Mitigating Branch Office Risks with SD-WAN
Branch Security Overview

The branch or remote office stands out as a point of vulnerability in an increasingly potent cyber threat environment. Despite the prevalence of more sophisticated malicious actors, branch security architectures, and the managed service offerings often used to deploy and operate them, have not significantly evolved in recent years. Point security appliances (usually firewalls or unified threat management [UTM] devices) or add-on software in a branch router are used to approximate perimeter data center security at the branch.

Security at the Branch: Enterprise Challenges

Enterprises with multiple branches today either manage their security devices in-house or leverage a managed service provider. Regardless, challenges emerge when multiple security technologies are deployed as separate resources in the branch:

**Cloud Apps**
Companies today have apps running both in the cloud and the corporate data center. If all traffic to and from cloud apps must be routed through the corporate data center for security functions, it will have a negative impact on system performance and end user experience.

**Network Connectivity**
Different branch office locations or sizes have different connectivity types (e.g., purely Internet vs. MPLS vs. hybrid). Thus, there are quite different security requirements depending on where the apps 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 of Ownership**
Having to purchase, deploy and manage point devices for different layers of security at locations where there is generally not any IT/security expertise available locally often results in very high CapEx and OpEx costs.

**Complexity and Risk of Error**
Having to integrate different layers of security together without minimizing overall protection.

**Lack of Agility**
Companies experience long deployment times due to hardware shipping and the scheduling of consultants or integrators to install, integrate and test equipment. This occurs not only at initial deployments, but also when capacity upgrades are required (e.g., if a new or larger WAN circuit is provisioned to a direct Internet access office, then a higher capacity firewall is required).
Leveraging Software-Defined Wide Area Networking

Recent technology advances can offset many branch office security challenges. Software-defined technology can significantly improve the deployment and management of security at the branch. In particular, virtualized network functions are evolving the previously hardware-centric network and security technologies into software-based solutions.

A core element of virtualized networks is the virtualized security or network function (VNF), which is a software-based, or virtualized version, of a specific function like a next-generation (NG) firewall. Much more than just converting from point hardware or appliances to virtualized software instances, VNFs are centrally managed and policy orchestrated, zero-touch provisioned, and service-chained, addressing many of the operational challenges noted earlier.

In essence, applying network virtualization and VNFs to enterprise security and managed security services results in the ability to “software-define” security in terms of both form-factor and operations / policy creation / enforcement. This is compounded by the fact that software-defined security created from virtualized networks de-couples security functions from proprietary hardware, enabling the use of security functions in software running on commodity x86 servers and white box appliances.

Taking an example of branch security, imagine an enterprise with a large number of geographically dispersed branch offices that needs to refresh or increase its branch security. Instead of scheduling new UTM or NG firewall appliances and shipping them to branch sites at the rate 20 per month (an aggressive schedule, at one installation per business day), and a project schedule of over 1.6 years. The enterprise or managed service provider can ship commodity white box appliances to 100 branches per month, and simultaneously activate and test 25 devices per week remotely, for a total project time of 4 months. The result is a far lower cost of deployment, as well as compliance and data protection delivered more than a year earlier.

Another key aspect of software-defined security using virtualized networks is the ability to service chain to easily achieve multi-layered security. For example, a service provider can service chain multiple security functions, like a NG firewall and a secure web gateway, to provide security for direct Internet access from the branch. As the service creation, service definition and service-chain rules are created using APIs, centralized orchestration, and management tools, each branch office security service is programmed to deploy in hours, instead of days or even months.
Centralized, Automated Operations

A software-defined, virtualized network-based approach to security also provides a way to deliver services from a single point of control, avoiding the challenging requirement for skilled personnel available on-site whenever needed. Instead, services can be deployed, capacity increased and enhanced with additional functions automatically, all without requiring any on-site presence, hardware refreshes or manual provisioning. Also, if a particular site 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.

Elasticity

When deploying branch security through a software-defined, virtualized network model, capacity can easily and dynamically be scaled up or down without having to replace proprietary security appliances. For example, a branch firewall can be doubled in capacity in minutes either automatically, or by using commands from the central provisioning portal, without requiring a firewall appliance swap-out.

Flexible and Distributed Service Architecture

With the advent of network virtualization, enterprises have the capability (and flexibility) to decide where to run each layer of required security — either on-premises in the branch office, or centrally in the data center or provider point-of-presence (PoP). For example, compute-intensive services such as malware sandboxing, intrusion prevention (IPS) and AV filtering can be run centrally, while services that are key in the branch, like firewall and web gateway, can be run locally, while the overall set of layered security functions are service-chained.
In summary, deploying SD-Security for the branch office involves adding additional layers of security for better defense-in-depth, when and where you need them. Adopting a software-defined and virtualized network-based approach gives enterprises and managed service providers the flexibility to deploy the right security functions necessary to meet an ever increasing complex threat landscape while reducing deployment times, operation complexity and significantly reducing CapEx and operating costs.

About CenturyLink Business
CenturyLink, Inc. is the third largest telecommunications company in the United States. Headquartered in Monroe, LA, CenturyLink is an S&P 500 company and is included among the Fortune 500 list of America’s largest corporations. CenturyLink Business delivers innovative private and public networking and managed services for global businesses on virtual, dedicated and colocation platforms. It is a global leader in data and voice networks, cloud infrastructure and hosted IT solutions for enterprise business customers.

For more information visit www.centurylink.com/enterprise.

About Versa Networks
Versa Networks was founded by network industry veterans Kumar and Apurva Mehta, who built the multi-billion dollar MX Series routers at Juniper Networks. Versa is an early innovator in the rapidly growing network function virtualization (NFV) market, which is forecast to grow to $11.6B in 2019 (Infonetics/IHS). The company has more than 35 patents in process around its unique system-level approach for creating virtualized network functions (VNF), a core NFV building block. Versa solutions enable service providers and large enterprises to transform the WAN and branch networks to achieve unprecedented business advantages. Versa’s VNF software provides unmatched agility, cost savings and flexibility vs. traditional network hardware.