FORTINET SECURE SD-WAN CHANNEL SALES PLAYBOOK

GET STARTED

Table of Contents

Overview

Business traffic is growing 20% per year and today's business is distributed, with an ever-expanding number of locations that require high-speed, reliable bandwidth for voice, video, internet, and data applications. One-fourth of the workforce is remote (and increasingly mobile), the number of locations is expanding, and a third of all applications run in the cloud. This expectation puts tremendous pressure on organizations with branch offices where IT must manage multiple sites with varying infrastructure.

For years, the distributed organization has relied on wide-area networks (WANs) to support reliable communications across locations. But traditional WANs are reaching full capacity and approaching the breaking point. And the cost of backhauling network traffic from data centers is prohibitive.

There's a better way: Using direct internet access for cloud applications allows distributed locations to improve performance while reducing cost and complexity. An application-aware network can prioritize business-critical applications, and traffic engineering can pick the best real-time link for high performance. A software defined WAN (SD-WAN) accomplishes all of this… but no organization can afford to ignore security.

Cyber criminals are increasingly targeting distributed environments, especially those without the traditional layer of security that would be provided by backhauling network traffic to the data center. Those investing in SD-WAN must ensure they choose a solution with built-in security to protect direct internet access at remote branches. That means a proven NGFW—one with SSL inspection, so it doesn't ignore the more than 72% of network traffic that is encrypted.

Market forecast, size and growth, trends

Market size

Gartner sees a growing market: They forecast SD-WAN to grow at a 59% compound annual growth rate (CAGR) through 2021 to become a $1.3 billion market.[1]

IDC agrees, and expands the view to incorporate SD-WAN infrastructure and services. According to their estimates, worldwide SD-WAN infrastructure and services revenue will see a CAGR of over 40% and they estimate the overall market will reach $4.5 billion by 2022.[2]

Market trends

According to the experts, the market is hot—and only getting hotter. Gartner[3] says that SD-WAN is a highly disruptive force, one that is dramatically reshaping the enterprise router market. By the end of 2019, 30% of organizations will use SD-WAN technology in all their branches, which is up from less than 1% today.[4] Keep in mind that not all SD-WANs are created equal, especially when it comes to the all-important issue of security. 90% of the SD-WAN vendors only provide a stateful firewall, which is not enough considering most customers will enable direct internet access.[5] For the best protection and performance, a Secure SD- WAN is required.

Firmographics and characteristics

What types of organizations are prime targets for Secure SD-WAN? Size matters, but it's not the only criterion. A number of vertical markets have unique requirements for Secure SD-WAN, but in reality, any distributed organization with the characteristics below is a good candidate.

Organization size

- Large organizations (>1,000 employees, $500M and above wallet spend)—almost half will use SD-WAN
- Midmarket $249M-$499M wallet spend
- Any organization with multiple locations, including headquarters, branches, corporate data centers, colocation/hosting facilities, cloud providers, and more

Verticals

- Retail: Need to digitize consumer shopping experience to remain relevant, but this increases attack surface. Concerns around PCI, guest Wi-Fi, omnichannel model.
- Hospitality: Need to protect all properties and guests. Secure guest Wi- Fi, in-room entertainment systems, and reservation systems. Presence analytics.
- Financial services: Always a high-value target. Branch and virtual office consolidation, simplified IT management, omnichannel models, constant security focus.
- Healthcare: Another high-value target. Healthcare patient records bring a high price on the black market; HIPAA compliance and the difficulty of dealing with inherited technologies/products due to M&A activity complicates matters.
- Government: Key target for attacks; need to provide citizen services and consolidate disparate networks.
- Education: Need to scale bandwidth, provide secure access across multiple locations.

