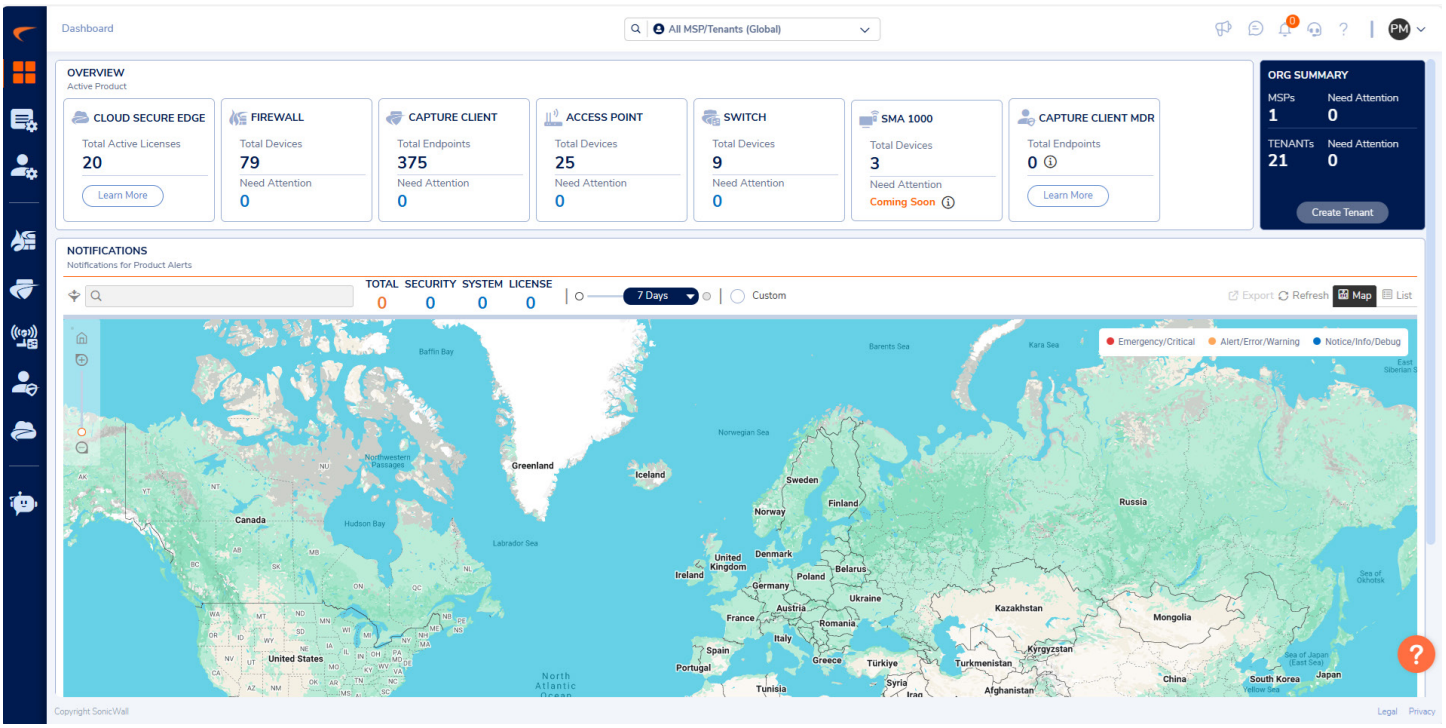
DATA SHEET

SonicWall Unified Management

A unified console experience, built to empower Managed Service Providers (MSPs).

SonicWall Unified Management is a next-generation cybersecurity platform built to meet the dynamic needs of Managed Service Providers (MSPs). It delivers a comprehensive, centralized approach to managing, securing, and scaling client networks with greater efficiency and control. Through a single unified console, MSPs can deploy, monitor, and manage SonicWall solutions—including firewalls, endpoints, access points and switches, MDR, and secure remote access.

The platform also features **SAMI**, SonicWall's AI-powered assistant, which automates repetitive tasks, delivers actionable insights, and helps apply the latest security best practices. Purpose-built for MSPs, SonicWall Unified Management simplifies cybersecurity operations while providing unmatched visibility, automation, and scalability across all client environments.



sonicwall.com

SONICWALL®

Why SonicWall Unified Management

Managing multiple security platforms across clients can quickly become complex. Disconnected systems create blind spots, slow response times, and increase operational overhead. SonicWall Unified Management eliminates these challenges by consolidating all SonicWall solutions and tenants into a single, intelligent console.

Boost Efficiency Through Consolidation

- **Single-pane visibility:** Centralized view of all tenants and products.
- **Faster actions:** Bulk provisioning, license updates, and service activations in one step.
- **Unified operations:** Streamlined search, filters, and exports simplify inventory and reporting.
- **Scalable design:** Multi-tenant workflows built for large MSP environments.

Strengthen Security & Continuity

- **Proactive management:** "Updates available" and license expiry alerts keep systems current.
- **Simplified compliance:** Consolidated license, update, and subscription insights support audits.
- **Full visibility:** Correlate endpoint, network, and user data for complete threat awareness.
- **Better client outcomes:** Detect and resolve issues before they impact operations.

