SOPHOS

Next Gen Firewall and UTM Buyers Guide

Implementing and managing a network protected by point solutions is far from simple. But complete protection doesn't have to be complicated. This buyers guide explains how to choose a unified threat management (UTM) solution that simplifies network security and data protection by integrating security capabilities within a single platform.

UTM defined: What it is and what it can do for you

For every new technology—such as wireless access points, mobile devices and cloud computing—new threats emerge. And as the threats expand a new class of security products comes to market. These hardware and software solutions are designed to reduce risk. But they complicate the IT infrastructure, increasing costs and risks.

You have to separately purchase, configure and manage each additional level of protection, while keeping your security policies consistent. Your IT department must have the appropriate skills and training, and be properly staffed to handle the additional operations. Few organizations have the budget to accommodate every point solution they need. Those that do face the risk of operating a disconnected security program.

To further complicate matters, businesses are increasingly distributed. Remote workers and branch offices require the same level of IT security as the main office. Extending consistent policies and protection across the organization increases complexity and costs. Moreover, it leads to vulnerabilities that put the network and data at risk.

Unified threat management (UTM) addresses the major challenge faced by many of today's IT organizations: how to deliver uniform protection everywhere. UTM is a suite of security software integrated into a single platform to uphold consistent security policies and protection across the organization. And a single platform offers a centralized management console. So your staff only needs to learn one product and deal with one vendor.

UTM: What Gartner says

According to the 2012 Gartner Magic Quadrant for Unified Threat Management:

> Gartner defines the UTM market as multifunction network security products used by small or midsize businesses (SMBs). Gartner defines midsize businesses as those with 100 to 1,000 employees, and with revenue ranging from $50 million to $1 billion. However, the majority of midsize business' annual revenue is in the range of $100 million to $500 million, with head count ranging from 20 to 1,000 employees. UTM products for this market need to provide the following functions as a minimum:

- Standard network stateful firewall functions
- Remote access and site-to-site virtual private network (VPN) support
- Web security gateway functionality (anti-malware, URL and content filtering)
- Network intrusion prevention focused on blocking attacks against unpatched Windows PCs and servers[1]

Go here to read the full report:

Sophos.com/magicquadrant

[1] Gartner, Inc. "Magic Quadrant for Unified Threat Management," by Joe Pescatore and Greg Young, March 5, 2012. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

What to look for in a UTM

Before selecting a UTM product you should evaluate your needs, current technology and what the market offers. After all, you aren't evaluating a single piece of software. You're evaluating and purchasing a suite of software to address your changing business needs. As you begin evaluating solutions, consider these questions.

1. Is it adaptable to your future needs?

Many UTM vendors use proprietary hardware and limit the features available on some of their models. This could require you to spend more money for the model that has the features you need. Similarly, the use of proprietary hardware limits how easy it is to add new options and features to the product. And the hardware may not fit in all environments.

Since you may not know what features you'll need in the future, choose a UTM with a consistent feature set across all models. And look for a solution that can be easily updated as your business needs change. That way you won't get locked into a product that can't deliver the protection you need.

Also consider vendors that offer different deployment models. A hardware appliance may be a good fit for your organization today. But it may not be the best option as you extend to the cloud. Vendors that offer hardware, software and virtual appliances will give you the flexibility you need as your infrastructure evolves.

2. Does it support virtualization and the cloud?

Don't forget to also consider your current and future plans to use virtualization and cloud technologies. The growing use of virtualization and hybrid cloud architectures is changing the IT environment. Be sure your UTM choice supports or can work with these solutions.

Bandwidth becomes increasingly important when you move to the cloud. Many UTM vendors tout network throughput numbers that are not achievable unless you use a specific set-up or disable many of the features. Consider your real-world bandwidth needs, and choose a product that fits those needs.

3. Does it offer add-ons?

A UTM product should provide a variety of capabilities with the option to add functionality. At a minimum, it should provide stateful firewall functionality, VPN support (both site-to-site and remote user), web security (content filtering and malware protection) and network intrusion protection (IPS). Additionally, you may also look for email security (protection for both servers and users), wireless LAN protection, web application control and endpoint protection. This is what is available today.

You also want a vendor that continues to invest in its UTM. The UTM you choose should be able to quickly evolve and add capabilities to address new threats, technologies and business practices.

4. Is it easy to use?

Most leading UTM vendors offer browser-based management and promise ease of use. But don't take the vendor's word for it. With such a varied suite of products, the UTM management interface should be intuitive enough that non-experts can understand and use these features. Take the product for a trial run or walk through a demo to see the user interface for yourself.

5. Does it offer complete security?

When choosing a UTM you should think about complete security for your entire organization. It's important to consider each feature to make sure that it will provide the functionality and protection you need everywhere. Don't just look at the features you need now. Take a look at the others in case you have a need for them in the future.

Here are the features you should consider:

- Network protection
- Web protection
- Email protection
- Webserver protection
- Wireless protection
- Endpoint protection

The following sections describe the UTM features and capabilities you need in each of these areas to keep your network and data secure.

