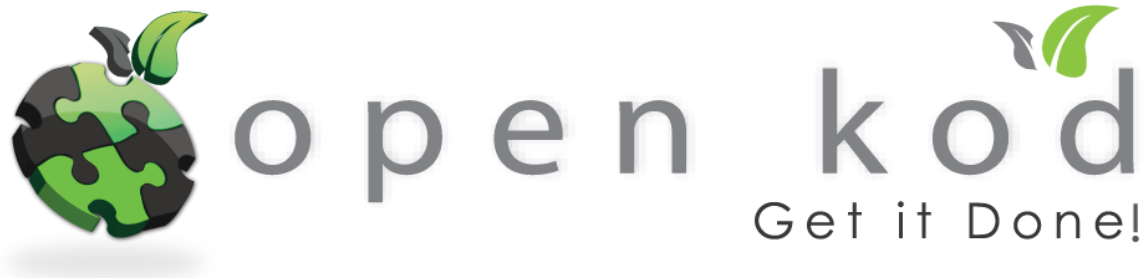
UNIFIED THREAT MANAGEMENT – SECURITY SIMPLIFIED



UTM offers an all-in-one solution that can plug security holes, reduce costs and shrink management requirements.

EXECUTIVE SUMMARY

Securing networks against any and all threats has become a major challenge for IT departments. And the task is increasing, exponentially as network administrators are forced to integrate additional components to stop a seemingly ever-growing list of security issues.

To offset the growing threat and reduce management complexity, IT managers are turning to unified threat management (UTM) solutions. Often used to replace time-intensive point security, UTM products have been growing in popularity the past few years. Traditionally used by small- and medium-sized organizations, these work-saving devices are now deployed by larger enterprises.

UTM delivers wide-ranging network protection from blended, external and insider threats. UTM solutions are flexible. The IT staff can deploy different scenarios and configurations that will work depending on the network design. In addition, they cost considerably less than a combination of stand-alone security tools, offer a single management console and take up less real estate in the wiring closet or data center rack.

Table of Contents

Security Landscape

The sophisticated threats organizations face from external, internal and blended attacks have created a shifting security landscape for network administrators.

How is the landscape changing? Report says that the new face of cybercrime and the ramifications of impending government legislation will significantly affect how CIOs position their security programs.

The reality for IT managers is that new threats emerge daily. Viruses and spyware present ongoing challenges for administrators, who have to maintain current security updates to protect their networks and systems.

Today's threat spread within hours and are more dynamic and malicious. In addition, they tend to be more organized and, in some cases, even designed for specific targets. Therefore, IT managers must consider security solutions that continually protect the organization without the need for manual intervention.

The research firm Gartner reports that more internet attacks target web applications than all other services combined. SQL injection and cross-site scripting (XSS), cross-site request forgery (CSRF) and botnet attack technologies give hackers a powerful arsenal to unleash. And hacker-controlled computers, or bots, carry out and increasing number of web attacks.

Insiders, who have easy access to valuable intellectual property, also pose a serious threat. These breaches may be malicious, but most of the time they are accidental. Often the employee doesn't even know they have compromised their employer.

The Bring Your Own Device trend or BYOD, combined with the increased use of social networks, also opens the door to more attacks. An organization's data now resides on devices that can be easily miss-configured by nontechnical employees, making it easier for cybercriminals to infiltrate the network.

In addition, Trojans and malware lurk in applications from social networking sites and may be unintentionally downloaded by many employees. Cybercriminals are also using social websites to target specific organizations, and even individuals, using readily available toolkits.

Blended threats make life for an IT chief even more unsettling. This type of threat is a multipronged attack that combines viruses, worms, Trojan horses and malicious code with server and Internet vulnerabilities. It is designed to propagate rapidly, like worms; but rather than depending on a single attack vector such as e-mail, it uses any propagation path available.

A good example is an executable file that arrives in an employee's e-mail and is opened. Other examples of blended threats include some of the most recent worms. Research from the market intelligence firm IDC shows that the larger the organization, the more likely it is to fall prey to network

threats. But whether an organization is large or small doesn't matter. All are vulnerable and need to take these threats seriously.

Stand-Alone Devices

The traditional enterprise network security model often uses stand-alone devices, or point solutions, for maintaining a secure network environment. Stand-alone network security products have generally been deployed as software, preinstalled on a PC, a router or an appliance.

