Managed Firewall Security & Unified Threat Management

Build a Wall Around Your Network with Advanced Gateway Security Suite (AGSS)

An effective information security program starts with a good Network perimeter security plan. You need reliable technology and best practices that will stop viruses, spyware, worms, Trojans, and key loggers and other intruders, before they enter your network. Firewalls and Unified Threat Management (UTM) provide the foundation necessary to protect your organization's data, network and critical assets from cyber criminals. But what if you don't have an in-house IT department, or the budget to hire a trained security expert? And what about the cost of the hardware and software you'll need to buy and maintain going forward? The solution is a managed security service with AireSpring.

SONICWALL ADVANCED GATEWAY SECURITY SUITE (AGSS)

AireSpring provides industry-leading software, now with SonicWall's newest Advanced Gateway Security Suite (AGSS), hardware technology, and the needed expertise to secure your information assets 24/7/365, all at a fraction of the cost of in-house security resources. AireSpring's Managed Security Service provides a comprehensive solution of technology and support services designed to defend your network against a wide range of emerging threats. AireSpring provides the configuration, monitoring, alerting and updating that your firewall and UTM hardware and software will need. Round-the-clock technical support and a 60-minute-or-less Call-Back SLA are included along with automatic weekly reports and analysis by certified security engineers. Ensure that your security solution will always be prepared to handle the latest threats with our ongoing hardware replacement and software upgrade program to keep you one step ahead of the cyber criminals. Strengthen your defenses, protect your business and lower your costs with AireSpring.

BENEFITS

- **Get an all-in-one solution.** Combines the features of traditional firewalls, gateway anti-malware products, intrusion prevention systems and content filtering packages into a single solution. All of these security technologies are installed, configured, deployed, and managed as one unit. All event data is available through one reporting system so it is easier to identify threats early and take appropriate measures BEFORE your security has been compromised.
- **Capture Advanced Threat Protection (ATP).** This cloud-based network sandbox utilizes new technology that analyzes suspicious code to help discover and stop newly developed malware. A multi-engine cloud-based sandbox, it includes SonicWall's Real-Time Deep Memory Inspection (RTDMI), virtualization, hypervisor level analysis and full-system emulation. Automated breach prevention is enabled by blocking files until a security verdict is determined, and near real-time signature deployment protects organizations from follow-on attacks.
- **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. RTDMI proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory.
- **Unified Threat Management (UTM).** UTM provides real-time network threat prevention using a continuously updated list of internet threat signatures. It also performs Reassembly-Free Deep Packet Inspection (RFDPI) on all network traffic, exposing hidden threats.
- **Gateway Anti-Malware & Anti-Virus.** Get greater virus-scanning capabilities, enhanced threat protection, scalability, a dynamically-updated database and granular reporting.
- **Intrusion Prevention Service (IPS).** IPS integrates an ultra-high performance deep packet inspection architecture and dynamically updated signature database to deliver complete network protection.

Protect your network with comprehensive security at a small business price.

ENHANCE PROTECTION AND DISASTER RECOVERY

- Now with AGSS real-time gateway anti-virus engine that scans for and blocks viruses, Trojans, worms, rootkits and polymorphic "zero-day" malware at the gateway, before they reach your network.
- Dynamic spyware protection blocks the installation of malicious spyware and disrupts existing spyware communications.
- Application Control provides a solution for setting policy rules for application signatures, including more targeted policies for global App Control and App Rules.
- Geo-IP Filtering allows administrators to block connections coming to or from a geographic location. Our Geo-IP Filtering Best Practices secure your network from undesired connections while giving you access to the resources you need to get things done.
- DPI-SSL Inspection - Gain visibility into SSL/TLS encrypted traffic, block hidden malware downloads, and much more to enhance security, application control and data leak prevention.
- Dynamically updated signature database provides continuous threat protection.
- Prevents "drive-by downloads" from infected web sites.
- Detects protocol anomalies and buffer overflow attacks.
- Blocks outbound botnet "command and control" traffic from stealing your customer lists, credit card information, patient or employee information, engineering designs, trade secrets, and other confidential information and intellectual property.
- Prevents employees from visiting websites containing content related to pornography, gambling, hate crimes and other objectionable topics.
- Ensures that high-priority applications (CRM, order processing) will get more bandwidth than less urgent applications (chat, video streaming).

Capture Advanced Threat Protection (Capture ATP)

- Rapidly deploys remediation signatures to other network security appliances.
- Establishes advanced protection against the changing threat landscape.
- Analyzes a broad range of file types.

Content Filtering Service (CFS)

- SonicWall Content Filtering Service (CFS) blocks inappropriate, unproductive and even illegal and malicious web content.

Managed Security Service

airespring®
Cloud, Fully Managed and Connected

A better IT approach from AireSpring

Many businesses struggle to protect their network with the necessary IT security protocols and lack the in-house technical expertise to properly configure, run and manage a firewall.

SonicWall Advanced Gateway Security Suite (AGSS) combined with AireSpring's Managed Security Service is the solution. Rest easy with 24/7 network monitoring by AireSpring's trained SonicWall AGSS security experts, and enjoy long-term peace of mind with ongoing software and security updates. Additionally, you'll be able to upgrade or exchange your firewall as your needs change, and as technology changes – further future-proofing your solution.

Compare the services included with an AireSpring Managed Security plan versus standard vendor support.

Feature/Capabilities	Run your own firewall and utilize standard vendor support	Managed Security from AireSpring
Firewall & Security Configuration		
Appliance Configuration by SonicWall-Certified Engineers (approx. 5 hours included)	No	Yes
Turn-key solution delivered to customer's doorstep	No	Yes
Network details and topology documentation (dramatically improves customer experience)	No	Yes
Multi-engine Sandbox monitoring, Alerting & Updating	No	Yes
Monitoring, Alerting & Updating		
Global Management System Monitoring	No	Yes
Hosted and Secure GMS Infrastructure	No	Yes
Proactive Response to Site Down	No	Yes
Analysis and updating of firmware, software, and security updates	No	Yes
Weekly offsite SonicWall configuration Backup	No	Yes
Reporting		
Automatic Weekly Network Reports	No	Yes
Report analysis by SonicWall-Certified Engineers	No	Yes
Support		
24x7 AGSS support with firmware updates and hardware replacement	No	Yes
Answer product related questions	Yes	Yes
Answer security related questions	No	Yes
24x7 Level-3 Technical Support	No	Yes
Superior support experience due to onboarding documentation of customer network	No	Yes
Live Operator During Business Hours - No Hold Queue	No	Yes
60-Minute or Less Call-Back SLA	No	Yes
Hardware Replacement		
Hardware Replacement for Manufacturing Defects during Warranty	Yes	Yes
Ongoing hardware replacement throughout managed service period	No	Yes
Upgrade appliance as future business and technology changes dictate	No	Yes
Overnight Hardware Replacement	No	Yes
Replacement Preconfigured with Most Recent Settings (from backup)	No	Yes

Ready to find out more? Contact us at 888-389-2899,
email sales@airespring.com, or visit our website at www.airespring.com