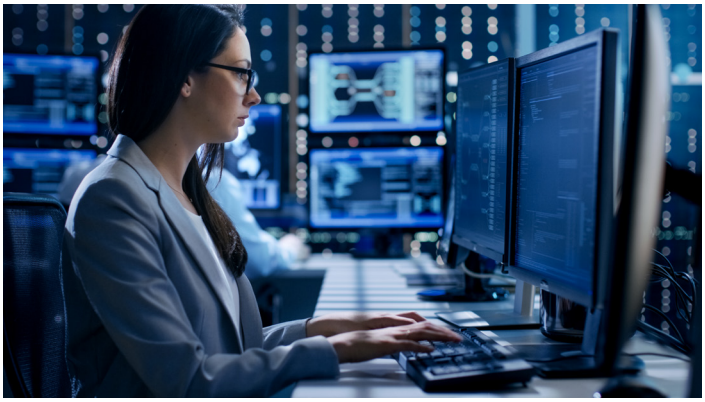
Solution Brief

Validating SD-WAN Security and Performance

You know why. Do you know how?



Protect the benefits of SD-WAN

There is no doubt that the adoption of software-defined wide-area networks (SD-WANs) can deliver significant benefits to IT and to your business. SD-WANs enable you to:

- **Cut costs by reducing dependency on MPLS:** SD-WANs can manage multiple types of connections, including MPLS, LTE, and broadband cable or DSL, while delivering a variety of services such as VPN, security and load-balancing—all at a lower cost than MPLS.
- **Improve performance** through better bandwidth allocation and the ability of SD-WAN controllers to dynamically route around congested or failed paths.
- **Accelerate deployment times** because there is no longer a need to provision circuits through a service provider with a range of contractual SLAs.
- **Support differentiated QoS** among various application flows; for example you can throttle Facebook traffic while providing guaranteed QoS to voice calls or Office 365 traffic.
- **Improve application policy enforcement** through centralized policy control and micro-segmentation, allowing IT organizations to define highly specific network and security policies for applications.
- **Increase revenue** by targeting new market segments in new geographies.

However, the advantages of SD-WANs accrue only to those who can consistently and verifiably secure the SD-WAN environment while maintaining high performance. And that can be a complex challenge.

SD-WANs shift IT organizations from centralized device-level WAN deployments to decentralized and distributed environments. This can alter the threat landscape and increase the attack surface area. At the same time, many customers are virtualizing SD-WAN circuits to gain economies of scale, opening up new sources of potential liability. And some of the unique characteristics of SD-WANs, such as their end-to-end use of encryption, micro-segmentation, and the need to integrate with legacy firewalls, next-generation firewalls, IDS/IPS and other security solutions, can create additional security concerns and complications.

The result is a growing need for effective SD-WAN security and performance validation.

Validating SD-WAN Security and Performance

You know why. Do you know how?

Simple, smart SD-WAN security and performance validation

Spirent assessment solutions remove the complexity from measuring, managing, and continuously improving SD-WAN security and performance. Our unique approach covers the full spectrum of security and performance validation requirements by combining:

- **Hyper-realistic emulation of attack scenarios:** We test both the security and applications aspects of SD-WANs at L4-7 with real-world, emulated, legitimate traffic mixes and malicious traffic, so you can keep your finger on the pulse of SD-WAN services.
- **Comprehensive and integrated intelligence across solutions and services:** Our solutions harness constantly updated threat and application assessment intelligence feeds for maximum accuracy.
- **Tried-and-true technologies:** There is virtually no data communications vendor or product on the market today that has not already leveraged Spirent to test and validate their equipment and/or networks, and our core competence in testing complex environments and building in security can accelerate your journey to SD-WAN security.
- **The combined experience of seasoned security professionals:** Our solutions leverage many years of security content cultivated by Spirent's Threat Research and SecurityLabs teams. These teams, along with external partnerships across the threat intelligence community, enable Spirent to continuously collect and use a wide variety of real-world attack components.
- **Continuous innovation that keeps us on the cutting edge:** Spirent is an established company that combines the agility and innovation of a start-up with the resources and backing of a large, revenue-positive enterprise, backed by decades of data communications test and assessment expertise. We constantly innovate and give you access to the latest technologies.