These types of solutions typically offer specific network security functions, such as firewall and virtual private network (VPN) capabilities. The firewall/VPN duo is a good example of commonly found dual-function appliances. This type of appliance was ubiquitous in the early days of enterprise security – roughly 10 years ago.

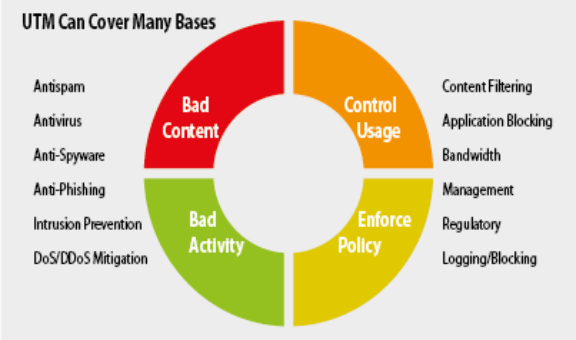
As might be expected, there are significant cost and complexity issues associated with managing and maintaining numerous point solutions. Of course, there are instances where organizations have already invested in multiple point solutions, but new, advanced security heft is needed.

Over the years, high-performance processors and optimized code have made it possible for stand-alone security appliances to be consolidated back into firewalls. This eliminates the need for organizations to buy multiple appliances and manage those devices individually.

Today, point security products are evolving into security appliances that are centrally managed and offer full protection at the edge of the network. The goal here is to create products that fall under the banner of unified threat management, which offers all-inclusive security.

UTM solutions are usually more cost effective. They deliver a single management console that increases simplicity and decreases compatibility issues.

With the plethora of added threats and new technologies such as virtual servers, storage and desktops, many organizations are rethinking their security infrastructure design. This is where new, ultra-fast UTM solutions can meet the needs of IT departments.



Unified Threat Management

Small organizations were once the primary users of UTM solutions, favoring the technology because it was less costly, more easily configured and provided enough protection. Today, whether deployed as onsite or virtual appliances, or simply as software, UTM is becoming popular with organizations of all sized.

Also known as integrated service appliances, UTM solutions have evolved from early firewall/VPN appliances into all-inclusive products capable of delivering security across an organization. This includes branch locations, remote telecommuting offices and mobile employees.

History has demonstrated that specialized hardware platforms are valuable because they can streamline network performance. UTM appliance designs are no exception, increasing performance while keeping the entry price reasonable.

Prices on UTM appliances range from a few thousand ringgit to even hundred thousand – depending upon an organization's needs. Interestingly, UTM providers have developed their products either by licensing or acquiring the missing technologies from third parties, or developing the missing capabilities in-house.

The upside for UTM providers, when working with a third party, is faster time to market. However, that can be a mixed blessing based on the quality of the added capability.

Many UTM products have evolved from companies that had one or two strong offerings and then added missing functionalities. According to *SD Times,* a software development news publication, a UTM solution's core competencies may be best of breed in some areas, but not in all areas.

UTM Plusses

Reduced complexity: Unified threat management solutions have a single, simplified management console.

Ease of deployment: Many UTM appliances can be brought up on the network and configured by nontechnical staff.

Integration capabilities: Typically, UTM solutions integrate with standard network configuration methodologies and technology standards.

Troubleshooting ease: A simplified management console reports data and events and may automatically guide administrators through a troubleshooting phase.

Easier Management: The unified management console lets administrators remotely manage their security environment.

Added Simplicity: Multiple devices from the same provider simplify troubleshooting, licensing and technical-support situations.

Better performance: The latest appliances use high-performance processors that are engineered to protect performance.

Reduced training requirements: One security solution required a single platform. And that can reduce the learning curve for IT staff.

Regulatory compliance: The console gives administrators more granular (and simultaneously, more simplified) individual and group policy management controls.

For instance, a product might have a great firewall, but its antivirus isn't the best. Or it may be good at content filtering, but not so good at sniffing out misformed packets. For IT managers making purchases, it's imperative to look into the background of the UTM provider, making certain that the solution's actual best of breed competencies align with organizational needs.

