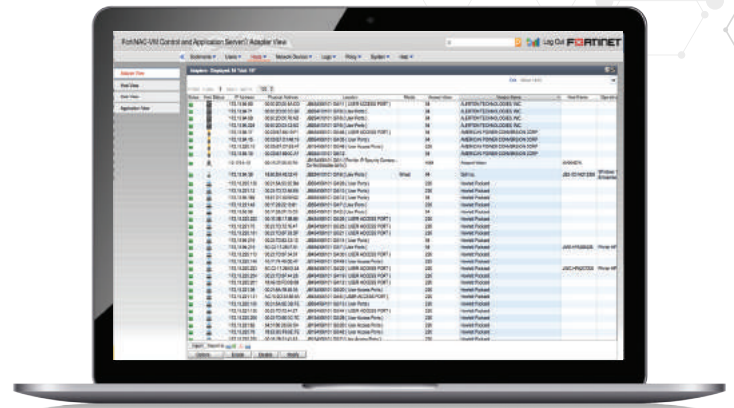


# FortiNAC™

FortiNAC 500C, 550C, 600C, 650C, 700C, 1000C, 2000C, VM and Licenses

FortiNAC is Fortinet's network access control solution that enhances the Security Fabric. FortiNAC provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events.



## Visibility across the network for every device, and user

FortiNAC provides detailed profiling of even headless devices on your network using multiple information and behavior sources to accurately identify what is on your network.



## Extend Control of the Network to Third-Party Products

FortiNAC can implement segmentation policies and change configurations on switches and wireless products from more than 70 vendors. Extend the reach of the Security Fabric in heterogeneous environments.



## Automated Responsiveness

React to events in your network in seconds to contain threats before they spread. FortiNAC offers a broad and customizable set of automation policies that can instantly trigger configuration changes when the targeted behavior is observed.



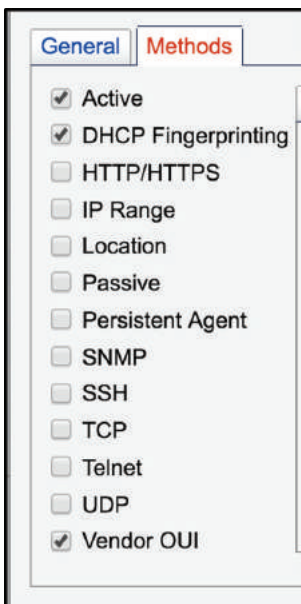
## Highlights

- Agentless scanning of network for detection and classification of devices
- Create an inventory of all devices on the network
- Event reporting to SIEM with detailed contextual data to reduce investigation time
- Assess risk of every endpoint on the network
- Automate onboarding process for large number of endpoints, users and guests
- Enforce dynamic network access control and enable network segmentation
- Reduce containment time from days to seconds
- Multiple canned reports for network reporting, compliance, and analysis

## FEATURES

### Device Visibility

Fundamental to the security of a constantly changing network is an understanding of its makeup. FortiNAC scans your network using agentless methods to discover every user, application and device. With up to 13 different techniques, FortiNAC can then profile each element based on observed characteristics and behavior, as well as noting the need for software updates to patch vulnerabilities. The user is also identified and the appropriate role-based network access policies are implemented within FortiNAC to protect critical data and sensitive assets while ensuring compliance with internal, industry and government regulations and mandates.



FortiNAC profiling methods for device identification

### Dynamic Network Control

Once devices and users are identified, FortiNAC enables detailed segmentation of the network to enable devices and users access to necessary resources while blocking non-related access. FortiNAC uses dynamic role-based network access control to logically create network segments by grouping applications and like data together to limit access to specific group of users. In this manner, if a device is compromised, its ability to travel in the network and attack other assets will be limited.

Ensuring the integrity of devices before they connect to the network minimizes risk and the possible spread of malware. FortiNAC validates a device's configuration as it attempts to join the network. If the configuration is found to be non-compliant, the device can be handled appropriately such as by an isolated or limited access VLAN.

Furthermore, FortiNAC will monitor the network on an ongoing basis and can adjust that level of access based on changes in behavior.

### Instant, Automated Response

With FortiNAC, once a compromised or vulnerable endpoint is identified, FortiNAC triggers an automated response to contain the endpoint in real time. Containment actions can include termination of connection, restrictions on network access, isolation into quarantine VLAN, and a range of notification actions. Automating this entire process essentially bridges the gap between the SOC and the NOC, and reduces the containment time from days to seconds.