More specifically, our testing solutions combine the features and capabilities that allow for proper SD-WAN assessment, including:

- **Tens of thousands of full network application and attack scenarios**
  - Allows for true L7 content inspection and content routing
  - Assess security policies efficacy with real attacks and malware
  - Puts the SD-WAN circuit chain under extreme, realistic mixed application traffic load
- **High-bandwidth, CPS, and TSP generation capability**
  - Full loading of NFV chain services for maximum performance assessments
- **Deep KPI measurement**
  - QoE, per-host statistics, trending and data mining
- **Realistic client-side assessments for protocols and tunneling**
  - Full Stack TCP/HTTP/HTTPS/TLS
- **Right tunneling technologies**
  - IPSEC
- **Capture / replay of "your traffic"**
  - Statefully recreate custom flows to validate specific application ID policies
- **Physical and virtual endpoint support**
  - CyberFlood Virtual for use in a multitude of virtual and cloud environments
  - Appliance hardware solution for scaling to carrier class performance capacities
- **Fully reproducible**
  - Repeatable high complexity of traffic for regression testing

Take a closer look at our capabilities

Our SD-WAN security and performance validation capabilities are delivered by our CyberFlood and SecurityLabs testing solutions, including CyberFlood Data Breach Assessment for assessing and stressing SD-WAN security policy environments, and CyberFlood Virtual for validating the performance and scale of traffic flowing through the SD-WAN. Highlights include:

CyberFlood CF20 Appliance

- **CyberFlood:** Our powerful, easy-to-use L4-7 testing solution generates realistic application traffic, attacks, and malware to test and validate the performance, scalability, and security of today's application-aware network devices and infrastructures. CyberFlood enables teams to harness a comprehensive security platform to test and enforce application policies; benchmark performance and capacities; and validate network security. CyberFlood improves testing today while evolving for the future to keep you ahead of the security curve, and CyberFlood TestCloud provides the industry's largest and most up-to-date set of assessment scenarios for applications, attacks and malware (over 50,000 scenarios and counting).

- **CyberFlood Data Breach Assessment:** This groundbreaking solution delivers automated, continuous and thorough assessment of your live SD-WAN environments, using always-up-to-date intelligence, so you can identify and address weaknesses in your security stance before attackers do. It safely generates hyper-realistic security assessment traffic on the exact services you are protecting—so you can assess your SD-WAN security with real attacks, malware, and data loss prevention (DLP) scenarios. It emulates attack propagation and pivoting behavior, so you get an accurate assessment and validation of complex security countermeasures. This in turn enables you to fine-tune security policies—more frequently and more completely.

- **CyberFlood Virtual:** This solution makes CyberFlood available as a virtual platform for on-premises and cloud deployments, simplifying SD-WAN testing by consolidating multiple test functions into a completely virtual test environment. CyberFlood Virtual enables you to test SD-WAN environments directly from within a virtual environment with multiple unbounded traffic generation endpoints; scale test solutions to handle vast amounts of traffic based on your needs; verify NFV security effectiveness with real attacks and exploits; assess Next Generation Firewalls; generate application load traffic from a growing database of over 13,000 user scenarios and application flows to verify application ID policies and performance; and much more.

- **Spirent SecurityLabs:** Our experts in managed security services can provide in-depth scanning and penetration testing of SD-WANs to uncover exploitable vulnerabilities including Insecure Server Configuration, Default System Passwords, Unpatched Servers with Known Vulnerabilities, Eavesdropping, Insecure Firewall Configuration, Insecure Communications, Information Leakage and Improper Error Handling. Our security consultants act as an extension of your in-house security team, proactively identifying vulnerabilities and mitigating risks.

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

Get the details.

And get a realistic assessment of your SD-WAN security.

We encourage you to get an accurate, continuous assessment of your SD-WAN security and performance—so you can achieve the benefits you expected and continuously improve your security posture.

For additional information about Spirent and any of our CyberFlood solutions, visit https://www.spirent.com/products/security-and-applications-performance-testing-cyberflood

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

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

Rev A | 10/19