Solving Security Challenges with SteelConnect

Businesses and users today are hyper security-aware. Unfortunately, training users and businesses to be aware of how data and personal identities are stolen does not stop or protect against the hacking, the digital thefts, breaches with direct access to the Internet, or the need for safeguarding data at rest and in flight. Something must change in the way threats, intrusions, breaches, and lapses are handled in protecting digital and cloud information.

Hacking and "black hat" hackers are now a multi-billion dollar industry. "Crimes in cyberspace will cost the global economy $445 billion in 2016—more than the market cap of Microsoft ($411 billion), Facebook ($314 billion), or ExxonMobil ($332 billion)—according to an estimate from the World Economic Forum's 2016 Global Risks Report.[1]" No one is immune to hacking.

What's the answer to these threats and challenges?

[1] An Inside Look at what is Driving the Hacking Community http://www.cnbc.com/2016/02/05/an-inside-look-at-whats-driving-the-hacking-economy.html, CNBC, Feb 6, 2016

Any security approach must include the following key ingredients:

- Built-in architectural security robustness
- IPSec VPN (AutoVPN and encrypted data)
- Hardened management and access control
- Automation and minimized attack surfaces
- Secure access for guests
- Visibility

"Security must be deployed at the gateways to the internet, at the end points, the edge and core of the data center whether physical or cloud, the core of the network plus mobile traffic, and the branch office – all of this has part of the platform and deep into all areas of the infrastructure. Seeing a threat in one area of your infra-structure and telling other areas how to respond is increasingly important. Of course, you can't do it with people where they have to reconfigure everything. It has to be automated throughout the entire infrastructure."
~ Nir Zuk, CTO of Palo Alto Networks, Riverbed Disrupt, Fall 2016

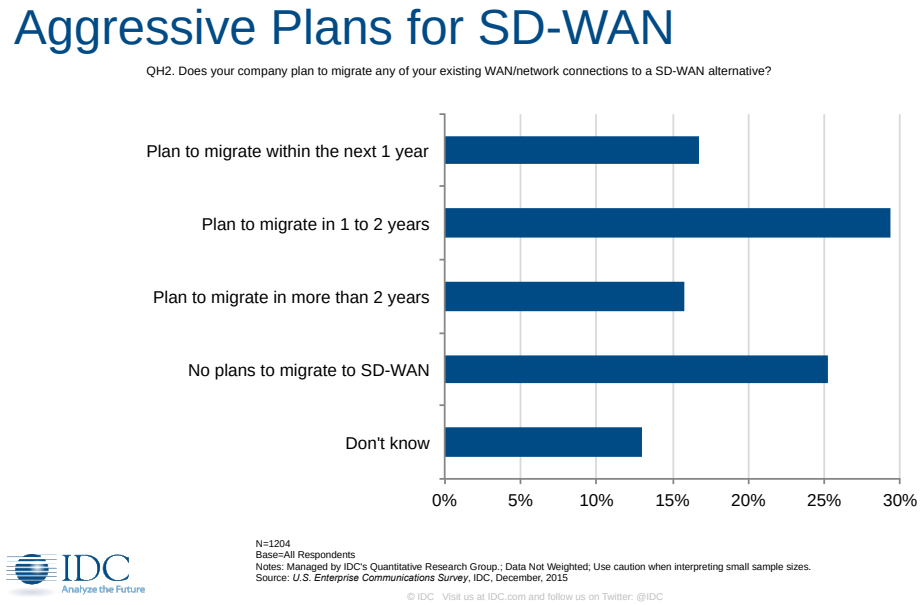

Figure 1
Surveyed Executives Plan to Migrate to SD-WAN. From "The Future Of The WAN Is Software-Defined, IDC/Forrester 2016.

Coupled with these key security ingredients, Riverbed® SteelConnect™ offers a unique approach that is simple and easy to use, thus delivering a new kind of security:

Security that is intrinsic to the SteelConnect system architecture and appliances.

Security that is centralized.

Security that is easily automated.

The Promise of SD-WAN

"SD-WAN is a new and transformational way to architect, deploy and operate corporate WANs, as it provides a dramatically simplified way of deploying and managing remote branch office connectivity in a cost-effective manner," according to Gartner.[2]

And businesses seem to agree with this prediction: 30% plan to migrate to SD-WAN within 1-2 years according to IDC/Forrester (Figure 1).

