IDC
Analyze the Future

WHITE PAPER

Containing Vendor Sprawl: Improve Security, Reduce Risk, and Lower Cost

Sponsored by: Symantec

Andrew J. Hanson Christian A. Christiansen

May 2009

IDC OPINION

Businesses are forced to integrate new applications on a regular basis. The cost of installing and integrating each new application has significantly declined in the past decade, but businesses still underestimate the cost of managing a heterogeneous environment. Although many look at immediate system integration and short-term fixes as a way to reduce time to deployment and overall cost, system integration is not the gift that keeps on giving; instead, it is the sin that keeps on punishing. IT departments that turn to a single vendor for integrated solutions that provide security, system, and storage capabilities have experienced a reduction in vendor sprawl within their architecture. Consequently, they have significantly reduced system complexity.

Key points of this white paper include:

- Integration costs, which include both year zero installation and continued operational expenses, can be as much as 40x each application's initial cost (e.g., software license and/or appliance) over the life span of a typical application.
- Mixed-vendor environments can cost 4x as much as a single-vendor environment on an annual basis.
- Integration of security, system, and storage management into a comprehensive solution from a single vendor lessens the burden placed on IT departments by significantly reducing time and cost to deploy new applications and maintain the system.
- Consolidating security, system, and storage management on an integrated console improves corporate risk posture and reduces the system vulnerabilities that are created by gaps that occur in customized solutions.

METHODOLOGY

IDC developed this white paper using existing market forecasts and direct, in-depth primary research. To gain insight into the needs of businesses and how such needs are being met by Symantec's security portfolio, IDC conducted interviews with IT executives at companies of various sizes in several industry sectors. Additionally, IDC met with representatives from Symantec to review their goals and tactics. This white paper uses all of these research perspectives to create a practical view of issues facing security and IT administrators and how Symantec's approach can provide a solution.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

IN THIS WHITE PAPER

In this white paper, IDC analyzes the benefits of reducing vendor sprawl associated with security, storage, and system management solutions. Corporate IT systems have grown extremely complex as point products are frequently integrated to address an acute security, system, or storage issue. The short-term integration strategies that tie each product into the overall system architecture save money and network downtime in the near future, but actually result in increased costs over the life of the system. This paper discusses the mounting need for solutions that integrate security, system, and storage management (3S).

SITUATION OVERVIEW

Enterprises worldwide embrace advances in information technology to improve their business. The growing capabilities available on the Internet empower businesses to reduce costs and improve profit opportunities by utilizing ecommerce, Web 2.0, and an increasingly mobile, always-connected workforce. However, as administrators open their systems to the innovative technologies and applications that are available, they find it difficult to cope with the system and security complexities that come with them.

To address the growing complexities, IT organizations have integrated point products by moving to single-vendor product suites, cautiously integrating selected multivendor environments with a common management console or focusing on parts of the problem such as system and storage management. These limited function solutions are pulled from a wide range of vendors, creating a heterogeneous environment that must be customized to function seamlessly. Every time a new application is introduced to the system architecture, both the system and the application must be adjusted to function properly with other processes and different vendors. In larger enterprises, system integration is often necessary to address unique system requirements, compliance regulations, or competitive differentiation.

The Cost of Integration

When examining the total cost of a new application, businesses must consider the system integration multiple, which is a comparison of the purchase price of a product and the system integration cost. This number varies considerably depending on security technology, administrative expertise, sophistication of the system integrator, desired level of integration, and customer size.

In the 1990s, the system integration multiple averaged 7–10x, meaning that for every $1 spent on a new product, between $7 and $10 was spent on customized solutions that integrated it into the existing system architecture. However, the cost has come down significantly in the past decade and is now generally estimated at approximately 3–5x.

At face value, this has been an acceptable cost for integration of point products from various vendors into a heterogeneous environment, given that the alternative of overhauling the entire system and implementing an entirely new architecture seemed unreasonable, demanding high investment and significant system downtime.

