Whitepaper

Meeting Branch Office Business Needs for Security and Networking

July, 2006

Mark Bouchard

CISSP and Independent Security Consultant

Missing Link Security Services, LLC

Part Number: 200163-002

Contents

About the Author

Mark Bouchard, CISSP, is the founder of Missing Link Security Services, LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security topics for nearly 10 years. He has established a reputation for thought leadership and is a sought after speaker in the areas of security architecture, DMZ design, secure remote access, network security, and related technologies (e.g., firewalls, intrusion prevention systems, and virtual private networking).

He is passionate about helping enterprises address their information security challenges. During his career he has assisted hundreds of organizations world-wide with everything from strategic initiatives (e.g., creating 5-year security plans and over-arching security architectures) to tactical decisions involving the justification, selection, acquisition, implementation and ongoing operations of individual technologies/products. In addition, he routinely works intimately with the creators and sellers of information security solutions, helping them to better understand and meet the needs of the market at large.

Introduction

Branch offices are a critical and potentially competitive component of modern companies. Often representing more than half of an organization's employees, they typically support any number of important business functions, not the least of which is having a physical presence in closer proximity to one's customers. According to the industry analyst group Nemertes Research, in 2005, approximately 91% of employees worked in locations other than headquarters – up from 85% in 2003. Not surprisingly, employees in these locations require access to many of the same applications and computing resources that are locally available to their colleagues operating in central-site and regional headquarter locations. However, common approaches for providing this access are proving to be inadequate in terms of performance, security, and cost of ownership. This is being caused by a variety of factors that are impacting the modern computing environment, including increasing traffic volumes, ramping Internet usage and dependency, new application types, an evolving threat landscape, and mounting regulatory pressures. The result is the need for a new branch office solution – one that provides robust protection from both external *and* internal threats while also achieving even greater consolidation of requisite security and networking capabilities.

Branch Office Trends and Challenges

A closer examination of the challenges impacting today's extended computing environment is essential to better understanding the requirements of an ideal security solution for branch offices.

Backhauling Breaking Down

In the past, access to centrally operated business applications was established by providing wide-area network (WAN) connections between branch and central-site offices. Subsequently, popular WAN technologies such as Frame Relay were replaced with the less expensive option of using Internet-based VPNs. Regardless, in both cases, these same connections were also used to convey traffic bound (and returning from) other locations on the Internet. This approach, commonly referred to as backhauling, was preferred because it obviated the need to replicate complicated and costly security infrastructure (e.g., firewalls, intrusion protection systems, gateway anti-virus, and URL filtering) at each and every branch office location. However, a number of factors are now causing the effectiveness of this approach to be called into question.

One such factor could be referred to as Internet connection "creep". The scenario is an all-too-common one where semi-autonomous branch personnel, looking to bypass bureaucracy and more efficiently meet their "own unique needs", take it upon themselves to establish local, direct connections to the Internet. This may indeed address their "special" connectivity requirements, as well as improve performance, but it inevitably also puts the entire organization at greater risk. After all, having security capabilities and policies that are inconsistent, or worse relaxed, relative to those employed at headquarters is a recipe for disaster.

A more significant issue, however, is that applications being used today are more complex, bandwidth intensive, and latency sensitive than those of the past. The growing adoption of VoIP technology, distance learning, and a wide range of multimedia applications are just a few examples driving this trend. At the same time, it is also the case for most organizations that a greater percentage of traffic is now destined for the Internet. Unfortunately, under these conditions, backhauling communications traffic will create performance issues for the growing population of modern business applications. It will also result in surging capacity requirements at the central site, in terms of raw bandwidth as well as security processing capability. In turn, this can be expected to further increase session latency, while also driving capital and operational costs for central site infrastructure significantly upward.

Yet another shortcoming of the backhauling approach is that it completely ignores the need to secure the internal network and systems at these locations. This practice, which makes good sense in any case, is also being driven by a host of regulations and legislation which, if not explicitly, at least implicitly require organizations to address the security of their internal computing environments. From a practical perspective, increasing mobility of users and their computing stations is a significant culprit in terms of introducing threats (e.g., worms and other malware) into these environments. And, of course, infected branch offices subsequently pose a risk to all other connected locations, particularly since inter-office communications are relatively open and not heavily secured (with the exception of being encrypted). Furthermore, even if the branch VPN device includes firewalling and a range of other security features, such perimeter-focused solutions are typically incapable of sufficiently solving the problem. This is due in part to these products (a) not having adequate capacity relative to typical LAN bandwidth rates, and (b) not having sufficient capability to segment the environment and establish multiple security domains.

