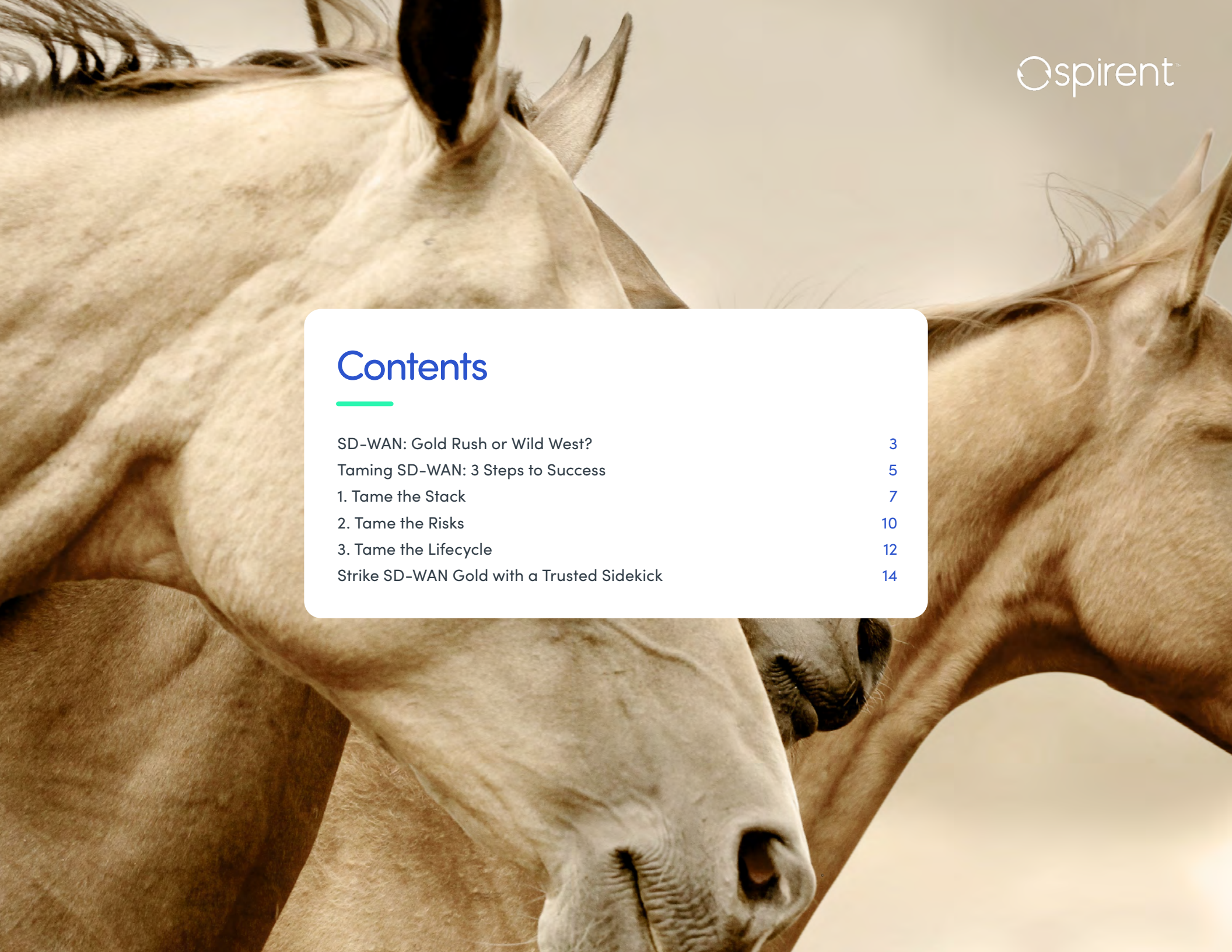
A SPIRENT E-BOOK

Taming SD-WAN



Contents

SD-WAN: Gold Rush or Wild West?