Characteristics

- Distributed organizations (often as result of mergers/acquisitions)
- Concerned about escalating cyber threats
- Need to adapt rapidly to changing business needs, turn on new services, bring up branch offices
- Want to simplify setting up and running remote locations
- Constantly trying to drive down costs
- Must stay in compliance with PCI DSS, HIPAA, SOX, other regulations

Customer analysis, key drivers

All too often, branch offices and remote locations have been assembled piecemeal, resulting in complicated infrastructures of incompatible pieces. Branch offices need local expertise in multiple types of hardware, software, and operating systems, difficult to install and configure, and all managed by separate consoles. While that may have worked for a time, three current trends spell problems for traditional WAN in distributed branch networks as we move forward.

Business growth

Organizations, as part of their digital transformation, are driving faster business growth by adopting cloud. Data-center applications are migrating to multi-cloud environments (e.g., AWS or Azure). Employees are increasing their direct access to business-critical SaaS applications. The problem is, existing WAN infrastructures weren't designed to secure this explosion in traffic (especially voice and video). Simply backhauling branch traffic through the data center to provide needed security doesn't work, due to limited visibility into SSL-encrypted traffic and other factors. This can actually result in an overall weaker security posture. But the organization can't afford to let security stand in the way of business growth security focus.

Improved user experience

At the same time, many organizations are moving toward an omnichannel user experience to increase relevance and customer satisfaction. Here, the impact of backhauling branch traffic through the data center often results in poor application performance at branches. This is the exact opposite of what we hoped to achieve: the best performance for users and customers alike that is also secure.

Integrated security

The legacy approach of adding new point products to keep up with evolving networking and security requirements has reached a tipping point, when it comes to supporting a geographically distributed organization. Instead, leaders look for a simplified solution that consolidates routing, security, SD-WAN, and WAN optimization. They need centralized management in a single console, and the ability to rapidly provision new branches. This would allow network engineering and operations leaders to simplify their infrastructure while providing better security and productivity at branch locations.

Pain points

Business growth, improved user experience, and integrated security all contribute to the move toward Secure SD-WAN, whether it's coming from the security team or the networking team. Digging a bit deeper reveals the true pain points behind these drivers.

Pain point 1 – complex operations

Business growth can be negatively impacted when the organization struggles to manage routing, security, SD-WAN, and WAN optimization separately, through way too many point products, each of which requires a specific set of expertise. They want fewer things to manage and fewer things to fail, without compromising productivity, security, or connectivity.

Pain point 2 – budgetary constraints

Another pain point aligned with business growth stems from budgetary concerns. With demand for connectivity increasing, many organizations are looking for a low-cost alternative to WAN. They want to avoid the expense of the private MPLS lines upon which WAN relies, and many have a mandate to reduce branch OpEx. At the same time, they need to look for ways to help maintain service-level agreements (SLAs) for applications by dynamically managing bandwidth allocation and monitoring link performance at a granular level. While many organizations are not discarding their MPLS networks, but rather scaling down their use as they adopt SD-WAN,[6] cost remains a big concern (as indicated by 47% of respondents in the Gartner survey).[7]

Pain point 3 – poor application experience

Without advanced capabilities, WAN solutions can slow down SaaS applications, video and voice, and negatively impact end-user productivity. The problem is that in today's branches, legacy routers don't give business-application-level visibility. All traffic is going to MPLS, then backhauling to the cloud, so the user experience continues to suffer. This may be why Gartner sees the overall branch router market declining at a –6.3% CAGR and believes the legacy router segment will suffer a huge –28.1% CAGR decline through 2020.[8] Distributed organizations need a solution that can manage a broad range of applications, applying routing policies at a granular level to route business-critical applications over the most efficient WAN connection at any given moment.

According to a Gartner survey, 58% of customers reported performance as a concern during WAN initiatives.[9]

Pain point 4 – network and security conflicts

Secure SD-WAN allows organizations to not just improve performance on the networking side but also simultaneously implement a security model that can keep pace with the rapid growth and changes of the digital transformation era. The ideal approach is to combine and consolidate WAN networking and security in a single, effective, secure solution. The same Gartner survey showed that 72% of respondents named security the top concern during WAN initiatives.[10]

Persona: VP/director of network engineering

The VP/director of network engineering is the primary audience for Secure SD-WAN discussions and sales efforts. This person reports to the CIO and is responsible for architecture design and management of corporate networks and policies. Overall job performance is measured on uptime, network performance, and elasticity of the network. The person is not typically responsible for security.

