



# Corporate Overview

Q3/2019

Speaker note: This corporate overview reflects the corporate performance as of August 31, 2019. It's published in Q3'19. This mirrors the Corporate Brochure, accessible from the FortiStore.

## Network Security Leader

Fortinet is among the **top 4** public cybersecurity companies in the world.

Its broad portfolio of solutions spans Network, Infrastructure, Cloud, and IoT Security.



**\$13.1B**  
Mkt Cap



**~\$1.8B - 2018**  
(revenue)



**415,000+**  
Customers



**4.9M+ Appliances**  
Shipments Worldwide  
(+30% units WW)

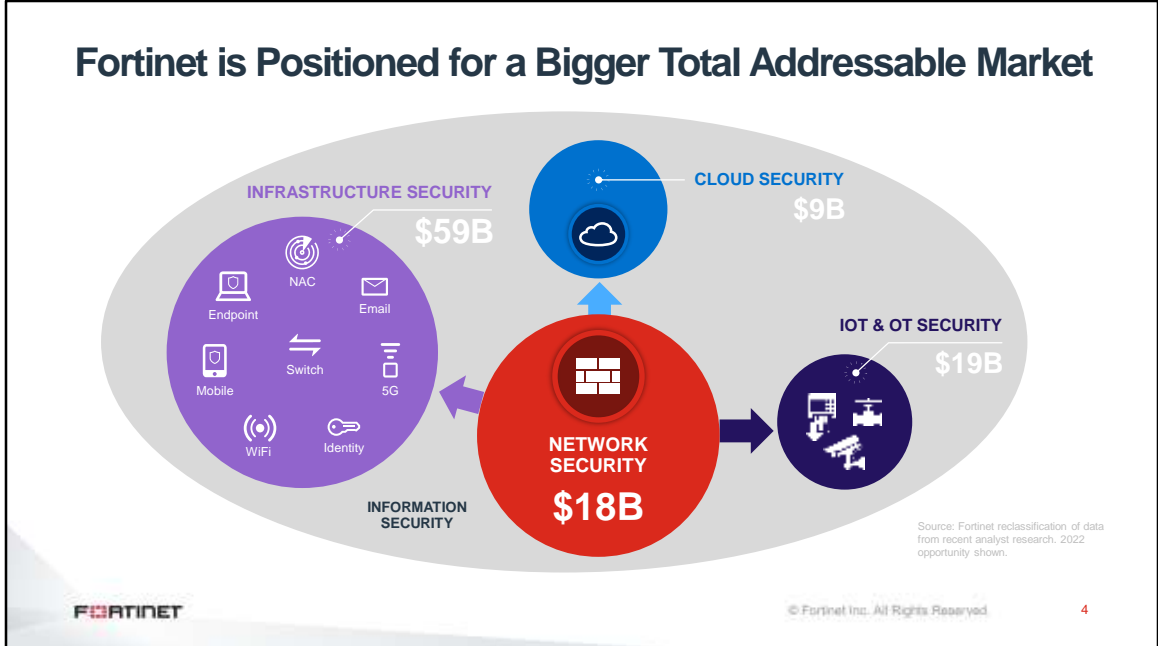
\* As of June 30, 2019

## 70% of F100 Are Fortinet Customers



And as you can see our customers include some of the largest companies in the world. In fact, 70% of the Fortune 100 are Fortinet Customers.

## Fortinet is Positioned for a Bigger Total Addressable Market



Our innovation and long term vision investment has enabled Fortinet to build leading technologies and products, covering a very large total addressable market.

**Fortinet's largest business is Network Security which includes many sub categories – Enterprise Firewall, UTM, VPN, IPS, SWG and more recently SD-WAN, with a relative projected size of \$18B**

In network security space, with our most recent announcements of FortiOS 6.2, FortiGate 100F and the FortiSPU SoC4, we continue to gain market share and be the leader both in unit shipment and revenue.