# INTEGRATION

FortiNAC-VM Control and Application Server Adapter View

Bookmarks Users Hosts Network Devices Logs Policy System Help

Adapter View

Adapters - Displayed: 84 Total: 197

Host View

User View

Application View

Status	Host Status	IP Address	Physical Address	Location	Media	Access Value	Vendor Name	Host Name	Operating
		172.16.94.80	00:60:2D:00:8A:DD	JB4S4506101 G14/11 ( USER ACCESS PORT )		94	ALERTON TECHNOLOGIES, INC.		
		172.16.94.71	00:60:2D:00:CC:BF	JB2S4510101 G17/9 ( User Ports )		94	ALERTON TECHNOLOGIES, INC.		
		172.16.94.69	00:60:2D:00:F0:AD	JB2S4510101 G17/9 ( User Ports )		94	ALERTON TECHNOLOGIES, INC.		
		172.16.95.224	00:60:2D:03:C2:5C	JB2S4510101 G17/9 ( User Ports )		94	ALERTON TECHNOLOGIES, INC.		
		172.16.94.17	00:C0:B7:6A:19:F1	JB4S4506101 G15/46 ( USER ACCESS PORT )		94	AMERICAN POWER CONVERSION CORP		
		172.16.94.15	00:C0:B7:D1:A8:19	JB5S4506101 G14/35 ( User Ports )		94	AMERICAN POWER CONVERSION CORP		
		172.16.220.10	00:C0:B7:CF:B3:47	JB1S4506101 G15/46 ( User Access Ports )		220	AMERICAN POWER CONVERSION CORP		
		172.16.94.10	00:C0:B7:69:9C:A7	JB3S4510101 G16/12		94	AMERICAN POWER CONVERSION CORP		
		10.172.4.10	00:1A:07:06:43:7A	JB1S4506101 G15/1 ( Port for IP Security Camera - Do-Not Enable dot1x )		4004	Arecont Vision	AV06437A	
		172.16.94.39	18:66:DA:43:02:41	JB2S4510101 G17/8 ( User Ports )	Wired	94	Dell Inc.	JB2-ID01A212308	Windows Enterprise
		172.16.220.136	00:21:5A:95:2C:BA	JB5S4506101 G14/26 ( User Ports )		220	Hewlett Packard		
		172.16.221.12	00:23:7D:72:A6:E8	JB5S4506101 G14/13 ( User Ports )		220	Hewlett Packard		
		172.16.95.164	78:E7:D1:A2:89:02	JB5S4506101 G14/12 ( User Ports )		94	Hewlett Packard		
		172.16.221.48	00:1F:29:22:16:81	JB5S4506101 G14/7 ( User Ports )		220	Hewlett Packard		
		172.16.95.96	00:1F:29:2F:10:C5	JB5S4506101 G14/2 ( User Ports )		94	Hewlett Packard		
		172.16.220.222	00:1E:0B:17:88:86	JB4S4506101 G15/26 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.221.75	00:23:7D:72:76:47	JB4S4506101 G15/25 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.220.181	00:23:7D:6F:33:DF	JB4S4506101 G15/21 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.94.216	00:23:7D:82:C3:12	JB5S4506101 G13/14 ( User Ports )		94	Hewlett Packard		
		172.16.94.219	6C:C2:17:28:07:51	JB5S4506101 G13/7 ( User Ports )		94	Hewlett Packard	JMS-HPA206228	Printer HP
		172.16.220.113	00:23:7D:6F:54:91	JB4S4506101 G14/30 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.220.148	10:1F:74:49:C6:47	JB1S4506101 G14/45 ( User Access Ports )		220	Hewlett Packard		
		172.16.220.223	6C:C2:17:26:6D:24	JB1S4506101 G14/22 ( USER ACCESS PORT )		220	Hewlett Packard	JWC-HPA207208	Printer HP
		172.16.220.254	00:23:7D:6F:44:2B	JB4S4506101 G14/19 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.220.201	18:A9:05:FD:9B:69	JB4S4506101 G14/12 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.221.39	00:21:5A:7B:40:35	JB1S4506101 G14/20 ( User Access Ports )		220	Hewlett Packard		
		172.16.221.131	AC:16:2D:3A:80:9A	JB4S4506101 G14/6 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.220.106	00:21:5A:8E:DB:FE	JB5S4506101 G12/13 ( User Ports )		220	Hewlett Packard		
		172.16.221.138	00:23:7D:72:44:27	JB4S4506101 G13/44 ( USER ACCESS PORT )		220	Hewlett Packard		
		172.16.220.208	00:23:7D:6E:3C:7C	JB1S4506101 G12/26 ( User Access Ports )		220	Hewlett Packard		
		172.16.221.62	64:51:06:25:EA:C4	JB1S4506101 G12/20 ( User Access Ports )		220	Hewlett Packard		
		172.16.220.78	78:E3:95:F9:BE:FE	JB1S4506101 G13/42 ( User Access Ports )		220	Hewlett Packard		
		172.16.220.220	00:1B:78:25:43:A3	JB1S4506101 G12/7 ( User Access Ports )		220	Hewlett Packard		

