SD-WAN Battle Card: Competitive Landscape

for Internal and Partner Audiences Only

SD-WAN Market Statistics

The SD-WAN market is poised for high growth. According to Frost & Sullivan, the global market revenue was $300M in 2017, but expected to reach $1.5B in 2022, following a 38% CAGR. Gartner reports that SD-WAN is the most frequent networking inquiry among Gartner clients, in addition to being one of the most popular I&O topics. Similarly, Gartner estimates the market to reach just under $2B by 2022.

Target Markets: distributed enterprises and mid-size enterprises, some selling opportunity exists for small business with mutli-WAN

Target Industries: retail, healthcare, finance & banking, government, manufacturing, distribution

SD-WAN & Networking Infrastructure Providers

Viptela, SilverPeak, Versa, Talari, etc. (Gartner tracks 23 different vendors). These companies formed to meet this market with a specialized SD-WAN product, and stake their name on their software and management platform. Large network infrastructure companies such as Cisco (Viptela), Citrix, VMware (Velocloud), and others have been acquiring SD-WAN point product providers, because they want to leverage their relationship with large customers to consolidate all networking including SD-WAN. Some infrastructure companies have a security offering as well, and may choose to combine the products into one solution (eg Cisco Meraki).

Internet Service Providers (ISPs)

Verizon (Cisco Viptela or Meraki), AT&T (Velocloud), Centurylink (Versa Networks), Deutsch Telekom, British Telecom (Nuage) and others have packaged SD-WAN solutions for businesses, many of which are OEM solutions from SD-WAN providers listed above. Ironically, these are the same companies profiting with more traffic using expensive MPLS and WAN connections, which may cause some potential customers to be naturally skeptical of the efficacy of their SD-WAN offering. WatchGuard partners may find themselves competing with ISPs, particularly with small businesses.

Security Providers

WatchGuard, Fortinet, SonicWall, Meraki, etc.: These are familiar competitors and they are all coming out with SD-WAN features. The advantage that we have over other SD-WAN options is that we are willing to provide SD-WAN at no/little cost in order to get the security business, which makes it hard for others to charge for it – except where they have a strong brand preference already built in the account, or they offer SD-WAN features beyond what the security providers typically offer, such as with a dedicated internet backbone for backhauling and prioritizing traffic (Cato, Bigleaf).

SD-WAN Product Characteristics

The following areas are commonly cited as the functional requirements for an SD-WAN product:

- perform the WAN routing necessary to distribute traffic across multiple WAN transport mediums (e.g. MPLS, Internet, 4G/LTE, etc.)
- allocate traffic dynamically based on user-defined policies and near-real time measures
- provide a simplified management GUI and zero-touch branch site provisioning
- include integrated VPN technology with 128-bit, or higher, encryption
- allow direct connection of other network appliances such as firewalls and WAN acceleration

SD-WAN Use Case

Products the perform SD-WAN feature dynamic path selection, where the solution measures the performance of each WAN connection and chooses the best one for each type of traffic based on pre-configured policies. In other words, VoIP and video packets are sent to only those connections that currently meet minimum measurements as defined for bandwidth speed, jitter, latency and packet loss. If several WAN connections meet minimum performance thresholds, then traffic is sent to the least expensive line – along with email and other traffic types not impacted by network performance.

Companies benefit from SD-WAN by reducing WAN costs and decreasing network complexity through the use of this automation.

NSS Labs Testing Results

1. The first SD-WAN product test published
2. Many missing SD-WAN players
3. WatchGuard did not participate in testing, this is before our dynamic path selection feature was released.
4. Download the value matrix for free here: https://www.nsslabs.com/test/software-defined-wide-area-network-sd-wan/

Recommended:	Verified:	Caution:
• Fortinet	• Citrix	• Barracuda
• Talari Networks	• FatPipe Networks	• Cradlepoint
• VMware	• Forcepoint	
	• Versa Networks	

12/11/18

SD-WAN Battle Card: Winning with WatchGuard

For Internal and Partner Audiences Only

WatchGuard's Strengths

SD-WAN is included with security!

