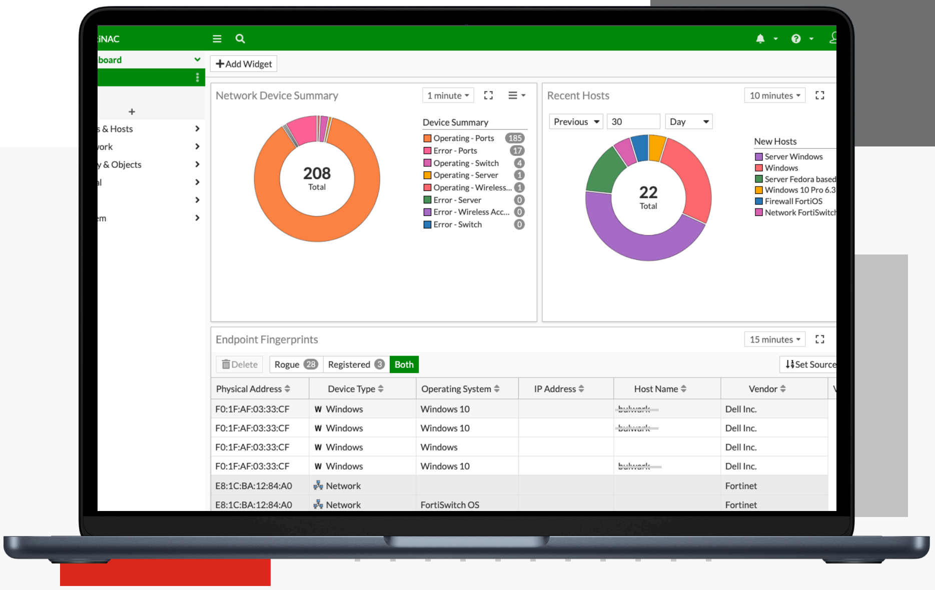
FortiNAC

FortiNAC 500C, 550C, 600C, 700C, VM, and Licenses



Network Device Summary

208 Total

Device Summary	
🟧 Operating - Ports	185
🟥 Error - Ports	17
🟪 Operating - Switch	4
🟨 Operating - Server	1
🟥 Operating - Wireless...	1
🟩 Error - Server	0
🟪 Error - Wireless Acc...	0
🟦 Error - Switch	0

Recent Hosts

Previous 30 Day

22 Total

New Hosts
- 🟪 Server Windows
- 🟥 Windows
- 🟩 Server Fedora based
- 🟨 Windows 10 Pro 6.3
- 🟦 Firewall FortiOS
- 🟪 Network FortiSwitch

Endpoint Fingerprints

Rogue 28 Registered 3 Both

Physical Address	Device Type	Operating System	IP Address	Host Name	Vendor
F0:1F:AF:03:33:CF	W Windows	Windows 10		~~bulwark~~	Dell Inc.
F0:1F:AF:03:33:CF	W Windows	Windows 10		~~bulwark~~	Dell Inc.
F0:1F:AF:03:33:CF	W Windows	Windows			Dell Inc.
F0:1F:AF:03:33:CF	W Windows	Windows 10		~~bulwark~~	Dell Inc.
E8:1C:BA:12:84:A0	Network				Fortinet
E8:1C:BA:12:84:A0	Network	FortiSwitch OS			Fortinet

Highlights

- Scan the network to detect and classify devices through automated methods
- Create a comprehensive inventory of all devices on the network
- Evaluate the risk of every endpoint on the network
- Centralize architecture to simplify deployment and management
- Support third-party network devices to ensure compatibility with the existing infrastructure, automate onboarding process, enforce dynamic network access control, and provide event reporting to SIEM with detailed contextual data to reduce investigation time

Security for Networks with IoT

FortiNAC™ is a network access control solution that enables organizations to easily manage their network access policies and ensure compliance with security policies. It offers a comprehensive view of all devices and users on the network, allowing for granular control of access based on user roles, device types, and network locations.

The solution provides automated onboarding of new endpoints, as well as continuous monitoring and remediation of non-compliant devices. FortiNAC also integrates with third-party security solutions and offers advanced reporting and analytics capabilities for enhanced visibility and compliance reporting. With FortiNAC, organizations can secure their network against unauthorized access and potential threats.

Available in

Appliance

Virtual

Features

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.

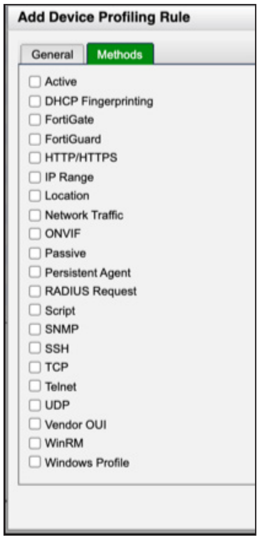
Extend Control of the Network to Third-Party Products

Implement micro-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



Add Device Profiling Rule

General | Methods

□ Active
□ DHCP Fingerprinting
□ FortiGate
□ FortiGuard
□ HTTP/HTTPS
□ IP Range
□ Location
□ Network Traffic
□ ONVIF
□ Passive
□ Persistent Agent
□ RADIUS Request
□ Script
□ SNMP
□ SSH
□ TCP
□ Telnet
□ UDP
□ Vendor OUI
□ WinRM
□ Windows Profile

FortiNAC 21 Profiling Methods for Device Classification

Device Visibility

Fundamental to the security of a constantly changing network is an understanding of its makeup. FortiNAC sees everything on the network providing complete visibility. FortiNAC scans your network to discover every user, application, and device. With up to 21 different techniques, FortiNAC can then profile each element based on observed characteristics and responses, as well as calling on FortiGuard's IoT Services, a cloud-based database for identification look-ups.

