



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at [wvOASIS.gov](http://wvOASIS.gov). As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at [WVPurchasing.gov](http://WVPurchasing.gov) with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

## Header 5

List View

**General Information** | [Contact](#) | [Default Values](#) | [Discount](#) | [Document Information](#)

Procurement Folder: 691866

Procurement Type: Central Contract - Fixed Amt

Vendor ID: 000000162797

Legal Name: INDICIUM TECHNOLOGY

Alias/DBA:

Total Bid: \$569,037.57

Response Date: 05/13/2020

Response Time: 13:06

SO Doc Code: CRFQ

SO Dept: 0803

SO Doc ID: DOT2000000157

Published Date: 4/30/20

Close Date: 5/13/20

Close Time: 13:30

Status: Closed

Solicitation Description: ADDENDUM 2 CISCO ROUTERS & SWITCHES OR EQUAL (63200125)

Total of Header Attachments: 5

Total of All Attachments: 5



Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

**State of West Virginia  
 Solicitation Response**

**Proc Folder :** 691866

**Solicitation Description :** ADDENDUM 2 CISCO ROUTERS & SWITCHES OR EQUAL (63200125)

**Proc Type :** Central Contract - Fixed Amt

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-05-13 13:30:00	SR 0803 ESR05132000000006658	1

VENDOR
000000162797 INDICIUM TECHNOLOGY

**Solicitation Number:** CRFQ 0803 DOT2000000157

**Total Bid :** \$569,037.57      **Response Date:** 2020-05-13      **Response Time:** 13:06:59

**Comments:** I also have a second configuration and alternate pricing I would like to submit.

**FOR INFORMATION CONTACT THE BUYER**  
 Crystal G Hustead  
 (304) 558-2402  
 crystal.g.hustead@wv.gov

<b>Signature on File</b>	<b>FEIN #</b>	<b>DATE</b>
--------------------------	---------------	-------------

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 1	10.00000	EA	\$2,325.820000	\$23,258.20

Comm Code	Manufacturer	Specification	Model #
43222612			

<b>Extended Description :</b>	3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 1 Smart Net Coverage
-------------------------------	--

**Comments:** Equal product quoted.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 2	10.00000	EA	\$748.000000	\$7,480.00

Comm Code	Manufacturer	Specification	Model #
43222612			

<b>Extended Description :</b>	3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 2 Smart Net Coverage
-------------------------------	--

**Comments:** Forticare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 3	10.00000	EA	\$748.000000	\$7,480.00

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 3 Smart Net Coverage
-------------------------------	--

**Comments:** Forticare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	3.1.1 Cisco ISR 4321 Series Chassis Bundle or Equal-Year 4	10.00000	EA	\$748.000000	\$7,480.00

Comm Code	Manufacturer	Specification	Model #
43222609			

**Extended Description :** 3.1.1 CISCO ISR 4321 Series Chassis Bundle or equal with Year 4 Smart Net Coverage

**Comments:** Forticare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 1	6.00000	EA	\$2,325.820000	\$13,954.92

Comm Code	Manufacturer	Specification	Model #
43222609			

**Extended Description :** 3.1.2 CISCO ISR 4331 Series Chassis Bundle or Equal with Year 1 Smart Net Coverage.

**Comments:** FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 2	6.00000	EA	\$748.000000	\$4,488.00

Comm Code	Manufacturer	Specification	Model #
43222609			

**Extended Description :** 3.1.2 CISCO ISR 4331 Series Chassis Bundle or Equal with Year 2 Smart Net Coverage.

**Comments:** FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
7	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 3	6.00000	EA	\$748.000000	\$4,488.00

Comm Code	Manufacturer	Specification	Model #
43222612			

<b>Extended Description :</b>	3.1.2 CISCO ISR 4331 Series Chassis Bundle or equal with Year 3 Smart Net coverage
-------------------------------	--

**Comments:** FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
8	3.1.2 Cisco ISR 4331 Series Chassis Bundle or Equal-Year 4	6.00000	EA	\$748.000000	\$4,488.00

Comm Code	Manufacturer	Specification	Model #
43222612			

<b>Extended Description :</b>	3.1.2 CISCO ISR 4331 Series Chassis Bundle or equal with Year 4 Smart Net coverage
-------------------------------	--

**Comments:** FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
9	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 1	55.00000	EA	\$2,325.820000	\$127,920.10

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.3 Cisco ISR 1101 4 port router or equal with Year 1 Smart Net Coverage
-------------------------------	--

**Comments:** FortiGate

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
10	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 2	55.00000	EA	\$748.000000	\$41,140.00

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.3 Cisco ISR 1101 4 port router or equal with Year 2 Smart Net Coverage
-------------------------------	--

**Comments:** Fortinet Fortigate

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
11	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 3	55.00000	EA	\$748.000000	\$41,140.00

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.3 Cisco ISR 1101 4 port router or equal with Year 3 Smart Net Coverage
-------------------------------	--

**Comments:** FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
12	3.1.3 Cisco ISR 1101 Series Port Router or Equal-Year 4	55.00000	EA	\$748.000000	\$41,140.00

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.3 Cisco ISR 1101 4 port router or equal with Year 4 Smart Net Coverage
-------------------------------	--

**Comments:** FortiCare

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
13	3.1.4 Cisco Extreme Networks 12 Port Switch or Equal	90.00000	EA	\$1,062.250000	\$95,602.50

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.4 Cisco Extreme Networks 12 Port Switch or Equal
-------------------------------	--

**Comments:** Fortinet FortiSwitches

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
17	3.1.5 Cisco Extreme Networks 48 Port Switch or Equal	70.00000	EA	\$1,900.630000	\$133,044.10

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.5 Cisco Extreme Networks 48 Port Switch or Equal
-------------------------------	--

**Comments:** FortiSwitch

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
21	3.1.6 Cisco Extreme Networks 24 Port Switch or Equal	15.00000	EA	\$1,062.250000	\$15,933.75

Comm Code	Manufacturer	Specification	Model #
43222609			

<b>Extended Description :</b>	3.1.6 Cisco Extreme Networks 24 Port Switch or Equal
-------------------------------	--

**Comments:** FortiSwitch





# **CISCO ROUTERS & SWITCHES OR EQUAL**

**RFP – WEST VIRGINIA DIVISION OF  
HIGHWAYS**

**CRFQ DOT2000000157**

# RFP – Fortinet Introduction

## TABLE OF CONTENTS

<b>1. Company Introduction .....</b>	<b>4</b>
<b>2. Fortinet—Your security business partner .....</b>	<b>6</b>
2.1 <i>Why Fortinet?</i> .....	6
Fortinet Security Fabric .....	6
Unparalleled Third-Party Certifications .....	7
More than 330,000 Customers and Growing .....	7
2.2 <i>Core Platform High-Level Overview</i> .....	7
<b>3. Fortinet Leadership .....</b>	<b>8</b>
3.1 <i>Industry Leadership</i> .....	8
3.2 <i>Unparalleled Third-Party Certification and Validation</i> .....	11
3.3 <i>Financial Highlights</i> .....	13
<b>4. Fortinet Advantage .....</b>	<b>15</b>
4.1 <i>In-House Security Research and Services</i> .....	15
FortiGuard Services .....	15
Industry-validated Security Effectiveness.....	15
FortiGate Solution Services .....	15
4.2 <i>FortiCare Services</i> .....	15
Support and Advanced Services .....	16
FortiCare Support Services .....	16
Advanced Services for Enterprise .....	16
Advanced Services for Service Providers .....	17
Professional Services .....	17
<i>Professional Services for Security Products</i> .....	18
Service Design & Transition Phase .....	18
Service Operation Phase .....	18
Security Analysis Services .....	19
4.3 <i>FortiOS Advantage</i> .....	19
4.4 <i>The Security Processor Advantage</i> .....	19
<b>5. Fortinet Security Solution Overview .....</b>	<b>20</b>
5.1 <i>Security for Enterprises and Mid-Sized Organizations</i> .....	20
5.1.1 <i>The Fortinet Enterprise Firewall Solution</i> .....	20
<i>Fortinet Next-Generation Firewall (NGFW) Solution</i> .....	20
<i>Fortinet Internal Segmentation Firewall (ISFW) Solution</i> .....	21
<i>Fortinet Data Center Firewall and IPS Solution</i> .....	22
<i>Fortinet SD-WAN Solution</i> .....	22
5.1.2 <i>Fortinet ATP (Includes Sandboxing)</i> .....	22
Prevent: Act on known threats and information.....	23
Detect: Identify previously unknown threats .....	23
Mitigate: Respond to potential incidents.....	23

5.1.3 Fortinet Data Center Security Solution.....	24
5.1.4 Fortinet Security Operations Solution.....	24
5.1.5 Fortinet Application Security Solution.....	25
Web application protection .....	26
Encryption/decryption with ADC .....	26
DDoS attack mitigation .....	26
5.1.6 Secure Access Solution.....	27
Integrated Wi-Fi .....	28
Controller Wi-Fi.....	28
Cloud Wi-Fi.....	28
FortiSwitch.....	28
<b>6. FortiSwitch Secure Switching .....</b>	<b>29</b>
Highlights .....	29
6.1 Secure Access Switches – Simple, Secure, Scalable Unified Access Layer Ethernet Switches.....	30
Security Fabric Integration .....	30
Key Features & Benefits.....	31
6.1.1 FortiSwitch Rugged.....	31
6.2 Data Center Switches – High Performance Switching with Data Center Capabilities.....	32
Security Fabric Integration .....	33
High-performance and resilient managed data center switch .....	33
Highlights .....	33
Key Features and Benefits .....	34
6.3 Deployment Options.....	34
6.3.1 FortiLink Mode.....	34
FortiLink Advantages .....	34
Capabilities: FortiLink Mode .....	35
6.3.2 Standalone Mode.....	35
6.5 Solution Integration.....	36
Retail .....	36
Connected UTM.....	36
Secure Access Architecture.....	37
FortiGate in HA.....	38
<b>7. FortiSwitch Common Requirement Specifications and Answers .....</b>	<b>38</b>
7.1. General system requirements.....	38
7.2. Layer 2 Requirements.....	40
7.3. Management requirements .....	42
7.4. Authentication Requirements.....	42
7.5. POE Requirements.....	43
7.6. Layer 3 Requirements.....	44
7.7. Security.....	44
7.8. QoS.....	47
7.9. IPv6 Support.....	47
7.9. VxLAN Support.....	48
7.10 FortiSwitch Rugged Environmental and Compliance.....	49

## 1. COMPANY INTRODUCTION

**Indicium Technology dba Innovative Solutions Technology** is an IT Solutions provider who leverages years of past performance supporting government agencies and businesses. We provide solutions to designed to secure the network and data on-premise or in the cloud. We provide certified personnel to design, implement and maintain the solutions we offer. In order to support WV Department of Highways we believe Fortinet was the best partner to put forth. The SD-WAN solution not only future proofs your network architecture, but with Fortinet you can implement a security driven networking strategy the provides cost savings as well as consolidated management and comprehensive visibility across your network. As you will see, the tightly integrated family of products is by design and intended to facilitate management of your network operation. By proposing Fortinet SD-WAN and Switches we have provided an opportunity to reduce the number of vendors and streamline your security solution stack. This is advantageous for the network operations team as well as from a support standpoint.

### Fortinet



**FORTINET**

---

Founded: Nov. 2000

---

First Product Release: May 2002

---

Fortinet IPO: Nov. 2009  
NASDAQ: FTNT

---

Headquarters: Sunnyvale, California

---

Employees: 4,900+

---

FY 2016 Revenue: \$1.275B

---

Q3 2017 Revenue: \$374M  
Q3 2017 Billings: \$432M  
Q3 2017 EPS (GAAP): \$0.15  
Q3 2017 EPS (non-GAAP): \$0.28  
Market Cap (Oct. 26, 2017): \$7B  
\$1.5B Cash and No Debt

---

Units Shipped to Date: 3.4M+

---

Customers: 330,000+

---

Global Patents Issued: 439  
Global Patents Pending: 291

From the start, the Fortinet vision has been to deliver broad, truly integrated, high-performance security across the IT infrastructure.

We provide top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Our unique security fabric combines security processors, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control—while providing easier administration.

Our flagship enterprise firewall platform, FortiGate, is available in a wide range of sizes and form factors to fit any environment and provide a broad array of next-generation security and networking functions. Complementary products can be deployed with a FortiGate to enable a simplified, end-to-end security infrastructure covering:

- Network security
- Data center security (physical and virtual)
- Cloud security (private, public, hybrid)
- Secure (wired and wireless) access
- Infrastructure (switching and routing) security
- Content security
- Endpoint security
- Application security

---

Fortinet is a true innovator and holds more than double the number of patents than any other dedicated network security vendor. Our market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and media outlets worldwide. We are proud to count the majority of Fortune 500 companies among our satisfied customers.

Fortinet is headquartered in Sunnyvale, California, with 100+ offices around the world. Founded in 2000 by Ken Xie, the visionary founder and former president and CEO of NetScreen, Fortinet is led by a strong and seasoned management team with deep experience in networking and security.

## 2. FORTINET—YOUR SECURITY BUSINESS PARTNER

### 2.1 Why Fortinet?

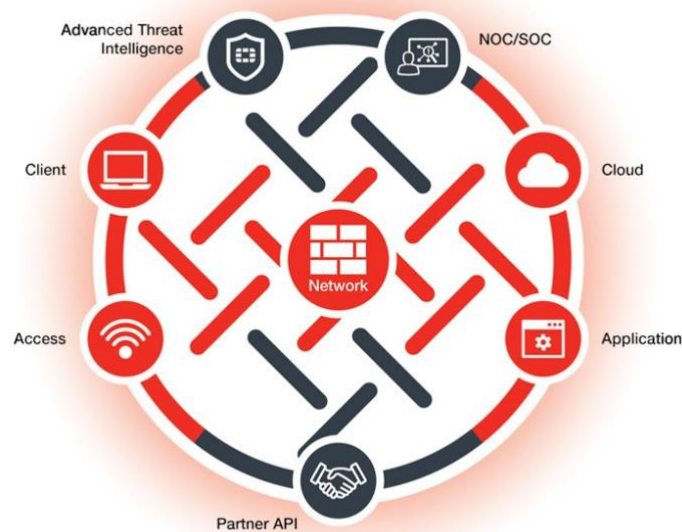
#### Fortinet Security Fabric

Organizations today require a fast and secure network to be successful. Whether or not you have the right protection immediately responding to threats throughout your network can determine if your business runs smoothly or is the victim of a security breach.

Fortinet is the only company with security solutions for network, endpoint, application, data center, cloud, and access designed to work together as an integrated and collaborative security fabric. This also means we are the only company that can truly provide you with a powerful, integrated end-to-end security solution across the entire attack surface.

To enable an effective defense, the data and security elements across all of your various environments must be well-integrated, able to share intelligence, and visible. The Fortinet Security Fabric gives you control, integration, and easy management of security across your entire organization, from IoT to the cloud.

The [Fortinet Security Fabric](#) is an intelligent framework designed for scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards.



The Security Fabric is built on three key attributes:

- **Broad:** The Security Fabric covers the entire attack surface. Security can be applied to the network, endpoints, access, applications, and cloud.
- **Powerful:** The Security Fabric uses security processors to reduce the burden on infrastructure, delivering comprehensive security without affecting performance.

- **Automated:** The Security Fabric enables a fast and coordinated response to threats. All elements can rapidly exchange threat intelligence and coordinate actions.

## Unparalleled Third-Party Certifications

Real-world testing is the best way to evaluate the effectiveness and speed of technology. The number of unverified claims from vendors about what their products can do is overwhelming. That's why we routinely submit our products and technologies for independent tests so that you can verify for yourself that our claims of top performance and effectiveness are valid.

We routinely receive top scores from organizations such as NSS Labs, ICSA Labs, and Virus Bulletin, and they also provide information on how we stack up against the competition.



## More than 330,000 Customers and Growing

Our customers come in all sizes, represent a wide range of industries and organizations, and are located throughout the world. We are proud to count the majority of Fortune 500 companies among our satisfied customers.

## 2.2 Core Platform High-Level Overview

The backbone of the Fortinet Security Fabric is our flagship network security platform, FortiGate. It consists of physical and virtual appliances that provide a broad array of security and networking functions, including firewall, VPN, anti-malware, intrusion prevention, application control, web filtering, anti-spam, DLP, WAN acceleration, and WLAN control. FortiGate appliances, from the FortiGate 30D for small businesses all the way up to the FortiGate 7000 series for large enterprises, data centers, and service providers, deliver top-rated security and performance with efficient management through:

- FortiGuard – Our large global threat research team discovers new threats and delivers protective services 24x365 across a rich array of consolidated security technologies, including application control, intrusion prevention, web filtering, vulnerability management, anti-malware, anti-spam, and more. By developing and delivering all of our threat research and protection services in-house, we provide you with the fastest and most integrated response to threats. FortiGuard protection is independently validated as highly effective versus today's advanced threats.
- Fortinet Security Processing Units – Our custom-designed SPUs accelerate processing of security and networking functions to radically boost performance and scalability and provide you with the fastest network security appliance performance available. This allows you to stay ahead of rapidly growing bandwidth requirements and prevents your security solution from becoming a choke point in your network.
- FortiOS – Our proprietary operating system provides the foundation for and integration of all security and networking functions. This allows IT managers to deliver consistent and coordinated policies across all security devices, creating a faster and more robust

response to threats with a far lower administrative burden. Flexible licensing of FortiOS features gives you the flexibility to deploy what you need, where you need it--leading to a simpler, easier to maintain infrastructure as well.

- Single-pane-of-glass management - Our easy-to-use management platform—available in hardware appliance, virtual machine, and cloud form factors—provides centralized configuration, security policy management, aggregate logging, reporting, and forensic analysis for up to 10,000 Fortinet devices.

By integrating and accelerating multiple proprietary security and networking functions with purpose-built SPUs and FortiOS, delivering dynamic proprietary security service updates via FortiGuard, all managed through a simple comprehensive management console, Fortinet's network security platform delivers broad protection against dynamic security threats while reducing the operational burden, response time, and costs associated with managing multiple point products.

Fortinet offers a broad set of complementary solutions that integrate to form the Fortinet Security Fabric, allowing customers to further secure and simplify their networks, including:

- Sandboxes
- Web application firewalls
- Secure email gateways
- DDoS protection
- Application delivery controllers
- User identity management/authentication and tokens
- Endpoint security for desktops, laptops, and mobile devices
- Secure wireless LAN and WAN
- And more...

### **3. FORTINET LEADERSHIP**

#### **3.1 Industry Leadership**

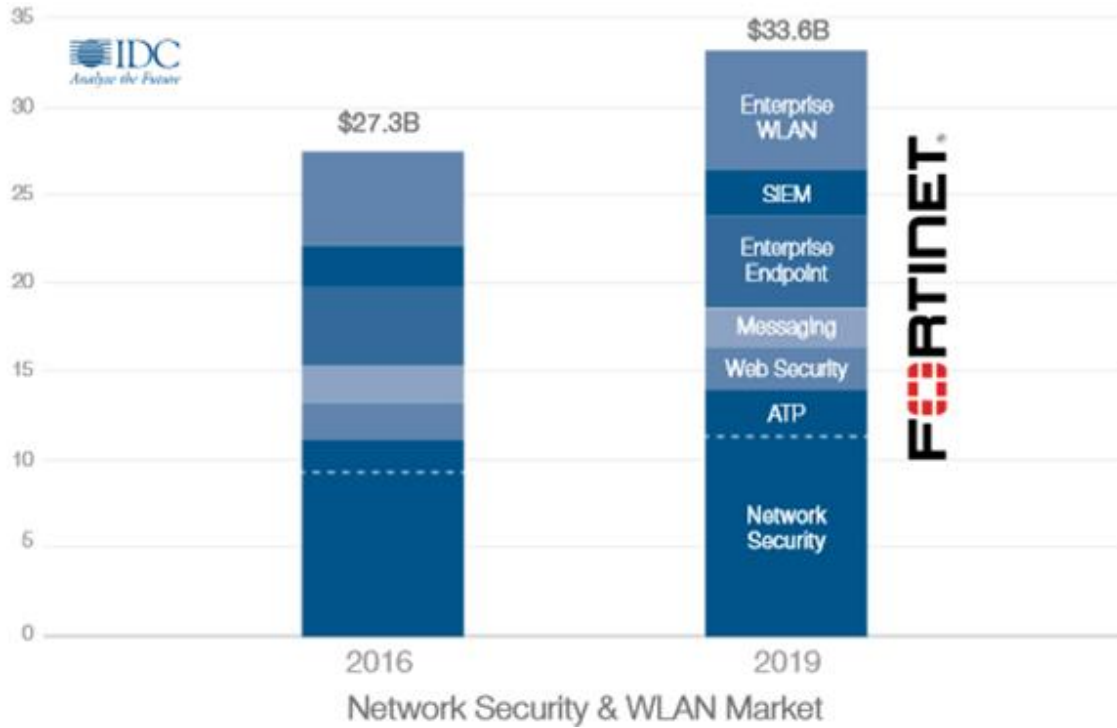
Fortinet's market leadership is recognized by the main industry research and analyst firms including IDC and Gartner:

##### **IDC**

Fortinet is the world's largest network security appliance vendor (unit share) and top 4 network security vendor (revenue share) according to IDC.



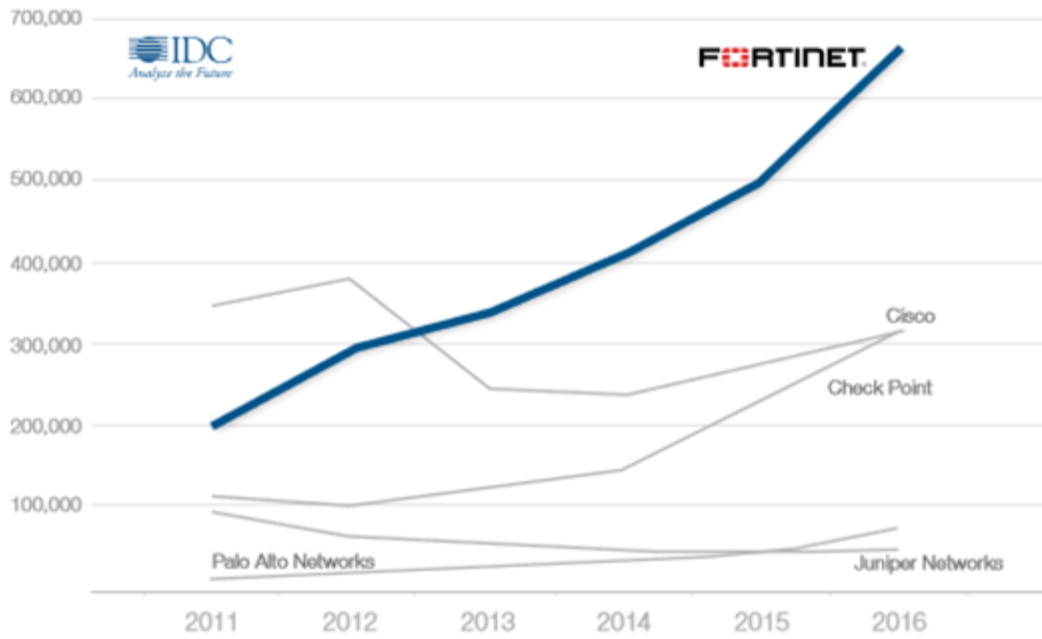
Fortinet is a major player in many segments of the fast-growing Network Security and WLAN markets.



