451 Research | Business Impact Brief

Security in SD-WAN: Centralized management means better control

The 451 Take

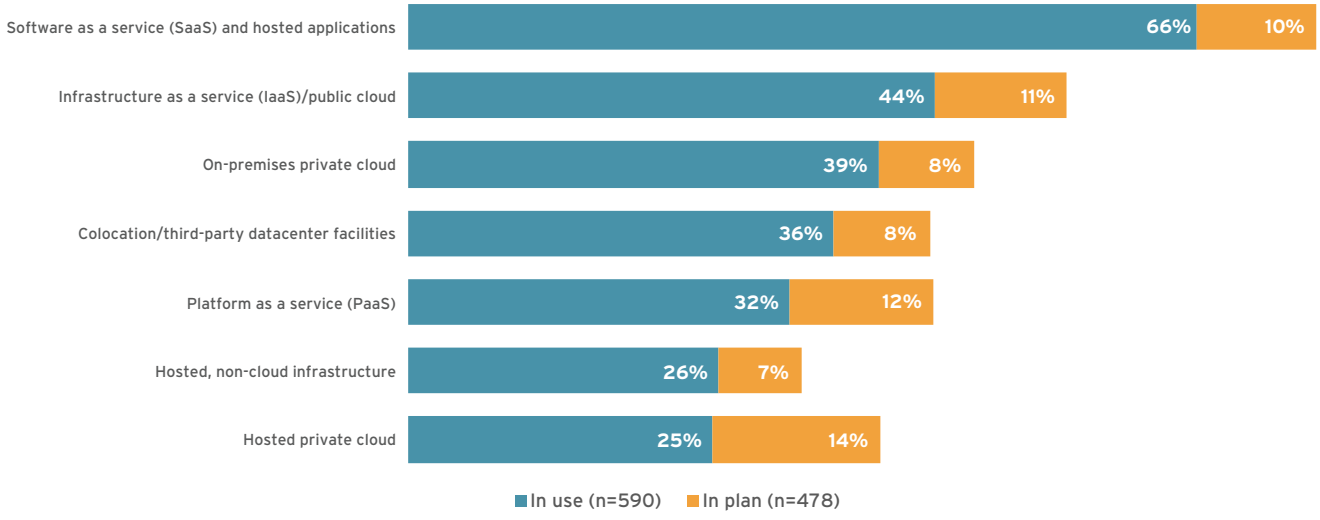
The migration of enterprise IT to the cloud forces organizations to consider a trade-off when it comes to networking. The internet provides a simple and inexpensive means of delivering traffic, but IP VPNs across private MPLS lines provide reliability and security that the internet lacks. One answer has been to implement software-defined wide-area networking (SD-WAN) to blend the options and help decide which traffic to send where. With security having become a more pressing enterprise concern, it only makes sense to consider the security of SD-WAN itself. The usual pattern in IT has been to implement a technology first, then add security to it. While this path could certainly be followed with SD-WAN, it would make more sense for the enterprise to onboard its SD-WAN with security already integrated.

The complexity of today's WAN stems from the fact that enterprise IT has distributed outward to multiple destinations. The public cloud is an obvious example – and, in fact, 72% of the enterprises using a public cloud are using more than one, according to 451 Research's Digital Pulse survey. But consider also services such as Salesforce, which, for networking purposes, can be thought of as additional cloud destinations. Overall, the number of cloud venues that the average enterprise reaches has increased in recent years. Further, enterprises expect to expand their usage of every type of cloud-based service, as indicated in a recent 451 Voice of the Enterprise survey.

Cloud and Hosted Services, in Use and in Plan

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Budgets and Outlook, 2019

Q: Which of the following types of cloud or hosted services, if any, does your organization currently use? Which does it plan to implement in the next 12 months?



451 Research | Business Impact Brief

The cloud isn't the only motivator for SD-WAN; the access network is transforming. A mobile workforce changes the shape of the modern branch office – employee access can originate from a home office, an airport lounge or a Starbucks. Separately, the Internet of Things is creating dense pockets of edge devices that will need network access. So, the situation is becoming more complex both in terms of who (or what) is accessing the network and what destinations they are connecting to. SD-WAN provides one platform to orchestrate all these permutations of connectivity.

