CAPABILITIES REVIEW

Unlimited | Network Security

GFI™
Aurea SMB Solutions

GFI Unlimited|Network Security provides multiple layers of security to protect small and medium businesses (SMB). SMBs (typically ranging from 10 to 500 employees) are caught between consumer solutions which they may have first turned to (and which don't offer enough protection), and enterprise-grade security (which can cost too much and/or be too complex for smaller teams to deploy).

Faced with a difficult choice, some do nothing, or install a single line of defence, such as an upgraded anti-virus. GFI Unlimited|Network Security offers an alternative, a solution with multi-layered security:

- Secure Network perimeter to block threats at your doorway
- Secure Traffic with Web & Email Antivirus and content filtering
- Secure Endpoints with Vulnerability monitoring and patching to prevent being exploited

Unlimited|Network Security creates these multiple layers of security through the deployment and usage of multiple security capabilities at each layer. Most importantly, it is available through a single, simple, value-priced solution delivering more capabilities than SMBs typically receive when they purchase one product from other vendors. Here is an overview of some of the most critical capabilities:

Firewall & intrusion prevention

Unlimited|Network Security delivers an all-in-one Unified Threat Management (UTM) solution providing comprehensive next-generation firewall protection of your network and data. It includes the following and more:

- Deep Packet Inspection (DPI)
- Stateful Packet Inspection (SPI)
- Intrusion Detection and Prevention System (IDPS)
- Application awareness
- DHCP server
- DNS forwarding
- NAT mapping (inbound/outbound)
- MAC filtering
- GeoIP filtering
- Zero-configuration networking
- Service Discovery forwarding
- Anti-Spoofing
- Guest network with captive portal
- 802.1Q VLAN support
- Traffic rules configuration wizard
- Time based rules
- Connection limits (DoS protection)
- Dynamic DNS
- Customizable routing table
- Reverse proxy
- Simultaneous IPv4 and IPv6 support
- IPv6 network prefix translation
- IPv6 router advertisements
- Multiple IP addresses on a single network interface (multihoming)

Secure VPN & site-to-site connections

Secure your client-to-site connections with a high-performance, configuration-free VPN client—or use an industry-standard IPsec VPN client, such as those pre-loaded on mobile devices.

To create secure, high-performance, server-to-server connections between offices running Kerio Control, use Kerio's easy-to-setup VPN technology. Or, to create a secure VPN connection to a remote office without Kerio Control deployed, use the industry-standard IPsec VPN protocol. Enable 2-step verification for an extra layer of security on all forms of remote access.

Our Secure VPN includes:

- VPN client for Windows, Mac & Linux
- Split tunneling
- Multiple client-to-site and site-to-site tunnels
- IPsec client-to-site/site-to-site
- L2TP/IPsec for mobile devices
- Persistent connection
- SSL encryption
- VPN tunnel failover
- NAT support
- Automatic or custom routing
- User authentication via directory services

Web antivirus & malware protection

Unlimited|Network Security includes web scanning for viruses and malware powered by Bitdefender. Configuring it takes only seconds and scanning will begin on multiple protocols.

You can always have the latest protection and definitions by configuring how frequently you receive definition updates, as well as see at-a-glance when your last update was.

Email antivirus & malware protection

Email traffic is a major source for viruses and malware. Unlimited|Network Security uniquely provides advanced email threat protection using four antivirus engines (powered by industry-leaders Bitdefender, Avira, Kaspersky and Cyren).

You can take advantage of the strengths of each engine. Antivirus engine vendors have different response times to new viruses and malware. This capability ensures your system will detect new threats in the shortest possible time.

Policy-based content & application filtering

Unlimited|Network Security provides two policy-based content filtering configurations that protect your company's web and email traffic.

Web traffic content filtering

Identify multiple traffic source types and then configure controls for web traffic and content including being aware of applications which might hold content that needs to be secure or prevented from leaving your organization. This capability includes 500 different web and application content categories, covering 99.9% of the active web at 99% accuracy, providing maximum protection and flexibility.

While powerful, filters are easy to set up in a few clicks and then displayed so that anyone managing them can quickly understand the situation. With the ability to configure even user and group settings with time limits, advanced web content filtering includes:

- Application awareness
- Configuring FTP policy
- Configuring HTTP policy
- Filtering web content by words
- Blocking inappropriate or explicit content
- Filtering HTTPS connections
- HTTPS filtering specifics
- Eliminating peer-to-peer traffic

Email traffic content filtering

Email traffic content is filtered using four advanced content filtering engines. Advanced user-based filtering rules enable flexible and granular filtering of any part of the email message--including message headers, subject, body, attachment name and attachment content using different types of pattern matching methods, including regular expressions.

You could for example use the keyword checking functionality to scan emails for keywords that are inappropriate or offensive. This can also serve as another spam filter if configured to block common spam keywords.

Email content filtering can also be applied to outbound emails to prevent data leakage of personal or private information using keywords related to credit cards, personal identification numbers and more. This is in addition to filtering outbound messages in the event of having been exploited as an SMTP relay.

Vulnerability scanning

Unlimited|Network Security's vulnerability scanner can identify more than 60,000 vulnerabilities. It scans devices, identifies and categorizes security vulnerabilities, recommends a course of action and gives you the tools to solve the problem. The graphic threat level indicator provides an intuitive, weighted assessment of the vulnerability status of scanned devices.

