riverbed

Solution Brief

Software-Defined Security for Robust Branch Protection

Increasingly, the branch or remote office is becoming a common entry point for cyber-attacks into the enterprise. The attack landscape has only broadened and become more sophisticated. However branch security architectures have not significantly evolved.

Point security appliances, usually firewalls or unified threat management (UTM) devices or add-on software in a branch router are used to approximate data center security at the branch.

With each passing day, security breaches and attacks are getting more sophisticated and frequent. Due to the rise of cloud-based applications and IoT (e.g. cloud managed HVAC or production line network sensors), the branch office is emerging as a point of concern that can potentially open the entire enterprise to a host of vulnerabilities from the outside.

Securing multiple globally distributed branch offices can get expensive and complex. Backhauling all branch traffic through a centrally deployed firewall in the datacenter often results in additional latency impacting application performance and frustrating end users.

Enterprise IT can either manage network security in-house or consume it as a fully managed security service. Regardless of in-house or outside management, there are various challenges to address when multiple security technologies are deployed as separate resources in the branch.

A recent Ernst and Young security survey[1] found that organizations are spending more on cybersecurity, devoting increasing resources to improving their defenses, and working harder to embed security-by-design. More than three-quarters (87%) of organizations do not yet have a sufficient budget to provide the levels of cybersecurity and resilience they want. Protections are patchy, relatively few organizations are prioritizing advanced capabilities, and cybersecurity too often remains siloed or isolated.

[1] Ernst and Young Global Information Security Survey 2018-19

76%

Increased their cybersecurity budget after a serious breach

53%

Have no program - or an obsolete one - for one or more of the following:

- Threat intelligence
- Vulnerability identification
- Incidence response
- Data protection
- Identity and access management

17%

Of organizations report a list of breaches in their information security reports

8%

Of organizations have information security functions that fully meet their needs

38%

Would be unlikely to detect a sophisticated breach

34%

Of organizations see careless/unaware employees as the biggest vulnerability

46%

Had no incidents (or don't yet know about them)

51%

Are spending more on cyber analytics

Source: EY Global Information Security Survey 2018-19

Enterprise Security Challenges with Legacy WAN

The legacy branch office network is increasingly becoming the most plausible target for cyber-criminals. The typical branch has evolved to become the hub of major digital services for both business productivity and customer services. Businesses across multiple industries are adopting direct internet access (DIA) to facilitate multi-cloud services. Branch offices are hubs of activity, especially in the banking, financial services, retail and manufacturing industries.

While disruptive technologies, like the cloud and IoT, have broadened the attack surface, branch security architectures have not evolved at a similar pace. Juggling between users demanding faster and more effective ways to access business applications, and legacy WAN architectures that are unable to keep pace with real-time enterprise demands, IT teams are battling a broad set of challenges:

Cloud, IoT and the Public Internet:

The use of cloud-based services, SaaS adoption and IoT devices have increased dependence on public internet connectivity. Backhauling branch traffic to the corporate data center is counter-productive, and the latency impacts application performance. Additionally, different branch locations, office sizes and the type of applications the users work with, may require different connectivity types (e.g. internet vs. MPLS vs. hybrid).

The public internet is not secure enough for mission critical business applications. There are different security requirements per application, depending on where they are being accessed, and over what type of connectivity.

This adds significant complexity when using traditional security appliances to create a standard branch security model.

Complexity and Cost:

The branch office network landscape is complex. There are diverse systems and a variety of security technologies that, over time, have made their way into the branch. Cloud and IoT have added yet another layer of complexity.

Creating and implementing a security strategy for disparate systems and multiple hardware devices is expensive and requires a lot of time and resources. Procuring, deploying and managing point devices for different layers of security at locations without IT/security expertise, often results in very high Capex and Opex. Not to mention – the more complex the system, the more difficult it becomes to monitor, manage, maintain and secure against potential vulnerabilities.

Lack of Visibility:

Most branches currently use a range of connectivity solutions (MPLS, LTE, broadband). Then, there is an array of hardware and software components sitting atop this connectivity layer. Due to this diversity, third-party network monitoring tools often fall short in providing a unified and coherent picture of the networks in real-time. As a result, most organizations end up discovering a breach or an anomaly way after its onslaught. And as most security experts will testify, timely detection and remedial action is critical to minimize the impact of a security breach.

