



Optimizing IT Security within Real-World Resource Constraints

A Practical Guide for Midsized Businesses

Executive summary

Today's businesses face a barrage of information security threats. From hackers seeking to pilfer customer data to malware that can destroy desktop performance, every company must maintain constant vigilance against the wide range of attacks that threaten the integrity of critical IT services.

No organization, however, has unlimited resources to devote to computing security. Midsized businesses, in particular, tend to have tight IT resource constraints - even though they face the same risks as their Fortune 500 counterparts. So, despite the seriousness of today's cyber-threats, companies have to be very careful about how much money they spend on security solutions and how much of their staff time they devote to security management.

Thus, the central problem that midsized businesses face today is not simply how to protect themselves from IT security threats. It's how to best protect themselves from those threats within their real-world resource constraints. In other words, the objective of any security strategy is to get optimized protection "bang" for the security "buck."

There are several principles that IT security managers should apply in formulating such a resource-optimized protection strategy. These include:

- ▶ Use of a layered architecture that provides multiple safeguards against threats
- ▶ The intelligent automation of key tasks to reduce labor costs and overcome shortfalls in technical expertise
- ▶ Consolidated technology acquisition to reduce both purchase and ownership costs
- ▶ The leveraging of technologies that provide operational benefits, in addition to helping secure the IT environment

By applying the principles, IT departments can best minimize the risks associated with data loss and business disruption without diverting resources that are needed to address other important business requirements. This realistic goal - rather than the resource-draining pursuit of some impossible-to-achieve state of absolute zero exposure to every threat - is the real objective of enterprise information security efforts.

Raritan's ComandCenter® and KVM solutions support this real-world security strategy by delivering multiple layers of protection as integrated, easy-to-implement appliances. With Raritan solutions, the midsized enterprise can effectively protect itself from a wide range of threats, while eliminating the costs and management hassles that arise when IT security is implemented using multiple security products from multiple vendors. At the same time, these solutions provide substantial additional operational benefits that generate sufficient ROI to make their security capabilities virtually free.

The security challenge for midsized businesses

Midsized businesses face a serious challenge when it comes to IT security. On one hand, they face the same wide range of escalating IT security threats as larger enterprises. The potential impact of viruses, hackers, and insider information theft can be as disastrous for one as for the other. Businesses of all sizes must therefore vigilantly protect themselves from IT-related risks.



On the other hand, in proportion to the threats they face, mid-sized businesses have comparatively fewer resources with which to protect themselves than large enterprises do. They have smaller IT staffs and are less likely to be able to devote dedicated headcount to security. They also have smaller budgets with which to purchase security-related technologies and tools. These mid-sized businesses may therefore find it particularly difficult to maintain the safety of their critical IT operations.

One of the keys to security success in any organization is the implementation of layered defenses. This principle holds true for mid-sized businesses as well. A firewall, for example, is a key component of any defense against intruders. But a firewall alone is insufficient for adequately minimizing the risks associated with hacking attacks. That's why it's also essential to put in place intrusion detection technology (which enables the IT security team to determine if someone has gotten past the firewall and is probing for vulnerabilities) and vulnerability management (which enables the IT security team to eliminate the vulnerabilities that hackers most commonly seek). This type of layered defense - firewall, intrusion detection, vulnerability management - provides the foundation for today's security best practices.

Of course, the need for such a layered defense only exacerbates the nature of the dilemma that mid-sized companies face. Because now, in addition to just acquiring, installing and administering a firewall, the company has to acquire, install and administer intrusion detection and vulnerability management tools. This can potentially take more time, money and expertise and more time climbing the learning curve than a mid-sized business may possess.

Because they face sophisticated threats that require a layered defense - and because the budget and manpower allocated to IT security simply can't be increased in proportion to the increasing dangers they face - mid-sized businesses must be particularly wise and creative when it comes to IT security. If they do not find ways to effectively address the conundrum of growing threats and flat resources, they will eventually succumb to an attack and suffer the consequences thereof.

