and **sophisticated**, targeting organizations of all sizes across all industries. From business email **compromise** to **ransomware** and **privilege escalation**, adversaries are capitalizing on the **weaknesses of traditional**, **perimeter-based defenses**. Recent data from SonicWall reveals:

- **Business Email Compromise** is tied to **1 in every 3 insurance claims**.
- **Ransomware** continues to rise, with a **259% increase** in certain regions (e.g., Latin America) and **198 million patient records** affected in 2024 alone.
- **Server-side request Forgery (SSRF)** has seen a **452% surge** in incidents, driven partly by **AI-powered vulnerability scanning**.

These figures underscore that **attackers can**, **and will**, **gain initial access and move laterally**. Once inside, they rely on tactics like **privilege escalatio**n or **"living-off-the-land"** (LOLBins) to deepen control without triggering alerts. Meanwhile, employees increasingly work remotely using **unmanaged mobile devices**, broadening the attack surface.

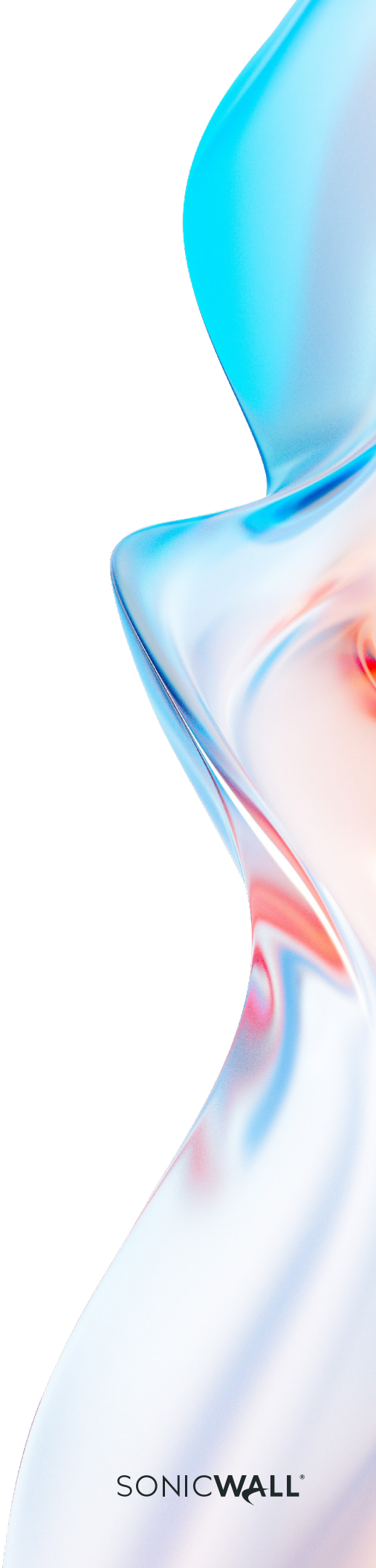
Zero Trust Network Access (ZTNA) is an essential strategy: it presumes **no implicit trust**—whether a user is on the corporate LAN or remote—and continuously verifies identity, device posture, and risk signals. SonicWall's **Cloud Secure Edge** solution aligns with this model, offering **segmentation**, **device trust**, **threat intelligence**, and **real-time visibility** to mitigate these rising threats.

259%

Ransomware increase in certain regions

198

million patient records affected



SONICWALL®

2

Evolving Threat Landscape

Historically, organizations relied on strong perimeter defenses—firewalls designed to keep threats "outside." In today's cloud-enabled, hybrid-work environment, users are often outside the protection of the corporate network—making them more vulnerable to phishing attacks, stolen credentials, and application exploits. Once inside, attackers can move laterally with ease if the network lacks proper segmentation and strong identity verification.

Key Drivers of Increased Threats

Hybrid Work
Employees and contractors access systems from anywhere—often using their own personal devices.

Proliferation of Cloud Services
Mission-critical apps (e.g., Microsoft 365, Google Workspace) must be accessible over the internet, widening the potential attack surface.

Automation & AI
Adversaries use large language models (LLMs) to develop sophisticated phishing emails, generate exploit scripts at scale, and automate vulnerability discovery.

SONICWALL®

3

Key Threat Vectors

3.1 Business Email Compromise (BEC)

BEC is a highly effective social engineering tactic where **criminals impersonate** a trusted individual—often an executive—to trick employees or partners into **transferring funds** or **revealing sensitive data**.

Impact

- A primary driver of **financial losses**; tied to **1 in 3 cyber insurance claims** in 2024.
- Difficult to detect because attackers leverage **legitimate email accounts** (stolen credentials or forwarding rules).

