



# ESG White Paper:

## Symantec and Security Best Practices

By Jon Oltsik

Senior Analyst, Information Security

July 2004

## Executive Summary

As business demands increase, the soft underbelly of today's security infrastructure is exposed leaving companies at risk. This report concludes:

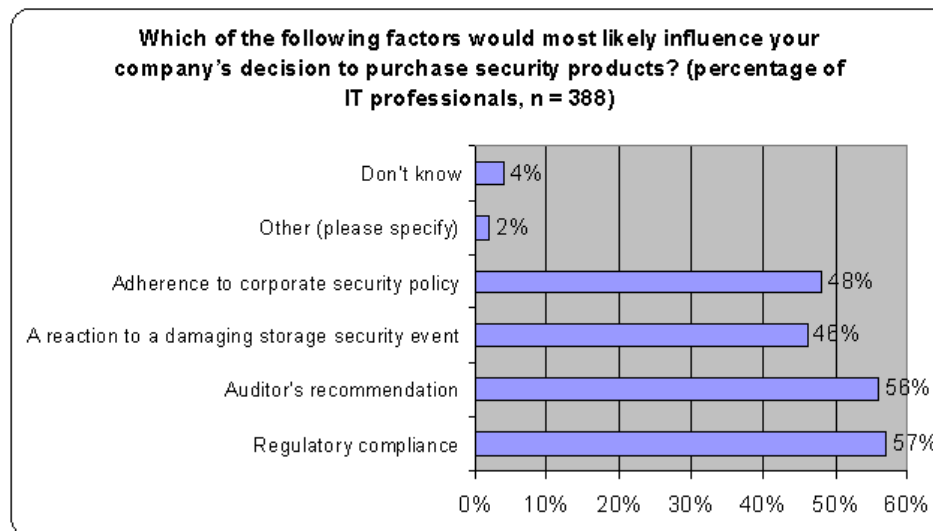
- **Today's security is broken.** To protect valuable assets against attacks, companies depend upon an assortment of security point tools, informal processes, and untrained IT and security professionals. This combination is a costly operation nightmare that leaves companies at risk with potentially devastating consequences.
- **The solution involves major changes.** In this instance, there is no quick fix. Firms need to start from the ground up by developing sound IT governance, addressing organizational weaknesses, and purchasing integrated tools from reputable vendors.
- **Symantec has the product, market leadership, and vision to help.** Symantec's combination of DeepSight Alert and Threat Management Services, Enterprise Security Manager, and On iCommand provide a comprehensive suite of security applications that meet the needs of security and IT organizations and facilitate process integration across the organization. Symantec product functionality and integration can help change from a company's security from reactive to proactive.

## Security Problems Continue To Escalate

Over the past few years, information security has become a major corporate concern from the desktop to the boardroom and CIOs consistently claim that security is one of their top priorities. This trend is underway because:

- **Danger from security events increases each year.** According to CERT, security incidents have increased more than 600% from 21,756 in 2000 to 137,529 in 2003. During this same period, reported vulnerabilities grew 346%. While the rate of vulnerabilities actually decreased by almost 8% between 2002 and 2003, this was also a timeframe featuring increasing propagation speeds and the most destructive worms and blended threats (like SQL Slammer, Blaster, and SoBig) ever. The International Computer Science Institute recently modeled a worst-case scenario of \$50 billion in lost productivity, missing data, damaged desktops and servers and repair expenses and impact at least 50 million computers.
- **Regulatory compliance demands security controls.** Government regulations like Gramm-Leach-Bliley (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley force companies to set minimum levels of security, making security a top IT priority. This trend was reflected in a recent ESG Research Report. When IT professionals were asked to identify the factors that would influence their company's decision to purchase security products, regulatory compliance was the most popular answer (see Figure 1).

Figure 1: Factors Most Likely To Influence Security Spending



- **Business demands more Internet technologies - and more security.** At the same time that threats and vulnerabilities climb, business managers are finding more and more ways to exploit the value of the Internet. Companies offshore software development to cut costs but open the network to untrusted outsiders in the process. New applications for e-commerce, CRM, and supply chain management improve productivity but also require many new servers and place mission critical information on the DMZ. Similar tradeoffs between Internet-drive business opportunities and security risks have become a daily reality. Thus information systems security is becoming more critical issue for business continuity.

Executive managers are beginning to understand the business risks of poor security and are more willing to spend accordingly to alleviate these risks. Most enterprise companies spend 5% to 10% of their IT budget on security today and this percentage grows annually. ESG estimates that companies spent over \$25 billion in 2003 for security products and services growing to over \$32 billion by the end of 2004.