Service providers see SD-WAN as a high-growth opportunity... if they can tame the complexity and rein in costs.

No matter where an organization is on its digital transformation journey, its technology leaders are assessing SD-WAN (software-defined wide-area networks). Whether already part of the strategy, or still under consideration, SD-WAN is essential for most organizations.

By abstracting the application layer from infrastructure, SD-WAN offers enterprises a more efficient and cost-effective way to manage and scale networks. Over the past decade, increasing numbers of organizations recognized how SD-WAN complements, in some cases replaces, MPLS networks with less expensive Internet connectivity. SD-WAN's policy-based forwarding, inherent security and centralized management have made it the on-ramp of choice to the cloud for many enterprises.

With these advantages, however, SD-WAN poses new challenges in simultaneously managing WAN connections (underlays), SD-WAN overlays, as well as virtualized SD-WAN endpoints, which introduce the complexity of network function virtualization (NFV). SD-WAN is also closely coupled with applications, further complicating management, as policies must be tuned to achieve the end-user's goals.

Enterprise adoption of SD-WAN has resulted in a large and diverse set of vendors with overlapping SD-WAN solutions targeting a variety of business networking requirements. Established network equipment vendors have become major players in the market, developing their own offerings and acquiring early movers. Different players highlight distinct features, leading

to a Wild West of differentiated capabilities and proprietary SD-WAN controllers. Despite this specialization, vendors increasingly label their products simply as 'SD-WAN' (so-called 'SD-WAN Washing'). Managed Service Providers (MSPs), vendors and end-users are often left scratching their heads, but a little confusion is better than getting left in the dust, and the industry has pressed ahead.

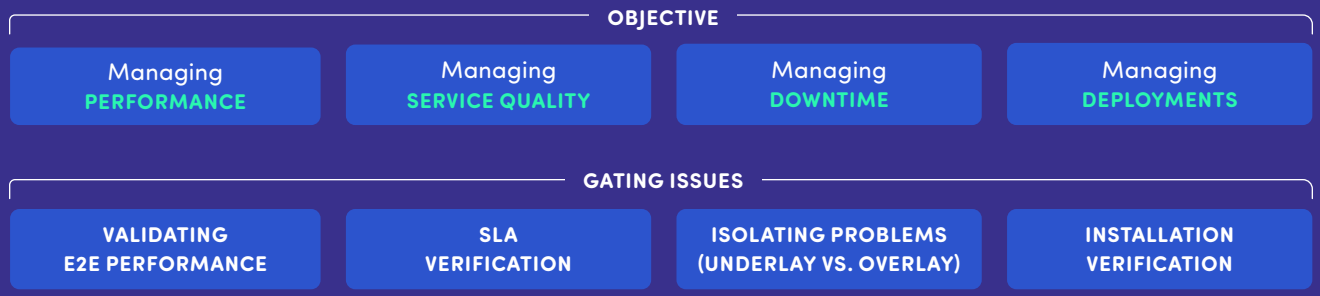
Initially, enterprises assumed responsibility for their SD-WAN Solutions (the "Do It Yourself" or "DIY" approaach) during the first wave of adoption. But now, more and more organizations have recognized the compelling benefits of delegating their SD-WAN networks to MSPs. This trend has accelerated as enterprises migrate applications and data to the cloud, and since 2019, SD-WAN managed services have represented the predominant deployment model.

SD-WAN MSPs have a unique opportunity to deliver superior value to enterprises and achieve better margins than they have historically achieved with legacy connectivity services. But taming the complexity of SD-WAN can be a serious challenge for MSPs integrating different SD-WAN vendors and tailoring services to their customer's varied business needs. To be successful, MSPs need to rapidly and effectively integrate specific SD-WAN capabilities across vendors, while reducing both costs and rollout times.

FIGURE 1

Barriers to Agile SD-WAN Deployment

MSPs must contend with a wide array of factors to manage successful SD-WAN deployments.



What are your biggest challenges to deliver SD-WAN managed services?

