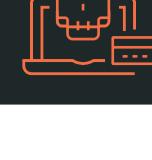
SONICWALL®

# Cyber Threats on the Rise

**How Zero Trust Secures Your Business** 



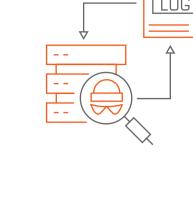
# The Modern Threat Landscape



Ransomware Spike Ransomware spike in LATAM, contributing

259%

to a dramatic rise in attack volume across the Americas—NOAM saw an 8% increase



452% Surge in SSRF **Attacks** 



Cyber Insurance Claims Involve BEC



Healthcare records hit by ransomware in 2024

bypass outdated defenses faster than ever.



# **Business Email Compromise (BEC)**

Top Attack Vectors



# **Mobile and BYOD Attacks**

Impersonated emails trick staff into

rights undetected.

**Privilege Escalation** 

Attackers use built-in OS tools

(e.g., PowerShell) to gain admin

Phishing via QR codes, fake apps, or

"MFA fatigue" on personal devices.



## to restore operations.

**Malware and Ransomware** 

Locks or steals data: demands ransom

**SSRF (Server-Side Request Forgery)** 



Forces web apps to call internal systems,

bypassing perimeter security.

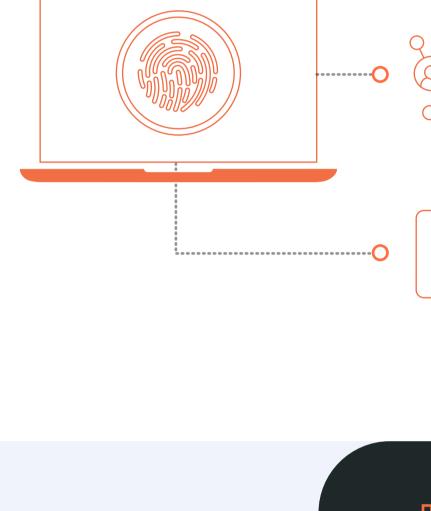
of exploited Microsoft vulnerabilities 38% in 2024 allowed privilege escalation.



# **Verify Everyone** Continuous checks on user identity,

Zero Trust Addresses

Modern Threats



## Segmentation ensures that a single breach can't spread network-wide.

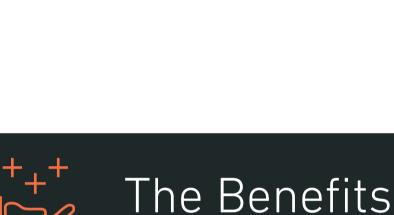
**Real-Time Monitoring** 

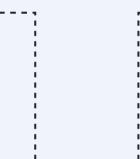
instant alerts or automated blocks.

Suspicious activity triggers

device posture, and real-time risk.

**Limit Lateral Movement** 





## **Contain Ransomware** Segmentation isolates compromised endpoints,

halting spread.

can't log in.

**Secure BYOD** 



**Stop BEC and Malware** 

**Prevent SSRF Exploits** 

App-level controls let only valid

requests reach internal services.

keep attackers out.

Strong MFA and device verification

**Map Out** 

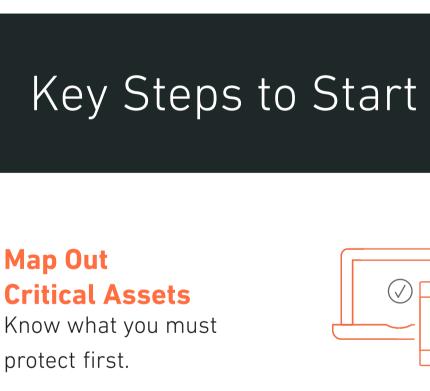
protect first.

**Segment** 

**Your Network** 

Don't let attackers roam

if one machine is hit.



 $(\vee)$ 

**Enable MFA and** 

**Posture Checks** 

Only healthy devices +

verified users get in.

**Use Real-Time** 

attacks instantly.

**Threat Intelligence** 

Leverage SonicWall's cloud

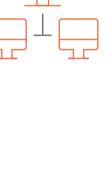
analytics to spot emerging

Conditional access ensures

unpatched or risky devices

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.

Enforces web usage policies to reduce risk from

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



## Ready to Learn More? **Explore SonicWall Cloud Secure Edge**

Download Our Whitepaper on Zero Trust essentials

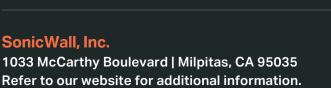
Cyber threats aren't slowing down—protect your business witha Zero Trust model that keeps attackers locked out.

**Web Usage Policies** 

high-risk web traffic.



actionable threat intelligence to partners, customers and the cybersecurity community.



**About SonicWall** 

SONICWALL®

www.sonicwall.com © 2025 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have

been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without

notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

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