Concerns:

- Protect the network without compromising performance
- Provision new branches quickly and easily while ensuring security in the face of an expanding attack surface
- Reduce the complexity of tracking, reporting, and managing network risk and compliance requirements
- Automate security workflows and threat intelligence sharing, to support limited networking staff and security skill sets
- Reliability, performance, integration
- Ensure low TCO

Fortinet Secure SD-WAN value add:

- Provides comprehensive protection in a single solution
- Easy (zero-touch) implementation
- Enables management of all branches via a single pane of glass
- Integrates with FortiGuard threat intelligence and sandbox to protect against latest threats and advanced threats
- Offers unbeatable performance and scalability
- Ensures the lowest TCO and compliance requirements
- Automate security workflows and threat intelligence sharing, to support limited networking staff and security skill sets
- Reliability, performance, integration
- Ensure low TCO

Persona: technical buyers/ influencers

There are several technical buyers and/or influencers, both from the security and the networking side of the business.

Security admin/architect/engineer

The security administrator, architect, and/or engineer is responsible for identifying and communicating risk, and designing/implementing solutions that balance business needs with security.

Concerns:

- How new technology will affect security
- Recent attacks that target unsuspecting employees through email and web

Fortinet Secure SD-WAN value add:

- Protects branches with FortiGate–with proven security effectiveness
- Offers multiple features such as SSL inspection, web filtering, DNS filtering, web application control, VPN
- Integrates with FortiGuard threat intelligence to protect against latest threats, and with sandbox to protect against advanced threats

Network engineer

The network engineer must provide assurance of secure direct internet access for the branches even during high-growth periods. They must centrally manage everything from HQ.

Concerns:

- Ensure sensitive applications like voice and cloud email meet performance SLAs
- Avoid service interruptions and burdensome administrative workflows
- Provide network connectivity using available physical interfaces such as Ethernet, cable, 4G, etc.
- Reduce extra work created by point solutions that have little or no integration

Fortinet Secure SD-WAN value add:

- Allows use of broadband to increase network application performance and reduce costs
- Prevents SLA breaches by prioritizing business-critical applications and dynamically sending them on the right WAN link
- Zero-touch provisioning
- Enables management and monitoring through a single pane of glass

Persona: business buyers/ influencers

Business buyers/influencers include both the branch office managers and the financial team at the purchasing organization.

Retail store manager

The retail store (or branch office or school) manager relies on the network to deliver services used for operations, communications, collaboration, and other business functions, and must ensure an optimal customer experience.

Concerns:

- Easy access to applications without compromising security
- Speed—business-critical applications must perform at the level expected by users
- Reliability and availability with no technical expertise required

Fortinet Secure SD-WAN value add:

- Offers the benefits of direct internet access without impacting performance or compromising security
- Provides the highest level of service
- Requires no technical expertise—all can be handled from HQ

CFO, finance/procurement

The CFO is responsible for overseeing financials and developing new business strategies. Personnel from the finance and procurement departments are also key players especially if an existing Fortinet customer.

Concerns:

- Affordable protection from the latest advanced threats
- Regulatory compliance
- Protecting branch office access, communications, applications, personal information—data security in motion and at rest

Fortinet Secure SD-WAN value add:

- Provides the most comprehensive protection against known and emerging threats
- Ensures the lowest TCO
- Assists with ensuring regulatory compliance, especially for protection of data in motion and at rest

Secure SD-WAN high-level messaging

Fortinet Secure SD-WAN | Security Driven Networking

How Fortinet addresses the pain points and persona-specific needs:

- **Complex operations:** Fortinet simplifies operations by consolidating point products in a single solution that boasts a zero-touch installation with automated provisioning. This reduces risk, improves operations, and tightens security. Fortinet SD-Branch also decreases TCO with one console instead of many, without the need for silos of expertise with management for wired LAN/WLAN, SD-WAN, and security via a single pane of glass.