Sources:

- IDC Worldwide Endpoint Security Forecast, 2016-2020
- IDC Worldwide Security and Vulnerability Management Forecast, 2016-2020
- IDC Worldwide Enterprise WLAN Forecast, 2016-2020
- IDC Specialized Threat Analysis and Protection Forecast, 2016-2020
- IDC Worldwide Web Security Forecast, 2016-2020
- IDC Worldwide IT Security Products Forecast, 2015-2019

Fortinet is the largest network security appliance vendor (units) and growing quickly, according to IDC...



**Gartner**

Fortinet is recognized by Gartner in six Magic Quadrants: Enterprise Firewall, UTM, Email Security, SIEM, WAF, and WLAN/LAN.

We are the leader and acknowledged pace-setter in the Gartner UTM Magic Quadrant, and Leader in the Enterprise Firewall Magic Quadrant

*Gartner Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)*



\*Source: <https://www.gartner.com/doc/reprints?id=1-43QT4Y6&ct=170621&st=sb>

**3.2 Unparalleled Third-Party Certification and Validation**

Fortinet believes that independent, third-party tests provide a critical and impartial measure of the quality of a product, and a mandatory reference for anyone making an IT security purchase decision. Fortinet participates in unbiased, credible testing so customers can see how we compare to alternative solutions and select the solution that is right for their needs.

Since its inception, Fortinet has received more certifications to validate our solutions than any other network security vendor. These test results are proof that in real world traffic and deployment scenarios, our products earn top ratings and perform as advertised or better. The quality of our security functionality is certified by ICSA Labs, NSS Labs, AV Comparatives, Virus Bulletin, and others. We also meet numerous government standards, such as FIPS 140-2, Common Criteria EAL4+, as well as other important certifications for IPv6 and ISO 9001.

Fortinet is NSS Labs “Recommended” in the following tests:

- NGFW
- DCIPS
- NGIPS
- Web Application Firewall
- Endpoint Protection
- Breach Detection (Sandbox)

Fortinet has participated in the following real-world group tests, open to the industry, and conducted by NSS Labs. In doing so, Fortinet stands out as the only vendor to provide an ATP Solution that is NSS Labs “Recommended” from the data center to the edge to the endpoint in the latest group tests.

*The seven-year summary of Fortinet ratings in NSS Labs group tests shows a growing list of “Recommended” ratings.*

Product	2011	2012	2013	2014	2015	2016	2017
Firewall	Neutral		Recommended				
NGFW		Neutral	Recommended	Recommended		Recommended	Recommended
Data Center IPS				Neutral		Recommended	
NGIPS					Recommended	Retested & Passed	
Breach Detection				Recommended	Recommended	Recommended	
Web Application Firewall				Recommended			Recommended
Adv. Endpoint Protection					Recommended		Recommended
DDoS						Neutral	

*As of June 2017*

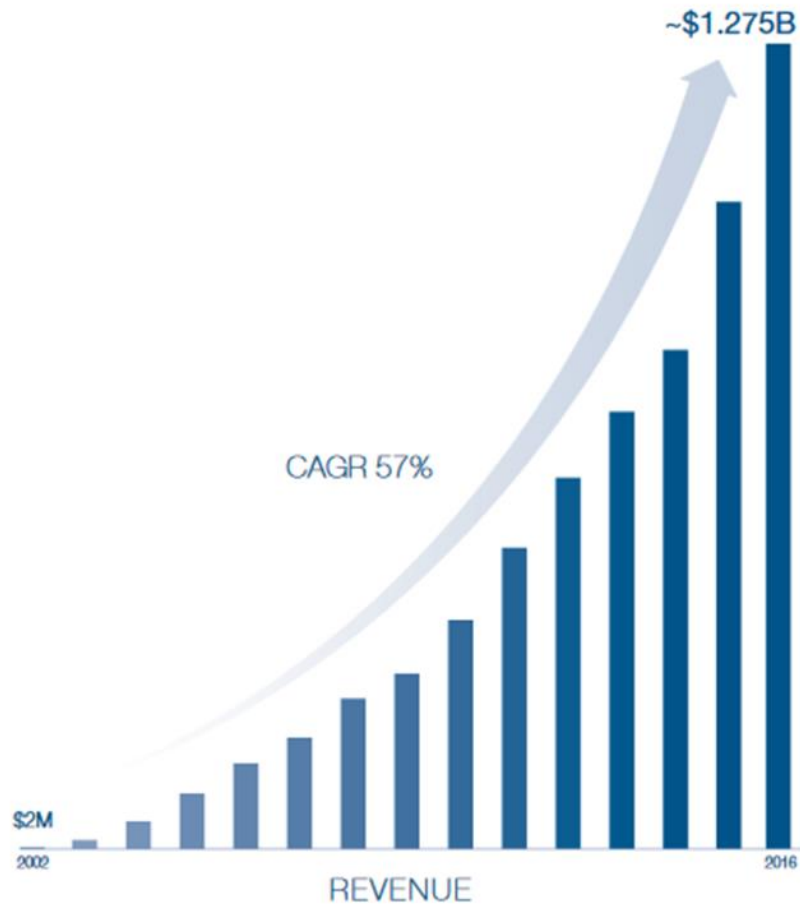
*Fortinet is the only vendor to receive NSS Labs “Recommended” from the edge to the endpoint.*

	RECOMMENDED	NEUTRAL	CAUTION	RETESTED & PASSED		
Certification	Fortinet	Check Point	Cisco	Palo Alto	Juniper SRX	FireEye
NSS Labs Next-Gen Firewall	■	■	■	■	■	×
NSS Labs Data Center Firewall	■	×	×	×	×	×
NSS Labs Breach Detection System	■ ■	■	□	■ ■	×	□
NSS Labs WAF	■	×	×	×	×	×
NSS Labs NG IPS	■	×	■	□	×	×
NSS Labs DC IPS	■	×	×	■	■	×
NSS Labs Advanced Endpoint	■	×	×	×	×	×
BreakingPoint Resiliency Score	■	×	×	□	×	×
ICSA Firewall	■	■	×	■	■	×
ICSA IPS	■	×	×	×	×	×
ICSA Antivirus	■	×	×	×	×	×
ICSA WAF	■	×	×	×	×	×
ICSA ATD (Sandbox)	■	■	×	■	×	■
ICSA ATD (Email)	■	×	×	×	×	×
VB100 Virus	■	■	×	×	×	×
VBSpam	■	×	×	×	×	×
AV-Comparatives	■	×	×	×	×	×
Common Criteria	■	■	■	■	■	■
FIPS	■	■	■	■	■	■
UNH USGv6/IPv6	■	■	■	■	■	×

### 3.3 Financial Highlights

Fortinet enjoys a strong financial stability, making the company a long-term player in the IT security industry.

Fortinet generated over \$1.275B in revenue and 26% year-over-year revenue growth in 2016, a growth rate far superior to the overall market.



Year	2012	2013	2014	2015	2016
<b>Revenues</b>	\$534m	\$615m	\$770m	\$1B	\$1.275B
<b>YoY Growth</b>	+23%	+15%	+25%	+31%	+26%
<b>Cash &amp; Investments</b>	\$740m	\$843m	\$991.7m	\$1.16B	\$1.31B

The company is solidly profitable and has been cash-flow positive for more than eight years.

---

## 4. FORTINET ADVANTAGE

### 4.1 In-House Security Research and Services

Extensive knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation for providing effective security. Hundreds of researchers at [FortiGuard Labs](#) scour the cyber landscape every day to discover emerging threats and develop effective countermeasures to protect more than 330,000 Fortinet customers around the world. Fortinet solutions, including the flagship FortiGate firewall platform, are powered by security services developed by FortiGuard Labs.

#### FortiGuard Services

FortiGuard security services are available as subscriptions for use in the FortiGate next-generation firewall and IPS platforms as well as with a number of other Fortinet products such as the FortiMail secure email gateway, FortiClient endpoint protection, FortiSandbox, FortiCache, and FortiWeb. You can choose individual services, or get access to all available services with the Enterprise Bundle.

#### Industry-validated Security Effectiveness

Fortinet solutions with FortiGuard services are consistently confirmed by NSS Labs, Virus Bulletin, AV Comparatives, and ICSA tests to deliver superior security effectiveness.

- 2016 VB Web test found that FortiGuard Web Filtering blocked 97.7% of direct malware downloads. It's the only web filtering service in the industry to receive VB Web certification.
- 2015 VB100 Reactive and Proactive Test ranked Fortinet one of the industry's most effective AV solutions at stopping both known and zero-day threats.
- 2016 VBSPAM test ranked Fortinet Antispam security effectiveness at 99.97 with a 99.998% spam catch rate (the second highest catch rate in the industry).
- 2015 AV Comparatives awarded its highest-level award, the Advanced+ rating to Fortinet for anti-phishing, file detection, and real-world protection.
- NSS Labs consistently awards Fortinet "Recommended" status for NGFW, NGIPS, and Breach Detection (Sandboxing).

#### FortiGate Solution Services

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with the FortiGuard Enterprise Bundle. This bundle contains the full set of FortiGuard security services plus FortiCare service and support offering the most flexibility and broadest range of protection in one package.

### 4.2 FortiCare Services

At Fortinet, we put a lot of care into making sure our customers are satisfied with our products and support. Our FortiCare support offerings are specifically designed to provide you with the support you need for all Fortinet products and services no matter where in the world you are.

---

## Support and Advanced Services

With FortiCare Services, you can rest assured that your Fortinet security infrastructure is performing at its absolute best and protecting your critical assets and data. FortiCare Services includes both Support Services and Advanced Services.

### FortiCare Support Services

FortiCare Support Services give you global support on a per-product basis. By subscribing to these services, you'll receive a timely response to any technical issue as well as complete visibility on ticket resolution progress.

All FortiCare Support Services include firmware upgrades, access to the support portal and associated technical resources, reporting on technical incidents (via the web, chat, and telephone), as well as a hardware return option.

- **FortiCare 8x5 Service**  
Get access to technical support via the web portal, online chat system, and telephone, including return and replace for hardware failures. You'll also have fast and easy written access to technical support requests.
- **FortiCare 24x7 Service**  
If you need 'round-the-clock access to mission-critical support services, the 24x7 Service will meet your requirements. You'll get access to technical support 24x365 as well as advanced replacement service for hardware failures.
- **FortiCare 360° Service**  
FortiCare 360° Service includes all the services of FortiCare 24x7 Service and provides recurring health checks with a personalized monthly audit report of FortiGate and FortiWiFi appliances. Fortinet engineers will perform device environmental and performance audits and make recommendations. You'll be aware of any potential issues and can take action to avoid service disruptions or performance slowdowns.

**FortiCare Premium RMA Service** is designed to minimize downtime. There are three options:

- Next-day delivery: Parts are delivered the day following RMA approval by Fortinet support.
- 4-hour courier: Parts are delivered on-site 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support.
- 4-hour on-site engineer: Parts are delivered on-site with an engineer, 24 hours a day, 7 days a week within 4 hours of RMA approval by Fortinet support.

**FortiCare Secure RMA Service** allows for non-return of an appliance for those customers with strict rules and requirements for physical data protection.

### Advanced Services for Enterprise

FortiCare Advanced Services for Enterprise provides integrated support to sustain and optimize Fortinet appliances. The service is delivered by the Advanced Services team, experts in Fortinet and security technology that is deployed in a typical enterprise environment. This scalable service has different service levels ranging from focused



technical support to a comprehensive set of services to help with IT business continuity objectives. FortiCare Advanced Services for Enterprise includes the following options:

- **Premium** service provides technical support excellence through fast track access to the Advanced Services team. It also includes training and certification, a customized account plan, and proactive after-hours support.
- **Business** service includes a designated engineer who will become familiar with your environment and assist in regular ticket reviews. This level also includes bi-annual and root-cause analysis reporting, as well as Advanced Service Points which may be used to select the most appropriate service for your operational requirements.
- **First** service provides a technical account manager (TAM), who collaborates with you to build and maintain a long-term technical engagement, providing technical support, operational reviews, and quarterly reporting. The service also includes best practice guidance, upgrade assistance, extended software support to facilitate upgrade planning, and advanced notifications.
- **Global First** service provides larger geographical coverage by including a designated lead engineer per major region.
- The **Advanced Services Coordinator** acts as the single point of contact for Fortinet services, facilitating your overall service delivery and ensuring timely responses through a focused communication channel.

### Advanced Services for Service Providers

FortiCare Advanced Services for Service Providers delivers integrated support to sustain and optimize Fortinet appliances for communications and managed security providers. Incident resolution is enhanced by engagement with the Advanced Services team, experts in security technologies deployed in typical service provider environments. This scalable service has two levels that provide a comprehensive set of services to help customers achieve their IT business continuity objectives:

- **Select** service delivers support excellence through fast-track access to technical experts. It also includes training and certification, a customized account plan, and a designated service delivery manager (SDM) who will build business-level relationships, driving the established objectives, as well as measuring and reporting on service quality.
- **Elite** service includes a designated lead engineer, who collaborates with you to build and maintain a long-term technical engagement using customer knowledge to enhance service delivery. The lead engineer will provide best practice guidance, upgrade assistance to facilitate upgrade planning, and advanced notifications of critical incidents. The SDM will assure service delivery and act as the voice of the customer within Fortinet support and service teams.

### Professional Services

Fortinet's comprehensive product portfolio enables secure mission-critical environments. Our Professional Services organization has services to provide technical consulting on Fortinet solutions. The team has expertise with Fortinet and other vendor platforms, as well as industry network and security standards knowledge.

---

## Professional Services for Security Products

### Service Design & Transition Phase

- **Network Design & Integration:** Optimizes the integration of the Fortinet solution and advises on proposed design solutions.
- **Design & Configuration Review:** Provides a review of design documentation and accompanying configuration files.
- **Design & Configuration Validation:** Concentrates on the verification of the business-centric aspects of the customer environment and includes implementation of customer-specific test plans.
- **Firewall Migration & Replacement Campaign:** Provides “production-to-production” project support for customers migrating from a third-party vendor.
- **Software Upgrade & Platform Migration Campaign:** Assures a software upgrade or hardware migration.
- **Product Workshops:** Provide tailored training on a design solution created by Fortinet Professional Services.
- **Technical Design Authority & Implementation:** Provides a design lead throughout the project to ensure any issues that may arise are taken care of.

### Service Operation Phase

Service Operation includes the following service offerings:

- **FortiGate Health Check:** Measures operational performance of the firewall in the customer’s production environment and provides a firewall review to identify issues and provide configuration-tuning recommendations.
- **Security Hardening:** Provides up-to-date platform and version-specific hardening advice.
- **Compliance Audit Preparation:** Gives guidance on audit and compliance processes, including advice on the correct and optimal configuration of the deployed Fortinet solution.
- **Configuration Verification:** Recalibrates, restructures, or redesigns the customer’s solution so that it is optimally deployed to meet current demands.
- **Lab Testing & Validation:** Gives assistance in performing functional testing as well as making planned network change (e.g., configuration change, upgrades, etc.) outcomes predictable and measurable.
- **Dedicated Resource Service:** Provides operational technical assistance by a Fortinet certified engineer. This service is available either remotely or on-site.

## Security Analysis Services

With the increased frequency, volume, and impact of security attacks, such as Distributed Denial of Service (DDoS), more and more enterprises are deploying Fortinet products as essential elements of a complete security strategy.

The FortiCare Security Analysis Service, available for the **FortiDDoS** and **FortiWeb** product families, maximizes your investment by optimizing the configuration of your appliances for your specific security environment. Fortinet security experts analyze your infrastructure and security requirements to give your team a more in-depth understanding of the technology, resulting in the optimal configuration for your environment.

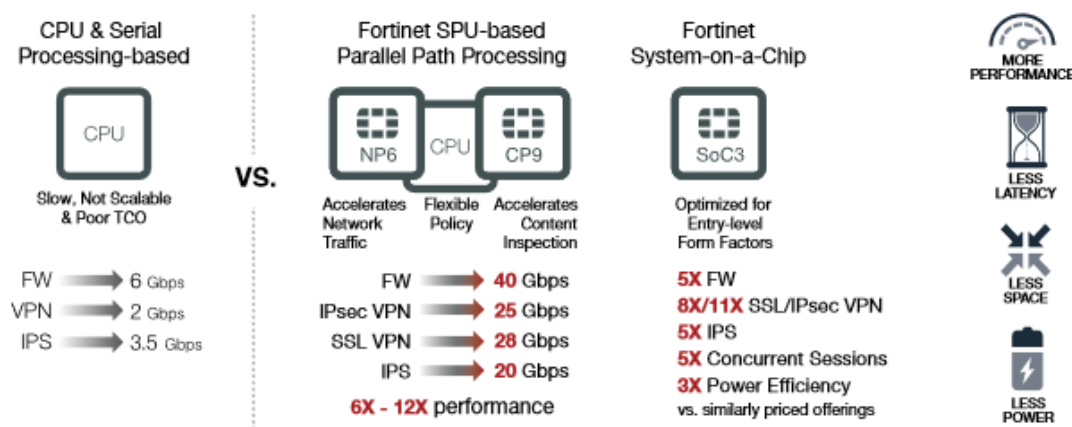
### 4.3 FortiOS Advantage

The Fortinet Security Fabric is an intelligent framework connecting your security devices together for effective, efficient, and comprehensive security. FortiOS enables the Security Fabric, letting you control the security and networking capabilities in all your Fortinet Security Fabric elements with one intuitive operating system.

Networking	Security	Integration	Management
Firewall	Intrusion Prevention	Email	NOC/SOC/Policy
VPN	Application Control	WAF	Reporting & Compliance
Routing	Anti-malware	Endpoint	Topology Views
Switching	Anti-botnet	Sandboxing	Management
SD-WAN	Web Filtering	Vulnerability	Analytics
Wi-Fi Controller	Mobile Security	Partner APIs	VDOM/ADOM
More...	More...		More...

### 4.4 The Security Processor Advantage

Fortinet Security Processors radically increase the security performance, scalability, and throughput of Fortinet solutions while greatly shrinking space and power requirements compared to CPU-based solutions.



---

## 5. FORTINET SECURITY SOLUTION OVERVIEW

### 5.1 Security for Enterprises and Mid-Sized Organizations

Enterprise networks are evolving rapidly and adopting new technologies to meet business demands, but this also opens the door to cyber attacks. An integrated, collaborative security approach is required to close the security gaps and share intelligence for automatic, fast response to threats.

All Fortinet solutions work together in the Fortinet Security Fabric for easy management, full visibility, shared intelligence, and automatic remediation.

#### 5.1.1 The Fortinet Enterprise Firewall Solution

Under constant attack, organizations cannot afford to choose between security and maintaining a high-performance business infrastructure. Your extended enterprise needs proven security that won't compromise performance: from deep within internal segments, to physical and virtual data centers, to dynamic cloud environments.

Deploying network security solutions from multiple vendors causes unnecessary complexity and introduces security gaps. Our Enterprise Firewall Solution delivers industry-leading security effectiveness with unmatched performance capabilities—through one operating system managed within a single pane of glass.

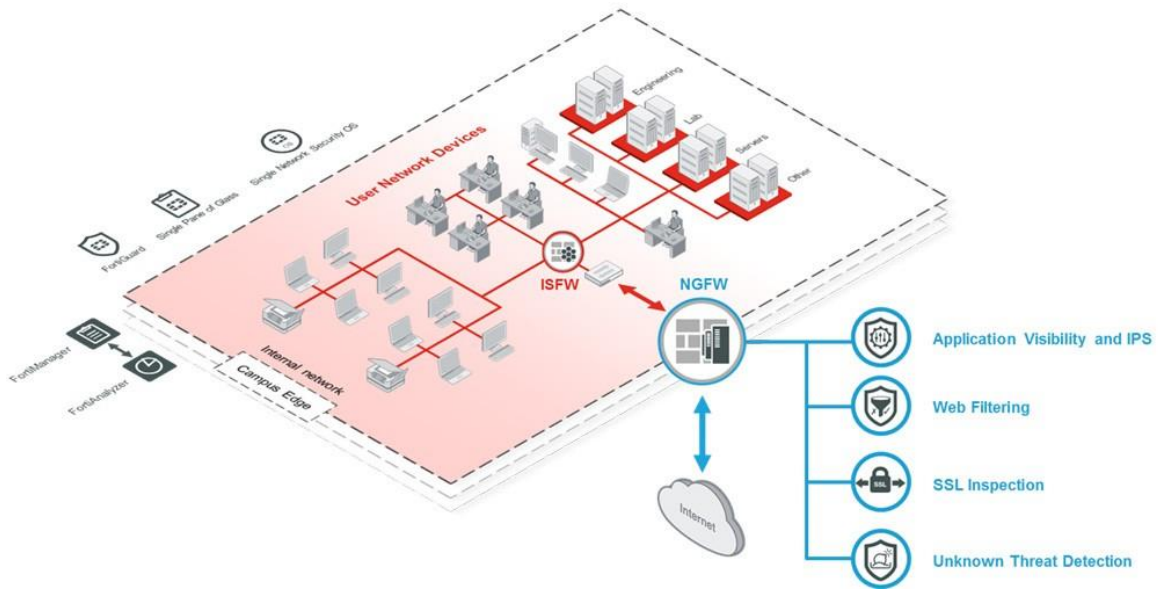
This consolidated architecture gives you an immediate responsive and intelligent defense against malware and emerging threats with an integrated security fabric that extends across your borderless network.

#### Fortinet Next-Generation Firewall (NGFW) Solution

Effective protection is an absolute necessity in today's rapidly growing threat environment, as is having a fast, reliable network. You can't afford to choose between comprehensive security and network performance, and with Fortinet solutions, you don't have to.

The FortiGate next-generation firewall is a high-performance network security appliance that adds intrusion prevention, application and user visibility, SSL inspection, and unknown threat detection to the traditional firewall. Our NGFW appliance protects the edge of the campus and internal segments using the high performance of the [FortiGate family](#) with the security intelligence of [FortiGuard Labs](#) to:

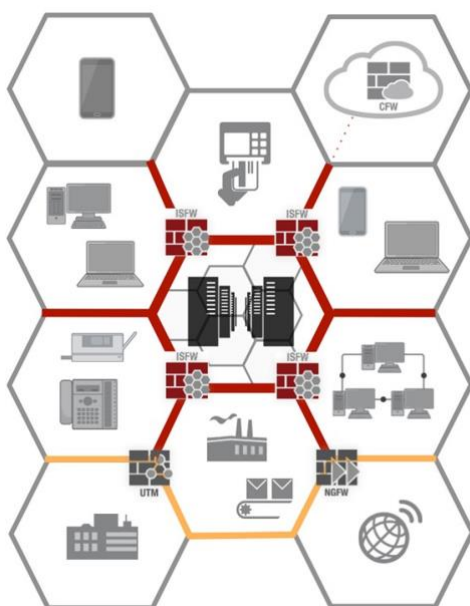
- Enforce security policies with granular control and visibility of users and devices for thousands of discrete applications
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual content of your network traffic
- Perform high-performance SSL inspection using industry-mandated ciphers
- Proactively detect malicious unknown code using our cloud-based sandbox service
- Provide you with real-time views into network activity with actionable application and risk dashboards and reports
- Deliver superior, multi-function performance by running on purpose-built appliances with custom security processors



### Fortinet Internal Segmentation Firewall (ISFW) Solution

With advanced threats growing rapidly in number and sophistication, perimeter security is no longer enough to keep your sensitive information safe. Once a threat gains entry, it can spread and eventually extract the valuable assets it was sent to retrieve.

