SONICWALL®

EXECUTIVE BRIEF

Are Your Branch Sites an Open Door to Cyberattacks?

Why increased exposure, limited resources and rising costs demand secure SD-Branch

Abstract

Traditional methods of deploying and maintaining security at branch sites has become ineffective, expensive and unmanageable. An SD-Branch solution can form a cornerstone for boundless security in distributed enterprise environments.

An explosion of exposure points

SonicWall Capture Labs threat researchers recorded 9.9 billion malware attacks in 2019. For the last five years, cybercriminals overwhelmed organizations with sheer volume. Their objective was simple: cast as big a net as possible and reap the rewards. And as cyber defenses evolved, attacks have become more targeted, with higher degrees of success.

In addition, the network and security landscape are undergoing a digital transformation with the explosion of mobile and IoT devices. Hence, there is a trend of enterprises relying on mobile clients, creating mobile-first networks. Another catalyst to this change is the move to the cloud and adoption of cloud applications. With business-critical applications like MS Office moving to the cloud and companies leveraging cloud applications like Salesforce or Workday for their everyday tasks, it has become essential to secure these cloud applications. This digital transformation drives the demand for high-performance appliances that can keep up with the increasing data demands.

The ever-growing cost of connectivity

Mobile-first offices or branches rely heavily on high-bandwidth applications to perform day-to-day activities. It may be as simple as streaming video or other content or working on Office 365. Of these high bandwidth applications, some of them may be business-critical, while some of them are not. It is essential to segregate this traffic efficiently or it becomes prohibitively expensive: imagine having to backhaul all branch traffic over expensive MPLS links to corporate HQ.

Fortunately, expenses can be slashed by using low-cost Internet access for non-critical data traffic, while business-critical data traffic can be prioritized by dynamic path selection mechanism. However, some of these applications, critical to running a distributed enterprise or branch, would require redundant connectivity to ensure constant uptime.

One way to ensure redundant connectivity for these branches is to have a solution that provides high availability and high-performance WANs with WAN load-balancing. This can be achieved by relying on software-defined WAN (SD-WAN) technology.

By using low-cost Internet access (broadband, 3G/4G/LTE, fiber), organizations can cost-effectively replace expensive WAN connection technologies such as MPLS with SD-WAN. However, providing all this while managing the entire network security solution from a single pane of glass often becomes elusive.

Struggling with shrinking resources

The cost of conventional security is increasingly prohibitive and the shortage of trained personnel more acute. Constrained budget and staffing resources simply can't keep up and have created a cybersecurity business gap.

Multiple point products make it challenging for branches to deploy, configure, manage and troubleshoot the solution. Having an end-to-end security stack can unify firewalls, switches, access points, cloud security and end-point clients to provide a single-pane-of-glass management which amplifies cross-product visibility and control. This end-to-end security stack provides a strong, unified security posture.

Changing the way that you maintain networks is critical. You can keep up with this digital transformation by providing a strong security posture. Failing to provide a unified security posture will lead to complications for organizations to manage and control the growing number of devices on the network. There would be threats are failed to be identified and businesses will be forced to take a reactive approach as opposed to a proactive one.

Furthermore, deployment at scale can be challenging without technologies like Zero-Touch Deployment. Technicians would have to travel to these branch locations to manually configure each of these devices. This adds to the overall cost and time spent to roll out the solution across branches, perhaps spread out globally.

Also, branches as much as the corporate HQ need to provide secure wireless access that provides high-performance and superior user experience. Wi-Fi being ubiquitous employees and guest alike expect reliable, fast Wi-Fi performance.

Why you need SD-Branch

Today, evolution of technology at the branch is essential. Traditional branches cannot keep up with the increasing demands from multiplying mobile and IoT devices. With the proliferation of devices, management and security becomes a challenge as they may need different policies. Having unified policy across your LAN and WAN from a single pane of glass (SPOG) becomes critical.

Moreover, SPOG management can provide rich analytics comprehensively across the security ecosystem. As cloud adoption picks up, WAN connectivity across branches must be architected intelligently to leverage cheaper internet links over more expensive MPLS links, as well as enable Zero-Touch Deployment.

This brings about operational agility. Organizations can rapidly deploy and roll out devices with Zero-Touch Deployment capability, eliminating or reducing the need for skilled IT personnel to visit multiple branch locations to configure and deploy these solutions. To ensure continuity, integration and scalability, organizations optimally should seek streamlined SPOG management with services from a single vendor.

An SD-Branch solution augments SD-WAN to provide the next level of connectivity and flexibility. SD-Branch transforms SD-WAN technology into a tailored solution for branch office deployments. It adds more features and goes beyond dealing with connectivity between branch locations. SD-Branch encompasses SD-WAN, LAN connectivity and security. Further, Zero-Touch Deployment and SPOG management reduces the need of IT staff which further drives down operational costs.

Conclusion

Distributed enterprises struggle with securing branch sites due to increased exposure points, limited resources and rising costs. This all contributes to a growing cybersecurity business gap.

An effective solution combines the agility of SD-Branch with end-to-end security, network segmentation and compliance. This enables unified policies across the network ecosystem, providing granular security controls to identify and prevent today's stealthiest and never-before-seen attacks from compromising your network.

SonicWall sees SD-Branch as a cornerstone of boundless security for the hyper-distributed era. The SonicWall SD-Branch solution secures connectivity and transforms user experience at the branch office by delivering an integrated platform that enables branches to take advantage of cheaper connectivity (SD-WAN), enable BYOD, adopt SaaS applications, and connect to HQ or other branches. It integrates SD-WAN, Zero-Touch Deployment, single-pane-of-glass management, unified visibility and threat detection, next-generation firewalls, secure switches, wireless access points, endpoint security and cloud app security.

Learn more: Read our SonicWall SD-Branch Solution Brief.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

ExecutiveBrief-AreYourBranchSites-US-VG-1980