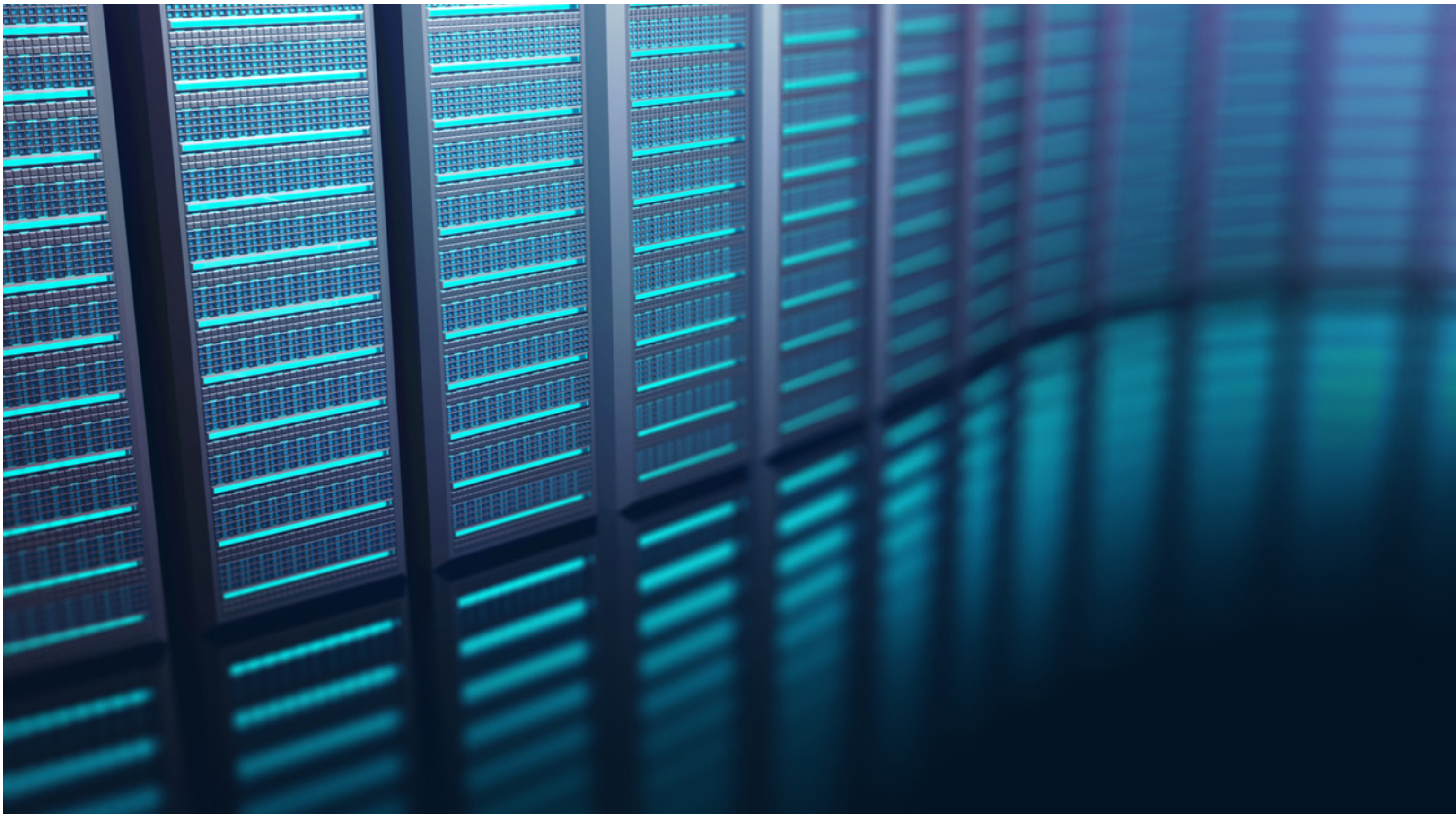
SonicWall product lines



Overview

Secure your organization's public/private cloud, applications, users and data with a deep level of protection that won't compromise network performance. The SonicWall Capture Cloud Platform tightly integrates security, management, analytics and real-time threat intelligence across the company's portfolio of network, wireless, email, mobile, web and cloud security products. This approach enables small and mid-sized businesses, to large enterprise environments, government, retail point-of-sale, education, healthcare and service providers to experience our complete security ecosystem that harness the power, agility and scalability of the cloud.

The Capture Cloud Platform strategy and vision for the future is continuous innovation and development of containerized as-a-service security applications that are easily programmable and provisioned on-demand. It is comprised of 10 key core components and capabilities:

- Network security
- Wireless network security
- Web application security
- Endpoint security
- Cloud app security
- Advanced security services
- Remote access
- Email security
- Security management and analytics

The combination of these delivers mission-critical layered cyber defense, threat intelligence, analysis and collaboration, and common management, reporting and analytics that work synchronously together.