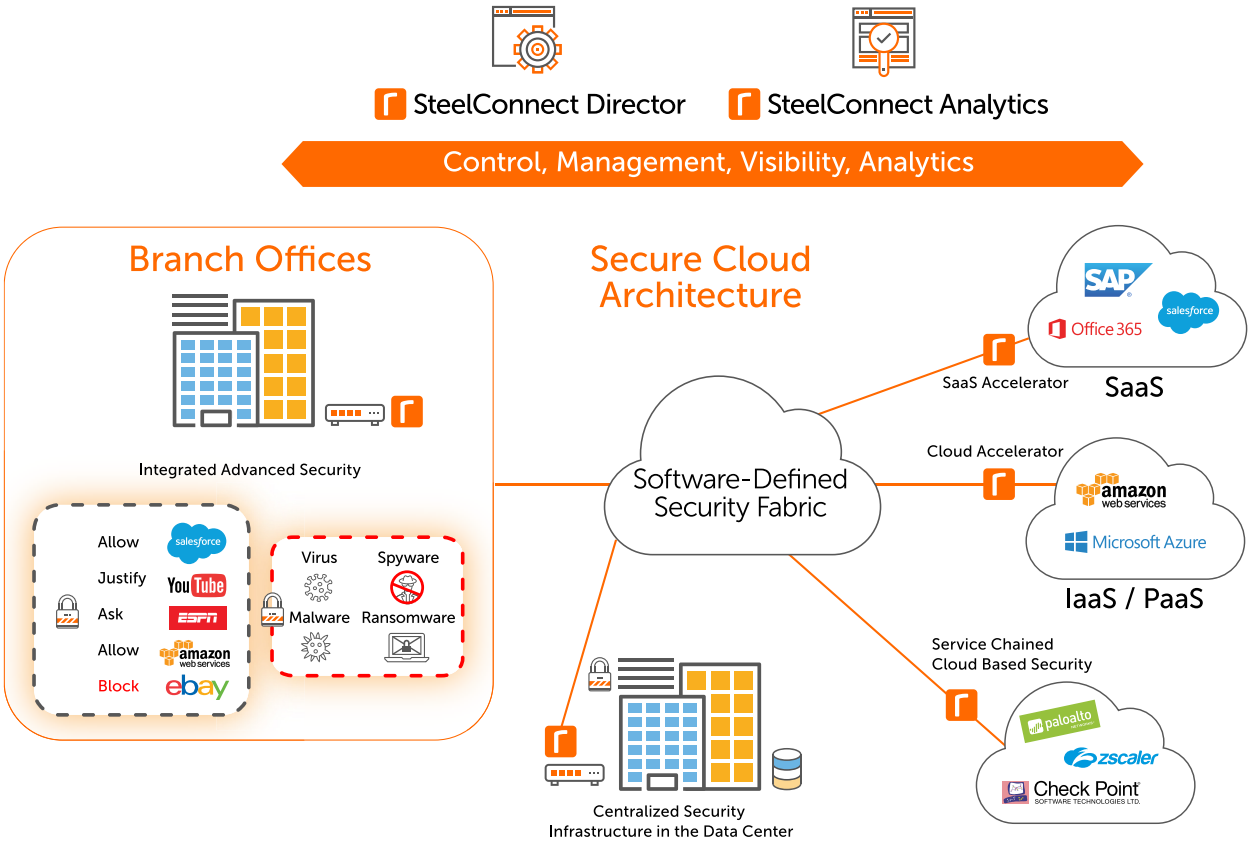
Decentralized Architecture:

Time-to-remediate is critical in the event of a security breach. Every minute lost gives the invader an edge and advantage to strengthen their attack. A centralized management console enables IT teams to dynamically apply role-based access, enforce security policies and configurations per application and centrally manage the security configurations around its applications and networks.

Riverbed® Software-Defined Security

While the issues with branch security are very real, emerging approaches can offset many of these challenges. Software-defined technology can significantly improve the deployment and management of security at the branch.

A core element of Riverbed® SteelConnect™ EX WAN-edge solution is the ability to "software-define" security functions and operations (e.g. policy creation and enforcement). Our software-defined security architecture provides greatest flexility to deploy various advanced security functions on-demand within the SteelConnect EX platform or service chain with on-prem or cloud-based 3rd party security services.



Here are the key features of Riverbed's SteelConnect EX that help enhance branch security:

Flexible and Distributed Security Services Architecture

IT teams can decide where to run each layer of required security – either on-premises in the branch office, or centrally in the data center or in the cloud. For example, compute-intensive services such as malware sandboxing, intrusion prevention (IPS) and AV filtering can be run centrally, while key branch services like firewall and secure web gateway, can be run locally, with the overall set of layered security services defined with a simple policy template.