These various, intersecting factors and trends lend themselves to two apparent conclusions. First, from the perspective of both economics and performance, it is increasingly making good sense for branch offices to be outfitted with direct access to the Internet. The intended approach would still use VPN connections to access centrally operated resources, but it would otherwise obviate the need to backhaul Internet-bound traffic. The second conclusion then, is that even greater advantage can be gained if this "outfitting" is accomplished in such a manner that it also yields a comprehensive security solution for the branch office – that is, one that not only addresses external threats but also those which originate from within.

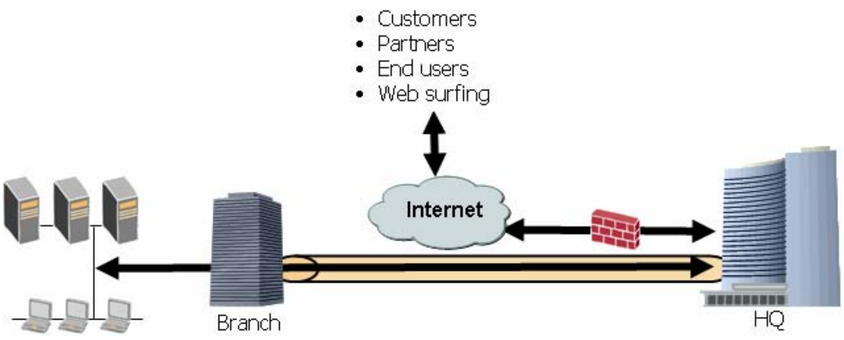

Figure 1: Backhauling forces all branch traffic through headquarters

Compounding Factors

A handful of additional, underlying conditions must also be acknowledged prior to establishing the detailed criteria and characteristics that define an ideal security solution for branch offices.

Practical Matters

The first practical matter that must be addressed is that branch offices rarely have sufficient personnel to justify the presence of local IT support staff. The implication is that any solution which is implemented must be capable of being administered remotely. The importance of remote management should not be underestimated. At a minimum, complete device configuration should be accessible across any one of several different means such as HTTP/S, SSH, SSL, Telnet, etc. Ideally, the scope of remote management should entail mechanisms to perform global updates with a few keystrokes, streamline mass deployments and minimize configuration errors.

Another relatively obvious issue is the fact that branch offices are often quite numerous. Even relatively small businesses are likely to have a dozen or so remote offices, while large enterprises may have as many as a hundred, and retailers will have potentially thousands of such locations. In any case, it should not be expected that any given office will be entitled to funding that is significantly disproportionate to its size – or, more pointedly, that any business is going to be keen on spending tens of thousands of dollars per branch office to achieve a comprehensive security solution across all of its locations.

And speaking of size, it is also important to acknowledge that, with the possible exception of the retail industry, not all branch offices are created equal. Indeed, even within a single organization branch offices can vary considerably, supporting anywhere from just a handful to several hundred employees, having different degrees of business criticality, and involving local networks that range from being relatively simple to surprisingly complex.

The net result of these items is that a branch office security solution must not only accommodate a range of different office sizes and needs, but in doing so it should also be easy to deploy and operate and, above all else, remain relatively economical. Consequently it should be clear that all-in-one appliances – especially those with a range of price points and corresponding capabilities – are particularly well suited to the branch office environment.

Of course, this same reasoning can be advanced yet another step. Specifically, assuming that no corners are cut in the process, branch office appliances should ideally include not only a full set of security services, but a complete complement of networking capabilities as well (e.g., routing, WAN connectivity). This then introduces the potential to simplify branch office infrastructure even further by eliminating the need for a separate networking device.

Additional Security Issues

Shifting gears just a bit, another condition that must be accounted for is the changing threat landscape. In particular, threats are emerging and spreading more quickly than ever before. New attacks are being launched only days after the vulnerabilities they exploit have been announced. In addition, many of these are able to spread at a frighteningly fast pace. For example, in 2003 the Slammer worm achieved an infection doubling rate of 8.5 seconds on its way to infecting 90% of all susceptible hosts within 10 minutes. The problem with this situation is that with increasing frequency patches cannot be installed and reactive, signature-based countermeasures cannot be updated quickly enough to provide protection during the early phases of new, or unknown, attacks.