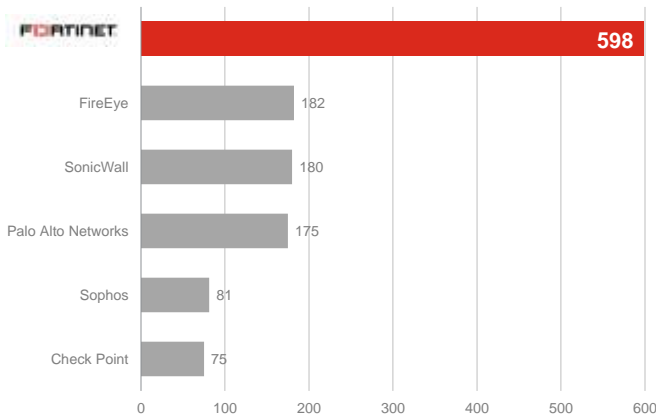
**However, we provide solutions across 3 other large security markets. These are:**

- **Infrastructure security (which includes endpoint, email and web application security, wired and wireless LAN, SIEM and more) with a relative projected size of \$59B**
  - **The Fortinet Security Fabric** together with Security Driven Networking will enable our customer and partner to meet the needs of today's 3<sup>rd</sup> generation infrastructure security

- **IOT/OT Security, with a relative projected market size of \$19B**
  - We continue to invest in both cloud and edge security solutions, and are leading the IoT and OT security going forward, including the connected car!
- **And of course, Cloud Security, including Private and Public Cloud, as well as Cloud Security Access Broker (CASB), with a relative projected size of \$9B**

## History of Leading Network Security Innovation

### Number of Patents



Based on information on USPTO website on 06/30/2019

FORTINET

### • #1 Security Innovator

- Competitor data based on patents issued as listed by the U.S. Patent and Trademark Office

598 U.S. Patents

30 International Patents

---

**628 Global Patents**

© Fortinet Inc. All Rights Reserved.

5

**The key to our success to date is our technology innovation. We have been awarded more than 598 U.S. patents (with many more still pending).**

- Innovation is one of the key culture of Fortinet, together with openness and teamwork.
- We continue to focus on innovation, and this innovation and long-term vision is one of the key differentiators compare with other competitors who more depends on acquisition to grow and meet customer need.

**As of June 30, 2019 we have been issued 628 global patents.**

## We Lead in Industry Recognition

						
	7	7	3	4	3	2
	9	2	4	0	0	3

# A Leader in Network Security

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Garner Magic Quadrant for Enterprise Network Firewalls, Adam Hill, Jeremy D'Holmes, Rajpreet Kaur, 4 October 2018  
 Garner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Garner research publications consist of the opinions of Garner's research organization and should not be construed as statements of fact. Garner disclaims all warranties, expressed or implied, with respect to its research, including any warranties of merchantability or fitness for a particular purpose.  
 Garner Peer Insights reviews constitute the subjective opinions of individual end-users based on their own experiences, and do not represent the views of Garner or its affiliates.  
 ©GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates, and is used herein with permission. All rights reserved.

FORTINET

Figure 1. Magic Quadrant for Unified Threat Management (SMB Distributed Enterprise)



Garner Magic Quadrant for Unified Threat Management (SMB Distributed Enterprise Firewalls), Rajpreet Kaur & Claudio Neves, 20 September 2018  
 Disclaimer: Garner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Garner research publications consist of the opinions of Garner's research organization and should not be construed as statements of fact. Garner disclaims all warranties, expressed or implied, with respect to its research, including any warranties of merchantability or fitness for a particular purpose.  
 ©GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates, and is used herein with permission. All rights reserved.

© Fortinet Inc. All Rights Reserved.

7

Garner provides analysis for many of these security markets. For more established markets they use the Magic Quadrant system to position each vendor.