Network security products

SonicWall is one of the leading providers of next-generation firewalls (NGFWs). The proven SonicOS firmware is at the core of every SonicWall NGFW. SonicOS leverages our scalable, multi-core hardware architecture plus our patent-pending Real-Time Deep Memory Inspection (RTDMI™) and our patented*, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engines that scan all traffic regardless of port or protocol.

Our NGFWs ensure that every byte of every packet is inspected, while maintaining the high performance and low latency that busy networks require. Unlike competitive offerings, the single-pass RFDPI engine enables simultaneous, multi-threat and application scanning, as well as analysis of any size file, without packet reassembly. This enables SonicWall NGFWs to massively scale to extend state-of-the-art security to growing and distributed enterprise networks and data centers.

SonicWall NGFWs offer a range of robust capabilities, including:

- Capture ATP cloud-based multi-engine sandboxing
- SD-WAN
- REST APIs
- Decryption and inspection of encrypted traffic
- Intrusion prevention service (IPS)
- Malware protection
- Application intelligence, control and real-time visualization
- Website/URL filtering (content filtering)
- Virtual private networking (VPN) over SSL or IPSec
- Wireless security
- Hybrid and multi-cloud security
- Stateful failover/failback

Moreover, SonicWall firewalls deliver fast response and continuous protection against zero-day threats from the Capture Labs Threat Research Team. This team gathers, analyzes and vets cross-vector threat information from a variety of threat intelligence sources, including over one million globally placed sensors within its Capture Threat Network.

SonicWall Network Security services platform (NS*sp*) series

The SonicWall NS*sp* 12000 series NGFW platform is designed to deliver scalability, reliability and deep security at multi-gigabit speeds for large networks.

NSS Labs has assessed SonicWall firewalls using one of the most rigorous real-world performance test of NGFWs, and SonicWall excels in security effectiveness, performance, scalability, reliability and TCO. For the fifth time, SonicWall firewalls have set the standard for high performance application control and threat prevention in various deployment use cases, from small businesses to large data centers, carriers and service providers.

The NS*sp* 12000 series ensures high quality-of-service level with uninterrupted network availability and connectivity demanded by today's enterprises, government agencies, service providers and universities with 40/10 Gbps infrastructures. Leveraging innovative deep learning security technologies in the SonicWall Capture Cloud Platform, the NS*sp* 12000 series delivers proven protection from the most advanced threats without slowing performance.

**U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723*

SonicWall Network Security appliance (NS*a*) series

The SonicWall Network Security appliance (NS*a*) series is the one of the most secure, highest performing NGFW lines available. It delivers business-class security and performance without compromise, using the same architecture as the flagship NS*sp* 12000 NGFW line — initially developed for the world's most demanding carriers and enterprises. At the same time, it offers SonicWall's acclaimed ease of use and high value.

Based on years of research and development, the NS*a* series is designed from the ground up for distributed enterprises, small- to medium-sized businesses, branch offices, school campuses and government agencies. The NS*a* series combines a revolutionary multi-core architecture with cloud-based Real-Time Deep Memory Inspection (RTDMI) technology and a patented RFDPI single-pass threat-prevention engine in a massively scalable design. This offers industry-leading protection, performance, and scalability, with the highest number of concurrent connections, lowest latency, no file size limitations and superior connections-per-second in its class.

SonicWall TZ series

The SonicWall TZ series is comprised of highly reliable, highly secure unified threat management (UTM) firewalls designed for small- to medium-sized businesses (SMB), retail deployments, government organizations, and distributed enterprises with remote sites and branch offices. Unlike consumer-grade products, the TZ series consolidates highly effective anti-malware, intrusion prevention, content/URL filtering and application control capabilities over wired and wireless networks — along with broad mobile platform support for laptops, smartphones and tablets. It provides full deep packet inspection (DPI) at very high performance levels, eliminating the network bottleneck that other products introduce, and enables organizations to realize productivity gains.

As with all SonicWall firewalls, the TZ series inspects the whole file, including TLS/SSL-encrypted files, to enable complete protection. Additionally, the TZ series offers application intelligence and control, advanced application traffic analytics and reporting, Internet Protocol Security (IPsec) and SSL VPN, multiple ISP failover, load balancing and SD-WAN. Optional integrated Power over Ethernet (PoE) and high-speed 802.11ac wireless enable organizations to extend their network boundaries easily and securely. Combined with Dell N-Series and X-Series switches, the TZ series firewalls provide the flexibility to securely grow the business without adding complexity.