In addition, there is also an issue with threats becoming more elusive. Readily accessible exploit development frameworks are enabling hackers to generate blended threats with ease. Furthermore, over the past few years, attention has shifted dramatically from exploiting network-layer vulnerabilities to going after those within application themselves. As a result, a growing volume of threats are now able to penetrate the far more common network-layer defenses that organizations have historically implemented.

Effectiveness of a branch office security solution, therefore, will depend at least in part on: (a) supplementing reactive countermeasures with ones that are able to more proactively prevent unknown attacks, and (b) supplementing network-focused defense mechanisms with ones that can prevent attacks against application-layer services. Of course, at the same time this will all need to be done without compromising in terms of quality of the individual countermeasures and, of equal importance, without having to compromise in terms of overall system performance.

The Ideal Branch-Office Security Solution

At a high level, all of the applicable trends, challenges, and characteristics dictate that an ideal branch-office security solution be able to:

- Provide fast and secure site-to-site VPN connections. This is primarily to establish access to centrally operated applications and resources, but should also include support for employee remote access and having direct connections to local partners.
- Provide direct, secure Internet access. This is important to avoid the growing disadvantages associated with backhauling Internet traffic through a regional headquarters location.
- Provide improved security for internal networks and systems. This applies directly to the branch office, but will also indirectly benefit all other sites connected to it.
- Provide improved ease of use and economics. This can be accomplished by having an appliance, appropriately sized for the location, that can consolidate as many security and networking capabilities as practical without making any compromises, especially in terms of quality of the security functions, performance, and reliability.

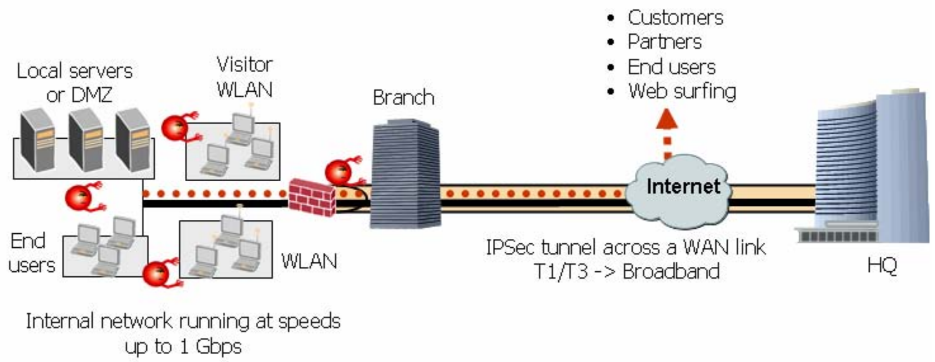

Figure 2: Ideal branch office security and networking solution delivers performance and advanced security features to protect the network against both internal and external attacks

For product evaluation purposes, it is helpful to decompose these high-level objectives into a corresponding set of detailed selection criteria that characterize an ideal branch office security *and* networking solution. These can conveniently be grouped into five logical categories: comprehensive security, rich inter-networking capabilities, performance and reliability, scalable management, and flexibility/compatibility.

Comprehensive Security

The desire to shift from backhauling Internet traffic to providing direct access necessitates having the same, comprehensive set of security services at the branch office that would typically be reserved for Internet access gateways established at central-site locations. In terms of general requirements, many of these have already been covered: each individual countermeasure should ideally be best-of-breed in its category; some countermeasures should be proactive in nature; and, some should be able to account for application-layer threats. Otherwise, specific capabilities that should be available include the following.

