SONICWALL

SonicWall Security-as-a-Service for Schools

Benefit from a flexible, affordable comprehensive network security solution to enhance K-12 security managed by a SonicWall-certified partner.

The urgency for K-12 IT security has grown substantially, but most school districts don't possess the financial resources to purchase and deploy the equipment necessary to make network security their top priority. SonicWall Security-as-a-Service (SECaaS) provides districts and schools with a comprehensive network security solution that requires no upfront capital investment, so it fits within any budget. SECaaS outsources day-to-day management of your network security infrastructure to an experienced SonicWall-certified partner who delivers a turnkey solution to your school. SECaaS is an affordable, monthly, subscription-based service that bundles:

- A SonicWall next-generation firewall (NGFW)
- A comprehensive security suite
- Mobile and wireless security
- Management and reporting
- 24x7 support

Block threats before they enter your network

Entry points into your network may now include student and teacher laptops, desktops and smartphones. SECaaS secures your network and data against sophisticated, modern-day threats with comprehensive protection that includes:

- Intrusion prevention
- Gateway anti-virus and anti-spyware
- Content/URL filtering
- Enforced client anti-virus and anti-spam services

Eliminate bottlenecks

The volume of traffic being scanned, as well as the increasing amount of threats and malware attacks, can easily paralyze your firewall. SonicWall next-generation firewalls protect your school, no matter the size, without slowing down your network — providing you with fast, reliable performance.

Keep your network productive

Your network performance can be bogged down by social media, web surfing, peer-to-peer file sharing and other unauthorized web activities that have nothing to do with getting schoolwork done. Ensure the applications critical to teaching and learning have the bandwidth they need with content and application control tools.

Provide secure mobile access from any platform

Your students, teachers and staff need access to email, files and applications wherever they are. Now you can give them access to your network with secure VPN remote access for Windows, Mac OS X, iOS, Android, Chrome OS and Kindle Fire devices and be assured it is secure and free from threats.

Get an all-in-one security solution

Combine the features of the latest firewalls, gateway anti-malware products, intrusion prevention systems and content/URL filtering software in a single solution. All of these security technologies are installed, configured, deployed, and managed as a single unit. Detailed event data is available through one reporting system, making it easier to identify threats early and take appropriate measures before your network is compromised.

Benefits:

- Outsource security to an expert provider
- No upfront capital investment
- Affordable monthly subscription rate
- Predictable annual expense model
- Turnkey solution
- Firewall configured by a SonicWall-certified partner
- Pro-active monitoring and alerting
- Software and firmware updates and upgrades
- Weekly SonicWall off-site configuration backup
- Automated weekly network and security reports
- Report analysis by SonicWall-certified engineers
- Upgraded appliances as business and technology changes dictate

Available through a SonicWall-certified partner. For more information contact us at SECaaS@sonicwall.com

Save with E-rate eligible solutions

SECaaS helps reduce budget demands even further with firewalls, wireless access points and WAN acceleration solutions that are eligible for discount to schools that have qualified for the government's E-rate program.

SonicWall SECaaS Bundle Features	
Feature	**Description**
Patented Reassembly-Free Deep Packet Inspection (RFDPI)	Performs stream-based bi-directional traffic analysis, without proxying or buffering. Uncovers intrusion attempts and malware and identifies application traffic, regardless of port.
Real-Time Deep Memory Inspection (RTDMI)	Proactively detects and blocks threats via deep memory inspection in real time, by forcing unknown, hidden and seemingly benign malware to reveal itself.
Intrusion Prevention System (IPS)	Leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Network-based malware prevention	The SonicWall RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
CloudAV malware prevention	References a continuously updated database, which resides in the SonicWall cloud server and houses over 30 million threat signatures. This augments the capabilities of the onboard signature database, providing RFDPI with extensive threat coverage.
Cloud-based multi-engine sandboxing	SonicWall Capture Advanced Threat Protection Service uses cloud-based, multi-engine sandboxing, including full system emulation, virtualization and hypervisor-level techniques to analyze suspicious files, detect malicious behavior and block unknown and zero-day attacks at the gateway.
Around-the-clock security updates	The SonicWall Threat Research Team analyzes new threats and releases countermeasures 24x7. New threat updates are automatically pushed to firewalls in the field with active security services, and execute immediately without reboots or interruptions.
SSL decryption and inspection	Decrypts and inspects SSL traffic on the fly, without proxying, for malware, intrusions and data leakage. Applies application, URL and content control policies in order to protect against threats hidden in SSL-encrypted traffic.
Application control	Controls applications, or individual application features, identified by the RFDPI engine against a continuously expanding database of over 3,500 application signatures, to increase network security and enhance network productivity.
Application bandwidth management	Granularly allocate and regulate available bandwidth for critical school-related applications or application categories while limiting nonessential application traffic.
Inside/Outside content filtering	Enforce acceptable use policies and block access to websites containing information or images that are objectionable or unproductive with Content Filtering Service. Extend policy enforcement to block internet content for devices located outside the firewall perimeter with the Content Filtering Client.
Global Management System (GMS)	SonicWall GMS monitors, configures and reports on multiple SonicWall appliances through a single management console with an intuitive interface, thereby reducing management costs and complexity.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the firewall to act as a VPN concentrator for thousands of locations within a school district.
SSL VPN and IPSec client remote access	Both the clientless SSL VPN technology and easy-to-manage IPSec client offer seamless remote access to email, files, computers, intranet sites and applications from a variety of platforms.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

Datasheet-SECaaS-forschools-US-VG-609

SONICWALL®