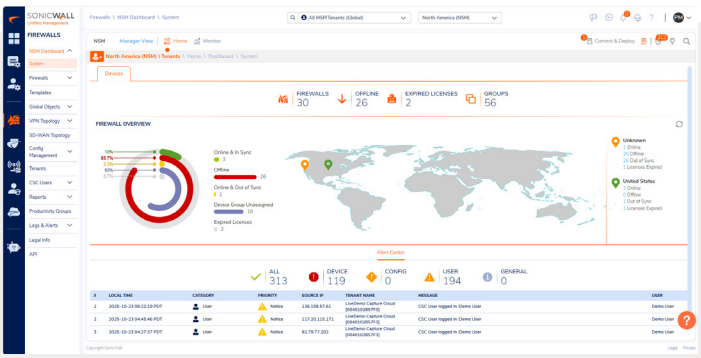
Key Features

- **Multi-Tenant Management for MSPs:** SonicWall Unified Management is designed for MSPs managing multiple, diverse client environments, providing a single console to monitor and secure them with ease.
- **Zero-Touch Deployment:** Quickly deploy and provision SonicWall firewalls and other security tools, automatically synchronizing licenses and pushing policies and firmware updates.
- **Active Monitoring & Alerts:** Receive real-time alerts to detect threats, troubleshoot issues, and remediate critical system conditions, ensuring peak performance.
- **Scalable Security Services:** Seamlessly expand security offerings as your client base grows, maintaining consistent protection without extra resources.
- **Enhanced Client Service:** Centralized management boosts operational efficiency, allowing MSPs to focus on delivering high-value services and improving client satisfaction.
- **SonicWall AI for Monitoring & Insight (SAMI):** AI-powered assistant delivering instant insights, recommendations, and faster troubleshooting.
- **Seamless Ecosystem Integration:** Manage firewalls, endpoints, access points, switches, and secure access solutions from one console.

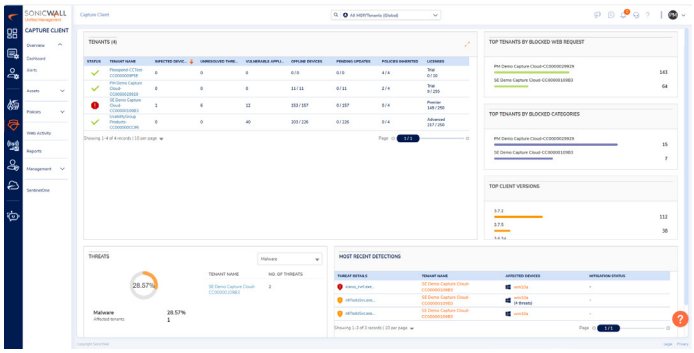
Unified View of the SonicWall Ecosystem

Gain complete visibility across your entire SonicWall environment from a single interface to monitor performance, manage configurations, and respond to threats in real time across:

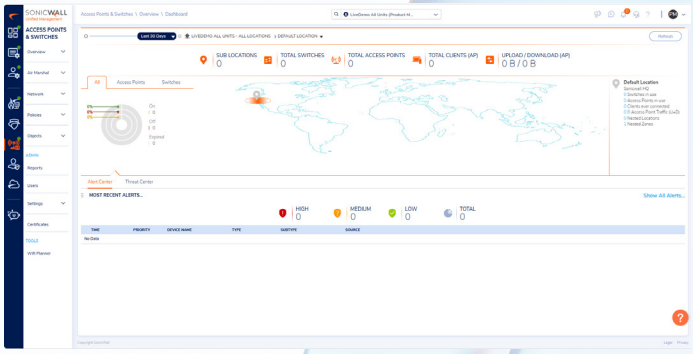
Firewalls: Manage all your firewalls from a single console, available as SaaS or on-premises, to monitor, configure, and respond to threats in real-time while maintaining compliance. With zero-touch onboarding, reusable templates, and built-in reporting, you can deploy consistent policies, streamline management, and gain full visibility across every device and tenant.



Endpoint and MDR: Connect your Capture Client endpoints for real-time threat detection, ransomware rollback, and seamless integration with SonicWall firewalls. With Capture Client MDR, benefit from 24/7 monitoring by our SonicSentry team, providing comprehensive visibility into threat activity and alerts.



Access Points & Switches: Manage your entire fleet of access points and switches from a single console with centralized policies, zero-touch onboarding, and automated firmware updates to ensure consistency and security across the network. Advanced analytics and reporting, such as RF surveys, spectrum analysis, and Wi-Fi planning, provide deep visibility and optimized performance.



Cloud Secure Edge: provides modern, cloud-native secure access built for today's cloud-first workforce, delivering fast, flexible remote connectivity with Zero Trust principles. It also protects against internet threats in real time, filtering malicious content and blocking risky domains to prevent malware, phishing, and data breaches.

SonicWall AI for Monitoring and Insight (SAMI)

SAMI is an AI-powered assistant built into SonicWall Unified Management that simplifies IT and network security operations. MSPs can use SAMI to:

- Streamline day-to-day management through a chat-based interface
- Gain actionable insights into network and security environments
- Apply the latest best practices automatically
- Work faster, smarter, and more effectively, whether you're a seasoned pro or just starting out

SonicWall, Inc.

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

© 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.

sonicwall.com

SONICWALL®