## Today's Security Depends on a Potpourri of Products and Processes

In spite of the rise in spending however, security challenges continue to overburden security and IT executives. The rate of incidents, number of vulnerabilities, and new advanced attack methods place the security team in constant firefighting mode. In a recent interview with ESG, one Chief Information Security Officer (CISO) summarized the overwhelming nature of the security problem as follows:

"It's difficult to get ahead of the scope of information security. This year we are working on securing our internal networks to deal with Internet worms. Next year we will begin an initiative to secure our data. In the meantime we're dealing with wireless security, sophisticated hackers, DOS attacks, and SPAM. The CEO is very supportive but the list keeps getting bigger and bigger." (Financial Services Company)

To detect, prevent, and react to security events, companies rely on a combination of point tools, public domain information, loosely defined controls, and manual processes. These include:

- **Employing firewall and IDS devices at the network perimeter.** Firewalls and IDS devices serve as the border patrol between the lawless Internet and protected corporate networks. Firewall rules provide a defense against static attacks while IDS devices monitor traffic for known attack patterns or behavior anomalies.
- **Depending upon antivirus solutions at the desktop.** Firms employ antivirus software on each desktop to scan disk drives and filter e-mail attachments for any known or potential viruses.
- **Monitoring security organizations and vendors to gauge impending problems.** Many companies depend upon web sites like CERT, bugtraq, and seclist.org to track threats and vulnerabilities. Security analysts labor through these sites for useful information, creating reports, and reacting to information.
- **Configuring and auditing systems.** Complying with regulations and internal policies is dependent upon many laborious efforts like creating consistent releases, configurations, and changes then auditing systems for conformity.
- **Collaboration between security and IT operations teams.** Ultimately, security depends upon harmony and cooperation between security and IT operations teams. Security groups are responsible for setting policies and monitoring status but IT operations is responsible for making changes that secure critical assets.

## Today's Security Approach Is Badly Broken

Disparate security tools and processes were sufficient when the Internet was used primarily for web surfing but this is no longer the case. Current security is insufficient because (see Figure 2):

- **Firewall and IDSs present a myopic view.** Firewalls are only as good as their rule set and can't protect against new forms of attack. IDSs can help against current attacks but these systems can be overly chatty masking real threats with extraneous data. Finally, both firewalls and IDS log files can be useful but present specific company threats only with no visibility into attacks in the wild.
- **Client protection needs more proactive approach, and client compliancy.** Antivirus software provides a good first level of defense but depends upon employees constantly updating their virus signatures - a difficult task for casual and remote users. In today's climate of rapid worm propagation, antivirus software must also be supplemented with an a management system that track each PC for configuration and patch level information so that IT operations knows which desktops need immediate attention when the next destructive attack occurs.
- **Security exposure demands real-time awareness.** Security organization web sites are rich in information but finding, consuming, and interpreting this data is time-consuming slog for security analysts burdened with a multitude of other tasks. Any pertinent information that is missed or ignored can lead to dire consequences.
- **Manual compliance methods aren't timely or thorough enough.** Developing a methodology for corporate policies or government regulations can take months to flesh out and require professional services help. Once in place, keeping up with compliance means tracking changes, scanning vulnerabilities, and managing configurations. Again, any mistake can have devastating results.
- **Security and IT operations groups struggle with process and workload problems.** Security and IT operations groups are often at odds on a daily basis. IT Ops groups may disregard security in favor of other tasks putting assets at risk. Security staff has been known to circumvent IT operations by patching devices themselves, only to have systems crash due to incompatible software issues.

Figure 2: Today's Security Is Badly Broken

Security tactic:	Function:	Weakness:
Firewall and IDS	Detect and prevent attacks	<ol style="list-style-type: none"> <li>1. Dependent upon firewall rules</li> <li>2. IDS chattiness may mask attacks</li> <li>3. Internal view only</li> </ol>
Scan security sites	Research vulnerabilities and threats	<ol style="list-style-type: none"> <li>1. Dependent upon time consuming process and analysis</li> <li>2. May miss real-time threats</li> </ol>
Manual compliance methods	Develop compliance model and audit methodology	<ol style="list-style-type: none"> <li>1. Dependent upon time consuming process and analysis</li> <li>2. Can't keep up with requirements</li> </ol>
Coordination between security and IT	Communicate and execute security changes to IT infrastructure	<ol style="list-style-type: none"> <li>1. Report to two organizations</li> <li>2. Different goals and motivation</li> <li>3. Lack of communication or process integration</li> </ol>

## Enterprise Companies Need a New Security Model

In today's Internet-connected global business world, security-related downtime can mean millions of dollars in lost revenue per minute, compliance violations, liability issues, and a PR nightmare. Security is especially important today given the frequency, propagation rates and severity of attacks. The lag time between vulnerability discovery and attack continues to shrink and the risk of a zero-day attack is becoming a real possibility.