Scanning can be done actively or passively and can utilize permanent agents, dissolvable agents, or no agents. Additionally, FortiNAC can assess a device to see if it matches approved profiles, noting the need for software updates to patch vulnerabilities. With FortiNAC deployed, the entire network is known.

In addition to knowing the entire network, FortiNAC's enhanced visibility can also use passive traffic analysis, leveraging Fortinet FortiGate appliances as sensors, to identify anomalous traffic patterns, a possible indication of compromise that can be followed up by the SOC team.

Highlights

Dynamic Network Control

Once the devices are classified and the users are known, FortiNAC enables detailed segmentation of the network to enable devices and users access to necessary resources while blocking non-authorized 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 a specific group of users and/ or devices. In this manner, if a device is compromised, its ability to travel in the network and attack other assets will be limited. FortiNAC helps to protect critical data and sensitive assets while ensuring compliance with internal, industry, and government regulations and mandates.

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 that has no access to corporate resources.

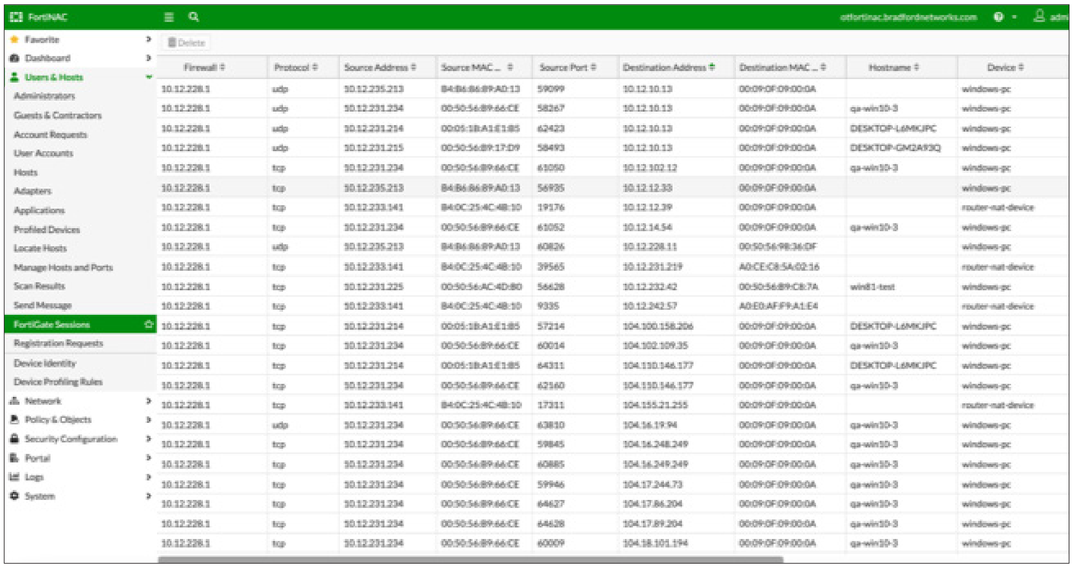
Automated Response

FortiNAC will monitor the network on an ongoing basis, evaluating endpoints to ensure they conform to their profile. FortiNAC will rescan devices to ensure MAC-address spoofing does not bypass your network access security. Additionally, FortiNAC can watch for anomalies in traffic patterns. This passive anomaly detection works in conjunction with FortiGate appliances. Once a compromised or vulnerable endpoint is detected as a threat, FortiNAC triggers an automated response to contain the endpoint in real-time.

Highlights

FortiGate Sessions View

The FortiGate Sessions view adds the ability to accept netflow data from third party devices. Flows from other devices would also show up in this view.

