



VOICE SERVICES
DATA & INTERNET SERVICES
VIDEO SERVICES
COMMUNICATION SERVICES
MANAGED SERVICES
ENTERPRISE SOLUTIONS

Managed Security

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.

STANDARD SERVICES

SYSTEM MANAGEMENT

Bright House Networks Business Solutions certified personnel install and configure customer firewalls or VPNs for maximum security. Our services include unlimited technical support, system maintenance, configuration backup and repair or replacement of defective equipment and up/down monitoring during normal business hours.

PRO-ACTIVE SECURITY MONITORING

Pro-active security monitoring by our trained professionals and automated systems provides a complete security solution for your network. Our monitoring systems track network usage and alert our staff in the event of an outage. Our personnel investigate the outage and, when appropriate, work together with you to determine the most secure resolution. We continuously monitor these security systems to assess the health of your network. In the event of a failure by any monitored device, our personnel are notified and can respond immediately.

FIREWALL TECHNOLOGY AND VIRTUAL PRIVATE NETWORK (VPN)

All Managed Security service offerings include a state-of-the-art firewall from SonicWALL, a world leader in network security products. Our Managed Firewall service provides traditional firewall protection (e.g. port and address blocking) as well as VPN support. It compares data to a signature database of thousands of known threats. In the event there is a match, the traffic is stopped before it can do any harm. The database is automatically updated every few hours protecting against frequently occurring zero-day threats.

A VPN is included with your Managed Firewall service. If you have employees at more than one location or employees that travel, they will likely need access to the network and information stores. With VPN solutions from Bright House Networks Business Solutions, we can extend the secure network to anywhere in the world as long as there is Internet access.

MANAGEMENT REPORTS

Managed Security Services provides access to a variety of real-time reports through the My Services portal to help you manage your network usage. Reports such as “Top Websites,” “Top Users” or “Bandwidth Usage” can help you quickly identify problem areas and reduce non-essential network usage.

THREAT DETECTION

Our automated systems sift through the records that result from normal Internet usage and search for events that indicate a problem. Sometimes the only indication of a problem is a simple change in behavior of a computer from one day to the next. For example, if a computer that never sends any email suddenly starts sending large quantities of email, it is most likely infected with malicious software and will trigger an event in our system.

Once our systems determine there is a potential problem, all of the related information is combined and presented to a security analyst whose job is to investigate the event and determine if there really is a threat. If there is a problem, we immediately contact you to resolve the issue.

BRIGHT HOUSE NETWORKS
business solutions



Where business gets personal.

OPTIONAL SERVICES

UNIFIED THREAT MANAGEMENT

Malicious software is now typically designed to be concealed within legitimate network usage. Unified Threat Management (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.

CONTENT FILTERING

UTM can also be used to control non-business-related Internet use such as access to inappropriate Internet sites. Content Filtering is included with UTM, enabling you to implement your company's Acceptable Use Policy (AUP) and prevent network abuse before it happens.

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.

MULTIPLE VIRTUAL PRIVATE NETWORK CONNECTIONS (VPNS)

One VPN license is included with your Managed Firewall service. If additional-use VPN licenses are required, Bright House Networks can provide a VPN solutions that is right for your business, ensuring your employees can securely access your network remotely.

LEARN MORE

Contact us at **1-877-424-9246** or visit brighthouse.com/business to discover how Managed Security from Bright House Networks Business Solutions can help your business do more with less.

brighthouse.com/business

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.

MANAGED SECURITY SERVICE LEVELS

Features & Service Levels	Basic Service & Monitoring	Guardian Threat Detection Response & Monitoring	Sentry Threat Detection Response & Monitoring
Responses to Outages	Mon-Fri 8 – 5		24 x 7
After Hours Emergency Support 24 x 7	Mon-Fri 8 – 5		
Unlimited Technical Support	Mon-Fri 8 – 5		
Web Portal with Online Reports, Network Health History, Customer Support	Mon-Fri 8 – 5		
Repair/Replace Defective Equipment related to Managed Security	Mon-Fri 8 – 5		
Guaranteed Response Time for Non-Emergency Support Requests	4 Hours *		
Guaranteed Response Time for Emergency Support Requests	1 Hour *		
Bright House Networks Threat Detection & Response	No	Mon-Fri 8 – 5	24 x 7
SonicWALL's UTM Enhanced Security Software	Available		

*Response times for non-emergency requests are 4 business hours; Monday through Friday 8:00 am to 5:00 pm. Response times for emergency requests are 1 hour 24x7.

BRIGHT HOUSE NETWORKS
business solutions



Where business gets personal.