These type of risks require a new security model that provides:

- **Proactive threat and vulnerability information.** Rather than depending upon security administrators sifting through mountains of security data, an enterprise company need proactive and comprehensive security information that details threats and vulnerabilities and is customized to their specific profile. To ensure protection, a federal agency needs to know about attack vectors 1) targeting other government departments, 2) emanating from hostile countries, and 3) focused on specific systems. Armed with this knowledge, security and IT can take the proper upfront steps.
- **Automated policy creation and auditing.** Companies need the ability to customize policies or apply standard templates for regulatory compliance like GLBA and HIPAA across all systems. They also need the ability to automate system monitoring to enable frequent system audits. When Microsoft announces a critical alert, security executives need to be able to query configuration databases to see which systems are vulnerable so they can plan their remediation process without delay.
- **Integrated and routine workflow between security and IT.** With proactive security and policy information in hand, security teams need remediation help from IT operations for activities like configuration and patch management. If the operations group depends upon manual processes and 'sneakernet' to complete these tasks however, they will remain a perpetual bottleneck. IT operations needs provisioning, configuration, and asset management tools to automate these critical tasks.

## The Right Mix: People, Process, and Technology

Although there are many leading technology products to help companies achieve their security goals, technology alone provides limited benefits. To maximize security protection what's needed here is the right mix of people processes and technology improvements. (see Figure 3).

### Start by Establishing the Right Processes

ESG believes that security protection depends upon the right foundation of sound policies and processes. This means that companies must:

- **Implement standard IT governance.** Approximately 78% of downtime can be attributed to changes made internally by someone with access and authority. These problems can be further traced to snafus like non-standard configurations, undocumented changes, or inappropriate patches. To alleviate these issues, ESG believes that companies should take a bottom-up approach to security management starting with strong IT governance (see Figure 4). The IT Infrastructure Library (ITIL) and IT Service Management (ITSM) are a good fit as they stress documented standards for change management, release management, configuration management, and problem resolution. ITIL and similar models can also help companies lower operating costs.

Figure 3: The Right Mix


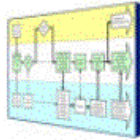

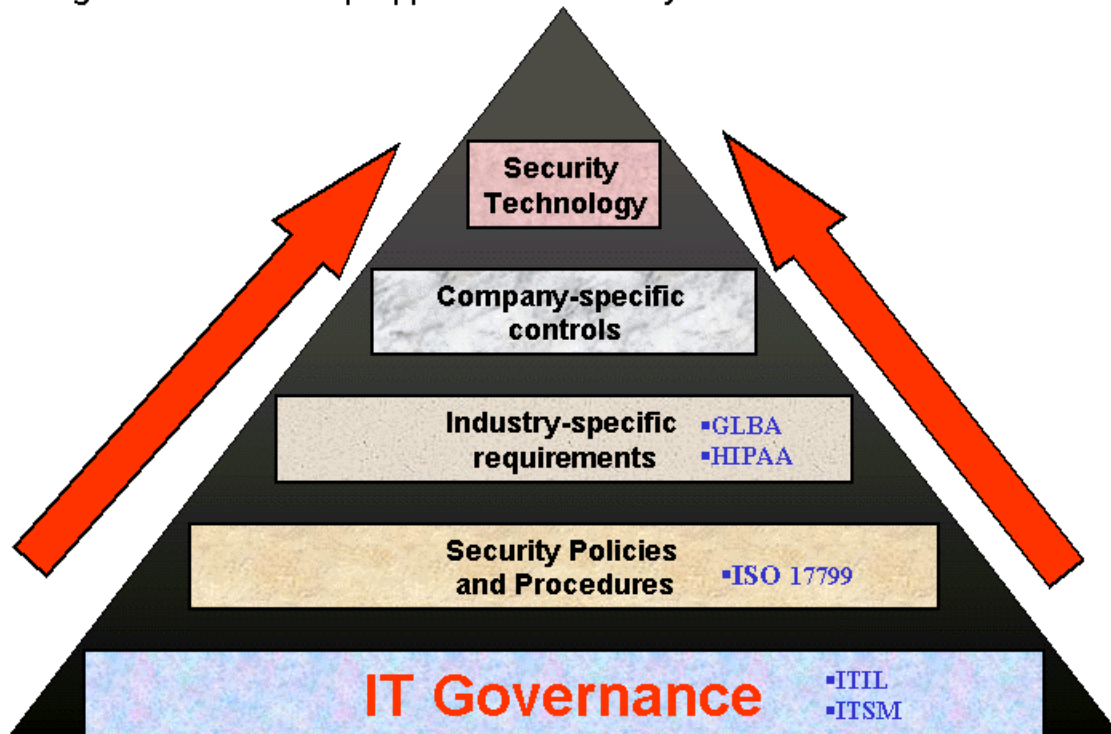
	<p><b>People</b></p> <ul style="list-style-type: none"> <li>✓ Dedicate a clear chain of command</li> <li>✓ Cross train security and IT teams</li> <li>✓ Set up communication channels</li> <li>✓ Develop ways to motivate staff</li> </ul>
	<p><b>Process</b></p> <ul style="list-style-type: none"> <li>✓ Implement IT governance standards</li> <li>✓ Create secure baseline configurations</li> <li>✓ Institute and IR methodology</li> <li>✓ Test, measure, and monitor</li> </ul>
	<p><b>Technology</b></p> <ul style="list-style-type: none"> <li>✓ Select an integrated security suite</li> </ul>

