SONICWALL®

WHITE PAPER

Delivering Better Security and Business Outcomes

The Challenge

As organizations increasingly move their applications, resources, and data to cloud-based environments, the traditional security perimeter is becoming obsolete. The shift to remote work and the rise of distributed, cloud computing has created a new attack surface that is difficult to protect with traditional perimeter security solutions. Cloud-based environments and Software-as-a-Service (SaaS) vendors all rely on different authentication and authorization methods resulting in security and usability compromises. To address this challenge, a new approach to security and access is needed, and that approach is the modern Security Service Edge (SSE).

The Cloud Secure Edge security platform extends our industry-leading Zero Trust Network Access (ZTNA) solution providing a device-centric Security Service Edge (SSE) which secures access to applications and resources from anywhere while empowering the modern workforce.

In this whitepaper, we will explore our modern approach to SSE in detail, including its architecture, benefits, and how it can help organizations improve their security posture in today's rapidly evolving threat landscape. By the end of this whitepaper, you will have a clear understanding of how Cloud Secure Edge's device-centric SSE helps organizations protect against modern cyber threats.

Background

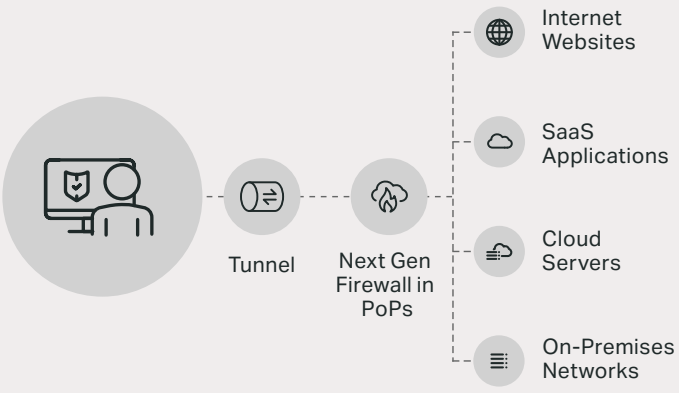
Organizations have relied on legacy approaches to securing their network perimeter. They've also depended on SaaS providers to provide a minimal amount of security. This has ultimately resulted in compromises to security and unsatisfactory user experiences.

While there are other vendors on the market promising to solve these problems, they usually rely on products repackaging "old school" technologies such as firewalls and edge proxies that have been virtualized, put in the cloud, and sold as a new service. Not only does this approach not scale, but it also relies on tunnel stitching which results in poor performance and added latency. Moreover, this approach requires private corporate data to be decrypted, inspected, and then re-encrypted by the vendor before being sent to its final destination. Not only does this take time, which again negatively impacts performance, but it has huge data privacy and sovereignty implications.

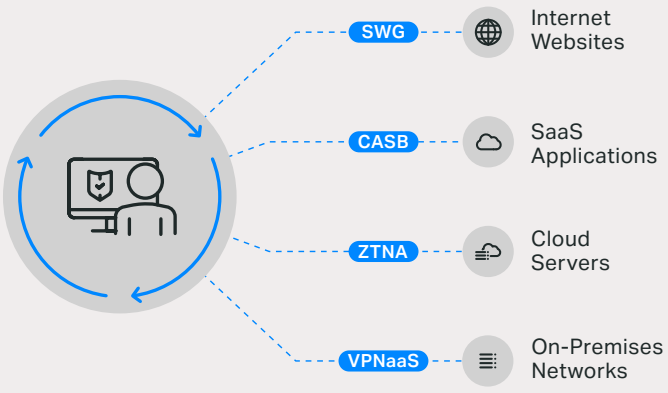
End users and the organization aren't better off with this approach either. End users need to remember to connect using the correct agent for each resource to get basic connectivity and security. From a security perspective, this complexity often motivates end users to circumvent the supplied agent thus putting the organization at risk.

SonicWall is a trusted vendor that understands the pains of living with legacy products and takes pride in not having the technical shortcomings of poor approaches to SSE.

Traditional Network-Based Access



Cloud Secure Edge



SONICWALL

Cloud Secure Edge's Approach

Cloud Secure Edge was built with ease of deployment and use in mind. It was developed from the ground up based on modern methods and technology rather than just old code, virtualized to run in the cloud. This results in exceptional performance.