But for any given IT technology, security has tended to be an afterthought. It is common for security functions to be added to a platform after it has been in use for considerable time. This bolted-on security can be clearly seen in the realm of networking, where functions such as firewalls and intrusion detection systems were initially introduced as stand-alone appliances.

This paradigm separates security and networking into silos, each with its own processes for visibility and control. SD-WAN would be no exception. If we simply add security elements to an existing SD-WAN platform, making no effort to integrate the two, we find ourselves with two sets of management tools, likely administered by two separate groups: networking and security. This would be especially likely if the security tools came from a separate vendor than did the SD-WAN technology.

This situation can be simplified by combining security functions with the SD-WAN platform. This convergence of security and networking would allow for SD-WAN to spin up virtualized security functions as necessary. In the context of customer-premises equipment (CPE), a modern SD-WAN CPE device should be well suited for hosting additional software functions such as virtualized security devices.

Business Impact

CONVERGENCE CAN IMPROVE SD-WAN SECURITY. By unifying the management of networking and security, the enterprise can avoid having gaps in its security posture. This can also help maintain a consistent security policy from the network core out to the branch.

REDUCED COMPLEXITY. A single management plane for SD-WAN and security avoids the complication of organizational silos. Moreover, security and networking teams can work more productively from a single 'source of truth.'

INCREASED AGILITY. Merged controls for networking and security can ease the process of responding to changes in the network. In addition to fluidly adding security elements, the enterprise can efficiently update security policies.

IMPROVED PERFORMANCE. With security built in, the SD-WAN platform does not have to route traffic through certain choke points in order to reach particular security elements.

Looking Ahead

The days of security as an add-on are waning. Security clearly should be integrated into systems and processes from an early stage to avoid a buildup of disparate security tools with separate control systems. Security shouldn't be yet another layer that's put on top of an increasingly complicated network stack. By choosing a converged SD-WAN and security platform, the enterprise can avoid adding one more facet of complexity to its already complex networking profile.

paloalto NETWORKS

Commissioned by Palo Alto Networks.

Palo Alto Networks, the global cybersecurity leader, offers secure SD-WAN for branches. Our native integration of SD-WAN and security simplifies operations and extends uniform protection from the data center and cloud all the way to the branches. Our global, cloud-native backbone enables high-performance connectivity while providing superior visibility and precise control of your network.

For more information, visit http://www.paloaltonetworks.com/network-security/sd-wan.