Customer Perception

However, the integration costs discussed earlier fail to recognize the true costs over the entire life of the system. As some CIOs have pointed out, the purchase and initial installation costs are only part of the story. One CIO who spoke with IDC emphasized that to calculate the true cost of integration, the entire life cycle of an enterprise application must be taken into account. She also said that integration really means customization. Finally, she pointed out that getting to a single vendor is ideal, but it is currently impossible. Instead, businesses can benefit from reducing the number of vendors in their environment to a small number of closely associated partners, which will significantly reduce system integration requirements.

Life-Cycle Integration

An enterprise application can have a life span as long as 20 years, with new releases every two to three years. Each time a new release is deployed, the customization that was necessary to integrate the application into the heterogeneous environment runs the risk of failing and must be recreated for the new release to function properly. This means partial to full repetition of the system integration and customization process. The 3–5x estimate for integration costs applies only to year zero — simply an installation fee. For a 5- to 20-year life cycle, the integration cost becomes an operational expense that repeats every two to three years for each application. Based on numerous conversations with IT administrators, IDC estimates that the true integration cost for a single application over the life span of a system is as much as 30–40x the cost of the original security products. This price grows exponentially as disparate point products from a variety of vendors with their own update releases are integrated into the environment. Vendor sprawl and the costs associated with integration are draining IT budgets and administrators' time.

Annual Costs

In addition to the system integration costs caused by the initial deployment and each subsequent update release, annual costs are associated with operating an integrated system. Integrated applications will operate together on the system, but they will still have different administration requirements, command consoles, and reporting mechanisms. Each application will require different skills and knowledge to operate the control interfaces, command structures, and data interpretation, among other issues. On a superficial but irritating level, different applications will likely use different nomenclature for the same term, consequently increasing the training costs and likely contributing to mistaken interpretations or failure to recognize similar vulnerabilities and attacks across multiple systems.

All these issues make correlation among integrated applications more difficult. Beyond the cost due to extra training and operational costs associated with management, they may cause administrators to miss attacks or relegate attacks to a minor status.

Perfect Storm

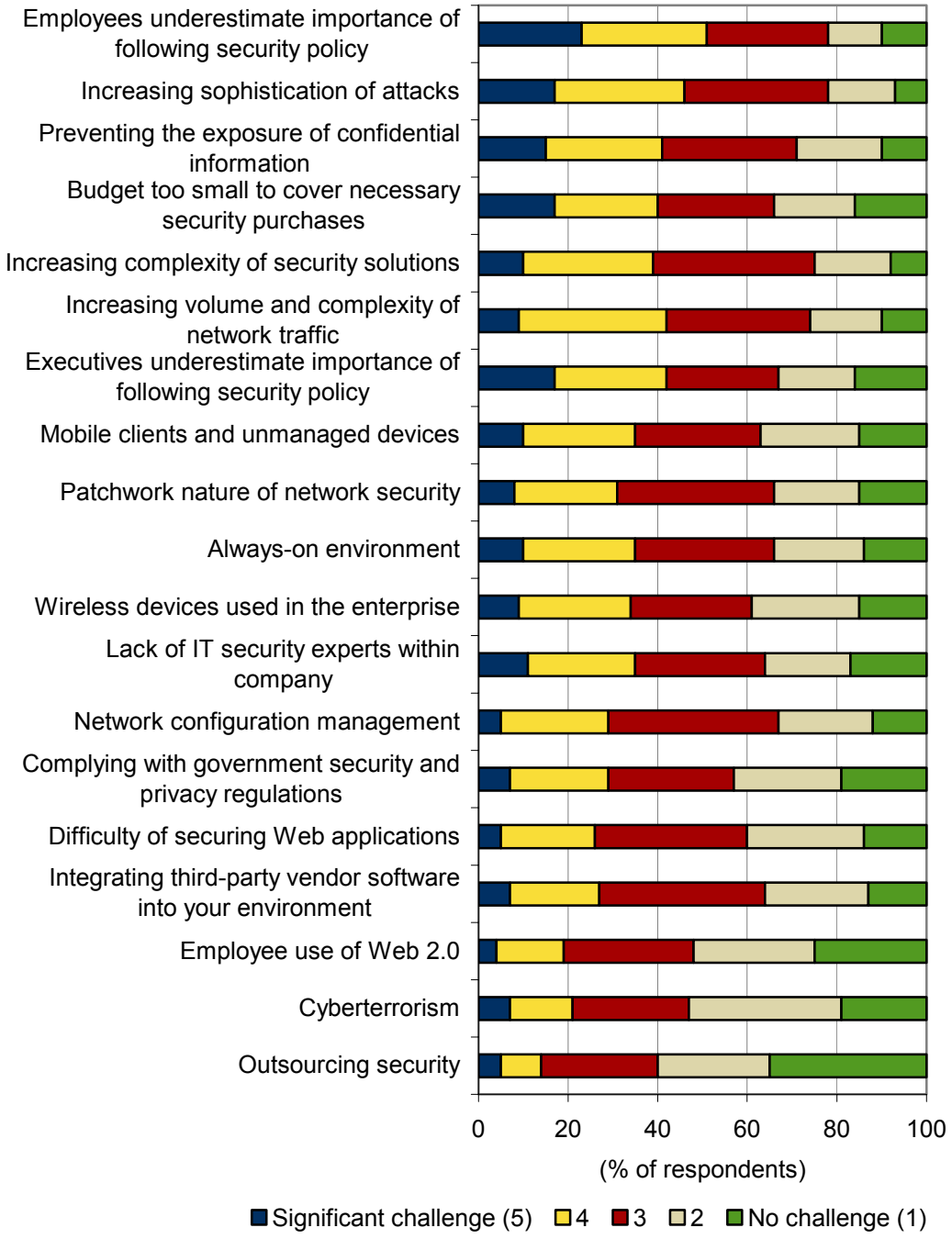
This integration challenge is compounded by powerful forces in the market that have collided at an opportune moment to create nightmarish conditions for system administrators. The threat landscape is growing at an alarming rate, creating the need to incorporate even more solutions that address key pain points in the system. As the worldwide economy has migrated to the Internet, criminals have followed suit. Today, thousands of viruses are released worldwide on a daily basis that are designed

