SONICWALL

SonicOS 7.0 and Services Datasheet

The SonicOS architecture is at the core of SonicWall physical and virtual firewalls including the TZ, NSa, NSv and NSsp Series. SonicOS leverages our patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) and patent-pending Real-Time Deep Memory Inspection™ (RTDMI) technologies to deliver industry-validated high security effectiveness, SD-WAN, real-time visualization, high-speed virtual private networking (VPN) and other robust security features.

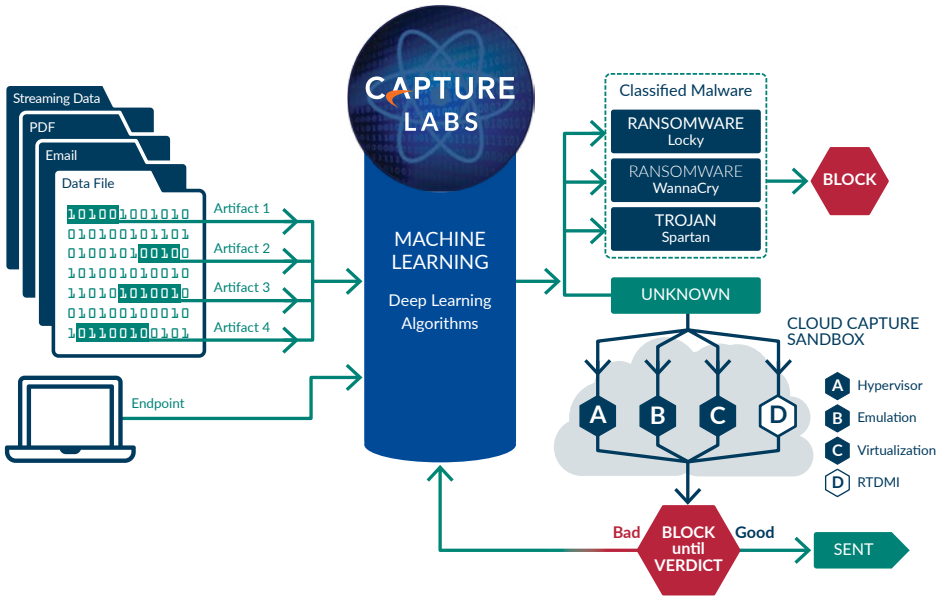
Our vision for securing networks in today's continually-evolving cyber threat landscape is automated, real-time threat detection and prevention. Through a combination of cloud-based and on-box technologies we deliver protection to our firewalls that's been validated by independent third-party testing for its extremely high security effectiveness. Unknown threats are sent to SonicWall's cloud-based Capture Advanced Threat Protection (ATP) multiengine sandbox for analysis. Enhancing Capture ATP is our RTDMI™ technology. The RTDMI engine detects and blocks malware and zero-day threats by inspecting directly in memory. RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds.

In combination, our RFDPI engine examines every byte of every packet, inspecting both inbound and outbound traffic directly on the firewall. By leveraging Capture ATP with RTDMI technology in the SonicWall Capture Cloud Platform in addition to on-box capabilities including intrusion prevention, anti-malware and web/URL filtering, our next-generation firewalls stop malware, ransomware and other threats at the gateway.

The introduction of the brand-new SonicOS 7.0 operating system (OS) further catapults next-generation firewall features and functionality to the next level. It integrates SD-WAN, TLS 1.3 support, real-time visualization, high-speed virtual private networking (VPN) and other robust security features. Built from the ground up, SonicOS 7.0 features advanced security, simplified policy management, and critical networking and management capabilities for distributed enterprises with next-gen SD-Branches and small- to medium-sized businesses.

Security Service Bundles

SonicWall security services turns firewall into a complete security solution. The security services is offered in three subscription bundles – Essential, Advanced and Premier. (i) SonicWall Essential Protection Service Suite provides all essential security services needed to protect against known & unknown threats. (ii) SonicWall Advanced Protection Service Suite offers advanced security to extend the security of your network with cloud essential security services. (iii) SonicWall Premier Protection Service Suite* provides total security with added security services, cloud visibility, analytics & endpoint services for ultimate protection.