A sound strategy is to create a checklist of functions needed and another list of platforms that can deliver those functions. It's not so important whether provider A calls their device a firewall, provider B refers to their solution as a UTM appliance or provider C calls it a next-gen firewall or even a data loss prevention system.

Look at all the providers that deliver the necessary functions needed. Regardless of how they classify their product, decision making should be based on how easily the solution will integrate into the organization.

Reduced Costs and More

The first UTM appliances entered the market around 2004. First-generation UTM devices were little more than basic firewalls with some added security firmware, which under high-traffic situations would overtax the firewall's processor.

Poor performance and a lack of reliability turned early UTM appliances into a little more than a novelty in the network security realm. This resulted in most administrators instead choosing dedicated appliances that focused on individual security services.

Fast forward to 2012 and much has changed. High-speed processors and enhanced code have made UTM solutions a viable approach which organizations have adopted to improve visibility, lower network complexity and create an environment where security falls under one technology umbrella.

Reduced cost is one of the main advantages of investing in a UTM security solution. UTM devices usually cost 25 percent less than equivalent, individual point solutions.

Another major consideration is that one UTM appliance can replace five or six separate point solutions or servers. This saves precious real estate in the enterprise data center and cuts energy consumption, reducing the electric bill and bolstering an organization's green programs.

UTM solutions have been the technology of choice of small- and medium-sized businesses (SMBs) as well as educational and government organizations. That's because they're user-friendly in an environment in which IT funds and staff are precious commodities.

The appliances are easy to install on the network and easy to manage, compared with managing five or six different security applications with multiple consoles.

With a single device, there's a reduced need for enhanced technical support packages, and there are fewer upgrades, patches and

contracts to manage. This pays off financially and increases IT staff productivity. Troubleshooting a single device is much simpler than trying to trace, diagnose and resolve an issue across multiple devices.

It's also easier to set more effective and flexible group policies from a centralized management dashboard because there's a sharing of intelligence and events between the security apps. Reporting, event analysis and correlation, and activity logs are compiled for all security functions and standardized, making it easier for the IT staff to analyze. The result is higher visibility, leading to more rapid identification of network threats.

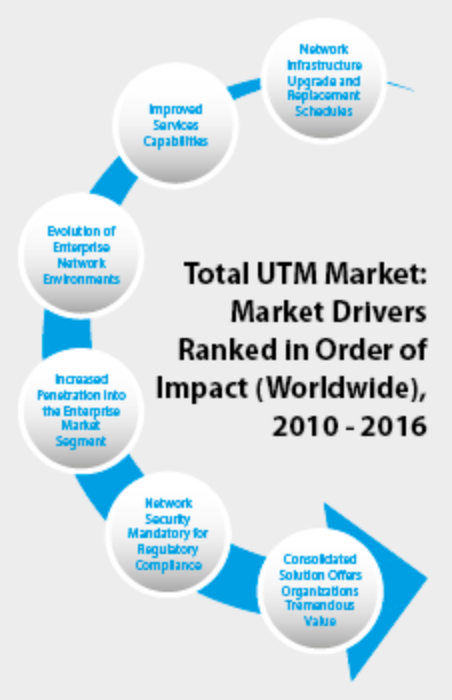
In addition, UTM appliances don't have repetitious processes, which saves time and increases performance. Common tasks such as packet scanning are done once and used for all applicable security modules rather than multiple times by each separate security application. For instance, packets are not scanned once for spam and then again by a gateway antivirus module.

The UTM appliance market has matured, and performance has increased to the point that the devices now deliver much more sophisticated functionality. Some UTM solutions can employ functionality that identifies the user along with relevant network data.

With identify and network data combined, organizations can identify specific user behavior patterns that may signify misuse, unauthorized intrusions or malicious attack launched either internally or externally. IT managers can place alerts based on predefined norms of behavior by individuals, groups or departments.

A significant insider behavior deviation can trigger a security alert. It's important to bear in mind that whether it's social plans, all misuse has financial consequences, ranging from lost employee productivity to system downtime.

Another major benefit offered by UTM solutions is scalability. Organizations can purchase only the security modules they need, adding more modules later as users are added and necessity dictates. IT managers can deploy multiple UTM appliances across an organization with branch offices as well as telecommuting and mobile employees, managing them all remotely from a centralized console.



