

Evolving Network Security Solutions Landscape

Report Prospectus

Overview

In the face of increasingly valuable applications, escalating threats, rising compliance pressures, more complex solutions, and a growing purchasing sophistication that demands real business return on information security investments, the security solution landscape is rapidly shifting.

The straightforward application of separate, best-of-breed security “point” solutions no longer is adequate. Both security technology and more effective overall IT management demand better integration in order to maximize security effectiveness and to contribute to the overall simplification and management of the IT fabric. “Consolidation” is a word that’s frequently used by both vendors and users to describe the technical and customer solutions required to increase value while simplifying operation.

These forces are emphasizing the system-level aspects of security: The integration and correlation of a broader source of event information; the definition and automatic evaluation of high-level policy definitions; the automation of as much of network and system operation as possible; the ability to systematically evaluate security vulnerabilities under modeled threats, and intelligently plan and evaluate potential mitigation and threat response strategies.

These driving forces are beginning to dramatically change the way security is interwoven into the infrastructure. In 2003 well-capitalized startups brought innovative new products to customer trials. Established companies like Cisco, Symantec and Juniper/Netscreen saw interest in their security offerings rise sharply. As the new offerings undergo the trial-by-fire of early customer use, the concepts behind these technologies will start to gain real market visibility and to drive broader purchase behavior.

Background

As network-connected and network-accessed applications became an important application model and of increasing importance to business operations, the need for, and importance of security solutions (starting with firewalls) has just grown and grown. Despite the Dot Com meltdown and resulting IT recession, categories such as Firewalls and IDS saw revenues grow steadily throughout. New and rapidly growing categories such as Security Incident Management, Vulnerability Management and Patch Management have emerged and taken off. Even though overall venture capital investment was low during these years, security focused startups grabbed nearly \$1B of new venture investment per year. Well funded by revenue growth and additional investment when needed, during these years we saw evolution within existing product lines in all dimensions – increased functionality and bandwidth throughput as well as price/performance improvement and cost reduction. In the same timeframe communications suppliers such as Cisco and Juniper, and the platform companies such as

Microsoft, IBM and HP kept upping their security investments and awareness in response to growing customer importance.

Market Drivers

The four big drivers behind the changing security landscape are these:

- (1) the rapid growth in the use and importance of network-enabled, server-based applications that necessarily service a geographically distributed, multi-organization user population
- (2) The ongoing pressure on CIO's to increase the effectiveness of IT and at the same time make it more cost effective
- (3) The growing threat posed by increasingly sophisticated, "zero day," and multi-faceted threats
- (4) The overall size of the security markets and the structural investments by major platform vendors (such as Cisco's network management initiative and Microsoft's broad security enhancement investment).

The Bigger Picture – Security Integration and Automation

While customers have been pleased with the business success, re-investment and rapid evolution in security best of breed products, they are simultaneously dismayed by the growing complexity and stovepipe designs that often create as many problems as they solve and require ever increasing investments for staff education, system integration and operation. At the same time the business is making demands on the security team to contribute to initiatives like regulatory compliance or service level management. Point solutions that are islands to themselves are increasingly technically ineffective and too complex and expensive to own and operate.

The 2004 NRG Research Report *The Changing Network Security Landscape* will examine the shifting landscape as vendors and customers alike respond to the shifting demands and opportunities of network security. Topics addressed include:

- (1) The shift from reactive to pro-active security
- (2) The emergence of near-real time log analysis
- (3) The next generation of IDS/IPS
- (4) Firewall evolution – the emergence of application firewalls
- (5) The broad potential of anomaly detection
- (6) Modeling, policy automation and next generation vulnerability management

Market Shifts / Investment Summary

The growth in product revenues and the market robustness during the broader downturn have combined to make security one of the favorites in the VC community, fueling the appearance of new companies and the emergence of new categories. Many categories have too many competitors for long term viability. The consolidation and integration

forces discussed in this report create both a need and an opportunity for consolidation within categories and among categories. The report will describe the relative size and growth rate of the categories, and discuss the consolidation fault lines.

The Changing Network Security Landscape

Chapter 1: Introduction

Chapter 2: An introduction to and overview of the landscape (the stovepipes)

- Routers
- Firewalls
- IDS
- IPS
- SEM/SIM
- Vulnerability management
- Patch management
- Network and system management

Chapter 3: A summary of the driving forces

- Network accessed applications
- Identity and Role management
- The need for broader context, integration and automation in security
- The evolution in threat sophistication and complexity
- IT service level management
 - service availability
 - change management
- Microsoft's and Cisco's directions
- Compliance
- Business justification focus

Chapter 4: Emerging Security technologies

- Network admission control
- End point security
- Anomaly detection
- Security modeling
- Security policy automation and management

Chapter 5: The current markets and players

- Cisco's Network Management and Security Directions
- Microsoft's Security Strategy
- HP's Service Desk Initiatives
- Symantec's Market Position

Chapter 6: The key near-term market shifts anticipated

Chapter 7: Market Growth forecast for the consolidated markets

Participation

NRG is soliciting charter subscriptions to the report. Charter subscribers benefit by the ability to give input on the structure and contents of the report before that fact (e.g. to assure that their critical market research questions are reasonably addressed by the work), as well as first access to the results. Please contact Peter Christy or John Katsaros (john@netsedgeonline.com) at NRG for additional details or questions.

This report is part of NRG's Information and Network Security Advisory Service – a comprehensive set of research reports and analyst advisory services aimed at improving business strategies. Future reports in the Security Advisory Service will include:

- Third Generation Vulnerability Management Systems: What's coming next, and why? How does that further tip the apple cart?
- Proactive Security Practices – How does the move to prevent attacks, minimize damage and deal with “zero day” threats change the value proposition of security offerings?
- Application Level Protection: Both the platform guys (e.g. Microsoft) and the network guys (Cisco & Juniper) think this is really important, but the way they attack the problem is completely different. How is this battle going to be joined?
- Email Anti-Abuse Systems: Network-based E-mail protection has been one of the hottest recent growth areas. Are we seeing the beginning of a tectonic shift in the email business or does Microsoft's announcement of Exchange Edge Services mean the giant is awakening to this opportunity?

Timeframe

The initial report in the Information and Network Security Advisory Service is scheduled for publication in early Q4, 2004.