Best practices for resource-efficient IT security

How can mid-sized businesses ensure that they get the maximum security "bang" for their security "buck?" How can they make sure that security-related tasks don't consume a disproportionate percentage of their limited technology acquisition budgets or their IT staff's limited time?

Based on the recent experiences of mid-sized IT organizations, three key efficiency strategies have emerged:

Apply automation wherever possible

One of the most straightforward and effective strategies being used to reduce the strain that security places on IT organizations is to automate wherever possible. By applying technology to ease security-related workloads, mid-sized businesses can considerably enhance their ability to protect their IT environments from a variety of threats. These technologies can also compensate for any shortfalls in staff skill-sets by leveraging the vendor knowledge and expertise.

A classic example of this automation strategy can be found in vulnerability management. Without automation, IT staff can spend an enormous amount of time trying to keep up with the latest security bulletins and comparing newly announced vulnerabilities with the various system configurations in their own environments. With a well-automated vulnerability management tool, on the other hand, all this work can be eliminated. The tool can scan the environment against a set of vulnerability "signatures" that are maintained and automatically distributed by the vendor. Because maintenance of these signatures is a core competency for the vendor, this approach makes it far less likely that a given vulnerability will be missed - and will therefore remain exposed to intruders.

Acquire integrated, multi-function solutions

This is another simple, intuitively obvious strategy for achieving security objectives with maximum resource-efficiency. By purchasing integrated solutions that fulfill multiple functional requirements, midsized companies can achieve a variety of efficiencies, including:

- ▶ Reduced total capital spending on security
- ▶ Reduced total cost of ownership - including less maintenance, fewer upgrades and reduced training requirements
- ▶ Fewer vendor relationships to manage
- ▶ Less strain on existing skills/manpower resources

Integrated, multifunction solutions can streamline security operations and reduce costs in other ways, as well. For example, a vulnerability management solution with a built-in asset inventory database will be easier and less time-consuming to deploy and operate over time than one that requires IT to purchase a separate inventory tool and then do the integration work necessary to get the two to work together. Typically, built-in inventory capabilities will also integrate more seamlessly than those provided by a third-party solution. This seamless integration is important for ensuring that newly installed devices are assessed for potential vulnerabilities as soon as they are "discovered" by the asset inventory software.

Multifunction solutions also boost staff productivity, since technicians don't have to constantly shift from one tool to another (or one workstation to another) as they perform their daily management tasks. For example, some solutions integrate diagnostic functionality with remote access capabilities. Technicians can therefore gain immediate access to the affected device by simply clicking on the problem alert. This interface-level integration enables them to respond more quickly to emerging issues - without leaving their chair, and a single sign-on makes the tools themselves more secure.