to produce the most efficient financial gain, discretely stealing sensitive data and critical business information.

Figure 1 shows the top challenges to enterprise security over the next 12 months, according to IDC's 2008 *Enterprise Security Survey*.

FIGURE 1

Top Security Challenges in the Next 12 Months



Source: IDC's *Enterprise Security Survey*, 2008

Worldwide Economic Trouble

After struggling but limping along in 2008, the worldwide economy suffered a series of severe setbacks at the end of the year and into the beginning of 2009. As heads of state, economists, and business leaders worldwide strive to rectify the situation, the global economy continues on unsteady legs. As the downturn continues with no end in sight, businesses are caught in a perfect storm of danger that combines reduced resources to commit to security, increased threats, and growing system complexities.

Growing Threat Landscape

The threat landscape is gaining an advantage amid the turmoil due to increasing personnel layoffs and reductions in budgets that are straining the ability of IT administrators to properly configure and manage corporate systems. IDC tracks vendor revenue and customer spending trends across a wide range of technologies as budgets are reduced and key purchases must be prioritized. IDC has concluded that, although not invincible, security spending will not suffer significantly, relative to other major technology areas. Companies worldwide recognize the necessity of maintaining a strong security posture in turbulent times, but new projects may be delayed without proof of immediate relevance. However, as companies continue to spend on security technology, it is likely that IT departments will not be sheltered from companywide layoffs. This means that IT personnel will be forced to face a looming threat environment with fewer people. In many cases, such as SMBs and branch offices, there may have been designated employees for different sectors of the IT department, but they will be aggregated into a single area. Administrators who were previously tasked with a narrow area of concentration will now be required to manage a variety of functions.

Internal Threat and Data Loss Prevention

The danger of employees intentionally stealing valuable and sensitive information is expected to increase as trusted employees brace for layoffs. The state of the economy has caused people, who in any other circumstances would be reliable and critical personnel, to consider illegal actions, such as stealing confidential information. With increasing layoffs, security administrators are responsible for restricting access privileges for all terminated employees immediately. When larger companies are cutting hundreds or thousands of employees across various departments and at different levels of the company, administrators are faced with a heavy burden.

Data loss prevention (DLP) and identity and access management, along with logging and security information and event management (SIEM), are increasingly important in this environment. Such capabilities go well beyond basic security needs that lock down the system from the evolving threat landscape and will require many IT departments that are already struggling to adjust to current conditions to take a new look at their security and systems architecture.