HeavyReading Managed SD-WAN Services Report, Jan 2021

KEY TAKEAWAY

The challenge for MSPs is that enterprises are selecting different SD-WAN vendors and tailored services depending on business needs, creating unwieldy complexity. MSPs need a normalized and neutral partner for validating that SD-WAN managed services are performing as expected.

Taming SD-WAN: 3 Steps to Success

A strategy for managing SD-WAN complexity must be built around industry standards and innovative best practices from successful deployments.

It's no surprise that enterprises are outsourcing SD-WAN deployment and management to MSPs. With multiple layers, multiple vendors and multiple clouds, it's a lot to rein in. And until now, the multifaceted SD-WAN market has been evolving at breakneck speed, without standards. Fortunately, that's changing.

MEF (originally Metro Ethernet Forum), a global industry forum for network and cloud providers, created the industry's first SD-WAN standard in 2019, with Spirent as its exclusive provider of certification services. Spirent is a neutral and trusted source for both MEF certification and comprehensive next-gen SD-WAN testing, validation and assurance.

Over time, standardization and certification have the potential to manage SD-WAN chaos and accelerate the pace of innovation.

Standardization instills order, for both vendors and operators, and helps the industry make much-needed strides towards multi-vendor SD-WAN and widespread adoption. A MEF certification is the industry's seal of confidence, and leading service providers and vendors are relying on it in growing numbers. As the industry embraces MEF certification, a coherent SD-WAN ecosystem is emerging.

Spirent is privileged to have been embedded in this ecosystem with leading vendors and MSPs since SD-WAN first emerged. Through our involvement with MEF, along with experience testing a wide array of SD-WAN environments, we have developed a simple three-step guideline for taming SD-WAN complexity:

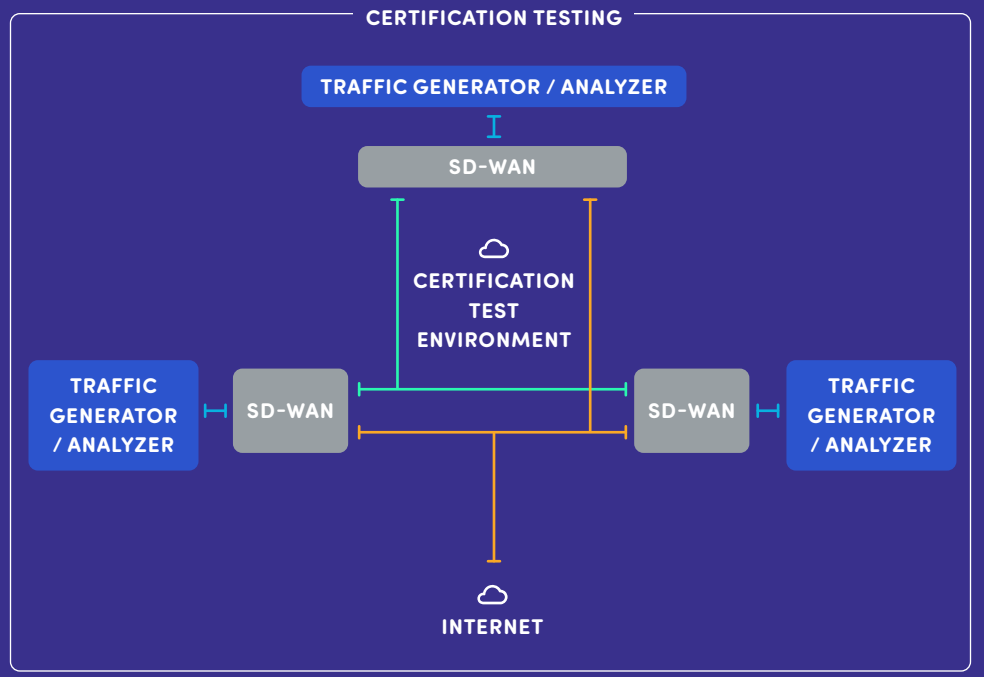
1. Tame the Stack
2. Tame the Risks
3. Tame the Lifecycle

KEY TAKEAWAY

Taming SD-WAN must draw from best practices developed by seasoned testing experts embedded in the ecosystem, who leverage the industry's collective and qualified knowledge revealed through the MEF SD-WAN certification program.