Enterprise Benefits

UTM solutions play a major role today in enterprise security, both for midsize and large organizations. Midsize organizations can make use of UTM devices as primary security for their network and large organizations can use them to guard the borders.

A large organization may benefit from an investment in a UTM security solution in a number of ways. For example, it might deploy UTM for border security needs while using point solutions in other areas. Or IT management may choose a UTM solution that's best of breed in the area in which the organization needs coverage, for example, insider threats.

In another example, multiple devices can be deployed across an enterprise and at satellite sites, and still be centrally managed from a single console. Policies and features can be replicated across sites using simple techniques, while granular access controls can limit who can do what.

IT chiefs may also choose a distributed approach. For example, the enterprise may deploy a UTM device on the perimeter of an enterprise data center, then deploy multiple UTM devices at other organization locations and flexibly configure them to prioritize and handle specific security tasks.

Each UTM device would give priority to a specific security task, such as intrusion prevention or antivirus scanning, across the network. Management would still be handled from a centralized location and unified console.

By taking a common-sense approach to network security, an organization doesn't have to rely on a single device (or fear a single point of failure) when protecting its network. A workaround for this concern is to deploy a load balancer and additional UTM appliances as needed.

UTM Flavors

There are different flavors of UTM to choose from. Physical UTM appliances make up the largest share of the market. There are also UTM software solutions that IT departments install on servers or PCs. Virtual UTM appliances are also available for consideration. Each has its own pluses and minuses.

Physical UTM appliances: Organizations choosing this type of UTM receive validated hardware with specified UTM software preinstalled that can easily be brought up on the network. These appliances come with specialized ASIC chipsets that are built to handle the processing required to scan for multiple threats simultaneously. In addition to the appliance, physical UTM solutions feature a robust network security operating system that integrates with the UTM appliance's individual components.

Once the UTM appliance is configured for the network, administrators can immediately begin setting up functions; adding users and groups, and establishing security policies, such as group and

individual permissions and rules, event logging, reporting schedules and report delivery methods.

Individual components are license-based; for example, an organization may purchase a UTM solution with a basic firewall, antivirus and antispam engine, or purchase the entire suite of network security components. Individual licenses typically require upgrading, usually on an annual basis. Upgrades tend to be straightforward, given that the software licenses are all from the same provider.

Integration of all security functions is enhanced because the solutions have a centralized, common management console. Additionally, this unified approach to security makes for easier troubleshooting if needed.

Physical UTM appliances as an all-in-one security strategy are not without potential downsides. Many organizations have existing investments in point solutions that will not be maximized if the decision is made to purchase UTM appliances, leading to higher overall hardware expenditures.

From a technical standpoint, adopting a UTM appliance may put an organization in the position of having a single point of failure unless a backup strategy is put in place to ward off the service interruption.

UTM systems can experience degraded performance, as there are limitations in all hardware processing abilities when so many applications and users are simultaneously in play. As a result, some organizations may disable or degrade a specific function (such as content filtering) that is particularly slow, to keep the system operational if IT starts getting complaints.

Stateful Versus Stateless Packet Inspection

A stateful firewall performs stateful packet inspection (SPI). It keeps track of the state of network connections, such as Transmission Control Protocol (TCP) streams or User Datagram Protocol (UDP) one-way communication traffic traveling across the network. In SPI, only packets that match a known active connection are allowed through the firewall.

All others are rejected. In other words, the firewall distinguishes legitimate packets for different types of connections. Most firewalls today are connect-aware and give administrators better visibility and control over network traffic. A stateless firewall treats each network packet individually. The advantage of this kind of packet filter is that it functions more efficiently at the network layer because it looks only at the packet header.

The downside is that it is stateless, which means it has no memory of previous packets, and thus cannot detect whether packets are legitimate traffic, which makes them vulnerable to spoofing. This type of technology does not permit the firewall to know if the packet is part of an active connection.

This places limitations on the solution's ability to scale and may happen if the UTM appliance is not correctly sized according to

its maximum usage requirements. It's a serious problem that can lead to the UTM appliance, and therefore the network, being compromised.

Additionally, there are different methods of packet inspection and protection. The two main techniques are deep packet inspection (or stateful inspection) and static packet inspection (or stateless inspection), that may rely on disparate UTM flavors, leading to the possibility of poor integration.