Import Export to: Options Enable Disable Modify

FortiNAC Adapter view

Extensive integration with desktop security software, directories, network infrastructure and third-party security systems provides unparalleled visibility and control across the network environment. The FortiNAC family integrates with\*:



## Network Infrastructure

Aerohive, Adtran, Alcatel-Lucent, Allied Telesis, Alteon, Apple, APC, Avaya, Brocade/Foundry Networks/Ruckus, Cisco/Meraki, SonicWall, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Culubris/3Com/Aruba, Huawei Technology, Intel, Juniper, Riverbed/Xirrus

## Security Infrastructure

CheckPoint, Cyphort, Cisco/SourceFire, FireEye, Juniper/Netscreen, Qualys, Sonicwall, Tenable

## Authentication & Directory Services

RADIUS — Microsoft IAS, Cisco ACS, Free RADIUS  
LDAP — Microsoft Active Directory, OpenLDAP, Google SSO

## Operating Systems

Microsoft Windows, Apple MAC OSX and iOS, Linux, Android

## Endpoint Security Applications

Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Kaspersky, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Webroot SpySweeper, Vexira, Zone Alarm

\* FortiNAC can be integrated with other vendors and technologies in addition to those listed here. This list represents integrations that have been validated in both test lab and production network environments.

## DEPLOYMENT OPTIONS

### Easy Deployment

FortiNAC is a flexible and scalable solution that spans from mid-enterprise to very large enterprise deployments. There are four elements to the FortiNAC solution:

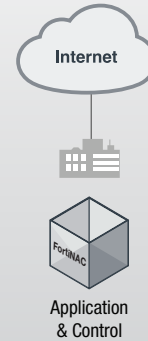
- **Application** (required)
- **Control** (required)
- **Management** (optional)
- **Reporting and Analytics** (optional)

The Application provides the visibility and the Control provides the configuration capabilities and automated responsiveness features. The Management portion enables the sharing of concurrent users across a multi-server deployment. The Reporting and Analytics provides the reporting and analytics based on the information gathered from the network.

FortiNAC can be deployed in virtual machines (VMware or Hyper-V) or on hardware appliances. The Application and Control Servers

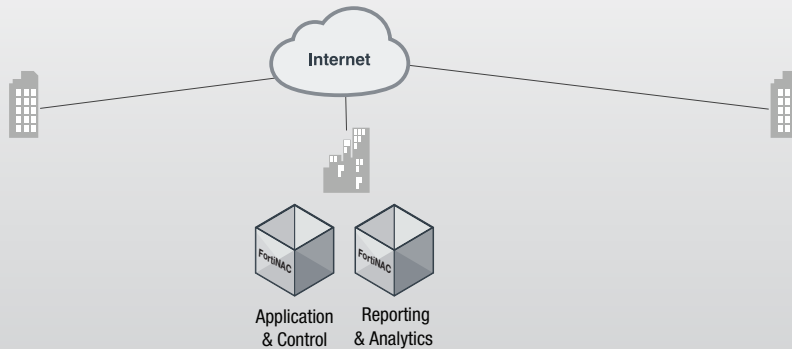
can be deployed in a variety of sizes, depending on the number of ports they need to support.

#### Deployment Examples – Small



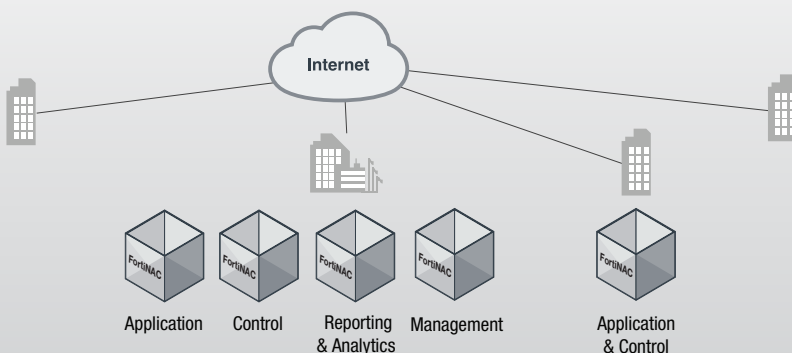
For 250–15,000 Total Ports + Max Wireless Devices

#### Deployment Examples – Medium



For 12,000–15,000 Total Ports + Max Wireless Devices

#### Deployment Examples – Large



For 20,000–35,000 Total Ports + Max Wireless Devices

## LICENSING

### FortiNAC Licensing

FortiNAC offers flexible deployment options based on the level of coverage and functionality desired.