You can dramatically improve your security by adding FortiGate Internal Network Segmentation Firewalls to your network to prevent the proliferation of threats once they get inside. ISFWs provide network segmentation inside the perimeter. They may sit in front of specific servers that contain valuable intellectual property or a set of user devices or web applications sitting in the cloud.



---

## Fortinet Data Center Firewall and IPS Solution

The enterprise data center is evolving rapidly, incorporating technologies such as virtualization, software-defined networking, and public cloud computing, along with advanced cyber security. Trying to apply traditional security solutions to these sorts of new technologies generally will not be effective. Enterprises need to evaluate their data center initiatives and how they will impact network security to ensure all areas of the data center remain protected.

In today's dynamic and complex data centers, security must be flexible, effective, and easy to manage. It needs to bring order to the chaos—not add to it. Fortinet can protect your physical, virtual, and cloud servers with one solution—whether it's for data center, private cloud, or public cloud deployments.

## Fortinet SD-WAN Solution

Today's distributed enterprises typically spend a lot of time and resources on overly complicated security deployments that may not even be effective. As bandwidth requirements continue to increase at an alarming rate, many organizations are moving from MPLS to the Internet to increase bandwidth and reduce costs. In addition, groups within enterprises are directly accessing cloud applications. Both of these trends raise serious security concerns.

It doesn't have to be complicated to deploy and manage the right security in all the right places. The [FortiGate Enterprise Firewall](#) and [Hybrid Virtual Appliance](#) enable software-defined WAN (SD-WAN). It links network and security paths across the world through the Internet, 3G/4G, or private WAN links, making it a truly borderless infrastructure for the enterprise. It provides application visibility for encrypted traffic and smart load balancing which help to reduce WAN costs without impacting the SLA for business applications. With our new dynamic cloud application list, customers can easily migrate to SaaS applications and get the most optimized and secured path.

Multiple security features are commonly applied including: IPsec VPN, IPS, web filtering, and the industry's highest SSL inspection performance based on our purpose-built security processors. All of these features are managed via our orchestrator and centralized manager which enable zero-touch deployment and simplified administration.

### 5.1.2 Fortinet ATP (Includes Sandboxing)

Today's threats are more sophisticated and successful than ever. According to our [Fortinet Threat Landscape Report](#), on average, organizations were compromised by more than six active bots communicating back to their command and control infrastructures. Based on botnet activity, it was found 36% of organizations exhibited ransomware activity, so it should come as no surprise that an estimated \$850M was paid in ransoms in 2016.

Of course, that implies that the other 64% of organizations that exhibited botnet activity were impacted by other malware—highlighting the importance of stronger measures to deal with the volume and sophistication of today's threat landscape.

With a dynamic attack surface due to the rise of IoT and cloud services, it's clear that no single technology will be able to stop every threat. To protect your enterprise against sophisticated threats, it is important to establish a comprehensive and cohesive security

infrastructure that is broad enough to cover all attack vectors, powerful enough to run the latest security technologies, and automated to keep pace with fast-moving attacks.

This is exactly what [Fortinet Advanced Threat Protection](#) delivers with its integrated, top-rated components spanning prevention, detection, and mitigation:



### **Prevent: Act on known threats and information**

The most efficient way to protect your organization is to immediately block a variety of known threats without impacting network performance at the network, application layer, or endpoint. This is typically accomplished with next-generation firewalls, secure email gateways, web application firewalls, and endpoint security clients to stop malware, intrusions, botnets, etc.

### **Detect: Identify previously unknown threats**

Zero-day attacks and sophisticated threats are often engineered to evade traditional security solutions. Advanced threat detection technologies must be added to automatically detect previously unknown threats and create actionable threat intelligence. Sandboxing in particular, tests unknown items in a secure, instrumented environment to see how they behave, in order to turn the unknown into the known. Extending prevention across all layers with this deeper inspection is critical to getting ahead of the more sophisticated threats.

### **Mitigate: Respond to potential incidents**

Once a new threat is identified, it needs to be immediately mitigated. This can be handled automatically using direct intelligence sharing between detection and prevention products, or with assisted mitigation: a combination of people and technology working together.

Further, protections from previously unknown threats can be put into place across all the layers to complete the cycle and improve the organization's security posture in advance of future attacks.

Not only are all Fortinet Advanced Threat Protection components powered by the leading security intelligence of [FortiGuard Labs](#), they also leverage local intelligence dynamically generated by FortiSandbox and shared across the interconnected security infrastructure. This sharing automatically responds to the latest targeted attacks, continually improves an organization's security posture, closes natural gaps between multi-vendor point products, and reduces the time spent managing IT security.

### **5.1.3 Fortinet Data Center Security Solution**

The enterprise data center is evolving rapidly with technologies such as virtualization, software-defined networking, and public cloud computing. Trying to apply traditional security to new technologies generally will not be effective. Enterprises need to evaluate their data center initiatives and how they will impact network security to ensure all areas of the data center remain protected.

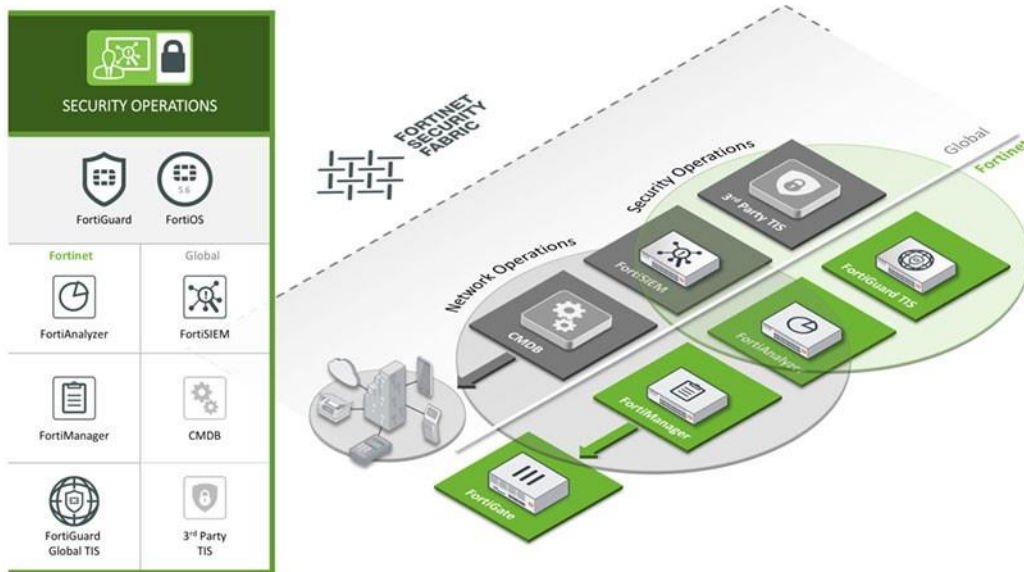
Today's data centers are dynamic and complex. Security solutions need to be flexible, effective, and easy to manage so they bring order to the chaos instead of adding to it. Fortinet can protect your physical, virtual, and cloud servers with one solution—whether data center, private cloud, or public cloud deployments.

### **5.1.4 Fortinet Security Operations Solution**

The increase in frequency and sophistication of cyber attacks has taken a toll on security, compliance, performance, and availability. The number of organizations that have suffered a breach is growing rapidly and will continue to increase if organizations are not able to discover threats and respond to them more quickly.

Enterprise networks are seeing an evolution of their network environments, going from centralized control to distributed networks with the advent of mobility, and now becoming borderless with the rapid adoption of virtual and cloud solutions. To monitor risks, enterprises have both a network operations center (NOC) and a security operations center (SOC), but they don't correlate or integrate the information they collect. But if a SOC and a NOC could share information, they'd be able to discover threats and initiate remediation much faster.





Our Security Operations solution covers both IT and security risk management across the entire enterprise, including pre-existing and future infrastructure. While Fortinet security products are already unified into a Security Fabric with a single OS and shared intelligence, the Security Operations solution includes information from network elements beyond the Fortinet devices. It breaks down the barrier between NOC and SOC, giving you a comprehensive view of your entire network so you can quickly find and respond to threats. It also helps manage and monitor compliance, increase application availability, and save IT resources.

Fortinet’s Security Operations Solution delivers:

- Adaptive awareness of the threat landscape
- Rapid local and global threat detection for rapid response
- Reduced complexity in managing the onslaught of alerts and alarms
- A comprehensive and more holistic approach to managing risk
- Reporting and analytics that enable IT, line of business managers, C-level, and board members to better understand how the organization’s risk profiles are being managed.

### 5.1.5 Fortinet Application Security Solution

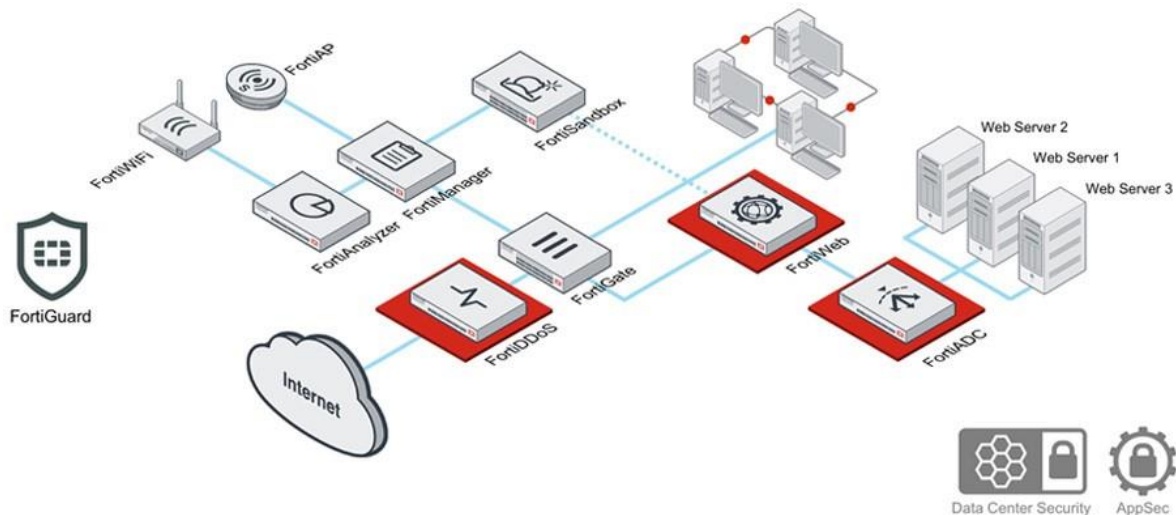
Web applications and email systems have long been favorite targets of hackers because they have access to valuable information and they are relatively easy to exploit. A successful attack can result in a variety of devastating consequences including financial loss, damage to brand reputation, and loss of customer trust. Most organizations do not recover from a major security breach, making it absolutely critical to protect your users and customers from threats that target applications and email systems.

Our Data Center Application Security solution consists of a robust and integrated set of products to protect against these attacks. We are the only company that delivers a complete

single-vendor solution with the proven performance and security effectiveness to meet the increasing demands of today's data centers. In addition, our application security solutions can be integrated with FortiGate next-generation firewalls and FortiSandbox sandbox for extra defenses against advanced persistent threats (APTs).

Fortinet's Data Center Application Security Solution includes:

- Web application protection
- Encryption/decryption
- DDoS attack mitigation



### Web application protection

It's impossible to ensure all web applications on your system are free of vulnerabilities at any given time. Whether it's a previously undiscovered vulnerability, a vulnerability waiting to be patched, an out-of-support system, or some other issue, vulnerabilities are there, waiting to be exploited. Fortinet's [FortiWeb](#) Web Application Firewalls protect web-based applications from attacks that target vulnerabilities.

### Encryption/decryption with ADC

When a secure web application begins to grow, new servers need to be added to handle the user capacity and encryption needs. When you reach this point, new problems arise: something needs to control the additional servers and servers can only handle limited amounts of secure traffic encryption and decryption.

FortiADC's SSL offloading provides class-leading secure traffic encryption and decryption, alleviating this task from the web application servers. [FortiADC](#) can provide up to a 20 times increase in secure application traffic capacity versus using only servers.

### DDoS attack mitigation

Distributed Denial of Service (DDoS) attacks continue to be the top threat to IT security. DDoS attacks targeting the application layer tend to be small and hard to detect, but a successful attack will still shut down your vital services.

Fortinet's **FortiDDoS** DDoS Attack Mitigation appliances inspect all inbound and outbound traffic from a data center using 100% hardware and 100% behavior-based detection methods. FortiDDoS blocks all attacks including large bulk-volumetric and small application-layer attacks.

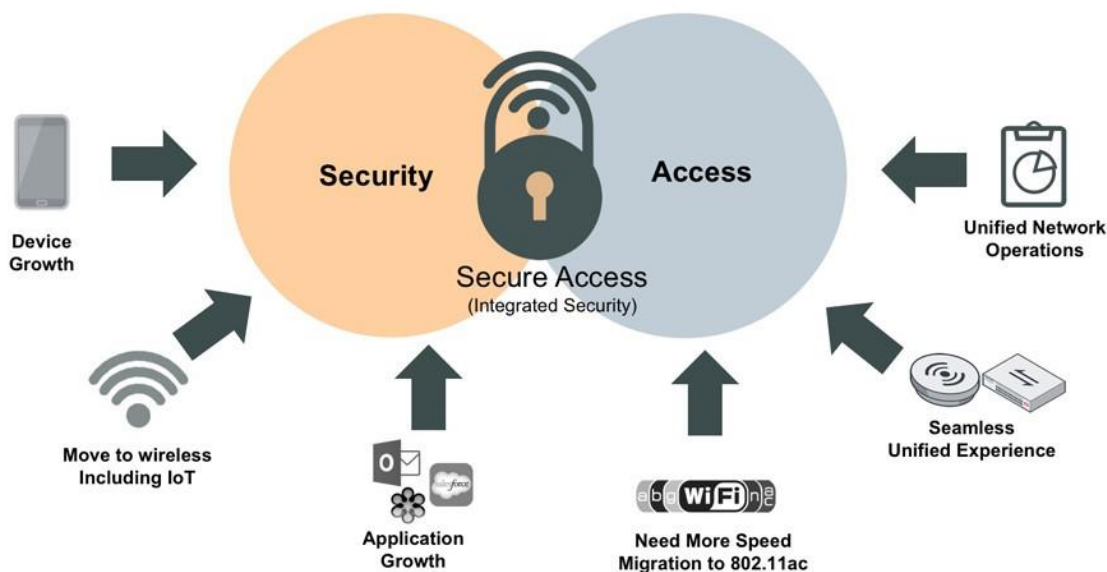
### 5.1.6 Secure Access Solution

Organizations are changing the way they deploy access networks, connect devices, and enable business applications to address a number of challenges:

- The number and types of network-connected wireless devices and mobile applications continue to grow exponentially, presenting new vulnerabilities and increasing the attack surface.
- Users want fast Wi-Fi and a smooth experience across wired and wireless networks.
- IT needs reduced complexity of network management, application management, and device management.

Securing business communications, personal information, financial transactions, and mobile devices involves much more than network access control. It requires scanning for malware, preventing access to malicious websites, endpoint integrity checking, and controlling application usage. As a result, IT departments are faced with the difficult task of balancing the requirements of network security with the flexibility to onboard the growing number and diversity of clients.

Typical Wi-Fi solutions cannot satisfactorily address these requirements. Only Fortinet's Secure Access solution delivers three WLAN deployment options to meet the different WLAN requirements of today's enterprises. In addition to WLAN services, our secure access portfolio also provides the most flexible security platform with end-to-end enforcement.



Our three offerings: Integrated, Controller, and Cloud enable any organization to choose the topology and network management that best fits its needs, without having to compromise on security.

### **Integrated Wi-Fi**

Our Integrated offering is a family of controller-managed access points that function in cooperation with a FortiGate next-generation firewall. In addition to consolidating all the functions of a network firewall, IPS, anti-malware, VPN, WAN optimization, web filtering, and application control in a single platform, FortiGate also includes an integrated Wi-Fi controller. Fortinet access points are either integrated into the FortiGate (FortiWiFi) or are connected directly to the FortiGate to provide comprehensive wireless coverage.

### **Controller Wi-Fi**

Our Controller offering combines on-premises controller-based management, network applications, and a range of high-performance indoor and outdoor access points. This is the ideal solution when an organization needs a dedicated wireless network that can be separated from the underlying network's security infrastructure. The Controller solution offers flexible channel deployment options to drastically reduce site survey and channel planning work while securing traffic through wireless traffic segmentation. This solution scales for implementations ranging from medium to large enterprises.

### **Cloud Wi-Fi**

Our Cloud solution is unlike any other Cloud Wi-Fi offering. Based on the FortiCloud Provisioning and Management Service and a new class of access points, the FortiAP-S series combines the elements of advanced firewall protection at the network edge with the simplicity and convenience of cloud management.

### **FortiSwitch**

Our Ethernet LAN switches are available in a large range of models to fit any environment.

Ideal for small to medium businesses, distributed enterprises, and branch offices, FortiSwitch secure access switches deliver superior security, performance, and manageability. In addition, they help increase productivity for next-generation applications through faster network access speeds.

## 6. FORTISWITCH SECURE SWITCHING

FortiSwitch Ethernet Access and Data Center Switches are a feature-rich yet cost-effective range of devices, supporting the needs of enterprise campus and branch offices, as well as data center environments.



The FortiSwitch Secure Access Switch series integrates directly into the FortiGate Connected UTM, with switch administration and access port security managed from the familiar FortiGate interface. Regardless of how users and devices connect to the network, you have complete visibility and control over your network security and access through this single pane of glass, perfectly suited to threat-conscious organizations of any size.

Virtualization and cloud computing have created dense high-bandwidth Ethernet networking requirements in the data center, pushing the limits of existing data center switching. FortiSwitch Data Center switches meet these challenges by providing a high performance 10 or 40 GbE capable switching platform, with a low Total Cost of Ownership. Ideal for Top of Rack server or firewall aggregation applications, as well as enterprise network core or distribution deployments, these switches are purpose-built to meet needs of today's bandwidth intensive environments.

<b>Integrated Security</b>	Pervasive Security through Fortinet Security Fabric Integration addressing the broadest threat surface.
<b>Simplified Management</b>	FortiGate integration creates one interface to manage security and access.
<b>Scalable</b>	Able to scale from desktop to datacenter across platforms allowing flexibility to grow as devices and traffic increase.

### Highlights

**Wide Range of Models** – With 1 GbE, 10 GbE and 40 GbE models, as well as Power over Ethernet options, there is a FortiSwitch to suit any deployment scenario.

**Power over Ethernet (PoE)** – Simplifies the installation of PoE equipment in the network, eliminating the need for the installation of additional power sockets to support APs and VOIP handsets.

**Flexible management** – Various management capabilities are available including CLI, Web or directly from a connected FortiGate GUI.

**Network Segmentation Support** – You can configure a single physical switch to support the convergence of voice, data and wireless traffic, while still meeting compliance requirements.

**40GbE Capability** – Future proofed 40 GbE will meet the bandwidth requirements of even the most intensive data center and network core applications.

**Port Level Network Access Security Features** – Secure Access Switch Series devices enable true port level network access security with 802.1X technology, managed centrally from any FortiGate.

**Offering Limited Lifetime Warranty (hardware replacement)** - Refer to policy at Fortinet Warranty Policy: <http://www.fortinet.com/doc/legal/EULA.pdf>

**Security Fabric** – FortiSwitch devices are essential part of Fortinet’s Security Fabric, offering visibility, user access control, and threat mitigation at the switch port level.

## **6.1 Secure Access Switches – Simple, Secure, Scalable Unified Access Layer Ethernet Switches**

Outstanding network security, performance, and manageability

Single-pane-of-glass management through tight integration with the industry leading FortiGate using FortiLink

FortiSwitch Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat conscious small to mid-sized businesses, distributed enterprises and branch offices. Tightly integrated into the FortiGate® Network Security Platform, the FortiSwitch Secure Access switches can be managed directly from the familiar FortiGate interface. This single pane of glass management provides complete visibility and control of all users and devices on the network, regardless of how they connect.

When a device connects to a Secure Access Switch Ethernet port, it is first identified, and then the user is authenticated. Once authenticated, access to the network is granted based on pre-defined security policy from the FortiGate, ensuring secure network access across the enterprise, without impacting the user experience. If any attacks sent by the user is detected by FortiGate, the user can be quarantined on FortiSwitch to stop it from spreading malicious traffic to other hosts in the network.

### **Security Fabric Integration**

Reduces complexity and decreases management cost with network security functions managed through a single console via FortiGate.

This integration allows all users to be authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

In addition, same security policy can apply to a user or device regardless of how or where they connect to the network.

Models: FS-108D-POE, FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124D, FS-124D-POE, FS-224E, FS-224E-POE, FS-224D-FPOE, FS-248E, FS-248E-POE, FS-248E-FPOE, FS-424D, FS-424D-POE, FS-424D-FPOE, FS-448D, FS-448D-POE, FS-448D-FPOE, FS-524D, FS-524D-FPOE, FS-548D and FS-548D-FPOE.

## Highlights

- Secure Access switches suitable for wire closet and desktop installations.
- Devices are identified and users authenticated prior to being granted access to the network.
- Security Fabric integration with actions taken on switch port level (user quarantine, Access VLAN, etc).
- Stackable up to 256 switches per FortiGate depending on model
- Centralized security management and reporting from FortiGate interface.
- Up to 48 ports in a compact 1 RU form factor.
- Power over Ethernet capable, including PoE+
- Ideal for converged network environments; enabling voice, data and wireless traffic to be delivered across a single network

## Key Features & Benefits

**Single Management Framework:** Reduces complexity and decreases management cost with network security functions managed through a single console.

**Single Policy Provisioning:** The same security policy can apply to a user or device regardless of how or where they connect to the network. Enables access to certain network ports based on the role of a user within the organization, such as in shared conference rooms or engineering facilities.

**Centralized Authentication:** All users are authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

**Role-Based Ports:** Enables access to certain network ports based on the role of a user within the organization, such as in shared conference rooms or engineering facilities.

### 6.1.1 FortiSwitch Rugged

FortiSwitch Rugged switches deliver all of the performance and security of the trusted FortiSwitch Secure, Simple, Scalable Ethernet solution, but with added reinforcement that makes them ideal for deployments in harsh outdoor environments.



Resilient, sturdy and capable of withstanding intense temperature fluctuations, FortiSwitch Rugged ensures the integrity and performance of mission-critical networks in even the most challenging of deployments.

## Add Ruggedized FortiGate for Tough and Powerful Protection

Engineered to survive in hostile environments with an extreme temperature range, the combination of FortiGate Rugged network security appliances with the FortiSwitch Rugged provides a connected network security solution.

### Simple Network Deployment

The Power over Ethernet (PoE) capability enables simple installation of cameras, sensors and wireless access points in the network, with power and data delivered over the same network cable.

There is no need to contract electricians to install power for your PoE devices, reducing your overall network TCO.

### Highlights

- Mean time between failure greater than 25 years
- Fanless passive cooling
- DIN-rail or wall-mountable
- Power over Ethernet capable including PoE+
- Redundant power input terminals
- Controlled by FortiGate

### Key Features and Benefits

<b>Sturdy IP30 construction</b>	Built to ingress protection 30 standards, the construction is designed to perform while enduring hostile conditions.
<b>Passive cooling</b>	With no fan and no moving parts, the mean time between failure is greater than 25 years.
<b>Redundant power inputs</b>	Maximizes network availability by eliminating the downtime associated with failure of a power input.
<b>Power over Ethernet capability</b>	Seamless integration of peripheral devices such as cameras, sensors and wireless access points into the network.