- **Poor application experience:** Fortinet provides an optimal user experience. Because Secure SD-WAN is business-application aware, it can route applications across the most efficient WAN connection at any given moment. This is especially important for business-critical applications.

- **Poor application experience:** Fortinet provides an optimal user experience. Because Secure SD-WAN is business-application aware, it can route applications across the most efficient WAN connection at any given moment. This is especially important for business-critical applications.

- **Budgetary constraints:** Fortinet reduces the cost of moving from MPLS to direct internet connectivity by almost 40%. Further cost reductions come from the Fortinet low TCO, with fewer products to manage, less product expertise required, and lower overall maintenance requirements.

Value proposition and benefits

Fortinet Secure SD-WAN supports business growth, provides a better user experience, and delivers integrated security while reducing costs.

- Fortinet supports business growth through a low TCO: zero-touch deployment, ease of management, and support for multiple communications channels are combined in a single multi-path WAN solution.
  - **Benefit:** aids organizations to achieve rapid growth while reducing cost
- User experience: better visibility into business applications, and the ability to steer application traffic dynamically over any WAN link. Fortinet provides the best routing possible for more than 5,000 applications.
  - **Benefit:** ensures optimal user experience due to quick and efficient routing of applications across the best WAN link
- Integrated security: proven built-in next-generation firewall with SSL inspection, threat intelligence, IPS, WAN controller, anti-malware FortiSandbox Cloud, and more. No need for separate products, installation, configuration, management, and maintenance
  - **Benefit:** ensures optimal user experience due to quick and efficient routing of applications across the best WAN link

The experts agree:

Gartner says Fortinet should be shortlisted for all WAN edge opportunities globally[11] and should be considered by organizations of all sizes and verticals for SD-WAN projects globally, especially when strong, built-in security capabilities are a key requirement.[12]

NSS Labs says Fortinet Secure SD-WAN delivers exceptional total cost of ownership: $5@749 Mbps.[13]

Buying scenarios

There are many opportunities to introduce Fortinet Secure SD-WAN. Some of the more common ones:

- **Third-party NGFW in place.** Third-party NGFWs may only support WAN link load balancing and provide only one component of a secure SD-WAN solution, so branch offices are still left with the burden of complexity and management of individual products. Fortinet Secure SD-WAN is a tightly integrated solution for branch consolidation. Customers who want to preserve their existing non-Fortinet firewall investment can still benefit from deploying Fortinet Secure SD-WAN as a VM solution.
- **No next-gen firewall.** Customers who do not have a firewall solution in place can expect to see both performance and scalability issues. Deploying a FortiGate NGFW with Fortinet Secure SD-WAN offers a consolidated solution that combines branch networking and security capabilities.
- **FortiGate NGFW in place.** Having sold the FortiGate NGFW, it is now just a simple matter of turning on secure SD-WAN as a value-added service to the existing deployment. If you do not, you are leaving money on the table.
- **Router replacement.** This is a quick path to revenue, as Secure SD-WAN can be introduced in a nondisruptive manner into the existing WAN when legacy routers are nearing their end of life. Keep in mind that the alternative is more routers, WAN optimization, and security devices like firewalls and secure web gateways—and more cost and complexity.
- **Replace other vendor's SD-WAN.** Going with another vendor can be a risky proposition, since many SD-WAN vendors are startups or early-stage companies, most have little to no built-in NGFW security, and they do not have the track record of Fortinet. Remember that without SSL decryption support, SD-WAN products are blind to malware and exploits. Fortinet brings it all: superior security as validated by NSS Labs test results, corporate stability and scalability, the simplicity of a single pane of glass, and a less-complex, tightly integrated solution for branch consolidation.

Use cases

Fortinet has a strong track record of success with large distributed enterprises and organizations, managing more than 10,000 branches. Some recent customer success stories include

World's largest independent claims management company

Problem: Crawford & Company wanted to reassess its network infrastructure as it came up for renewal: The traditional WAN connecting more than 150 locations did not provide the agility or cost efficiency the company needed in a rapidly changing marketplace. They wanted to use SD-WAN technology to scale network capacity and drive efficiency.