451 Research | Business Impact Brief

Making Secure SD-WAN Manageable: Take an Integrated Approach

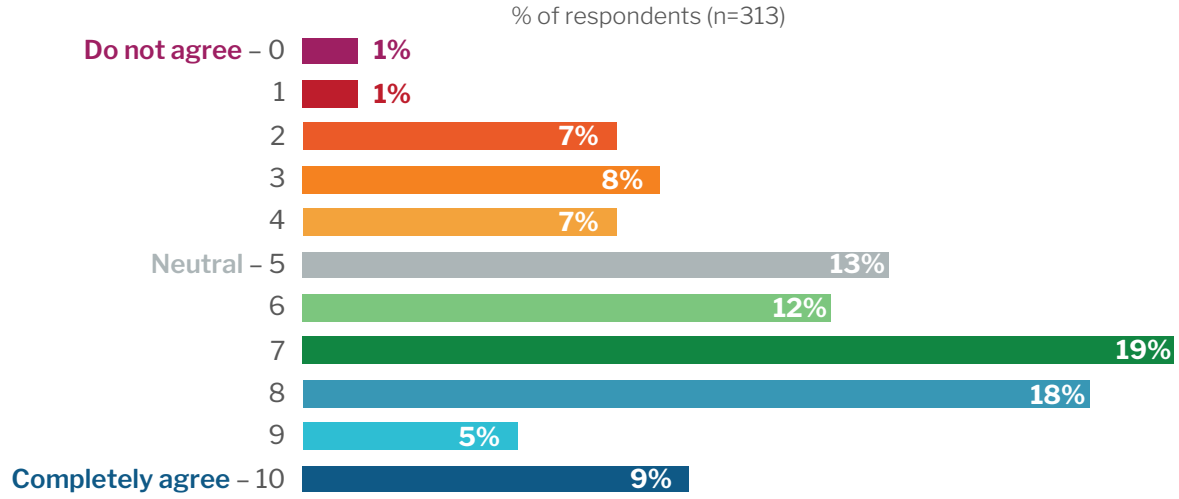
The 451 Take

IT spends too much time on operations and maintenance, which erodes the time IT can spend adding value to the business. Consolidating network functions in the branch is about more than merely reducing hardware count – management and operations must be streamlined as well. One of the primary benefits of SD-WAN is simplified operations via policy-driven management, but those benefits disappear when multiple, unintegrated products are deployed in the branch and management isn't unified. Consolidating and integrating networking and security functions, as well as unifying management and monitoring with SD-WAN in the branch, leads to more secure and efficient operations.

Enterprises Agree That IT Ops and Maintenance Take Up Too Much Time

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Organizational Dynamics 2019

Agreement with: 'Day-to-day IT operations and maintenance take up too much of the IT department's time, leaving not enough time to focus on new IT-enabled business initiatives and projects.' (0=do not agree at all, 10=completely agree)



Business Impact

IT SPENDS TOO MUCH TIME ON OPERATIONS. Bandwidth-hungry applications and cloud-based services and productivity tools are putting pressure on IT to offer fast, reliable networking in the branch. The availability of high-speed business broadband, LTE and, soon, 5G offers cost-effective high capacity and resiliency by adding more WAN links. However, branch networking becomes more complicated when a second or third – or more – active WAN connection is added to each location because the network is no longer a simple topology. Routed networks require additional networking expertise to design, deploy, manage and troubleshoot. The additional overhead is compounded by the number of branches that are managed. Overall, multiple WAN connections will increase management workload for all branch operations. Time spent on ongoing maintenance and operations is time that IT could otherwise spend adding value to both IT and the business.

451 Research | Business Impact Brief

Business Impact (continued)

FUNCTION CONSOLIDATION DOESN'T STREAMLINE OPERATIONS. Consolidating multiple vendors' products to a universal CPE (uCPE) in the branch has all the benefits that IT gained with server virtualization in the datacenter – less power, less rack space, less cooling, less noise – but operational management workflows remain unchanged because the same number of products must be managed. Network and security IT staff will still spend the same time on maintenance and operations. Unfortunately, a lack of management integration in a multivendor branch network and security environment is the norm for most enterprises. Without integrated management, policy and configuration changes require multiple steps, which can lead to errors and misconfigurations that reduce management efficiency and possibly create security problems. IT manages complexity today with change control processes, which can reduce the chance of error but actually extend the time that implementing a new policy or configuration change can take. Adding networking and security products to the branch further complicates management.

MULTIPLE SINGLE-FUNCTION ARCHITECTURES ARE DIFFICULT TO AUTOMATE AT SCALE. Complexity is the enemy of IT when trying to automate provisioning and ongoing operations. The more networking and security products in use, the more APIs must be used and maintained throughout the product deployment lifecycle. Developers and network IT must ensure that configuration changes don't negatively impact the network or adjoining products and services, which adds to management overhead. Similar to operations, consolidating multiple vendors' products to a uCPE doesn't reduce the work developers undertake in automating ongoing operations because the number of different products under management hasn't been reduced.

Looking Ahead

Enterprises can tackle the growing complexity of multivendor, multifunction product strategies by consolidating multiple functions into a single, integrated multifunction branch network appliance that includes SD-WAN and using centralized management to apply network configurations and security policies in a consistent manner. The integrated strategy worked well for UTM products, allowing administrators to create holistic polices for firewalls, VPN, intrusion prevention, anti-malware and other security controls.