SonicWall Network Security virtual (NS*v*) series

SonicWall Network Security virtual (NS*v*) firewalls extend automated breach detection and prevention into hybrid and multi-cloud environments with virtualized versions of SonicWall next-generation firewalls. With full-featured security tools and services equivalent to a SonicWall NS*a* firewall, NS*v* effectively defends your virtual and cloud environments from resource misuse attacks, cross-virtual-machine attacks, side-channel attacks and all common network-based exploits and threats.

NS*v* is easily deployed and provisioned in a multi-tenant virtual environment, typically between virtual networks (VNs). It establishes access control measures to preserve data and VM safety while capturing virtual traffic between virtual machines and networks for automated breach prevention. With infrastructure support for high availability (HA) implementation, NS*v* fulfills scalability and availability requirements of Software Defined Data Center (SDDC). Easily deployed as a virtual appliance in private cloud platforms such as VMWare or Microsoft Hyper-V, or in AWS or Microsoft Azure public cloud environments. Leverage flexible licensing model with NS*v* and provide organizations all the security advantages of a physical firewall with the operational and economic benefits of virtualization.

SonicWave wireless network security series

SonicWall makes wireless networking secure, simple and affordable with the innovative SonicWall Wireless Network Security solution. The solution combines high-performance SonicWave Series 802.11ac Wave 2 wireless access points with SonicWall WiFi Cloud Manager (WCM) or industry-leading SonicWall firewalls to achieve next-gen network security and performance on your wireless network, WCM is an intuitive, scalable and centralized cloud-based WiFi network management system suitable for networks of any size. It can be accessed through SonicWall Capture Security Center. WiFi planner, available through WCM, enables you to optimally design and deploy a WiFi network. When deploying APs, the SonicWiFi mobile app allows you to set up, manage and keep track of WiFi networks. Together, these wireless solutions ensure a secure WiFi user experience.

Our solution goes beyond mere secure wireless solutions by securing wireless networks with RTDMI and RFDPI technologies and delivering dual protection by encrypting wireless traffic and decontaminating it from network threats, while also protecting the network from wireless attacks. Additionally, SonicWave APs performs advanced security functionality like Capture and CFS, directly in the AP.

With fast roaming, users can roam from one location to another seamlessly. The feature-rich portfolio includes auto channel selection, spectrum analysis, air-time fairness, band steering, and signal analysis tools for monitoring and troubleshooting. SonicWall lowers total cost of ownership (TCO) by enabling administrators to avoid implementing and separately managing an expensive wireless-specific solution that runs in parallel to their existing wired network.

SonicWall Web Application Firewall (WAF) series

SonicWall Web Application Firewall (WAF) series protects web applications running in a private, public or hybrid cloud environment. It features advanced web security tools and services to keep compliance data unexposed and web properties safe, undisrupted and in peak performance. WAF applies Layer-7 application delivery capabilities that enable application-aware load balancing, SSL offloading and acceleration for resilience and an enhanced digital engagement and experience.

WAF employs a combination of signature-based and application-profiling deep-packet inspection engines to protect against typical web application attacks like those outlined by the Open Web Application Security Project (OWASP), as well as more advanced web application threats like denial-of-service (DoS) attacks and context-aware exploits. In addition to protecting web applications, WAF also prevents data loss through the use of data masking and page-blocking techniques for specified patterns of sensitive data like Payment Card Information (PCI) and government issued identification.

For optimal protection against malicious downloads, malware injections or advanced threats, WAF leverages SonicWall Capture Labs threat research, and adds SonicWall Capture ATP with and RTDMI™ service options to its suite of web security services. Additionally, APIs are provided to give administrators the ability to monitor and orchestrate WAF operations programmatically for improved web security automation and efficiency.

WAF provides economy-of-scale benefits of virtualization and can be deployed as a virtual appliance in private clouds based VMWare ESXi or Microsoft Hyper-V, or in AWS or Microsoft Azure public cloud environments.

Capture Client

The management and security of endpoints is critical in today's business climate. With end users in and out of the network with their devices, as well as encrypted threats reaching endpoints unchecked, something must be done to protect these devices. With the growth of ransomware and the persistent use of credential theft, endpoints are the battleground of today's threat landscape.

Additionally, administrators struggle with the visibility and management of their security posture. They are also challenged by having to provide consistent assurance of client security, along with easy-to-use and actionable intelligence and reporting.