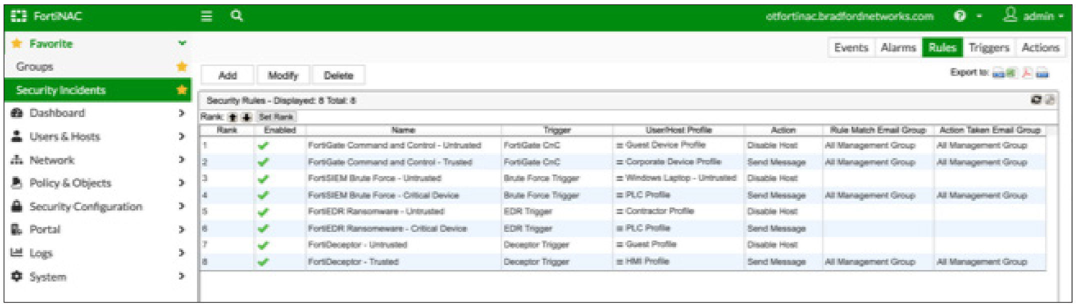


Firewall	Protocol	Source Address	Source MAC ...	Source Port	Destination Address	Destination MAC ...	Hostname	Device
10.12.228.1	udp	10.12.235.213	B4:B6:86:89:A0:13	59099	10.12.10.13	00:09:0F:09:00:0A		windows-pc
10.12.228.1	udp	10.12.231.234	00:50:56:89:66:CE	58267	10.12.10.13	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	udp	10.12.231.214	00:05:1B:A1:E1:85	62423	10.12.10.13	00:09:0F:09:00:0A	DESKTOP-L6MKJPC	windows-pc
10.12.228.1	udp	10.12.231.215	00:50:56:89:17:D9	58493	10.12.10.13	00:09:0F:09:00:0A	DESKTOP-GM2A93Q	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	61050	10.12.102.12	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.235.213	B4:B6:86:89:A0:13	56935	10.12.12.33	00:09:0F:09:00:0A		windows-pc
10.12.228.1	tcp	10.12.233.141	B4:0C:25:4C:4B:10	19176	10.12.12.39	00:09:0F:09:00:0A		router-nat-device
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	61052	10.12.14.54	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	udp	10.12.235.213	B4:B6:86:89:A0:13	60826	10.12.228.11	00:50:56:98:36:DF		windows-pc
10.12.228.1	tcp	10.12.233.141	B4:0C:25:4C:4B:10	39565	10.12.231.219	A0:CE:C8:5A:02:16		router-nat-device
10.12.228.1	tcp	10.12.231.225	00:50:56:AC:4D:80	56628	10.12.232.42	00:50:56:89:C8:7A	win81-test	windows-pc
10.12.228.1	tcp	10.12.233.141	B4:0C:25:4C:4B:10	9335	10.12.242.57	A0:E0:AF:F9:A1:E4		router-nat-device
10.12.228.1	tcp	10.12.231.214	00:05:1B:A1:E1:85	57214	104.100.158.206	00:09:0F:09:00:0A	DESKTOP-L6MKJPC	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	60014	104.102.109.35	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.231.214	00:05:1B:A1:E1:85	64311	104.110.146.177	00:09:0F:09:00:0A	DESKTOP-L6MKJPC	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	62160	104.110.146.177	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.233.141	B4:0C:25:4C:4B:10	17311	104.155.21.255	00:09:0F:09:00:0A		router-nat-device
10.12.228.1	udp	10.12.231.234	00:50:56:89:66:CE	63810	104.16.19.94	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	59845	104.16.248.249	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	60885	104.16.249.249	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	59946	104.17.244.73	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	64627	104.17.86.204	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	64628	104.17.89.204	00:09:0F:09:00:0A	qa-win10-3	windows-pc
10.12.228.1	tcp	10.12.231.234	00:50:56:89:66:CE	60009	104.18.101.194	00:09:0F:09:00:0A	qa-win10-3	windows-pc

FortiNAC 21 Profiling Methods for Device Classification

Security Fabric Integrations

FortiNAC integrates with multiple Fortinet products such as FortiGate, FortiSIEM, FortiAnalyzer, FortiEDR, and FortiDeceptor. The Security Rules are triggered by syslog/snmp messages from the other Fortinet products as shown below.

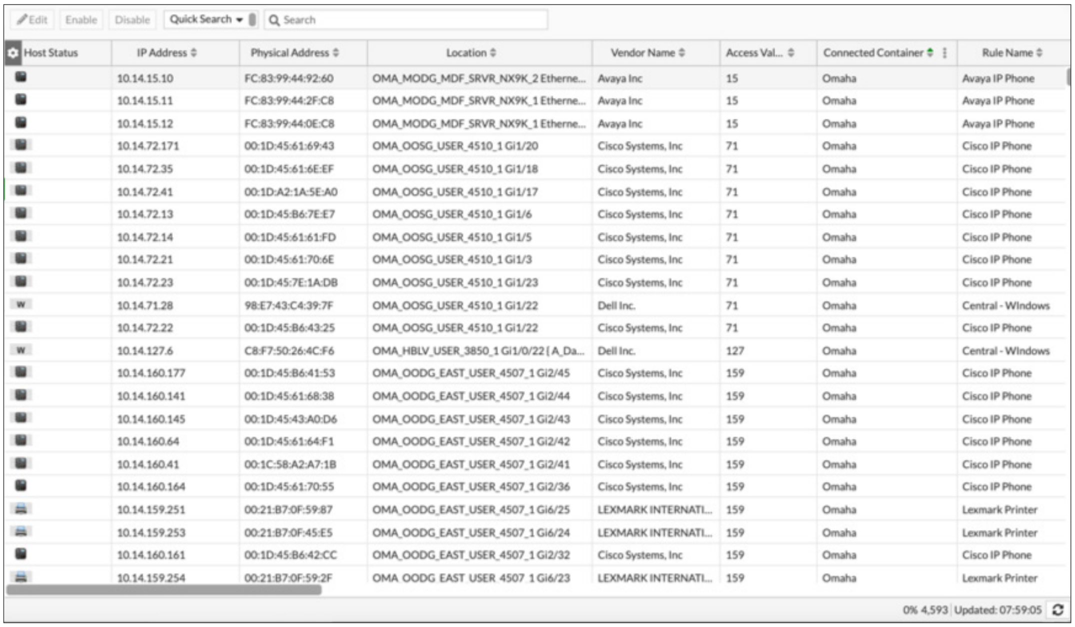


Security Rules - Displayed: 8 Total: 8

Rank	Enabled	Name	Trigger	User/Host Profile	Action	Rule Match Email Group	Action Taken Email Group
1	✓	FortiGate Command and Control - Untrusted	FortiGate CnC	= Guest Device Profile	Disable Host	All Management Group	All Management Group
2	✓	FortiGate Command and Control - Trusted	FortiGate CnC	= Corporate Device Profile	Send Message	All Management Group	All Management Group
3	✓	FortiSIEM Brute Force - Untrusted	Brute Force Trigger	= Windows Laptop - Untrusted	Disable Host		
4	✓	FortiSIEM Brute Force - Critical Device	Brute Force Trigger	= PLC Profile	Send Message	All Management Group	All Management Group
5	✓	FortiEDR Ransomeware - Untrusted	EDR Trigger	= Contractor Profile	Disable Host		
6	✓	FortiEDR Ransomeware - Critical Device	EDR Trigger	= PLC Profile	Send Message		
7	✓	FortiDeceptor - Untrusted	Deceptor Trigger	= Guest Profile	Disable Host		
8	✓	FortiDeceptor - Trusted	Deceptor Trigger	= HMI Profile	Send Message	All Management Group	All Management Group

