Bitdefender®

IT Security: Creating Heroes Instead of Headaches

In This Paper

- Organizations using legacy security systems suffer from high costs, increased risk and a competitive disadvantage
- Modern IT security systems can become proactive business enablers rather than reactive systems
- Upgrading IT security systems requires investment, but for many organizations the cost of inaction is even higher

a QuinStreet Executive Brief. © 2014

CIO INSIGHT

Executive Brief

Introduction

IT security is in the spotlight as never before, and for good reason:

- Damaging data breaches of high-profile companies — including Sony, eBay, Target, Home Depot, and Anthem — are in the news on a regular basis.

- The average cost to a company for a data breach in 2014 was $3.5 million, up 15 percent from the prior year.[i]

- New threats are emerging at the astonishing rate of 390,000 per day.[ii]

In light of this steady flow of headlines and drama, focus needs to shift toward proactively solving the problem in a way that security becomes a business enabler. Organizations strapped with legacy systems and long-standing license agreements can find themselves at a disadvantage in more ways than one.

Costs: Legacy systems need just as much, if not better, protection. Take the cost of protecting both legacy and modern datacenter infrastructures, add to this the management costs across both, and security can quickly become a cost and management nightmare. Trying to "bolt on" traditional security is unwise, as these solutions were not built for virtual environments. Many businesses will consider the cost of upgrading or replacing their existing security systems to be prohibitive. But in fact, the cost can be greater if the existing, "traditional" solutions create too many failure points — due to the technology itself, the management of the solution, or the ability to scale as the datacenter changes and evolves (which it likely will).

Risks: Organizations may express concern over the risk that comes with change — of systems, applications, or processes. All of these can be useful and help increase productivity and profitability, but there is an inherent cost. There may also be mistrust of newer, more innovative approaches to doing business (or securing that business). Why? Because organizations are almost all playing "catch-up" to the rapid growth and change taking place all around us — witness the advances in cloud computing, virtualization and mobility.

Competitive race: Customer experience has changed dramatically in a very short period of time. The focus for many organizations is, first and foremost, to support and enhance the customer experience. In the race to always be better and faster in responding to customer needs (often through IT innovation), many companies will struggle to keep up on the security side if they are relying on traditional security solutions.

Cost, Risk, and Competition: these are just a few of the challenges to be considered when approaching an overall IT strategy (which must include security). Overcoming these challenges is a matter of choosing a security solution that straddles the gap, provides the highest protection possible, and helps organizations move into the next generation — enabling the business to grow and serve the needs of customers (both internal and external).

There are three primary ways in which modern IT security solutions can become proactive business enablers, rather than solely reactive defenders.

Business Enabler No. 1: Reduced Risk

When business leaders think about IT security, they don't think in terms of firewalls and intrusion detection; they think in terms of business risk. The costs of a data breach can be staggering, not only in terms of dollars spent in reparations, but also in terms of brand perception and market valuation. A data breach tarnishes the image of a company and can affect revenue for an extended period of time.

For these reasons, CEOs want to have the best protection available, and "good enough" is no longer good enough.

With every high-profile corporate breach that we hear about, it becomes more evident that organizations cannot depend on out-dated security technology designed for the datacenters of the past. Relying on traditional solutions can be the difference between success and failure in keeping the company safe from attack, and keeping the brand reputation intact.

Reducing risk means that the security solution must, as much as possible, be innovative enough to close the protection gap between legacy and new datacenter solutions. Such solutions remove multiple points of potential failure, including common points of failure like AV storms and boot-time security gaps. They prevent security management, and therefore policy, from being spread across disparate consoles, as well as ensuring scalability, flexibility, and high-availability of management and protection mechanisms.

Business Enabler No. 2: Ease of Management

Many legacy security environments are cobbled together from point solutions, either due to mergers and acquisitions, preferred vendors of former staff, or due to organic growth and piecemeal adoption of different security technologies. Such heterogeneous environments are often inefficient in terms of both protection and management capabilities.

Modern IT security platforms can provide multiple levels of security, including the protection of physical endpoints, virtual endpoints and mobile devices. Current methods of protection can also harness the power of cloud computing, removing the headache of hosting and maintaining the hardware (for both workloads and/or security management). Organizations should look for security vendors that can secure across these multiple device types, as well as work across virtualization platforms and operating systems, and provide centralized management for it all. This alone is a significant business enabler because it gives IT managers a single view and a single console to set policies, freeing the security team and IT admins to deal with other tasks. The cost savings, management improvements, and advantages in policy management are realized when internal groups no longer struggle with patch-work security for endpoints.

Business Enabler No. 3: Cost Reduction

A security strategy that gives resources back to the business will always earn the respect of any CEO and the board.

At the nuts-and-bolts level of IT security, any strategy that can reduce costs without compromising quality is a plus. Unified security solutions consume fewer resources (i.e., fewer hours and less money) around installation, training and management. This means more resources (human and capital) can be directed at business goals.

Organizations should seek out security vendors that offload security functions to a central appliance, as this eliminates duplication of processing functions, scanning, etc. Centralizing these operations (rather than deploying an agent on every machine) results in higher consolidation ratios, fewer hardware resources and simplified management. This avoids redundancy of processing power (CPU, RAM), storage impact and network load, significantly reducing costs.

When security is not viewed as a 'hampering' technology, but rather a 'helping' technology, especially in a modern datacenter — it's a win-win for all.

The Price of Complacency

Deploying new security technology obviously carries a cost in terms of both budget and time for implementation and training. However, a careful examination of the big picture will often prove that the cost of not implementing such technology can be even higher.

Budget issues: Given the reality of existing contracts and limited budgets, moving to a new solution may not make financial sense from the limited perspective of one department and one line item. However, it may offer a more attractive ROI when the total IT budget is taken into account. The higher consolidation ratios and increased performance benefits can justify the cost of implementation in a relatively short period of time.

Training/resource issues: The training required to implement a new security system is a one-time expenditure of resources. Once in place, however, the reduction in manual tasks and the simplicity of a centralized console can reduce resource requirements year over year.

The recent media coverage of security breaches and hacking scandals has brought IT security concerns to the forefront. It's very hard to speculate about every fine detail involved in the recent breaches, but the recent increase in successful attacks does raise concerns around how organizations — of all sizes — approach their security operations. Yet, to simply continue patching security together with myriad solutions across complex and dynamic infrastructures will end up hampering IT and security teams with too many point solutions and is tantamount to setting the teams up for failure.

Organizations would be wise to carefully weigh the total costs of sticking with their current (and perhaps limited) security against moving forward with the best solution available. The cost of indecision is too high, and organizations must think forward if they want to protect the present.

About Bitdefender

Bitdefender is a modern, proven, cloud-based IT security solution that does a demonstrably better job of reducing business risk. Bitdefender delivers platform-neutral protection designed for today's complex datacenter. It unifies enterprise-wide security by protecting virtualized desktops and servers, traditional systems, as well as mobile devices. Its security technology protects more than 500 million users globally and conducts 7 billion interrogations daily in its cloud infrastructure, providing a three-second immune response to combat zero-day attacks.

No other security platform is designed to enhance security and reduce administrative overhead like Bitdefender GravityZone. To learn more about its innovative technology, visit http://enterprise.bitdefender.com.

[i] http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
[ii] http://www.av-test.org/en/statistics/malware/