- Niche Players are for entrants or smaller players who serve a very specific market segment
- Visionaries are players who show an interesting long term vision
- Challengers have established a good customer base
- Leaders have been executing will terms of both vision and customer base

Fortinet is recognized as meeting the enterprise requirements in more than 6 Gartner Magic Quadrants.

For Network Security the two main Magic Quadrants are Enterprise Firewalls (Includes NGFW) and Unified Threat Management (UTM- focused on SMB and Distributed Enterprise).

Fortinet is a LEADER in both these Magic Quadrants showing our vision and customer success for all use cases and segments.



## Unparalleled 3<sup>rd</sup> Party Validation

■ Recommended / Certified 
 □ Neutral 
 ■ Caution 
 ○ Undisclosed 
 X – did not participate

CERTIFICATION	Fortinet	Check Point	Cisco	Palo Alto Networks	Juniper	FireEye
NSS Next-Gen Firewall	■	■	○	■	○	x
NSS DC Security Gateway	■ ■	■	■	■	■	x
NSS Next-Gen IPS	■ ■	x	■	■	■	x
NSS DC IPS	■ ■	x	■	x	x	x
NSS Breach Detection	■	x	■	x	x	■
NSS Breach Prevention	■	■	■	■	■	x
NSS WAF	■	x	x	x	x	x
NSS Advanced Endpoint	■	■	■	○	x	x
NSS SD-WAN	■	x	x	x	x	x

**FORTINET**

Updated August 1, 2019

© Fortinet Inc. All Rights Reserved.

8

At the same time, we have earned more independent certifications than any competitor. Rigorous testing, with yourself and /or by a credible and experienced test lab is essential before making a major Network Security decision. Although vendors try to make data sheets accurate, and reflective of what they can do, every customer has their own environment and it's critical to ensure the solution you select will meet your specific requirements in production.

Fortinet has received more industry recognition and validation than any other vendor and we continue to maintain our lead with recommendations across 9 product categories, more than double compare with all other competitors

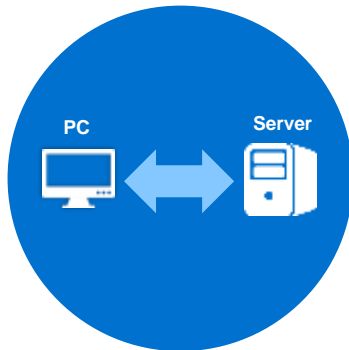
Tests such as NSS labs and other third party certifications we take part in, show the fact that we are committed to this process and committed to ensure that we can demonstrate to our customers that our price, performance and security efficacy can accurately address their unique requirements.

# 1st Generation Network Security : Connectivity

<2000

Network vs Security

Networking



Security



FORINNET

© Fortinet Inc. All Rights Reserved.

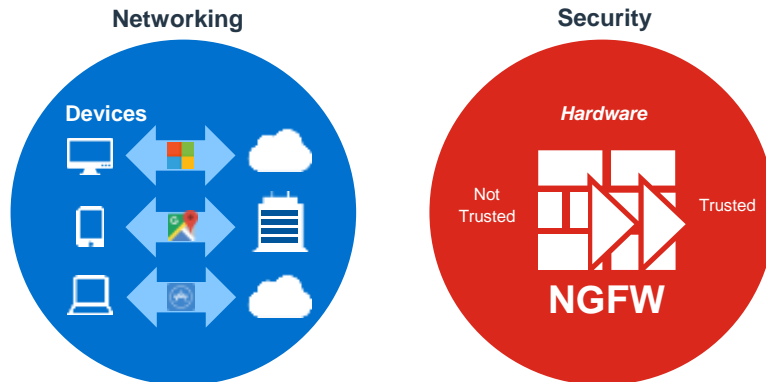
9

- In the last 30-40 years, The networking and cyber security space has been changed and evolved a lot. We all need to keep learning quick everyday to follow these changes.
- In 1980s and 1990s, network connection was few and speed was in the kbps, most traffic were simple text based, and the first generation network security FW was placed at the edge of Wide Area Network (WAN) and Local Area Network (LAN) to control the connectivity into the trusted LAN zone inside enterprise.