FortiNAC Security Rules

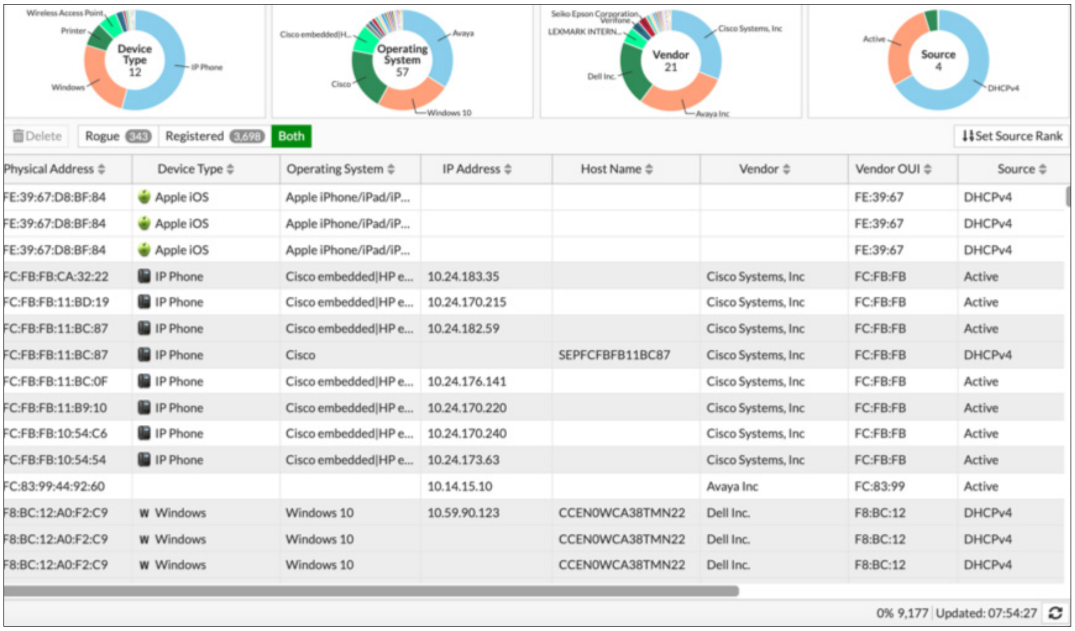
Integration



Host Status	IP Address	Physical Address	Location	Vendor Name	Access Val...	Connected Container	Rule Name
■	10.14.15.10	FC:83:99:44:92:60	OMA_MODG_MDF_SRVR_NX9K_2 Etherne...	Avaya Inc	15	Omaha	Avaya IP Phone
■	10.14.15.11	FC:83:99:44:2F:C8	OMA_MODG_MDF_SRVR_NX9K_1 Etherne...	Avaya Inc	15	Omaha	Avaya IP Phone
■	10.14.15.12	FC:83:99:44:0E:C8	OMA_MODG_MDF_SRVR_NX9K_1 Etherne...	Avaya Inc	15	Omaha	Avaya IP Phone
■	10.14.72.171	00:1D:45:61:69:43	OMA_OOSG_USER_4510_1 Gi1/20	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
■	10.14.72.35	00:1D:45:61:6E:EF	OMA_OOSG_USER_4510_1 Gi1/18	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
■	10.14.72.41	00:1D:A2:1A:5E:A0	OMA_OOSG_USER_4510_1 Gi1/17	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
■	10.14.72.13	00:1D:45:B6:7E:E7	OMA_OOSG_USER_4510_1 Gi1/6	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
■	10.14.72.14	00:1D:45:61:61:FD	OMA_OOSG_USER_4510_1 Gi1/5	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
■	10.14.72.21	00:1D:45:61:70:6E	OMA_OOSG_USER_4510_1 Gi1/3	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
■	10.14.72.23	00:1D:45:7E:1A:DB	OMA_OOSG_USER_4510_1 Gi1/23	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
W	10.14.71.28	98:E7:43:C4:39:7F	OMA_OOSG_USER_4510_1 Gi1/22	Dell Inc.	71	Omaha	Central - Windows
■	10.14.72.22	00:1D:45:B6:43:25	OMA_OOSG_USER_4510_1 Gi1/22	Cisco Systems, Inc	71	Omaha	Cisco IP Phone
W	10.14.127.6	C8:F7:50:26:4C:F6	OMA_HBLV_USER_3850_1 Gi1/0/22 { A_Da...	Dell Inc.	127	Omaha	Central - Windows
■	10.14.160.177	00:1D:45:B6:41:53	OMA_OODG_EAST_USER_4507_1 Gi2/45	Cisco Systems, Inc	159	Omaha	Cisco IP Phone
■	10.14.160.141	00:1D:45:61:68:38	OMA_OODG_EAST_USER_4507_1 Gi2/44	Cisco Systems, Inc	159	Omaha	Cisco IP Phone
■	10.14.160.145	00:1D:45:43:A0:D6	OMA_OODG_EAST_USER_4507_1 Gi2/43	Cisco Systems, Inc	159	Omaha	Cisco IP Phone
■	10.14.160.64	00:1D:45:61:64:F1	OMA_OODG_EAST_USER_4507_1 Gi2/42	Cisco Systems, Inc	159	Omaha	Cisco IP Phone
■	10.14.160.41	00:1C:58:A2:A7:1B	OMA_OODG_EAST_USER_4507_1 Gi2/41	Cisco Systems, Inc	159	Omaha	Cisco IP Phone
■	10.14.160.164	00:1D:45:61:70:55	OMA_OODG_EAST_USER_4507_1 Gi2/36	Cisco Systems, Inc	159	Omaha	Cisco IP Phone
🖶	10.14.159.251	00:21:B7:0F:59:87	OMA_OODG_EAST_USER_4507_1 Gi6/25	LEXMARK INTERNATI...	159	Omaha	Lexmark Printer
🖶	10.14.159.253	00:21:B7:0F:45:E5	OMA_OODG_EAST_USER_4507_1 Gi6/24	LEXMARK INTERNATI...	159	Omaha	Lexmark Printer
■	10.14.160.161	00:1D:45:B6:42:CC	OMA_OODG_EAST_USER_4507_1 Gi2/32	Cisco Systems, Inc	159	Omaha	Cisco IP Phone
🖶	10.14.159.254	00:21:B7:0F:59:2F	OMA OODG EAST USER 4507 1 Gi6/23	LEXMARK INTERNATI...	159	Omaha	Lexmark Printer

