

Discover. Determine. Defend.



ENTERPRISE THREAT
MANAGEMENT (ETM) —
WORK SMARTER, NOT HARDER



supplied and supported by Phoenix Datacom

SOURCEfire®
Security for the real world.

PHOENIX
DATA COM
NETWORK PERFORMANCE AND SECURITY

www.phoenixdatacom.com

01296 397711

info@phoenixdatacom.com

TABLE OF CONTENTS

Why is a New Approach to Information Security Necessary?	3
The Threat Landscape	3
<i>Figure 1. The Threat Landscape</i>	4
The Technology Landscape	4
The Regulatory Landscape	4
What is Enterprise Threat Management (ETM)?	5
Intrusion Prevention (IPS)	5
<i>Figure 2: Enterprise Threat Management</i>	5
Network Behavior Analysis (NBA)	6
Network Access Control (NAC)	6
Vulnerability Assessment	6
Shared Intelligence	6
Consolidated Management	7
Why is ETM the Right Approach?	7
<i>Figure 3. The Viewpoint of ETM</i>	8
But Why This Particular Set of Technologies?	9
How does ETM Compare to Other Approaches and Technologies?	9
Unified Threat Management (UTM)	9
Security Information and Event Management (SIEM)	9
Security Product Suites	10
How Will ETM Evolve?	10
Conclusion	11



WHY IS A NEW APPROACH TO INFORMATION SECURITY NECESSARY?

When it comes to information security today, most organizations are struggling just to tread water. They continue to make substantial investments but are still experiencing breaches and other types of incidents at an unacceptable rate. The primary issue is that conditions have changed, driving up the cost and complexity and reducing the effectiveness of the conventional approach to security – an approach that is heavily dependent on a disjointed, disconnected set of point products. In particular, some of the more significant changes and challenges confronting today's IT-dependent organizations include a highly dynamic threat landscape, an ever-evolving technology landscape, and an increasingly onerous, regulatory landscape.

The Threat Landscape

The “good ol’ days” when organizations only had to contend with a handful of file-level viruses and network worms each year are fading fast. Now the threat landscape (see Figure 1) is far more dynamic, due primarily to a relatively recent shift in hacker motivation from gaining notoriety and building a reputation to actually making money. Specific changes and associated implications for an enterprise security solution include the following:

- ▶ The quantity of threats that must be addressed in any given period is rising. This is supported by a number of vendor-published reports, and although a relatively basic consequence of the shift in hacker motivation, it nonetheless indicates that threat management solutions must become more efficient.
- ▶ Threats are being generated more quickly than ever before. The average period of time between the announcement of a new vulnerability and the release of a corresponding exploit, once measured in months or weeks, is now only a handful of days. In fact, according to the Symantec Internet Security Threat Report (Volume XI), nearly twenty-five percent of the time the gap is less than a day. With so little time to respond, the effectiveness of reactive countermeasures, such as antivirus tools and patch management systems, are diminishing, signaling the need to supplement them with ones that are more proactive in nature.
- ▶ Threats are becoming more diverse. Viruses, worms, and DoS attacks are life form joined by spam spewing botnets, spyware, rootkits, and a veritable smorgasbord of techniques for attacking web technologies and applications. Therefore, organizations need more types of countermeasures and greater efficiency when operating all of them, or, they need ones that are inherently capable of addressing new types of threats that emerge without always having to add a new product.
- ▶ Threats are becoming more elusive. Techniques such as blending (i.e., using multiple propagation or exploit mechanisms) and targeting (i.e., building customized, organization-specific attacks) only compound the general trend of threats migrating up the computing stack – an approach that involves taking advantage of application-layer weaknesses to slip through the network-focused defenses currently deployed by most organizations. The result, in addition to countermeasures with better visibility and control at the application layer, is the need for ones that detect previously unknown threats, either independently or by working together.
- ▶ Threats are coming from the inside, too. Whether this item qualifies as a “change” is debatable. Many security professionals would maintain that the insider threat has not only been present, but significant, since the beginning. What has changed, though, is the degree of recognition the insider threat is currently receiving, which emphasizes the need for security solutions that provide closer scrutiny of internal users and systems – not just network perimeters and external users.