Networking functions like SD-WAN, advanced routing and monitoring fit naturally into an integrated branch appliance, and this results in more efficient management across networking and security, with a lower chance of misconfiguration compared to a multivendor approach. Employees, partners and customers in branch offices will enjoy better application experiences as the SD-WAN adapts to changing network conditions in real time while implementing the IT performance and security policies that the enterprise requires.

Integrated branch products that include SD-WAN simplify programmatic integration to other IT management systems such as service-ticketing systems, alerting, monitoring and automation platforms because integration can be bound to a centralized management platform or controller. Developers can often write less code – reducing errors – by defining all of the network and security policies and sending them to the management or network controller.

Managing branch networks is becoming more complex – the number of branches is growing, the number and locations of network applications in the branch are growing, and the expectations for fast performance are increasing. IT must juggle these demands while simultaneously protecting users from internal and external threats. A significant outcome of consolidating network functions in an SD-WAN appliance is consistent, policy-based security and performance management, ensuring that these competing demands are met while reducing the time IT spends on operations and maintenance.

451 Research® Now a Part of S&P Global Market Intelligence | Business Impact Brief

SD-WAN Delivers Compliance Controls

The 451 Take

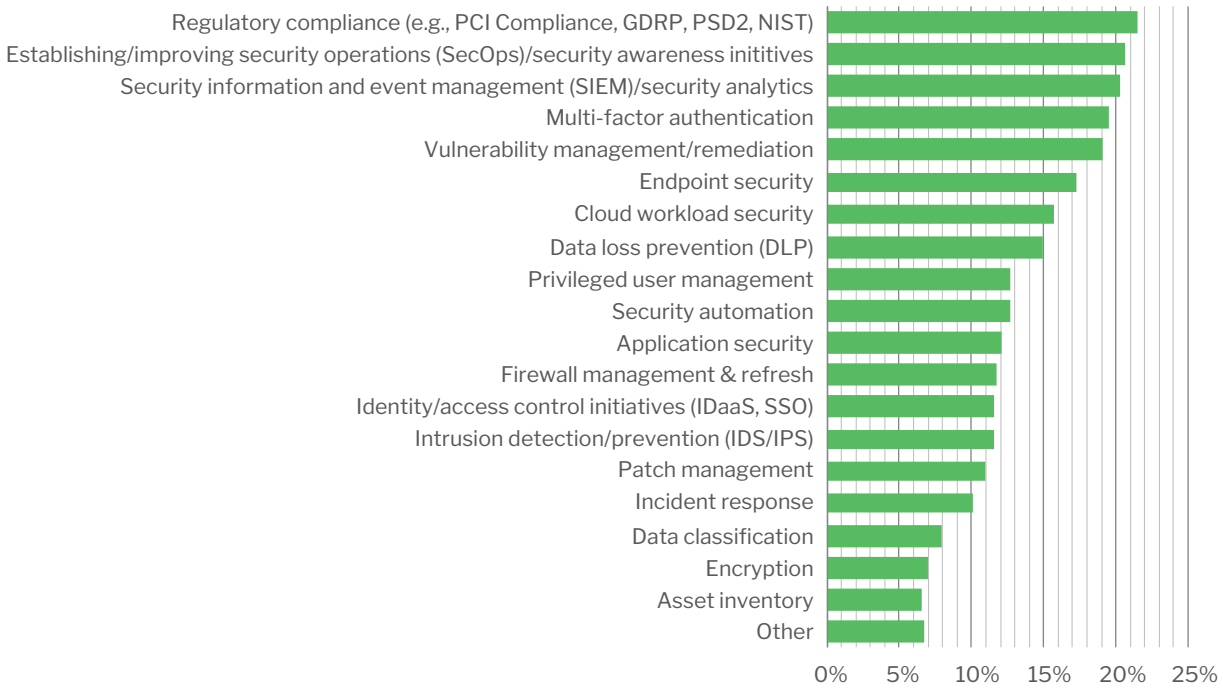
While there are many challenges in the world of enterprise IT, compliance concerns are a perennial leader in the minds of IT executives. And no wonder. The variety of compliance imperatives, their regional variability, and the complexities of proving adherence consume considerable resources. In the midst of all of this, though, there is good news in one of the hotter areas in IT – SD-WAN initiatives can have a significant and positive effect on enterprise compliance. Where many new technologies throw an additional wrinkle into compliance efforts, SD-WAN offers tools that can be put to work as effective compliance controls.