## 2nd Generation Network Security : Content

>2000

Network vs Security



FORTINET

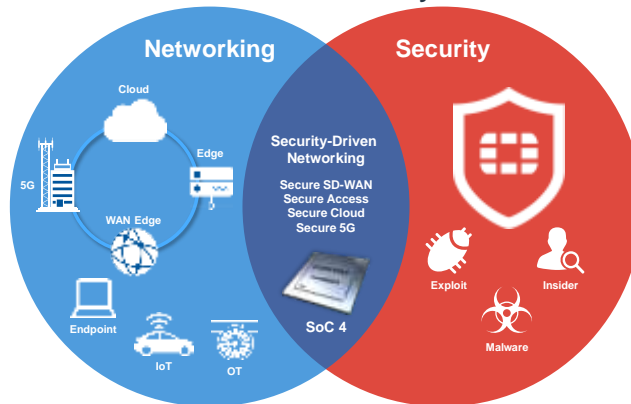
© Fortinet Inc. All Rights Reserved.

10

- About 20 years ago, servers and PC replaced most mainframes and terminal, network speed started to reach to Mbps and Gbps. Network traffic data and content became rich, active and executable. The connection based 1<sup>st</sup> gen FW could not stop the new content and agent based virus and intrusion attack.
- Fortinet was founded 19 years ago to pioneer and lead the new, next generation FW or UTM.
- This 2<sup>nd</sup> generation FW address the issue that most malware and intrusions were coming from permitted connections which the 1<sup>st</sup> gen FW cannot identify and stop.
- But Most NGFW still positioned at edge of WAN and LAN replacing the 1<sup>st</sup> gen FW, to secure the trusted zone but also had to inspect network content, which require 50 to 100 times more computing power compare with networking and switching to process the traffic. Resulting network security much slow and much more expensive. ASIC based FortiSPU, the Security Process Unit, is the key to solve the performance issue, and Fortinet is the only company using SPU to close the huge performance and cost gap between networking and security.

## 3rd Generation - Security-Driven Networking

**Now**  
Network vs Security



© Fortinet Inc. All Rights Reserved.

11

- In the last few years, mobile and cloud has started to replace PC and servers. Data is constantly traveling outside the company network, to mobile, to IoT, to edge and cloud. The trusted zone inside a company's LAN is no longer secure, and the border between inside LAN and outside WAN is disappearing.
- Valuable Data needs to be secured as it moves between networks, devices, users, and countries. Secure routing valuable data away from high risk and highly polluted area is vital.
- This is causing security and networking to converge, accelerating the third generation of Infrastructure security – **Security-Driven Networking**.
- Security is no longer like a moat protecting a castle or Fortress, but more like the immune system in the human body that moves around to block and neutralize threats.
- To have the best, strongest immune system, security and networking need to converge into the security-driven network. 10 years ago Fortinet led the integration of Security and Wi-Fi. Today we are leading the integration of Security

and SD-WAN, and going forward we will continue to lead the integration of Security and 5G.

## Fortinet Security Fabric

### Broad

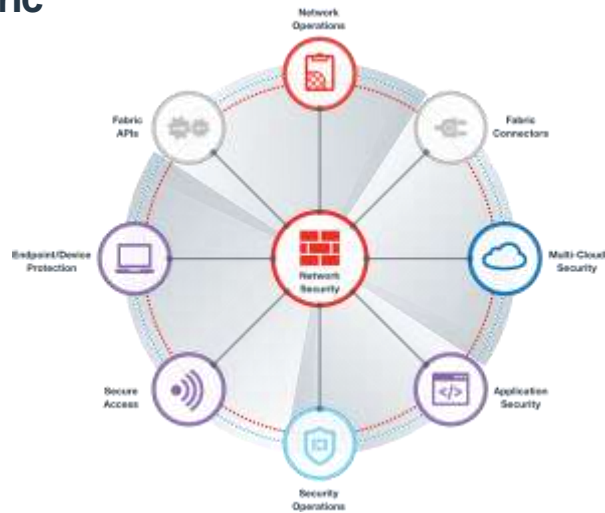
Visibility of the entire digital attack surface