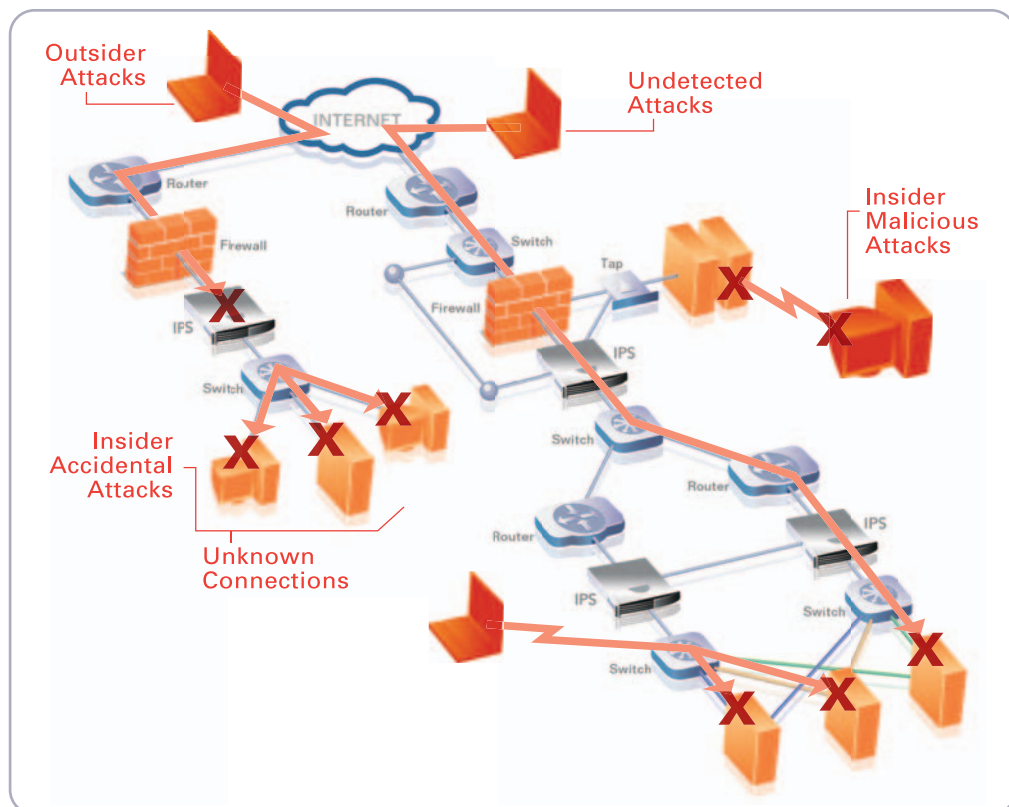


Figure 1. The Threat Landscape - Threats are coming from inside and outside the enterprise and are becoming more sophisticated and diverse.

The Technology Landscape

Driven by the typical forces of business, the technology portfolio for most organizations is also highly dynamic. This, in turn, is directly responsible for a highly dynamic vulnerability landscape.

To remain competitive, organizations are constantly adopting new technologies, buying or building new applications, and implementing new versions of the ones they already have. Consequently, not only must more infrastructure be managed and secured, but a significant portion of it is different, complex, and quite possibly decentralized. The result is a steady flow of code-flaw vulnerabilities, as well as weaknesses introduced by configuration errors, leading to the need for security solutions that exhibit greater degrees of efficiency and adaptability.

At the same time, the desire to improve operational efficiency and boost revenues has been responsible for the trends of increasing user mobility, the proliferation of remote offices, the growth of online customer services, and greater inter-connectivity between business partners. But there is also a downside to these trends. The introduction of more points of entry into an organization's network is a condition that further emphasizes the need to deploy countermeasures that help secure internal networks and systems.

