



IT SERVICES WITHOUT BOUNDARIES: RETHINKING THE DISTRIBUTED ENTERPRISE

Distributed enterprises have come to recognize that remote work centers are strategic to their success, housing both staff and functions that create value and contribute directly to the bottom line. Today, upward of 90 percent of employees work outside of headquarters, according to Nemertes Research.¹ Yet until recently, remote offices, regional offices, and headquarters were outfitted with an assortment of network and security hardware with varying capabilities. As a result, user experience varied from site to site, and enterprise IT found it difficult and expensive to respond effectively to changing application and service delivery requirements. Forward-thinking companies are remedying this problem by deploying a consistent set of technologies and products enterprise-wide.

The challenge for distributed enterprises is delivering IT services without boundaries—that is, providing each work center with the IT services necessary to function as an integral part of the enterprise, without breaking the bank or overburdening IT staff. For example, organizations need to provide high-performance, secure network services for employees, customers, and partners even at sites with no IT presence. In addition, network and

security solutions must accommodate a mobile workforce so that users who move between locations get the same services regardless of where they sit on a given day.

In these economic times, distributed enterprises need IT solutions that help ensure full productivity from high-value work centers while lowering total cost of ownership. Next-generation solutions can help a distributed enterprise connect, secure, and manage remote work centers more

cost-effectively, enabling them to deliver IT services without boundaries.

Recognizing the value of every location

The terms *remote office*, *branch office*, and *satellite office* no longer convey the strategic importance of the distributed enterprise's many sites, which is why the term *work center* has gained prominence. For example, retail chains know that convenience stores, restaurants, and other retail outlets are not only revenue centers but also the primary point of contact between an organization and its customers.

Likewise, health care, financial services, and other professional organizations as well as government agencies count on their distributed work centers to deliver services directly to clients or constituents. For manufacturers, software developers, and similar organizations, many work centers function as the innovation engine for the enterprise, housing highly skilled and/or strategic employees who create new products or intellectual property.

Remote work centers come in all sizes, from single-person sites to multi-building campuses. A distributed enterprise may comprise several types of work centers. For example, a consumer electronics firm may have both revenue-generating and innovation-based work centers.

¹ *Building the Successful Virtual Workplace*, Nemertes Research

Requirements of high-value work centers

Understanding the connectivity and security requirements of each type of work center is an essential first step in delivering network services without boundaries. Let's examine three common high-value work center examples.

Transaction- and revenue-generating work centers

Convenience stores, supermarkets, chain restaurants, and other retail sites support a variety of traffic types (for example, credit/debit card processing, lottery, and inventory control data), resulting in a fairly complex infrastructure. A typical retail site may have the following requirements:

- Retail work centers rarely have technical staff on site, so they need IT products that support auto-configuration as well as remote visibility and management.
- To protect the integrity of financial information and ensure rapid transactions, these sites require secure connectivity over broadband connections.
- Enterprises often drive down connectivity costs for these sites by connecting them directly to the Internet, which necessitates anti-virus, deep packet inspection, Web filtering, and firewall security

functions. These sites may also need role-based pre- and post-admission network access controls to restrict resource use by employee role (for example, store manager, cashier, and stocking clerk).

- If the site accepts credit card payments, it needs to comply with payment card industry (PCI) data security standards.

Work centers that provide service and support

Increasingly, distributed enterprises that operate remote service work centers—such as health care clinics, bank branches, or law offices—are cutting costs by implementing software as a service, cloud computing, and/or data center consolidation. This leads to several unique requirements:

- When enterprises centralize application delivery and storage, service work centers require a network optimized for secure application delivery.
- To accommodate users who work at more than one site, the network needs to offer an identical user experience and consistent access to applications and data, regardless of location.
- Due to the sensitive, sometimes critical nature of the transactions at these sites, they need reliable, secure connectivity, including identity-based access control for wired and wireless networks, as well as the ability to segment and manage mission-critical application traffic differently than lower priority traffic.

- Depending on the business functions performed, these sites may need to comply with industry-specific standards such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), or other regulations.

Collaboration and innovation work centers

Typically remote research and development facilities, innovation work centers are often large locations that house a professional white-collar staff. Among their unique requirements are:

- High-performance networks that facilitate effective and secure collaboration through technologies such as video conferencing.
- WAN connectivity on par with headquarters.
- Robust security, including real-time threat detection and mitigation in addition to identity-based access control, to protect intellectual property while meeting user expectations for free and unrestricted Internet access.
- The ability to host full-time employees as well as diverse user groups such as contractors, consultants, part-time employees, and guests—specifically, the ability to alter network segmentation and application access permissions depending on the user groups and their job responsibilities.

Drawbacks of current solutions

Clearly, not all work centers are the same. Historically, vendors tried to meet the needs of various types of work centers by



Next-generation solutions can help a distributed enterprise connect, secure, and manage remote work centers more cost-effectively, enabling them to deliver IT services without boundaries.

developing point products scaled to fit a particular location, and some entrenched vendors continue this strategy. But it's complex and costly, if not impossible, to deliver IT services without boundaries by simply patching together a disparate collection of routing, security, and connectivity devices.