0% 4,593 | Updated: 07:59:05

FortiNAC Adapter View



Physical Address	Device Type	Operating System	IP Address	Host Name	Vendor	Vendor OUI	Source
FE:39:67:D8:BF:84	Apple iOS	Apple iPhone/iPad/iP...				FE:39:67	DHCPv4
FE:39:67:D8:BF:84	Apple iOS	Apple iPhone/iPad/iP...				FE:39:67	DHCPv4
FE:39:67:D8:BF:84	Apple iOS	Apple iPhone/iPad/iP...				FE:39:67	DHCPv4
FC:FB:FB:CA:32:22	IP Phone	Cisco embedded|HP e...	10.24.183.35		Cisco Systems, Inc	FC:FB:FB	Active
FC:FB:FB:11:BD:19	IP Phone	Cisco embedded|HP e...	10.24.170.215		Cisco Systems, Inc	FC:FB:FB	Active
FC:FB:FB:11:BC:87	IP Phone	Cisco embedded|HP e...	10.24.182.59		Cisco Systems, Inc	FC:FB:FB	Active
FC:FB:FB:11:BC:87	IP Phone	Cisco		SEPFCFBFB11BC87	Cisco Systems, Inc	FC:FB:FB	DHCPv4
FC:FB:FB:11:BC:0F	IP Phone	Cisco embedded|HP e...	10.24.176.141		Cisco Systems, Inc	FC:FB:FB	Active
FC:FB:FB:11:B9:10	IP Phone	Cisco embedded|HP e...	10.24.170.220		Cisco Systems, Inc	FC:FB:FB	Active
FC:FB:FB:10:54:C6	IP Phone	Cisco embedded|HP e...	10.24.170.240		Cisco Systems, Inc	FC:FB:FB	Active
FC:FB:FB:10:54:54	IP Phone	Cisco embedded|HP e...	10.24.173.63		Cisco Systems, Inc	FC:FB:FB	Active
FC:83:99:44:92:60			10.14.15.10		Avaya Inc	FC:83:99	Active
F8:BC:12:A0:F2:C9	W Windows	Windows 10	10.59.90.123	CCEN0WCA38TMN22	Dell Inc.	F8:BC:12	DHCPv4
F8:BC:12:A0:F2:C9	W Windows	Windows 10		CCEN0WCA38TMN22	Dell Inc.	F8:BC:12	DHCPv4
F8:BC:12:A0:F2:C9	W Windows	Windows 10		CCEN0WCA38TMN22	Dell Inc.	F8:BC:12	DHCPv4

0% 9,177 | Updated: 07:54:27

FortiNAC New Endpoint Fingerprints View

Integration

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 the following*.

Network Infrastructure	Adtran, Aerohive, AlaxalA Networks, Alcatel-Lucent, Allied Telesis, Alteon, APC, Apple, APRESIA Systems, Avaya, Brocade/Foundry Networks/Ruckus, Cisco/Meraki, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Intel, Juniper, NEC, Riverbed/Xirrus, and SonicWall
Security Infrastructure	CheckPoint, Cisco/SourceFire, Cyphort, FireEye, Juniper/Netscreen, Qualys, Sonicwall, Tenable
Authentication and Directory Services	RADIUS — Cisco ACS, Free RADIUS, Microsoft IAS, LDAP — Google SSO, Microsoft Active Directory, OpenLDAP
Operating Systems	Android, Apple MAC OSX and iOS, Linux, Microsoft Windows
Endpoint Security Applications	Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Vexira, Webroot SpySweeper, Zone Alarm
Mobile Device Management	AirWatch, Google GSuite, MaaS360, Microsoft InTune, Mobile Iron, XenMobile, JAMF, Nozomi Networks

* 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-size to very large enterprise deployments. There are three elements to the FortiNAC solution.

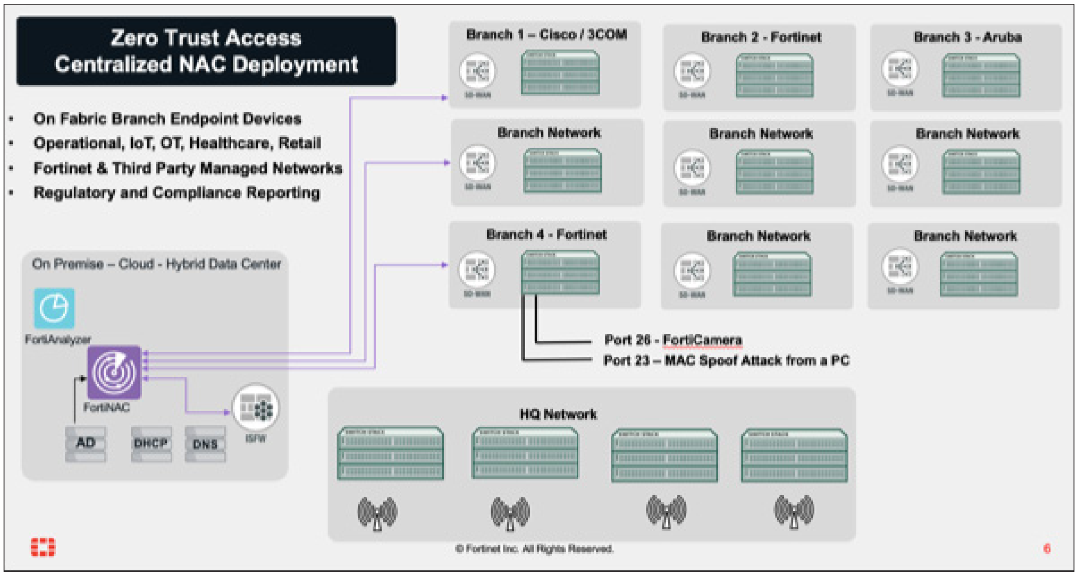
- Application and Control (required)
- Management (optional)
- FortiAnalyzer for Reports (optional)