One of the driving forces towards SD-WAN is the desire for better security. According to an IDC/Forrester survey, current WAN architectures don't meet the top technology priorities.

> "Network managers place high importance on security, high bandwidth capacity, and reliability, but their current WAN architectures fall short of the ideal. Compounded with legacy challenges, network managers reported that hybrid WAN architectures exacerbate the problem of ensuring consistent security and performance in a cost-efficient manner. Deploying new applications and delivering highly available connectivity are also key challenges."

In fact, 89% of those interviewed said security was the #1 priority, and 55% said managing security across public and private connections was the #1 priority for the branch. [3]

[2] Gartner, July 2015 "Technology Overview for SD-WAN"

[3] IDC/Forrester, "The future of the WAN is Software-defined. Software-defined WAN gives network managers better control over their networks to ensure security, reliability, and cost efficiency, " 2016

SteelConnect and Security

SteelConnect is the cornerstone of Riverbed's solution for next-generation, application-defined enterprise networking where the network adapts to application requirements. SteelConnect dramatically simplifies and streamlines the process of designing, deploying, and managing distributed networks, enabling organizations to modernize and secure their network architecture to realize the full potential of digital and cloud transformation. Riverbed SteelConnect is a complete SD-WAN system for securely connecting users and business to the applications they need, wherever they reside—on a remote LAN, in a data center, or in the cloud. SteelConnect provides a fully integrated line of secure WAN SteelConnect Gateways, remote LAN SteelConnect Switches, and WiFi SteelConnect Access Points, all managed centrally within SteelConnect Manager's single and intuitive user interface.

SteelConnect has several key differentiators:

- Ubiquitous and unified connectivity across LAN, WAN and Cloud.
- Business aligned orchestration for fast, agile and secure application delivery.
- Unique cloud-centric workflow and easy menu-driven network design of sites, zones, uplinks, and rules. It leverages an easy-to-implement, intent-based and application-centric global business policy for users and devices—or groups of either, as well as provides centralized management.

Most importantly, SteelConnect offers integrated policy-based security.

SteelConnect security highlights include, for example:

- **Built-In Security**—Security was part of SteelConnect's design—not added later to respond to security breaches. For example, the management console port typical of a router-based approach simply does not exist for SteelConnect, thus reducing attack/vulnerability surfaces.
- **Policy-based approach** to designing SD-WAN overlays and security over the overlays. There are 3 types of policy in SteelConnect – traffic rules (what user should take what path using which app), security rules (what inbound/outbound rules do I want to apply to user and application traffic) and hardware port assignment rules (Port 5 is assigned to Zone X). Not only is security designed within SteelConnect Manager, but it can be easily deployed, managed, and changed universally throughout the system—without any command-line interface (CLI) configuration that is often prone to human error.
- **Service Automation, Including Security**—A centralized, secure, global management system based on a single global policy automates services and is easily changed for rapid response to changing conditions or new needs.
- **Simplified and Secure Access**—both guest and branch. User identity-based control provides an easy and intuitive way to define network access. You can identify users by name, roles, or job functions. Centralized support for embedded security, firewalls, access points, and switches simplifies and consolidates the overall management of branch equipment.
- **Visibility**—Offers a unified at-a-glance view of your network topology, including registered and online appliances. It also provides continuous automatic monitoring of network events, site, and tunnel status. Integration with Riverbed SteelCentral Insight for SteelConnect (formerly SteelCentral NetProfiler for SteelConnect) offers new SD-WAN reporting and troubleshooting capabilities.

Building In Architectural Security Robustness

SteelConnect SD-WAN is an alternative approach to designing and deploying enterprise WANs. SteelConnect is architecturally different from traditional WAN deployment architectures.

SteelConnect pointedly and uniquely avoids the notion of multiple control planes and multiple controllers. Instead, SteelConnect conflates the control plane function into the SteelConnect Manager for ease and speed of design

and deployment. With SteelConnect, customers see the Control Plane and SteelConnect Manager as a single solution, separate from the data plane that SteelConnect Gateways, Switches and Access Points execute.