Example Incidents

The situation described in this document has created a series of common cases that call for a change in security and systems architecture.

Case 1: Employee Information Rights

A trusted employee is preparing to leave a company in the near future, whether by choice or because he or she expects to be included in the next round of layoffs. Consequently, the employee has decided to download sensitive information, including data on current projects, trade secrets, company information, customer contacts and details, and ideas for the future. Such information would put the former employee in a good position to solicit a competitor or underbid his or her previous employer with clients. Many options exist for extracting sensitive information, such as media devices with large storage capabilities, USB storage devices, PDAs and smartphones, digital cameras, and Web-based email.

The company is responsible for preventing the employee from accessing and downloading sensitive data, which means that it is crucial for administrators to be able to control the access privileges and device usage of employees. DLP policies and technologies empower administrators to control inbound and outbound transit of critical resources. It is important for companies to control how their information is moved, what types of devices are allowed into corporate systems, and who has privileged access. Most importantly, DLP can go beyond simply preventing information loss: In the event that information is removed from the system, DLP solutions can provide logging and reporting features that identify the user and provide details on what information was removed, when it was taken, and how it was extracted from the corporate system. These forensic capabilities will provide businesses with a great advantage in recovering from the loss of critical data as well as any legal actions that need to follow.

Case 2: IT Freezes New Purchases

To decrease spending and reduce overall budgets, many companies have decided to limit or completely freeze PC replacements. From a hardware perspective, companies can realize considerable cost savings by doing so: If PCs are replaced on a three-year cycle, companies are committed to replacing 33% of their computers every year. By reducing the replacement cycle or canceling it altogether, businesses have decreased spending but have left their employees with older machines that may not be able to support software updates. Essential budget cuts, which come from the executive level, are leaving employees struggling to use lagging machines and IT departments working to keep them running efficiently. Security solutions are a primary concern on older computers because many virus scans hog system resources.

Many companies that are decreasing costs by freezing PC replacements are investing in new security architectures that employ lightweight endpoint clients to improve system performance on older computers. By standardizing on a common, lightweight endpoint solution, IT administrators are able to improve performance and simplify maintenance and support obligations.

Case 3: Budget Cuts

The economic downturn has caused businesses to reanalyze their expenditures, and the goal is to cut costs wherever possible. Senior management in businesses around the world is cutting budgets and demanding lower capital and operating expenditures. However, senior management also expects IT administrators to reduce corporate risk.

For several years, IDC has asked security administrators what they would do with reduced budgets, and the number 1 answer has not changed in the face of a declining economy: conduct risk assessment and prioritize needs. As a result of reduced budgets, administrators must assign risk ratios to servers, applications, and data based on vulnerabilities and the criticality of each asset. They must analyze the importance of each asset, the danger it faces, the likelihood of a vulnerability being exploited, the cost to address the risk, and the cost that would result from an exploit. These issues must be weighed against each other as administrators look to lower expenses.

Vulnerability assessment solutions with logging capabilities can analyze a company's IT architecture and assign tolerable risk ratios associated with each asset. This will give administrators a clear picture of the priorities within their system. Compliance management solutions provide risk scoring in terms of sensitivity to failure and the costs associated with failure. Finally, SIEM products will provide the ability to track, monitor, and control the architecture in a fashion that will allow for future adjustments. By deploying these solutions in a SaaS model, companies can further reduce capex and opex while maintaining investment in security and IT personnel.