Solution: Fortinet Secure SD-WAN was selected because of its ease of use at scale and its robust, integrated security. The company is also deploying management, analytics, and network access control (NAC) from Fortinet for the global network.

Results: Crawford & Company realized significant efficiencies due to streamlined reporting and analytics, significant cost avoidance for rolling out the legacy NAC solution globally, and seven-figure annual savings by retiring the network at headquarters.

Major home retailer

Problem: This customer wanted to reduce WAN edge costs by replacing MPLS links with an SD-WAN solution. They hoped to maintain a high-level application experience at the same time.

Solution: The customer chose Fortinet Secure SD-WAN over competitors to consolidate WAN solutions with LAN Wireless and Access Switching solutions, nearly 1,000 FortiGate solutions along with centralized management, centralized logging and analysis, and support services.

Results: Cost reduction and simplified operations across all its branch locations. Fortinet ensures a high-quality experience for business-critical applications. Cloud optimization capabilities for applications across multi-cloud environments futureproof the investment.

Large North American educational institution

Problem: This customer was looking to enable secure direct internet access for each of their 80,000 students and guarantee a consistent application experience across data-center and public cloud deployments. All of this at a low cost, but without sacrificing security.

Solution: Fortinet Secure SD-WAN was chosen due to its unique architecture that provides unified SD-WAN and SSL inspection capabilities within a single-pane-of-glass management solution. The deployment included more than 150 FortiGates with SD-WAN optimized for remote school bandwidth requirements, as well as additional services and support.

Results: Fortinet aligned with the district's business goals and achieved cost savings by consolidating multiple key services into one management platform. Fortinet integrated logging and analysis, centralized management, and support for all remote locations make this an efficient and cost-effective solution.

Validation

Why Fortinet Secure SD-WAN?

Fortinet enables organizations to solve the secure communications problem for distributed locations quickly and easily. And it provides a solution that is easy to manage, agile, reliable, flexible, and ultimately secure. The only vendor with a custom-designed ASIC to provide the fastest application identification and steering in the industry, while providing connectivity and advanced security capabilities 10x faster than the competition, Fortinet is the market-share leader in providing security solutions to the distributed organization.

Industry recognition:

Gartner 2019 Magic Quadrant for WAN Edge Infrastructure

- Placed highest in ability to execute and completeness of vision in the Challenger quadrant
- Fortinet should be shortlisted for all WAN edge opportunities globally
- The Fortinet Secure SD-WAN helps reduce WAN costs, enhances application experience, and reduces complexity
- Unlike most SD-WAN vendors, Fortinet provides fully integrated security

NSS Labs' Software-Defined Wide Area Networking Test Report

- Fortinet has received its second consecutive SD-WAN Recommended rating
- Voice and video experienced virtually no loss of quality
- Fortinet Secure SD-WAN delivers the lowest total cost of ownership: $5@749 Mbps, 8x better than the average TCO from all other vendors
- Legacy of security and strong pedigree in connectivity

Peer Recognition—Gartner Peer Insights

- "We tested some other full-stack SD-WAN solutions like Cisco Meraki and Aruba DS-Branch before and concluded that Fortinet was our best choice"
- "Easy to manage yet powerful"
- "Value for money in terms of features vs. cost in comparison to the competition"
- "The Fortinet security solution is powerful, and their adaptation of SD-WAN makes them a compelling component of any network"
- "SD-WAN features along with NGFW security is a win-win combination"
- "Best quality hardware with secure solution along with SD-WAN features"

Why now?

SD-WAN is growing rapidly, and Fortinet has the leading solution.

- By 2023, more than 50% of the existing installed base of branch office routers will have been replaced by modern WAN edge solutions.[14]
- SD-WAN revenue will grow at the expense of traditional routers and by capturing funds that would have been spent on WAN optimization controllers, firewalls, and MPLS services.[15]
- Partners can provide high-demand SD-WAN solutions, implement quickly, increase revenue streams, and improve customer satisfaction with Fortinet
- Secure SD-WAN.