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. FortiAnalyzer provides reports and analytics based on the information gathered from the network through FortiNAC.

FortiNAC can be deployed in virtual machines (VMWare/Hyper-V/ AWS/ Azure/ KVM) 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. FortiNAC is ideal for support distributed architectures, including SD-Branch locations.

High Availability

FortiNAC offers High Availability for disaster recovery to ensure redundancy. This state is achieved through active and passive instances where the passive (backup) becomes active when the main is no longer functioning normally. FortiNAC Manager can manage multiple high availability clusters distributed throughout the network as needed



Zero Trust Access
Centralized NAC Deployment

- On Fabric Branch Endpoint Devices
- Operational, IoT, OT, Healthcare, Retail
- Fortinet & Third Party Managed Networks
- Regulatory and Compliance Reporting

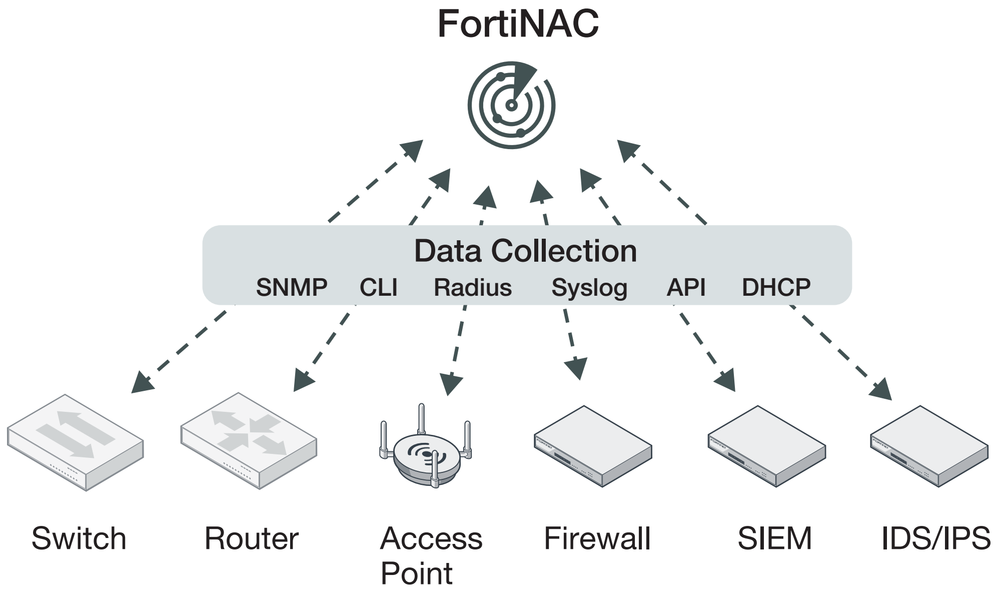
© Fortinet Inc. All Rights Reserved.

Deployment Options

Centralized Architecture

FortiNAC is an 'out of band' solution, meaning it does not sit in-line of user traffic. This architecture allows FortiNAC to be deployed centrally and manage many remote locations. Visibility, control, and response are achieved by integrating with, and leveraging the capabilities of, the network infrastructure. Control can be applied at the point of connection, at the very edge of the network while security device integrations allow FortiNAC to process security alerts and treat them as triggers for automated threat mitigation through customizable work flows.

Data collection is gathered from multiple sources using a variety of methods. SNMP, CLI, RADIUS, SYSLOG, API and DHCP fingerprints can all be used to achieve the detailed end-to-end visibility necessary to create a truly secure environment.



Licensing

FortiNAC Licensing

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

Base License

The BASE 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 micro-segmentation and network lockdown. The BASE license level is appropriate for organizations that need to secure IoT and headless devices, and enable network lockdown with dynamic VLAN steering, but do not require more advanced user/network controls or automated threat response.

Plus License

The PLUS license level builds on all the functionality of BASE with enhanced visibility and 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.

Pro License

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.

Licensing

		FORTINAC LICENSE TYPES	BASE	PLUS	PRO
Visibility	**Network**	Network Discovery	✓	✓	✓
		Rogue Identification	✓	✓	✓
		Device Profiling and Classification	✓	✓	✓
	Endpoint	Enhanced Visiblity	✓	✓	✓
		Anomaly Detection	✓	✓	✓
		MDM Integration	✓	✓	✓
		Persistent Agent	✓	✓	✓
	User	Authentication		✓	✓
		Captive Portal		✓	✓
Automation / Control		Network Access Policies	✓	✓	✓
		IoT Onboarding with Sponsor	✓	✓	✓
		Rogue Device Detection and Restriction	✓	✓	✓
		Firewall Segmentation	✓	✓	✓
		MAC Address Bypass (MAB)	✓	✓	✓
		Full RADIUS (EAP)	✓	✓	✓
		BYOD / Onboarding		✓	✓
		Guest Management		✓	✓
		Endpoint Compliance		✓	✓
		Web and Firewall Single Sign-on	✓	✓	✓
Incident Response		Event Correlation			✓
		Extensible Actions and Audit Trail			✓
		Alert Criticality and Routing			✓
		Guided Triage Workflows			✓
Integrations		Inbound Security Events			✓
		Outbound Security Events	✓	✓	✓
		REST API	✓	✓	✓
Reporting		Customizable Reports	✓	✓	✓

Services

FortiCare Services

As your business rapidly evolves, it is critical to advance your security capabilities as well. Often though, you do not have expertise within your organization to deploy, operate, and maintain these new capabilities or are up against tight deadlines to implement change. We understand this challenge and help thousands of organizations every year tackle this problem with FortiCare Services.