FUTURE OUTLOOK

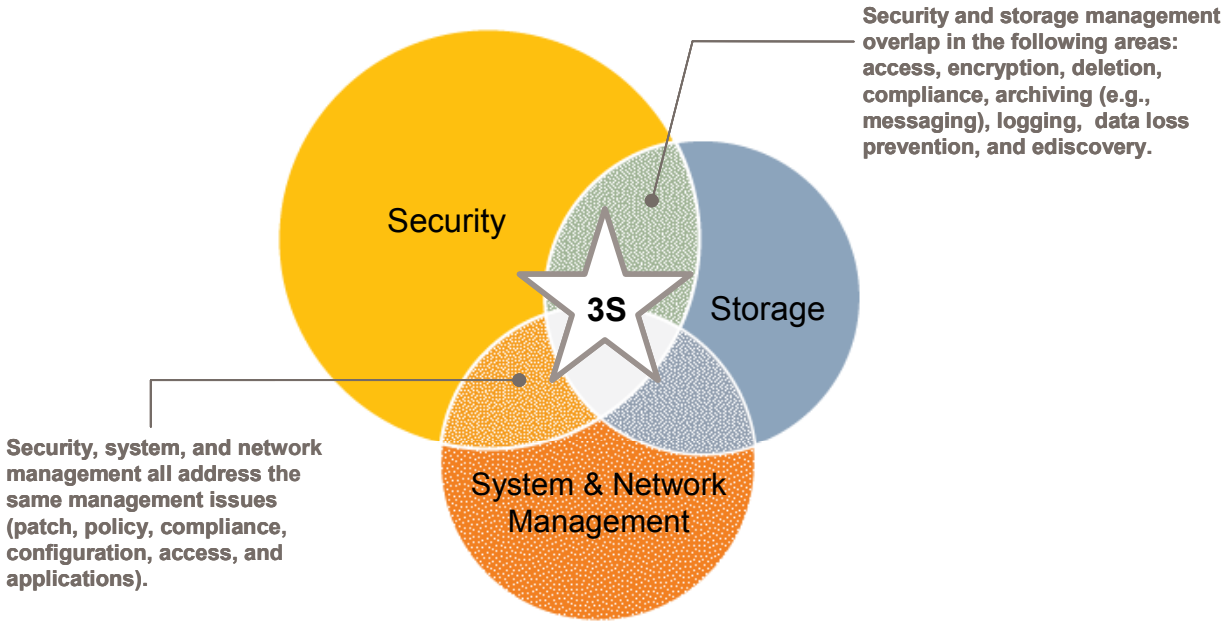
3S: Integration of Security, System, and Storage Management to Reduce Vendor Sprawl

As the threats to enterprises increase and the budgets for managing corporate systems decrease due to the economy, IT departments are forced to do more with less. They are turning to suites that leverage a broad range of capabilities in an integrated package. The overlap of security, system, and storage management products, which is epitomized by the quote "A well-managed endpoint is a secure endpoint," is already evident and will continue to grow in the future.

The integration of security, system, and storage management, or 3S, into a comprehensive solution from a single vendor provides enhancements to each of the areas (see Figure 2). Seamless integration reduces vulnerabilities, improves system function and efficiency, and increases visibility into sensitive information that is stored on the system.

FIGURE 2

3S Convergence



Source: IDC, 2009

The integration of these segments into a 3S solution from a single vendor provides numerous business enablement features by creating a stable and controlled environment on the endpoint:

- Simplified management by converging security management, system/endpoint management, and storage management capabilities into a centralized platform that enforces client policies for all three disciplines
- Consistent control across a variety of devices in any size deployment (Integrating security and storage provides critical archiving, logging, and ediscovery capabilities that are important for sensitive resources as well as for compliance audits.)
- Application and configuration control issues that are being addressed by independent security and management suites and can be simplified on a single platform
- Access control and visibility into managed and unmanaged devices attempting to connect to the corporate network
- Integrated inbound and outbound messaging protection
- Comprehensive system and security backup, recovery, event management, and logging

Most importantly, 3S solutions directly negate the 40x cost of integration that was discussed earlier. By leveraging strategic vendor relationships and streamlining product integration and functionality on a single platform with one vendor, 3S solutions avoid the need for customization to make products function properly in the overall architecture. Patch management and updates for security and other applications are controlled and coordinated by a single source, which means fewer complications and no need for customization by IT administrators. Therefore, upgrades to each component will occur at the same time in an efficient fashion, reducing the time to deploy changes.

Essential Guidance for Vendors

Key issues that 3S vendors must take into account are the following:

- Security should provide business enablement, which is especially important during these economic times.
- Security professionals will also be looking toward security solutions that provide preventative security instead of reactive security. Because companies have less staff and less time to deal with repairing security problems, security solutions must be able to be set and offer high levels of effectiveness without being constantly maintained.
- Extending PC amortization pleases finance people.
- Lightweight security clients lessen the need for PC replacement.