

The Emerging IT Security Management Market

The IT security management market is emerging out of the need to transform raw security data into information that can be used to quickly correct security problems.

A new market is forming to meet the needs of IT security operations personnel in midsize-to-large enterprises who:

- Require useful information from the flood of raw data and alerts that are generated by security devices.
- Require documentation of system audit compliance.
- Want to consolidate the security operations of a heterogeneous environment.

What Is IT Security Management?

Enterprise IT security management focuses primarily on the tools, technologies and services that are needed by IT security operations to manage security devices and the security of IT infrastructure, applications and transactions (see “Enterprise IT Security Management Defined”). The core value proposition of IT security management is the correlation of security data from multiple devices and systems to enable better security assessment and support corrective action. The primary driver of this nascent market is the failure of intrusion detection systems (IDSs) to separate real threats from the background noise of ineffective probes, false alarms and normal system changes.

IT Security Management Vendor Approaches

A new set of IT security management software vendors has emerged to meet the need to manage security events. These IT security management point-solution vendors have introduced products that are focused on the consolidation and correlation of security device information. Sensing an opportunity, several broad-scope security software vendors and network and systems management (NSM) providers also have introduced IT security management products. Each of these vendors has a set of common strengths and challenges (based on the vendor type), in addition to a set of strengths and challenges that are unique to a particular vendor.

Although the point-solution vendors have focused on the most-pressing operational issue of managing IDSs, IT security management is not just about intrusion detection. Enterprises also are under increasing regulatory pressure and audit scrutiny in the area of security policy compliance. Some IT security management products, primarily from broad-scope security software vendors and NSM providers, focus on the IT infrastructure layer to provide a consolidated view of policy compliance and system vulnerability with reference to best-practice models. Many vendors in this space are planning new functions that will evaluate a given threat with respect to the vulnerability of a target system through an assessment of relevant system configuration information.

Gartner

An Evolving Market and an Uncertain Future

Although the user and vendor aspects of IT security management satisfy Gartner's definition of a market — that is, a set of buyers with common needs and a set of vendors supplying products to meet those needs — the market's long-term viability is not guaranteed. IT security operations remain fragmented in many enterprises. Therefore, organizational issues may limit the number of buyers for consolidated management products, and they may also limit the ability of IS organizations to effectively deploy technologies.

NSM providers have been promising pre-defined (or dynamic) correlation of systems management data, but they have only delivered very narrow, pre-defined correlation and toolkits that require extensive user customization. Nearly every vendor in the IT security management space is promising pre-defined correlation, but vendor execution in this area can only be validated by customer field experience, which currently is limited.

In the longer term, the IT security management market may be superseded by security platforms that operate "in line" with the network data stream, integrating IDS, firewall and antivirus functions, to provide real-time intrusion prevention automation.

Today, IT security operations personnel should evaluate IT security management technology as a tactical way to improve the effectiveness of IDS, audit and vulnerability assessment; an instrument to consolidate security operations; and a bridge to the as-yet unrealized potential of intrusion prevention.

Features

"IT Security Management Market Drivers and Inhibitors" — Examine vendor viability and organizational issues that are critical to success in the IT security management market. **By Mark Nicolett and Matthew Easley**

"IT Security Management Technology Evaluation Criteria" — Map IT security management products against operational requirements. **By Mark Nicolett and Matthew Easley**

"IT Security Management Point Solutions: Part of the Cure" — Use point-solution vendor offerings to help cure the intrusion detection system false-alarm epidemic. **By Matthew Easley and Mark Nicolett**

"Broad-Scope Software Vendors for IT Security Management" — Consider broad-scope security software vendors when selecting an IT security management solution. **By Mark Nicolett and Matthew Easley**

"NSM Vendor Strategies for IT Security Management" — Examine network and systems management vendors that provide IT security management to leverage their event management technology and customer base. **By Mark Nicolett and Matthew Easley**

"NetIQ to Acquire PentaSafe for Critical Mass in Security" — Review NetIQ's proposed acquisition of PentaSafe Security Technologies for opportunities to expand security management across operating systems and security devices. **By Mark Nicolett, Cameron Haight and Roberta Witty**