Top Three Information Security Projects Over the Next 12 Months

Source: Voice of the Enterprise: Information Security, Workloads & Key Projects Q1 2019

Q2. What will be your top three information security projects over the next 12 months?

Base: All respondents (n=503)



Compliance challenges

Businesses have always worked hard to build effective security capabilities, but have often struggled to achieve their compliance goals. With a slew of new technologies and capabilities to implement, IT teams are often challenged to sort out how to wrap controls around them to ensure compliant use. Controls often don't exist within the native technology, and, when they do, they are often inconsistent. SD-WAN is a technology that can actually aid teams in compliance efforts, since it can deliver comprehensive controls and visibility – and often can do it in ways that reduce the work required to maintain compliant environments.

The network controls that SD-WAN can offer operate at a critical point in application architectures and typically have a level of sophistication that allows granular partitioning of traffic in ways that work well for compliance enforcement. When they're aligned with existing security capabilities, they can provide control consistency that can simplify policy management.

The 451 Take (continued)

SD-WAN benefits

The key benefits of SD-WAN implementations are their ability to simplify operations and deliver consistent policy controls. They do that by acting as a control overlay that has the benefit of high-level abstractions for policy design and reducing the amount of low-level network reconfiguration that traditional approaches require. Overlay approaches have the advantage of using the same controls across a range of access technologies, ensuring that the right policies are in place, no matter how users and applications are connected.

Deployment options

To minimize any complications in the transition to SD-WAN from traditional branch and remote networks, it's important to consider how these new capabilities will be blended with existing environments. Being able to maintain control compatibility with security functionality that's already in place can smooth the integration. It will reduce the work to align policies and validate that the appropriate controls are in place. Many SD-WAN offerings have reporting functionality that can provide insights and ensure operational simplicity. The goal for any deployment should be to take full advantage of the benefits that SD-WAN can deliver.

Business Impact

SD-WAN DEPLOYMENTS CREATE OPPORTUNITY. New deployments of WAN technology present an opportunity for enterprises to put more effective security controls into place in an area that's been challenging.

OVERLAY CONTROLS. SD-WANs offer overlay controls to segment and encrypt traffic across the varied access networks that may be in use.

CONSISTENCY. Policy consistency is an important benefit of capable SD-WAN offerings, reducing operational complexity. Capable SD-WANs can provide reporting functionality that can make audits simpler.

ISOLATION AND SEGMENTATION. Ensuring that network traffic is properly segmented from remote locations into the network core offers important compliance controls.

Looking Ahead

Organizations have an opportunity to step beyond many of the traditional limitations of security infrastructure by looking to cloud-based security services to deliver compliance controls. In contrast to traditional approaches, cloud-delivered options have important benefits. To start, they can scale in ways that on-premises systems simply can't. Being able to respond rapidly to scale up to meet demand and scale down to manage cost is hard to achieve with fixed infrastructure. Cloud-delivered services also bring the potential to have more performant access to mobile connectivity – an important factor for increasingly mobile and remote users. That access can also have adjacency to SaaS and cloud-based applications, removing networking issues such as traffic hair-pinning. It can put controls in place where they're most effective and in ways that keep users productive.

There are operational aspects as well. The ability to have the overarching control infrastructure that cloud-delivered security capabilities offer can deliver consistent security policies, when they align with existing systems. That consistency can reduce the work required to assure that the controls that are in place match the requirements for their use. Coordinated user identities and application definitions reduce the possibility for error in important segmentation efforts, such as network micro-segmentation. Having the right controls with consistent policies can greatly simplify the tasks of ensuring compliance and reporting requirements. Cloud delivery makes it simpler to do across an entire organization.