Our experts provide accelerated implementation of your technology, reliable assistance through advanced support, and proactive care to ensure your success with Fortinet investment. No matter the size or location of your organization, we are ready to provide you with an elevated experience to help you achieve your business goals with superior security and performance.

FortiCare Support

A FortiCare Support contract entitles you not only to receive updates to the FortiNAC firmware, but also receive two important feeds.

1) Network device database update FortiNAC supports more than 2500 switching, wireless, or firewall devices on the market. As new devices are released, FortiNAC's network device database should be updated to reflect these new models. The weekly update from the FortiNAC team will keep your deployment up to date.

2) FortiGuard IoT Service. One of the means that FortiNAC has to identify devices is to use the cloud-look up service hosted by FortiGuard Labs. A FortiCare Support contract entitles you to use that service at no additional cost, giving you access to a database of millions of devices

Specifications

<table>
<tr><th></th><th>FNC-M-550C</th><th>FNC-CA-600C</th><th>FNC-CA-500C</th></tr>
<tr><td colspan="4"><b>System</b></td></tr>
<tr><td><b>CPU</b></td><td colspan="2">Intel Xeon Silver 4210 2.2G, 10C/20T, 9.6GT/s, 13.75M Cache, Turbo, HT (85W) DDR4-2400 (Qty 2)</td><td>Intel Xeon E-2124 3.3GHz, 8M cache, 4C/4T, turbo (71W) (Qty 1)</td></tr>
<tr><td><b>Memory</b></td><td colspan="2">8GB RDIMM, 3200MT/s, Single Rank (Qty 4)</td><td>8GB 2666MT/s DDR4 ECC UDIMM (Qty 2)</td></tr>
<tr><td><b>Hard Disk</b></td><td colspan="2">1TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)</td><td>1TB 7.2K RPM SATA 6 Gbps 3.5in Hot-plug Hard Drive RAID1 (Qty 2)</td></tr>
<tr><td><b>BMC</b></td><td colspan="2">iDRAC9 Express, integrated (Qty 1)</td><td>iDRAC8 Express (Qty 1)</td></tr>
<tr><td><b>Network Interface</b></td><td colspan="2">4× 10/100/1000 Ethernet, RJ45</td><td>4× 10/100/1000 Ethernet, RJ45</td></tr>
<tr><td><b>RAID Card</b></td><td colspan="2">PERC H330 Integrated RAID Controller (Qty 1)</td><td>PERC H330 Integrated RAID Controller (Qty 1)</td></tr>
<tr><td><b>RAID Configuration</b></td><td colspan="2">RAID 1</td><td>RAID 1</td></tr>
<tr><td><b>Console Access</b></td><td colspan="2">Yes *</td><td>Yes *</td></tr>
<tr><td><b>Form Factor</b></td><td colspan="2">1U Rack Mountable</td><td>1U Rack Mountable</td></tr>
<tr><td colspan="4"><b>Dimensions</b></td></tr>
<tr><td><b>Height x Width x Length (inches)</b></td><td colspan="2">1.68 × 18.9 × 29.73</td><td>1.68 × 17.08 × 24.60</td></tr>
<tr><td><b>Height x Width x Length (mm)</b></td><td colspan="2">42.8 × 482.4 × 755.12</td><td>42.8 × 434.0 × 625.0</td></tr>
<tr><td><b>Weight</b></td><td colspan="2">43.056 lbs (19.76 kg)</td><td>43.87 lbs (19.9 kg)</td></tr>
<tr><td colspan="4"><b>Environment</b></td></tr>
<tr><td><b>Power Supply</b></td><td colspan="2">Dual 550W Hot Plug Power Supply</td><td>Dual 350W Hot Plug Power Supplies</td></tr>
<tr><td><b>Input Power</b></td><td colspan="2">100-240V AC Autoranging</td><td>100-240V AC Autoranging</td></tr>
<tr><td><b>Input Current</b></td><td colspan="2">6.25 A</td><td>3.0 A</td></tr>
<tr><td><b>Cooling</b></td><td colspan="2">7 fans</td><td>4 fans</td></tr>
<tr><td><b>Panel Display</b></td><td colspan="2">No LCD</td><td>20 Char LCD</td></tr>
<tr><td><b>Heat Dissipation</b></td><td colspan="2">2559 BTU/hr</td><td>1357.1 BTU/hr</td></tr>
<tr><td><b>Operation Temperature Range</b></td><td colspan="2">50°–95°F (10°–35°C)</td><td>50°–95°F (10°–35°C)</td></tr>
<tr><td><b>Storage Temperature Range</b></td><td colspan="2">-40°–149°F (-40°–65°C)</td><td>-40°–149°F (-40°–65°C)</td></tr>
<tr><td><b>Humidity (Operating)</b>
<b>Humidity (Non-operating)</b></td><td colspan="2">10%–80% non-condensing
5%–95% non-condensing</td><td>10%–80% non-condensing
5%–95% non-condensing</td></tr>
<tr><td colspan="4"><b>Certification</b></td></tr>
<tr><td><b>Safety</b></td><td colspan="3">Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), European Union (CE).</td></tr>
<tr><td><b>Electromagnetic (EMC)</b></td><td colspan="3">Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), European Union (CE).</td></tr>
<tr><td><b>Materials</b></td><td colspan="3">Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).</td></tr>
</table>

* The console port can be used for access if the appliance has an issue i.e. you can connect a monitor and a keyboard to it. FortiNAC does not use the console port for access.