- The **Basic license level** provides easy, one-step IoT security solution to close pressing endpoint security gaps by seeing all endpoint devices on the network, automating authorization, and enabling network lockdown. The Basic license level is appropriate for organizations that need to secure IoT and headless devices, and enable network lockdown, but do not require more advanced user/network controls or automated threat response.
- The **Plus license level** builds on all the functionality of Basic with more advanced Network Access Controls and automated provisioning for users, guests, and devices as well as reporting and analytics. The reporting and analytics can greatly assist in providing audit documentation of compliance. The Plus license level is appropriate for organizations that want complete endpoint visibility and a granular control, but do not require automated threat response.
- The **Pro license level** provides the ultimate in visibility, control and response. Pro license offers real-time endpoint visibility, comprehensive access control, and automated threat response and delivers contextual information with triaged alerts. The Pro license level is appropriate for organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat response.

FortiNAC LICENSE TYPES		BASIC	PLUS	PRO
Visibility	Network	Network Discovery	•	•
		Persistent Agent	•	•
	User	Domain Authorization	•	•
		Captive Portal	•	•
		Rogue Identification	•	•
		Captive Portal	•	•
	Endpoint	Device Profiling & Classification	•	•
		Domain Authorization	•	•
		MDM Integration	•	•
		Network Access Policies	•	•
Automation / Control		BYOD / Onboarding	•	•
		Guest Management	•	•
		IoT Onboarding with Sponsor	•	•
		Endpoint Compliance	•	•
		Rogue Device Detection & Restriction	•	•
		Web & Firewall Single Sign On	•	•
		Firewall Segmentation	•	•
		Event Correlation		•
Incident Response		Extensible Actions & Audit Trail		•
		Alert Criticality & Routing		•
		Guided Triage Workflows		•
		Inbound Security Events		•
Integrations		Outbound Security Events	•	•
		REST API	•	•
Reporting		Live Reporting	•	•
		Historical Analytics	•	•

## SPECIFICATIONS

	FNC-M-550C	FNC-CA-600C	FNC-C/A-1000C	FNC-R-650C	FNC-CA-500C
System					
CPU	Intel Xeon Silver 4110 2.1 G, 8C/16T, 9.6 GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400 (Qty 2)			Intel Xeon E3-1220 v5 3.0 GHz, 8M cache, 4C/4T, Turbo (Qty 1)	
Memory	8 GB RDIMM, 2666 MT/s, Single Rank (Qty 4)			4 GB UDIMM, 2400 MT/s, ECC (Qty 3)	
Hard Disk	1TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)			1TB 7.2K RPM SATA 6 Gbps 3.5in Hot-plug Hard Drive RAID1 (Qty 2)	
Optical Drive	None Required			DVD ROM SATA Internal (Qty 1)	
BMC	iDRAC9 Express, integrated (Qty 1)			iDRAC8 Express (Qty 1)	
Network Interface	Broadcom 5720 QuadPort 4x 1 GB Ethernet, RJ45			4x 10/100/1000 Ethernet, RJ45	
RAID Card	PERC H330 Integrated RAID Controller (Qty 1)			PERC H330 Integrated RAID Controller (Qty 1)	
RAID Configuration	RAID 1			RAID 1	
Console Access	None			Front LCD Panel	
Form Factor	1U Rack mountable			1U Rack mountable	
Dimensions					
Height x Width x Length (inches)	1.68 x 18.9 x 29.73			1.68 x 17.08 x 24.60	
Height x Width x Length (mm)	42.8 x 482.4 x 755.12			42.8 x 434.0 x 625.0	
Weight	43.056 lbs (19.76 kg)			40.96 lbs (18.58 kg)	
Environment					
Power Supply	Dual 550W Hot Plug Power Supply			Dual 350W Hot Plug Power Supplies	
Input Power	100-240V AC Autoranging			100-240V AC Autoranging	
Input Current	6.25 A			3.0 A	
Cooling	7 fans			4 fans	
Panel Display	No LCD			20 Char LCD	
Heat Dissipation	2559 BTU/hr			1357.1 BTU/hr	
Operation Temperature Range	50–95°F (10–35°C)			50–95°F (10–35°C)	
Storage Temperature Range	-40–149°F (-40–65°C)			-40–149°F (-40–65°C)	
Humidity (Operating)	10–80% non-condensing			10–80% non-condensing	
Humidity (Non-operating)	5–95% non-condensing			5–95% non-condensing	
Certification					
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), European Union (CE).				
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), European Union (CE).				
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).				