SteelConnect components handle the following functionality:

- **Management Plane**—SteelConnect Manager, a single, global management system for all SteelConnect systems
- **Control Plane**—Unique software control modules within SteelConnect Manager and within the appliances, including SteelConnect Gateways and SteelConnect Access Points, that enable WAN network control operations
- **Data Plane**—Secure SteelConnect Gateways, SteelConnect POE LAN Switches, and SteelConnect WiFi Access Points

Traditional WANs often added security to the architecture after the original design. SteelConnect delivers complete security integration from the start of the design. Security is a core tenet of SteelConnect Manager's configuration profile resulting in one approach across all devices and planes, woven into an overlay network.

Secure Management—SteelConnect Manager

SteelConnect Manager is a cloud-based, multi-tenant management portal hosted as a service in Riverbed's Cloud, or as a self-hosted virtual appliance in the customer's private cloud.

SteelConnect Manager is a singular management and visibility system on a global scale; it is the tool that allows the definition of application-based security and traffic path policies. With it, you always have a clear picture of your network. By deploying a centrally managed system of products designed from the ground up to work together, you get a complete, unified view into your application and network health.

Many competitive industry offerings that use the label SD-WAN do not provide a centrally managed system. SteelConnect implements a single centralized, global management system for any WAN—MPLS, Internet VPN, public Internet, branch LAN, cloud-based resources and any combination of them.

With SteelConnect Manager, you can design a virtual network with a simplified workflow before touching any hardware by using the concept of a shadow appliance. IT can easily create sites, zones, uplinks, shadow appliances, and hardware assignments virtually, leveraging the global policy and built-in application intelligence, and then automatically deploy and provision remote resources without touching the physical appliance. This is true zero-touch deployment (Figure 2)

Application Intelligence

SteelConnect offers unique Application Intelligence where it identifies and classifies over 1300 applications, automatically leveraging deep packet inspection. The application database is used with policy rules enforcing the security for applications or groups of applications, the steering of applications, and metrics-based reporting. With application intelligence, you can enforce performance SLAs and security for each application regardless of source/destination.

Figure 2 SteelConnect Manager's Simplified Workflow

Applications are networked services that run in the internal network or on the Internet. Application definitions are a way to attach a business relevancy to all traffic that goes through your network. A separate application definition allows you to make multiple policy rules using the same application.

You can regulate access to applications using policy rules. For convenient rule and policy creation, SteelConnect Manager predefines a number of Application Groups such as Business or Web Services. When you use an Application Group in a traffic path rule, a single rule handles many applications based on similar properties. For example, the Business Voice application group classifies all traffic that requires low latency and a high queue priority, while the Recreational Application Group may require little or no security and low priority. Application Groups simplify management using policy rules, including policy rules for security.

Hardened management and access control

Management with SteelConnect is applied centrally—with no device-level access.

SteelConnect Manager offers a hardened console and access control that is user- and identity-based. SteelConnect Manager enables policy enforcement based on user identity—not just the IP address, for secure direct access, control of access, and the ability to ensure the same experience on all the user's devices.

All communication between SteelConnect Manager and the appliances (gateways, switches, and access points), as well as all interoperating services inside of SteelConnect Manager, are protected through HTTPS and x509 certificate validation. These Riverbed-owned certificates are exchanged and validated for authenticity (Figure 3).

With the exception of the agent VPN clients, all communication is sourced from the site out to the SteelConnect management service. There's no need to set up elaborate firewall or forwarding rules to establish the dynamic full mesh VPN or to gain connectivity to the Cloud. After you register an appliance, it receives its assigned configuration automatically.

Intent-based policy including security

SteelConnect Manager removes human error by eliminating manual CLI-based configuration of routers, creates network overlays with policy including security policy independent of the network underlay, and allows IT to automatically and securely provision resources remotely.