To play it safe, purchase all the security appliance modules from the same provider. It's similar to a marriage: Good ones are great and last a long time. Poor ones take a toll in both cost and productivity.

Virtual UTM appliances: Driven by cloud computing and data center buildouts. Infonetics Research forecasts that from 2010 to 2015, the virtual security appliance market wills more than quadruple, to $1.75 billion.

This represents significant confidence by IT decision-makers. IT departments are taking a pragmatic, albeit positive, approach and slowly accepting software for use in virtual appliances; in other words, appliances deployed remotely in the cloud.

Virtual appliances are designed to sit on a virtualized server, such as a VMware, Microsoft or Citrix server. They provide security for multiple virtual machines on a single server. Once the server is virtualized, it only sees the bulk inbound and outbound traffic. It can't do anything about what's going on in between individual servers. Traffic can pass freely between them without being inspected at all.

Virtualized appliances are typically a requirement if an organization has a virtualized server environment such as a data center; if it is using a cloud service provider. Without a virtualized appliance, the traditional firewall is blind to everything that's going on within that server.

The decision to move to the cloud has all the standard advantages that cloud technology brings: reduced hardware costs, easier upgrades, scalability and better business continuity. The IT department will appreciate that there are more options than there were a few years ago.

Despite the growth of the market, virtual UTM (or multifunction security appliances) face some interesting challenges. Adopting cloud technologies to deliver IT services creates significant change in the technical requirements for security solutions. Network design becomes intricate.

Device compatibility, complex management and technical support, as well as the cost of making untested infrastructure decisions, are a few of the possible downsides. Other challenges exist, including resolving the threat between inter-virtual machines and avoiding the costly mistake of installing security software on every virtual machine while deploying security technology that protects the applications running in virtualized environments.

Virtual Security Trends

Virtualization is changing the face of network security requirements. There are several issues IT managers need to consider when planning their migration to a virtual infrastructure.

* **Inter-VM threats:** These have become a significant new issue. Security devices sitting on the network's edge simply can't see potential threats when traffic is travelling between virtual machines on a single physical server.

* **Rising costs:** In the past, preventing inter-VM threats meant installing individual security technologies (with licenses) per virtual machine. While this does work to prevent threats from crossing VMs, it can be costly and challenging to manage.

* **Evolving architectures:** As virtualization providers continue to develop and improve security application programming interfaces that allow security products outside the virtual (or physical) server to have visibility into traffic, security architectures will continue to change.

* **Selecting a sufficiently broad product:** In small environments, where virtualized servers run a broad range of applications, there is a need for virtual appliances with a broad range of security functionality.

* **The impact of the cloud:** In cloud environments, virtual security solutions may need to deal with a narrower set of applications and protocols (mostly web-based). Still, they will need to scale and provide multitenancy features that allow providers to deliver services to many customers from one solution.

* **Improvements in switching technology:** With new data center-focused switches that have virtualization-aware switching built in – including the ability to hairpin traffic back to the same server it just came from – it will be easier for security technology outside the physical and virtual servers to enforce policies and keep traffic safe.

Finally, it can be challenging to weed through the lengthy lineup of providers, architectures, standards and APIs available for locking down the organization's virtual environment.

UTM Software: Another option available to IT professionals is to purchase UTM software separately and install it on existing hardware, thereby cutting the cost of hardware out of the equation. Licensing for this type of UTM solution is very similar to the licensing of applications preinstalled on a dedicated appliance.

The difference is that in addition to paying licensing fees for the UTM applications, such as antivirus or intrusion detection, the organization also must pay for the operating system installed on its own server or PC> this still represents a lower cost of ownership over appliance-based solutions. These systems have a specific minimum configuration based on the number of users and the applications that are run simultaneously.

Increased scalability is a big advantage that UTM software offers over an appliance-based solution. As an organization grows, it can add hardware, more memory, more processors and software licenses to scale. If

the organization purchases an appliance solution, when it becomes overloaded there won't be much it can do with the appliance.

A software solution enjoys the same integration and simplified management benefits that other UTM flavors do over point solutions. Software also offers another main benefit of UTM: reduced staff training costs.

An organization will spend significantly less bringing its IT staff up to speed with a single integrated product than it will with five or six separate point solutions. It avoids the problem of having one person who knows antivirus, another who knows intrusion detection systems and another who knows firewalls.