## SPECIFICATIONS

	FNC-CA-700C	FNC-C/A-2000C
System		
CPU	Intel Xeon Gold 6132 2.6 G, 14C/28T, 10.4 GT/s, 19M Cache, Turbo, HT (140W) DDR4-2666 (Qty 2)	
Memory	8 GB RDIMM, 2666 MT/s, Single Rank (Qty 12)	
Hard Disk	600 GB 15K RPM SAS 12 Gbps 2.5in Hot-plug Hard Drive (Qty 2)	
Optical Drive	None required	
BMC	iDRAC9 Express, integrated (Qty 1)	
Network Interface	Broadcom 5720 QuadPort 4x 1 GB Ethernet, RJ45 (Qty 1)	
RAID Card	PERC H730P+ RAID Controller, 2 GB Cache (Qty 1)	
RAID Configuration	RAID 1	
Console Access	No LCD Panel	
Form Factor	1U Rack mountable	
Dimensions		
Height x Width x Length (inches)	1.68 x 18.9 x 29.73	
Height x Width x Length (mm)	42.8 x 482.4 x 755.12	
Weight	43.056 lbs (19.76 kg)	40.96 lbs (18.58 kg)
Environment		
Power Supply	Dual 750W AC power supplies	
Input Power	100–240V AC, Autoranging	
Input Current	6.25 A	
Cooling	7 fans	
Panel Display	No LCD	
Heat Dissipation	2559 BTU/hr	
Operation Temperature Range	50–95°F (10–35°C)	
Storage Temperature Range	-40–149°F (-40–65°C)	
Humidity (Operating)	10–80% non-condensing	
Humidity (Non-operating)	5–95% non-condensing	
Certification		
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), European Union (CE).	
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), European Union (CE).	
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).	

## HARDWARE SERVER SIZING

HARDWARE			
Hardware Server	Type	Target Environment	Capacity
FortiNAC-CA-500C	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 2,000 ports in the network*
FortiNAC-CA-600C	High Performance Control and Application Server	Medium Environments	Manages up to 7,500 ports in the network*
FortiNAC-R-650C	On-Premises Analytics Server	N/A	N/A
FortiNAC-CA-700C	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 15,000 ports in the network*
FortiNAC-C-1000C	High-Performance Appliance Pair (Separate Control Server and Application Server)	Large Environments with many Persistent Agents	Manages up to 20,000 ports in the network*
FortiNAC-C-2000C	Ultra High Performance Control / Application Server	Very Large Environments with many Persistent Agents	Manages up to 30,000 ports in the network*
FortiNAC-A-2000C			
FortiNAC-M-550C	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Unlimited

\* "Ports" in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

### 軟體標VM版本

## VIRTUAL SERVER SIZING

VMware and Hyper-V			
Virtual Server	Type	Target Environment	Capacity
FortiNAC Control and Application VM	Ultra High Performance Control and Application Server	Large Environments with many Persistent Agents	Manages up to 15,000 ports in the network*
FortiNAC Application VM	Ultra High Application Server	Large Environments with many Persistent Agents	Manages up to 30,000 ports in the network*
FortiNAC Control VM	Ultra High Performance Control Server	Large Environments with many Persistent Agents	Manages up to 30,000 ports in the network*
FortiNAC Manager VM	Management Server (Provides centralized management when multiple Servers are deployed)	Multi-site Environments with multiple Servers	Unlimited
FortiNAC Reporting VM	FortiNAC VMware On-Premises Analytics Server	N/A	N/A