This capability ships with a thorough vulnerability assessment database, including standards such as OVAL (11,500+ checks) and SANS Top 20. This database is regularly updated with information from BugTraq, SANS Corporation, OVAL, CVE and others. The auto-update system keeps it continuously up-to-date with newly released Microsoft security updates and vulnerability checks.

It keeps your switches, routers, access points and printers secure from attack. It also supports vulnerability scanning on smartphones and tablets running Windows®, Android™ and iOS®, plus a number of network devices such as printers, routers and switches from manufacturers like HP®, Cisco® and many more.

Patch management

Unlimited|Network Security not only scans for vulnerabilities, it also remediates patches and updates for operating systems and applications. Compatible with Microsoft®, Mac OS X® and Linux®, operating systems, as well as many third-party applications. Scan your network automatically or on-demand. Auto-download missing patches or roll-back patches.

In addition to core operating systems, the third-party patch support is extensive: providing management of popular applications like Apple QuickTime®, Adobe® Acrobat®, Adobe Flash® Player, Adobe Reader®, Adobe Shockwave® Player, Mozilla® Firefox®, Mozilla Thunderbird®, Java® Runtime and supports all major browsers (Microsoft Internet Explorer® Mozilla Firefox®, Google Chrome™ Apple Safari® and Opera™).

Threat level reporting

Unlimited|Network Security organizes devices that it scans, grouping them based on type, OS, or by where you place each device and network. Using scan results, it provides a view of the threat and risk levels for each group, network, or device, and provides a breakdown of threat and risk levels based on severity of open vulnerabilities and patches.

In addition, the dashboard will report your vulnerabilities and patches based on several view types:

- Dashboard overview
- Computers view
- History view
- Vulnerabilities view
- Patches view
- Ports view
- Software view
- Hardware view
- System Information view

On each you have the ability to begin taking actions such as (remediate, acknowledge, ignore, change severity, and edit rules management.)

Compliance auditing

Unlimited|Network Security provides a wide range of detailed reporting to track risk and compliance over time. These reports ensure you have proof that you have an active safeguard strategy to stay compliant with regulations. If your company is not bound by specific compliance regulations, these reports can help guide your security actions to meet and exceed your business needs and customers expectations.

Compliance reports and auditing cover (pre configured), for:

- PCI DSS Compliance
- HIPAA Compliance
- SOX Compliance
- GLBA Compliance
- PSN CoCo
- CIPA
- FERPA Compliance
- ISO/IEC 27001 & 27002
- FISMA Compliance
- CAG Compliance
- NERC CIP

Traffic monitoring

Unlimited|Network Security provides traffic monitoring visibility into your real-time traffic, both incoming and outgoing. It also provides information about bandwidth management rules you have set and their quotas and limits.

This includes monitoring:

- Active hosts
- Active connections
- System health
- User statistics
- VPN clients

Traffic monitoring provides insights needed to set your QoS and bandwidth management rules. These rules can be based on traffic type, users, interfaces, link speeds, large data transfer detection, and time of day.

Capabilities Cheat Sheet

Firewall & intrusion prevention

All-in-one Unified Threat Management (UTM) solution providing comprehensive next-generation firewall protection of your network and data. Including intrusion prevention and many other enhanced security tools. (software & hardware appliances available).

Secure VPN & site-to-site connections

Secure your client-to-site connections with high-performance, configuration-free VPN clients—or use an industry-standard IPsec VPN client, such as those pre-loaded on mobile devices. Two-step verification, and L2TP/IPsec for mobile devices.

Web antivirus & malware protection

Web scanning for viruses and malware powered by Bitdefender. Configure it in seconds; scanning will begin on multiple protocols.

Email antivirus & malware protection

Uniquely provides advanced email threat protection using four Antivirus engines (powered by industry leaders Bitdefender, Avira, Kaspersky and Cyren).

Policy based content & application filtering

Provides two policy-based content filtering configurations that protect your company's web and email traffic. It includes 500 different web and application content categories covering 99.9% of the active web at 99% accuracy providing maximum protection and flexibility. Get email content filtering using four core engines that scan both inbound and outbound traffic.

Vulnerability scanning

The vulnerability scanner can identify more than 60,000 vulnerabilities. It scans devices, identifies and categorizes security vulnerabilities, and recommends a course of action. The vulnerability assessment database includes standards such as OVAL (11,500+ checks) and SANS Top 20. It is updated frequently from BugTraq, SANS Corporation, OVAL, CVE and others.

Patch management

Remediate patches and updates for operating systems and applications. Compatible with Microsoft®, Mac OS X® and Linux®, operating systems, as well as many third-party applications such as Apple QuickTime®, Adobe® Acrobat®, Adobe Flash® Player, Adobe Reader®, Adobe Shockwave® Player, Mozilla® Firefox®, Mozilla Thunderbird®, Java® Runtime and supports all major browsers (Microsoft Internet Explorer® Mozilla Firefox®, Google Chrome™ Apple Safari® and Opera™).

Threat level reporting

Using scan results it provides a view of the threat and risk levels for each group, network, or device, and provides a breakdown of threat and risk levels based on severity of open vulnerabilities and patches.

Compliance auditing

Provides a wide range of detailed reporting to track risk and compliance achievements over time. These reports ensure you have proof of an active safeguard strategy to stay compliant with regulations (credit card, healthcare, data privacy, etc.)

Traffic monitoring

Provides traffic monitoring visibility into your real-time traffic, both incoming and outgoing, giving you the insights required to set your QoS and bandwidth management rules.