The Regulatory Landscape

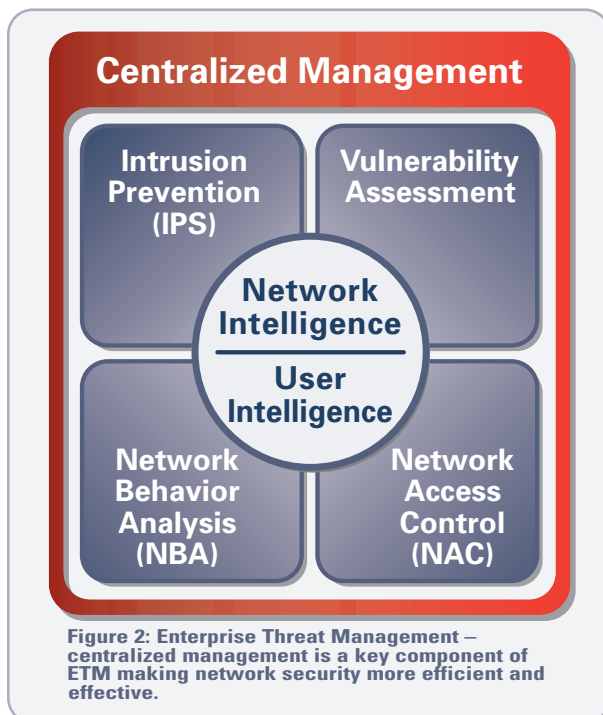
Yet another significant and, at times, highly dynamic challenge for modern organizations is the legal/regulatory landscape. Over the past decade, concerns pertaining to the privacy of individuals, the integrity of business operations, and the continuity of critical infrastructure have spawned a plethora of laws and industry-specific regulations having both direct and indirect impact on an organization's computing systems (e.g., HIPAA, SOX, PCI). Whether and to what degree these "rules" are having the originally intended effects is debatable. But one thing that is



not debatable is the diversion of resources required for organizations to demonstrate compliance. The implication in this case is the need for security solutions that, in addition to their other functions, can enforce, track, and report adherence to internally and externally derived policies.

Given all of these challenges, it should be clear that the patchwork defense associated with a point product approach to information security is simply not sustainable. It is subject to high capital costs, as each and every new issue that arises requires yet another product. It is subject to spiraling operational costs, both to maintain all of the products and to cobble together some degree of integration/collaboration between them. And, finally, it is also subject to incomplete and ineffective coverage, a product of the physical, functional, and logical gaps that inevitably arise. What organizations need instead is a new approach, one which achieves significantly greater degrees of effectiveness, for example, by emphasizing collaboration between components, adaptability/extensibility, and the potential for automation. Enterprise Threat Management is such an approach.

WHAT IS ENTERPRISE THREAT MANAGEMENT (ETM)?



ETM is the first-generation embodiment of the recognition that when it comes to protecting computing and information assets organizations need to work smarter, not harder. From a technological perspective, ETM is the combination of four highly complementary threat and vulnerability management technologies built on a foundation of shared intelligence and operating under the control of a single overarching management system. The result truly is a solution where the whole is greater than the sum of the parts.

As illustrated in Figure 2, the specific components that comprise an ETM system include Intrusion Prevention (IPS), Network Behavior Analysis (NBA), Network Access Control (NAC), Vulnerability Assessment, multi-faceted shared intelligence, and a consolidated management application.

Intrusion Prevention (IPS)

Fundamentally, the goal with intrusion prevention technology is to stop an attack as it is occurring. Doing so depends on detecting specific events, having sufficient confidence that those events indeed correspond to an attack, and engaging a mechanism to actually stop the flow of associated communications traffic. Knowing which events to detect in the first place is instrumental to minimizing the occurrence of false negatives, and is why a leading IPS should incorporate multiple techniques, including exploit-based rules, vulnerability-based rules, protocol anomaly rules, and heuristics (i.e., root-cause analysis rules). Of course, minimizing false positives is absolutely critical, too, which is why a leading IPS should also analyze a wealth of contextual information to further qualify the nature and impact of what is being detected.