\* "Ports" in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

## VM SERVER RESOURCE SIZING

Network Size	Target Environment	SKU	CPU	Memory	Disk
Up to 2,000 ports in the network*	Small Environment	FNC-CA-VM	Intel Xeon E3-1220 v5 3.0 GHz, 8M Cache, 4C/4T, turbo (Qty 2)	4 GB UDIMM, 2133 MT/s, ECC (Qty 3)	500 GB 7.2K RPM SATA 3 Gbps 3.5in Hot-plug Hard Drive RAID1 (Qty 2)
Up to 7,500 ports in the network*	Medium Environment	FNC-CA-VM	Intel Xeon E5-2620 v3 2.4 GHz, 15M Cache, 8.00 GT/s	4 GB RDIMM, 2133 MT/s, Single Rank, x8 Data Width (Qty 4)	1 TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
Up to 15,000 ports in the network*	Large Environment	FNC-CA-VM	Intel Xeon E5-2697 v3 2.6 GHz, 35M Cache, 9.60 GT/s QPI, Turbo, HT, 14C/28T (Qty 2)	8 GB RDIMM, 2133 MT/s, Dual Rank, x8 Data Width (Qty 8)	600 GB 15K RPM SAS 12 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
Up to 20,000 ports in the network*	Large Environment	FNC-C-VM	Intel Xeon E5-2620 v3 2.4 GHz, 15M Cache, 8.00 GT/s	4 GB RDIMM, 2133 MT/s, Single Rank, x8 Data Width (Qty 4)	1 TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
		FNC-A-VM	Intel Xeon E5-2620 v3 2.4 GHz, 15M Cache, 8.00 GT/s	4 GB RDIMM, 2133 MT/s, Single Rank, x8 Data Width (Qty 4)	1 TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
Up to 30,000 ports in the network*	Large Environment	FNC-C-VM	Intel Xeon E5-2697 v3 2.6 GHz, 35M Cache, 9.60 GT/s QPI, Turbo, HT, 14C/28T (Qty 2)	8 GB RDIMM, 2133 MT/s, Dual Rank, x8 Data Width (Qty 8)	600 GB 15K RPM SAS 12 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
		FNC-A-VM	Intel Xeon E5-2697 v3 2.6 GHz, 35M Cache, 9.60 GT/s QPI, Turbo, HT, 14C/28T (Qty 2)	8 GB RDIMM, 2133 MT/s, Dual Rank, x8 Data Width (Qty 8)	600 GB 15K RPM SAS 12 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
Unlimited	Large Environment	FNC-M-VM	Intel Xeon E5-2620 v3 2.4 GHz, 15M Cache, 8.00 GT/s	4 GB RDIMM, 2133 MT/s, Single Rank, x8 Data Width (Qty 4)	1 TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
N/A	N/A	FNC-R-VM	Intel Xeon E5-2620 v3 2.4 GHz, 15M Cache, 8.00 GT/s	4 GB RDIMM, 2133 MT/s, Single Rank, x8 Data Width (Qty 4)	1 TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)

\* "Ports" in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.



## ORDER INFORMATION

Appliances		
FortiNAC-CA-500C	FNC-CA-500C	FortiNAC 500, Network Control and Application Server with RAID and Redundant Power Supplies
FortiNAC-CA-600C	FNC-CA-600C	FortiNAC 600, High Performance Network Control and Application Server with RAID and Redundant Power Supplies
FortiNAC-CA-700C	FNC-CA-700C	FortiNAC 700, Ultra High Performance Network Control and Application Server with RAID and Redundant Power Supplies
FortiNAC-C-1000C	FNC-C-1000C	FortiNAC C1000C, High Performance Control Server with RAID and Redundant Power Supplies
FortiNAC-A-1000C	FNC-A-1000C	FortiNAC A1000C, High Performance Application Server with RAID and Redundant Power Supplies
FortiNAC-C-2000C	FNC-C-2000C	FortiNAC 2000, Ultra High Performance Control Server with RAID and Redundant Power Supplies
FortiNAC-A-2000C	FNC-A-2000C	FortiNAC 2000, Ultra High Performance Application Server with RAID and Redundant Power Supplies
FortiNAC-M-550C	FNC-M-550C	FortiNAC Manager 550, Network Manager with RAID and Redundant Power Supplies
FortiNAC-R-650C	FNC-R-650C	FortiNAC Reporting and Analytics Server Appliance with Redundant Power Supplies
Virtual Machines		
FortiNAC Control and Application VM	FNC-CA-VM	FortiNAC Control and Application VM Server (VMware or Hyper-V)
FortiNAC Application VM	FNC-A-VM	FortiNAC Application VM Server (VMware or Hyper-V)
FortiNAC Control VM	FNC-C-VM	FortiNAC Control VM Server (VMware or Hyper-V)
FortiNAC Manager VM	FNC-M-VM	FortiNAC Manager VM Server (VMware or Hyper-V)
FortiNAC Reporting VM	FNC-R-VM	FortiNAC Reporting and Analytics VM Server (VMware or Hyper-V)
Licenses		
FortiNAC Base License	LIC-FNAC-BASE-100	FortiNAC BASE License for 100 concurrent endpoint devices
FortiNAC Plus License	LIC-FNAC-PLUS-100	FortiNAC PLUS License for 100 concurrent endpoint devices
FortiNAC Pro License	LIC-FNAC-PRO-100	FortiNAC PRO License for 100 concurrent endpoint devices
FortiNAC Base-Plus Upgrade License	FNC-LIC-BASE-UPG-100	BASE to PLUS License Upgrade for 100 concurrent endpoint devices
FortiNAC Plus-Pro Upgrade License	FNC-LIC-PLUS-UPG-100	PLUS to PRO License Upgrade for 100 concurrent endpoint devices
FortiNAC Base-Pro Upgrade License	FNC-LIC-PRO-UPG-100	BASE to PRO License Upgrade for 100 concurrent endpoint devices
Training		
FortiNAC Classroom Training	FT-BNS-TR	One seat in a 3-day Administration and Operations training class. Classes are held in Concord NH and at regional locations.
FortiNAC Online Training	FT-BS-TWB	One seat in a 3-session (total 12 hours) web-based Administration and Operation overview training. Remote sessions are delivered online.



