

Missing Link 
Security Services
Mark Bouchard, Founder

Critical Criteria for Enterprise-Class UTM

Capsule

UTM technology definitely deserves consideration for enterprise-class implementation scenarios, but only if associated solutions fully address key criteria and the deploying organization is operationally prepared for functional consolidation.

About the Author

Mark Bouchard, CISSP, is the founder of Missing Link Security Services LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security topics for over 10 years. He is passionate about helping enterprises address their information security challenges. During his career he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and overall architectures to the justification, selection, acquisition, implementation and operation of individual security and privacy solutions.



Context

Unified Threat Management (UTM) involves combining multiple security capabilities and packaging them with hardware, typically in the form of a multi-function security appliance. At a high level, the point of UTM is consolidation, or enabling organizations to deploy numerous countermeasures without the need to deploy, manage, and maintain a corresponding number of separate, physical “boxes” and corresponding management consoles. But that is really just the tip of the iceberg. Additional benefits typically associated with UTM include stronger security, improved operational efficiency, and lower total cost of ownership.

Not surprisingly, the result over the past few years is an adoption rate that has been nothing short of tremendous. This is particularly true among SMEs and for remote/branch office locations. The nagging question that still remains, though, is whether UTM is “ready for prime time.” Is it suitable for enterprise-class deployment scenarios, such as in front of high volume/complexity/criticality Internet DMZs and data centers? The obstacle in this regard has been the relatively reasonable concern that combining numerous security services on a single device has, at least historically, involved making compromises in terms of depth/strength of capabilities, manageability, and solution scalability and performance.

Considerations

The answer to the question posed above is an emphatic though qualified “Yes, UTM is ready for prime time.” Leading solutions have had several years to mature and, in general, to address the concerns and requirements associated with enterprise-class deployment scenarios. That said, it should also be clear that not all UTM products are created equal. There will inevitably be significant variation, especially in terms of the degree of integration and unification of both the core security services and how they are managed. Indeed, whether any specific UTM solution is appropriate for enterprise-class deployments will depend on the extent to which it addresses the following key criteria:

Security

There are three aspects to this criteria: all of the individual security technologies must be very good, if not actually best-in-class; “all” in this case means a set of *complementary* services that provide relatively comprehensive protection against prevailing threats, but NOT everything under the sun; and security should be enhanced, not compromised, by having integration between individual services and by having a design where a flaw in one service does not allow other services performing traffic inspection to be bypassed.

Performance

A purpose-built system architecture, specialized hardware, innovative and scalable inspection mechanisms, support for high availability, and other related techniques should be present to ensure both non-stop operation and that rated throughput *and* low latency is consistently attainable with real-world traffic and all services operating.

Management

Centralized control is essential for all life-cycle management functions (e.g., configuration, monitoring, troubleshooting, and reporting) and helps to ensure consistency of policy enforcement. More importantly, though, there should be (a) substantial integration in terms of both data/event sharing and policy/rule development, and (b) extensive role-based administration capabilities.

Flexibility/Compatibility

For starters, which security services get used in any given instance of the UTM device should be selectable, not fixed. In addition, the solution should be modular/upgradeable (to account for future requirements) and, in general, should be designed to seamlessly “fit in” (e.g., by supporting core networking capabilities, multiple deployment modes, and numerous options for features such as authentication, encryption, and network interfaces).



Integration

This criterion is somewhat redundant, since it has already been mentioned elsewhere; but it deserves repeating. Without pervasive integration and coordination (e.g., in terms of processing packets, consolidating event alerts, and management functionality), the benefits of UTM diminish, yielding little more than physical consolidation.

Conclusion

UTM products that stack up well against key criteria in the areas of security, performance, management, flexibility, and integration are definitely appropriate for enterprise-class deployments. However, it is also important to recognize that product readiness is only half of the equation. The other half is readiness of the organization itself. In other words, deploying UTM in high volume/complexity/criticality scenarios will be less appropriate/worthwhile for organizations that (a) have not sufficiently depreciated any recent/significant investments in their security infrastructure, or (b) that are culturally and operationally “siloeed” in terms of security system ownership and/or functional responsibilities.