Contextually Aware Security Fabric

A key aspect of Riverbed's software-defined security is the contextual intelligence and awareness of users, devices, sites, circuits and clouds; enabling robust and dynamic policies to achieve a multi- layered security posture. For example, IT teams can deploy contextual network and security policies for specific users and devices, like anti-virus and URL-filtering, when utilizing certain site-to-site or internet links. IT security teams can set unique security policies, differentiated services or security service-chains for guest access, corporate access and partner access networks at the branch. This enables the enterprise to meet business security and compliance policies—all with a single unified software platform.

Elasticity

With a software-based model, IT teams can easily and dynamically scale capacity without having to replace proprietary security appliances. For example, a branch firewall can be doubled in capacity in minutes either automatically or using commands from the central provisioning portal, without a truck roll or firewall appliance swap-out.

Centralized and Automated Operations

One of the biggest benefits of software-defined security is that it delivers services from a single point of control, avoiding the need for on-site skilled personnel. Services can be deployed, and capacity can be increased without any on-site presence, hardware refreshes or manual provisioning. Also, if a site(s) requires a different set of security functions, it can be serviced individually from a single management portal within a few minutes instead of hours or days.

World-Class Security with Service Chaining

Riverbed provides IT teams the greatest flexibility to deploy advanced security on-demand. Organizations can pick and choose security services from advanced security integrated within SteelConnect EX, centralized security infrastructure in the data center and/or 3rd party cloud-based security solutions with flexible service chaining.

Up-to-date Protection

Riverbed continuously monitors for new security threats to identify and eliminate potential vulnerabilities. Riverbed collects intelligence from multiple sources (internet resources, commercial feeds such as TELUS and internal research) to keep track of the latest viral outbreaks and emerging threats. By continuously updating the threat libraries and automating the updates, Riverbed insulates its customers from attacks.

Riverbed's SD-WAN solution was built from the ground up, fully programmable and automated, and with integrated security, not as just another added feature or external bolt-on service. Security is an integral part of the Riverbed's software technology.

To learn more about Riverbed secure SD-WAN, visit riverbed.com/enterprise-sdwan.

Riverbed SD-WAN Security Functionality	
Stateful Firewall	Zone-based Firewall, support Address Objects, Address Groups, Services, Geo-Location, Time-Of-Day, Rules, Policies, Zone Protection, DDoS (TCP/UDP/ICMP Flood), Syn-cookies, Port-scans, ALG support, SIP, FTP, PPTP, TFTP, ICMP, QAT support.
Application Visibility	Identifies more than 3000 applications and protocols, Supports Application groups, Application filters, Application visibility and log.
Next-Generation Firewall	Policy Match Triggers: Applications, App Filters, App Groups, URL Categories, Geo Location, Application Identity based (AppID) policy rules, Application Group and Filters, Packet Capture on AppID, IP Blacklisting, Whitelisting, Custom App-ID signatures, SSL Certificate-based protection, Expired certificates, Untrusted Cas, Unsupported cyphers and key lengths, Unsupported Versions, NSSLabs Recommended Rating.
IP Filtering	Filtering of traffic based on Geo-Location, DNS name, Reputation of Source/Destination IP Addresses – support for both IPv4 and IPv6. Automatic updates of IP Reputation database.
URL Categorization and Filtering	URL categories and reputation including customer-defined, Cloud-based lookups, Policy trigger based on URL category, URL profile (blacklist, whitelist, category reputation), Captive portal response including customer defined, Actions include block, inform, ask, justify, and override.
Anti-Virus/Malware Protection	Network/Flow based protection with auto signature updates, HTTP, FTP, MTP, POP3, IMAP, MAPI support, 35+ file types supported (exe, dll, office, pdf and flash file types), Decompression support, Storage profile support, Auto signature updates.
IDS/IPS	Default and customer defined signatures and profiles, Riverbed and Snort rule formats, L7 DDoS, Layer7 Anomaly detection, Support for JavaScript attacks, Security package with incremental updates, Full incremental (daily) and real-time threat (every hour), Lateral movement detection.

About Riverbed

Riverbed enables organizations to maximize performance and visibility for networks and applications, so they can overcome complexity and fully capitalize on their digital and cloud investments. The Riverbed Network and Application Performance Platform enables organizations to visualize, optimize, remediate and accelerate the performance of any network for any application. The platform addresses performance and visibility holistically with best-in-class WAN optimization, network performance management (NPM), application acceleration (including Office 365, SaaS, client and cloud acceleration), and enterprise-grade SD-WAN. Riverbed's 30,000+ customers include 99% of the *Fortune* 100. Learn more at riverbed.com.

riverbed

© 2020 Riverbed Technology, Inc. All rights reserved. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed Technology or their respective owners. MS-1372_RSW_SB_US_090220