- Virtual Private Networking. The ability to establish IPSec VPN tunnels is clearly a fundamental necessity of a branch office solution. From a practical perspective there should be sufficient capacity in terms of simultaneous tunnels (e.g., >100) and encrypted throughput (e.g., > 100 Mbps) to meet any business objectives that may arise. At a more mundane level, a full range of common encryption (e.g., 3DES, AES), key exchange (IKE, X.509), and user authentication options (e.g., password, RADIUS, LDAP, tokens) and associated features (e.g., NAT traversal, L2TP within IPSec for Microsoft VPN clients) should be available to ensure a high degree of security as well as interoperability.
- Firewall. Another fundamental necessity, firewalling capability should entail far more than just the basic network and transport-layer access control (i.e., based on addresses, ports, and protocols) provided by many earlier products, as well as by the vast majority of networking devices that “play” at delivering security functionality. Indeed, as a positive model countermeasure, a firewall has tremendous potential to help stop unknown attacks. By permitting only that traffic which is explicitly allowed by policy and denying everything else, it inherently (and blindly) eliminates a wide range of both known and unknown threats. However, its effectiveness will be limited by the granularity with which its policies can be set. Specifically, if it only operates at the network layer, then it will not be able to stop application-layer attacks that are conveyed over protocols and connections that are allowed by its rule base. As such, it is critically important that today’s firewalls also include a heavy dose of application-layer awareness. And, to be clear, this coverage must be broad as well as deep. In other words, it should extend well beyond the handful of common “Internet” protocols to also account for those associated with web services and applications such as instant messaging, peer-to-peer file sharing, and voice over IP.

- Attack Protection. All firewalls eventually let some amount of traffic pass. Moreover, this is done without knowing whether it contains an attack. Thus, it is prudent that this traffic, upon being blessed by the firewall function, subsequently be examined further to ensure that it does not include any bad elements. This is where intrusion detection and prevention technology fit in. For a branch office solution, this countermeasure should include at a minimum a signature-based mechanism for identifying known attacks. More advanced implementations should also (or alternatively) incorporate one or more techniques that are capable of identifying unknown attacks, such as protocol anomaly detection, vulnerability based signatures, or heuristics (i.e., root-cause signatures that represent broad-based behaviors that are known to always be bad). Finally, statistical anomaly detection, or another similar mechanism, should be present to help thwart denial-of-service attacks.
- Advanced Content Filtering. This is not really a single countermeasure, but rather a collection of related items that are all appropriate for sites where users will have direct access to the Internet. Arguably, the most significant of these is anti-virus. Although it is limited in the sense that it is completely reactive, anti-virus is still important from the perspective that by focusing on known, file-based attacks it completes yet another piece of the overall security puzzle.

  Closely related to and increasingly delivered in conjunction with anti-virus are anti-spyware and anti-spam capabilities. Anti-spyware is necessary to keep annoying adware at bay, while also providing protection against more serious threats such as keylogger trojans. And anti-spam is essential for eliminating unwanted email messages and, more recently, those that include phishing attacks.

  Finally, there is web/URL filtering. This safeguard is a bit different in that it prevents threats by focusing on outbound traffic, whereas all of the other mechanisms focus *primarily* on inbound traffic. One advantage of web/URL filtering is that it can be used to keep users from connecting to websites that are known to be unsafe (e.g., because they host spyware or phishing attacks). Of course, it can also be used to keep them from visiting sites that may introduce the organization to liability issues (e.g., pornography), or which are otherwise not explicitly related to their job function.
- Segmentation and Security Domains. This is a straightforward yet surprisingly uncommon feature set that is instrumental to achieving internal security at branch office locations. It requires the associated appliance have, at a minimum, multiple LAN interfaces, and ideally VLAN capabilities as well. These physical and logical means for segmenting different groups of users and computing resources are then bolstered by enabling a unique security policy to apply to the traffic both entering and leaving each domain. Such an ability to create separate security zones ensures that resources with different levels of trust need not commingle (e.g., a guest WLAN and help desk workstations). It also provides a measure of containment in the event that a device in one of these domains somehow gets infected.