Endpoint security products have been on the market for years but administrators struggle with:

- Keeping security products up to date
- Enforcing policies and compliance
- Getting reports
- Threats coming through encrypted channels
- Understanding alerts and remediation steps
- License management
- Stopping threats like ransomware
- Fileless attacks and infected USB devices bypassing perimeter defenses

SonicWall Capture Client is a unified client platform that will deliver multiple endpoint protection capabilities. This solution features a cloud-based management console and complete integration with SonicWall next-generation firewalls for a unified security experience for SonicWall customers. Combined with enforcement capabilities, SonicWall Capture Client can ensure that endpoints are running security software and/or have an embedded SSL certificate in place for the inspection of encrypted traffic. Furthermore, in order to make the inspection of SSL traffic (DPI-SSL) easier with a better end user experience, Capture Client enables administrators to push SSL certificates the endpoint much easier than before.

On top of this, Capture Client features an advanced antivirus engine designed to stop the most ingenious malware with a rollback option to return to a previously uninfected state. Furthermore, Capture Client Advanced integrates with SonicWall Capture Advanced Threat Protection (ATP) to examine suspicious files to better stop attacks before they activate.

SonicWall Capture Client Features include:

- Security enforcement
- DPI-SSL certificate management
- Continuous behavioral monitoring
- Highly accurate determinations achieved through machine learning
- Multiple layered heuristic-based techniques
- Unique rollback capabilities (Capture Client Advanced only)
- Capture Advanced Threat Protection network sandbox integration (Capture Client Advanced only)
- One-click lookup of suspicious files against Capture ATP's threat intel database of convictions and acquittals
- Web Threat Protection to block known malicious sites and IP addresses
- Policy-based Device Control to block potentially infected storage devices

The SonicWall WAN Acceleration (WXA) series

The SonicWall WAN Acceleration (WXA) series reduces application latency and conserves bandwidth, significantly enhancing WAN application performance and user experience for small- to medium-sized organizations with remote and branch offices. After initial data transfer, the WXA series dramatically reduces all subsequent traffic by transmitting only new or changed data across the network. The WXA deduplicates data traversing the WAN, remembers previously transferred data, and replaces repeated byte sequences with an identifier, thus reducing application latency and conserving bandwidth. Other acceleration features include data caching, file deduplication, metadata caching, HTTP (web) caching and data-in-flight compression.

Unlike standalone WAN acceleration products, WXA solutions are integrated add-ons to SonicWall NS*a* and TZ series firewalls. This integrated solution streamlines the placement, deployment, configuration, routing, management and integration of the WXA with other components, such as VPNs. When deployed in conjunction with a SonicWall NGFW running Application Intelligence and Control Service, the WXA offers the unique combined benefit of both prioritizing application traffic and minimizing traffic between sites, resulting in optimal network performance.

Learn more about SonicWall network security products at: www.sonicwall.com/en-us/products.

Network security services and add-on products

SonicWall network security firewall services and add-ons offer highly effective, advanced protection for organizations of all sizes, to help defend against security threats, gain greater security control, enhance productivity and lower costs.

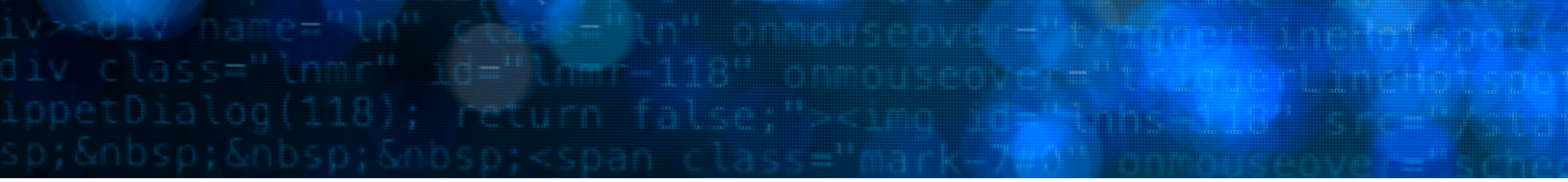
Services and add-ons include:

- TotalSecure Advanced bundle – Firewall plus the Advanced Gateway Security Suite bundle (multi-engine sandboxing, anti-virus, anti-spyware, intrusion prevention, application intelligence, content/web filtering and 24x7 support)
- Advanced Gateway Security Suite bundle – Capture Advanced Threat Protection, gateway anti-virus, anti-spyware, intrusion prevention, content/web filtering and 24x7 support
- Gateway security services – Gateway anti-virus, anti-spyware, intrusion prevention and application intelligence and control
- Capture Advanced Threat Protection (ATP)
- Content filtering services
- Enforced client ant-virus and anti-spyware software
- Comprehensive anti-spam service
- Deep packet inspection of TLS/SSL-encrypted traffic (DPI-SSL)
- Application intelligence and control
- Intrusion prevention system (IPS)

Learn more about network security services and add-ons at: www.sonicwall.com/en-us/products/firewalls/security-services.