Figure 4: A Bottom Up Approach To Security Starts With IT Governance



- **Create secure baseline configurations.** Before any piece of equipment becomes part of the IT infrastructure, it must be hardened with a standard secure configuration. For example, each Windows server should be implemented with all unnecessary TCP services disabled, limited file shares, and no guest accounts. Once standard settings are established, all additional systems should be provisioned in an identical state. These steps will improve initial security while limiting risky one-off configurations down the line.
- **Institute a standard incident response methodology.** History proves that even companies with strong security are attacked and compromised so every company needs a formal Incident Response (IR) plan. IR activity starts with the creation of a matrix that defines specific security incidents and maps them to an appropriate set of responses. The matrix defines processes like when to alert business managers and users, which devices to disconnect from the network, remediation steps including disaster recovery and the responsibilities of security and IT operations teams. The goal is to have a detailed plan in place to address incidents quickly, limit problems to network segments and minimize any business interruption. Once incidents are addressed, IR should continue with forensic investigations and process improvement.
- **Test, monitor and measure.** No process is complete without the right metrics for assessing performance and creating ways for improvement. Security processes must measure metrics like Mean Time Between Failure (MTBF), Mean Time To Repair (MTBF), and Time To Respond (TTR). These metrics should be reviewed after each incident to determine process breakdowns, bottlenecks, and areas for improvement. By tracking trends over time, companies can judge progress and pinpoint troublesome trends.

## Ensuring the Right Skills Set and Organization

Just as people are the biggest security risk, the security and IT staff make up the last line of defense. If they are ill prepared or can't work together, the whole organization can suffer. To alleviate this circumstance, enterprises should:

- **Dedicate a clear chain of command.** When the directors of security and IT management report to different bosses with different goals, there are bound to be some security holes. To avoid this, companies should appoint a Chief Information Security Officer (CISO) or Chief Risk Officer (CRO) responsible for developing policies, coordinating administration, and introducing a model for technical support. When it comes to security execution, executive management must identify this person as the ultimate authority and empower them to get the job done.
- **Cross train personnel on processes and skills.** As companies implement IT governance, all IT and security personnel must be required to participate in training and be tested to judge their aptitude. In addition, security and IT operations staff must receive cross training in each other's respective areas. Savvy companies will rotate staff back and forth to provide 'real-world' experience creating a stronger bond between the groups, spreading knowledge and instituting a dialogue for process improvement.
- **Set up communication channels.** Security depends upon strong communications between all involved constituencies. To facilitate this, CISOs should establish regularly scheduled meetings between security and IT groups with a common agenda, metrics, and standard reports. Communication processes must also be introduced into the IR process so security and IT teams know how to proceed when an attack is in progress. Finally, communications should include business managers who may not require technical details but certainly need to remain in the loop.
- **Develop ways to motivate staff.** While all employees should have a vested interest in security, new processes and tasks may seem like additional work to over-worked staff. Smart executives will recognize this and make sure that security progress is rewarded with compensation bonuses, public recognition, and other attractive incentives.

## Select an Integrated Product Suite

The current mix of security point tools results in an operational burden and leave too many security holes wide open. ESG believes that it is time for companies to develop migration plans away from legacy 'best-of-breed' security tools in favor of integrated solutions.