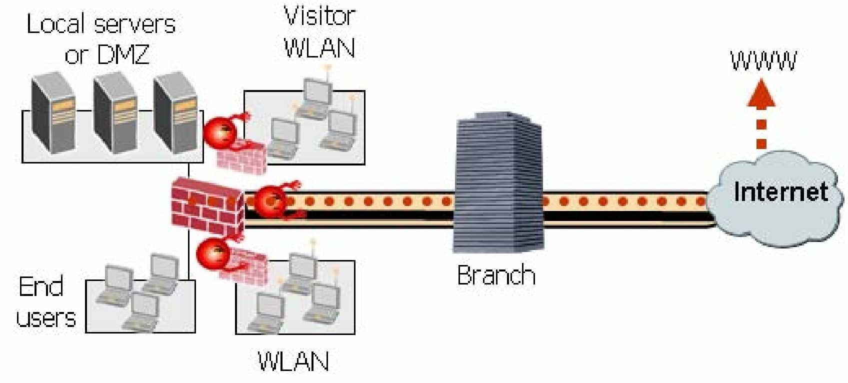

Figure 3: Network segmentation means assigning unique security policies to different groups or subnets for internal network security

Networking

As already discussed, an ideal branch office security solution should give organizations the option of not having a separate, standalone networking device at each location. In order to accomplish this objective, the associated appliance will need to support a variety of core networking capabilities. Multiple LAN interfaces and VLAN capabilities, useful for security purposes, will need to be accompanied by *proven implementations* of a variety of LAN/WAN interface modules (which should be replaceable to keep pace with future connectivity options) along with appropriate routing protocols and WAN encapsulations. Support for virtual routers could also be useful, particularly for larger offices.

Performance and Reliability

The key to achieving top-notch performance and reliability is having a purpose-built "system" that is optimized for its intended functions and implementation scenarios. In this regard, having an operating system that is pre-hardened and pre-tuned to best meet the needs of the specific applications that are being run is only a starting point. Another consideration is how the various security and networking capabilities are brought together. Specifically, an appliance that is designed from the outset to jointly provide security and networking functions will typically be superior to a former networking device that has subsequently had security "bolted on", or vice versa.

Fundamentally, ensuring adequate performance also entails having sufficient processing, memory, and I/O capacity to achieve rated throughput and reasonable latency under all operating conditions (i.e., even with small packets). Remember, without sufficiently high performance a solution will not be able to support the proper operation of modern applications, not to mention simultaneously providing features such as advanced content filtering and security for internal networks.

In general, it would be a mistake to equate the size of a branch office with its degree of importance to the business. Indeed, based on the nature of the functions and processes being supported, there will inevitably be some instances where it is deemed essential to ensure non-stop operations. At a minimum, this means incorporating features such as: additional ports and protocol support to accommodate various types of backup WAN connections (e.g., ISDN BRI, V.92, Serial); native failover and/or clustering to account for an appliance failure; the option for redundant or hot swappable components (e.g., fans, power supplies); and an out-of-band management interface (i.e., to ensure that management functions are accessible under conditions of heavy load). Better yet is a design that also minimizes the number of moving parts, for example, by using Flash memory as opposed to a hard drive to store system software. Finally, it is important not to overlook the value of using a vendor that has established an excellent track record, both in terms of delivering reliable products as well as subsequently supporting them.

Scalable Management

The cost effectiveness of a branch office security solution is dependent on more than just being able to consolidate a number of necessary functions into a single device. Indeed, without scalable management capabilities, the benefit of such consolidation would be significantly, if not completely, eroded. Fortunately, ease of deployment, an essential first step, is an inherent characteristic of plug-and-play appliances. However, physical installation is only a one-time effort and, therefore, is significantly less important than a solution's operational management capabilities.

As a result, centralized management, or the ability to remotely manage multiple devices at once, is a critical requirement. Equally important, though, is having ease of use be a pervasive characteristic which extends across the full suite of life-cycle management functions. Consequently, specific capabilities that should be considered necessary for an efficient and comprehensive management system for branch office devices include:

- Policy development that is facilitated by flexible and hierarchical grouping of devices and rules;
- Device set-up that is facilitated by configuration wizards or templates covering default settings;
- Real-time monitoring that is facilitated by views of device status and associated security events;

- Robust logging and reporting that is facilitated by a range of options (e.g., pre-defined, customized, ad-hoc, scheduled);
- Software maintenance that is facilitated by automatic updates of system software, hosted applications, and associated content (e.g., signatures);
- Unified management, which involves the use of a single management system to administer all of a vendor's security products, be they branch office or central site models; and
- Role-based administration that provides *complete* flexibility in terms of assignment of rights when it comes to managing specific devices and/or individual services (e.g., security vs. networking, or firewall vs. anti-virus).