Models: FSR-112D-POE, FSR-124D

See datasheet environmental and compliance information.

## 6.2 Data Center Switches – High Performance Switching with Data Center Capabilities

Outstanding throughput, resiliency, and scalability

Single-pane-of-glass management through tight integration with FortiGate using FortiLink



FortiSwitch Data Center switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding throughput, resiliency and scalability for organizations with high performance network requirements. They are ideal for Top of Rack server or firewall aggregation applications, as well as enterprise network core or edge deployments, where high performance 10 GE or 40 GE is required. Purpose-built to meet the needs of today's bandwidth intensive data centers and enterprise networks, FortiSwitch Data Center switches deliver high-performance with a low Total Cost of Ownership.

### **Security Fabric Integration**

Reduces complexity and decreases management cost with network security functions managed through a single console via FortiGate.

This integration allows all users to be authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

In addition, same security policy can apply to a user or device regardless of how or where they connect to the network.

### **High-performance and resilient managed data center switch**

Designed in a compact 1 RU form factor, FortiSwitch Data Center switches are equipped with dual hot swappable power supplies to maximize network uptime. With 10 GE access ports and a high-throughput backplane, the FortiSwitch Data Center switches satisfy the Top of Rack server or firewall aggregation performance requirements of today's virtualization centric data centers. Advanced Link Aggregation with 802.3ad, Link Aggregation Control Protocol (LACP) and Multi-Chassis Link Aggregation Groups (MCLAG) provide increased uplink, server aggregation, or firewall aggregation throughput. Other advanced switch capabilities, such as large MAC address tables, jumbo frame support and port security, are standard features. The high-speed switching fabric is also well suited to enterprise network core or backbone network installations. FortiSwitch Data Center switches are a future-proof investment, providing the flexibility of deploying 1 GE, 10 GE or even 40 GE if required.

Models: FS-1024D, FS-1048D, FS-3032D

### **Highlights**

- High capacity switch suitable for Top of Rack or enterprise network deployments.
- Stackable up to 256 switches per FortiGate depending on model
- Maximum availability through dual hot swappable power supplies.
- Simply management via web-based or command line interface.
- Switch security features protect vulnerable infrastructure without adding latency.
- 1 GE or 10 GE access ports, in a compact 1 RU form factor.
- 40 GE capability options.

## Key Features and Benefits

**10 GE Capability:** Future-proofed 10 GE to satisfy the bandwidth requirements of intensive data center and network core applications.

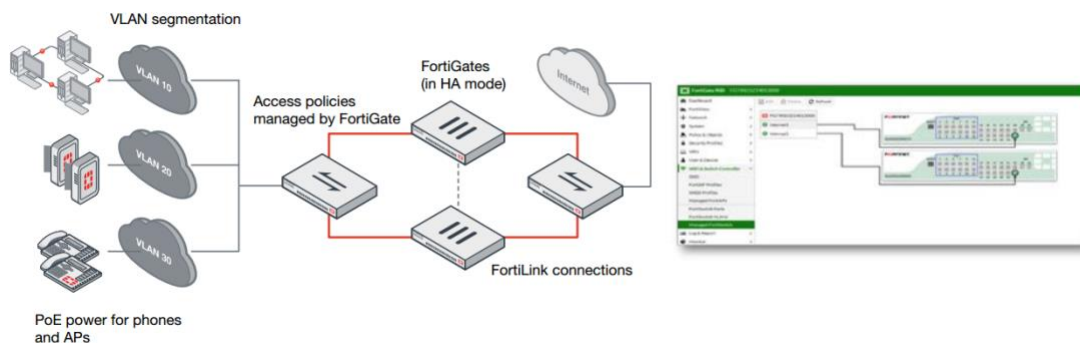
**Dual Power Supply Units:** Maximizes network availability by eliminating the downtime associated with single power supplies.

**FortiLink, Web and CLI Management:** Configuration and visibility into the network is made simple via FortiLink, web-based interface or CLI.

## 6.3 Deployment Options

### 6.3.1 FortiLink Mode

The FortiSwitch Secure Access Switch series integrates directly into the FortiGate\* Connected UTM, with switch administration and access port security managed from the familiar FortiGate interface. Regardless of how users and devices connect to the network, you have complete visibility and control over your network security and access through this single pane of glass, perfectly suited to threat conscious organizations of any size. (\* selected models only)



## FortiLink Advantages

Feature	Fortilink Advantage
Auto Discovery	FortiGate discovers FortiSwitch without need of additional configuration
Segment Network Centrally	With FortiGate it becomes simple to attach policies to ports
Upgrade Image	FortiGate upgrades FortiSwitchOS
Zero-touch provisioning	FortiGate automatically authorizes and configures FortiSwitch

Security Fabric Integration	Security applied to the switch port – FortiSwitch is simple extension to FortiGate
Wired and Wireless Central Control	FortiGate as central Switch+Wireless controller
POE Management	Control power budget centrally
Centralized Authentication	All users are authenticated against the same user database
Centralized Management	Use FortiManager to centrally manage FGTs and corresponding managed FortiSwitch
Stack	Control up to 256 FortiSwitch from the same FGT GUI

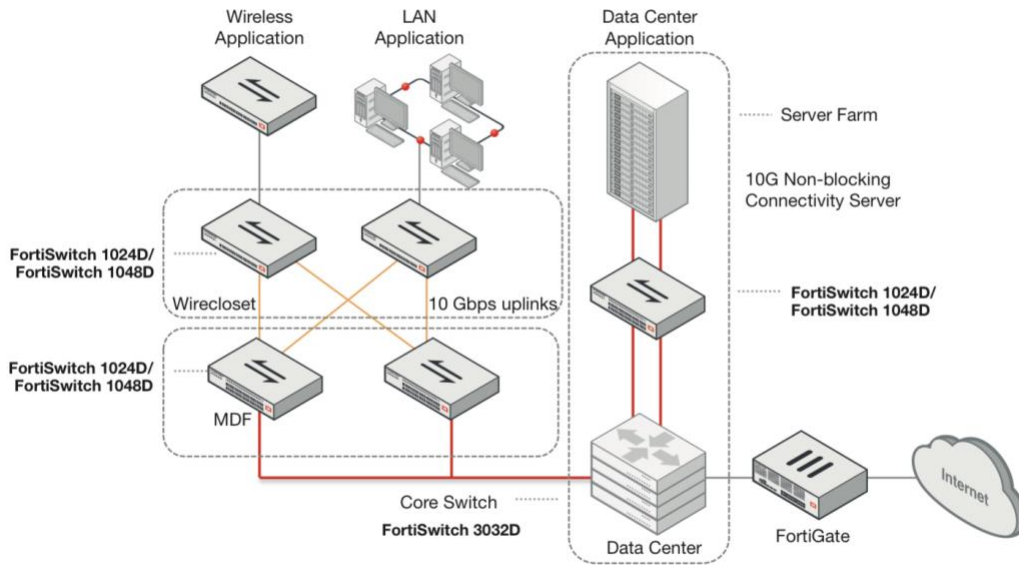
### Capabilities: FortiLink Mode

FORTISWITCH FORTILINK MODE (WITH FORTIGATE)	
<b>Management and Configuration</b>	
Auto Discovery of Multiple Switches	Yes
Number of Managed Switches per FortiGate	8 to 256 Depending on FortiGate Model (Please refer to admin-guide)
FortiLink Stacking (Auto Inter-Switch Links)	Yes
Software Upgrade of Switches	Yes
Centralized VLAN Configuration	Yes
Switch POE Control	Yes
Link Aggregation Configuration	Yes
Spanning Tree	Yes
LLDP/MED	Yes
IGMP Snooping	Yes (not supported on 108D-POE, 224D-POE, 1xxE-Series)
L3 Routing and Services	Yes (FortiGate)
Policy-Based Routing	Yes (FortiGate)
Virtual Domain	Yes (FortiGate)
<b>Security and Visibility</b>	
802.1x Authentication (Port-based, MAC-based, MAB)	Yes
Syslog Collection	Yes
DHCP Snooping	Yes
Device Detection	Yes
MAC Black/White Listing	Yes (FortiGate)
Policy Control of Users and Devices	Yes (FortiGate)
<b>UTM Features</b>	
Firewall	Yes (FortiGate)
IPC, AV, Application Control, Botnet	Yes (FortiGate)
<b>High Availability</b>	
Support FortiLink FortiGate in HA Cluster	Yes
LAG support for FortiLink Connection	Yes
Active-Active Split LAG from FortiGate to FortiSwitches for Advanced Redundancy	Yes (with FS-2xx, 4xx, 5xx)

### 6.3.2 Standalone Mode

Virtualization and cloud computing have created dense high-bandwidth Ethernet networking requirements in the data center, pushing the limits of existing data center switching. FortiSwitch Data Center switches meet these challenges by providing a high performance 10 or 40 GE capable switching platform, with a low Total Cost of Ownership. Ideal for Top of

Rack server or firewall aggregation applications, as well as enterprise network core or distribution deployments, these switches are purpose-built to meet the needs of today's bandwidth intensive environments.

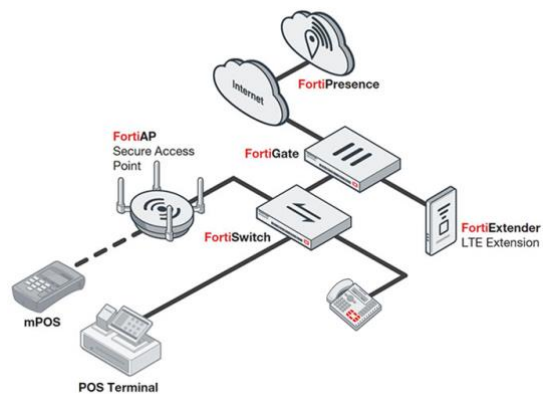


## 6.5 Solution Integration

### Retail

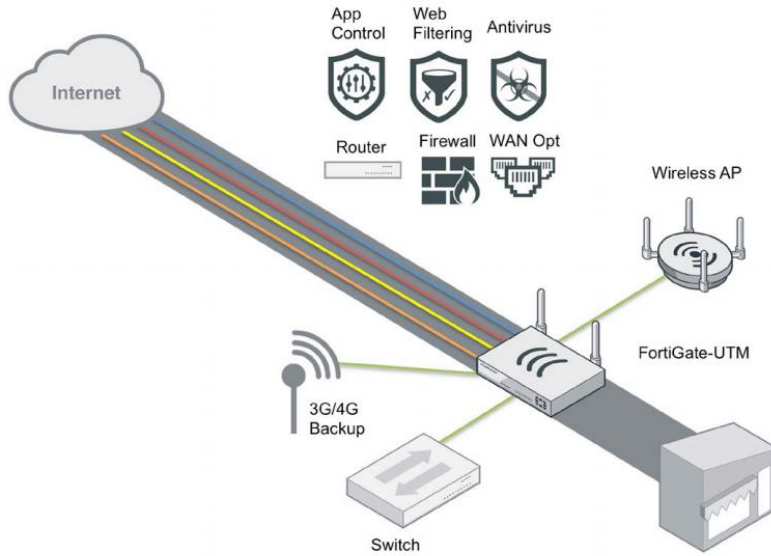
FortiSwitch integrates with Fortinet's complete solution for retail business. Benefits:

- Cost reduction
- Standardization
- Easy deployment in high scale
- Visibility
- Easily adapt to new retail tech



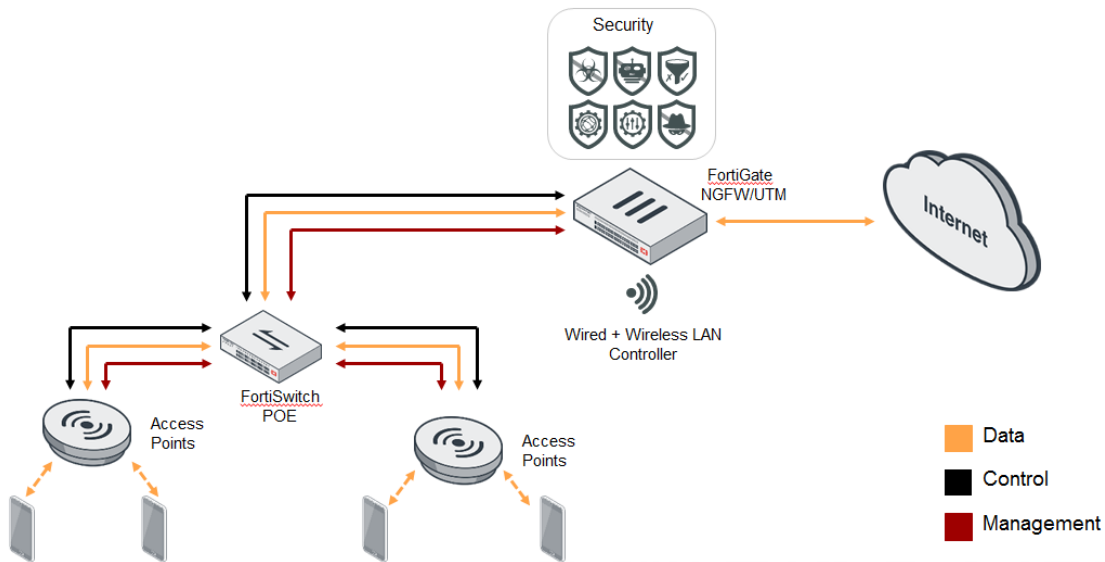
### Connected UTM

FortiSwitch integrates with Connected UTM solution providing extended connectivity and POE for SMB deployments. With FortiLink, FortiSwitch becomes an extension to FortiGate and it's possible to easily enforce policies for all of the different wired and wireless devices, kiosks, systems, and terminals in the network from a "single pane of glass".



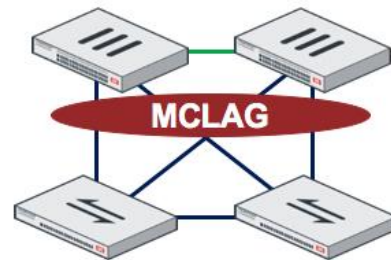
### Secure Access Architecture

FortiSwitch integrates with Secure Access Architecture solution providing network infrastructure necessary to interconnect wired and wireless. It also provides POE to power wireless access points and other devices in the network. The complete network can be controlled via FortiGate in a “single pane of glass”.



## FortiGate in HA

With the use of MCLAG, FortiGate HA pair can be connected in full mesh to FortiSwitch pair, providing complete link and switch level redundancy to the security solution.



Supported in FortiLink or Standalone mode.

## 7. FORTISWITCH COMMON REQUIREMENT SPECIFICATIONS AND ANSWERS

Use the following list to help answering RFP questions and, when possible, to tailor RFPs to Fortinet's favor. For supported models, check feature matrix in release notes. For physical/environmental specifications, refer to datasheets. For any unsupported feature, consult your regional SME/CSE.

### 7.1. General system requirements

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support simple management access i.e. without the need for local management clients (HTTPS preferred)	Yes	Yes	<b>Fully Compliant:</b> FortiSwitch has a CLI however this is for initial setup and includes some debugging commands for convenience. All configuration and management of the platform is web based using standard browsers.
<b>MUST</b> support SNMP for polling of system statistics	Yes	Yes	<b>Fully Compliant:</b> FortiSwitch supports SNMP v1, v2c and v3. FortiSwitch MIBs are available for download from the Fortinet Technical Support web site.
<b>MUST</b> support SNMP Traps for key system thresholds (specify)	Yes	Yes	<b>Fully Compliant:</b> FortiSwitch supports configurable SNMP TRAPS for key system thresholds.
<b>MUST</b> support SNMP MIB download from system GUI	Yes	Yes	<b>Fully Compliant:</b> FortiSwitch MIBs are available in the GUI.
<b>MUST</b> display a visual representation of authentication in the GUI	Yes	Yes	<b>Fully Compliant:</b> FortiSwitch includes a "Logout" button showing that user is logged in the system and offering the option to logout.
<b>MUST</b> log all authentication events:			

Locally	Yes	Yes	<b>Fully Compliant:</b> All authentication attempts are logged to the local file system under Event logs with the sub-type “admin” with details of the authenticating system, username, disposition (success, failed) and details of any failure. Local logs can be stored up to maximum file size specified by the administrator, at which point the file overwritten or logging stops.
Via syslog	Yes	Yes	<b>Fully Compliant:</b> Logs can be automatically replicated out to multiple external SYSLOG in their entirety or selectively based on the SYSLOG level and facility. Logs are automatically exported to FortiGate in FortiLink mode.
<b>MUST</b> be simple to install, manage and upgrade	Yes	Yes	<b>Fully Compliant:</b> FortiSwitch is delivered in a fully self-contained appliance format consisting of a hardened OS and all preconfigured applications. FortiSwitch requires simple initial CLI configuration. Following installation, all configuration is performed via a simple web based GUI.  All upgrades to the OS and application are performed via the upload of a firmware package available from the Fortinet Support Web Site. The file is simply downloaded to the desktop and uploaded to the appliance.
<b>MUST</b> support backup of the full system configuration via the GUI	Yes, as part of FortiGate config	Yes	<b>Fully Compliant:</b> Configuration can be backed up via the GUI.
<b>MUST</b> support a local user database	Yes, from FortiGate No need to login to the FSW	Yes	<b>Fully Compliant:</b> FortiSwitch allows configuration of multiple administrator accounts and corresponding access profiles to restrict permissions per configuration sub-system.
<b>MUST</b> support remote authentication users (LDAP, RADIUS and/or TACACS+)	No	Yes	<b>Fully Compliant:</b> FortiSwitch allows the configuration to remote authenticate users’ logins. For full details on parameters please refer to the FortiSwitchOS admin guide.
<b>MUST</b> have built-in tcpdump-like tool and log collecting functionality	Yes	Yes	<b>Fully Compliant:</b> Packet Capture and diagnose features in CLI offer similar packet capture capabilities like tcpdump.

<b>MUST</b> support REST API for configuration and monitoring	<b>Yes</b>	<b>Yes</b>	<b>Fully Compliant:</b> Based on JSON API.
<b>MUST</b> support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback.	<b>Yes</b>	<b>Yes</b>	<b>Fully Compliant:</b> Configuration backup/restore and alternate boot partition
<b>MUST</b> support dual power supply	<b>Yes</b>	<b>Yes</b>	<b>Available on:</b> FS-424D, FS-448D, FS-448D-FPOE, FS-5xx, FS-10xxD, FS-3032D
<b>MUST</b> support external RPS	<b>Yes</b>	<b>Yes</b>	<b>Available on:</b> FS-124D-POE, FS-224D-FPOE, FS-248D-FPOE, FS-424D-POE, FS-424D-FPOE, FS-448D-POE, FS-224E-POE, FS-248E-POE, FS-248E-FPOE
<b>MUST</b> support breakout cables (40G to 4x10G)	<b>No</b>	<b>Yes</b>	<b>FS-5xx and FS-3xxx models</b>
<b>MUST</b> offer hardware lifetime warranty	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support auto-ranging power supply with input voltages between 100 and 240V AC	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support 802.3ah (100BASE-X single/multimode fiber only)	<b>Yes</b>	<b>Yes</b>	Supported on 108D-POE/112D-POE/224D-POE
<b>MUST</b> support 802.3az for energy efficient Ethernet	<b>No</b>	<b>No</b>	

## 7.2. Layer 2 Requirements

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support jumbo frames	<b>Yes</b>	<b>Yes</b>	Max frame size = 9216
<b>MUST</b> support link auto-negotiation	<b>Yes</b>	<b>Yes</b>	<b>Fully Compliant:</b> 10G ports work also at 10/100/1000 speeds
<b>MUST</b> support manual link negotiation	<b>Yes, CLI</b>	<b>Yes</b>	<b>Fully Compliant</b>
<b>MUST</b> support Spanning Tree Protocol	<b>Yes</b>	<b>Yes</b>	<b>Fully Compliant:</b> MSTP (802.1s) native, and backwards compatible with RTSP (802.1w) and STP (802.1d)
<b>MUST</b> support Edge Port / Port Fast	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support STP Root Guard	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support BPDU Guard	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support IEEE 802.1p Mapping to priority queue	<b>Yes</b>	<b>Yes</b>	



<b>MUST</b> support IEEE 802.1q VLAN tagging	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support 4096 VLANs	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support Private VLAN	<b>Yes</b>	<b>Yes</b>	Except on FS-108D-POE and FS-224D-POE In FortiLink mode, Access VLAN
<b>MUST</b> support IEEE 802.3ad Link Aggregation with LACP	<b>Yes</b>	<b>Yes</b>	<b>Fully Compliant:</b> maximum number of link members depends on model
<b>MUST</b> support load balancing algorithms with Link Aggregation	<b>Yes</b>	<b>Yes</b>	<b>Fully Compliant:</b> dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac
<b>MUST</b> support MCLAG (MultiChassis Link Aggregation)	<b>Yes</b>	<b>Yes</b>	<b>FOS 5.6.0</b> <b>FSWOS 3.6.0</b> Not supported on FS-1xx models
<b>MUST</b> support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors	<b>Yes</b>	<b>No</b>	Supported if managed by FGT, all ISLs are automatically provisioned
<b>MUST</b> support MVR (Multicast VLAN Registration)	<b>No</b>	<b>No</b>	
<b>MUST</b> support load balancing algorithms with Link Aggregation	<b>Yes</b>	<b>Yes</b>	<b>Fully Compliant:</b> dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac
<b>MUST</b> support virtual wire	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support full line rate without traffic oversubscription	<b>Yes</b>	<b>Yes</b>	<b>Available on all models:</b> non-blocking, store-n-forward architecture
<b>MUST</b> support low latency mode (cut-through)	<b>No</b>	<b>Yes</b>	<b>Available on models:</b> FS-10xxD and FS-3032D
<b>MUST</b> support Ethernet protection mechanisms (IEEE 802.3ah or ITU-G.8031/8032)	<b>No</b>	<b>No</b>	<b>Check with CSE/PM for potential feasibility</b>
<b>MUST</b> support Shortest Path Bridging (SPB IEEE 802.1aq)	<b>No</b>	<b>No</b>	<b>Check with CSE/PM for potential feasibility</b>
<b>MUST</b> support Unidirectional Link Detection (UDLD)	<b>No</b>	<b>No</b>	<b>Cisco proprietary</b> <b>Use stp-loop-protection instead</b> <b>Or single member LAG with LACP</b> <b>Or Ethernet OAM (802.3ah) (roadmap)</b>
<b>MUST</b> support DCB (802.1Qbb and 802.1Qaz)	<b>No</b>	<b>No</b>	

### 7.3. Management requirements

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support zero-touch provisioning	Yes	No	Auto-discovery of switches
<b>MUST</b> support stacking	Yes	No	FortiGate is the stack controller, with single pane of glass.
<b>MUST</b> support stacking topology auto-discovery	Yes	No	
<b>MUST</b> support firmware update from a central point	Yes	No	
<b>MUST</b> support end device identification	Yes	No	
<b>MUST</b> support integration with Fortinet Security Fabric	Yes	No	
<b>MUST</b> support complete view of all switching solution from a single pane of glass	Yes	No	
<b>MUST</b> support 802.1x MAC-based authentication	Yes	Yes	
<b>MUST</b> support MAC Authentication Bypass (MAB)	Yes	Yes	
<b>MUST</b> support Time-Domain Reflectometry (TDR) Support	No	Yes	Except FS-108D-POE, FS-224D-POE
<b>MUST</b> support telnet/SSH	Yes	Yes	
<b>MUST</b> support SNMP	Yes	Yes	
<b>MUST</b> support firmware download via TFTP/FTP/GUI	Yes	Yes	
<b>MUST</b> support RMON I and II standards	No	No	
<b>MUST</b> support Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically	Yes	No	
<b>MUST</b> support MAC address notification	No	No	
<b>MUST</b> support Bridge MIB (RFC-1493)	Yes	Yes	
<b>MUST</b> support POE MIB (RFC 3621)	No	No	