Competitive information

There are more than 60 competitors in the SD-WAN space, but few offer SD-Branch capabilities.

And none offer the completeness of vision of Fortinet with security, SD-WAN, Ethernet, and wireless, consolidated into one platform.

	Fortinet	VeloCloud	Versa Networks	Cisco ISR/Viptela	Cisco Meraki	Palo Alto Networks (not available untill 2020)
WAN Path Controller w/ Application SLA	Yes	Yes	Yes	Yes	Limited	Limited
NGFW w/SSL Inspection	Yes	No	Limited	Yes	Limited	Yes but slow
Application Awareness	Yes	Yes	Some	Yes	Limited	Basic
Dynamic Failover Time	Short	Short	Short	Short	Very long	No
Scalable Auto IPsec VPN Overlays	Yes	Limited	Limited	Yes	Limited	No
Single Management Console for Security & SD-WAN	Yes	No	??	No	Yes	Yes
Zero-touch Provisioning	Yes	Yes	Yes	No	Yes	No
TCO	Low	High	Moderate	High	Moderate	Moderate

Differentiators

The SD-WAN market has become overcrowded, and there is a lot of noise that confuses customers. It is important to understand the four types of competitors, and the strengths and weaknesses of each.

Pure-play vendors (e.g., VMware [VeloCloud], Versa Networks, Oracle [Talari], CloudGenix)

What they are:

- Early-stage solutions or startup vendors with no or primitive NGFW security, no access layer components

How to compete:

- SECURITY—stress the NSS Labs test results and Recommended rating
- STABILITY—Fortinet will be around to support you and grow with you (unlike startups or niche players that may be acquired or go out of business)
- SIMPLICITY—Fortinet has true single-pane-of-glass management, zero-touch install
- Lower TCO

Networking vendors (e.g., Cisco Meraki, ISR + Viptela)

What they are:

- Products where SD-WAN is a feature (not the entire solution) but with built-in NGFW and access layer solutions

How to compete:

- SECURITY—Fortinet is extremely effective (reference NSS Labs report)
- SCALABILITY—Fortinet has unbeatable performance and scalability
- SIMPLICITY—Fortinet has true single-pane-of-glass management and easy zero-touch install. With Cisco, the sale will involve more products and require more silos of expertise
- Lower TCO

WAN optimization (e.g., Citrix, Riverbed, Silver Peak)

What they are:

- These vendors claim SD-WAN to stay relevant. But SD-WAN is only a component or a feature, and they lack NGFW and access layer components

How to compete:

- SECURITY—all branch offices now need a full security stack with unbeatable performance and scalability
- VALIDATED—go with the best, award-winning (NSS Labs), true single-pane-of-glass management, tightly integrated solution
- Lower TCO

Traditional NGFW vendors (e.g., PANW)

What they are:

- These vendors only support legacy WAN link load balancing, and provide only a component of a secure SD-WAN solution

How to compete:

- Modern Secure SD-WAN—Fortinet has it, traditional NGFW vendors don't
- SECURITY—Fortinet is the leader when it comes to security effectiveness
- SIMPLICITY—Fortinet has true single-pane-of-glass management
- Lower TCO

Learn

A variety of resources are available to partners to understand the opportunity:

Access the NSE Institute and Sales Center. Complete the Security Fabric Workbook, Customer Presentation and Value-Added Selling. Complete NSE 3 FortiGate Firewall Entry-level Products.

Study this playbook.

Learn how your teams can have comprehensive conversations and guide customers through Secure SD-WAN Specialization Training. (Partner Portal log-in required)

Review the Secure SD-WAN Hub:

- Video: Product Demonstration
- NSE Insider: SD-WAN Landscape
- Change to Product: What is SD-WAN

Review the Product Pages.