FIGURE 2

MEF SD-WAN Certification Workflow



1. Tame the Stack

Taming the full SD-WAN stack requires validation across vendors, layers and services. Expert guidance can help bring order to the chaos.

Taming the stack with traditional Ethernet/MPLS test methods on their own for SD-WAN is insufficient. MSPs might understand performance for one end-user, but distinct applications, diverse vendors, and policies may result in very different performance requirements. A major challenge is how to cope with the increasingly complex stack of services, protocols and configurations. The goal is to ensure quality SD-WAN experiences by simultaneously analyzing the entire set of implementation layers that must ultimately work together seamlessly. An overarching and comprehensive approach is needed. Best practices for taming the SD-WAN stack consists of three elements.

Validate the layers.

Evaluating only the network connectivity is no longer sufficient; service providers now need to validate multi-vendor underlay and overlay network layers, as well as the service and virtualization layers in between. If the vendor deploys a virtualized network function on white box hardware, complexity rises even more. Validating the layers proactively exercises the dependencies among the layers, to rapidly pinpoint problems long before deployment. In addition, SD-WAN endpoint configuration may be optimized as well.

Ensure service readiness.

The wide variety of end-user environments, applications, and user requirements further complicates the deployment of SD-WAN services. For connectivity services, service providers execute Service Activation Testing (SAT) to thoroughly exercise the path to preempt problems, before end-users are impacted.

SD-WAN introduces additional complexity as the first widely deployed Software Defined Network (SDN) based service. As a result, Service Readiness Testing (SRT) is required to complement SATs, resulting in end-to-end testing that verifies all layers prior to operation.

TAMING SD-WAN

Potential issues are exposed and mitigated proactively, before the customer experience is degraded.

Certify for certainty.

The MEF SD-WAN certification program ensures that multi-vendor, multi-provider services work together without any disruption. A certification program promotes standards conformance to enable the evolving SD-WAN ecosystem.

The more companies participate, the more valuable the certification becomes and the healthier the overall industry will be. Operators benefit through a common set of functionality across vendor solutions. Vendors benefit by freeing up R&D resources to focus on value add. And with a proliferation of SD-WAN products, certification provides a normalized means of validating vendor claims and a benchmark for common, core functionality. As the standard matures, certification emerges as an important tool to qualify vendors' solutions for deployment, which ultimately streamlines procurement, benefiting both operators and vendors.