### 7.4. Authentication Requirements

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support LLDP	Yes	Yes	

<b>MUST</b> support LLDP-MED	<b>Yes</b>	<b>Yes</b>	MED-TLVs: inventory and network policy
<b>MUST</b> support MAC based VLAN assignment (802.1v)	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support IP based VLAN assignment (802.1v)	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support protocol based VLAN assignment (802.1v)	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support 802.1x port-based authentication	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support 802.1x authentication via certificate EAP-TLS and EAP-TTLS	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support 802.1x guest VLAN assignment	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support 802.1x authentication fail VLAN for unauthenticated users	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support 802.1x MAC-based authentication	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support MAC Authentication Bypass (MAB)	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support captive portal	<b>Yes</b>	<b>No</b>	
<b>MUST</b> support LDAP	<b>No</b>	<b>Yes</b>	
<b>MUST</b> support RADIUS	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support RADIUS Accounting	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support RADIUS Change of Authorization (CoA)	<b>No</b>	<b>Yes</b>	
<b>MUST</b> support TACACS+	<b>No</b>	<b>Yes</b>	

## 7.5. POE Requirements

Requirement	FortiLink	Standalone	Response
<b>MUST</b> display total POE power consumption	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> display per port POE power consumption	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support POE port enable/disable	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support POE port reset	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support IEEE 802.3af	<b>Yes</b>	<b>Yes</b>	

<b>MUST</b> support IEEE 802.3at (POE+)	<b>Yes</b>	<b>Yes</b>	All "-POE" and "-FPOE" models except FS-108D-POE and FS-224D-POE
---	------------	------------	--

## 7.6. Layer 3 Requirements

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support static routing	<b>Yes, via FortiGate</b>	<b>Yes</b>	
<b>MUST</b> support line rate L3 forwarding	<b>Yes, via FortiGate</b>	<b>Yes</b>	Refer to release notes for supported models
<b>MUST</b> support RIPv2	<b>Yes, via FortiGate</b>	<b>Yes</b>	Requires Advanced license. Not supported on FS-1xx models.
<b>MUST</b> support OSPFv2	<b>Yes, via FortiGate</b>	<b>Yes</b>	Requires Advanced license. Not supported on FS-1xx models.
<b>MUST</b> support BGP	<b>Yes, via FortiGate</b>	<b>Roadmap</b>	
<b>MUST</b> support VRRP	<b>Yes, via FortiGate</b>	<b>Yes</b>	Requires Advanced license. Not supported on FS-1xx models.
<b>MUST</b> support IGMP	<b>Yes, via FortiGate</b>	<b>Roadmap</b>	
<b>MUST</b> support PIM	<b>Yes, via FortiGate</b>	<b>Roadmap</b>	
<b>MUST</b> support ECMP	<b>Yes, via FortiGate</b>	<b>Yes</b>	
<b>MUST</b> support BFD	<b>No</b>	<b>Yes</b>	
<b>MUST</b> support GRE	<b>No</b>	<b>No</b>	
<b>MUST</b> support L2TP	<b>No</b>	<b>No</b>	
<b>MUST</b> support MPLS, MPLS-TP	<b>No</b>	<b>No</b>	
<b>MUST</b> support ISIS	<b>No</b>	<b>Roadmap</b>	

## 7.7. Security

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support Storm Control	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support LoopGuard	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support IGMP snooping	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support IGMP querier	<b>Yes</b>	<b>Yes</b>	
<b>MUST</b> support DHCP snooping	<b>Yes</b>	<b>Yes*</b>	
<b>MUST</b> support DHCP relay	<b>Yes, via FortiGate</b>	<b>Yes</b>	Includes option 82

<b>MUST</b> support DHCP server	<b>Yes, via FortiGate</b>	<b>No</b>	
<b>MUST</b> support Port mirroring	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support sFlow	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support ACL	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support ACL classifier	<b>Yes, CLI only</b>	<b>Yes</b>	<b>Fully Compliant:</b> src-mac, dst-mac, ether-type, src-prefix, dst-prefix, service-id, vlan-id
<b>MUST</b> support ACL drop action	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support ACL policer action	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support ACL counter action	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support ACL mirror action	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support ACL redirect action	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support security checks	<b>Yes, CLI only</b>	<b>Yes</b>	<p>sip-eq-dip - TCP packet with Source IP equal to Destination IP.</p> <p>tcp_flag - DoS attack checking for TCP flags.</p> <p>tcp-port-eq TCP packet with Source and destination TCP port equal</p> <p>tcp-flag-FUP - TCP packet with FIN, URG and PSH flags set, and sequence number is zero.</p> <p>tcp-flag-SF - TCP packet with SYN and FIN flag set.</p> <p>v4-first-frag - DoS attack checking for IPv4 first fragment.</p> <p>udp-port-eq - IP packet with source and destination UDP port equal.</p> <p>tcp-hdr-partial - TCP packet with partial header.</p> <p>macsa-eq-macda - Packet with source MAC equal to Destination MAC.</p>
<b>MUST</b> support port MAC limit	<b>Yes, CLI only</b>	<b>Yes</b>	
<b>MUST</b> support MAC-IP binding	<b>Yes</b>	<b>Yes</b>	Map a MAC address to an IP address to avoid untrusted hosts
<b>MUST</b> support static MAC	<b>Yes</b>	<b>Yes</b>	Map a MAC address to a port to avoid flooding
<b>MUST</b> support Dynamic ARP Inspection	<b>Yes, CLI only</b>	<b>Yes</b>	

---

<b>MUST</b> support Sticky Mac	<b>Yes, CLI only</b>	<b>Yes</b>	
--------------------------------	----------------------	------------	--

## 7.8. QoS

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support 8 queues per port	Yes	Yes	
<b>MUST</b> support packet classification	Yes	Yes	
<b>MUST</b> support packet marking	Yes	Yes	
<b>MUST</b> support packet queuing	Yes	Yes	
<b>MUST</b> support 802.1p	Yes	Yes	
<b>MUST</b> support TOS/DSCP	Yes	Yes	
<b>MUST</b> support strict scheduling mode	Yes	Yes	
<b>MUST</b> support Round Robin (RR)	Yes	Yes	
<b>MUST</b> support Weighted Round Robin (RR)	Yes	Yes	
<b>MUST</b> support policer	Yes	Yes	
<b>MUST</b> support QoS per VLAN	Yes	Yes	

## 7.9. IPv6 Support

FortiSwitch supports IPv6 for device management. L2 and L3 features are expected in the second half of 2018.

Requirement	FortiLink	Standalone	Response
<b>MUST</b> support IPv6 Ready logo	No	No	
<b>MUST</b> support IPv6 unicast static routing	Yes	Yes	Only for device management
<b>MUST</b> support MLDv1 and v2 snooping	No	No	
<b>MUST</b> support option processing	Yes	Yes	Only for device management
<b>MUST</b> support fragmentation	Yes	Yes	Only for device management
<b>MUST</b> support ICMPv6	Yes	Yes	Only for device management
<b>MUST</b> support TCP/UDP over IPv6	Yes	Yes	Only for device management
<b>MUST</b> support Ping	Yes	Yes	Only for device management
<b>MUST</b> support Traceroute	Yes	Yes	Only for device management

<b>MUST</b> support SSH	<b>Yes</b>	<b>Yes</b>	Only for device management
<b>MUST</b> support SNMP	<b>Yes</b>	<b>Yes</b>	Only for device management
<b>MUST</b> support HTTP/HTTPS	<b>Yes</b>	<b>Yes</b>	Only for device management
<b>MUST</b> support Syslog	<b>Yes</b>	<b>Yes</b>	Only for device management
<b>MUST</b> support RADIUS	<b>Yes</b>	<b>Yes</b>	Only for device management
<b>MUST</b> support TACACS+	<b>Yes</b>	<b>Yes</b>	Only for device management
<b>MUST</b> support NTPv4 over IPv6	<b>Yes</b>	<b>Yes</b>	Only for device management
<b>MUST</b> support IPv6 First Hop Security	<b>No</b>	<b>No</b>	
<b>MUST</b> support RA Guard	<b>No</b>	<b>No</b>	
<b>MUST</b> support DHCPv6 Guard	<b>No</b>	<b>No</b>	
<b>MUST</b> support Binding Integrity Guard	<b>No</b>	<b>No</b>	
<b>MUST</b> support ACL	<b>No</b>	<b>No</b>	

### 7.9. VxLAN Support

VxLAN support is expected in the second half of 2018.



## 7.10 FortiSwitch Rugged Environmental and Compliance

See datasheet environmental and compliance information for each model.

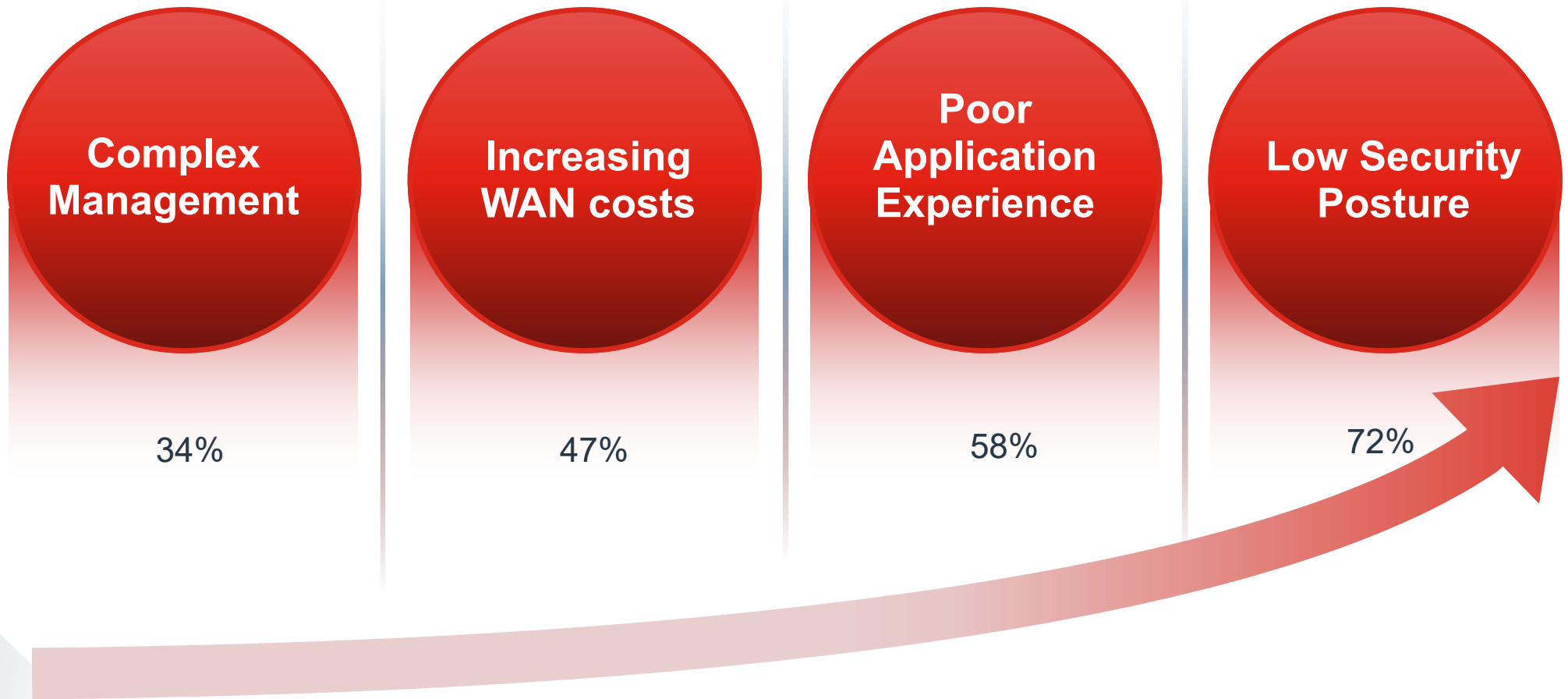
Requirement	FortiLink	Response
<b>MUST</b> support operating temperature range <b>-40 - +75 Celsius</b>	Yes	
<b>MUST</b> support storage temperature range <b>-40 - +85 Celsius</b>	Yes	
<b>MUST</b> support humidity (non-condensing) <b>5-95%</b>	Yes	
<b>MUST</b> support <b>EMI</b> : Radiated Emission: CISPR 22, EN55022 Class B Conducted Emission: EN55022 Class B	Yes	
<b>MUST</b> support <b>EMS</b> : ESD: IEC61000-4-2 Radiated RF (RS): IEC61000-4-3 EFT: IEC61000-4-4 Surge: IEC61000-4-5 Conducted RF (CS): IEC61000-4-6	Yes	
<b>MUST</b> support RoHS (Pb free) and WEEE	Yes	
<b>MUST</b> support MTBF >30 years	Yes	
<b>MUST</b> support fanless cooling	Yes	
<b>MUST</b> support Ingress Protection <b>IP30</b>	Yes	
<b>MUST</b> be <b>plenum-rated</b>	No	
<b>MUST</b> support <b>NEMA TS-2</b>	No	
<b>MUST</b> support <b>FCC Part 15, Class A</b>	Yes	
<b>MUST</b> support <b>CE</b>	Yes	
<b>MUST</b> support <b>UL</b>	No	
<b>MUST</b> support <b>CAN ICES-3 (A) / NMB-3 (A)</b>	Yes	
<b>MUST</b> support <b>KEMA, ODVA Industrial EtherNet/IP, PROFINETY2, ABB IT Certificate</b>	No	
<b>MUST</b> support <b>Shock IEC 60068-2-27</b> (Operational Shock, Non-Operational Shock)	No	
<b>MUST</b> support <b>Vibration IEC 60068-2-6, IEC 60068-2-64, EN61373</b> (Operational Vibration, Non-operational Vibration)	No	



# Fortinet Secure SD-WAN

Proposed by Innovative Solutions Technology

# Existing WAN Challenges at the Branch – Gartner Survey



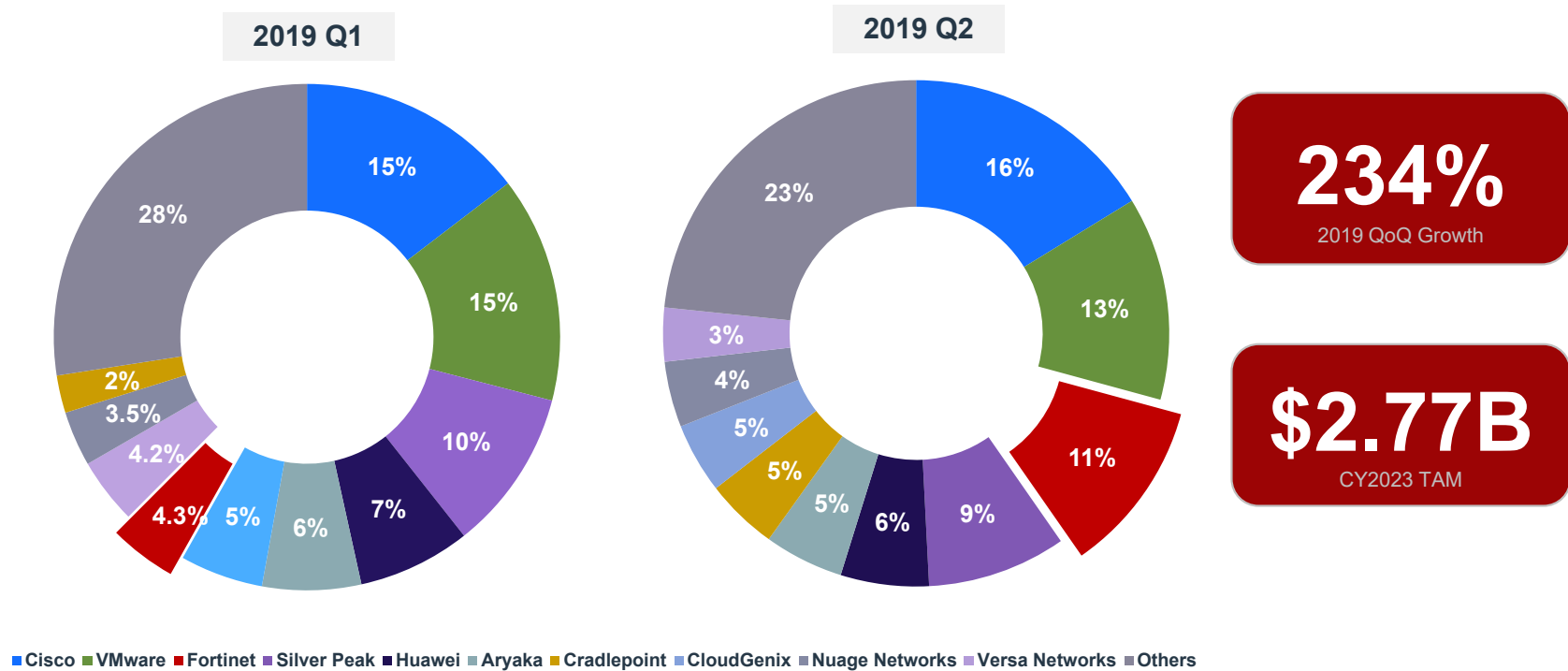
# SD-WAN is the New Business Outcome Driven WAN



# Fortinet Secure SD-WAN Evolution

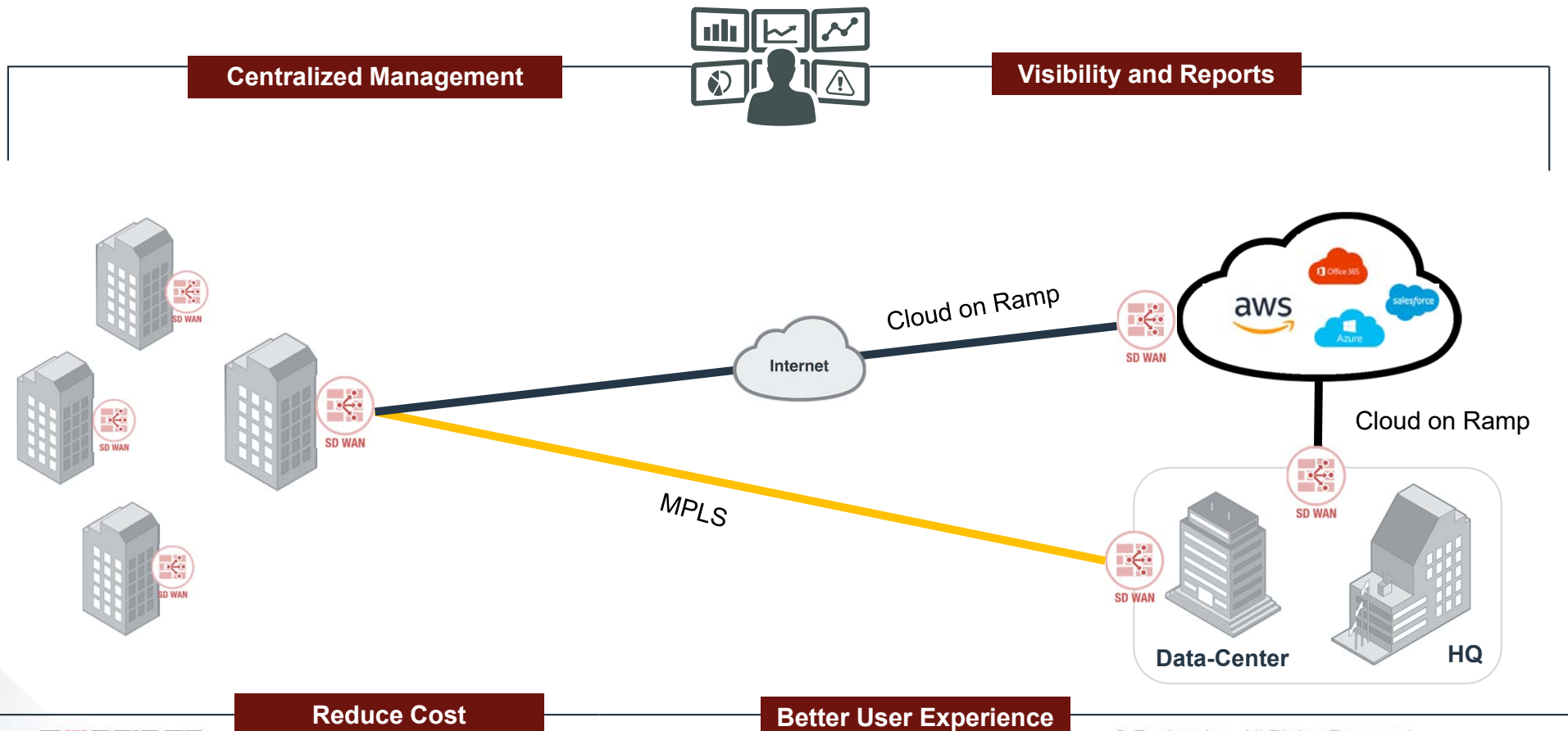


# SD-WAN - Fortinet in Top 3 SD-WAN Vendors

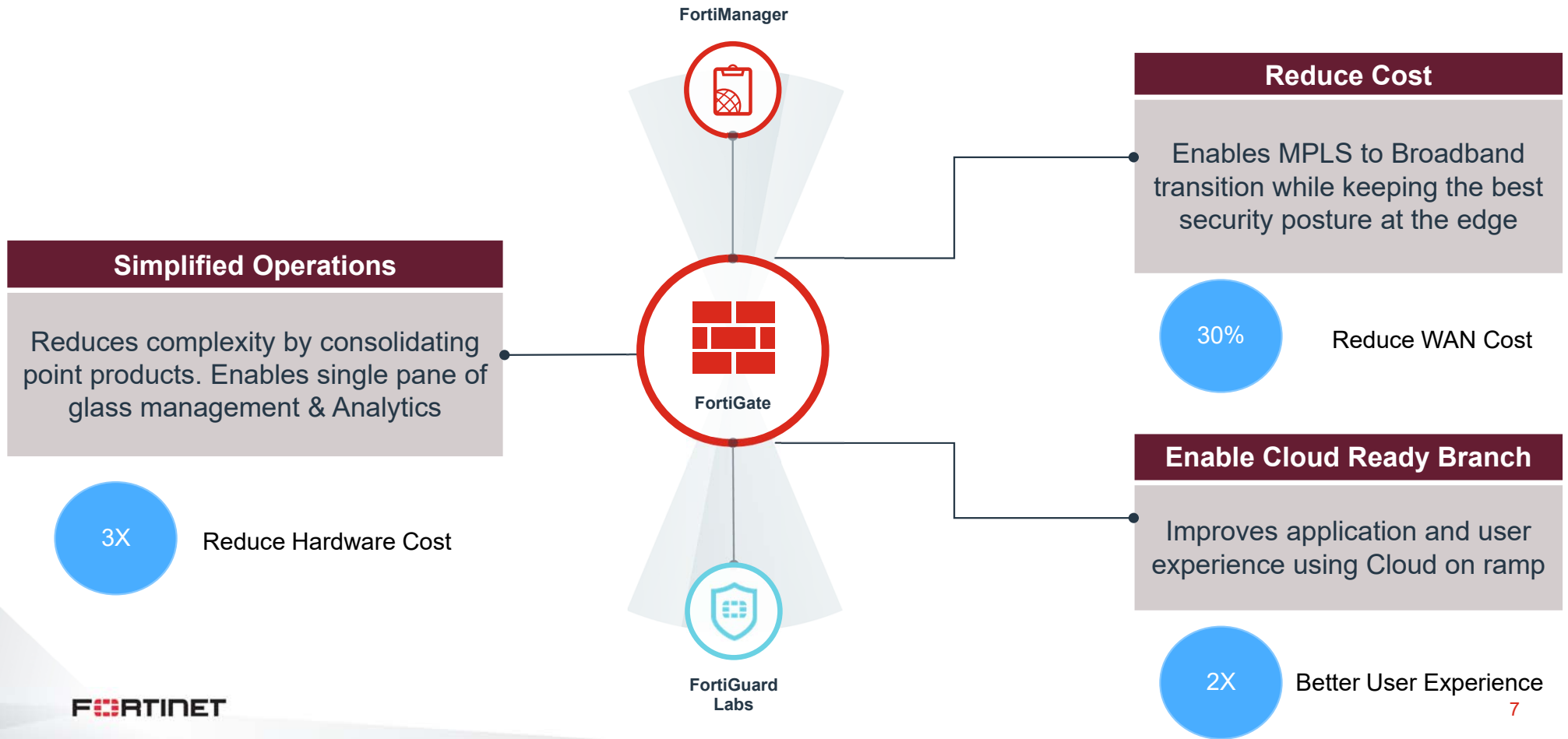


Source: Gartner: Enterprise Network Equipment by Market Segment, Worldwide, 2016-2023, 3Q19 Update, Gartner Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 2Q19