### Integrated

AI-driven breach prevention across all devices, networks, and applications

### Automated

Operations, orchestration and response



FORTINET

© Fortinet Inc. All Rights Reserved.

12

**IN OUR CASE, THE SECURITY FABRIC IS THE RESULT OF ALMOST 20 YEARS OF INNOVATION, ORGANICALLY BUILT FROM THE GROUND UP.**

Fortinet build 3 layers of architecture for broad, integrated and automated cybersecurity solutions.

The core in the middle is our FortiGate system with FortiOS and FortiSPU chip, offering more functions cover both security and networking than any other competitors, and archived the best performance and cost leverage our FortiSPU ASIC chips.

### IT IS BROAD -

- **PROVIDING VISIBILITY AND PROTECTION ACROSS THE ENTIRE CONNECTED DIGITAL ATTACK SURFACE TO PROTECT YOUR DATA- FROM THE END POINT AND ACCESS LAYERS, THROUGH THE NETWORK AND APPLICATIONS, ALL THE WAY OUT TO CLOUD AND IOT.**
- **INCLUDING OUR ROBUST ECOSYSTEM OF INDUSTRY PARTNERS INCLUDING MAJOR INFRASTRUCTURE VENDORS LIKE IBM, INTEL, MICROSOFT, AWS AND GOOGLE**

### **IT IS INTEGRATED –**

- Expanding to second layer is our Fabric architecture, with more than 20 product family integrated cover the whole infrastructure security to meet the 3<sup>rd</sup> generation cyber security needs. Most of these 20+ products are internal innovated and developed, integrate well together, compare with other competitors who has to acquire different company and product, which has hard time to integrate. And Integration is the key for automation.
- **ENCOMPASSING ADVANCED TECHNOLOGIES, LIKE THOSE FOR DETECTION OF ZERO DAY AND UNKNOWN THREATS, THAT CAN BE APPLIED ANYWHERE ACROSS THE FABRIC**

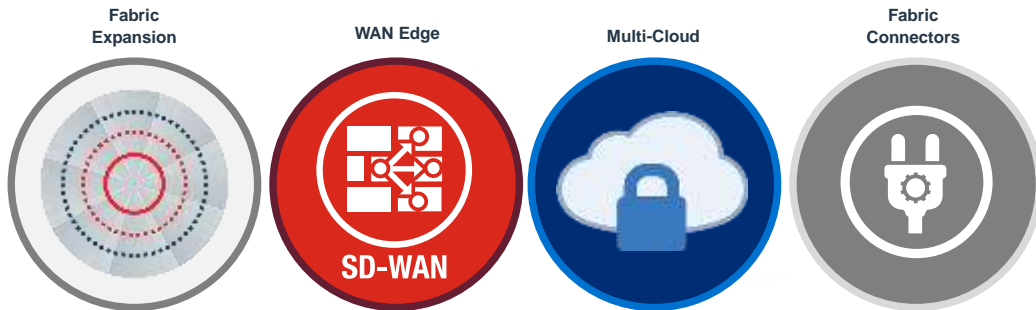
### **IT IS AUTOMATED-**

- **FOR FAST RESPONSE TO ISSUES REQUIRING REMEDIATION, WHICH NEEDS TO BE APPLIED AS QUICKLY AS POSSIBLE, AS WELL AS CONTINUOUS TRUST ASSESSMENTS THAT HELP KEEP YOUR SECURITY POSTURE CURRENT.**
- The big outside circle is Fabric partner eco-system with 57 Fabric ready partners like Symantec, offer the industry best visibility of the entire digital attack surface and full data protections.