Common Attack Pattern

- Attackers gain **initial email account access** (phishing or password reuse).
- Set up **stealth forwarding rules**, sometimes deleting forwarded messages from the victim's inbox.
- Await **financial transactions** (invoices, wire transfers) to divert or impersonate internal approvals.

Zero Trust Mitigation

- Enforce **adaptive MFA** on all corporate email access.
- Restrict email access to **managed devices** or devices with a **valid certificate** and acceptable posture.
- Monitor for **anomalous login** locations (a.k.a. **"impossible travel"** flags).

259%

rise in ransomware attacks

198

million patient records affected

3.2 Malware & Ransomware

Ransomware encrypts data and demands payment for decryption keys, while malware can steal information or **establish persistence** for deeper breaches.

Recent Trends

- **There was a 259%** rise in ransomware attacks in some regions.
- **198 million** healthcare patient records were affected by ransomware in 2024 alone.
- Attackers use **EDR evasion** techniques, often leveraging **PowerShell** (LOLBins) to avoid detection.

Propagation Tactics

- **Phishing links or attachments** deliver malicious payloads.
- Exploiting **unpatched systems**.
- Lateral movement across **flat networks**.

Zero Trust Mitigation

- **Micro-segmentation** and access control ensure an infected endpoint cannot spread ransomware laterally.
- **Automated URL filtering** blocks malicious sites.
- **Endpoint posture checks** verify that devices run up-to-date EDR and patches before granting network access.

3.3 Server-Side Request Forgery (SSRF)

SSRF attacks trick web apps into making **unauthorized requests** to internal services. Many frameworks (WordPress, Drupal, etc.) have had SSRF vulnerabilities, allowing attackers to:

- **Exfiltrate** internal data.
- **Scan internal network** ports.
- **Abuse "metadata" services** in cloud environments (e.g., AWS, Azure).
- **452% Growth**:
  - Modern **AI-driven** tools can **mass-scan** for SSRF entry points.
  - Once found, attackers pivot within a supposedly "internal" network.

- **Zero Trust Mitigation**:
  - Limit access to **internal application services** only for **authenticated**, authorized users and devices.
  - **Continuous patching** of web frameworks.
  - **App-layer** controls (e.g., WAF) integrated with a Zero Trust architecture to **deny unauthorized internal requests**.

3.4 Mobile Attack Surface

As employees increasingly rely on **smartphones** and **tablets** for corporate tasks, attackers see an opening via:

- **Malicious QR codes**, fake productivity apps, or **phishing SMS**.
- **MFA fatigue**—bombarding users with repeated MFA requests until they approve out of habit.
- **Unpatched operating systems** or **jailbroken** devices lacking security controls.
- **Zero Trust Mitigation**:
  - Restrict application access to devices **meeting posture requirements** (e.g., not jailbroken, security patches up-to-date).
  - **Geolocation** or "impossible travel" analysis to detect unusual logins.
  - Conditional policies that may **limit certain high-risk operations** (e.g., code repository access) from mobile devices.

3.5 Privilege Escalation & Living-off-the-Land (LOLBins)

Attackers assume **initial compromise** is inevitable—often through stolen credentials or insider threats. Once inside:

Privilege Escalation

- Exploit OS vulnerabilities for **admin privileges**.
- In 2024, 38% of exploited Microsoft vulnerabilities were for **elevating privileges**.

Living-off-the-Land (LOLBins)

- Tools like **PowerShell** or **schtasks.exe** come pre-installed on Windows, making them **hard to detect**.
- Attackers can download additional malware, create backdoors, or exfiltrate data without using "traditional" malicious executables.

Zero Trust Mitigation

- Enforce **least privilege**: normal users do not get admin rights unless expressly granted.
- **Monitor** baseline usage of built-in tools to spot anomalies (e.g., suspicious PowerShell commands).
- Micro-segmentation ensures that even with elevated privileges on one system, **attackers cannot traverse** to critical assets without re-authentication and posture checks.

4

AI-Driven Cyber Threats

Attackers increasingly leverage **large language models** and AI automation to:

- Generate **highly sophisticated phishing** campaigns that mimic genuine communication.
- **Automate SSRF** and scanning for known exploits.
- Churn out scripts to evade endpoint detection.

Zero Trust is especially critical here because AI makes it faster and cheaper for attackers to launch **tailored** attacks at scale. Human defenders, meanwhile, benefit from **AI/ML-powered security tools**—like those in SonicWall's threat detection engine—that identify **unusual patterns** in network or user behavior.