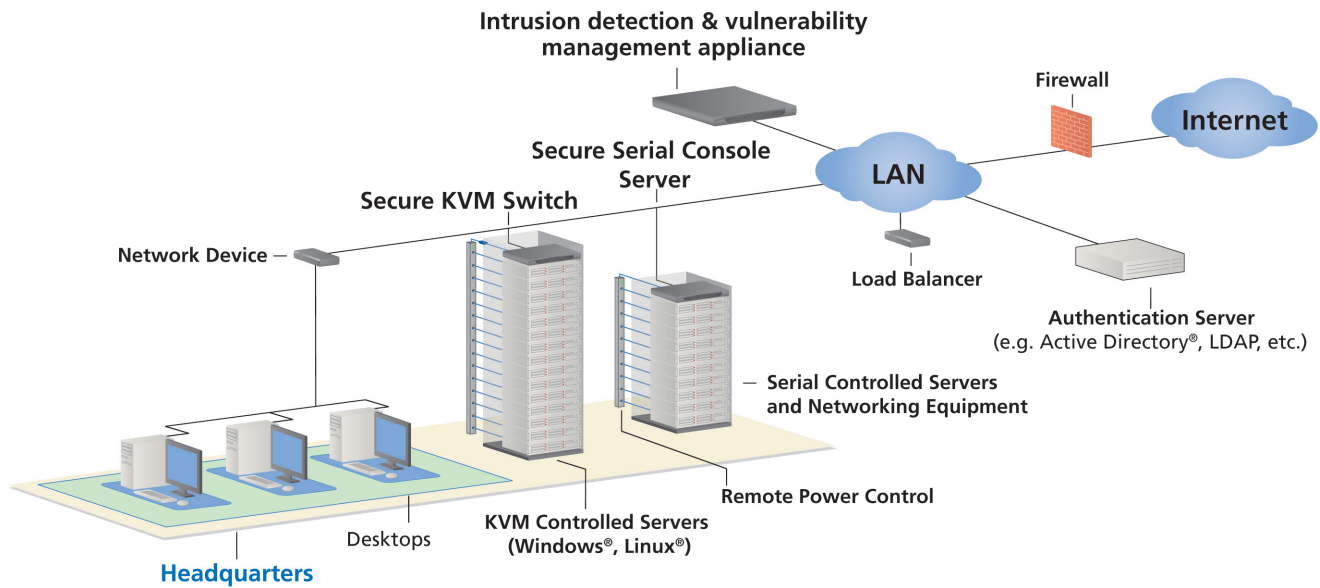
Use of appliance-based solutions

Another practical strategy for midsized businesses seeking to maximize their security "bang-for-the-buck" is to use appliance-based solutions, rather than software-only products that require installation on a separately purchased server. Appliance-based solutions are self-contained units that provide a complete package, including specialized server hardware and security software running on a hardened operating system. They therefore offer:

- ▶ Out-of-the-box implementation that eases initial deployment and ensures immediate realization of critical security benefits
- ▶ Elimination of the ownership costs associated with general-purpose servers and their operating system, e.g. server administration, OS upgrades and patches, optimization of the server configuration to support the security software, etc.
- ▶ Greater reliability and uptime, due to reduced need for manual administration

An appliance-based solution running a hardened OS kernel is also less vulnerable to attack than a general-purpose server running an OS that is well-known to the hacker community. In fact, because it does not use an easily identified OS such as Windows®, the internal functions of such an appliance are extremely opaque and inaccessible to any unauthorized user inside or outside the IT organization. Appliance-based solutions are therefore far more secure than their server-based counterparts.

The bottom line for midsized businesses is that they have to keep their security toolkit simple and easy-to-manage. An overly complex toolkit will be too expensive to buy and own. Even worse, complexity and cost will eventually result in some critical task going undone - which will negate the entire investment. Midsized businesses should therefore be as selective and efficient as possible in their acquisition of security solutions, and should focus on highly automated, appliance-based solutions that integrate multiple essential security capabilities.



By using multifunction, appliance-based solutions, midsized businesses can significantly reduce the capital and ongoing management costs associated with IT security.

Leveraging operational benefits to pay for security

An important, often-overlooked strategy that can significantly lower the total cost of security for midsized businesses is to implement solutions that address both operational and security needs at the same time. This way, security investments can pay for themselves in other ways - such as reducing IT costs or improving service levels.

A classic example of such an acquisition is KVM (Keyboard, Video, Mouse) technology. KVM solutions significantly reduce the cost of server ownership by enabling technicians to access managed systems from anywhere at any time. This remote access capability also reduces average time-to-fix, which means faster restoration of service and reduced downtime in the event of a system problem.

However, KVM technology can also be an integral component of a layered security strategy - since it ensures strict control of physical access to sensitive equipment. This access control is also important for compliance with IT-related regulations such as Sarbanes-Oxley, the Health Information Portability and Accountability Act (HIPAA) and Basel II. Thus the security and compliance benefits provided by KVM can essentially be gained for "free" by virtue of the operational benefits it also provides.

Another example of this strategy can be found with solutions that combine network management with intrusion detection. These technologies are closely related, since they both involve the monitoring and analysis of data traffic. Network management is obviously essential for any IT organization, since it is necessary for maintaining the performance of distributed applications and for planning infrastructure growth. By "piggybacking" intrusion detection on top of this management functionality, the added benefits of a layered security model can be gained with minimal incremental cost.