Our device-centric approach is also vastly superior to competitor's legacy models. Modern devices have the processing power to enable local functionality that improves the end user experience, minimizes the need to send traffic for inspection, and truly allows for a secure mobile workforce.

Advantages of a device-centric approach:

- **Granular Control:** Device-centric security provides on-device granular control over the security settings and policies for each individual user, device, and resource ensuring that they are protected against potential threats.
- **Enhanced Visibility:** The device, being the source of traffic and resource interactions, is the ideal place to learn about where they are going and what they are doing once they access the resources.
- **Improved Compliance:** Device-centric security helps organizations meet regulatory and compliance requirements by ensuring that devices are configured to meet industry standards and best practices while also enforcing acceptable use policies (AUPs).
- **Protection Against Advanced Threats:** Device-centric security helps protect against advanced threats such as zero-day attacks and advanced persistent threats by providing enhanced security features and continuous monitoring and blocking outbound traffic attempts even when users click on links they shouldn't.
- **Improved User Experience:** Device-centric approaches improve the user experience by providing secure access to corporate resources from any device, anywhere, with minimal client or agent interaction. Convenient access and always-on security are provided even when a user is not logged in to the agent.
- **Cost-Effective:** Device-centric security is more cost-effective than traditional network-centric security approaches, as it reduces the need for costly security appliances, lowers cloud service provider (CSP) traffic charges, and improves overall security posture.

Cloud Secure Edge's approach does not require traffic to be routed to our cloud for inspection, resulting in more uptime and stability. Many customers have switched to us after putting up with unplanned outages, lost revenue, increased helpdesk calls and unhappy executives and employees elsewhere.