*Pending availability

FEATURE	ESSENTIAL	ADVANCED	PREMIER*
Gateway Anti-Virus, Intrusion Prevention, Application Control	√	√	√
Content Filtering Service	√	√	√
Anti-Spam	√	√	√
24x7 Support	√	√	√
Network Visibility	√	√	√
Capture ATP (Multi-Engine) Sandboxing	√	√	√
RTDMI Technology	√	√	√
Basic DNS Security	√	√	√
Cloud Management	!	√	√
Cloud based Reporting – 7 Days	!	√	√
Advanced Cloud Analytics – Virtual, 365 Days Reporting	!	!	√
Advanced DNS Security	!	!	√
Firewall System Check Tool	X	X	√
Cloud App Security Starter Pack	X	X	√
Capture Client Starter Pack	X	X	√
Premier Support	X	!	!

√ *Part of the bundle*
! *Not available with the bundle, but can be purchased separately*
X *Not supported with the bundle*
* *Pending availability*

Enhanced Dashboard

ENHANCED DASHBOARD	
Feature	**Description**
Enhanced Dashboard	Dashboard with actionable alerts.
"Enhanced Device view with display of Front-View,Back-View and Storage Stats of the hardware"	User can now find out from the UI home tab, about the real-time status of front panel, back-panel and storage module usage statistics. Giving you similar experience as if you are physically in front of the hardware.
Real-time System usage and bandwidth usage	User can now view real-time system usage of Core and Bandwidth in the network.
Summarized traffic distribution	Traffic distribution usage on user's firewall with real-time update of most used application.
Summary of top users	Summary of top users based on allowed or blocked sessions; by data sent and received.
Summary of Observed threats	Real-time threat summary of threats seen within customer's network like virus, zero-day malware, spyware, vulnerabilities and risky applications.
Services Summary	Real-time status of enabled or disabled security services like IPS, GAV, Anti-Spyware, Capture ATP or DPI-SSL.
Insights on infected hosts	Displaying the total number of infected host machines in the network in real-time.
Insights on critical attacks	Displaying the total number of mission-critical attacks in the network in real-time.
Insights on encrypted traffic	Displaying the total number of encrypted traffic in the network in real-time.
Summary of top applications	Displaying the top applications used in the network with additional options of sorting by sessions, bytes, access-rule blocks, virus,spyware and intrusions.
Summary of top addresses	Displaying the top address objects used in the network with additional options of sorting by sessions, bytes, access-rule blocks, virus, spyware and intrusions.
Summary of top users	Displaying the top users used in the network with additional options of sorting by sessions, bytes, access-rule blocks, virus, spyware and intrusions.
Summary of top website ratings	Displays the top website ratings by session.
Summary of top country statistics	Displaying the top country statistics by session, dropped traffic, bytes sent or received.
Summary of real-time threat	Displaying top threats with separate statistics for Virus, Intrusions, Spyware and Botnet by sessions.
Enhanced Access Point Snapshot	Displaying statistics on Access Point status in the network and Client associations real-time statistics
Access Point Traffic Rate	Provides real-time bandwidth usage by access-points.
WiFi Client Report	Provides real-time Wi-Fi client report based on OS type, frequency and top client chart

