

**Missing Link**   
**Security Services**  
Mark Bouchard, Founder

## Management Considerations for Enterprise-Class UTM

### Capsule

Having enterprise-class management capabilities is not only a crucial prerequisite to deploying UTM technology in high volume/complex/critical scenarios, but also the key to unlocking truly meaningful reductions in cost of ownership.

### 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

To date, the promised benefits of Unified Threat Management (UTM) technology – including consolidation and simplification of security infrastructure, stronger security, improved operational efficiency, and lower total cost of ownership – have done relatively little to generate uptake beyond SMBs and the branch-office locations of larger enterprises. However, this situation is poised to change. In general, UTM products have matured considerably over the past couple years and initial concerns pertaining to inadequate performance and security capabilities are steadily being addressed.

That said, there is still one further area to which prospective customers are encouraged to pay close attention. Specifically, the suitability of UTM technology for enterprise-class scenarios also depends on having a solution with enterprise-class management capabilities. Indeed, having a comprehensive set of management features that are flexible yet efficient is instrumental not only to establishing and maintaining effective defenses but also to achieving significantly greater cost savings.

## Considerations

The importance of a UTM solution's management capabilities to support both initial deployment and ongoing operations cannot be overstated. Overall, granular configuration control should be complemented with optional presets/defaults and other ease-of-use features to enable organizations to optimize their implementations in terms of both effectiveness and efficiency. Furthermore, it should be recognized that having an appliance-based solution – where all of the associated software has been pre-loaded and pre-hardened and the resulting “system” has been engineered to maximize performance – is merely a starting point. Additional characteristics and capabilities that organizations should insist on (and ideally evaluate) prior to embracing UTM for enterprise-class deployments include the following:

- Management that is centralized, consolidated, and simplified. This entails, respectively, the ability to manage multiple UTM devices at once, having a single management system that covers all of the incorporated countermeasures, and a high degree of intuitiveness and ease of use that is pervasive across the full set of lifecycle management functions (i.e., configuration, monitoring, troubleshooting, and reporting). The result, ideally, will be significantly enhanced operational efficiency and unified/consistent policy enforcement.
- Device set-up that is facilitated by configuration wizards and pre-defined, yet customizable templates (e.g., pertaining to different security levels).
- Policy development that is sufficiently granular to account for complex scenarios yet efficient in that it is hierarchical/tiered (e.g., with policy inheritance) and supports flexible grouping of resources, users, and rules.
- Active monitoring that facilitates rapid response/troubleshooting by providing alerts and in-depth views of device status, user activity, security events, etc.
- Extensive logging and highly flexible reporting (e.g., real-time/historical, ad-hoc/scheduled, templates/customizable, summary/drill-down) to support trending, troubleshooting, and all manner of auditing/compliance requirements.
- Granular, role-based administration for assignment of management rights (e.g., by function/service or devices).
- Automatic delivery, notification, and optional implementation of updates for system software, security applications, and associated content (e.g., signatures).
- High reliability and scalability, ideally in the form of having support for load-balanced, redundant pairs of management systems.



## Conclusion

---

The consolidation and simplification of security infrastructure that it affords is certainly an attractive, cost-saving feature of UTM technology. However, it is the unification, robustness, and flexibility of associated management capabilities that enable recurring returns, and therefore much greater gains, due to both improvements in ongoing operations and greater security effectiveness. Of course, such capabilities are also one of the primary prerequisites to having UTM be suitable for enterprise-class deployments in the first place (with top-notch security, performance, integration, and flexibility being the others).