Inspect Deep Memory

A patent-pending technology, the SonicWall Real-Time Deep Memory Inspection (RTDMI) engine proactively detects and blocks unknown mass-market malware via deep memory inspection in real time. Available now with the SonicWall Capture Advanced Threat Protection (ATP) cloud sandbox service, the engine identifies and mitigates even the most insidious modern threats, including future Meltdown exploits.



Cloud App Security

Cloud App Security

SonicWall Cloud App Security delivers next-gen security for SaaS applications such as Office 365 and G Suite, protecting email, data and user credentials from advanced threats, while ensuring compliance in the cloud. If you are moving to the cloud, SonicWall provides best-in-class API-based security with low TCO, minimal deployment overhead and a seamless user experience.

Next-Gen Security for Cloud Email

In addition to traditional email security layers of SPF, DKIM and DMARC checks, as well as URL filtering by leveraging three major data sources for URL blacklists, Cloud App Security's unique architecture provides protection that is impossible for an external gateway solution:

1. Adds a layer of advanced threat protection: Cloud App Security blocks phishing messages missed by Office 365 and G Suite. The solution utilizes machine learning, artificial intelligence and big-data analysis to provide powerful anti-phishing, attachment sandboxing, time-of-click URL analysis and impersonation protection.
2. Monitors inbound, outbound and internal email: Cloud App Security's SaaS integration can scan and quarantine every email before it reaches the user's inbox, whether it is coming from outside the organization or from a compromised internal account.
3. Scans historical messages for threats: On first connect, Cloud App Security scans historical messages (even closed accounts) for potential breaches or compromised accounts.
4. Global Email Retraction: Malicious messages can be edited or retracted at any time, whether they are malicious, contain confidential information or due to an employee's accidental reply-all.

Because Cloud App Security's email protection is applied before the inbox but after the native Microsoft or Google filters (as well as any external MTA gateway that might be deployed), its machine-learning algorithms are uniquely tuned to identify threats that they miss. Cloud App Security is also able to incorporate the results of the native scans into its own detection algorithms.

Next-Gen Security for the complete productivity suite

Cloud App Security offers complete, defense-in-depth security for Office 365 or G Suite. Whether you use email, share drives, IMs or the full collaboration environment, the solution helps you perform the following security actions:

1. Prevent phishing and malware from propagating within your organization or spreading to your customers and partners.
2. Check every file for malicious content using Capture ATP sandboxing and active-content analysis to quarantine threats before they are downloaded by your users.
3. Identify confidential information and apply cloud-aware policies that keep it within an organization or work group. Your users can harness the full power of cloud-based productivity suite while automated work-flows enforce regulatory compliance, ensuring PCI, HIPAA, PII or other confidential data is not shared externally.

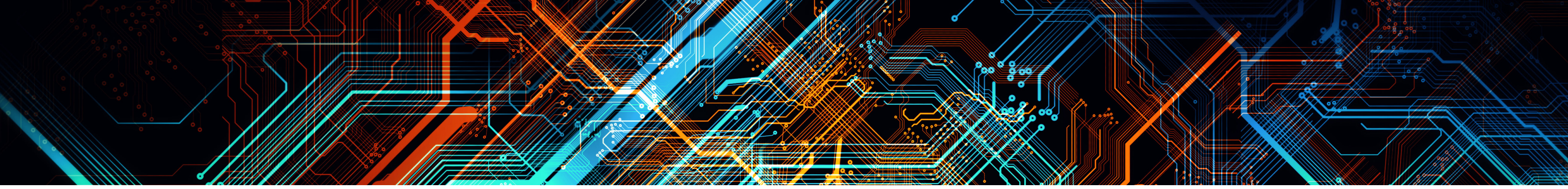
Sanctioned IT Security

SonicWall Cloud App Security analyzes all traffic (log events, user activities, data files and objects, configuration state etc.) and enforces the necessary security policies through direct integrations with native APIs of the cloud service. Since the solution leverages native APIs, the solution does not use a proxy or sit in-line between the user and the cloud. This enables the solution to provide coverage for sanctioned apps regardless of the user's device or network. In addition, the API-based approach allows for easy deployment, granular control, and zero impact to the user experience.

Shadow IT Visibility and Control

SonicWall NGFWs analyze and log all traffic entering and leaving the network. Logs generated for outbound traffic data do not clearly distinguish the cloud applications being used, and don't provide a risk score for each application used by employees. For remote employees redirected through NGFW using VPN, the solution gathers additional details from these logs on the actions users take within cloud services. Cloud App Security processes log files from SonicWall NGFWs and reveals which cloud services are in use by which users, data volumes uploaded to and downloaded from the cloud, and the risk and category of each cloud service. In effect, the Cloud App Security makes the existing infrastructure cloud-aware. With employees increasingly using cloud applications for work, Cloud App Security enables administrators to detect gaps in security posture, classify cloud applications into sanctioned and un-sanctioned IT applications, and enforce access policies to block risky applications. Cloud App Security is a critical part of SonicWall's vision to provide automated real-time breach detection and prevention capabilities for customers as they adopt cloud technologies.