Network protection

Attackers are continually changing their attack methods to avoid detection. The best way to protect the network against these new and emerging threats is through multiple layers of defense. A UTM's network security software should be an integrated suite of capabilities that provides defense-in-depth. It should also permit secure remote access and basic network management functionality.

You need a UTM product that provides a solid network security foundation even before you add network protection subscriptions or licenses. At a basic level UTM should include static routing, DNS proxy services, DHCP server options, NTP functionality, stateful firewall, network address translation, basic remote access VPN, local user authentication, local logging and daily reports, and basic management functionality.

Network protection should build on these features with the following:

- Intrusion prevention system (IPS)
- Bandwidth control/quality of service (QoS) features
- Site-to-site VPN options
- Remote access options
- Remote office support
- Detailed network/bandwidth usage and network security reports

Capability to look for	Description	Questions to ask your vendor
Intrusion prevention system	Bolsters your firewall's security policy by inspecting approved traffic for malicious packets. Can drop packets that match a signature list of threat patterns.	‣ What kind of expertise is needed to properly use the system? ‣ How are rules delivered and configured?
Bandwidth control/Quality of service	Prioritizes traffic based on the rules you set and allows you to control how a fixed resource is used during different conditions.	‣ How many WAN connections can you support on a single appliance? ‣ How easy is it to identify and control the bandwidth applications use?
Site-to-site VPN options	Links remote sites with the main office, allowing users to send and receive information via a secure connection. Also allows employees to use devices such as file servers and printers that are not in the same office.	‣ What protocols does your VPN support? ‣ How much experience or VPN knowledge is required to set up a VPN?
Remote access options	Allows users to securely connect to the UTM appliance from any location.	‣ Do you offer multiple remote access options including clientless VPN? ‣ Is remote access supported from any OS and/or device? ‣ Is the clientless VPN truly clientless or are applets required on end-user devices? ☐ Additional licenses required
Remote office support	Connects remote office networks to the UTM appliance to protect them with the same policies and capabilities.	‣ How easy is it to connect remote offices? ☐ technician required ‣ Can remote offices be centrally managed? ‣ Are additional subscriptions or licenses needed?
Detailed reports	Provides detailed real time and historical statistics and reports on network/ bandwidth usage, network security, etc.	‣ Does the UTM contain a built-in hard drive? ‣ What kind of reports are available without a separate application?

Web protection

You may already block access to potentially dangerous URLs with a web filter. But many filters inspect traffic from the sidelines, providing little if any malware scanning. They rely solely on reputation for security, which leaves users vulnerable to sophisticated malware threats on the web.

You need web protection that allows you to apply terms and conditions to where and how users spend their time online, and stops spyware and viruses before they can enter the network. Detailed reports should show you how effective your policy is so you can make adjustments.

Web protection should include the following:

- URL filtering
- Spyware protection
- Antivirus scanning
- HTTPS scanning
- Application control
- Interactive web reporting

Capability to look for	Description	Questions to ask your vendor
URL filtering	Controls employee web usage to prevent casual surfing and to keep inappropriate content and malware off the network.	‣ Are live updates available? ‣ How many web surfing profiles can be created and used?
Spyware protection	Prevents malicious software from installing on employees' computers, consuming bandwidth and sending sensitive data out of the network.	‣ Are live updates available?
Antivirus scanning	Scans content before it enters the network to prevent viruses, worms and other malware from infecting computers on the network.	‣ Are live updates available?
HTTPS scanning	Provides visibility into encrypted web traffic to protect the network against threats that can be transmitted via HTTPS.	‣ Can HTTPS traffic be inspected and checked against policies?
Application control	Provides visibility into how employees are using the web and controls which applications they can use and how.	‣ Are live updates available?
Interactive web reporting	Provides flexible reporting capabilities to allow administrators to build their own reports.	‣ Are real-time and historical usage reports available? ‣ Can reports be scheduled for delivery? ‣ Is a third-party reporting application required?

Email protection

Protecting email against spam and viruses isn't a new problem. But that doesn't mean all products perform equally. Email security threats continually evolve, making email protection a full-time job that never ends. You need email protection so that common email problems don't affect the business, such as spam, viruses and keeping confidential information private. You need a sophisticated email protection solution supported by a vendor that researches new threats and develops proactive protection.

Email protection should include the following capabilities:

- Anti-spam
- Antivirus scanning
- Email encryption
- User portal

Capability to look for	Description	Questions to ask your vendor
Anti-spam	Stops spam and other unwanted email from being delivered to employees' inboxes.	‣ What are your spam detection and false positive rates? ‣ What techniques do you use to identify spam?
Antivirus scanning	Scans and blocks malicious content at the gateway to stop viruses and other malware from infecting computers.	‣ How many antivirus engines does your solution use? ‣ How often does your solution scan content?
Email encryption	Renders email illegible to prevent eavesdroppers and other unintended recipients from obtaining sensitive and confidential information.	‣ What does a user have to do to encrypt and decrypt email? ‣ How is encryption managed?
User portal	Gives employees control over their email, including spam quarantine and message activity.	‣ Can end users handle their own email quarantine?