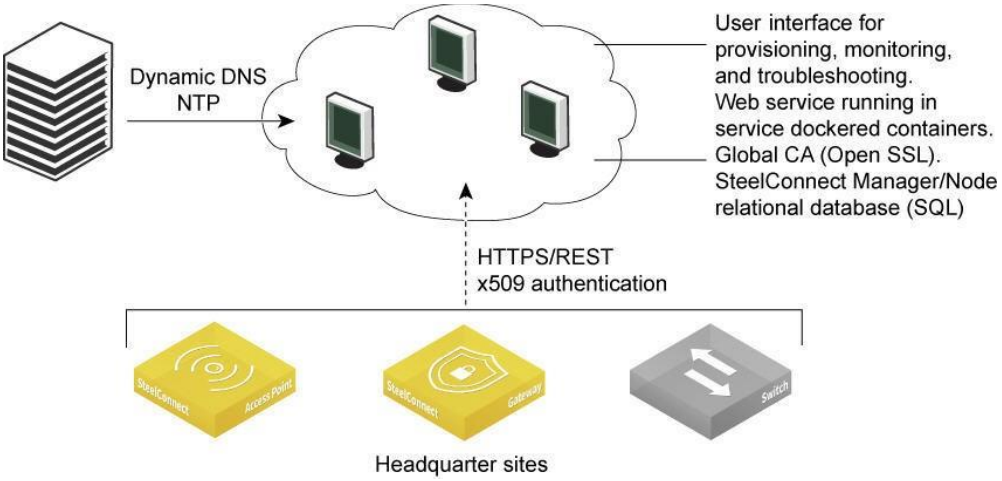

Figure 3 SteelConnect Registration and Communication

Change management across the enterprise requires only a change to policy that includes traffic, security, and port policy.

Establishing a security policy

Before deploying SteelConnect hardware, you need to establish a policy that the sites have permission to recognize each other. Because the traffic is going to be transiting zones, create an outbound/ internal rule within a policy that allows this. To create a policy rule, it's as simple as choosing a new policy rule for all users excluding guests. Under Applications / Targets, choose selected zones. And then choose all the LANs except the guest LAN in the headquarters to make them accessible from the users/zones. The rules match on the source and destination selected.

To make the zones reachable over WiFi, you can add a short name, or service set identifier (SSID), that contains the WiFi definition with authentication options. An SSID distinguishes one wireless network from another. By default, an SSID uses WiFi protected access 2 (WPA2) for security. A default SSID also includes a randomly generated password. Changing the default password secures it and makes it easier to remember. Optionally, you can authenticate against RADIUS/NPS servers. After adding the network SSIDs, you can broadcast them by site.

Unified Views

SteeConnect Manager offers unified, end-to-end views of users, devices, and groups of either, thus minimizing security risks by easily identifying new devices and users on the network and what they are doing.

Secure Control

Fundamental to the secure operations of SteelConnect is the establishment of a secure overlay Virtual Private Network (VPN) and security policies for traffic flows. SteelConnect Manager performs the setup and enforcement of overlay networks and policies. Based on the sites and WANs available, SteelConnect Gateway automatically calculates a route map through a process referred to as AutoVPN.

AutoVPN (Full Mesh and Hub and Spoke)

SteelConnect Gateways delivers AutoVPN full-mesh or Hub and Spoke VPN connectivity with a simple click, thus securing and fully automating WAN connectivity between local area networks, data centers, and home offices. It ensures secure application delivery from Cloud to WAN to LAN that works over any network underlay such as Multiprotocol Label Switching (MPLS) and Internet.

The AutoVPN, based on IPsec with AES 256 encryption, is a fast way to create a resilient, secure VPN backbone between all your sites. You can deploy AutoVPN between gateways, between an access point and gateway, between access points, as well as connect to a third-party VPN (ClassicVPN). Secure, encrypted AutoVPNs are supported over all WAN types including Internet and MPLS.

In addition to the establishment of AutoVPN and ClassicVPN, SteelConnect Gateway (control plane) maps and enforces security policies onto the appropriate overlay VPN.

Zones and secure Interconnection

A zone is equivalent to a Layer-2 IP segment within a site. Every site has at least one zone and can have multiple zones. When you create a site, SteelConnect automatically adds a default zone. AutoVPN interconnects zones via secure encrypted overlay tunnels in accordance with service policies set up in the management system (SteelConnect Manager). AutoVPN supports both L3 route (RouteVPN) and L2 bridge (Switch VPN) interconnection of zones.

With AutoVPN overlay, SteelConnect Gateway controls zone policy interconnections and enforces them. SteelConnect Gateways, Switches and Access Points (data plane devices) execute packet-level data manipulations.

Sustained appliance communications with Connectivity Loss

In the event that SCM goes down/loses connectivity, all SteelConnect appliances (gateways, switches and

access points) can still communicate with each other and establish VPNs to continue to operate, while network policies continue to be enforced—one of the advantages of an out-of-band control plane.

Secure Data Plane—Secure Appliances and Transport

SteelConnect Gateways offer the benefits of software-defined networking (SDN) automation coupled with the ability for customers to protect their privacy using IPSEC. The gateway appliances allow you to easily set up a secure connection between local area networks, data centers, and home offices.