Learn more about SonicWall Cloud App Security at: www.sonicwall.com/casb.



Remote Access security products

SonicWall SMA is the unified secure access gateway for organizations facing challenges in mobility, BYOD and cloud migration. The solution enables organization to provide anytime, anywhere and any device access to mission critical corporate resources. SMA's granular access control policy engine, context aware device authorization, application level VPN and advanced authentication with single sign-on empowers organizations to embrace BYOD and mobility in a hybrid IT environment.

In addition, SMA reduces the surface area for threats by providing features such as Geo IP and Botnet detection, Web Application Firewall and Capture ATP sandbox integration.

Mobility and BYOD

For organizations wishing to embrace BYOD, flexible working or offshore development, SMA becomes the central enforcement point across them all. SMA delivers best-in-class security to minimize surface threats, while making organizations more secure by supporting latest encryption algorithms and ciphers. SonicWall's SMA allows administrators to provision secure mobile access and role-based privileges so end-users get fast, simple access to the business applications, data and resources they require. At the same time, organizations can institute secure BYOD policies to protect their corporate networks and data from rogue access and malware.

Move to the cloud

For organizations embarking on a cloud migration journey, SMA offers a single sign-on (SSO) infrastructure that uses single web portal to authenticate users in a hybrid IT environment. Whether the corporate resource is on-premises, on the web or in a hosted cloud, the access experience is consistent and seamless. Users do not need to remember all the individual application URLs and maintain exhaustive bookmarks. With Workplace, a centralized access portal, you give users one URL to access all mission critical applications from a standard Web browser. SMA provides federated SSO to both cloud hosted SaaS applications that use SAML 2.0 and campus hosted applications that use RADIUS or Kerberos. SMA integrates with multiple authentication, authorization, and accounting servers and leading Multi-factor authentication (MFA) technologies for added security. Secure SSO is delivered only to authorized endpoint devices after checks for health status and compliance.

Managed service providers

For organizations with data centers or for managed service providers, SMA provides turnkey solution to deliver a high degree of business continuity and scalability. The SonicWall's SMA can support up to 20,000 concurrent connections on a single appliance with the ability to scale upwards of hundreds of thousands users through intelligent clustering. Reduce costs at data centers with active-active HA clustering (Global High Availability) and built-in dynamic load balancer (Global Traffic Optimizer), which reallocates global traffic to the most optimized data center in real-time based on user demand. SMA empowers service owners through a series of tools to deliver a service with zero downtime and allows very aggressive SLAs to be fulfilled.

SMA Appliances

SonicWall SMA can be deployed as a hardened, high-performance appliance or as a virtual appliance leveraging shared computing resources to optimize utilization, ease migration and reduce capital costs. The hardware appliances are built on a multi-core architecture that offers high performance with SSL acceleration, VPN throughput and powerful proxies to deliver robust secure access. For regulated and federal organizations, SMA is available with FIPS 140-2 Level 2 certification. The SMA virtual appliances offer the same robust secure access capabilities on major virtual platforms such as Hyper-V and VMware. Whether you choose to deploy physical appliances, virtual appliances or a combination of the two, SMA fits seamlessly into your existing IT infrastructure.

Management and Reporting

SonicWall provides an intuitive he web-based management platform to streamline appliance management while providing extensive reporting capabilities. The easy-to-use GUI brings clarity to managing multiple machines. Unified policy management helps you create and monitor access policies and configurations. One single policy manages your users, devices, applications, data and networks. Automate routine tasks and schedule activities, freeing up security teams from repetitive tasks to focus on strategic security tasks like incidence response.

Empower your IT department to provide the best experience and the most secure access depending on the user scenario. Choose from a range of fully clientless web-based secure access for vendors and 3rd party contractors, or a more traditional client-based full tunnel VPN access for executives. Whether you need to provide reliable secure access to 5 users from a single data center or scale up to thousands' of users from globally distributed data centers, SonicWall SMA has a solution for you.

Learn more about SonicWall mobile security products at: www.sonicwall.com/en-us/products/remote-access.

Email security products

Email is crucial for your business communication, but it is also the #1 attack vector for threats such as ransomware, phishing, business email compromise (BEC), spoofing, spam and viruses. What's more, government regulations now hold your business accountable for protecting confidential data and ensuring it is not leaked and that email containing sensitive customer data or confidential information is securely exchanged. Whether your organization is a growing small-to medium-sized business, a large, distributed enterprise or a managed service provider (MSP), you need a cost-effective way to deploy email security and encryption, and the scalability to easily grow capacity for — and delegate management across — organizational units and domains.