Webserver protection

Every weakness in your web application is exposed when you connect a server to the Internet. Every mis-configuration and insecure programming technique is open to exploits. Securing each and every configuration and line of code is probably out of the question.

You need protection from common webserver and web application threats like SQL injection and cross-site scripting. Webserver protection should stop hackers from using attacks like these to steal sensitive information like credit card data and personal health information. And it should help you achieve regulatory compliance when a web application firewall is required. A web application firewall scans activity and identifies attempts to exploit web applications to prevent network probes and attacks.

A web application firewall and reverse proxy serve as the foundation of any webserver protection and support the following capabilities:

- Form hardening
- Antivirus scanning
- URL hardening
- Cookie protection

Capability to look for	Description	Questions to ask your vendor
Form hardening	Inspects and validates the information submitted by visitors via forms on your websites. Prevents invalid data from damaging or exploiting your server as it is processed.	‣ Is a complete form analysis performed? ‣ Can the system detect tampered forms?
Antivirus scanning	Scans and blocks malicious content at the gateway to stop viruses and other malware from infecting computers.	‣ How many antivirus engines does your solution use? ‣ How often does your solution scan content?
URL hardening	Prevents your website visitors from accessing content they aren't allowed to see.	‣ Do I have to enter the structure of my website manually, or can it be done automatically with dynamic updates?
Cookie protection	Protects from tampering the cookies given to your website visitors.	‣ Does the system protect my ecommerce site against manipulation of product prices?

Wireless protection

Wireless networks require the same security policies and protection as the main corporate network. Unfortunately, they are often operated by network administrators as two separate networks. As a result, enforcing consistent security policies across the organization is a challenge. Wireless protection from your UTM vendor should reduce if not eliminate that challenge.

You need wireless protection that extends UTM security features to your wireless networks. It should also provide a way for you to centrally manage the wireless network. So you can protect your network and data equally, regardless of whether your employees are plugged in or accessing the network over the air.

Wireless protection should include the following capabilities:

- Plug-and-play deployment
- Central management
- Integrated security
- WPA/WPA 2 encryption options
- Guest Internet access
- Detailed reporting

Capability to look for	Description	Questions to ask your vendor
Plug-and-play deployment	Provides fast and simple set-up because access points are configuration-less.	• How long does it take to set up and deploy access points and policies?
Central management	Simplifies management of the wireless network by centralizing configuration, logging and troubleshooting within a single console.	• Do I have to configure the access points one-by-one in the local GUI or command line?
Integrated security	Offers instant protection to all wireless clients through complete UTM security.	• Can all wireless traffic be forwarded directly to the security gateway?
WPA/WPA 2 encryption options	Enterprise-level encryption that prevents data loss and theft by rendering data illegible to unauthorized recipients.	• Are multiple encryption and authentication methods supported? • Is an interface to my RADIUS server available?
Guest Internet access	Protects multiple wireless zones, each with different authentication and privacy settings. Enables and supports wireless hot spots.	• How many different wireless network zones are supported? • What type of hot spots are supported? ☐ terms-of-use acceptance ☐ password of the day ☐ voucher-based
Detailed reporting	Provides information about connected wireless clients and network usage.	• Is there built-in reporting? • Is a separate tool required for reports?

Endpoint protection

Today's corporate networks lack a well-defined, stable perimeter. With laptops and mobile devices coming and going, the network expands and changes with each device that connects. And each device introduces new vulnerabilities to threats as well as the risk of data loss.

To maintain a secure network, you need endpoint protection that checks connecting devices for current updates and security policies. The endpoint protection should also protect company-owned devices both on and off the network. When endpoint capability is integrated into the UTM appliance, you can further reduce your management effort and save money. It can also help you achieve regulatory compliance when different antivirus engines run at the gateway and on the endpoint.

Endpoint protection should include the following capabilities:

- Ease of deployment
- Antivirus scanning
- Device control
- Real-time reporting

Capability to look for	Description	Questions to ask your vendor
Ease of deployment	Gives the organization the ability to easily deploy and manage endpoint clients to prevent malware and data loss.	• How is the endpoint client deployed?
Antivirus scanning	Scans the endpoint for viruses and other malware to prevent it from entering the network.	• How many different antivirus engines are used? • Does the solution provide live updates via the cloud?
Device control	Allows the organization to prevent the use of modems, Bluetooth, USB ports, CD/DVD drives, etc.	• What devices can be controlled through your solution? • Does endpoint protection only work if endpoints are in the domain or connected through a VPN tunnel?
Real-time reporting	Provides visibility into endpoints with up-to-date statistics.	• Is real-time reporting built in?

Conclusion

A UTM solution should provide complete security in one appliance. And it should allow you to extend protection from the network to the endpoint. The right UTM product simplifies security everywhere, and lets you consolidate your budget too.

By focusing on the checklists in this buyers guide and working closely with your vendor, you can find a UTM product that provides the protection you need now and in the future. So you get network threat protection with less effort, less complexity, and for less money.

United Kingdom and Worldwide Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

2904.bg.04.12

SOPHOS