

Defining the “U” in UTM: Unified, Ubiquitous or Useless?

Ted Ritter, Research Analyst

Executive Summary

The challenge today is that IT is accelerating, putting the CSO between a rock and a hard place. On the one hand he or she must uphold corporate policies and manage security and compliance. On the other hand, the CSO cannot be seen as business prevention; security cannot be the big red stop button on the IT assembly line. Simultaneous with IT acceleration, an evolution is occurring in the security realm, defined by unified threat management (UTM). Sitting at the confluence of security and networking, UTM is evolving from a simple consolidation value proposition to a ubiquitous solution that holds the potential to provide the CSO with the tools to meet the corporate risk tolerance while fully supporting the agility goals of the business.

The Issue: Threat Management Must Evolve

From Nemertes’ conversations with IT executives, we know that security can be both business enablement and business prevention. For example, two-thirds of organizations that participated in Nemertes’ *Security and Information Protection (Sec-IP)* benchmark have avoided a new technology because of security concerns. Our research also indicates that CSOs are mostly successful in implementing security: nearly 95% of participants in *Security and Information Protection (Sec-IP)* consider their security efforts successful. (Please see Figure 1: Rating of Security Success, Page 2). Yet at the same time, nearly 35% of participants have had a security breach in the past year. This tells us that security, and threat management in particular, still leaves much room for improvement.

Overall Success in Security

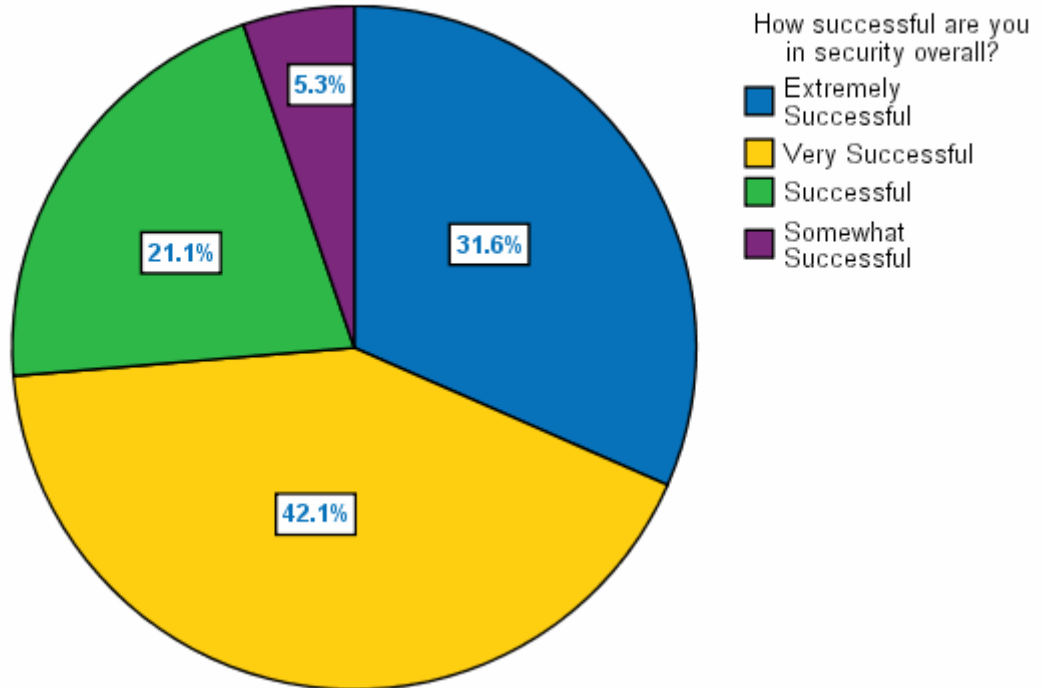


Figure 1: Rating of Security Success

UTM as Consolidator

“UTM” means different things to different people. The initial intent of UTM is the consolidation of multiple security-related technologies into one system. Initially, UTM solutions were integrated Firewalls with Intrusion Detection/Intrusion Prevention Systems (IDS/IPS). Now, most UTM solutions also include Anti-X (SPAM and malware) and VPN functionality. UTM continues to evolve with expanding functionality. Potential UTM technologies include: Identity management, data leak prevention (DLP), VOIP security gateways, unified communications and collaboration (UCC) security gateway, and network access control (NAC). Some UTM solutions are even expanding beyond security unification to include routing and switching functionality.