## FortiOS 6.2 has 300+ New Features



### Security Fabric Evolution Continues



FORTINET

© Fortinet Inc. All Rights Reserved.

13

- At Accelerate, we announced the new FortiOS 6.2 with 300+ new features.
- FortiOS is the most broadly adopted operating system globally with close 400,000 customers worldwide, and about 5 million FortiGate deployed since company founded 19 years ago.
- FortiOS 6.2 includes many enhancements to our SD-WAN capabilities, Security Fabric, AI and many others.



# Fortinet Fabric-Ready Technology Alliances

**SDN/NFV & VIRTUALIZATION**

**CLOUD**

**ENDPOINT**

**MANAGEMENT**

**IDENTITY MGMT.**

**IoT/OT/NAC**

**SIEM**

Fortinet Fabric-Ready

Fortinet

Snapshot in 2019; new partners added continuously.

© Fortinet Inc. All Rights Reserved.

14

The Fabric-Ready technology alliance program has experienced massive program growth, since it was launched 3 years back with an initial set of 12 partners. Since then, the program has grown to 60+ partners as of Q3 2019, which is 5 times the initial number, with new partnerships being added every quarter. Key new Fabric-Ready partners over the last year include Google Cloud, IBM Security, VMware and ServiceNow.

This slide illustrates the broad landscape of alliances we have built, categorized by the API areas that these joint solutions are focused in. You can see that there is a nice, healthy mix of companies. There are large, industry-leading companies such as IBM Security, Google Cloud, AWS, Microsoft, etc. but we also have smaller, highly innovative companies that are very relevant to many customer and market needs. These alliances provide comprehensive ecosystem coverage of key security areas.

# Creating The Cybersecurity Workforce Of The Future

Fortinet Network Security Expert Institute



FORTINET

© Fortinet Inc. All Rights Reserved.

15

- We are partnering with 172 university in 63 countries, and reached 230,000+ certifications today.

**To ensure that customers and the broader industry are able to take full advantage of the Security Fabric approach, Fortinet has established a leading training and certification program called the Network Security Expert (NSE) program. To date, 230,000+ NSE certifications have been issued.**

In the last 5 years, Fortinet has been building the biggest WW cybersecurity training program the Network Security Expert or NSE. The NSE Institute offer deep and broad training for our partners, customers, employees and the industry as a whole.

**The program has 8 levels.**

**NSE 1 and 2 are open to everyone through [training.fortinet.com](https://training.fortinet.com).**

**NSE 1 covers The Threat Landscape** and the problems facing organizations and individuals.

**NSE 2 The Evolution of Cybersecurity**, covers the types of security products that have been created by security vendors to address those problems.

**Level 3 provides product level training on the Fortinet offerings**  
**At Level 4 the more detailed training starts, focused on FortiGate and FortiOS**  
**Level 5 continues with technical training on management and analytics offerings**  
**Level 6 does the same for each of the products within the Fabric solution areas**  
**Level 7 is technical training on multiple products working together as a solution,**  
**And Network Security Expert Level 8 covers advanced architecture, trouble**  
**shooting, issue resolution, API customization and more as both a written and then**  
**practical test**

**In addition to Level 1 and 2 offered free to everybody, Fortinet partners are entitled to all available online training at no charge...although live training is also available.**

**Finally Fortinet is introducing new “Bite Sized” Fast Track training modules, designed as incremental, 2 hour update sessions to cover the very latest advances in each area. It is also “Train the trainer” orientated.**

The image shows the Fortinet logo centered on a dark blue background with a radial pattern of lines. The logo consists of the word "FORTINET" in a white, sans-serif font. The letter "O" is replaced by a red square containing a white grid pattern.