Flexibility and Compatibility

The final category of criteria that defines an ideal branch office security *and* networking solution is no less important than the others that preceded it. And, in fact, the most basic aspect of flexibility and compatibility has already been covered as part of the earlier categories. Specifically, the longevity and interoperability of a branch-office solution depends on supporting, at the outset, multiple options for its software and hardware features alike. User authentication, encryption algorithms, physical interfaces, and routing protocols are but a few of the more obvious examples. Modularity, upgradeability, and abundant processing capacity are further, general characteristics that also align with this objective.

An additional aspect of flexibility and compatibility to consider is support for multiple deployment modes. In particular, a branch office security device should function equally well in all environments, regardless of whether they utilize network translation, are fully routed, or require transparent operation (i.e., layer 2 bridging).

This category of criteria is also where the need to support branch offices of various sizes fits in. As previously discussed, branch offices are not all the same and, therefore, a one-size-fits-all appliance will not be appropriate. Instead, multiple models should be available such that each location need only pay for the amount of performance/capacity that it actually requires. In addition, while it is important for ease of management purposes that the core set of capabilities remain consistent across all models, having multiple options will enable an appropriate degree of functional variation. For example, smaller branch offices may benefit from having an integrated WLAN access point, while larger ones will typically require support for a broader set of routing and high availability features.

Finally, it is important to recognize that a security and networking solution which meets all of the criteria identified in this paper should in fact be able to support a number of possible use cases and, as such, fill a role in just about any enterprise. Indeed, associated appliances could optionally be deployed either as single-function devices (e.g., firewall, VPN, router) as shown in figure 4, or as multi-function solutions taking advantage of virtually any combination of the supported security and networking capabilities, as shown in figure 5. Furthermore, while the focus to this point has been branch offices, it should be clear that some of the appliances would also ably meet the needs of the main locations of many small and medium-sized businesses.

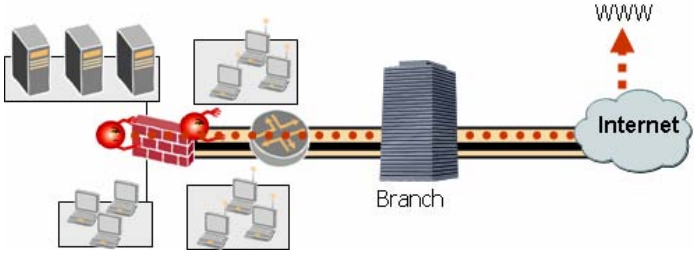

Figure 4: Deployed as a standalone firewall in conjunction with a router to maintain separation of security and routing

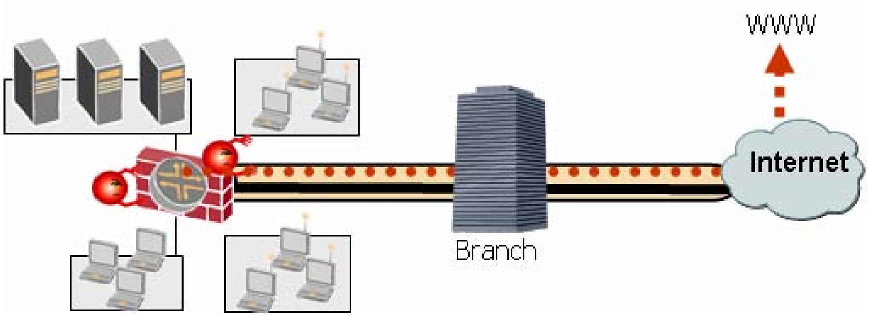

Figure 5: Deployed as a combination firewall and router to consolidate devices at a branch office

Summary

Branch offices and the personnel that work in them are an important, if not strategic, business asset. As such, it is essential to efficiently and effectively provide them with access to necessary computing resources, regardless of whether those resources are operated within central-site locations or at other points on the Internet. At the same time, an evolving threat landscape and mounting regulatory pressure are requiring that organizations enhance the internal security at branch offices. And, of course, all of this needs to be done without breaking the bank.

An ideal solution to address all of these business needs would be a purpose-built appliance that combines a full range of best-of-breed security services with an equally comprehensive set of proven networking capabilities. Ultimately, however, the effectiveness of such a solution will depend on the extent that it fulfills key criteria, not only in the areas of security and networking, but also in the critical categories of performance and reliability, flexibility and compatibility, and scalable management.