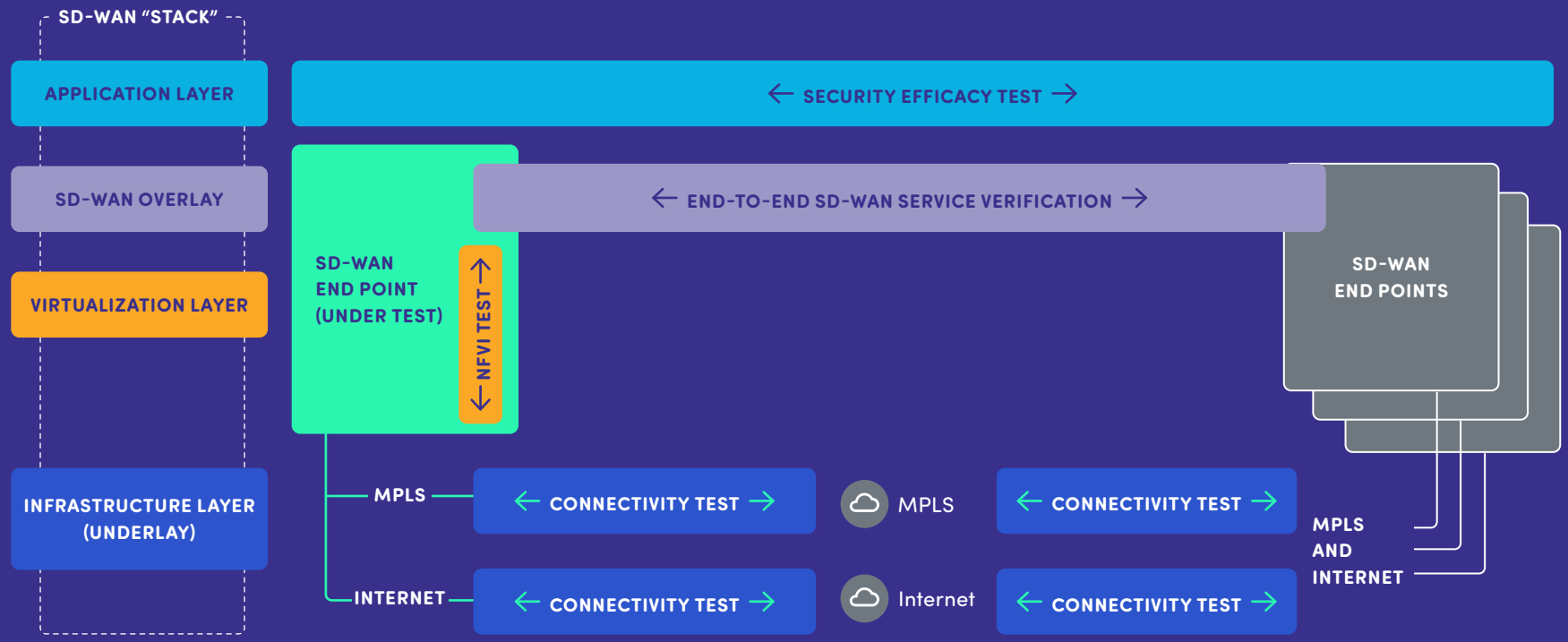
KEY TAKEAWAY

Traditional testing methods are inadequate on their own to tame the stack. Sophisticated and intelligent multi-layer validation analyzes all layers and their dependencies to proactively expose issues before the end-user experience is impacted. Certification validates vendor and operator claims, which ultimately accelerates the buying process.

FIGURE 3

Tame the Stack

Spirent recommends multi-layer validation testing of the SD-WAN overlay and underlay. On the overlay, end-to-end tests determine readiness for launch, while segment tests help isolate application and service issues. On the underlay, end-to-end and network segment validation tests isolate network performance and service issues. Full visibility of the stack accelerates troubleshooting of issues in all phases of the lifecycle, from lab validation to certification to deployment and operation.



2. Tame the Risks

Take a proactive, vendor-neutral approach that spans the lifecycle to validate SD-WAN security defenses against a new generation of threats.

An essential goal of security is to create predictable responses to unpredictable events. Compared to traditional wide area networks (WANs), SD-WANs are commonly virtualized and rely heavily on the public Internet, along with a range of private connections. As a result, the SD-WAN attack surface is constantly growing, as are the challenges to addressing them. This requires the rapid development and deployment of enhanced security functions and the best practices to validate them. We recommend three:

Validate security readiness.

Identifying security vulnerabilities during deployment is essential so they are preempted before going live. Security readiness testing should exercise specific and real-world deployment configurations prior to activation to ensure issues are proactively exposed and mitigated before disrupting service availability.

Assess operational security.

Security efficacy testing in the lab exposes vulnerabilities and problems before end-user applications and data are compromised. Efficacy testing doesn't just measure the performance and configuration of security, but also whether they are behaving as expected. You're more likely to successfully tame the risk if you consistently gather and verify with up-to-date and critical data.

Certify for security.