GLOBAL HEADQUARTERS  
Fortinet Inc.  
899 KIFER ROAD  
Sunnyvale, CA 94086  
United States  
Tel: +1.408.235.7700  
[www.fortinet.com/sales](http://www.fortinet.com/sales)

EMEA SALES OFFICE  
905 rue Albert Einstein  
06560 Valbonne  
France  
Tel: +33.4.8987.0500

APAC SALES OFFICE  
8 Temasek Boulevard  
#12-01 Suntec Tower Three  
Singapore 038988  
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE  
Sawgrass Lakes Center  
13450 W. Sunrise Blvd., Suite 430  
Sunrise, FL 33323  
United States  
Tel: +1.954.368.9990

產品	效能	Description	作業版本
Fortinet 標準版資安防護系統 一年授權	防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN, SSL VPN, SLB(主機負載平衡) 及 無線網路控制器 (Wireless Controller)	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 標準版資安防護系統 防護升級模組 一年授權	防護升級模組 一年授權		
Fortinet 高階版資安防護系統 一年授權	高階版防護系統 一年授權	提供防火牆控管存取政策，使用者身份辨識，IPSEC VPN, SSL VPN, SLB(主機負載平衡) , 無線網路控制器 (Wireless Controller) , 入侵防禦，應用程式式控管，防毒，不當網頁過濾，防垃圾郵件	Vmware Hyper-V Citrix Xen OpenXen KVM AWS
Fortinet 高階版資安防護系統 防護升級模組 一年授權	高階版資安防護系統 防護升級模組 一年授權		
FMG-VM-Base Fortinet 集中管理系統	集中管理系統 10 台設備	Fortinet 防火牆管理，設定和集中派送（政策，資安防禦資料庫）的中央管理系統，支援 10 台設備	Vmware Hyper-V AWS
FMG-VM-10-UG Fortinet 集中管理系統	集中管理平台設備 數量升級 - 10 台設備		
FAZ-VM-BASE Fortinet 集中日誌報表系統	集中日誌報表系統	Fortinet 防火牆的集中日誌報表管理系統	Vmware Hyper-V AWS
FAZ-VM-GB1 Fortinet 集中日誌報表系統 紀錄數量升級 - 1 GB/Day	集中日誌報表系統 紀錄數量升級 - 1 GB/Day		
FSA-VM Fortinet 先進威脅防護系統 (ATP)	先進威脅防護系統 (ATP)	即時執行沙箱檢測，提供虛擬的運行環境來分析高風險或可疑的程式，研判威脅完整的生命週期，協助用戶智慧地立即偵測出既存與新興的 網路威脅。	Vmware
FWB-Base Fortinet 網站應用程式式防火牆(WAF) 25Mbps	網站應用程式式防火牆(WAF) 25Mbps	提供網站應用程式式防火牆功能（WAF），網頁防置換，網頁自動備份及回復等功能	Vmware Hyper-V Citrix Xen Open Xen AWS
FWB-100-UG Fortinet 網站應用程式式防火牆(WAF) 頻寬升級 100Mbps	網站應用程式式防火牆(WAF) 頻寬升級 100Mbps		

