

Cloud Secure Edge

Zero Trust. Every Agency. Every Location.

What Is SonicWall Cloud Secure Edge?

SonicWall Cloud Secure Edge (CSE) is a cloud-native Security Service Edge (SSE) platform that consolidates ZTNA, Secure Web Gateway (SWG), CASB, and VPN-as-a-Service into one per-user subscription. No appliances. No controllers. Managed from a single cloud console.

CSE integrates with existing SonicWall firewalls out of the box and supports multi-tenant management — ideal for agencies and the MSPs that serve them. Continuous trust verification, device posture checks, and audit-ready logging satisfy compliance mandates without added complexity.

ZTNA / VPNaaS | Secure Web Gateway | CASB | DNS Filtering | Audit-Ready Logging | FW Integration

1 Government Agencies:
Prime Ransomware Targets

2 CJIS, StateRAMP, and NIST
Compliance Required

3 Legacy VPN Can't Protect
Distributed Agencies

Why Sell CSE to State and Local Government?

State and local agencies are prime ransomware targets — and they must protect essential services while working within tight budgets and complex regulatory requirements. Legacy VPNs often create security gaps, limit visibility, and require costly hardware to support distributed teams and locations. SonicWall Cloud Secure Edge (CSE) delivers scalable, zero-trust access with least-privilege controls and comprehensive audit logging — helping agencies support CJIS, HIPAA, and state-specific cybersecurity requirements from one easy-to-manage cloud console, at a predictable per-user cost.

COMPLIANCE READY

NIST / CJIS

Zero trust controls satisfy mandates

NO HARDWARE REQUIRED

Low TCO

Cloud-native, per-user subscription



If we hadn't deployed SonicWall, critical county departments would have been shut down.

Jay Terrell, CTO
Fulton County Government

Key Use Cases

- **When the Invoice Email Is Actually an Attack**

A county finance clerk clicks a link in what looks like a vendor invoice. The phishing page is blocked before it loads — stopping credential theft before the clerk ever knows it happened.

- **Regulatory Compliance — NIST, HIPAA, PCI-DSS**

A detective queries a criminal history record from a personal laptop. Device posture verified, access granted, and every query is automatically logged — meeting CJIS audit requirements.

- **Secure Access to Citizen & Case Records**

A social services officer opens a citizen's case file while working remotely. Identity and device trust are verified before access is granted, and every session is automatically logged to meet compliance requirements.

Key Benefits

- **Replaces Legacy VPN — No Rip-and-Replace**

Guided 3-step setup wizard. First secure tunnel live in 15 minutes. Connects directly to existing SonicWall firewalls out of the box.

- **Satisfies State Specific Cybersecurity Requirements**

Continuous device posture verification, audit-ready logs, and least-privilege access controls are built in — not bolted on.

- **Single Console for All Agencies and Sites**

Multi-tenant cloud management lets IT oversee every office, agency, and remote user from one dashboard — no per-site hardware to manage or patch.

- **Shadow IT Visibility Included**

CASB surfaces unauthorized cloud applications accessed by staff, giving IT full visibility into what is running across the government network.

- **Per-User Subscription Fits Government Budgets**

Predictable annual cost. No capital expenditure. Scales with headcount. Avoids lengthy procurement cycles tied to hardware refresh.

- **Zero Hardware — Low TCO for Lean IT Teams**

No appliances to rack, patch, or replace. Small IT departments can manage the full deployment without adding headcount.

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.

EN_NOAM_CSE_State and Local_OnePager_SonicWall_12447

sonicwall.com



SONICWALL®