You can provide peace of mind for your customers by extending network certification programs to verify cybersecurity. It's critical to choose a testing partner with proven expertise that offers a range of packaged and custom services to assess and validate the security posture of SD-WAN products and services. Pre-deployment assessment services expose problem areas and offer insights on how the network will perform under different attack scenarios.

Spirent SecurityLabs provides a deep bench of expertise supporting SD-WAN security testing. Spirent is a leading contributor to the MEF SD-WAN Security standards, including Application Security for SD-WAN (MEF 88), along with the emerging Secure Access Service Edge (SASE, MEF 117) and Zero Trust Framework (ZTF, MEF 118) projects. Spirent is leading the Security Test and Certification Incubation Group to explore how MEF can certify the emerging security standards.

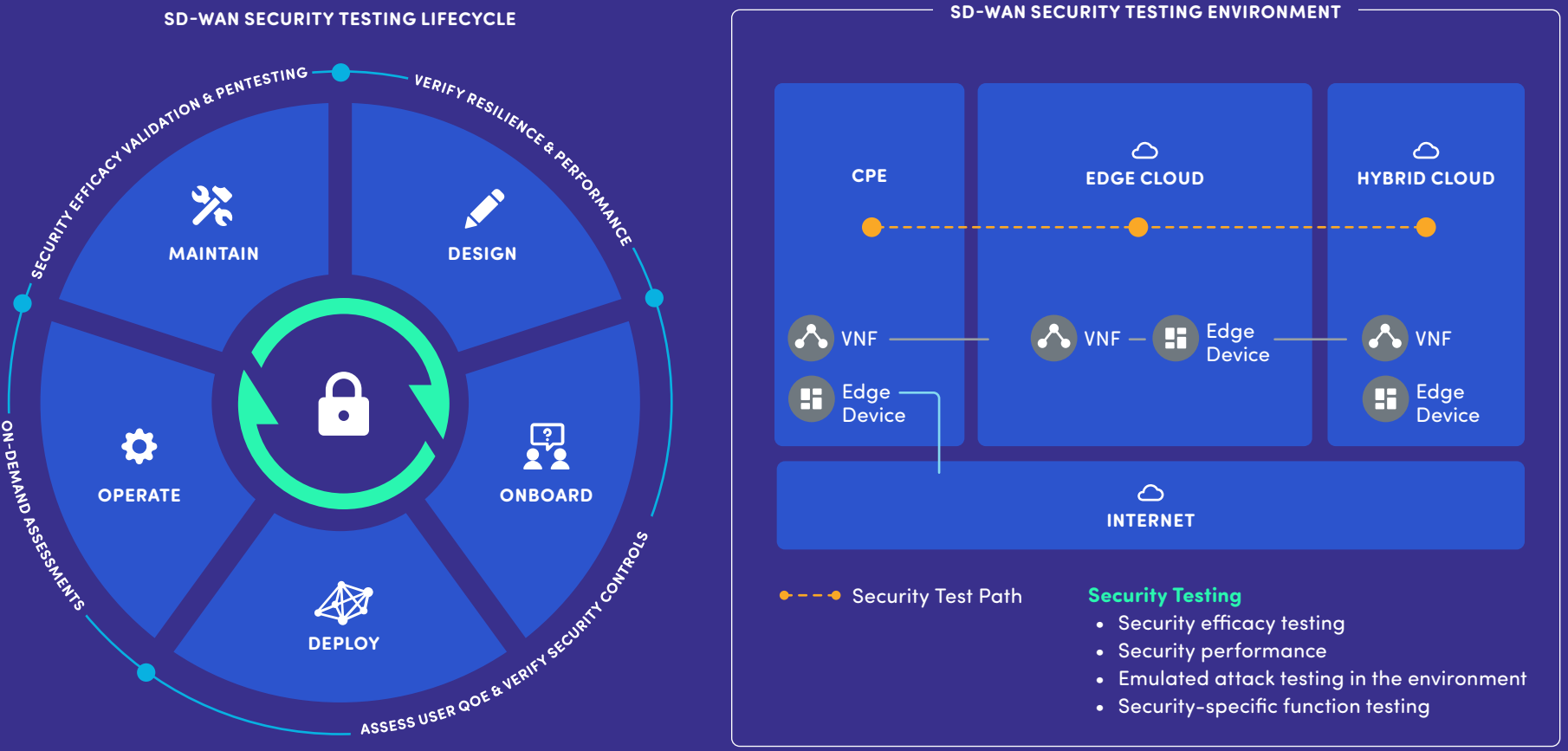
KEY TAKEAWAY

Automated security testing throughout the lifecycle, guided by emerging MEF standards, improves an organization's security posture with proactive security visibility, and ensures products and services are behaving and performing the way they are anticipated.

FIGURE 4

Tame the Risks

Taming the Risks begins in the Design and Deployment phases and extends through operations and maintenance. Security and application layer performance testing validates security controls efficacy and the quality of the user experience. The ability to assess "what-if" scenarios with continually updated actual attack and malware testing proactively exposes security weaknesses ahead of the curve, enhancing security throughout the entire SD-WAN lifecycle.



3. Tame the Lifecycle

Overcoming deployment complexity requires testing, validation, and assurance throughout all phases of the SD-WAN lifecycle.

Introduction of software-defined services accelerates the rate of change, and increases the complexity incurred in the multi-layer, multi-vendor environment. To address this, increased automation is essential to verify each change prior to operations. Spirent recommends a holistic testing strategy throughout the entire service delivery lifecycle, in order to:

Optimize before deploying.

Extensive testing in the lab offers an opportunity to exercise policy management, product configurations, and assess key features to optimize performance. This is especially important for virtualized deployments, where NFV resources are constrained. Because each layer is distinct, diverse testing methods are required. Whereas simulated traffic is sufficient to analyze the lower layers, emulated real-world transactions at the higher layers are required to precisely evaluate application and security behavior and performance.