FWB-VM01/VM02/VM04/VM08 Fortinet 網站應用程式防火牆(WAF) (授權方式: 依照 CPU 數量 1/2/4/8 四個授權方式出貨)	網站應用程式防火牆(WAF) 支援 1 CPU		
FAD-Base Fortinet 主機負載平衡系統 (SLB) 1Gbps	主機負載平衡系統(SLB) 1Gbps	支援網路的主機負載平衡, 全球服務負載平衡 (GSLB) 及線路負載平衡 (LLB) 等功能	VMware
FAD-1000-UG Fortinet 主機負載平衡系統 (SLB) 頻寬升級 1Gbps	主機負載平衡系統(SLB) 頻寬升級 1Gbps		
FAD-VM01/VM02/VM04/VM08 Fortinet 主機負載平衡系統(SLB) (授權方式: 依照 CPU 數量 1/2/4/8 四個授權方式出貨)	主機負載平衡系統(SLB) 支援 1 CPU		
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡 400Mbps	網路負載平衡系統(WAN) 400Mbps	提供網路線路負載平衡, 整合不同 ISP 的線路同時並存, 提供進出 Internet 的資料流量	VMware ESXi / ESX 5.5, 6.0
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡頻寬升級 400Mbps	網路負載平衡頻寬升級(WAN) 400Mbps		
FC-10-FWV02-851-02-12 Fortinet 網路線路負載平衡 一年續約授權	網路負載平衡系統(WAN) 一年續約授權		
FortiWAN-VM02/VM04 Fortinet 網路線路負載平衡系統(SLB) (授權方式: 依照 CPU 數量 2/4 二個授權方式出貨)	網路負載平衡系統(WAN) 支援 2 CPU		
FSM-AIO-BASE Fortinet 稽核管理系統 50 台設備一年授權	稽核管理系統 50 台設備一年授權	SIEM 應用解決方案, 提供收集和整合各種網路和安全資訊, 匯整之後進行統一分析和統計, 藉以收集、監視和報告企業中的網路設備和資安產品發生的行為, 持續進行企業內全面的安全風險評估。	Vmware ESX, Microsoft HyperV, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure
FSM-AIO-100-UG Fortinet 稽核管理系統升級 100 台設備一年授權	稽核管理系統升級 100 台設備一年授權		
FSM-WIN-ADV-50-UG Fortinet 稽核管理系統 Windows Agent 50 台設備一年授權	稽核管理系統 Windows Agent 50 台設備一年授權		

FC1-15-EMS01-158-02-12 Fortinet 端點(End Point)資安防護 200 Clients 一年授權	端點(End Point)資安防護 200 Clients 一年授權	提供防病毒與惡意軟體檢測、雙因子認證、VPN 等功能，強化企業資安建置。FortiClient 主動防禦高級攻擊。它與 Security Fabric 的緊密集成使基於策略的自動化能夠控制威脅並控制爆發。FortiClient 與 Fabric-Ready 合作夥伴兼容，進一步加強企業的安全態勢。	Microsoft Windows, Windows Server
Fortinet 物聯網安全管理系統 100 台終端設備 一年授權	物聯網安全管理系統 100 台終端設備 一年授權	提供物聯網上每個終端設備的詳細分析以增強其可視性，控管設備之物聯網存取以保障資訊安全，並具備資料分析與報表功能。	VMware, Hyper-V
Fortinet 物聯網安全管理系統升級 100 台終端設備 一年授權	物聯網安全管理系統升級 100 台終端設備 一年授權		
FML-Base Fortinet 反垃圾郵件及郵件保全系統 100 人版	反垃圾郵件及郵件保全系統 100 人版	提供電子郵件主機功能、過濾並攔截垃圾郵件	VMware Hyper-V Citrix Xen KVM
FML-300-UG Fortinet 反垃圾郵件及郵件保全系統使用者數量升級 300 人	反垃圾郵件及郵件保全系統使用者數量升級 300 人		
FML-VM01/VM02/VM04/VM08 Fortinet 反垃圾郵件及郵件保全系統 (授權方式：依照 CPU 數量 1/2/4/8 四個授權方式出貨)	反垃圾郵件及郵件保全系統支援 1 CPU		
FAC-VM-Base Fortinet 身份認證系統 (Authenticator) 100 人版	身份認證系統(Authenticator) 100 人版	整合 RADIUS、LDAP 伺服器，提供標準及安全的雙因子認證	VMWare Hyper-V
FAC-VM-100-UGFortinet 身份認證系統 (Authenticator) 使用者數量升級 100 人	身份認證系統(Authenticator) 使用者數量升級 100 人		