SteelConnect Gateways provide fundamental network services to zones and handles one or more uplinks either by concurrent use or as backup, as well as enables policy enforcement, extended reporting for connected zones, and automated VPN.

SteelConnect Gateways provide dynamic native routing, firewalling, live threat protection, simple network services to zones, policy enforcement including enforcing security policies, automated VPN based on IPsec with AES 256 encryption, and extended reporting. VPN links are constantly monitored, and traffic is included in policy controls.

Router replacement

SteelConnect has the ability to eliminate or reduce the use of routers as another point of entry for security intrusions and breaches. SteelConnect Gateways can coexist with branch (customer edge) routers or replace the router with SteelConnect's native routing, thus eliminating time spent manually coding CLI for the legacy router configuration. By using SteelConnect Gateways as routers, customers benefit from SteelConnect's ability to eliminate network complexity with its design-first approach and its centralized, policy-based management, including security policy.

Distributed firewalling

SteelConnect Gateways enable next generation user- and application-based firewalling in a distributed fashion since one central policy is applied organization-wide (or globally) against all network resources. SteelConnect also works in combination with existing firewalls and switches, extending existing installations with new functionality.

The SteelConnect Gateway firewall functionality provides excellent branch firewall capability, negating the need for a separate firewall in the majority of branch situations. SteelConnect Gateways are not intended to provide Unified Threat Management (UTM) functions, but will work with them when the customer chooses to deploy them, which is typical in data center environments.

Network zoning (Network segmentation)

Based on policy, zoning provides unified segmentation of LAN and WiFi users and devices–-dynamically and in all locations. Organization-wide virtual SteelConnect network zones reduce attack surfaces and contain possible breaches.

When SteelConnect Gateway is handling gateway functionality for a zone, it will provide DHCP, NTP and DNS services automatically. It also provides security for devices and reporting functionality for connected zones.

Hardening: Automation and Reduced Attack Surfaces

In addition to providing robust security features, SteelConnect's system has been architected to reduce exposures that would otherwise have to be secured. Tools used to harden the system include automated operations and minimized attack surfaces. This strategy applies to all SteelConnect appliances as well as SteelConnect Manager. For instance, SteelConnect Switches automate deployment of the VLAN and XLAN configurations, eliminating manual configuration errors and enabling automatic network trunking. SteelConnect Switches are enabled with advanced features that allow IT administrators to efficiently design, deploy, and operate distributed LAN and WiFi infrastructures and to do so in a secure manner.

Here are some examples of the hardening approach used in SteelConnect:

- **Attack Surfaces**—Role-Based Access Controls prevent certain UI options from being displayed to lower RBAC categories
- **Automation (via profiles) that significantly reduces the possibility of configuration errors and security holes**—The organization-wide automated deployment of VLANs reduces attack surfaces and contains possible breaches, thus increasing security
- **Zero-Touch Provisioning**—Non-technical personnel can quickly install a switch without the need for on-site, error prone manual configuration
- **Cloud Stacking**—Ports are managed across the entire network as if working with a single switch. The ports are highly secure since only known and allowed devices can obtain network access. Authentication is through MAC learning or 802.1x (wireless)
- **Port Visibility**—Global view of all switch ports and connected devices provides an always current network inventory
- **Guest and Bring Your Own Device Ready**—Control over wired and wireless device proliferation is enabled using captive portals and authenticated user self-enrollment/self-registration
- **Auto Trunking**—Self-configuring trunk ports between appliances eliminate VLAN configuration errors and security holes

Secure Access for Guests and Branches

User Identity Control

SteelConnect Manager provides an easy and intuitive way to define any network access by user identity. SteelConnect associates those accessing the networks with the devices they are using, providing granular and automated user-to-device assignments, with an interface in each zone.

You can identify users by name, roles, or job functions. You also can add users manually or automatically populate them using directory synchronization with Windows Active Directory or Google Apps. You can perform Active Directory synchronization for corporate users even if they are in a remote location such as a branch.

User identity control is central to allowing direct Internet access, since direct Internet access is not a VPN based on IPsec with AES 256 encryption and thus is inherently less secure. Direct Internet access poses security challenges that include network isolation, data confidentiality/integrity, intrusion/attack prevention, content inspection and malware detection.