Point solutions are expensive to own, requiring significant capital outlay. They're also costly to operate since each device is configured and managed separately. IT is not only burdened with supporting multiple devices at each site but also must learn each device's feature set, operating system, and management platform. In many cases, IT must cope with this learning curve and ongoing operations overhead even when a single vendor's products are used.

As a result of this complexity, IT has limited visibility into activity at remote sites, which makes it difficult to identify and troubleshoot problems or comply with industry and governmental regulations. Adding to this complexity is the lack of common features across network and security gear because each runs a different OS; this inhibits business agility, making it a challenge to roll out new applications and services. In addition, when different sets of devices are in use at remote work centers, IT has a hard time implementing a consistent security policy enterprise-wide, which poses a security risk.

While equipment and "site siloing" are lucrative for vendors, they create artificial boundaries that are expensive and complex for today's enterprises. To deploy network services without boundaries, enterprises need to look beyond traditional remote office offerings to next-generation work center solutions.

Next-gen solutions for distributed enterprises

Next-generation network solutions coming to market have been designed

to meet the needs of highly distributed enterprises with consistent connectivity, security, and management across all corporate locations. These new platforms include integrated services gateways and Ethernet switches that share the same operating system and management software, and come in form factors that scale from the largest campuses down to the smallest work centers. This allows them to deliver predictable, consistent services for any size site across the entire enterprise.

Enterprises should look for new services gateways that combine routing, modular WAN connectivity, and collaborative security functions (including firewall, IDP/IPS, and IPsec VPNs that share information) in an affordable, scalable form factor. By combining the functionality of multiple devices into one box, integrated services gateways reduce both CapEx and OpEx while yielding a significantly better approach toward delivering services without boundaries. Enterprises have fewer devices to buy, install, and manage, making it possible to support dozens, even hundreds, of work centers without breaking the bank.

Similarly, look for vendors whose switch families scale from backbone and data center devices to entry-level Ethernet switches that have "big switch" functionality. For example, entry-level switches are available that offer: flexible WAN interfaces; integrated Layer 3 support as a standard feature; 802.1X for network access control (NAC); partial or full power over Ethernet, without the need for power management; and support for the Link Layer Detection Protocol for Media Endpoints (LLPD-MED) for easy connection of voice over IP (VoIP) phones and other devices.

Recognizing how critical remote work centers are, some new entry-level Ethernet switches include high-availability features such as field replaceable power supplies and fans. When no IT staff is on

location, an employee can change out a failed component, speeding repair and reducing downtime. Some entry-level switches even give IT the option to configure an external power supply, making the power supply hot-swappable—a feature typically found only on high-end switches.

The benefits speak for themselves

In addition to being "right-sized," three other characteristics of next-generation work center solutions are fundamental to the delivery of IT services without boundaries:

1. A single management system across all network and security components.

A single management system reduces OpEx by simplifying initial configuration and deployment as well as ongoing operations. IT can centralize management and reporting, which enables enterprises to leverage skilled staff, gain visibility into activity at remote locations, and more easily comply with regulations.

Look for next-generation services gateways and switches that support auto-configuration; once plugged in, the device "calls home" and gets its configuration information from the central management console. Auto-configuration is ideal for retail and other work centers that have no IT presence. Auto-configuration also reduces the burden on limited IT staff in some work centers.

2. A single operating system across devices.

With the same OS running on services gateways, switches, and other devices, enterprises can be assured of having a consistent feature set and control plane across their work centers. Having a single OS boosts business agility by greatly simplifying rollout of new features, applications, and services enterprise-wide.

A single OS also simplifies software upgrades and other network modifications. IT can configure and manage each feature the same way, with the same

effect, throughout the network and use the same tools to monitor, manage, and update multiple devices.

3. A consistent set of security services across components. Having a common set of security services reduces

enterprise risk because varied security products can cooperate and find attacks that evade point security

CONTINUED ON PAGE 7

JUNIPER NETWORKS SRX SERIES SERVICES GATEWAYS

INTEGRATED SECURITY AND ROUTING WITHOUT COMPROMISE

Juniper Networks SRX Series Services Gateways are next-generation solutions that enable uninterrupted expansion and growth of network infrastructures without compromising security. These solutions connect, secure, and manage workforce centers ranging in size from fewer than 10 users to thousands of users.

The SRX Series consolidates fast, highly available switching, routing, security, and applications in a single box. The robust, carrier-class engine provides physical and logical separation of data and control planes to allow deployment of consolidated routing and security devices. This allows enterprises and service providers to economically deliver new services, safe connectivity, and optimal end user experiences.

Juniper Networks JUNOS® Software, which enables these solutions, lowers deployment and operational costs with a single-source OS, single release train, on an open architecture. JUNOS also provides continuous carrier-class reliability and the stringent service integration that organizations need to quickly align the network with changing business requirements.