This type of combined operational/security acquisition strategy is particularly important when it comes to cost-justifying purchases to CFOs and other executives. Security purchases are often very difficult to cost-justify, because their value has more to do with the potential losses they can prevent - rather than the hard savings they can definitely return. The return-on-investment for operational solutions, on the other hand, is relatively easy to calculate based on staff time savings, reduced downtime and other factors. An ideal way for midsized business to put multiple levels of security protection in place is therefore to acquire as many of those levels as possible via solutions that pay for themselves with predictable, quantifiable operational benefits.

Raritan's security solutions for midsized businesses

Raritan solutions fulfill the crucial requirements of midsized businesses by providing security solutions that:

- ▶ Automate key security tasks
- ▶ Integrate multiple security capabilities
- ▶ Are appliance-based
- ▶ Offer high-ROI operational benefits beyond security

Raritan's CommandCenter® NOC family of multifunction IT infrastructure management appliances enables midsized businesses to implement a layered security model, while also addressing key network performance monitoring challenges. It integrates world-class network and systems management, traffic analysis, vulnerability scanning, intrusion detection, asset management and reporting functionality into a single, easily deployed appliance. It is also designed to facilitate monitoring and management by service providers - enabling midsized businesses to offload IT tasks as appropriate.

CommandCenter NOC provides a full range of key security capabilities, including:

- ▶ Automatic discovery of suspicious network activity
- ▶ Diagnosis of common security problems and suggested solutions
- ▶ Consolidation of log files from firewalls, antivirus software and servers
- ▶ One-click reporting on vulnerabilities and unpatched systems
- ▶ Reporting support for Sarbanes-Oxley, HIPAA, Basel II and other regulatory mandates

At the same time, CommandCenter NOC provides a wide range of other high-value management capabilities that help ensure service levels, control licensing costs, and rapidly troubleshoot potential problems before they occur.

Raritan's award-winning KVM and serial solutions can also play an invaluable role in any layered security implementation, while significantly improving the efficiency and effectiveness with which IT staffs manage and administer servers and other IT resources. From a security perspective, these solutions help protect critical resources by limiting physical access to sensitive equipment and providing an effective means of controlling and auditing logical access to servers by IT staff. From an operational perspective, these solutions reduce labor costs and speed responsiveness by enabling authorized personnel to perform critical IT tasks from anywhere at any time.

IT organizations can further streamline security and management using Raritan's CommandCenter Secure Gateway, which provides unified access to servers and other devices on the network via a single sign-on. Ideal for any business with midsized to large data centers or multiple remote offices, CommandCenter Secure Gateway offers secure, centralized policy-based management of the end-to-end infrastructure from an intuitive, graphical interface, combining both "out-of-band" and "in-band" access, digital KVM, analog KVM, serial-over-IP and embedded remote management tools in a single, integrated view. As a browser-based solution, CommandCenter Secure Gateway also enables technicians to discover, diagnose and resolve infrastructure problems from anywhere, anytime. Plus, with its support for IPMI and HP's iLO, CommandCenter Secure Gateway delivers complete BIOS-level control of managed devices - allowing remote power control and other tasks to be performed even when a server's operating system fails.

Midsized businesses seeking to optimize security and safeguard customer data without making disproportionate investments in security technology should strongly consider implementing Raritan's CommandCenter Service Management Architecture. With Raritan, organizations can quickly and cost-efficiently build an effective, automated layered security model while gaining many other valuable capabilities that will greatly defray the expense of protecting the business.

About Raritan

Raritan is a leading supplier of solutions for managing IT infrastructure equipment and the mission-critical applications and services that run on it. Raritan was founded in 1985, and since then has been making products that are used to manage IT infrastructures at more than 50,000 network data centers, computer test labs and multi-workstation environments around the world.

From the small business to the enterprise, Raritan's complete line of compatible and scalable IT management solutions offers IT professionals the most reliable, flexible and secure in-band and out-of-band solutions to simplify the management of data center equipment, applications and services, while improving operational productivity. More information on the company is available at Raritan.com.