Secure Access Points

SteelConnect Access Point (AP) appliances provide secure enterprise-grade mobility and WiFi for guests, employees, and internet-enabled devices across all locations. Organizations assign users to a virtual network zone only once. From then on, these virtual zones automatically follow users across all locations, no matter which device is used. Smart roaming streamlines connectivity handover between access points and sites, and user-based network access control secures bring-your own-device (BYOD) environments.

With SteelConnect, Guest WiFi access utilizes authenticated (via the authentication portal or social media) and identity-based registration and then directs all guest traffic over the Internet—with a firewall between the guest zones and the internal zones. Guest restrictions are based on the policy attached to each guest device. For maximum convenience and secure control of device proliferation, guests can self-register each device in a matter of minutes, and then the administrator attaches the security policy to each device registered by that user. Web content restriction and malware filtering are also based on the SteelConnect policy you set up.

While the guest network is never able to connect to the secured corporate zones or VPN, secure SteelConnect Access Points can be used to create remote WiFi, extending the enterprise WAN to home offices over public Internet connections.

Visibility for Security

You can't protect what you don't see. That is why SteelConnect has made ubiquitous and industry-leading visibility a key ingredient of its approach. SteelConnect Manager provides a unified view of users, devices, and groups of either. You can quickly identify what traffic is consuming bandwidth. Because SteelConnect Manager automatically detects new devices and users, you can minimize security risks. The dashboard offers a unified at-a-glance view of your network topology, including registered and online appliances, and new events. It also provides continuous automatic monitoring of network events, site, and tunnel status.

Network visibility provides this information to manage network workflow:

- An activity log by user and application
- DHCP address assignment
- IP address by user
- IP address by device
- User location and WiFi information
- Full visibility into what's occurring in the network, in real time
- Any blocked connections
- A list of unknown, detected devices with their OS, vendor, and owner information, if it's available

In addition, SteelConnect includes support for Riverbed SteelFlow export (Netflow-like data) to Riverbed SteelCentral Insight for SteelConnect (formerly SteelCentral NetProfiler for SteelConnect), enabling SteelConnect and SteelCentral Insight to communicate and exchange information with each other.

With SteelCentral Insight, IT has a centralized, dynamic view and understanding of an enterprise's application and SD-WAN performance environments. SteelCentral Insight provides analysis of the flow data into information reports and problem–focused troubleshooting. It offers path quality and QoS reporting with events overlaid on reports and four SteelConnect SD-WAN specific views and reports, including:

- **Overall organization's network summary**— provides detailed usage information about links, applications, and users
- **Site summary**— shows overlay and underlay views, top users, and top site interactions
- **Application summary**— helps you understand how apps are being used, where, and by whom
- **User summary**— provides a breakdown of the users' activities

The ability to validate policies, especially security policies, are working as expected, troubleshoot problems quickly, and plan for changes can help ensure the success and security of your SD-WAN.

Conclusion

Companies trying to realize the promise of the cloud and SD-WAN know that they must place an equal emphasis on security to achieve business agility and cost efficiencies. Vigilance, strong system-wide and built-in security, and business partners who are equally dedicated to keeping hackers and intruders away from the business and customers are the core of a networking, datacenter, branch and cloud defense.

Not only does Riverbed build strong security into its hardware and software for a secure IT profile but it also has joined forces with the leaders in security and secure solutions such as Zscaler for providing protection from malware, viruses and other Internet threats in real time over the Internet; Palo Alto Networks with a next generation security platform that detects and prevents advanced cyberattacks; Amazon Web Services (AWS) with its security profile that offers more controls and compliance, scales with you, and keeps data safe in AWS data centers; and Microsoft Azure with its embedded security and privacy, transparency, and compliance.

Riverbed is ensuring the most recent advances in security are available now and in the future as part of its own product portfolio and through its partnerships in anticipation of increasing security demands wherever people do business.

For more information, please visit:
riverbed.com/steelconnect

About Riverbed

Riverbed, at more than $1 billion in annual revenue, is the leader in application performance infrastructure, delivering the most complete platform for the hybrid enterprise to ensure applications perform as expected, data is always available when needed, and performance issues can be proactively detected and resolved before impacting business performance. Riverbed enables hybrid enterprises to transform application performance into a competitive advantage by maximizing employee productivity and leveraging IT to create new forms of operational agility. Riverbed's 27,000+ customers include 97% of the *Fortune* 100 and 98% of the *Forbes* Global 100. Learn more at Riverbed.com/SteelConnect