Proactively assure service levels.

Proactive SD-WAN services active testing improves user experience, ensures SLA compliance and avoids penalties. End-to-end testing may reveal performance issues before they impact end-users. Continuous SD-WAN testing is essential because these networks evolve constantly. Software is upgraded, configurations altered, new network virtual functions are integrated, and new hardware is added. In addition, the network is subject to an ever-changing range of threats from nefarious actors from around the globe.

To assure service quality, comprehensive SD-WAN testing is required for each site added, once the network is activated, and for each upgrade. Such continuous and consistent testing exposes performance issues, often before the end-user is even aware of a problem. Problems found earlier in the development cycle can be fixed faster, usually at a significantly lower cost than if they had been discovered in the field. Continuously tame each phase of the service lifecycle to ensure every element performs as expected prior to introducing them to the live network.

Automate lifecycle troubleshooting.

Lab testbeds and development sandboxes keep the network up-to-date, and are used to proactively troubleshoot and isolate real-world SD-WAN problems. Spirent recommends using common and automated DevOps testing practices across Development and Operations teams to to ensure consistent results across multiple vendors from the Lab to Live network. The testing approach should ensure that exhaustive multi-vendor, multi-layer test methodologies are applied across the entire service delivery lifecycle. Standardized, simulated connectivity and virtualization testing should be melded with precisely emulated application and security testing to expedite site turn-up, quickly expose and isolate operational problems, and reduce downtime overall.

KEY TAKEAWAY

Employing automated continuous testing for optimization and troubleshooting throughout the lifecycle ensures products and services are behaving and performing as anticipated.

FIGURE 5

Tame the Lifecycle: Lab-to-Live, SD-WAN Testing/Validation/Assurance

Attributes of the Lab-to-Live strategy:

- Network and security testing methodologies
- End-to-End, domain, and device coverage
- Physical and virtual SD-WAN endpoints
- Multi-layer testing
- Common test cases

Strike SD-WAN Gold with a Trusted Sidekick

Ensure success by partnering with a neutral, vendor-agnostic SD-WAN expert.