# Fortinet Secure SD-WAN Enables WAN Edge ROI

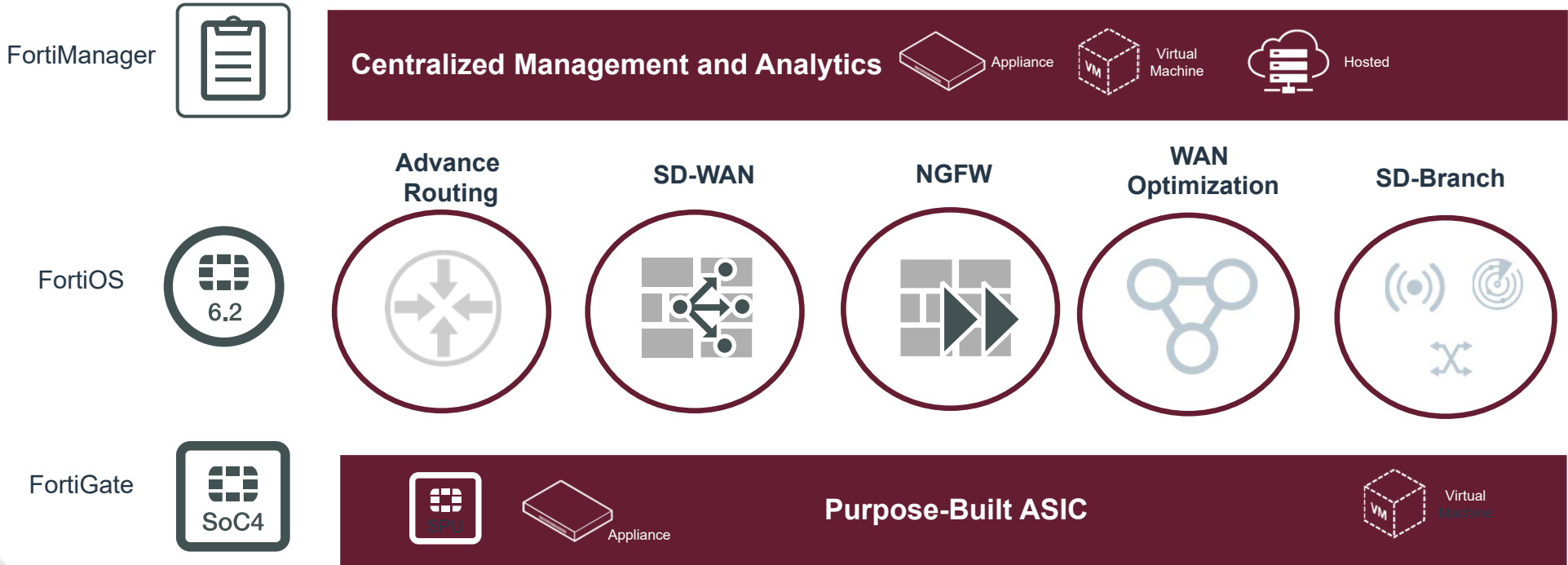


# Fortinet Secure SD-WAN Use-Cases





# Fortinet Secure SD-WAN – Security Driven Networking



# Fortinet Secure SD-WAN Innovations

FortiManager



**New Centralized SD-WAN Policy and Analytics**

FortiOS



**Advance SD-WAN and NGFW Features**

FortiGate



**Industry's First Secure SD-WAN ASIC**

# Best of Breed SD-WAN Capabilities



- Visibility into 5000+ Applications
- High Application Identification Accuracy



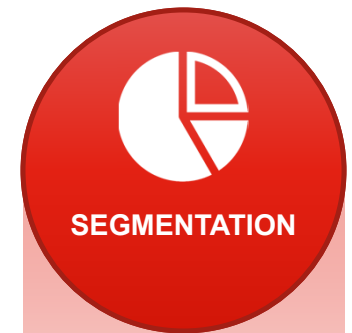
- Application Steering Based on Expanded SLAs
- Automated Fail-Over Capabilities



- WAN Path Remediation (FEC)
- Tunnel Bandwidth Aggregation (Per Packet Steering)



- High-level Monitoring of SD-WAN Devices on a Map
- Expanded Historical SLA Analytics



- Multi-Tenancy with Patented VDOM
- User Level Segmentation for Applications

# Flexible SD-WAN Rules

## Best Quality

- Automatically select the best interface based on latency jitter, packet loss

## Lowest Cost (SLA)

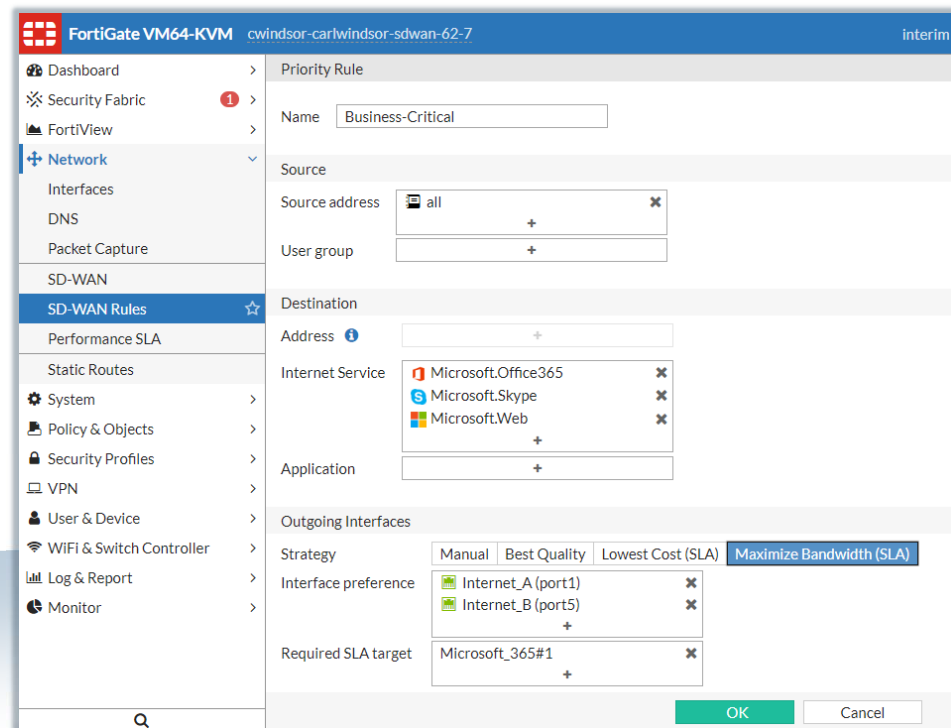
- Use the lowest cost interface which is within SLA
- Best for primary/backup link scenarios

## Maximum Bandwidth

- Distribute traffic across all interfaces that meet SLA

## Manual

- Used to pin an application to a specific interface (e.g. O365 -> WAN1)

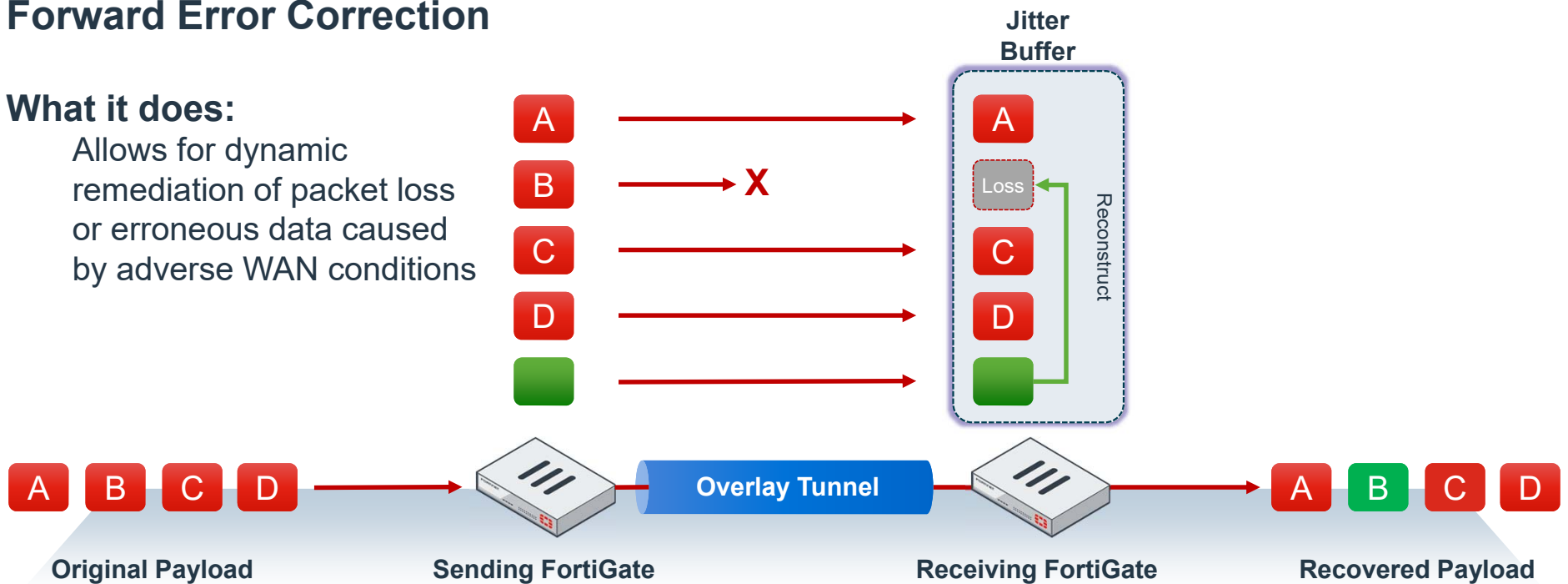


# WAN Path Remediation for Business Critical Applications

## Forward Error Correction

### What it does:

Allows for dynamic remediation of packet loss or erroneous data caused by adverse WAN conditions



# Evolution of SD-WAN Feature

	2.8	3.0	5.2	5.4	5.6	6.0	6.2
Policy Route	✓	✓	✓	✓	✓	✓	✓
Equal-cost multipath (ECMP)		✓	✓	✓	✓	✓	✓
Dead Gateway Detection		✓	✓	✓	✓	✓	✓
Wan Link Load Balance			✓	✓	✓	✓	✓
Zero Touch			✓	✓	✓	✓	✓
ISDB				✓	✓	✓	✓
Best Path Selection				✓	✓	✓	✓
SD-WAN Interface					✓	✓	✓
Security Fabric					✓	✓	✓
Minimum SLA enforcement link steering						✓	✓
Application Control						✓	✓
FortiManager Template and Monitor						✓	✓
IPv6						✓	✓
Dynamic Routing (BGP)						✓	✓
Interface percentage based traffic shaping						✓	✓
Forward Error Correction							✓
SD-WAN rule load balance							✓
Per packet load balance							✓
Additional BGP path							✓
ADVPN							✓
Cloud-Assist Monitoring							✓
Factory default health checks							✓

# New Purpose-Built Secure SD-WAN ASIC



## Ultra Fast SD-WAN

Industry's Fastest Application Steering for efficient business operations

## Best of Breed Security

Enable Best of Breed, Certified SD-WAN and Security with high performance

## Ease of Use

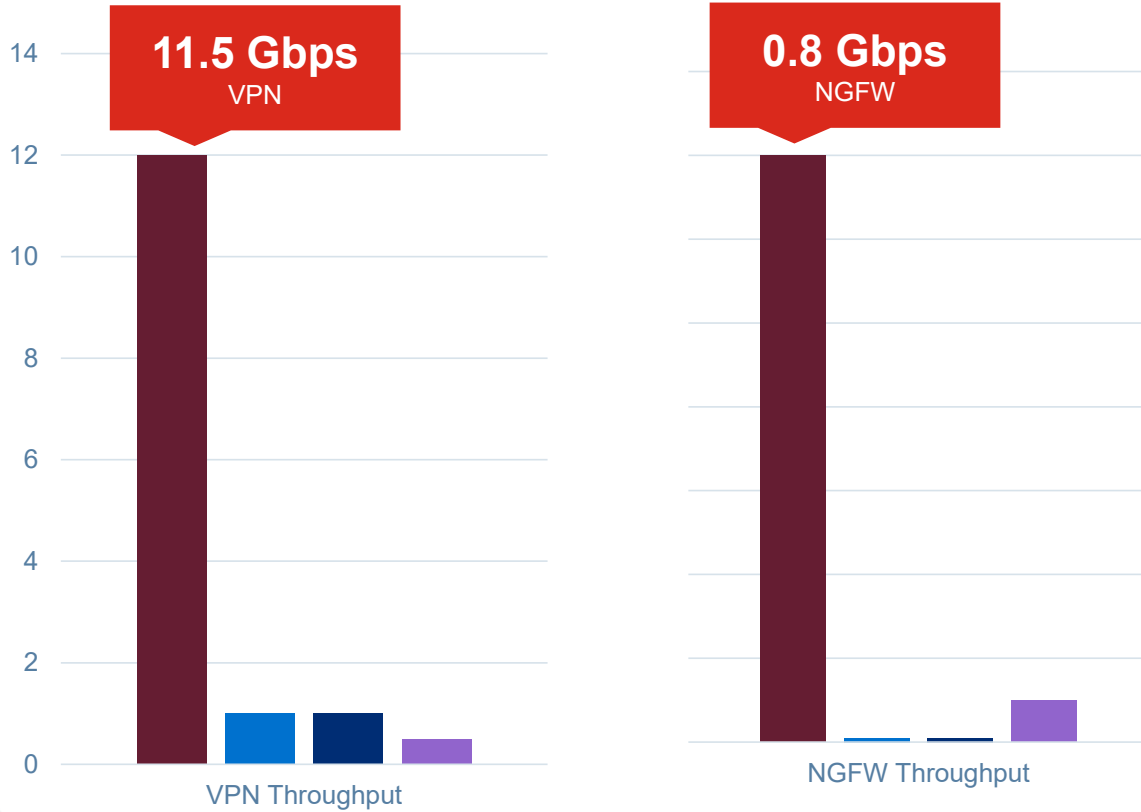
Best user experience with responsive accelerated overlay WAN

## SD-Branch Enabled

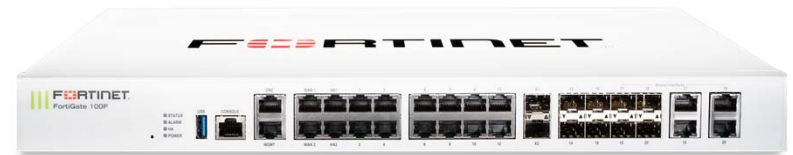
Accelerated Security extension to access layer to enable SD-Branch transformation



# FortiGate 100F SD-WAN Competitive Comparison



	Fortinet	VMware Velocloud	Cisco Viptela	Cisco Meraki
	FortiGate 100	Edge-840	vEdge-1000	MX 100
1G	✓	✓	✓	✓
10G	✓	✗	✗	✗
SSL	✓	✗	✗	✗
Tunnel	2500	400	N/A	250
SD-Branch	✓	✗	✗	✓

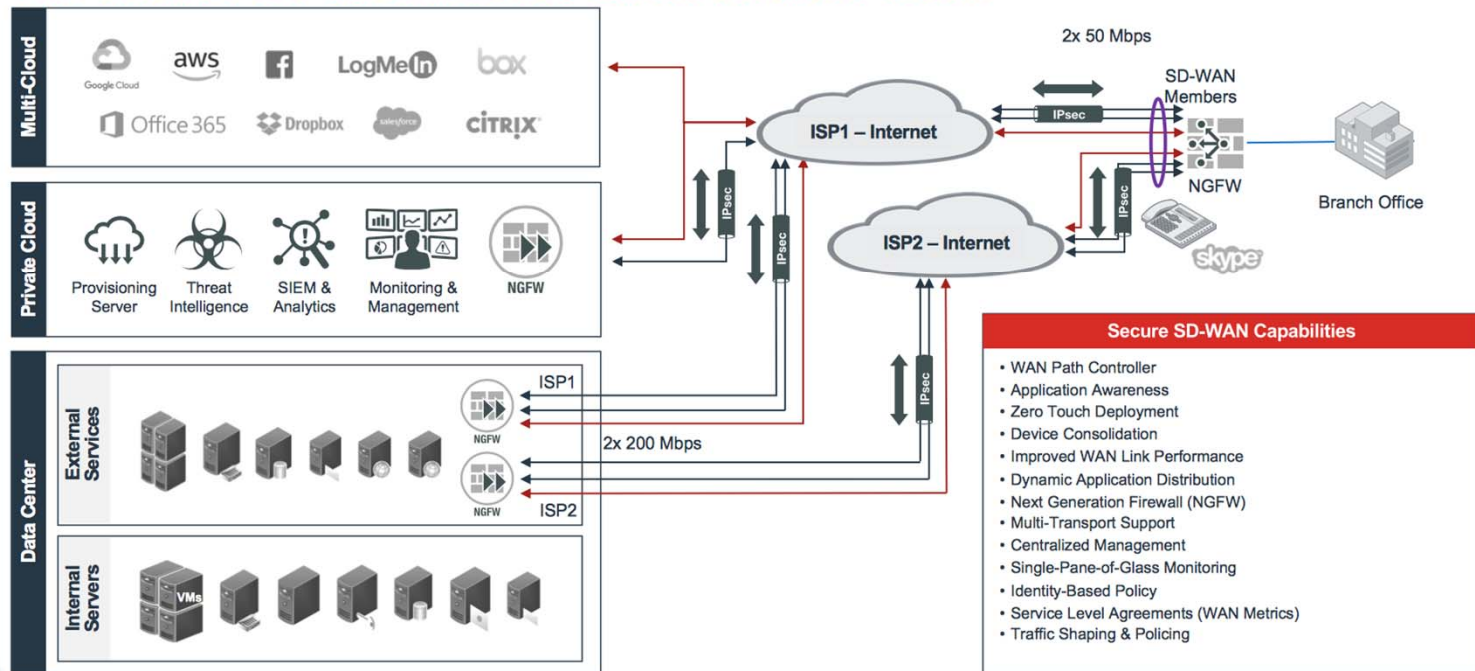




# Reference Architecture for Secure SD-WAN

## Redundant Broadband Enterprise Branch

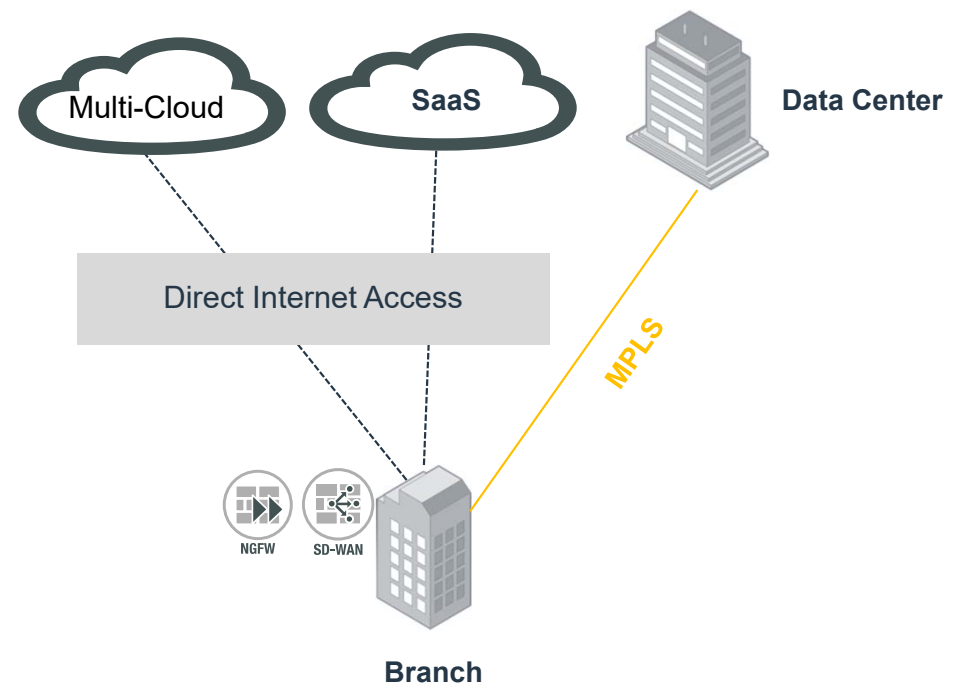
Two Internet Service Providers Direct Internet Access



# Use Case 1 : Cloud Ready Branch with Enhanced Security

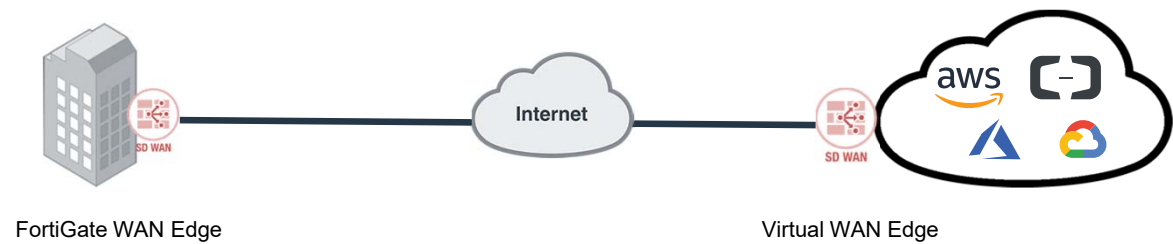
## Key Goals

- Faster Access to Multi-Cloud
- Efficient Adoption of SaaS
- Enterprise-grade Security