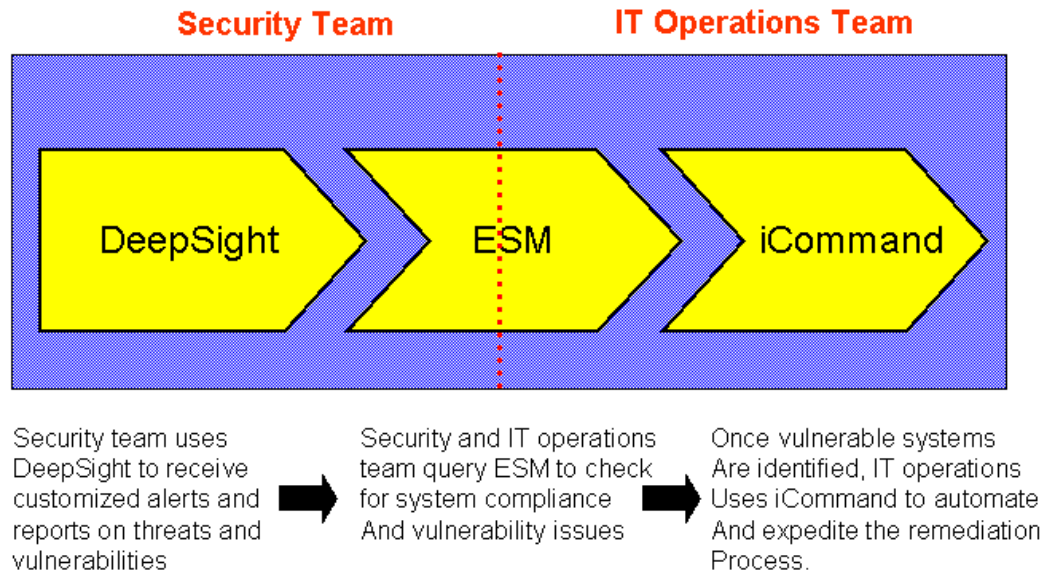
Symantec Corporation offers a portfolio of enterprise-class products that fit this model. Symantec offerings include:

- **DeepSight Threat Management System and Alert Services.** DeepSight Threat Management System is a web-based early warning system that continuously aggregates and correlates attack data from over 20,000 sensors in over 180 countries giving insight into the active threats in Internet. DeepSight Alert Services provides organizations with intelligence on emerging vulnerabilities and malicious code. Currently Alert Services monitors 18,000 distinct technologies, operating systems, and application software product versions of 4,200 products from 2,200 vendors by tracking information from over 150 authoritative sources. Companies use these services to keep up to date on threats and vulnerabilities so they can plan to mitigate risks from future attacks or take immediate actions on newly found worms.
- **Symantec Enterprise Security Manager (ESM).** ESM automatically evaluates critical business delivery systems including servers, applications, networks, and security controls to ensure that they are configured and being used in accordance with established policies. ESM enables security and IT groups to create their own policies for internal control or select one of the preconfigured compliance templates for regulations like HIPAA, GLBA, or Sarbanes-Oxley compliance. The system performs more than 2,500 security checks automatically across Windows, UNIX, Linux, AS/400, NetWare, and VMS Systems. ESM allows companies to effectively manage business risks by identifying threats and measuring compliance to operational security practices while reducing administration costs and increasing productivity.
- **On iCommand.** On iCommand is an IT operations management application that centralizes activities like installation design, software provisioning and delivery, patch management, help desk operations, asset management, and disaster recovery. By centralizing and automating these tasks, On iCommand eliminates the need for manual processes and allows IT operations to quickly address imminent threats and open vulnerabilities. When the security manager mandates that all desktop systems receive a patch ASAP, On iCommand can turn this job around in hours - not days.

Combined with people and process improvements, Symantec's leading products can provide a high level of protection and facilitate process integration for companies of all sizes (see Figure 5). Along with Symantec's Security Management System, this process can be completed with the addition of an Information Management Solution and Incident Response system. Symantec Incident Manager correlates security events from a wide variety of sources into actionable security incidents, which can be escalated into BMC Remedy™ trouble ticket system and tracked in HP Openview Operations™.

In this way, Symantec's integrated suite would eliminate many of today's security pitfalls by reducing security resources, operations, and expenses while improving timeliness and overall security.

Figure 5: Symantec Product Suite And Security Processes



## Bottom Line

Security circa 2000 is no longer appropriate as it has become too costly and ineffective. There are no band aid solutions here, what's needed is a complete overhaul that demands, organizational adjustments, strict IT governance, and integrated technology tools. Once companies establish a foundation of strong processes accompanied by training, they can look to Symantec to provide a solid offering of technology that spans security and IT requirements.



20 Asylum Street  
Milford, MA 01757  
Tel: 508-482-0188  
Fax: 508-482-0218

[www.enterprisestrategygroup.com](http://www.enterprisestrategygroup.com)