- We provide layered security, with fast HTTPS inspection – the best way to implement hybrid WAN.
- SD-WAN is offered at no additional charge for best value
- Dynamic path selection automates WAN selection for a simplified approach.
- All included in one management platform from one provider means lower network complexity and TCO
- We've proven that our RapidDeploy service is successful with over 12,000 deployments to date.
- Our platform is designed for distributed and midsize enterprises – allowing for higher utilization of IT staff.
- We make the optional dedicated backbone use case available by integrating with Bigleaf.
- We're not stopping - further releases of SD-WAN enhancements are planned for release in 2019.

Competitor's Weaknesses

SD-WAN Providers

These vendors tend to have very limited security, if they provide any at all. Helping prospects realize the close association between enabling direct access from the branch to Cloud resources and the need for upgraded security will allow you to pivot to WatchGuard's all-in-one solution.

ISPs

These are the same companies profiting with more traffic using expensive MPLS and WAN connections, and it should cause potential customers to be naturally skeptical of the efficacy of their SD-WAN product. Also, they are selling a marked-up OEM solution for higher overall cost.

Other Security Providers

SonicWall is just getting their zero-touch deployment started – and it will take a while to work out the kinks. Cisco Meraki does not inspect HTTPS traffic, creating a security vulnerability, and SonicWall appliances slow to a crawl with HTTPS. Fortinet adds a new license and expense for each security layer for higher overall cost, even though they appear competitively priced at the onset.

Claims	How-to-Win Response
Dedicated backbone is needed	Most SD-WAN adopters find that they don't really need a dedicated backbone for back haul, but if you are one of the few who does, then WatchGuard offers an integration with Bigleaf to address your use case.
Recommended by NSS Labs	This is the first known test of SD-WAN solutions, and only a small number of the solutions on the market were involved. When evaluating solutions for your business, testing a full range of products can give a better picture of the market options and solution pricing.
SD-WAN as a service	Many WatchGuard partners are managed solution providers, and can package a solution that includes WatchGuard's SD-WAN and much, much more.
100% Cloud-based management	Some companies say that they offer 100% Cloud Management, but it's only for their SD-WAN product, and doesn't include security or other IT features. WatchGuard provides centralized management for Firebox networking and security, as well as many Cloud-based interfaces where it makes the most sense.
Mean Opinion Scores	WatchGuard measures jitter, latency, and packet loss to assess link quality…which are the most widely-used. All providers, including WatchGuard, will continue to look at additional measures, like mean opinion scores, and will implement them once they reach the requisite maturity to add value to the overall solution.

SD-WAN + Security = Optimal IT Benefits

Be careful to not introduce gaps in coverage at the remote site. Are you opening the location up to direct attacks if you only deploy Cloud-based security? Is your branch office security comparable to HQ? When looking at the overall business requirements for your SD-WAN deployment, security is almost always a consideration. Therefore, the cost and simplicity benefits of an all-in-one solution consistently outweigh the other options.

	Core SD-WAN Features	Optional SD-WAN Features*	Enterprise-Grade Security	Reduced Network Complexity	Lowest Overall Cost
SD-WAN appliance with **embedded security**	✔	✔		✔	
SD-WAN appliance with **Cloud-based security**	✔	✔			
SD-WAN appliance with **security appliance in line**	✔	✔	✔		
Network security appliance with **SD-WAN embedded**	✔		✔	✔	✔

*SD-WAN with a dedicated backbone is an optional feature not required with all deployments.

Competitive Comparison: SD-WAN Features

For Internal and Partner Audiences Only

	UTM						SD-WAN								
	WatchGuard	Meraki	Fortinet	Sophos	SonicWall	Barracuda	Viptela	Versa	Bigleaf	Talari	Cato	Silverpeak	Fatpipe	Nuage	Velocloud
Multiple WAN Links	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
4G/LTE connections	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Link monitoring for jitter/loss/latency	yes	yes	yes	no	coming	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
Dynamic path selection	yes	yes	yes	no	coming	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
Application traffic management	yes	yes	yes	yes	yes	yes	yes	yes	yes	No	yes	yes	yes	yes	Yes
Quality of service (QoS)	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
VPN	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
Cloud based Management GUI	partial	yes	partial	partial	partial	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
Zero touch Deploy	yes	partial	yes	no	coming	yes	yes	yes	yes	yes	yes	yes	yes	yes	Yes
Works on standard hardware	no	no	yes	no	no		yes	yes	No	yes	No	Yes	yes	Yes	yes
Dedicated Internet backbone	no*	no	no	no	no	no		no	yes		Yes				No
NSS SD-WAN SVM	NA	NA	recc'd	NA	NA	caution	caution*	verified	NA	recc'd	NA		verified		recc'd