5

Zero Trust: Principles & Benefits

Zero Trust assumes **no implicit trust**—inside or outside the corporate LAN. Instead, **every** request to access data or an application undergoes the following:

1. **User Authentication** (e.g., strong MFA tied to role-based policies)
2. **Device Verification** (posture checks, certificates, OS patch level)
3. **Continuous Authorization** (session-based risk scoring, anomaly detection)

Benefits

- **Reduced Attack Surface**: Attackers cannot freely move once inside.
- **Stronger MFA**: This minimizes the success of credential theft or phishing.
- **Comprehensive Visibility**: IT can see—and control—who is accessing what, from where, and on which device.

SONICWALL®

6

ZTNA in Action: How SonicWall Helps

SonicWall has developed a complete solution set across endpoint security, identity services, and threat intelligence that delivers **Zero Trust** access for real-time risk assessment.

6.1 SonicWall Cloud Secure Edge (CSE)

Unified Zero Trust Platform: Integrates identity, endpoint posture checks, and application access.

Policy-Driven Access: Granular **allow/deny** rules based on user, device, location, and resource sensitivity.

Dynamic Threat Detection: SonicWall threat research continuously updates detection signatures to block malicious URLs, suspicious files, and known exploit techniques (e.g., SSRF patterns).

6.2 Next-Generation Firewalls & Advanced Threat Protection

Layered Security: SonicWall NGFWs perform **deep packet inspection**, **SSL decryption, and advanced threat analysis**.

Captured Telemetry: Cloud intelligence from millions of data points worldwide helps identify new malware variants and malicious domains in real time.

7

Recommendations & Best Practices

Adopt a "Breach Mindset"

- Assume attackers already have initial access.
- Build micro-segmentation to minimize damage.

Enforce Strong MFA & Device Posture

- Eliminate reliance on static passwords and check device health (patch, AV/EDR running).

Monitor & Analyze User Behavior

- Detect anomalies like **MFA fatigue** approvals or suspicious PowerShell usage.

Regular Patch Management

- Close known vulnerabilities quickly, especially on internet-facing services.

Comprehensive Backup Strategy

- Ransomware thrives on unprotected backups.
- Secure offline or read-only copies are essential.

Leverage Threat Intelligence

- Use real-time data feeds (like SonicWall's) to block emerging threats.

Educate Your Workforce

- Frequent security awareness training prevents phishing, especially BEC.

SONICWALL®

8

Conclusion

Cyber threats—**BEC**, **ransomware**, **SSRF**, **privilege escalation**, **mobile exploits**—are rising in frequency and potency. Attackers exploit implicit trust wherever it's given, leveraging **AI** to scale and customize their attacks.

Zero Trust Network Access with continuous verification at every step is the proven strategy to mitigate these risks **and address security gaps of traditional networking solutions**. By combining strong identity management, device posture, network segmentation, and real-time threat intelligence, organizations can dramatically reduce the chance of a catastrophic breach.

SonicWall is dedicated to helping **organizations** adopt a holistic Zero Trust posture. Through solutions like Cloud Secure Edge, Next-Gen Firewalls, and SonicSentry, SonicWall integrates robust threat research, simplified policy management, and advanced analytics to defend critical assets against modern cyber threats.

9

Appendix: Practical Steps & Glossary

9.1 Practical ZTNA Implementation Steps

1. Identify & Classify Assets: Catalog your applications and data, mapping out who needs access.
2. Deploy a Pilot: Start with a pilot group (e.g., specific department) to fine-tune Zero Trust policies.
3. Establish Device Posture Requirements: Define minimum OS versions, endpoint protection standards, patch levels, etc.
4. Set Up MFA: Use app- or token-based MFA (avoid basic SMS if possible); integrate with IDP solutions.
5. Implement Micro-Segmentation: Separate critical databases or servers so that an intruder in one segment can't traverse to another.
6. Continuously Monitor: Use SIEM or SOC resources to watch for anomalous patterns and refine policies.

9.2 Glossary

- **BEC (Business Email Compromise)**: Impersonation of a trusted email account to initiate fraud.
- **MFA (Multi-Factor Authentication)**: Requires two or more factors (e.g., password + token) for access.
- **SSRF (Server-Side Request Forgery)**: Exploits an app's trust in itself to call internal services.
- **LOLBins (Living-off-the-Land Binaries)**: Legitimate OS utilities (PowerShell, etc.) used maliciously to avoid detection.
- **Zero Trust Network Access (ZTNA)**: A security framework that requires continuous verification of every user or device attempting to access resources.

For more information

Visit SonicWall.com to explore our Zero Trust solutions or learn more about how you can start your Zero Trust journey with our eBook, Zero Trust Made Simple: A Practical Guide for Modern Security.

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035 | Refer to our website for additional information.