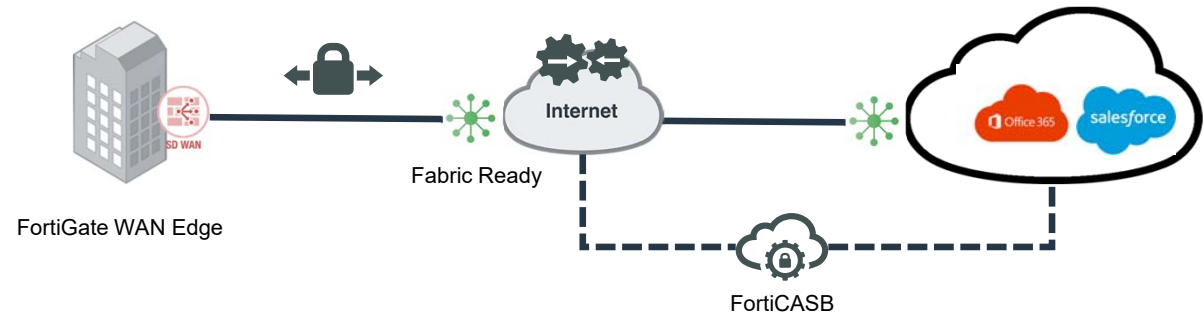


# SD-WAN – Cloud on Ramp to IaaS and SaaS

Last Mile Optimization

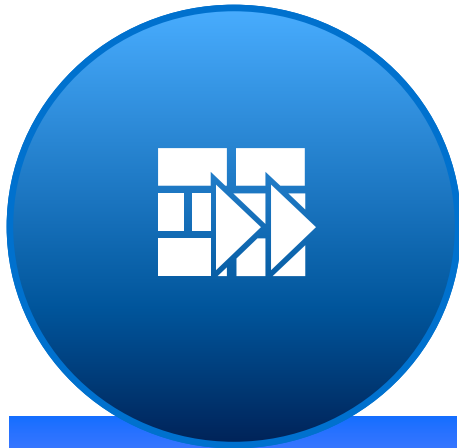


Middle Mile Optimization



# Key Security and Cloud Optimization Capabilities

## Threat Prevention



Gartner MQ Leader  
IPS, URL Filtering, ATP  
Cloud Sand-box

## SSL Inspection



Deep SSL Inspection  
TLS 1.3 Supported  
Best Performance

## Cloud On-Ramp



Middle-Mile Optimization  
Multi-Cloud SD-WAN  
Presence

## FortiCASB

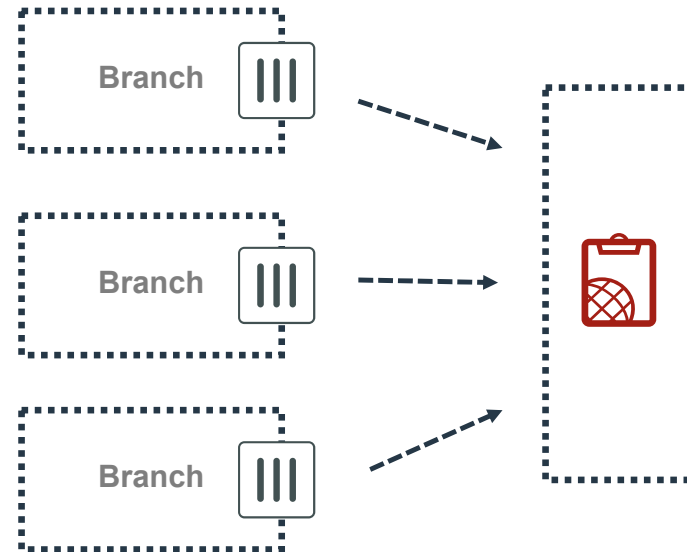


User Behavior Monitoring  
Shadow IT Discovery  
Major SaaS App supported

# Use Case 2 : Simplified Operations

## Key Goals

- Faster deployment with ZTP
- One centralized management
- Analytics and Reports for SD-WAN



# WAN Edge Orchestration – Single Pane of Glass

## Centralized Management



SD-WAN Policy Template  
NGFW Policy  
Multi-Tenancy

## Analytics and Reporting



NOC-SOC Monitoring  
SD-WAN Historic SLA

## Zero Touch Deployment



ZTP with FortiCloud  
SD-WAN and SD-Branch

## Compliance

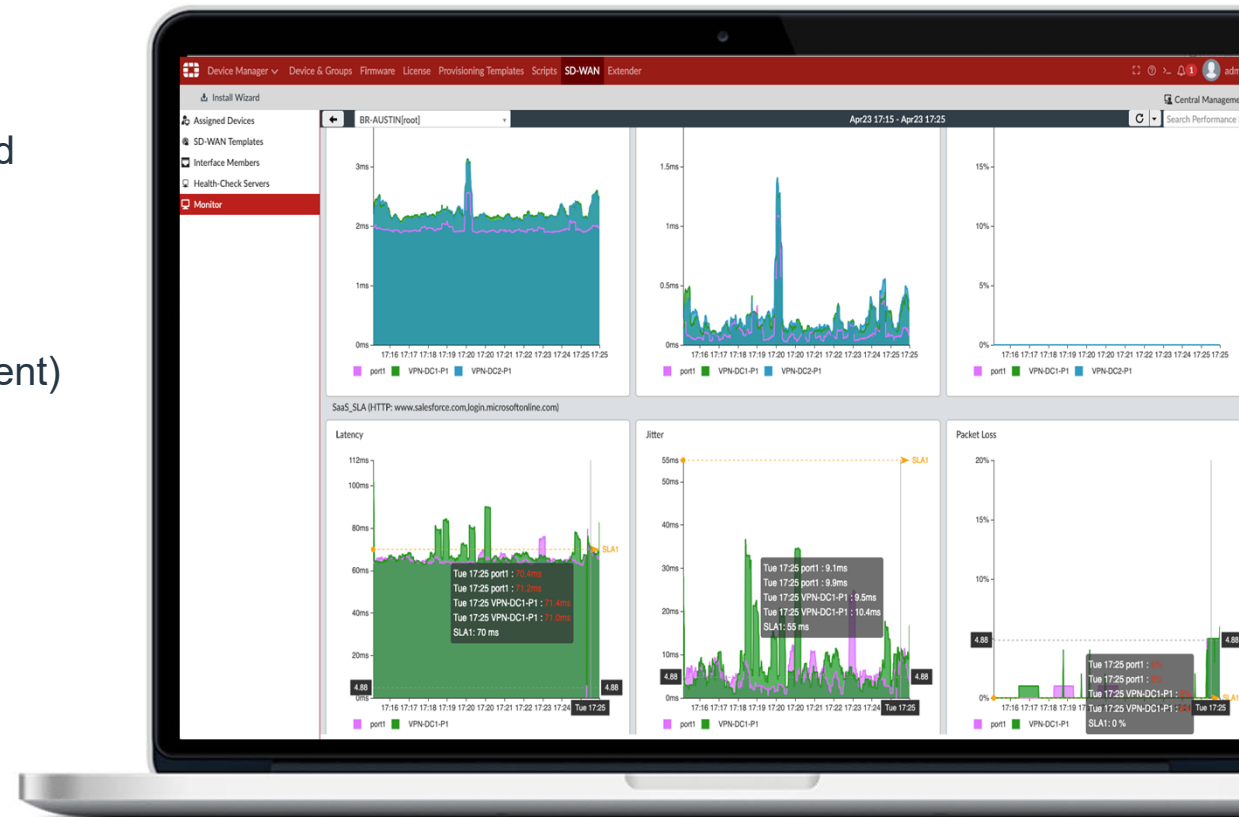


Security Rating  
PCI/HIPPA Best Practices

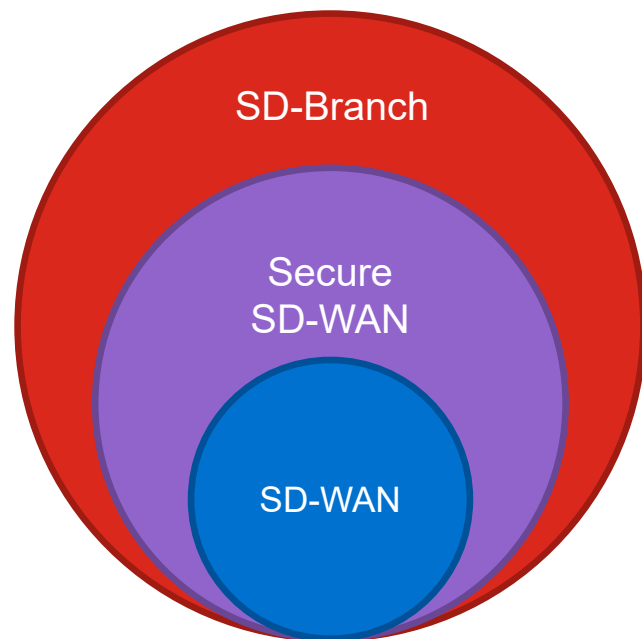
# Single Pane of Glass Management – FortiManager



- SD-WAN Templates and NOC dashboard
- SD-WAN Expanded SLA Monitoring
- Security Policy and SOC dashboard
- SD-Branch (Switches and AP Management)



# Evolution of Wide Area Networking at the Branch



- **Secure SD-WAN**  
Provides visibility and security but there are too many additional point products
- **SD-Branch**  
Provides Consolidation and Integration of Secure SD-WAN features into Ethernet and Wireless network.



# Fortinet Secure SD-Branch

## Consolidation through Convergence

### Consolidation

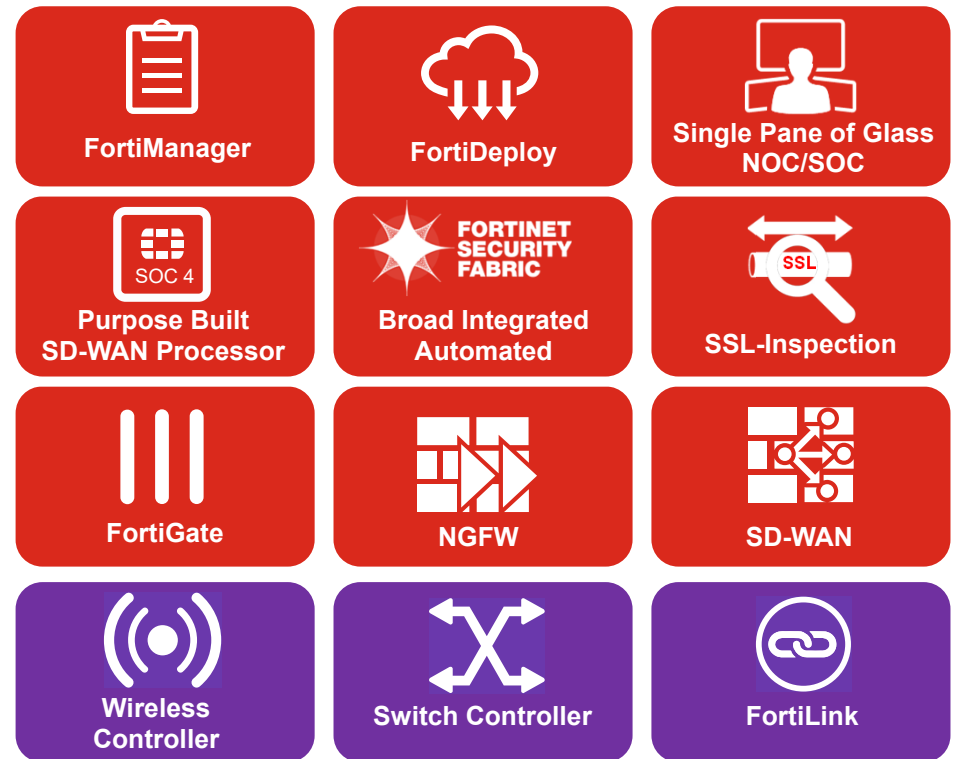
- The consolidation of branch services
- Not just a single box. Offers flexibility to grow from one switch or AP to many.

### Integration

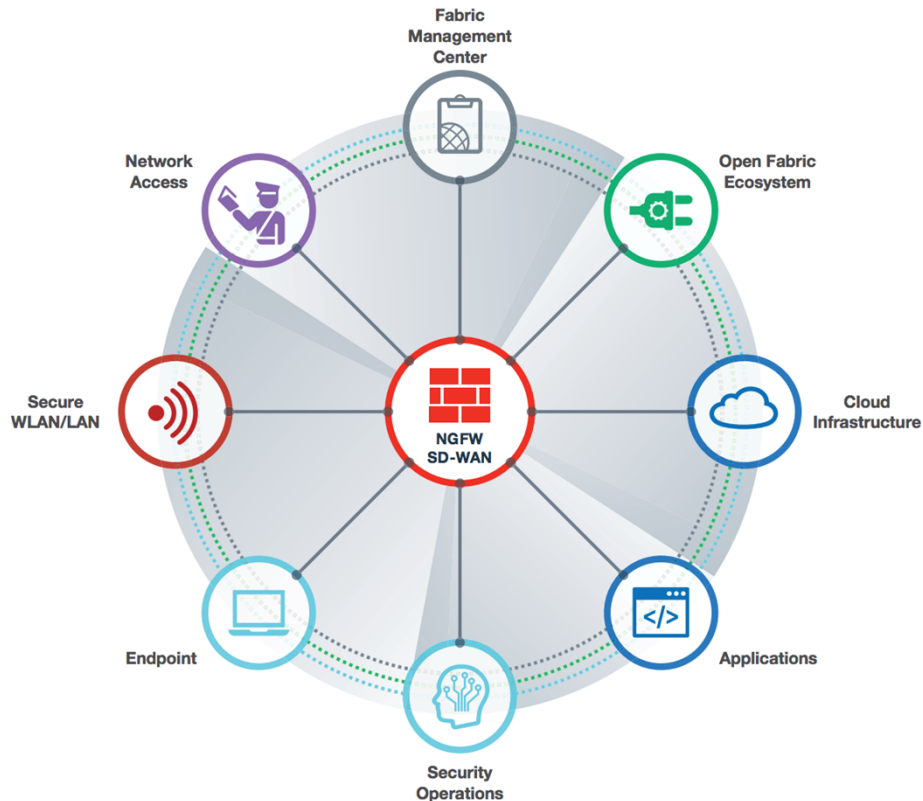
- Access management built into FortiOS directly integrated into the FortiGate
- Ethernet ports and WLANs are FortiGate interfaces.

### Simplicity

- Zero touch deployment
- Single interface to manage SD-WAN, Security and Network Access



# Fortinet Secure SD-Branch



## FortiOS Enables Broad, Integrated, Automated Security

FortiOS is the network operating system of the entire Fortinet Security Fabric. Every component—from the next-generation firewalls (NGFWs) to the access points and switches to the NAC solution—is driven by the same FortiOS code. This means that the Security Fabric components:

- Are configured and managed the same way, so network and security administrators who know one Security Fabric product need minimal training to manage them all
- All receive consistent OS updates, enabling consistent life cycle and policy management
- All log events in the same way, facilitating communication and data compilation for reporting and analysis
- Are able to coordinate to address multipronged attacks across the organization's attack surface

# FortiGate Access Management Through FortiLink

## Simplicity

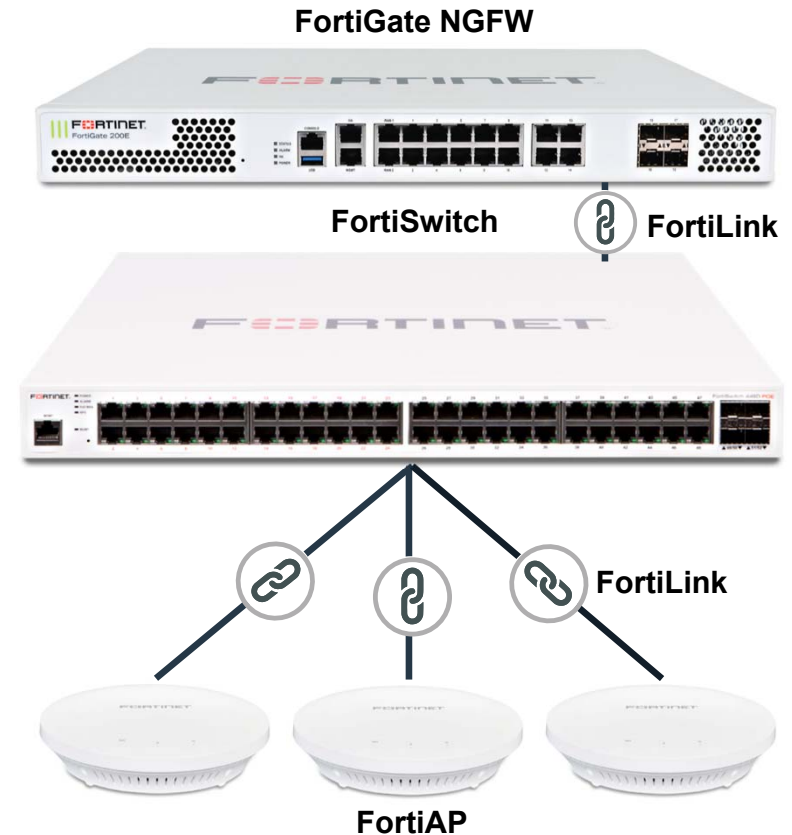
- Automated provisioning of access layer
- Visibility and analytics across wired, wireless, and security
- Flexible architecture, scales as needs change

## Security

- Firewall and switch ports equally secure, SSIDs tied directly to firewall policies
- Global Security polices down to port and WLAN level

## Lower Cost of Ownership

- Access Management included with SD-Branch. No licenses required



# Market Validation



# Gartner's 2018 Magic Quadrant for WAN Edge



Fortinet should be **shortlisted for all WAN edge** opportunities globally,

The vendor's **vision and roadmap** to deliver increasing levels of automation align with Gartner's view of emerging customer needs

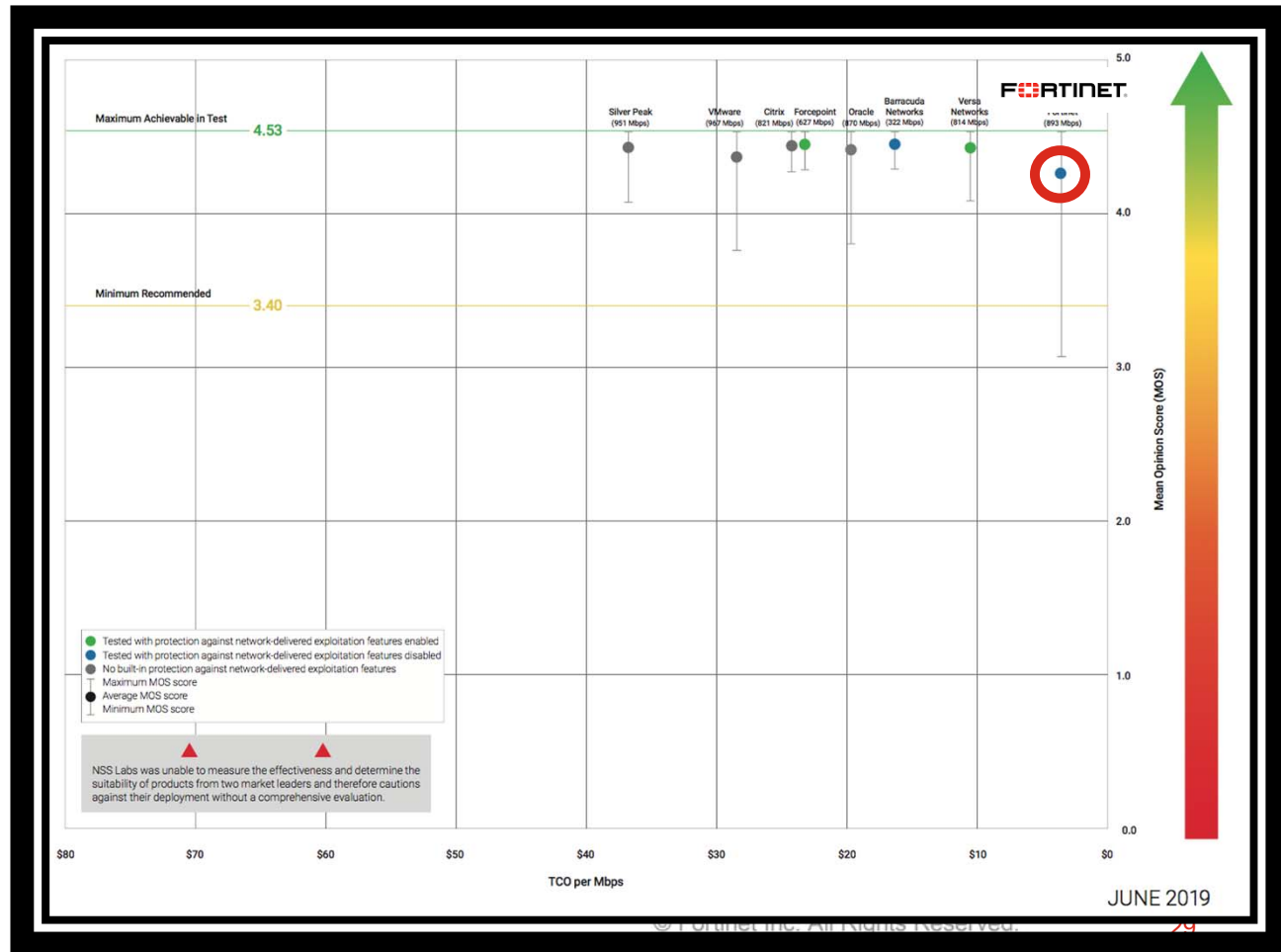
Marked as a "Challenger" with **Furthest "Completion of Vision"**

# NSS Labs Network Value Map (NVM) SD-WAN 2019

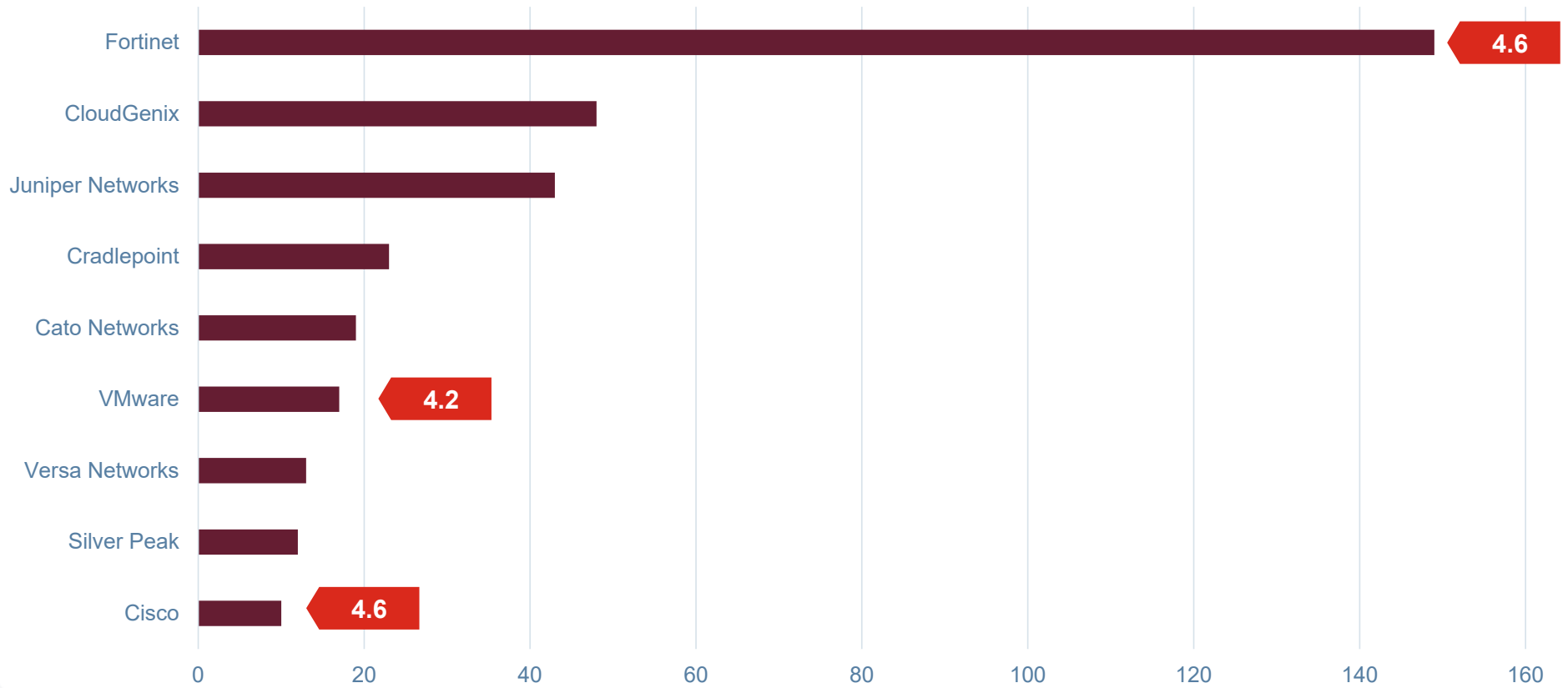


## FortiGate SD-WAN Results

- ✓ Second SD-WAN **Recommended** Rating
- ✓ **Best TCO** among all 8 vendors (\$3.5)
- ✓ Zero Touch Deployment **in 6 Minutes**
- ✓ Reliable QoE Score



