

Meeting Real Needs of Real Customers Across the Spectrum: Intellitactics Introduces the SAFE Product Family

Abstract

On April 8, 2008, Intellitactics, a leader in Security Information and Event Management (SIEM) and a member of the PCI Standards Council, announced a new suite of SIEM products designed to meet the requirements of a broad range of organizations. The Intellitactics SAFE suite delivers simplified implementation, management and administration of SIEM through a family of appliance-based products, each one designed to be complete solution for the organization at a given level of maturity in security management. These appliance-based products provide organizations of all sizes the ability to implement event management in a manner that best fits their environment and their budgetary constraints. The completeness of each product in the suite is a departure from competitor strategies that either take a one-size-fits-all approach to the mid-market, or more piecemeal approaches that may leave customers with an incomplete solution just to meet budget constraints. Enterprise Management Associates (EMA) believes that Intellitactics' SAFE product strategy opens a new range of possibilities for organizations of all sizes to reap the benefits of actionable visibility into IT risk events and risk-relevant information critical to effective IT risk management. The move showcases Intellitactics' thought leadership—as well as a distinctive degree of sensitivity to the realities of *all* its customers—in providing solutions that serve a well-thought-out set of capabilities at multiple levels of the market.

EMA believes that Intellitactics' SAFE product strategy opens a new range of possibilities for organizations of all sizes.

Context

The security market has long been one of the most prolific and innovative in IT. Driven by an unending parade of threats that range from the maddeningly simple to the truly ingenious, security vendors must constantly innovate in order to deliver the countermeasures critical to business survival.

This has led to a profusion of security tools and technologies in the enterprise—a profusion which poses a substantial management challenge. On the one hand, businesses must maintain an appropriate and comprehensive toolset to assure the confidentiality, integrity and availability of information and stay ahead of the threat. On the other, they must make the most efficient use of resources in order to meet constrained budget limitations, while simultaneously delivering on business priorities and enabling business innovation.

Security Information and Event Management is a technology domain uniquely positioned to help enterprises achieve this difficult balancing act. By consolidating events and other information from a wide range of management tools, critical applications, database transactions, system level alerts, and other sources, SIEM helps organizations correlate risks and threats, identify high priority issues, and maintain an effective security posture in the face of constantly changing risks. They also support more efficient auditing and reporting processes that help reduce the total impact of regulatory compliance. Together, these values support better alignment with business priorities for more effective IT governance.

In particular, SIEM solutions simplify the incident management process into two parts: alert and response. Without a SIEM solution, even the most efficient security team will be forced to manually investigate multiple countermeasures in the majority of attacks. This investigation will likely require multiple logs, multiple people, and multiple technologies to correlate.

While a SIEM solution is by no means a replacement for this type of process, it does narrow the focus of what necessitates an investigation. In other words, organizations can leverage SIEM technology to automate the initial phases of the incident response process for a large percentage of incidents. Pre-incident research reduces the chance of incidents escalated prematurely, which, in turn, has a positive impact on the rising costs of incident response. Beyond these values, SIEM solutions offer a central point for investigating incidents in depth when necessary.

While many businesses see these benefits of SIEM, making the technology accessible to a wider market has been a challenge for vendors and would-be customers alike. For many years, the sophistication of SIEM limited its adoption to businesses where high maturity in security management is critical, or to the largest, most complex, or most resource-

rich enterprises. Some vendors have made inroads into increasing the wider accessibility of SIEM, but many approaches frustrate customers with a one-size-fits-all approach that fails to take into account the fact that organizations vary in security management maturity. This leaves the broader market with options that are, on the one hand, too much for the less mature organization, and too little on the other for the more mature. Taking a modular approach to this market can produce a product set that can be more flexibly adapted, but if customers are sold just enough to close a deal, they may find that the resulting solution is not as complete as expected, forcing them to consider further investment when limited resources might have been better applied to increasing maturity when needed.

Some vendors have made inroads into increasing the wider accessibility of SIEM, but many approaches frustrate customers with a one-size-fits-all approach.

Event

It is for these reasons that Intellitactics has developed their new appliance-based SAFE product suite that allows a wide range of organizations to become compliant and secure through SIEM solutions. The new product line spans all types of organizational and infrastructure models to deliver a spectrum of event management products, each product a complete offering appropriate to the needs of the customer at a specific level of maturity in security management.