Network Behavior Analysis (NBA)

A relatively unique capability of NBA is the extent to which it can assist with the detection and mitigation of unknown attacks. Indeed, by baselining network activity and subsequently identifying events that exceed established thresholds, NBA has the ability to identify attacks for which the corresponding threats and/or vulnerabilities have not yet been widely disclosed and defined. As powerful as this sounds, it is important to recognize that the degree of effectiveness ultimately depends on the quality, or value, of the data source being used to build the baselines. A high value data source will provide breadth, in terms of the types of traffic it supports, and depth, in terms of the granularity of details it yields for each type. In contrast, low value data sources, such as summarized network flows, are considerably more opaque.

Having a rich data source is also important for another significant capability of NBA. Specifically, NBA can provide organizations with extensive visibility into the composition of their networks and endpoint systems and how they are being used. This facilitates a number of derivative capabilities – including policy development, vulnerability assessment, incident recovery, asset management, and network troubleshooting – not to mention that it serves as a crucial source of the contextual information that forms the backbone of an effective ETM system.

Network Access Control (NAC)

The technology commonly referred to as NAC consists of two distinct services. The first service involves an assessment of the security and configuration status of a client device attempting to access a network. Although it is helpful, this pre-connect phase of NAC is considerably less effective than the second service, which is responsible for setting and enforcing the extent of access the user/client is ultimately allowed. Indeed, by scrupulously embracing this post-connect phase of NAC, organizations can effectively implement the principle of least privileges and thereby dramatically decrease their exposure to all types of threats (e.g., known and unknown, outsider and insider). It is important to recognize, however, that an essential prerequisite entails having extensive visibility of network activity, both to initially shape and then continuously refine the associated access rules.

Vulnerability Assessment

The power of Vulnerability Assessment lies in the fact that it is a proactive technology. It enables organizations to identify vulnerable resources and remediate them, or at least to configure intermediate countermeasures (e.g., a firewall or IPS) to protect any known weaknesses. The primary limitations with Vulnerability Assessment, at least historically, have been: the periodic nature of the scans, the disruptive nature of the additional traffic introduced by the scans, and the abundance of raw findings produced by the scans. The first two of these issues can be alleviated by relegating active Vulnerability Assessment technology to targeted and/or less-frequent scans and complementing it with always-on, passive Vulnerability Assessment technology. As for the third issue, it can be addressed by (a) once again, having sufficient contextual information, in this case to qualify a given vulnerability and the specific instances of it in a given network, and (b) taking advantage of the resulting prioritization to automate at least a subset of available corrective measures.

Shared Intelligence

This is not another technology per se, but rather is one of two keys necessary for enabling an ETM system to be greater than the sum of its constituent parts. The other key, consolidated management is covered in the next section. The point is that each of the component technologies, as a matter of routine, has some pieces of information pertaining either to the composition of the environment that is being protected or how that environment is being used: IPS has information on actual and possible threats; Vulnerability Assessment has information on actual and possible vulnerabilities; NAC has information on endpoints; and, NBA has information on





endpoints, normal and abnormal activities, and even potential threats. And although these pieces of information are clearly useful within the domain of each individual technology, very often they are also useful to one or more of the other domains.

For example, an IPS that has access to endpoint and vulnerability details can automatically discount (/elevate) all known or suspected threats that are irrelevant (/relevant) due to the absence (/presence) of systems that are actually susceptible to them. In this case, shared intelligence helps eliminate ambiguity and dangerous assumptions, enabling a better real-time decision to be made. Similarly, available contextual information could be used to proactively or reactively configure NAC to disallow communications that are considered unproductive, too risky as a matter of routine, or too risky as a result of immediate conditions.

Finally, it should be noted that additional sources of contextual information can enhance the overall solution even further. For instance, data indicating the identity of users operating specific devices and generating specific traffic provides yet another level of qualification for detected events. But that's not all. Indeed, the power, and therefore criticality, of this sort of "user awareness" should not be under-estimated. User identity and associated role information can be used to prioritize vulnerability scanning and remediation efforts, to significantly enhance the granularity of NAC policies, and, in general, provide more in-depth enforcement and tracking of compliance requirements.