UTM software has challenges, many of which are shared with the other UTM options. Whereas an appliance is more locked down, more of a closed box, and operating systems have fewer flaws, UTM software is another layer of vulnerability. Another downside is that updating patches and licenses is time-consuming because IT staff needs to monitor and renew both the software and operating system licenses.

UTM Caveats

There are some things to be aware of when choosing a UTM solution. When configured as a border solution, UTM can see only incoming traffic. The burning question for the IT department is whether or not the threats are internal or external. Recent statistics would suggest that more than 50 percent of threats are perpetrated by insiders.

Under these circumstances, UTM could give an organization a false sense of security. It's not enough to check off the network security box on the IT checklist just because the organization has deployed UTM, in any of its flavors, at its border.

The unified management console is often a double-edged sword. With some solutions, it's a single-user interface, which, at first glance, makes it look easy to configure. In fact, once into the individual functionality of the user interfaces, it can get complicated. The result is that the IT administrator ends up leaving the UTM with default settings which might not prove best for the security needs of the organization.

On the other hand, the organization may have staff that can configure each console area with expertise. For instance, someone from the software side may be talented with antivirus software, some else from networking could be an expert in firewalls, or someone might have knowledge regarding IP content filtering. In all fairness, this scenario could also apply to point solution configurations.

The Right Choice

When it comes to UTM solutions, there is no one-size-fits-all approach. Administrators will have to weigh price against performance against scalability to choose which flavor of UTM solution best fits the needs of the organization.

However, the future of network security does lie with UTM solutions. And picking a UTM product is not a matter of “if”, but a matter of “when”. The days of single-function appliances and stand-alone security products are quickly waning and administrators need to start planning now for the future of effective network security.

Next Generation Firewall or UTM

UTM architecture is evolving to meet market expectations for next-generation firewalls (NGFWs). These products are application-aware firewalls that solve the performance issues that UTM solutions may be affected by when all functions are fully enabled.

NGFWs enforce policies on the application layer and can detect prevalent threats like SQL injection or cross-site scripting. They differ from conventional firewalls that typically work on the network layer and use protocols to enforce access policies.

In addition, NGFWs deliver intrusion prevention system/intrusion detection system (IPD/IDS), virtual private network (VPN) and web application firewall technologies. Their core functionality is protecting the network from external and internal threats.

The security market is in tune with the market shift. As a result, most major security hardware providers and some software makers have developed next-generation firewalls. However IT chiefs should be cautious because some security providers have added features to their UTM appliances and are defining them as “next-generation” simply to remain competitive.

Open Kod: Your Security Partner

Unified threat management refers to a comprehensive security product offering a simplified, all-encompassing way to prevent malicious attacks from entering your network and corrupting systems and data.

Open Kod offers a wide selection of security solutions that protect the five key network areas most susceptible to threats. These include: gateway and network, server security, end point security, data loss prevention and application security.

Our account manager and solution architects are ready to assist with every phase of choosing and leveraging the right threat prevention solution for your IT environment. Our approach includes:

- An initial discovery session to understand your goals, requirement and budget.
- An assessment review of your existing environment and definition of project requirements.
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept.
- Procurement, configuration and deployment of the final solution.
- 24x7 telephone support as well as ongoing product lifecycle support

Security Assessments

Open Kod security assessments are custom-tailored to reflect individual business needs. Each security report highlights individual concerns and goals. Open Kod security assessments include analysis of any or all of the following:

- Internet Security
- Internal Network Security
- Partner / Extranet Security
- Comprehensive Assessment
- Dial-Access Security
- Wireless Network Security
- Data Loss Assessment

To learn more about Open Kod's security solutions, contact our office, call 03-8948 6696 or visit openkod.com

DURIO

Durio offers high performance Unified Threat Management with content inspection at top speed. Featuring the latest Intel® Multi-Core Technology and advanced networking functionality, the UTM deliver a comprehensive security solution from small-to-large network environments.

Integrated security services such as stateful inspection firewall, VPN, gateway antivirus, antispam, Web and e-mail content filtering offer granular protection in a single appliance, reducing management time and costs.

We design Durio to meet the needs of small-to-large businesses requiring a highly available and powerful appliance for demanding networks.