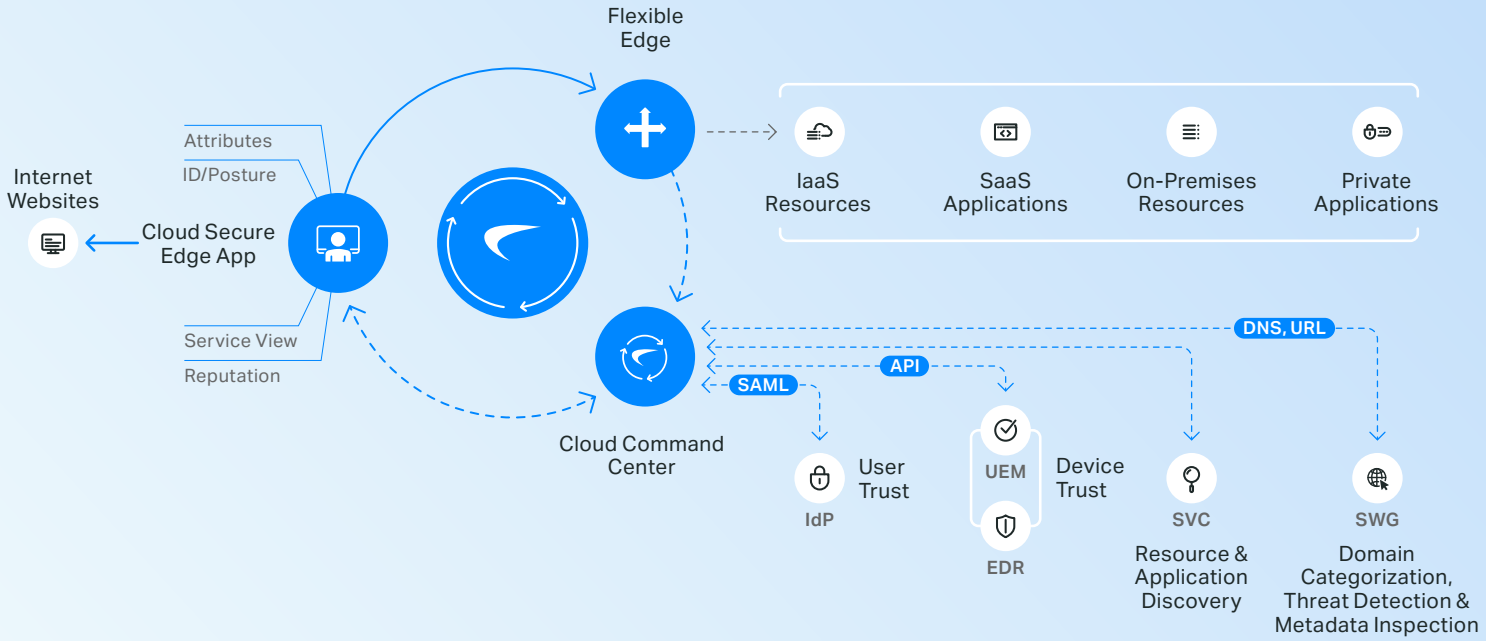
SONICWALL®

Cloud Secure Edge

Cloud Secure Edge securely connects users to applications, resources, and infrastructure while protecting them from internet threats. Risk and security are continuously evaluated and enforced in real-time across hybrid, multi-cloud, and SaaS environments.

The Cloud Secure Edge solution provides the following capabilities:

- Zero Trust Network Access (ZTNA)—application and infrastructure access—simple, least privilege access to applications and services across hybrid- and multi-cloud infrastructure, leveraging your existing enterprise identity and security tool investments.
- Virtual Private Network as a Service (VPNaaS)—network access—modern, high-performance, tunnel-based access to networks, incorporating zero trust enhancements like continuous authorization and device trust.
- Cloud Access Security Broker (CASB)—SaaS application access security—layered security that provides easily managed controls for who, using what specific devices, can access your SaaS applications.
- Secure Web Gateway (SWG)—internet threat protection —protects users from being phished, straying onto malicious web sites, and ransomware exposure. Organizations can also block specific categories of web sites, like gambling and pornography.



The Cloud Secure Edge Security Platform is comprised of the following key components:

- Cloud Command Center—Centralized dashboard and policy engine provides least-privileged access to sensitive corporate applications and resources.
- Cloud Secure Edge App—Real-time risk metric computation algorithms, continuously updated to quantify and score user/device context and behavior.
- Flexible Edge—A multi-cloud identity-aware access proxy that securely cloaks cloud applications and servers from malicious attacks or inadvertent exposure and also provides real-time enforcement of accessibility due to policy infractions.
- Threat Feeds—A collection of direct and third-party information used to learn about existing traffic flows and websites and make real-time threat and risk decisions.
- Integrations—Industry standard methods such as APIs, SAML, and OIDC are used to help deploy, manage, and secure our solution end-to-end. These integrations also share intelligence, taking advantage intelligence, taking advantage of existing network and security investments.

SONICWALL®

Key Benefits

Cloud Secure Edge provides impactful benefits to both organizational security and user experience.

Cloud Secure Edge Capability	Customer Benefit
Single admin platform and end user application	**A unified approach to access and security** • Single method for authentication and authorization • Policies created in one place regardless of end user or resource location • Single application that provides access and security • Visibility into all users, devices, and resources
Deploys a distributed trust model in any enterprise environment	**Tighter security for critical internal assets** • Applications are invisible to untrusted devices • Users do not have broad access to the network • Unified controls for HTTP, SSH, RDP and inter-service communications
Secure internet traffic	**Enforce compliance and reduce internet threats** • Enforce Acceptable Use Policies (AUPs) • Automatically block malware and phishing attempt activity • Provide granular URL access without blocking entire sites
Service Tunnels	**Provide tunneled access without giving full network access** • Single solution with proxied and tunneled connectivity • Provide encrypted tunnels that can double-encrypt traffic or add encryption to unsecured legacy applications • Domain-based split-tunneling enables quick white/blacklisting of traffic
Employs a trust score-based framework for continuous authorization	**Manage controls based on user context and behavior** • Users get fast, direct access to applications • Quickly create policies using pre-built templates • Integrate signals from UEBA and EDR tools
Architected for multi- and hybrid- cloud environments	**Simplify network operations** • Employ automation and CSP-native capabilities • App segmentation without complex network segmentation • Portable, containerized connectors that can be deployed anywhere
Enables customers to retain ownership of their data plane	**Maintain security and compliance across hybrid clouds** • Consistent policies across IaaS, SaaS, and on-premises • Don't hand over keys or admin rights to third parties
Enable advanced authentication and device awareness to SaaS and legacy applications	**Maintain consistency across all resources** • Enable advanced authentication to SaaS applications • Enable single sign-on and device-awareness to legacy applications without code changes • Gain visibility into how users are accessing cloud-based applications • Enforce source IP restrictions on SaaS applications
Utilizes standard security protocols—Mutual TLS, SAML, and OpenID Connect	**Accelerate enterprise-wide adoption** • Avoid vendor lock-in • Future proofed for Kubernetes and microservices
Discover and publish servers and services	**See the unknown and quickly react** • Discover servers, services, and applications on-premises, in the cloud, and SaaS • Discover shadow IT resources deployed and used within the organization • Quickly publish (or block) these resources in a granular, workflow-driven way