In addition, to manage costs and resources, organizations are adopting Microsoft Office 365 and Google G suite. While Office 365 and G suite offers built-in security functionalities, to combat advanced email threats organizations require a next-generation email security solution that seamlessly integrates with Office 365 and G suite, to protect them against today's advanced threats.

SonicWall Email Security Appliances

Easy to set up and administer, SonicWall Email Security is designed to cost-effectively scale from 10 to 100,000 mailboxes. It can be deployed as a hardware appliance, as a virtual appliance leveraging shared computing resources, or as software — including software optimized for Microsoft Windows server or Small Business Server. SonicWall Email Security physical appliances are ideal for organizations that need a dedicated on-premises solution. Our multi-layered solution provides comprehensive inbound and outbound protection, and is available in a range of hardware appliance options that scales up to 10,000 users per appliance. SonicWall Email Security is also available as a virtual appliance or as a software application that is ideal for organizations that require the flexibility and agility that come with virtualization. The solution can be configured for high availability in split mode, to centrally and reliably manage large-scale deployments.

SonicWall email security solution uses technologies such as machine learning, heuristics, reputation and content analysis, time-of-click URL protection, and sandboxing for attachments and URLs to deliver comprehensive inbound and outbound protection. The solution also includes powerful email authentication standards – Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) - to stop spoofing attacks and email fraud.

- Stop advanced threats before they reaches your inbox
- Protect against email fraud and targeted phishing attacks
- Get up-to-date security with real-time threat intelligence
- Secure your cloud email service (Office 365, G-Suite)
- Enable email data loss prevention & compliance
- Easy management and reporting
- Flexible deployment options

Administration of the Email Security solution is intuitive, quick and simple. You can safely delegate spam management to end users, while still retaining ultimate control over security enforcement. You can also easily manage user and group accounts with seamless multi-LDAP synchronization. The solution also provides easy integration for Office 365 and G suite to defend against advanced email threats.

For large, distributed environments, multi-tenancy support lets you delegate sub-administrators to manage settings at multiple organizational units (such as enterprise divisions or MSP customers) within a single Email Security deployment.

SonicWall Hosted Email Security service

Trust fast-to-deploy and easy-to-administer hosted services to protect your organization from email-borne threats such as ransomware, zero-day threats, spear phishing and BEC while meeting email compliance and regulatory mandates. Get the same level of advanced email protection with our hosted solution, which offers feature parity with physical and virtual appliances. The solution also offers email continuity to ensure that emails are always delivered and productivity is not impacted during planned and unplanned outages of on-prem email servers or a cloud provider such as Office 365 and G suite.

SonicWall Hosted Email Security offers superior, cloud-based protection from inbound and outbound threats, at an affordable, predictable and flexible monthly or annual subscription price. You can minimize upfront deployment time and costs, as well as ongoing administration expenses without compromising on security.

SonicWall offers VARs and MSPs a greater opportunity to compete and grow revenue while minimizing risk, overhead and ongoing costs. SonicWall Hosted Email Security includes MSP-friendly features such as robust multi-tenancy, central management for multiple subscribers, Office 365 integration, flexible purchase options and automated provisioning.

Learn more about SonicWall Email Security products at: www.sonicwall.com/en-us/products/secure-email.

Management, reporting and analytics

SonicWall believes a connected approach to security management is not just fundamental to good preventative security practice, it also forms the basis for a unified security governance, compliance and risk management strategy. With SonicWall management, reporting and analytics solutions, organizations get an integrated, secured and extensible platform to establish a strong, uniform security defense and response strategy across their wired, wireless, endpoint, mobile and multi-cloud networks. The full adoption of this common platform gives organizations deep security insight to make informed security decisions, and move quickly to drive collaboration, communication and knowledge across the shared security framework.

SonicWall Global Management System

Deployable on premises as software or a virtual appliance, the SonicWall Global Management System (GMS) cohesively manages network security operations by business processes and service levels as opposed to a less efficient device-by-device siloed approach. GMS enables organizations of varying sizes and types to easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities and federate all operational aspects of the security infrastructure. This includes centralized policy management and enforcement, real-time event monitoring, granular data analytics and reporting, audit trails, Zero-Touch Deployment, SD-WAN provisioning and more under a unified enterprise platform.

GMS also meets the firewall change management requirements of organizations through workflow automation. This intrinsic, automated process assures the correctness and the compliance of policy changes by enforcing a rigorous process for configuring, comparing, validating, reviewing and approving security management policies prior to deployment. The approval groups are flexible, enabling adherence to company security policies and assuring the right firewall policies are deployed at the right time and in conformance to compliance regulations.