Consolidated Management

As indicated, consolidated management is the second key to enabling an ETM system to be greater than the sum of its parts. Indeed, consolidated management is effectively the technological component that creates shared intelligence. At a minimum, it is responsible for coordinating the "sharing." More importantly though, it is responsible for applying the intelligence (i.e., analysis and correlation steps) that transforms what is accurately described as raw data into actual, actionable information. In this regard, consolidated management is an invaluable contributor to the higher levels of security effectiveness, not to mention efficiency, that are possible with an ETM system. Better, stronger protection is achieved in an automated manner, or at least in a semi-automated manner if human interpretation and confirmation is preferred or required.

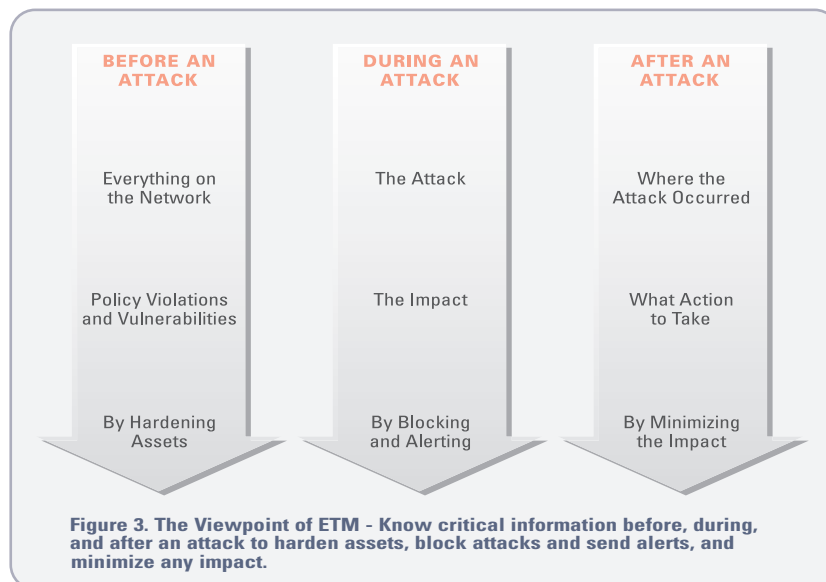
Of course, consolidated management has other advantages as well. Operational tasks and ongoing maintenance are greatly simplified by reducing the number of management consoles from four to one. Policies can be integrated, or at least linked, across the different technologies, which helps reduce the occurrence of conflicts, or worse, gaps. Integration with other security tools, especially those associated with remediation or mitigation response activities can be leveraged for use with all of the component technologies. And reporting is also integrated, yielding a more holistic perspective of the state of security and compliance for the organization. The bottom line: more is possible with less, which is definitely consistent with working smarter, not harder.

WHY IS ETM THE RIGHT APPROACH?

The previous section established what ETM is from a technological perspective. It also provided some insight regarding the key characteristics that differentiate a best-in-class ETM offering. But why is ETM the right approach for organizations to take? The short answer is that ETM is appropriate because of the extent that it addresses the myriad of challenges confronting today's organizations. Some of the details supporting this position have already been revealed. However, a more complete treatment of the topic requires closer consideration of what ETM actually achieves. To this end, ETM is appropriate because from a functional perspective:

- ▶ It establishes "blended defenses" by incorporating countermeasures that use a range of proactive, preventive, reactive, positive-model, and negative-model techniques. Furthermore, this blending is not only present in terms of functional coverage, but is also present with respect to time, meaning that ETM ensures continuous protection before, during, and after an attack.