ENHANCED DASHBOARD (CONTINUED)	
Real-Time Wifi Client Monitor	Determines the host machine, OS type, frequency, Access-Point info and data transfer.
Insights to Capture ATP verdicts	Displays verdicts given for File analysis by Capture ATP.
Insights to FileTypes	Displays the type of files based on Capture-ATP report.
Insights to Destination Address	Displays the top destinations being used by malicious files.
Malware Analysis statistics	Displays in-depth statistics on dynamic vs static malware analysis per file.
Location based zero-day Attack Origin Analysis	Displays attack origin by countries.
Capture ATP statistics	Displays insights to total files submitted, dynamically analyzed files, malicious files and average processing time using Capture ATP.
Network Topology View	Topology View displaying hosts, access-points connected in user's network based on device name, mac-address and IP Address
API Driven Management	Management of the firewall is API-driven
SDWAN Wizard	Wizard to automatically configure SDWAN Policy on the firewall
Notification Center	New notification center with summary of threats, event logs and system alert.
Improved Online Help	Online help with links to technical documentation on each and every model.
SDWAN Monitoring	Displays SD-WAN Performance probes and top connections.
Enhanced Packet Monitor Utility	Packet Monitor enhanced to include access rule, NAT Rule and route information.
Storage Device Configuration	Configuration support of storage modules including extended modules. Module usage statistics.
Capture Threat Assessment (CTA) 2.0	New CTA 2.0 report supports new report template with customization options like logo, name and sections. Support for file analysis and malware analysis. Company statistics with industry and Global Average for each section. Separate Executive template with recommendations.
System logs downloads	System logs including console logs that can be downloaded from diagnostics section without user requiring to connect machine to console port to capture console logs. This simplifies debug methods and time for troubleshooting.
SSH Terminal on UI	SSH terminal can be accessed from Web UI.
Grid Check Utility	This utility enables checking IP address of the Grid IP for diagnostics.
Debug Utility	User can enable debug mode within the same firmware and execute debug commands from SSH terminal within the UI.
System Diag Utility Tools	Support for more diagnostic tools like GDB, HTOP and Linux Perf Tool.
Switch Network Overview	SonicWall Switch view like physical view, list view and VLAN view.
Bandwidth Usage per SwitchPort	SonicWall Switch Info displays bandwidth usage per port.
WWAN Status	WWAN Modem and Network status display.

Firewall Features and Services

REASSEMBLY-FREE DEEP PACKET INSPECTION (RFDPI) ENGINE	
Feature	**Description**
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

FIREWALL AND NETWORKING

Feature	Description
Secure SD-WAN	An alternative to more expensive technologies such as MPLS, Secure SD-WAN enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using readily-available, low-cost public Internet services.
REST API	Allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
High availability/clustering	Supports Active/Passive (A/P) with state synchronization, Active/Active (A/A) DPI[2] and Active/Active clustering high availability modes. Active/Active DPI offloads the deep packet inspection load to passive appliance to boost throughput.
DDoS/DoS attack protection	SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
Flexible deployment options	The firewall can be deployed in wire, network tap NAT or Layer 2 bridge[2] modes.
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods. Policy-based routing creates routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage.
Advanced quality of service (QoS)	Guarantees critical communications with 802.1p, DSCP tagging and remapping of VoIP traffic on the network.
H.323 gatekeeper and SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.
SonicWall Switch Integration	SonicWall's first-ever switches provides seamless integration with firewalls for a single-pane-of-glass management and visibility of your network
Single and cascaded Dell N-Series and X-Series switch management	Manage security settings of additional ports, including Portshield, HA, PoE and PoE+, under a single pane of glass using the firewall management dashboard for Dell's N-Series and X-Series network switches.
Biometric authentication	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access.
Open authentication and social login	Enable guest users to use their credential from social networking service such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.
Multi-domain authentication	Provides a simple and fast way to administer security polices across all network domains. Manage individual policy to a single domain or group of domains.
Full API Support	Complete API support for each and every section of firewall UI.
SDWAN scalability	Scalable tunnel interfaces for distributed enterprises.

MANAGEMENT, REPORTING AND SUPPORT

Feature	Description
Cloud-based and on-premises management	Configuration and management of SonicWall appliances is available via the cloud through the SonicWall Capture Security Center and on-premises using SonicWall Global Management System (GMS).
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Analytics or other tools that support IPFIX and NetFlow with extensions.
Compliance-centered malware detection	Analyze suspicious files in your own environment without sending files or results to a third-party cloud.

VIRTUAL PRIVATE NETWORKING (VPN)	
Feature	**Description**
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the firewall to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless, automatic failover and failback of
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.
Improved Match Object	Match Object supports adding applications with an enhanced user experience.
Profile Based Objects	Profile Objects for Endpoint Security, Bandwidth Management, QoS Marking, Content Filter, DHCP Option and AWS VPN.
Action Based Objects	Action Objects for Application Rule and Content Filtering Rule Action.
Enhanced Access Rules	Enhanced Rule Display for intuitive user experience
Customizable Grid Settings	Customizable and movable columns within Access Rules, NAT rules and Routing Rules.
Active and Inactive Rule Display	Displays the rules which are enabled or disabled.
Used and Unused Rule Display	Displays the rules which are actively used or not being used.
Exporting Access-Rules	Exports all the access rules to CSV file.
Live Counter on Access-Rules	Enables capture live statistics on access rules.
Rule Diagram	Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics.
Security Profile in an Access-Rule	Ability to add a security profile within a rule to allow or block DPI, DPI-SSL, Botnet and Geo-IP.
Endpoint Security Rules	Ability to add security rules for endpoint security using Capture Client.
CONTENT/CONTEXT AWARENESS	
Feature	**Description**
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix/Terminal Services SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. Eliminates unwanted filtering of IP addresses due to misclassification.
Regular expression matching and filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