SonicWall Capture Security Center

Part of the SonicWall Capture Cloud Platform, Capture Security Center is an open, scalable cloud security management, monitoring, reporting and analytics platform that is delivered as a cost-effective Software-as-a-Services (SaaS). It is designed for organizations of various sizes and use cases including distributed enterprises and service providers that are adopting cloud computing for its cost efficiency. Capture Security Center is the ideal cloud security management platform to establish a sustainable, fully coordinated security operation across any networks.

For customers, Capture Security Center offers the ultimate in visibility, agility and capacity to govern the entire SonicWall network security ecosystem with greater clarity, precision and speed – all from one place regardless of location. With an enterprise-wide view of the security environment and real-time security intelligence reaching the right people in the organization, accurate security policies and controls decisions can be made towards a stronger security posture.

For service providers, Capture Security Center simplifies the discrete management of multiple clients' security operations. It creates opportunities for MSP/MSSPs to increase their security services agility while reducing the operating expenses and complexities of supporting a solely owned infrastructure.

SonicWall Analytics

Going beyond security management and reporting, SonicWall Analytics provides an eagle-eye view into everything that is happening inside the network security environment. Its powerful, intelligence-driven analytic engine automates the aggregation, normalization and contextualization of security data flowing through all managed SonicWall firewalls. The accompanying dashboard offer single-pane visibility, authority, and flexibility to perform deep investigative and forensic analysis.

Analytics presents the security data in a meaningful, actionable and easily consumable way for stakeholders to interpret, prioritize, make decisions upon and take appropriate defensive actions. This deep knowledge and understanding of the security environment provides full visibility and capacity to not only uncover but also orchestrate remediation to security risks, and monitors and track the results with greater clarity, certainty and speed. Moreover, weaving Analytics into the business process helps operationalize the analytics by automating real-time, actionable alerts; orchestrating security policies and controls in a proactive and automated fashion; and monitoring the results for security assurance.

Analytics is optimized for both cloud and on-premises deployment use cases. It is licensable as a cost-effective Software-as-a-Services (SaaS) via the Capture Security Center, as a virtual appliance in VMWare or Microsoft Hyper-V private cloud environments, or in AWS or Microsoft Azure public cloud environments. While this gives organizations the operational and economic benefits of virtualization and cloud computing, it also enables dynamic upscaling of storage to fulfill the growing data retention requirements from a virtually unlimited number of firewall nodes.

Learn more about SonicWall management and reporting products at: www.sonicwall.com/en-us/products/firewalls/management-and-reporting.

SonicWall Enterprise Services

Achieve more from your SonicWall network security solution and get the support you need, when you need it. With SonicWall enterprise support and professional services, you'll gain superior long-term value from your solution.

Global Support Services

Get convenient support to keep your business humming along smoothly:

Technical Support

- **8x5** – Monday through Friday, 8 a.m. to 5 p.m. for non-critical environments.
- **7x24** – Around the clock support, including weekends and holidays, for business-critical environments.

Value Add Support

- **Premier Support** provides enterprise environments with a dedicated Technical Account Manager (TAM). Your TAM acts on your behalf as a trusted advisor who works with your staff to help minimize unplanned downtime, optimize IT processes, provide operational reports to drive efficiencies and is your single point of accountability for a seamless support experience.
- **Dedicated Support Engineer (DSE)** provides a named engineering resource to support your enterprise account. Your DSE will know and understand your environment, policies and IT objectives to bring you fast technical resolution when you need support.

Global Professional Services

Need help determining the best security solution for your business, as well as setting it up within your existing infrastructure? Let us take care of it. With Global Professional Services, you get a single point of contact for all your deployment and integration needs. You'll receive services tailored to your unique environment and assistance with:

- **Planning:** Scoping and understanding your firewall requirements.
- **Implementation/Deployment:** Assessing and deploying your solution.
- **Knowledge transfer:** Using, managing and maintaining your device.
- **Migration:** Minimizing disruption and ensuring business continuity.

SonicWall enterprise services are available with NS*sp*/NS*a*/TZ Series/SRA/SMA/Email Security/GMS.

Learn more: https://support.software.com/essentials/support-offerings.

Conclusion

Discover SonicWall security products

Integrate your hardware, software and services for best-of-breed security. Learn more at www.sonicwall.com. Learn about purchase and upgrade options at www.sonicwall.com/how-to-buy. And try out SonicWall solutions for yourself at www.sonicwall.com/trials.

RSA SECURED

ConnectWise CERTIFIED Partner

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.

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.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com