Interest in UTM as a consolidation solution is high, especially for branch operations. In Nemertes Research’s *Building The Successful Virtual Workplace* benchmark, 48% of participants say that they are implementing, or plan to implement, integrated (all-in-one) solutions at the branch. (Please see Figure 2: Plans for Integrated Platform at Branch, Page 3). The focus of the discussion with participants is integration of communication functions: router, switch, Wi-Fi. Yet it’s clear that integration of security technology is also considered an integrated device goal. This makes sense since branch offices are particularly well-suited for a consolidated platform where space, cooling and expertise are at a premium.

Are you using all-in-one devices at the branch?

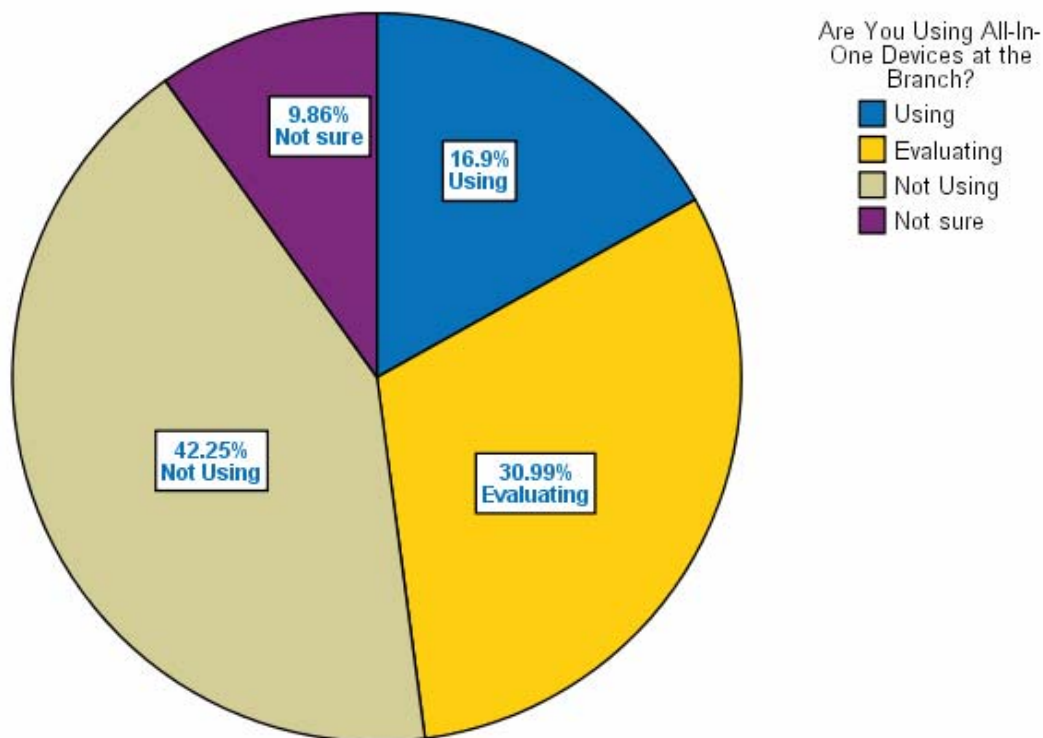


Figure 2: Plans for Integrated Platform at Branch

UTM as a consolidator is a simple premise that holds great promise: reduced CapEx (fewer boxes) and reduced OpEx (streamlined operations, and reduced physical and environmental footprints). The reality of UTM as consolidator is that consolidation is a good thing, but consolidation without performance is unacceptable. In fact, performance has been the Achilles heel of many UTM solutions. Performance is characterized by three metrics: throughput, latency and operational efficiency:

- **Throughput** – The amount of information that can transit the UTM device. Typically, this is measured in gigabits per second (Gbit/s), megabits per second (Mbit/s) and, unfortunately, in some instances, kilobits per second (Kbit/s). The more processing required, the greater the potential effect on performance.
- **Latency** - Like throughput, latency also ties to the intensity of operations: the more processing, the greater and more variable the potential latency. Though most applications are tolerant of moderate and variable latency, real-time applications such as voice and video are extremely intolerant. As more networking functions meld with UTM, the importance of managing latency increases dramatically.