Promote

Drive your business by using these assets on our SD-WAN Hub in the partner portal to promote Secure SD-WAN with your customers and prospects:

- Email Campaign
- eBook: Network Leader's Guide to Secure SD-WAN
- Video: Addressing the WAN and Access Edge with SD-Branch

Use the Cisco Takeout Campaign to accelerate sales of Fortinet Secure SD-WAN by highlighting the dangers of legacy routers, leveraging Cisco's confusing array of offerings and showing the benefits of the Fortinet approach.

Use this elevator pitch with prospects:

Fortinet Secure SD-WAN lets …

Multibranch organizations improve efficiency and reduce operating expenses while accelerating adoption of cloud applications and other digital transformation initiatives without sacrificing security, performance, or cost.

By delivering the ability to …

Centrally define and manage security posture across the extended enterprise while maintaining consistent visibility and network performance.

Unlike disparate point products, Fortinet Secure SD-WAN delivers …

A tightly integrated, easy to deploy, easy to manage and fast time-to-value branch networking solution that reduces the burden on IT/sec teams. This ultrafast SD-WAN ensures efficient business operations and best-of-breed security with high performance and ease of use to enable branch office transformation.

Sell

Tips to consider for converting prospects into deals:

Know your audience: See the Persona section of this playbook for details.

Use the Network Leader's Guide to Secure SD-WAN to help network buyers/influencers understand how Secure SD-WAN helps them in multiple ways.

Perform a needs analysis with both the technical and the business buyers to understand the organization's needs. Engage with Purchasing early on.

Use CTAP for SD-WAN to understand your prospect's router usage and identify potential security risks. The resulting report will include actionable recommendations specific to your customer's network; use it to educate key decision-makers on the need to invest in a branch network infrastructure.

Identify key regulations such as PCI, HIPAA, GLBA, GDPR, CCPA in order to understand pressures to avoid fines and noncompliance.

Demonstrate the solution—show the demo and/or the use-case video.

Initiate a Proof of Concept using partner's own templates.

In addition, the SELL section on the SD-WAN Hub in the partner portal includes the following assets:

- Secure SD-WAN Customer Presentation
- Gartner Peer Reviews—provides information from third-party organizations about which SD-WAN solution is right for you
- Cyber Threat Assessment for SD-WAN
- Partner Sell Sheet: Secure SD-WAN

TIPS TO CONSIDER
QUALIFYING AND OBJECTION HANDLING

Sell: qualifying and objection-handling

Qualify the opportunity

Use the drivers, pain points, and differentiators in this playbook and the call scripts to qualify opportunities.

- What strategic initiatives do you have—e.g., grow business by bringing new branch offices online (how many?), move applications to the cloud (concerns about latency?), refresh branch equipment (timing?).
- Is cost an issue? Do you face increasing traffic requirements to handle cloud or VoIP phones, cost of multiple links, high cost and complexity of MPLS? What would it be worth to replace MPLS or avoid it?
- Does complexity cause problems? Do you lack the resources, expertise to manage multiple products? Would you like to simplify branch office communications while guaranteeing QoS?
- Do you need optimal performance for business-critical applications? Do you experience latency when turning on content-processing features? Are LOB managers telling you they need specific response levels to meet SLAs?
- Is regulatory compliance with GDPR, HIPAA, GLBA, PCI a concern? Do you need to secure data at rest or in motion?

Once prospects have been uncovered and qualified, deal with any objections as shown below. Use the proof points and industry validation from page 14 to move the deal along.

Objection-handling

I'm concerned about the ability to provide adequate security to my branch offices.

- Fortinet Secure SD-WAN provides best-of-breed security because it is integrated with FortiGate, a leader in the 2019 Gartner Enterprise Firewall MQ.

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 Secure SD-WAN is easy to implement and manage, with a single pane of glass to monitor and manage everything.

My LOB/branch managers have specific requirements for application QoS, and we have more than one type of connectivity link.

- Fortinet Secure SD-WAN is a multi-path WAN solution that can automatically switch links based on the quality of the connection. You can link your network and security paths across the world, through the internet, 3G/4G, or private WAN links. And you can achieve the higher SLAs for the business applications your branch offices depend on.

I need to reduce my WAN costs, but I haven't budgeted for this expenditure.