- **Before an attack, visibility is provided into everything running on the network. Vulnerabilities and policy violations can be detected providing the opportunity to harden assets and minimize overall target area.**
 - **During an attack, specific threats can be accurately identified, assessed in terms of their impact, and dealt with accordingly (e.g., alert or block).**
 - **After an attack, the impact can be minimized by pinpointing what occurred and accelerating corrective actions.**
- ▶ It accounts for both known and unknown threats, including those associated with increasingly common zero-day attacks. This is accomplished by combining deterministic threat detection techniques (e.g., exploit-based rules) with ones that are non-deterministic, yet proven (e.g., vulnerability-based rules), and ones that are completely indiscriminate (e.g., policy enforcement).
 - ▶ It is highly adaptable and extensible, which helps reduce the need to continuously purchase new point products every time a new type of threat or technology emerges. New detection rules or even entirely new detection mechanisms can be implemented as routine updates or periodic upgrades to the system. Notably, during any interim before such updates and upgrades are implemented, organizations will still be protected by one or more of the other ETM mechanisms of the system. For example, Vulnerability Assessment and NAC could be used to disallow all vulnerable endpoints from participating in IM sessions and NBA would still be operational to uncover any related exploits in the event that the IPS required an update to deal with a new IM vulnerability.



- ▶ It provides practical protection for internal networks and systems, not just for high-profile interfaces to customer, partners, or the Internet in general. Although all of the ETM technologies support this objective, the combination of NBA and NAC is particularly well suited to the task. By observing operations passively and then steadily implementing rules that selectively eliminate unnecessary, unproductive, and risky activities, organizations can harden their internal environment in a manner that is largely non-disruptive.
- ▶ It enables setting, enforcing, tracking, and reporting of compliance-related policies and requirements. This ability to address the full life cycle of compliance management functions is a significant advantage. It alleviates the all-too-common need to cobble a solution together from multiple tools, each of which covers only a single technology domain (e.g., Windows servers, Cisco networking devices) and/or a single function (e.g., enforcement, reporting). Once again, the combination of NBA and post-connection NAC capabilities are particularly relevant in this case.

On top of everything else, it is important to acknowledge the value of having pervasive, shared intelligence and consolidated, coordinated management. These are essentially force multipliers, boosting the effectiveness, efficiency, and affordability of ETM well beyond that achievable with point products alone.



But Why This Particular Set of Technologies?

This is a logical follow-up to the previous question. To begin with, it has already been demonstrated that IPS, NBA, NAC, and Vulnerability Assessment provide a relatively broad and highly complementary range of capabilities. More importantly though, along with the key enablers of shared intelligence and coordinated management, these technologies establish a robust foundation for a more comprehensive, long-term, security solution. This is an important distinction. At least at this point in its evolution, ETM is not trying to be or do everything that is security. Thus, the actual technologies that are incorporated are a bit less important than the overall concept. In fact, an ideal ETM system should be modular by design. This way organizations can start with the subset of components that best meet their functional needs and budgetary resources but are still able to add more pieces to the solution over time. Furthermore, bi-directional interfaces should be available to support integration with other products and technologies as needed – whether to extend the coordinating effect of ETM to other essential security tools (e.g., firewalls, VPNs, patch management, antivirus) or simply to “feed” data to other management consoles (e.g., security information and event management systems).

HOW DOES ETM COMPARE TO OTHER APPROACHES AND TECHNOLOGIES?

Another way to characterize ETM and its value to IT organizations is to compare it with and position it relative to other approaches and technologies, such as Unified Threat Management (UTM) devices, Security Information and Event Management systems (SIEMs), and security product suites in general.

Unified Threat Management (UTM)

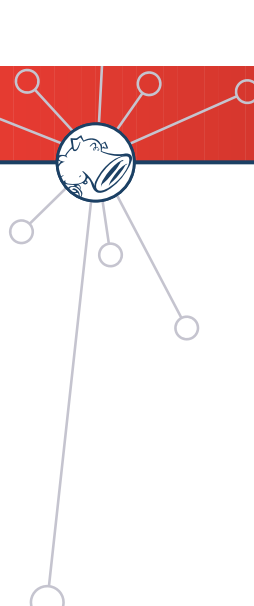
UTM is primarily concerned with reducing the complexity of security infrastructure through physical consolidation. Specifically, with UTM the number of separate devices that need to be purchased, operated, and maintained is reduced by combining multiple security functions into a single platform. This characteristic of UTM is certainly advantageous, but unfortunately it is not universally applicable. Indeed, performance and capacity constraints that are an inevitable consequence of supporting many functions in one device typically limit UTM implementations to small/medium businesses and branch offices.

