



#WeAreExclusive

In partnership with
FORTINET®

Go to Market Battlecard



SD-WAN Battlecard

What is it?

Secure SD-WAN is a fully managed service from [PARTNER]. We are using Fortinet Next Generation Firewalls on-site in place of the traditional router. This provides a router, a security appliance and the intelligence to detect over 3,000 different business applications. We can then apply a single security and application acceleration policy across the whole organisation. Every location has faster access to their business apps and is more secure than ever before.

Elevator Pitch

Your teams are using new digital ways of working to provide a personal and unique experience to your customers. They use multiple devices, working on mobile or tablet devices and spending less time sat at fixed workstations. Staff are working remotely and business data has moved to cloud-based SaaS applications. There is more dependence on reliable Internet access than ever before. Has your network evolved to keep up?

LISTEN OUT FOR CUSTOMERS WHO:

- Are growing rapidly due to success, mergers or acquisitions
- Are in the hospitality and retail sectors where controlling Internet access performance is critical
- Are moving more workloads to the cloud and need to guarantee performance and security
- Are rolling out new VoIP or Unified Communications Solutions and want to guarantee performance
- Are concerned about unauthorised applications taking up bandwidth or causing security risks

Buyer Engagement

It's best to get buy-in for SD-WAN from business decision makers to start rather than technical managers or procurement teams. SD-WAN supports business change initiatives such as digital transformation and removing security/compliance issues from business risk registers.

THE TECHNICAL BUYER

The key points to emphasise are all around how we make life easier for the tech team. Reducing the risk of data breach by securing each location. Optimising network bandwidth to reduce "slow" applications. Identify unapproved applications and block them quickly. Get new sites up and running quickly with 4G/5G solutions. They benefit from high levels of resilience network availability.

THE BUSINESS DECISION MAKER

It's all about controlling costs and reducing risk. We have fixed price bundles. The solutions minimises network downtime and improves application performance for all internal and external customers. We provide performance on demand, keep all their apps working quickly and provide a secure flexible foundation for the business to grow.



SD-WAN Battlecard

Traditional Competitive Vendors

The standard range of Next Generation Firewall (NGFW) vendors all play here as well as some modern “born in the cloud” vendors. It’s key to position Fortinet as a leader not just in WAN Edge but also NGFW and Secure Remote Access. Typical competition would be Cisco (Viptella), Meraki and Silverpeak.

Long-standing providers of security appliances such as Cisco and Meraki are still offering siloed solutions; a dedicated firewall appliance which then needs a number of additional solutions to bring capabilities such as IDS/IPS, Anti-Malware or Web Filtering. **Only Fortinet offers a complete offering.**

Non-Traditional Competitive Vendors

Secure Access, Secure Edge (SASE) providers have predominantly been moving away from hardware-based solutions. This new set of providers offer services using cloud-hosted platforms like Zscaler and Cloudflare. The most realistic competitor here is Zscaler. They are the leader in Secure Web Gateways hosted in the public cloud and have a very comprehensive set of features to rival our offering with Fortinet. The key things to know are; A client would need to take Zscaler’s most expensive package to get all the required features; MSP’s report application performance issues as every piece of data is sent to the Cloud for inspection; Zscaler works well in an entirely remote workforce but is not a good branch office solution.

Summary

A number of these “born in the cloud” offerings provide a single point of service which is included in the overall portfolio we offer in our Fortinet solution. This should be the primary pushback in any competitive discussions. These solutions offer part of the answer and then leave the customer with a disparate set of tools to manage in order to achieve the overall security required.



© Gartner 2020 Magic Quadrant for WAN Edge

SD-WAN CAN REPLACE THESE TECHNOLOGIES

Application Accelerators | Intrusion Detection and Prevention Systems | VPN Concentrators | Web Content Filtering Solutions



SD-WAN Battlecard

Good to Know: Meraki messaging suggests customers don't need an MSP

One of the common vendors in this space is Meraki. Their messaging to Enterprise customers encourages a self-service approach to SD-WAN i.e. Take Meraki routers, add simple Direct Internet Access (DIA) connects and remove the Managed Service Provider and MPLS from the equation. In this model, they would suggest that SD-WAN is cheaper. There are drawbacks to this model such as;

Lack of expertise in Managed WAN

As an MSP, you have years of experience managing IT Solution, vendors and suppliers. Customers who self-serve are unlike to have this scale or breadth of experience.

Meraki provides an incomplete solution

In order to provide a simplified single dashboard, compromises have been made around the security and level of control available. The features are not as comprehensive when compared to the Fortinet solution. Meraki requires additional Cisco software products to be able to provide the same level of application control and security. All of this is included in the Fortinet solution.



2020 LEADER
by Gartner for WAN Edge
2019 RECOMMENDED
by NSS Labs for SD-WAN



2020 LEADER
by Gartner for Firewalls
2019 RECOMMENDED
by NSS Labs for NGFW



SD-WAN Battlecard

Conversation Starters

What concerns, risks or challenges do you perceive with your current connectivity solutions?

Is it matching your business goals? Is it reliable? Do you have a good service partner?

What is the impact of an outage on your network?

Loss of productivity, loss of earnings, loss of business reputation, loss of status?

Do your applications perform well wherever your team are based?

Is there a marked difference when working remotely, over WIFI or at certain site locations?

Do you use online Collaboration solutions such as Microsoft Teams or Cisco Webex?

How well does it perform for you, are you able to use the HD Video calling without issues?

Are you able to control which applications take priority on your network?

Do some apps just take over unexpectedly and saturate the network? Can you identify unapproved applications and see what impact they are having?

Keywords

Reduce business risks, improve speed, improve network availability, slow performance, home working, mergers and acquisitions, network security, application performance, shadow IT

Co-Sell Opportunities

- ✓ LAN and WIFI
- ✓ Connectivity
- ✓ Professional Services
- ✓ Cloud or Hosting Solutions
- ✓ Backup and DR Services