Breach prevention subscription services

CAPTURE ADVANCED THREAT PROTECTION[1]	
Feature	**Description**
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
Real-Time Deep Memory Inspection (RTDMI™)	SonicWall RTDMI is a patent-pending technology and process utilized by the SonicWall Capture Cloud to identify and mitigate even the most insidious modern threats, including future Meltdown exploits. It even detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Broad file type analysis	Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR and APK plus multiple operating systems including Windows, Android, Mac OS and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases.
Capture Client	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and rollback to a previous uninfected state.

ENCRYPTED THREAT PREVENTION

Feature	Description
TLS/SSL decryption and inspection	Decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden inside of encrypted traffic. Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspects data traversing over SSH tunnels to prevent attacks that leverage SSH.
TLS 1.3 Support	Support for TLS 1.3 to improve overall security on the firewall. This is implemented in Firewall Management, SSL VPN and DPI.

INTRUSION PREVENTION[1]

Feature	Description
Countermeasure-based protection	Tightly integrated 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.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly	Identifies and blocks attacks that abuse protocols as they attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.

THREAT PREVENTION[1]

Feature	Description
Gateway anti-malware	The 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.
Capture Cloud malware protection	A continuously updated database of tens of millions of threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
Bi-directional raw TCP inspection	The RFDPI engine scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP. Decodes payloads for malware inspection, even if they do not run on standard, well-known ports.

APPLICATION INTELLIGENCE AND CONTROL[1]

Feature	Description
Application control	Controls applications, or individual application features that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures. This increases network security and enhances network productivity.
Custom application identification	Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications. This helps gain further control over the network.
Application bandwidth management	Application bandwidth management granularly allocates and regulates available bandwidth for critical applications (or application categories), while inhibiting nonessential application traffic.
Granular control	Controls applications (or specific components of an application) based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.

CONTENT FILTERING[1]	
Feature	**Description**
Inside/outside content filtering	Enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.
Enforced content filtering client	Extends policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter.
Granular controls	Blocks content using any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.
Local CFS Responder	Local CFS Responder can be deployed as a virtual appliance in private clouds based on VMWare or Microsoft Hyper-V. This provides deployment flexibility option (Light weight VM) of CFS ratings database in various customer network use cases that require a dedicated on premise solution that speeds up CFS ratings request and response times, supports large number of allowed/blocked URL list (+100K), and adds up to 1000 SonicWall firewalls for CFS rating lookups.
ENFORCED ANTI-VIRUS AND ANTI-SPYWARE[1]	
Feature	**Description**
Multi-layered protection	Utilizes the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block viruses entering the network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure every computer accessing the network has the appropriate antivirus software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management.
Automated deployment and installation option	Machine-by-machine deployment and installation of anti-virus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Next-generation antivirus	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.
ADVANCED SECURITY	
Feature	**Description**
Advanced DNS Security	DNS Security provides better TTD(Time to Detect) and improving TCO(Total cost of ownership). DNS security inspects DNS fields to identify malicious domains and thus block connection at very early stage of connection establishment. SonicWall has petabytes of threat data that helps classify domain as malicious, reducing false positives.
Firewall System Check Tool	Identify risks and enhance the compliance and security. Available on the firewall UI, the Heath Check Tool constantly monitors security infrastructure, gateways, technologies, policies and configuration settings, in real time.
Network visibility	It provides granular network visibility of network topology along with host info
Cloud management	Manage firewalls via cloud through Network Security Manager tile of Capture Security Center
Cloud-based reporting	Includes seven day cloud-based reporting

[1] *Requires added subscription*

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at **www.sonicwall.com/PES**.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com

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

Datasheet-SonicOSplatform-COG-2584