

# Fortinet SD-Branch

## Market Opportunity

- At Fortinet, SD-Branch is a use case of Secure SD-WAN. SD-WAN is a feature included at no additional charge in every FortiGate Next-Generation Firewall (NGFW). SD-Branch offers additional hardware and services at the edge beyond the FortiGate. This increases the value of most opportunities upwards of 3x.
- SD-WAN is dramatically reshaping the enterprise router market.
- IDC predicts an SD-WAN CAGR of over 40% and estimates that the overall market will reach \$4.5 billion by 2022.<sup>1</sup>
- In comparison, the wireless opportunity is a **\$5.84B market in 2020** with a 7.9% CAGR 2018 – 2023. The campus switching market is a **\$14.6B market** with a 1% CAGR. This presents a significant opportunity.

## Why Fortinet

The Fortinet Secure SD-Branch solution consolidates the management of SD-WAN, firewalls switches, and APs into a single solution. This lets distributed organizations reduce complexity, lower costs, and enable security at the WAN and edge.

With Fortinet Secure SD-Branch:

- Security-driven networking ensures top security and performance at the edge, unifying WAN and LAN environments.
- Global policies are enforced at the WAN edge, at the branch, and across all endpoint devices (including IoT).
- Automated discovery, classification, and security of IoT devices is enabled, along with anomaly detection and remediation.
- Zero-touch provisioning enables distributed organizations to scale rapidly. New offices gain agility without the need for IoT experts at each location.
- Centralized management reduces the need for onsite resources, lowering TCO.

## Addressing Business Challenges

Business Challenges	Fortinet Solutions
<b>Complex operations</b>	Fortinet Secure SD-Branch simplifies operations and eliminates silos. Convergence of the WAN, security, and edge (wired and wireless) consolidates management, reduces risk, and increases agility.
<b>Network/security conflicts</b>	With Fortinet, network and security capabilities are managed together via a single pane of glass. This provides visibility and control over all branch offices and remote locations from the edge to the WAN edge. Simplified protection and monitoring extend throughout the branch for seamless security.
<b>Budgetary constraints</b>	Fortinet reduces the cost of branch management by reducing the number of disparate vendor products that need to be managed. This offers several financial benefits including lower licensing and support costs, which in turn lower operating expenses and overall TCO.



## Target Companies and Personas

### Organization Size

- Mid-market and large organizations with a wallet spend of \$249 million and above.
- Any organization with multiple locations, including headquarters, branches, corporate data centers, colocation/hosting facilities, cloud providers, and more.

### Personas

- **Primary audience.** VP/director of network engineering
- **Technical buyers/influencers.** VP of IT, security administrator/architect, networking engineer
- **Business buyers/influencers.** Branch/store manager, CFO, finance/procurement

## Key Differentiators

As the SD-WAN market has grown, more and more vendors have attempted to position themselves as SD-Branch solution providers as well, but few offer a complete solution. Fortinet, on the other hand:

- Is one of the only vendors represented in three applicable Gartner Magic Quadrants:
  - February 2020 Gartner Magic Quadrant for Network Services
  - November 2020 Gartner Magic Quadrant for WAN Edge Infrastructure
  - November 2020 Gartner Magic Quadrant for Wired and Wireless LAN Access Infrastructure
- Placed in the November 2020 Gartner Magic Quadrant for WAN Edge Infrastructure.<sup>2</sup>
- Differentiates Fortinet Secure SD-Branch from all other vendors through its integration of services (SD-WAN, edge and security) into a common framework (the Fortinet Security Fabric).
- Does not require a license for SD-Branch. Like SD-WAN, edge management is included in FortiOS.
- Provides fully-integrated NGFW security, unlike most SD-Branch vendors.

## Qualifying Questions

NOTE: Most questions for qualifying SD-WAN opportunities also work for SD-Branch. Questions below are specific/important to SD-Branch.

- How are you currently securing remote branch networks, including dealing with IoT devices?
- How do you currently manage your branches? Does complexity cause problems? Do you lack the resources/expertise to manage multiple products?
- Do you have a global security policy? How is that enforced?
- Is regulatory compliance with GDPR, HIPAA, GLBA, PCI a concern? Do you need to secure data at rest or in motion?

## Overcoming Objections

### **I only use best-of-breed technology OR I see Fortinet as a security vendor only.**

In addition to being a Leader in both the Network Firewall MQ and WAN Edge MQ, Fortinet is positioned as a Visionary in the Wired and Wireless LAN Infrastructure MQ.

### **Our project is only for (SD-WAN, Security, Wireless etc).**

Many companies are looking to reduce overall branch complexity. Having one vendor allows you to reduce the number of contracts, shorten time to resolve issues, etc.

### **We are focused only on the cloud. We do not want any hardware onsite.**

There will always be a need for some hardware at the branch as a cloud on-ramp and your users will need to connect to your network through either wired or wireless access. Since you will need to deploy this equipment anyway, why not do it securely?

### **We are short on people resources and expertise to use or manage this type of solution, especially if it calls for multiple management consoles.**

Fortinet simplifies deployment and management, letting you bring new branch offices online faster and more easily. Fortinet SD-Branch is easy to implement and manage, with a single pane of glass to monitor and manage everything.



## Additional Resources

- [Secure Access and SD-Branch on the Fortinet Partner Portal](#)
- [On-demand webinar](#)
- [Secure SD-Branch Channel Sales Playbook](#)

## Competitive Landscape

NOTE: There are few vendors that offer a comprehensive SD-WAN, wired, wireless, and NAC solution. Many SD-WAN vendors that do not offer access layer or IoT management will try to point to a SASE model. This architecture would point security operations to the cloud and leave the onsite edge and device layers unprotected. At Fortinet we do not see this as good practice. Our SD-Branch architecture provides security for the WAN, edge, and device edge, while still offering cloud-based security models.

Features	Fortinet	Cisco Meraki	HPE / Aruba	Cisco ISR / Viptela	Juniper / Mist	Forcepoint	VeloCloud	Palo Alto Networks	Versa Networks
NGFW w/SSL Inspection	Yes	Limited	No	Yes	Limited	Yes	No	Yes (but slow)	Limited
Application Awareness	Yes	Limited	Yes	Yes	Yes	Yes	Yes	Basic	Some
Wired and Wireless Offering	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Single Management Console (Wired, Wireless, Security, SD-WAN)	Yes	Yes	Yes	No	Limited (in development)	No	No	No	No
IoT Visibility and Enforcement	Yes	Limited	Yes	Yes	Yes	No	No	No	No
Zero-Touch Provisioning	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes
TCO	Low	Moderate	Moderate	High	Moderate	Moderate	High	Moderate	Moderate

1 ["SD-WAN Infrastructure Market Poised to Reach \\$4.5 Billion in 2022,"](#) IDC, August 8, 2018.

2 ["2020 Gartner Magic Quadrant for WAN Edge Infrastructure,"](#) Gartner, 2020.

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.