Despite this limitation, UTM has the potential to yield some of the same benefits as ETM, albeit on a smaller scale. For example, to the extent UTM enables organizations to operate a greater number of security mechanisms than they otherwise could (perhaps due to resource limitations), the result will be a relative improvement in security effectiveness. Similarly, to the extent that a given UTM product involves integration, either in the form of shared data or even just shared management functions, the outcome will be another boost in effectiveness, as well as operational efficiency.

Lastly, it would be unfair to ignore the potential for UTM as a platform for at least some of the instances of the core ETM technologies that will be required to provide complete coverage for an organization’s entire networked environment. In other words, although UTM is not equivalent to ETM, it can certainly have a role to play within a comprehensive ETM implementation.

Security Information and Event Management (SIEM)

Technically, the consolidated/coordinated management component of ETM is essentially a domain-specific SIEM system. After all, it does all the same things that a SIEM system supposedly does – providing event consolidation, analysis, correlation, response, and reporting functions – albeit just for the core ETM technologies versus everything under the sun. And while this qualification may sound like a limitation, it is actually an advantage. By focusing on just a few



technologies, the ETM's version of SIEM is able to "be the best it can be." This is in contrast to broad-spectrum SIEM systems which often struggle to achieve a meaningful degree of analysis and correlation due to the scope and volume of data they are typically attempting to process. Nonetheless, another important characteristic of an ideal ETM system is the ability to work with an enterprise SIEM system. This way organizations that have invested in SIEM products can continue to use them, at least as a relatively comprehensive reporting solution.

Security Product Suites

ETM is clearly a technology-centric approach to information security. More precisely, it is a security system, a collection of technologies that are effectively bound together as a result of the emphasis placed on integration, shared intelligence, and coordinated management. This systems orientation is what distinguishes ETM from run-of-the mill security product suites available from numerous vendors. Generally, these suites are just large collections of products, offering little advantage beyond the opportunity for one-stop shopping. Various subsets of these collections may be organized by themes, but rarely do these combinations exhibit sufficient integration and coordination to yield a truly meaningful improvement in security effectiveness or operational efficiency.

One point deserves to be repeated: It is the presence and scope of shared intelligence and coordinated management capabilities that sets ETM apart from all other threat management technologies, products, and solutions. They are the force multipliers that make ETM more than the sum of its component parts.

HOW WILL ETM EVOLVE?

Having established what ETM is and how it compares to other approaches and technologies of note, it is also reasonable to ask how ETM is expected to change over time. In this regard, specific details are not as important as general ones. Overall, it certainly makes sense to aim for ever greater degrees of effectiveness and efficiency by continuing to integrate or even completely incorporate additional threat and vulnerability management technologies into the system. For example:

- ▶ In terms of hardening assets in advance of an attack, candidate countermeasures include patch management and configuration management;
- ▶ In terms of stopping attacks that are underway, possibilities include firewalls, host intrusion prevention, content filtering, and antivirus, anti-spyware, and anti-spam software; and,
- ▶ In terms of aiding discovery and recovery after an attack, tools deserving attention include those addressing incident management, log analysis, visualization, and forensics.

However, more important than which components are addressed next is how they are added. Ideally, new technologies should only be incorporated in a manner that maintains the high degree of intelligence sharing and management unification that distinguishes ETM from other approaches. And, to reiterate an earlier point, it is exactly because this is hard to do that it is best to start with a solid foundation and then methodically build from there, as opposed to cobbling everything together at once.





CONCLUSION

There remains little doubt that the point product approach to information security is incapable of keeping pace with prevailing changes to the threat, technology, and regulatory landscapes – at least not in a manner that yields a reasonable degree of effectiveness and affordability. In contrast, Enterprise Threat Management is a new approach based on the premise that maintaining an appropriate level of protection for one's computing systems depends on the ability to work smarter, not harder. By emphasizing shared intelligence and consolidated, coordinated management as the binding medium for a set of complementary and highly capable security technologies – namely intrusion prevention, network behavior analysis, network access control, and vulnerability assessment – ETM provides a solid foundation for meeting both current and future information security requirements.