

SOLUTION BRIEF

Traditional VPN solutions are broken—it's time to modernize.

Secure Remote Access Made Simple with CSE

Running a small- to medium-sized business (SMB) comes with enough challenges—managing customers, growing your team and keeping operations running smoothly—while also staying up to date with the latest technology. On top of all that, cyberattacks targeting SMBs are becoming more frequent at a rate that can no longer be ignored.

In fact, recent reports indicate that 43% of cyberattacks are aimed at small businesses, yet only 14% are adequately prepared to defend themselves.

It's no surprise attackers frequently target smaller firms, assuming many SMBs are not equipped to handle security breaches.

One of the most critical areas where SMBs should focus their security investments is in upgrading their remote access strategy to a secure, modern solution. As your business—and the world—transitions to cloud-first applications and supports a modern workforce that values flexibility to work in the office, at home or even at a coffee shop, ensuring secure access is essential.

For an SMB, malware, ransomware and beyond aren't just annoying issues—they're costly and devastating. Leading analysts in the cybersecurity industry estimate the average cost of an attack on SMBs can range from \$25,000 to as much as \$3 million. The good news: proactively securing your business is far less expensive (and far less stressful) than dealing with the aftermath of a cyberattack. Investing in solutions that offer comprehensive protection can help you avoid the steep costs, downtime and recovery challenges that follow an attack.

The Challenge: SSL VPNs Aren't Enough

Many SMBs still rely on traditional SSL VPNs to enable remote work. However, VPN devices are a frequent target for attackers due to their vulnerabilities and limitations. With two out of three attackers infiltrating networks using stolen credentials, VPNs become prime entry points for lateral movement across network infrastructure to install malware, steal sensitive data or launch ransomware attacks. VPNs often fail to assess device posture or provide granular security controls, making compromised credentials a major risk.

If you've been using an SSL VPN to enable remote work, you may have noticed some frustrating issues:

- **Security Gaps:** SSL VPNs are frequently exploited within just 48 hours of a vulnerability being discovered. Meanwhile, organizations typically take 120 to 150 days to apply patches. Attackers often scan for unpatched SSL VPN devices and exploit known vulnerabilities to gain unauthorized access to your data and network.
- **Slow Performance:** SSL VPNs are often sluggish, frustrating employees and impacting productivity—especially as your business scales.
- **Difficult to Manage:** VPN clients can be challenging to deploy, maintain and troubleshoot, particularly if you lack dedicated IT resources.

While these pitfalls pose serious risks, there's a better way to stay secure and provide a seamless remote access experience for your employees.

The Solution: Modern Secure Remote Access as a Practical First Step Toward Zero Trust

For SMBs looking to improve their security posture without having to overhaul their infrastructure overnight, SonicWall's Cloud Secure Edge (CSE) provides a powerful starting point with modern Secure Remote Access. While terms like "Zero Trust" and "Zero Trust Network Access (ZTNA)" can feel complex, modern Secure Remote Access delivers the core principles of Zero Trust in a way that is approachable and easy to adopt. Instead of relying on legacy VPN architectures that grant broad network access after a single authentication, CSE

applies least-privilege access and continuous verification to protect users, applications, and data.

With cloud-delivered Secure Remote Access, organizations can eliminate many of the operational and security challenges associated with traditional SSL VPNs while ensuring users can securely access the resources they need without disruption. Rather than maintaining and patching internet-facing VPN infrastructure, businesses can rely on SonicWall to deliver a modern, centrally managed access architecture that reduces risk, simplifies management, and bridges the gap between legacy remote access models and a Zero Trust-based approach.

Why Start With Modern Secure Remote Access?

- **Simple Deployment and Centralized Management:** Already using SonicWall firewalls? CSE integrates seamlessly into existing environments, making deployment fast and straightforward. Because it is cloud-delivered, ongoing updates and infrastructure maintenance are handled centrally, reducing administrative burden and freeing IT teams to focus on core priorities.
- **User-First Solution:** CSE is designed for simplicity. Users connect securely to the applications and resources they need without managing complex VPN clients or manual connection processes. The result is a streamlined remote work experience that improves productivity while maintaining strong protection.
- **Continuous Verification Based on Zero Trust Principles:** Unlike traditional VPNs that authenticate users once and grant broad access, CSE continuously verifies user identity, device posture, and session context. This significantly reduces the likelihood that compromised credentials lead to unrestricted network access.
- **Granular, Least-Privilege Access Control:** Users are connected only to the specific applications and resources required for their role, not the entire network. By limiting access at the application level, organizations reduce attack surface and restrict lateral movement, even if a device is compromised.
- **Built to Scale With Your Business:** CSE scales easily with your business as you add users and expand your cloud presence, ensuring your security strategy evolves with your organization without requiring hardware refresh cycles or complex reconfigurations.

A Partner in Your Zero Trust Journey

Adopting Zero Trust does not require a disruptive overhaul. It begins by modernizing how users access private applications and data. SonicWall CSE enables SMBs to take that first step by replacing legacy VPN architectures with cloud-delivered Secure Remote Access built on Zero Trust principles. Organizations immediately benefit from stronger security controls, reduced management complexity, and a faster, more reliable remote access experience. Over time, businesses can expand their Zero Trust capabilities as needed, ensuring that every access request is verified, authorized, and continuously evaluated based on risk.

Secure Remote Access, Built for SMBs

SMBs need remote access solutions that are simple to deploy, affordable to manage, and strong enough to defend against modern threats. SonicWall CSE delivers cloud-delivered Secure Remote Access that protects users, applications, and data wherever they reside — without the operational overhead of traditional VPN infrastructure. Legacy VPNs were built for a different era. Modern Secure Remote Access is designed for today's distributed workforce and evolving threat landscape.

Don't let outdated VPNs put your business at risk. Connect your users securely and seamlessly to the resources they need. [Contact SonicWall](#) today for a personalized demo and see how much easier secure remote access can be.

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035 | [Refer to our website for additional information.](#)

© 2026 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.

Solution Brief - Secure Remote Access Made Simple with CSE - 12119

sonicwall.com



SONICWALL®