- **Operational efficiency** – The more integrated the management of the security functions, the higher the operational efficiency. For example, integrating all functions under one common user interface (UI) lowers training costs and integrating policy management so that policies are defined once, which reduces planning, implementation, trouble-shooting and auditing OpEx.

To put UTM as consolidator in perspective, some compare UTM to a Swiss Army knife. The advantages of the knife are reduced CapEx (cheaper than buying all the equivalent tools), reduced OpEx (all tools operate on the same platform) and reduced footprint (compact and takes much less energy to transport than a tool box). Anyone who has tried to use a Swiss Army knife to drive screws, cut wood or clean a fish finds that it works, but it doesn't compare with using a screwdriver, a saw or a hunting knife. That's OK, since the real value proposition of the Swiss Army knife is the portability: accepting sub-optimal tools *everywhere all the time*, versus having the best tools *somewhere, some of the time*. Unfortunately, this isn't OK for security. Saving footprint cannot justify compromising performance or security: security requires the optimal tools *everywhere all the time!* For this reason, despite high interest, the success of UTM as consolidator has been mixed. Of the three main goals of UTM – reduction of CapEx, OpEx and footprint – the only ones that have been achieved consistently are reduced CapEx and physical footprint: consolidation of multiple boxes to one reduces cost and rack space.

UTM Evolution

The good news is that UTM is on an evolutionary path of integration and performance that may be defined by three phases: Consolidation, Integration and Unification. (Please see Table 1: Evolution of UTM, Page 4).

Phase	Value Proposition	Issues
I – Consolidation	Consolidation with the ROI centered on reduction of CapEx and footprint	Poor UI integration and significant performance problems
II – Integration	Integration of technology and UI with ROI centered on reduction of CapEx, footprint and OpEx	Better UI integration though performance problems still exist
III – Unification	Phase II with expanded functionality to offer improved ROI while maintaining performance across the enterprise threat exposure	Strong UI integration and performance issues addressed. Still needs higher level management/policy integration

Table 1: Evolution of UTM

Phase I UTM is discussed above. Phase II UTM is defined by integration: the seamless integration both of the applications on the UTM devices and of the management console. Early phase II UTM implementations were nothing more than management mash-ups in which multiple management consoles were presented on one interface. However, most phase II UTM solutions have evolved to now provide an integrated management solution with a consistent UI across security technologies. One challenge that still remains is the level of this integration. One example is policy management: Is it possible to create one policy that supports FW, IPS and NAC? It is this higher level of management integration that will be needed before UTM solutions will fully support the dynamics of today's IT and business environments.

In addition to limitations in management integration, many of the phase II UTM solutions also have significant performance issues. It is not uncommon to have a UTM firewall operating at 1 gbit/s throughput with performance dropping by 50% when the IPS is turned on, and dropping further when additional functionality is engaged. Integrated management and integrated applications are of little value when performance is so severely affected.

Phase III UTM solutions are addressing these performance issues, primarily through custom-built hardware and silicon. Beyond performance, what differentiates phase III UTM from phase II UTM is the scope of the solution. A phase III UTM solution is the integration of security technologies – with performance - across the entire enterprise threat exposure, including end-point protection, network protection, server protection, application protection and content protection. Further, phase III UTM is defined by the integration of these technologies under one unified management umbrella.

Phase III UTM is the first real example of a unified threat management solution.

Avoiding an IT "U" Turn

This is where things get interesting. UTM evolution has been taking place over the past three to four years. During the same timeframe, there have been tectonic shifts occurring in the IT infrastructure focused on increased business agility that are putting significant pressure on security and networking.

One tectonic shift is the continuing opening of the enterprise, with the gradual federation and interpenetration of IT systems between an enterprise and its partners, customers, and suppliers. Parallel to this shift is the movement to unified communications and collaboration (UCC). Organizations see UCC as a means to increase worker productivity, partner collaboration and a reduced environmental footprint. Both increase demand on the network through increased porosity and thus, the need for even tighter integration of security with the network.

Another tectonic shift is the rise of service-oriented architectures (SOAs). As enterprise applications gain services interfaces, each service creates a new set of access points; perhaps tens or hundreds of times as many as there were before.

Things that used to happen within an application, on a single server, become network traffic among servers, data centers and partners.