- We can help you build a business case and obtain budget and approval, by looking at your planned security and networking investments and factoring in the cost savings that can be achieved by implementing Fortinet Secure SD-WAN.

I have Palo Alto/Cisco and want to look at their solutions for secure SD-WAN.

- Either vendor's option will require additional management, since they both require more appliances and multiple management consoles. This not only puts pressure on people resources but increases your TCO including the overhead costs of implementing these solutions. Security is a feature and not native like Fortinet Secure SD-WAN.

Partner benefits

Partner benefits:

Partners who sell the Fortinet Secure SD-WAN solution to their customers benefit in several tangible ways.

Increased revenue.

Generate new or additional streams of revenue. The SD-WAN market is large and growing. According to IDC, the market opportunity for SD-WAN is $4.5B in 2022—a 40% YOY growth. With quick configuration and deployment, the opportunity for recurring revenue—in the form of managed services—can arrive sooner.

Consolidated solution.

With Fortinet Secure SD-WAN, there are fewer things to manage, fewer things to fail. Customers get the same connectivity benefits of standalone SD-WAN without having to worry about how to ensure both performance and security. The Fortinet security processor delivers the industry's best IPsec VPN and threat protection—both critical for SD-WAN use cases.

Scalable solution.

No matter how large the branch or distributed organization, with Fortinet Secure SD-WAN it is the same operating system, the same management, the same operation and process parameters. Fortinet provides scalable management and zero-touch deployment, to reduce complexity and provide a single pane of glass across all branches. Fortinet is the only vendor capable of managing 10,000 plus branches and has a proven track record of large distributed organization deployments worldwide.

Native SD-WAN.

Simplify the sales cycle with an all-in-one solution. FortiGate provides best-of-breed integrated SD-WAN networking and security capabilities in a single device, with reduced TCO. FortiGate is the market-share leader in enterprise branch security and adds enhanced SD-WAN capabilities in the latest FortiOS 6.0. The WAN path controller allows customers to efficiently distribute applications per WAN link while maintaining performance SLAs. And the new SaaS application database enables efficient, direct internet access.

Improved sales cycle.

Quicker sales and a quicker path to revenue. Fortinet Secure SD-WAN offers the flexibility to be nondisruptively introduced into the existing WAN with eventual replacement of the legacy routers. Once architected, the security is not only world class but also built in. When you engage the security architect, It is not for them to pick a firewall. It is to have a high-level discussion about how their new infrastructure can be easily secured.consoles. This not only puts pressure on people resources but increases your TCO including the overhead costs of implementing these solutions. Security is a feature and not native like Fortinet Secure SD-WAN.

Footnotes

[1] Danielle Young, et al., "Gartner Group: SD-WAN Survey Yields Surprises," IEEE ComSoc Technology Blog, November 19, 2017.

[2] "SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022," IDC, August 8, 2018.

[3] Gartner quote from Playbook SD-WAN Final, April 8, 2019, slide 3.

[4] Andrew Lerner, "Predicting SD-WAN Adoption," Gartner Blog Network, December 15, 2015.

[5] "In Search of the Right SD-WAN Solution: Cisco SD-WAN Security," Gartner, January 2019.

[6] John Burke, "2019: The Year of SD-WAN," Nemertes, 2019.

[7] Gartner Survey Analysis—op. cit.

[8] Gartner SD-WAN Early Findings—op. cit.

[9] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth," Gartner, November 12, 2018.

[10] ibid

[11] Christian Canales, et al., "2018 Magic Quadrant for WAN Edge Infrastructure," Gartner, October 18, 2018.

[12] Mike Toussaint, et al., "2019 Magic Quadrant for WAN Edge Infrastructure," Gartner, November 26, 2019.

[13] John Maddison, "NSS Labs NGFW Report: Fortinet Receives 4th Consecutive Recommended Rating," Fortinet, July 26, 2017.

[14] Mike Toussaint, et al., "Critical Capabilities for WAN Edge Infrastructure," Gartner, December 3, 2018.

[15] Gartner MQ – op. cit.