Specifications

	FNC-CA-700C
System	
CPU	Intel Xeon Gold 6240 2.6G, 18C/36T, 10.4GT/s, 24.75M Cache, Turbo, - HT (150W) DDR4-2933 (Qty 2)
Memory	8GB RDIMM, 3200MT/s, Single Rank (Qty 12)
Hard Disk	600 GB 15K RPM SAS 12 Gbps 2.5in Hot-plug Hard Drive (Qty 2)
BMC	iDRAC9 Express, integrated (Qty 1)
Network Interface	4× 10/100/1000 Ethernet, RJ45
RAID Card	PERC H730P+ RAID Controller, 2 GB Cache (Qty 1)
RAID Configuration	RAID 1
Console Access	Yes *
Form Factor	1U Rack Mountable
Dimensions	
Height x Width x Length (inches)	1.68 × 18.9 × 29.73
Height x Width x Length (mm)	42.8 × 482.4 × 755.12
Weight	43.056 lbs (19.76 kg)
Environment	
Power Supply	Dual, Hot Plug, Redundant Power Supply (1+1), 550 W
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) **Humidity (Non-operating)**	10%–80% 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).

* The console port can be used for access if the appliance has an issue i.e. you can connect a monitor and a keyboard to it. FortiNAC does not use the console port for access.

Appliance

Hardware Server Sizing

HARDWARE			
Hardware Server	**Type**	**Target Environment**	**Capacity[1]**
FortiNAC-CA-500C	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 2000 ports in the network
FortiNAC-CA-600C	High Performance Control and Application Server	Medium Environments	Manages up to 15 000 ports in the network
FortiNAC-CA-700C	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 25 000 ports in the network
FortiNAC-M-550C	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Unlimited

[1] 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.

Virtual

VM Server Resource Sizing

VIRTUAL MACHINE							
VM OS	**SKU**	**Ports in the Network[1]**	**Target Environment**	**CPU Reference**	**vCPU Qty[2]**	**Memory (GB)**	**Disk (GB)**
CentOS	**FNC-CA-VM**	Up to 2 000	Small	Intel Xeon E-2124 3.3 GHz 4C/4T	4	16	100
		Up to 15 000	Medium	Intel Xeon Silver 4210 2.2G 10C/20T	20	32	100
		Up to 25 000	Large	Intel Xeon Gold 6240 2.6 G 18C/36T	36	96	100
	FNC-M-VM	Unlimited	Large	Intel Xeon Silver 4210 2.2G 10C/20T	20	32	100
FortiNAC-OS	**FNC-CAX-VM**	Up to 5 000	Small	Intel Xeon E-2278 GE 3.3 GHz 8C/16T	8	16	100
		Up to 15 000	Medium	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100
		Up to 25 000	Large	AMD Milan EPYC 7543P 2.8 GHz 32C/64T	32	96	100
	FNC-MX-VM	Unlimited	Large	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100

[1] Ports in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total ports count, not total number of devices.

[2] The values in the vCPU column were determined by using the CPUs in the CPU reference column and are guidelines only. VM resources may vary based on individual environments.

Ordering Information

PRODUCT	SKU	DESCRIPTION
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-M-550C	FNC-M-550C	FortiNAC Manager 550, Network Manager with RAID and Redundant Power Supplies
Virtual Machines		
FortiNAC Control and Application VM	FNC-CA-VM	FortiNAC Control and Application VM Server (VMWare or Hyper-V or AWS or Azure or KVM) (Running CentOS)
FortiNAC Manager VM	FNC-M-VM	FortiNAC Manager VM Server (VMware or Hyper-V or AWS or Azure or KVM) (Running CentOS)
FortiNAC Control and Application eXtended VM	FNC-CAX-VM	FortiNAC Control and Application eXtended VM Server (VMWare or Hyper-V or AWS or Azure or KVM) (Running FortiNAC-OS)
FortiNAC Manager eXtended VM	FNC-MX-VM	FortiNAC Manager eXtended VM Server (VMware or Hyper-V or AWS or Azure or KVM) (Running FortiNAC-OS)
Perpetual License		
FortiNAC BASE License 100	LIC-FNAC-BASE-100	FortiNAC BASE License for 100 concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 1K	LIC-FNAC-BASE-1K	FortiNAC BASE License for 1K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 10K	LIC-FNAC-BASE-10K	FortiNAC BASE License for 10K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 50K	LIC-FNAC-BASE-50K	FortiNAC BASE License for 50K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC PLUS License 100	LIC-FNAC-PLUS-100	FortiNAC PLUS License for 100 concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 1K	LIC-FNAC-PLUS-1K	FortiNAC PLUS License for 1K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 10K	LIC-FNAC-PLUS-10K	FortiNAC PLUS License for 10K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 50K	LIC-FNAC-PLUS-50K	FortiNAC PLUS License for 50K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PRO License 100	LIC-FNAC-PRO-100	FortiNAC PRO License for 100 concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 1K	LIC-FNAC-PRO-1K	FortiNAC PRO License for 1K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 10K	LIC-FNAC-PRO-10K	FortiNAC PRO License for 10K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 50K	LIC-FNAC-PRO-50K	FortiNAC PRO License for 50K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.

www.fortinet.com

April 28, 2023