

INDUSTRY INSIGHTS

Why Choose Fortinet Secure SD-WAN Over Cisco SD-WAN

Secure SD-WAN connectivity has become mission-critical for organizations needing to intelligently interconnect their remote locations quickly and securely. The challenge is that many SD-WAN solutions don't meet those requirements. Some only work in specific use cases. Others have significant technology limitations. Most have failed to seamlessly integrate security into their solution.

Cisco's SD-WAN solution is a case in point. Cisco continues to struggle with merging the Viptela SD-WAN software it acquired in 2017 and its point security offerings into its ISR platform, impacting the reliability, security, performance, and simplicity organizations like yours require.



Reliability – In May 2023, Cisco had a catastrophic certificate expiration issue that prevented CPEs from authenticating with the controller. This affected ALL legacy Viptela customers, taking down entire networks and causing widespread business disruption.

Fortinet Secure SD-WAN uses a decentralized, fully autonomous controller architecture to avoid single points of failure and controller scaling limitations.



Security – Cisco SD-WAN relies on point solutions never designed to work as a cohesive security system. ISR routers trying to perform deep packet inspection suffer from severe performance degradation. The solution's security effectiveness has also never been validated by a third party. Security is a critical component of any SD-WAN deployment and not just a checkbox.

Fortinet's fully validated Secure SD-WAN solution is built on our FortiGuard platform. It natively includes ASIC-accelerated security inspection, AI-powered threat intelligence, fully integrated security designed for SD-WAN environments, and seamless integration with the extended Security Fabric.



Performance – Because of its piecemeal architectural approach, Cisco SD-WAN has chronic performance and scaling limitations that can significantly impact user experience.

Fortinet's patented SD-WAN ASIC and decentralized fully autonomous controller architecture ensures optimal user experience under any load.



Complexity – Another example of Cisco's incomplete strategy is that its security, SD-WAN, switches, and APs are all managed using different consoles, creating unnecessary complexity and overhead.

Fortinet Secure SD-WAN provides true single-pane-of-glass management for both networking and security (SD-WAN, security, SD-Branch) to ensure consistency and simplicity in deploying, optimizing, and troubleshooting any aspect of your SD-WAN solution and lower your TCO.

Why Fortinet

While Fortinet pioneered the concept of Secure SD-WAN, it is our expertise in security, advanced routing, and integration that has made us a leader. It's why we are one of the top two vendors in the Leader's quadrant and placed highest in Ability to Execute, being recognized for the 13th time in the 2022 Gartner® Magic Quadrant™ for Network Firewalls.¹

¹ Gartner, Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hills, Tom Lintemuth, 20 December 2022.

GARTNER is a registered trademark and service mark, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner® does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner® research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner® disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.