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: VPNaaS as a Gateway to 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 VPN-as-a-Service (VPNaaS). While you may have heard buzz around "Zero Trust" and "Zero Trust Network Access" (ZTNA), VPNaaS offers a less complex and intimidating entry point to a modern security approach.

With VPNaaS, you can alleviate the struggles commonly experienced with SSL VPNs while gaining peace of mind knowing your users can securely access what they need without disruption. Confidently rely on—and outsource—your VPN needs to SonicWall to deliver a modern solution that bridges the gap between traditional remote access models and a Zero Trust approach.

Why Start With VPNaaS?

- **Easy Deployment and Management:** Already using SonicWall firewalls? CSE integrates seamlessly, making deployment fast and simple. CSE runs efficiently in the background, improving the user experience compared to VPNs that require clients and manual connections.
- **User-Friendly Experience:** CSE's VPNaaS solution is designed for simplicity. Businesses can outsource their VPN needs for less stress and more security. Employees enjoy a seamless remote work experience without needing to manage VPN clients or connections.
- **Enhanced Security With Zero Trust Principles:** Unlike traditional VPNs that authenticate users once, our VPNaaS continuously verifies identity and device health. This dramatically reduces the risk of compromised credentials leading to full network infiltration.
- **Granular Access Control**: CSE's VPNaaS ensures users only connect to the specific apps and resources they need. Even if a device is compromised, the risk to your entire network is minimized.
- **Built for Growth:** CSE scales easily with your business as you add users and expand your cloud presence, ensuring your security strategy evolves with your organization.

A Partner in Your Zero Trust Journey

SonicWall CSE empowers SMBs to embrace a Zero Trust strategy by starting with VPNaaS. By adopting VPNaaS, businesses can immediately see the benefits of improved security, reduced management complexity and a faster, more reliable remote access experience. Over time, businesses can partner with SonicWall to expand CSE's capabilities and adopt full ZTNA principles—ensuring every access request is verified and authorized.

Secure Remote Access, Built for SMBs

As an SMB, you need remote access solutions that are simple, affordable and designed to keep your business safe. SonicWall CSE's VPNaaS gives you peace of mind knowing your users can securely connect to the resources they need, wherever they are.

Don't let outdated VPNs put your business at risk. Let us connect your users safely and seamlessly to what 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.