

CSE Secure Private Access for Enterprises

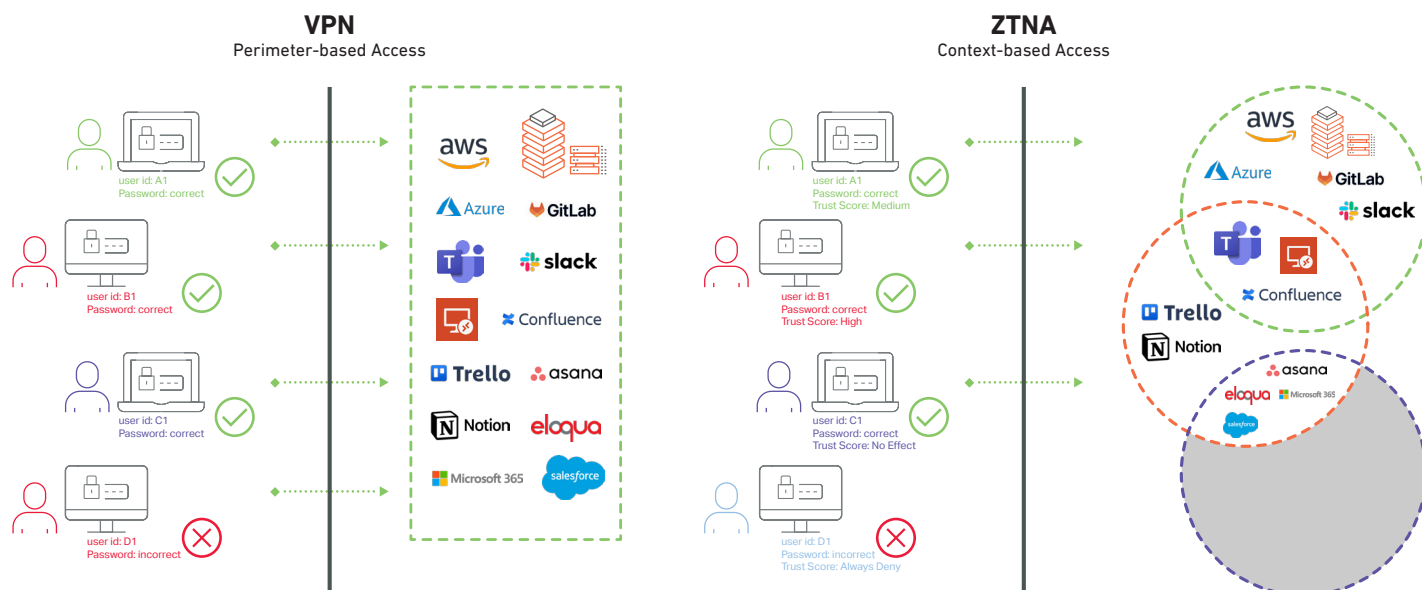
Empower your hybrid workforce while reducing business risk, improving productivity and lowering cost and complexity

What is CSE Secure Private Access?

Cloud Secure Edge (CSE) is SonicWall's all-in-one solution designed to deliver secure and scalable access to applications and resources users need across hybrid, multi-cloud and SaaS applications for modern workforces. Whether connecting remotely or on-prem, Secure Private Access (SPA) leverages zero-trust principles to authenticate users and devices before granting access, ensuring minimal attack surfaces.

Why Now?

The changing network landscape is forcing enterprises to modernize their approach and adopt network and security solutions that work together to ensure secure, seamless and scalable remote access. Legacy network security approaches are no longer sufficient to meet the demands of today's hybrid workforces. Furthermore, traditional SSL VPN solutions are complex to manage, vulnerable to cyber threats and often degrade performance as workforces become more distributed. These outdated networking architectures create gaps that expose businesses to increased risk and operational inefficiencies. Instead, by adopting a ZTNA solution like Secure Private Access, enterprises can deliver secure and reliable access to all their users anywhere and anytime. By continuously verifying that the user and the resource they're trying to access are safe, your users can experience uninterrupted productivity and collaboration.



Benefits:

- **Address VPN Security Gaps**
Reduce the attack surface and lateral movement caused by the limitations of legacy VPN solutions. Enable stronger and more granular security controls with zero-trust principles.
- **Secure High-Risk Users (Third parties, BYOD, M&A)**
Provide third parties simple, secure access to only the specific resources they need without over-provisioning. In addition, management of access is simple with groups and roles that can be pre-identified and applied as necessary from one central console.
- **Deliver Superior User Experience**
Improve performance and reduce the latency of your users' remote connectivity. Secure Private Access works transparently in the background with no user training required to successfully access applications.

Outcomes:

- **Reduce Business Risk**
Minimize the risk of data breaches, ransomware and insider threats by continuously verifying users and device health according to your policies. This not only prevents attackers and unauthorized users from moving across your network – it also helps mitigate the damage if they do gain access.
- **Improve Productivity**
Ensure users can access critical business applications securely and without disruption, driving efficient workflows.
- **Lower Costs and Complexity**
Save on the costs of traditional VPN hardware maintenance. Reduce the complexity of traditional VPN policy configurations that are needed to expand and deploy as your organization grows. By using a solution that unifies networking and security, organizations can decrease the complexity that comes along with ensuring safe, reliable and fast remote connectivity.

See how Lemonade modernized its remote access solution and see the above outcomes and benefits with Secure Private Access [here](#).

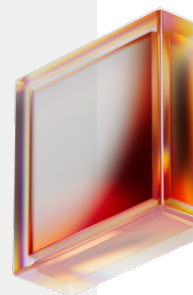
How Does CSE Compare with Traditional VPNs

Use Case	Traditional SSL VPNs	SonicWall CSE SPA
Performance	Routes traffic through VPN servers, causing slowdowns and poor user experience.	Intelligent routing streamlines user-to-application connections at the nearest point of presence to minimize delays and speed up workflows.
Security	Grants broad access once authenticated, allowing bad actors to fully infiltrate your entire network.	Adopts Zero Trust model which continuously authorizes users, devices and context to ensure that compromised users cannot move laterally across your network.
Cost Efficiency	Expensive hardware and ongoing maintenance	No expensive VPN hardware to maintain, saving valuable time and resources. Once CSE is deployed, you can immediately see the ROI with low TCO.
Scalability	Difficult and expensive to scale. Complex configurations needed to expand.	Cloud-based design means it's easy to scale effortlessly as your team grows.
Complexity of Deployment/Management	Often requires complex firewall and VPN policy configurations that are prone to misconfigurations, leading to potential breaches.	Easy cloud-based setup and management.
User Friendly	Requires users to constantly log in and out of VPN clients. Users need to be trained to properly utilize the VPN, which can be a huge headache.	CSE runs transparently in the background with little to no action or training required of end users.

Partner with SonicWall to Empower Modern Workforces

CSE Secure Private Access offers a modern alternative for enterprises seeking to replace outdated network security approaches and future-proof their organization. With secure and user-friendly remote access capabilities, Secure Private Access empowers organizations to embrace modern workforces confidently while maintaining robust security and productivity.

[Reach out to SonicWall](#) to get a personalized demo.



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®

© 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.