The strategy builds on Intellitactics' introduction of its SAFE LA product, which enables businesses to meet essential requirements for log acquisition. The SAFE LP product introduced with this announcement effectively represents a halfway point between SAFE LA and more fully-featured SIEM, providing capability for the parsing and normalization of logs and event data, event correlation, and persistent storage of compressed event information in the product's multi-dimensional Security Data Warehouse, in addition to capabilities for event retrieval, alerting, and compliance reporting. Intellitactics plans further SAFE product releases in 2008, with a planned mid-year release of a product, designed to augment log acquisition with parsing and normalization, persistence, retrieval and report-

ing capabilities. At the upper end of the spectrum, the Intellitactics vision for the SAFE family incorporates a much broader range of SIEM functionality, including complex correlation, service management integration, alerting and scoring, and integration with a wide range of security products and network operations center (NOC) environments.

Key Ramifications

The incorporation of a complete range of functionality for a specific level of customer maturity in each SAFE product is a distinctive departure from other vendor strategies that approach that problem in a less flexible or more piecemeal way. Each product in the SAFE family is specifically designed to provide comprehensive coverage for an organization at that level of need and maturity, rather than forcing customers to adopt either a middle-of-the-road approach or one that requires a greater investment in multiple modules than anticipated, just to assure the completeness of the solution. This is an important development as many organizations have been hesitant to adopt SIEM because existing offerings do not fit their budgetary constraints or the organization's capabilities for implementation. Intellitactics has designed their SAFE product line to fit organizations both large and small—the latter being a demographic all but forgotten by market-leading SIEM vendors. This does not mean that the solutions offered by Intellitactics will be any less feature rich. The SAFE product suite will still be capable of allowing organizations meet compliance and security goals through pre-defined reports, simple user interfaces and enhanced parsing of logs.

By offering a diverse suite of products, each with its own complement of valuable functionality, Intellitactics is now poised to deliver SIEM solutions to organizations previously overlooked or underserved by the SIEM market.

By offering a diverse suite of products, each with its own complement of valuable functionality, Intellitactics is now poised to deliver SIEM solutions to organizations previously overlooked or underserved by the SIEM market. This is an important development as the IT security market has created process bloat through offering multiple security technologies to address multiple issues, but not enough effective solutions for rationalizing these processes across a wide range of organizational maturity. The result for the overlooked segments of the market as a whole has been that affordable or usable offerings often miss the severity of particular events due to the lack of correlation between countermeasures.

By making a more effective set of SIEM solutions available to these environments, customers now have access to a new range of tools for creating efficiency in their efforts to address security risks. When more sophisticated attacks or events arise, those responsible for security across a wider range of businesses will have access a central point to investigate these incidents in depth and automate response processes. This capability enhances the security posture of the organization and simplifies management of security solutions for a far broader scope of the market.

EMA's Perspective

When experts describe best practices in IT security management, what they often mean is the management of security as practiced among the businesses that have the resources to implement high maturity. Event correlation and response, however, is something *every* business must address, regardless whether they have access to the best solutions the industry has to offer. Limited customer resources for investment in best practices should not mean limited customer value or benefit. The SIEM market should have evolved enough to be able to recognize this reality and provide solutions accordingly.

Many have tried, but few have sought to meet the needs of so many levels of customer demand in such detail, and with a set of products that each offers strong capability for event correlation, analysis and reporting in addition to aggregation. Fortunately for Intellitactics customers, this is one leader that recognizes the value of such an approach, and the value of having a set of solutions that offer a complete feature set appropriate to a given level of need.

EMA therefore believes that Intellitactics will see success with this new business model. It is clear that Intellitactics is a SIEM leader in product development, delivery, and thought leadership. Their new product line stands to deliver event management to organizations of many diverse sizes and purchasing power. This is an important development as many of Intellitactics' competitors have allowed the needs of smaller organizations to slip under the radar.

This is an important development as many of Intellitactics' competitors have allowed the needs of smaller organizations to slip under the radar.

This commitment to the real needs of real customers, no matter how mature, is reflected in Intellitactics' recent inclusion on the PCI council. This is an important development not only because compliance with the PCI Data Security Standard is one of the major concerns for IT executives, but also because the PCI standard is one of the most prescriptive from a technical perspective. It is because of the prescriptive nature of PCI that the council consists of only the leading vendors in their respective fields. Including Intellitactics on the council is not only a recognition of the company's achievement; it also gives the company a new platform for driving the direction of where the standard goes in terms of SIEM. Because of the implications of the standard for such a broad range of businesses, Intellitactics' sensitivity to such a wide scope of customer needs has significant and positive implications for the future of the PCI standard. Based on Intellitactics' thought leadership in these areas, the company is the right choice for this role—and nowhere is this more evident than in its newest product direction manifested in the SAFE suite vision.

Enterprise Management Associates, Inc.
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: 303.543.9500, Fax: 303.543.7687, Web: www.enterprisemanagement.com

ITT007.033108

©2008 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.