



## Nine Essential Elements of an Effective Secure SD-WAN Solution

The versatility of SD-WAN enables organizations to expand how and where it is applied. Connecting branch offices to the cloud or data center is only one possible scenario. A growing number of organizations also use SD-WAN to connect remote workers to cloud and campus resources, and to create high-speed, on-demand connections between clouds or between the cloud and the data center.

The challenge is, few solutions can effectively address all the use cases SD-WAN is able support—and fewer still can do so while securing the connections, data, and applications they deliver. This list identifies nine essential

elements every Secure SD-WAN solution should provide to help organizations choose a solution designed to grow and scale with their business.



at any edge with accurate application identification and steering, including encrypted traffic and dynamic link remediation



Secures work-from-anywhere with embedded ZTNA (zero-trust network access) Access Proxy for explicit per-user application access controls



Provides optimal support for cloud-first, security-sensitive, and global organizations by combining dynamic scalability and enterprise-grade security for all use cases

Simplifies, automates, and secures SD-WAN deployments across multi-cloud and hybrid cloud environments with cloud on-ramp support

Accelerates "Day 2+" operations by providing a unified and



consistent view of analytics and reporting to NOC and SOC teams, enabled by a single-pane-of-glass management system

Simplified zero-touch roll-out empowers IT to quickly build secure WAN networks to achieve operational efficiencies at any scale



Acts as a foundational platform for future-proofing SASE and secure SD-Branch frameworks



Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet<sup>®</sup>, FortiGate<sup>®</sup>, FortiCare<sup>®</sup> and FortiGuard<sup>®</sup>, 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.