Seamless expandability

The SRX Series focuses on integrated functionality in the branch and high performance in campus, data center, and service provider applications. At smaller sites, the SRX Series combines essential security services with routing and switching connectivity to deliver a simple, single-box solution suitable for small to mid-range locations.

At larger sites, the SRX Series offers seamless expandability with Juniper's Dynamic Services Architecture. Each services gateway can be configured with a flexible number of I/O cards, network processing cards, and service processing cards (SPCs) to provide the ideal balance of

performance and port density for each workforce center. This flexibility also decreases costs while increasing business agility. For example, organizations can add additional security simply by adding more SPCs.

SRX Series Services Gateways are available in a variety of form factors, enabling organizations to buy what they need for each location regardless of size, and expand as needed. Organizations can choose from:

- **SRX Series for the branch.** Simplified configurations combined with highly integrated services at price points as low as \$1,099 make these products ideal for midsize businesses, regional offices, and small work centers.
- **SRX3000 Line.** A midplane design secures medium to large enterprise data centers, co-located data centers, service provider infrastructures, and next-generation enterprise services/applications.
- **SRX5000 Line.** Support for up to 120 Gbps firewall lets large enterprises and service providers secure data centers, co-located data centers, managed services, and core service infrastructures.

minimal configuration. Using a combination of security zones and policies, administrators can quickly and securely deploy an SRX Series Services Gateway. For more complex security architectures, policy-based VPNs can be used to support dynamic addressing and hybrid WAN designs.

- **Content security.** Beyond perimeter protection, the SRX Series offers a complete suite of optimal unified threat management and intrusion prevention solutions (IPS). These protect the network from the latest content-borne threats.
- **Access and threat control.** These solutions integrate with other Juniper security products to deliver organization-wide universal access control and adaptive threat management. Local and remote access control for any user or role, combined with network-wide threat visibility, give IT administrators the tools they need to combat malicious activity and meet regulatory compliance requirements.

Find more information about Juniper Networks SRX Series Services Gateways at www.juniper.net/us/en/products-services/security/srx-series/

Built-in and extensible protection

The SRX Series Services Gateways protect the network with:

- **Perimeter security.** Best-in-class firewall and VPN secure the perimeter with consistent performance and



SRX3400



SRX3600



SRX5600



SRX5800

The SRX Series Services Gateways provide unrivaled performance and scalability to enable uninterrupted expansion and growth of your network infrastructure without sacrificing security.



Rather than treating remote sites like “stepchildren,” successful enterprises recognize that the right IT infrastructure is fundamental to realizing the full value of *all* of their work centers.

products. At the same time, having consistent security services lowers management overhead because IT no longer has to struggle to patch together a coherent security solution.

Next-generation platforms support identity-based network access control, both pre- and post-admission, as well as traffic segmentation, which ensures that only authorized users get onto the network and are restricted to authorized resources. As a result, enterprises can ensure that even the smallest sites are secure, protecting intellectual property and other high-value assets regardless of work center location or size. In addition, the same security controls are in place wherever a user logs in, so users enjoy a common experience no matter where they work.

Bringing standards home

Leading vendors of next-generation work center solutions now support open standards, which benefits enterprises in numerous ways. Standards allow for interoperability among devices, eliminating vendor lock-in. In addition, standards open the door for value-added functionality, such as cooperative threat management, within a multi-vendor environment.

For example, new security standards from the Trusted Computing Group enable security and network platforms to communicate with each other to identify and stop attacks in real time. Using these standards, intrusion prevention systems (IPS), firewalls, and other security devices throughout the network can share security state information with a policy server to detect and mitigate attacks traffic. These open protocols also support network-wide policy enforcement—that follows users no matter where they log onto the network: remotely over an SSL VPN, from a branch office, or within headquarters.

When a policy violation is detected, such as a user promulgating a worm, the local integrated services platform and Ethernet switch(es) can take action, informing the user that his/her machine has been quarantined, disconnecting the user from the production network, and directing him/her to a remediation server. Across the distributed enterprise, network and security devices share what they know about the threat and take corrective action, ensuring that malicious traffic doesn't propagate.

For more information about open standards, go to [Veer's Technology Feature—New Standard Lays the Foundation for Coordinated, Multi-Vendor Security](#)

The power of consistency

Rather than treating remote sites like “stepchildren,” successful enterprises recognize that the right IT infrastructure is fundamental to realizing the full value of

all of their work centers. Next-generation solutions are more comprehensive yet flexible enough to enable distributed enterprises to connect, secure, and manage their work centers consistently, increasing employee productivity and enterprise agility.

These new services gateways and switches consolidate functions and deliver high-end functionality at entry-level price points, making it possible for enterprises to deploy them widely. Features such as a single OS and management system further reduce total cost of ownership by lowering operations overhead. And by delivering network services without boundaries, next-generation work center solutions help enterprises retain customers and enhance value across all enterprise sites. **VEER**



View a brief video on the distributed enterprise at www.juniper.net/us/en/solutions/enterprise/

Tell us what you think of Veer.

[Take a Short Survey](#)