The Cloud Secure Edge Difference

Cloud Secure Edge is trusted by organizations of all sizes and in all verticals, around the world because of these uniquely valuable differences:

Device-Centric Approach

- Network simplicity and superior performance is achieved by limiting traditional network bottlenecks, eliminating unnecessary hops, and avoiding concentrators
- The compute power of modern devices is leveraged to enable risk-based routing. Making decisions at the traffic source lowers bandwidth consumption, sending traffic direct to destination. No need to send everything to a third-party cloud
- Privacy is safeguarded by building intelligence into the on-device app, rather than the cloud. Full-stack platform portability also means full data sovereignty.

Advanced Security

- Device trust is enforced in real-time using continuous authorization against granular Trust-Based Access Control (TBAC) policies.
- Only Cloud Secure Edge offers zero trust access that spans hybrid, multi-cloud, and SaaS-based environments.
- Always-on threat and malware security that doesn't require logging in to an agent.
- Double encryption of secure transport protocols such as HTTPS and SSL.
- Multi-factor authentication based on user and device factors.
- Harden edge connectors that only allow outbound session initiation.
- Sessions based on short-lived X.509 client certificate in the TLS handshake.
- Real-time domain categorization for DNS and content filtering.
- Source IP validation for SaaS application access.

Flexible Architecture

- The Flexible Edge—Cloud Secure Edge's mesh architecture extends security controls to distributed assets, spanning all environments and protocols. The cloud-native approach leverages public internet without requiring network tunnels or MitM clouds resulting in a highly performant, yet scalable solution that doesn't risk privacy or data sovereignty. Only Cloud Secure Edge flexibly supports cloud IaaS (Global Edge) while also offering the option for enterprises to self-host their edge (Private Edge).

Easy to Deploy and Use

- Get deployed in 15 minutes or less.
- One-click access to infrastructure and applications—Cloud Secure Edge integrates with customer IaaS and PaaS environments providing one-click access to applications and resources including SSH/RDP servers, VNC, Kubernetes, and databases—even SaaS applications are protected. Least privilege access allows differentiated access for FTEs and third parties alike that is a snap to deploy, administer, and audit.
- Service Tunnel offers a super-easy transition from legacy VPNs toward zero trust. It delivers high-performance, tunnel-based access to networks, and is built on a modern WireGuard foundation with continuous authorization and device trust enhancements.
- Fast, easy, and secure one-click passwordless access to hosted websites, IaaS infrastructure, and SaaS applications. Even complex datacenter and IaaS environments are a snap.
- Service Catalog simplifies access to Windows, Linux, and Kubernetes environments, including developer tools like GitLab, Jira, and Jupyter.
- Automated discover and publish capabilities enable administrators to inventory and rapidly make ephemeral applications and IaaS resources available to users.
- User-visible trust level enables self-remediation of device posture issues.
- Support for clientless deployment.
- Terraform support for automated deployment of zero trust security policies. Think of this as "zero trust as code".

Conclusion

Cloud Secure Edge provides modern Security Service Edge (SSE) functionality, built for the cloud from the ground up. Our platform offers industry-leading VPNaaS, ZTNA, CASB, and SWG without sacrificing user and administrator satisfaction or compromising security. Our device-centric approach is praised by customers for its simplicity and superior performance.

Cloud Secure Edge uniquely provides teams all the tools needed to secure access to applications and resources from anywhere while empowering your modern workforce of today and tomorrow.

> "The increased security we get with Cloud Secure Edge is tremendous. Compared to our VPN it's night and day."
>
> **Jonathan Jaffe**
> CISO, Lemonade, Inc

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 | Refer to our website for additional information.