# Gartner WAN Edge MQ Peer Insights



**FORTINET**<sup>®</sup>





# WV Dept of Transportation Technical Response

# Fortinet Security Fabric

## BROAD

Visibility of the entire digital attack surface

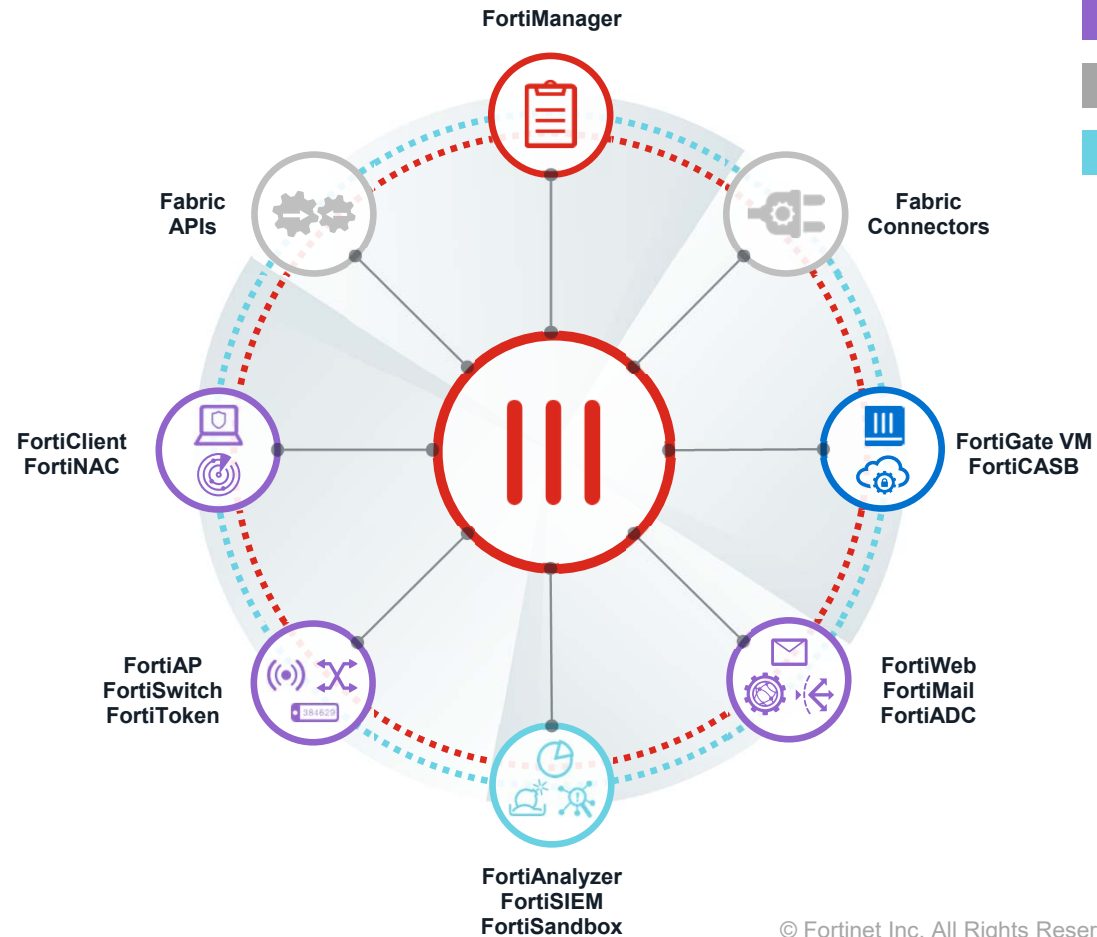
## INTEGRATED

Protection across all devices, networks, and applications

## AUTOMATED

Operations and response driven by Machine Learning

- Network Security
- Multi-Cloud Security
- Device, Access, and Application Security
- Open Ecosystem
- Security Operations



# FortiLink enables Secure Access

FortiLink protocols enable FortiGate to manage Fortinet's network access layer

## Simplicity

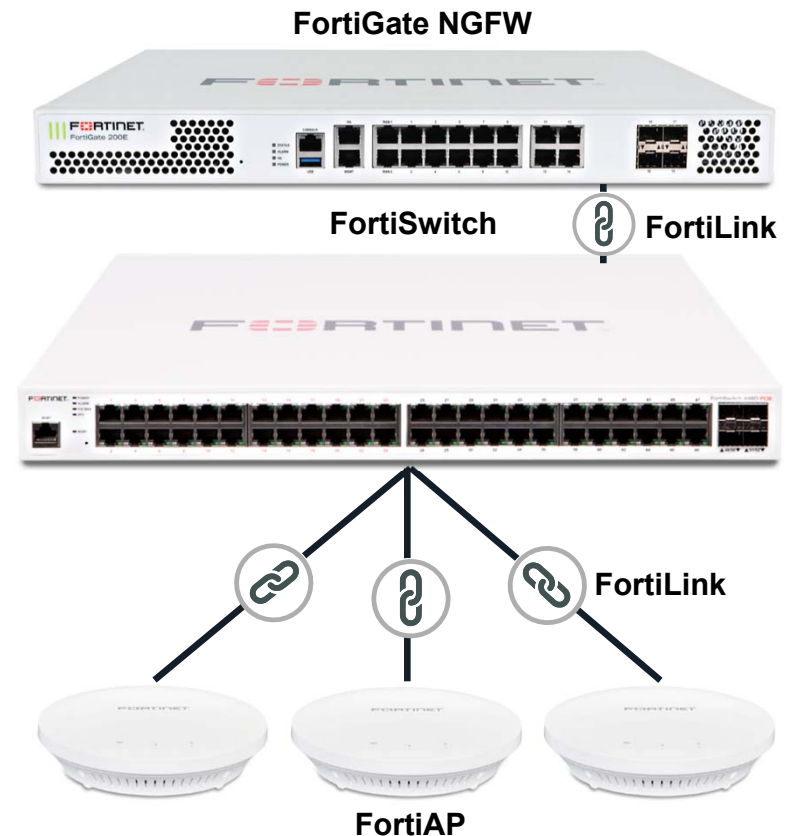
- Flexible architecture, scales as needs change
- Management visibility and analytics across wired, wireless, and security

## Security

- Firewall and switch ports equally secure, SSIDs tied directly to firewall policies
- Global Security polices down to port and WLAN level

## Lower Cost of Ownership

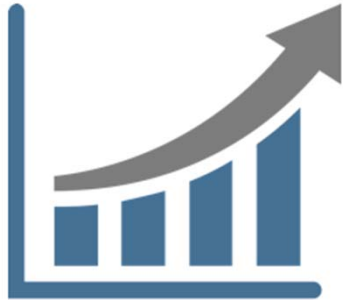
- Access Management included with SD-Branch. No licenses required



© Fortinet Inc. All Rights Reserved.

# A Secure Simple Scalable model to address Ethernet access

## Number of Devices



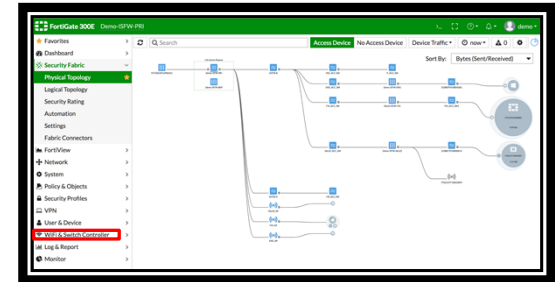
FortiSwitch Scales to support growth and higher bandwidth requirements

## Security



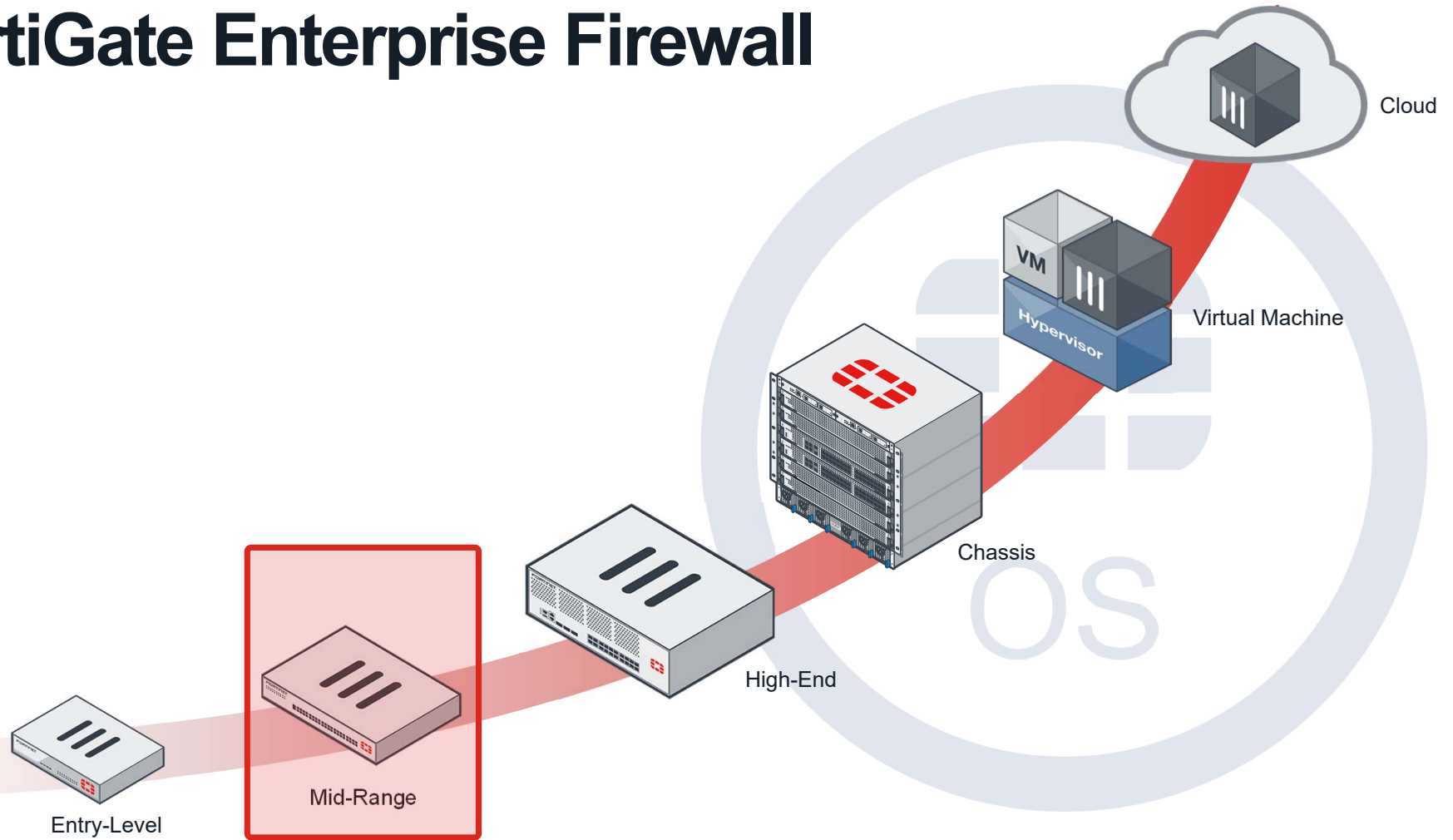
Security Integrated into Ethernet Access through FortiLink

## Management

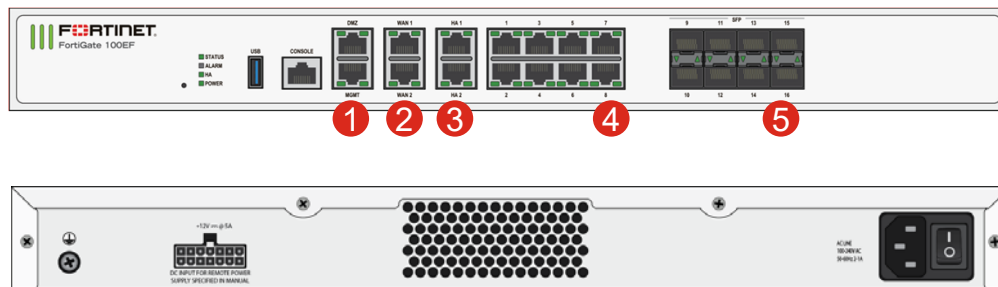


Single Interface to Manage Security, Access, and WAN.

# FortiGate Enterprise Firewall



# FortiGate 100F



- ① 2 x GE RJ45 MGMT/DMZ Ports
- ② 2 x GE RJ45 WAN Ports
- ③ 2 x GE RJ45 HA Port
- ④ 8 x GE RJ45 Ports
- ⑤ 8 x GE SFP Slots



**7.4 Gbps**

Firewall throughput

**30,000**

New Sessions/Sec

**2 Million**

Concurrent Sessions



**130 Mbps**

SSL Inspection Throughput



**500 Mbps**

IPS Throughput



**360 Mbps**

NGFW Throughput



**250 Mbps**

Threat Protection Throughput



**Enterprise Branch / Mid Enterprise**  
NGFW / Secure SD-WAN



**FORTINET**

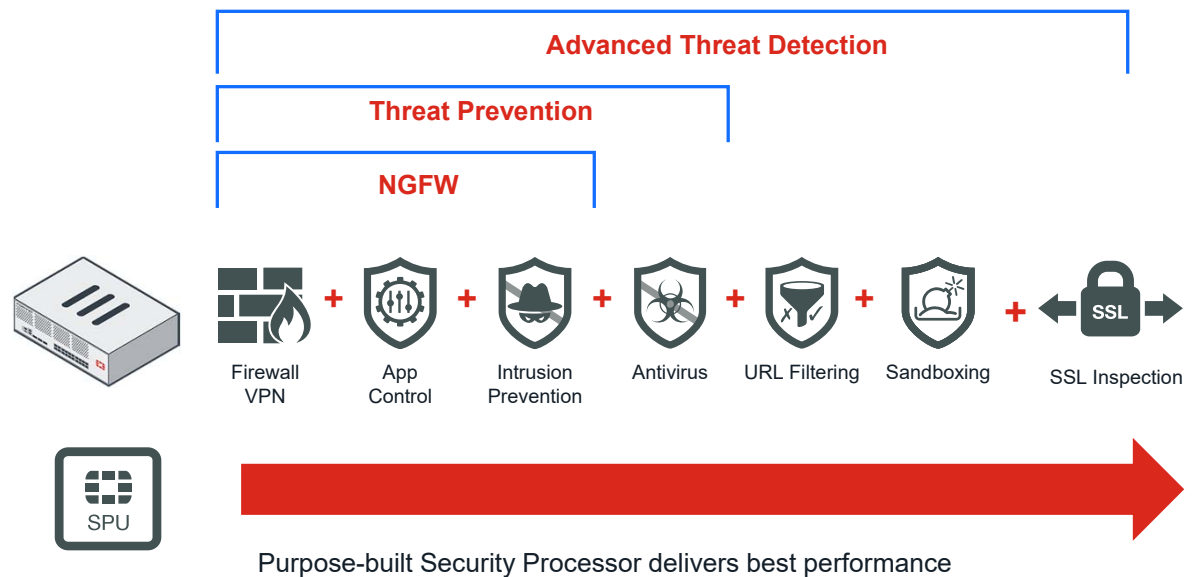
© Fortinet Inc. All Rights Reserved.

# Next Generation Firewall with Advanced Threat Detection

## Standalone



## FortiGate Next Generation Firewalls



























**FortiSwitch**



# FortiSwitch Family

48 ports		 FSW-248E-FPOE	 FSW-448D-FPOE	 FSW-548D-FPOE	
		 FSW-248D/E-POE	 FSW-448D-POE		
		 FSW-248D	 FSW-448D	 FSW-548D	 FSW-1048E FSW-1048D
32 ports				 FSW-3032E FSW-3032D	
24 ports		 FSW-124E-FPOE	 FSW-224D-FPOE	 FSW-424D-FPOE	 FSW-524D-FPOE
		 FSW-124E-POE	 FSW-224E-POE	 FSW-424D-POE	
		 FSW-124E	 FSW-224E	 FSW-424D	 FSW-524D
8 ports		 FSW-108E-FPOE			
		 FSW-108E-POE			
		 FSW-108E			
	<b>100 Series</b>	<b>200 Series</b>	<b>400 Series</b>	<b>500 Series</b>	<b>1000/3000 Series</b>
	+ 2x GE SFP uplink (except FS-124E/-POE/-FPOE)	+ 4x GE SFP uplink	+ 2x10 GE SFP+ uplink	+ 4x 10 GE SFP+ and 2x 40 GE stacking	<b>Data Center Switches</b>

# FortiSwitch 400 Series



- ① 24x GE RJ45 POE/POE+ Ports
- ② 2x 10GE SFP slots



- ① 48x GE RJ45 POE/POE+ Ports
- ② 4x 10GE SFP slots



## FS-424D-FPOE

## FS-448D-FPOE

Switch Capacity	88 Gbps	176 Gbps
MAC Address Storage	16K	16K
Network Latency (64b)	<1 $\mu$ s	<1 $\mu$ s
VLANs Supported	4K	4K
Max LAG Size	up to 12 ports	up to 12 ports
PoE Power Budget	370 W	370 W
Power Supply	Single PS, Optional FRPS-740	Dual Redundant PS

**FORTINET®**

West Virginia Ethics Commission  
**Disclosure of Interested Parties to Contracts**

(Required by W. Va. Code § 6D-1-2)

Name of Contracting Business Entity: Indicium Technology Address: 484 Williamsport Pike  
Suite 135

Name of Authorized Agent: JAMILA JONES-FLEET Address: Martinsburg, WV 25404

Contract Number: DOT2000000157 Contract Description: Cisco Routers or Equal

Governmental agency awarding contract: WEST VIRGINIA DIVISION OF HIGHWAYS

Check here if this is a Supplemental Disclosure

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below (attach additional pages if necessary):

**1. Subcontractors or other entities performing work or service under the Contract**

Check here if none, otherwise list entity/individual names below.

**2. Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**

Check here if none, otherwise list entity/individual names below.

Jamila Jones-Fleet

**3. Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**

Check here if none, otherwise list entity/individual names below.

Signature: Jamila Jones-Fleet Date Signed: 12 May 2020

**Notary Verification**

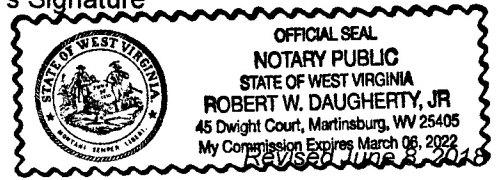
State of WV, County of Berkeley:

I, JAMILA JONES-FLEET, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this 12 day of MAY, 20.

Robert W Daugherty JR  
Notary Public's Signature

**To be completed by State Agency:**  
Date Received by State Agency: \_\_\_\_\_  
Date submitted to Ethics Commission: \_\_\_\_\_  
Governmental agency submitting Disclosure: \_\_\_\_\_



STATE OF WEST VIRGINIA  
Purchasing Division

# PURCHASING AFFIDAVIT

**CONSTRUCTION CONTRACTS:** Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

**ALL CONTRACTS:** Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

**EXCEPTION:** The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

**DEFINITIONS:**

**"Debt"** means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

**"Employer default"** means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

**"Related party"** means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

**AFFIRMATION:** By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (W. Va. Code §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

**WITNESS THE FOLLOWING SIGNATURE:**

Vendor's Name: Indicium Technology

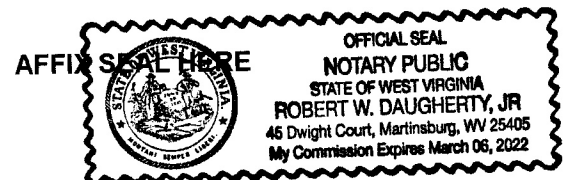
Authorized Signature: *Jamila Jones Fleet* Date: 12 May 2020

State of WV

County of Beekley, to-wit:

Taken, subscribed, and sworn to before me this 12 day of MAY, 2020.

My Commission expires 03 - 06, 2022



NOTARY PUBLIC *Robert W Daugherty Jr*  
*Purchasing Affidavit (Revised 01/19/2018)*

# VENDOR PREFERENCE CERTIFICATE

Certification and application is hereby made for Preference in accordance with **West Virginia Code**, §5A-3-37. (Does not apply to construction contracts). **West Virginia Code**, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the **West Virginia Code**. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. **Application is made for 2.5% vendor preference for the reason checked:**  
\_\_\_\_ Bidder is an individual resident vendor and has resided continuously in West Virginia, or bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia, for four (4) years immediately preceding the date of this certification; **or**,  
\_\_\_\_ Bidder is a resident vendor partnership, association, or corporation with at least eighty percent of ownership interest of bidder held by another entity that meets the applicable four year residency requirement; **or**,  
\_\_\_\_ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or**,
2. **Application is made for 2.5% vendor preference for the reason checked:**  
\_\_\_\_ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or**,
3. **Application is made for 2.5% vendor preference for the reason checked:**  
\_\_\_\_ Bidder is a nonresident vendor that employs a minimum of one hundred state residents, or a nonresident vendor which has an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia and employs a minimum of one hundred state residents, and for purposes of producing or distributing the commodities or completing the project which is the subject of the bidder's bid and continuously over the entire term of the project, on average at least seventy-five percent of the bidder's employees or the bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years and the vendor's bid; **or**,
4. **Application is made for 5% vendor preference for the reason checked:**  
\_\_\_\_ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or**,
5. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**  
\_\_\_\_ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or**,
6. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**  
\_\_\_\_ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.
7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with West Virginia Code §5A-3-59 and West Virginia Code of State Rules.**  
\_\_\_\_ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.
8. **Application is made for reciprocal preference.**  
\_\_\_\_ Bidder is a West Virginia resident and is requesting reciprocal preference to the extent that it applies.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) rescind the contract or purchase order; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

**Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.**

Bidder: \_\_\_\_\_

Signed: Amelia Jones - Fleet

Date: \_\_\_\_\_

Title: \_\_\_\_\_