Finally, a third tectonic shift involves virtualization. Servers can be provisioned and deprovisioned on the fly, “frozen” and “thawed,” moved from place to place. Problems created by rapid (re)provisioning of physical servers are exacerbated and amplified by virtualization. Combine virtualization with SOA and the security environment becomes, potentially, even more wildly variable.

The pressure from these shifts is felt at all layers of the ISO stack. Although attacks at layers two through four of the ISO stack are still active and dangerous, many attacks and attackers are moving up the stack to layers five through seven. Reasons for targeting the upper layers of the ISO stack include:

- SOA drives applications to swap internal, binary communications for externalized XML interchanges. This XML traffic is a primary target for malware and direct attack.
- The move to unified communications puts SIP into the center of converged and integrated voice and data systems. SIP is a protocol that is quite exposed to attack, unlike the well-protected signaling channels for TDM voice.
- The move to virtualization removes much of what was previously protected on the network into the internal world of hypervisors and virtual machines. Targeting a guest OS in a VM world via malware is a primary attack vector for exploit.

Putting this all together, attacks are climbing the network stack to evade enterprise defenses at the lower levels. At the same time, as application infrastructure shifts to a more dynamic, services-based, diffuse and virtualized environment, the upper levels of the ISO stack are becoming more vulnerable to exploit. To combat these evolving threats, organizations need tighter coupling of security and networking and tighter security; from the physical to the application layers. To do this, security must be more than just an overlay, as it traditionally has been. But, at the same time, to implement one security solution for virtualization, one for SOA, one for the network doesn't work. This brings us full circle back to the discussion of UTM.

From Unified To Ubiquitous: Achieving the New "U"

Today some vendors are delivering phase III UTM solutions, though most UTM architectures are an overlay of security on top of the network, typically with some level of policy and management integration. An exciting aspect of UTM is the evolution of UTM and the tectonic changes in the IT environment are aligning so that UTM has the potential to extend way beyond its initial value proposition. The reason for this is because UTM sits at the confluence of security and networking and therefore is in the perfect position to become the platform to build an agile threat management infrastructure, based on the melding of security and networking. To accomplish this, UTM must evolve beyond phase III to a higher state, characterized by integration across multiple dimensions:

- Security/Networking Infrastructure – UTM must extend across the entire network including beyond the firewall to include partners, guests and teleworkers.
- ISO Stack Through Application Level – UTM must be application aware and support security at all layers of the ISO stack. Areas where UTM extends include DLP, identity management and XML/SOAP/SIP firewall support.
- Security/Network Operations – For UTM to be ubiquitous, it's crucial that security and network operations be fully integrated. Some aspects of security will always be segregated due to separation of duties requirements (SoD). Still, there must be tight coupling of policy, configuration, event and identity management.

Solutions that meet these criteria transcend unified to become ubiquitous. Ubiquitous UTM enables the CSO to implement a truly agile security solution, aligning enterprise agility to the corporate risk appetite.

6.0 Conclusion

UTM is one of the rare solutions where the current potential is far greater than the initial purpose. Rather than remaining an IT Swiss Army knife, UTM has evolved to become a fundamental security solution for the rapidly evolving enterprise of the 21st century. Because of this IT and security people need to realign their thinking from “Old UTM” to “New UTM.” (Please see Table 2: Old UTM vs. New UTM, Page 7).

Old UTM	New UTM
Consolidation	Integration
Trade Performance for Convenience	Uncompromising Performance
Consolidation of Security	Security and Networking Unity
Security Management Mash-ups	Seamless Management Integration
Business Hurdle	Business Enablement

Table 2: Old UTM vs. New UTM

The bottom-line for UTM is that the sum of the parts can be greater than the whole. A true UTM solution, implemented enterprise-wide, can be an agile, dynamic and adaptable platform that both achieves the initial goals of UTM (reduced CapEx, OpEx, space and environmental footprints) and actually transcends threat management to become secure business enablement.

About Nemertes Research: Founded in 2002, Nemertes Research specializes in analyzing the business value of emerging technologies for IT executives, vendors, and venture capitalists. Recent and upcoming research includes Web services, security, IP telephony, collaboration technologies, and bandwidth optimization. For more information about the analyst, please contact Nemertes at research@nemertes.com.