



## Managed Security - Optional Services

**Managed Security Services from Bright House Networks Business Solutions protect your business against Internet threats that put your data – and your bottom line – at risk. These services incorporate technology to detect those threats, and the ability to respond quickly to prevent adverse impact to your business-critical information. Small and medium size organizations face many of the same network security issues as larger enterprises. Bright House Networks Business Solutions Managed Security is suited to businesses of all sizes, with comprehensive network security services.**

### UNIFIED THREAT MANAGEMENT

The SonicWALL platform provides unsurpassed price-performance and multi-layer security services ranging from basic firewall protection to full Unified Threat Management (UTM).

Malicious software is now typically designed to be concealed within legitimate network usage. UTM includes gateway anti-Virus, Anti-Spyware and Intrusion Prevention services. These services use deep packet inspection (DPI) technology to check all network traffic attempting to pass through the firewall, compare the data to a signature database of thousands of known threats and, in the event a match is found, block the traffic in the firewall before it can penetrate the network and do any harm. The signature database is automatically updated to ensure the maximum level of security.

UTM can block viruses and other threats that could potentially attack your network such as those that are embedded in web pages, attached to email messages or may be using a “back door” that a traditional firewall would not stop.

UTM can also be used to control non-business-related Internet use such as access to inappropriate Internet sites. With SonicWALL Content Filtering which is included with UTM, you can implement your company’s

Acceptable Use Policy (AUP) and prevent network abuse before it happens. Your Managed Security Service from Bright House Networks Business Solutions includes Management Reports that enable you to determine how your employees are using your network.



## **UNIFIED THREAT MANAGEMENT (cont'd) -**

You can see if employees are visiting objectionable sites, determine whether certain sites or activities such as the use of streaming media, peer-to-peer network applications (frequently used to share music) and Instant Messaging should be blocked, and then block them for only those employees that you specify.

By proactively implementing your AUP using UTM, you can prevent undesired network usage before it occurs and that will result in increased worker productivity and reduced legal risks from inappropriate use of your network. Bright House Networks highly recommends that you add our UTM service option to your Managed Security Service.

## **THREAT DETECTION SYSTEM**

Today's multi-layer firewall-based technology that uses updated anti-virus databases will stop nearly all known malicious software before it penetrates your network, but not all threats are known and not all threats enter from the Internet. When new harmful viruses are released into the Internet, the security community responds as quickly as possible by developing and distributing anti-virus software to minimize the damage caused. Viruses that infect your mobile users' laptops while they are away from your secure internal network may circumvent your gateway-based protection when the infected laptop is then plugged back in to your internal network.

Today's most sophisticated firewalls are designed to catch problems before and not after they penetrate your network. If viruses and other malicious software do get inside your network, they need to be detected and eliminated right away. To protect your network from the inside, our Threat Detection System continuously examines what's happening on your network and detects suspicious activity. Each day our Threat Detection System examines millions of event records received from firewalls all over the country.

Our automated systems sift through these records and use them to help learn what your normal network usage patterns are and what would constitute abnormal usage that may indicate a problem.

Often the only indication of a problem is a simple change in the behavior of a computer from one day to the next. Our Threat Detection System performs dozens of tests every few minutes and every hour to determine if there are active threats operating within your business network.

For example, if a computer that never sends any email suddenly starts sending a large quantity of email, it may indicate that it is infected with malicious software, and this behavior will trigger an event in our Threat Detection System. If our system determines there is a potential problem, all of the related information is combined and presented to a security analyst whose job it is to investigate the event and determine if the threat is real or not. If the incident is determined to be a problem, we immediately contact you or your designated systems administrator to resolve the issue.

Our Guardian and Sentry packages provide our Our Guardian and Sentry packages provide our advanced Threat Detection service and can be optionally added to any SonicWALL platform. This technology allows us to identify threats inside your network and notify you in the event of a problem. You can choose to have your network monitored Monday-Friday 8:00 am to 5:00 pm (Guardian-level service) or 24/7/365 (Sentry-level service).

## **MULTIPLE VIRTUAL PRIVATE NETWORK CONNECTIONS (VPNS)**

An optional feature of your Managed Firewall Service is the support for Multiple VPNs. If you have more than one location or employees who work from multiple locations such as home, on the road or from customer or vendor locations, Bright House Networks Business Solutions can provide a VPN solution with your Managed Firewall Services that is right for your company.

## **SECURE WIRELESS ACCESS FOR YOUR BUSINESS**

Our security experts will help design a wireless solution for your business that is highly secure and can remain so even when providing guest access. We can help deploy wireless services that enable guests to connect to your wireless network and have access to the Internet or email – but without having access to your business-critical data.