Key Insight: SD-WAN features are extremely consistent across products. Offering a dedicated backbone is rare, and not often a requirement.

*WatchGuard can offer a dedicated backbone with it's Bigleaf integration.

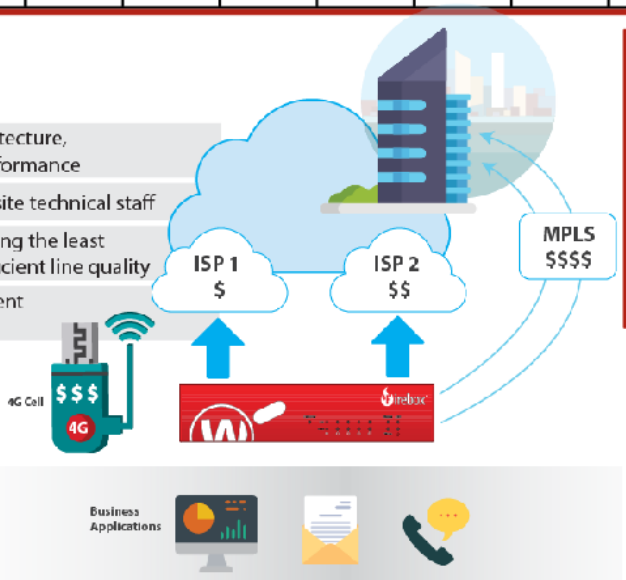
12/11/18

Competitive Comparison: Security Features

For Internal and Partner Audiences Only

	UTM						SD-WAN								
	WatchGuard	Meraki	Fortinet	Sophos	SonicWall	Barracuda	Viptela	Versa	Bigleaf	Talari	Cato	Silverpeak	Fatpipe	Nuage	Velocloud
Stateful Firewall	yes	yes	yes	yes	yes	yes		Yes	No	No	partial	yes	no	no	Yes
IPS	yes	yes	yes	yes	yes	yes	No	yes	No	No	No	No	No	No	No
GAV	yes	yes	yes	yes	yes	yes	No	yes	No	No	Yes	No	No	No	No
Web Filtering	yes	yes	yes	yes	yes	yes	No	yes	No	No	Yes	No	No	No	No
Sandboxing	yes	yes	yes	yes	yes	yes	No	no	No	No	No	No	No	No	No
DNS Firewall	yes	yes	yes	no	no	partial	No	no	No	No	no	No	No	No	No
Endpoint Malware detect & response	yes	no	yes	yes	3rd party	no	No	no	No	No	no	No	No	No	No
HTTPS Inspection	yes	no	yes	yes	yes	?	No	?	No	No	yes	No	No	No	No
NSS NGFW SVM	recc'd	NA	recc'd	caution	recc'd	recc'd	NA	recc'd	NA	NA	NA	NA	NA	NA	NA
3rd Party Integrations	Bigleaf								WGRD	Zscaler; PaloAlto	no				Zscaler

Common IT Problems	SD-WAN Benefits
Cloud-based applications that are sensitive to latency	✔ Build a hybrid WAN architecture, for better Cloud app performance
Difficulty finding skilled IT staff	✔ Reduce the need for on-site technical staff
Increasing bandwidth needs and WAN costs	✔ Control WAN costs by using the least expensive path with sufficient line quality
Greater network complexity	✔ Simplify WAN management with automation



Key Insight: SD-WAN providers are not security experts, and have generally not included these features in their products. Businesses needing to upgrade remote site security with their SD-WAN should find an all-in-one approach most advantageous.

Partners: contact your WatchGuard Sales Representative with questions and additional competitive insight.

12/11/18