There is no doubt that SD-WAN is still untamed, complex and changing rapidly. The SD-WAN landscape includes a large and diverse set of vendors. The set of applications that must be supported is limitless and constantly evolving. Dependence on hyperscalers adds yet another layer of complexity, especially since many enterprises work with more than one cloud provider. But for SD-WAN to scale effectively across the industry, and succeed in the long term, organizations need to unite with one objective: to converge on an open and inclusive SD-WAN ecosystem.

A trusted partner can make all the difference. As a neutral, trusted authority for SD-WAN testing, validation, and assurance, Spirent is the exclusive certification partner for the industry's first SD-WAN standard with MEF and is leading the charge for the industry's first SD-WAN security testing standards.

Spirent's SD-WAN portfolio spans the lifecycle and traverses the stack to address the broadest range of SD-WAN use cases and validates security efficacy and performance with advanced lab and test automation solutions. As SD-WAN continues to evolve as the predominant onramp to the cloud for enterprises, Spirent enables an organization's SD-WAN journey, now and for the foreseeable future.

Keep a big picture perspective of SD-WAN's promise.

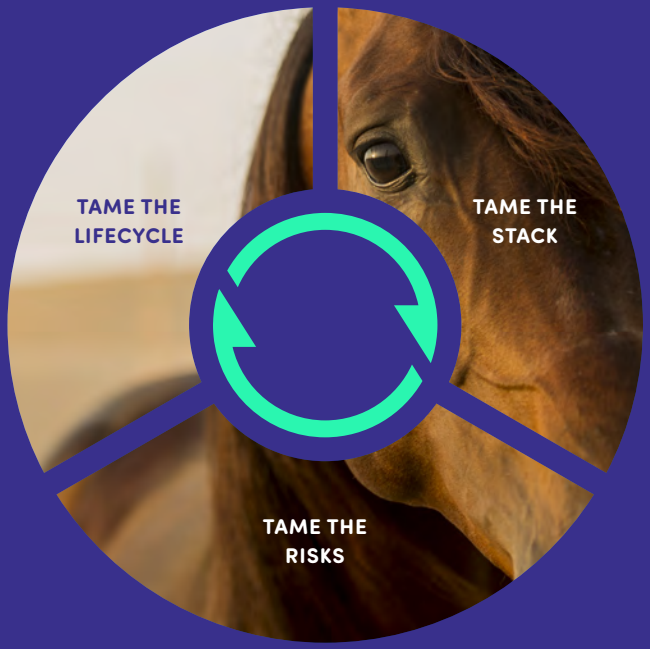
While the devil is always in the details, the only route to success involves a holistic approach to all the testing challenges. Only then can the full benefits of SD-WAN be realized. The three essential best practices shared in this Ebook—taming the stack, the risks, and the lifecycle—are key to achieving this objective.

No successful taming happens sporadically—it must be extensive, consistent and responsive to evolving conditions. Continuous, automated testing ensures network connectivity, service quality, application performance, and security efficacy across the entire service lifecycle. The goal is to catch issues as early as possible in the development cycle to minimize downtime and ensure the user experience. As testing standards continue to be adopted, SD-WAN best practices and the standards that adopt them will also emerge, along with the tools to implement them. Consider Spirent as your trusted and neutral SD-WAN testing partner, no matter where you are in your journey.

FIGURE 6

Continuous Taming of SD-WAN

The enduring value of the right approach. Spirent's SD-WAN solutions for testing, validation and assurance, tame SD-WAN by proactively exposing issues and vulnerabilities up and down the stack, and throughout the entire service delivery lifecycle. Spirent is a proven neutral and trusted partner for SD-WAN testing today, and as your journey evolves.



About Spirent Communications
Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled. For more information visit: www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

© 2021 Spirent Communications, Inc. All of the company names and/or brand names and/or product names and/or logos referred to in this document, in particular the name "Spirent" and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice. Rev A | 02/21

spirent