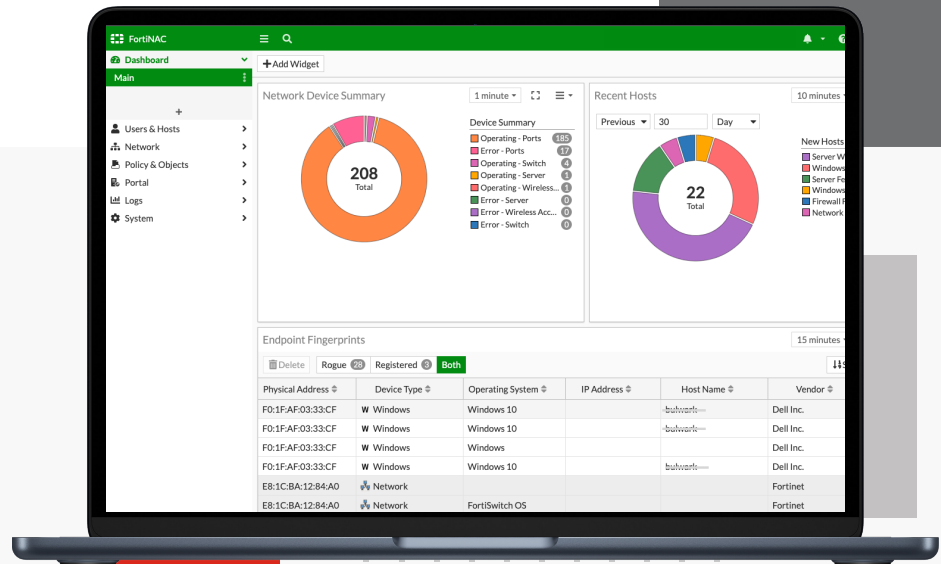


FortiNAC

FortiNAC F Series Hardware, VM, and Endpoint Licenses



Highlights

- Discover and maintain an updated inventory of all network devices, including BYOD, IoT, OT, and IoMT
- Continuously assess risks for every endpoint using real-time threat intelligence and behavioral patterns
- Implement dynamic network scanning to classify and analyze device behaviors using continuous, automated techniques
- Expand Zero Trust to end devices with always-on identity checks and least privilege access
- Integrate with various third-party network tools ensuring compatibility
- Relay real-time contextual data to SIEM, improving incident response.

Visibility, Zero Trust Access, and Incident Response for Connected Assets and Users

FortiNAC continues to be a cutting-edge network access control solution, enabling organizations to enforce network access policies and assure adherence to security protocols in light of increasingly sophisticated threats. It provides a comprehensive snapshot of all devices and users on the network, facilitating granular control of access based on user roles, device types, network locations, and now enhanced with the behavioral patterns of devices and users.

The solution's capability now extends beyond automated onboarding of new endpoints; it incorporates real-time threat intelligence and continuous risk assessment of devices, leveraging machine learning and AI technologies from FortiGuard Services. Given the rising prominence of BYOD (Bring Your Own Device) and IoT (Internet of Things), the FortiNAC continuous monitoring and immediate remediation of non-compliant devices have become even more crucial.

Moreover, FortiNAC's integration goes beyond third-party networking and security solutions; it integrates with a wide range of cloud-based platforms and DevOps tools to ensure seamless and secure network operations in hybrid IT environments. FortiNAC leverages its integration with FortiAnalyzer to gain deep insight into network security posture, encompassing real-time visibility, predictive analytics, and more robust compliance reporting. Organizations can use FortiNAC to build a solid foundation for a secured network that can more effectively protect against unauthorized access, potential threats, and increasingly, the insider threats. The net result aligns with the emerging Zero Trust security model that emphasizes "never trust, always verify".

Features

Available in



Appliance



Virtual

Granular Visibility Across the Network for Every Device and User

FortiNAC leverages AI and machine learning from FortiGuard Security Services to provide detailed profiling of devices (FortiNAC native 27 categories + FortiGuard 133 categories), including headless devices and IoT assets on your network. This profiling incorporates multiple information sources, behavior patterns, and real-time threat intelligence to accurately identify and assess what is on your network.

Seamless Integration and Control Across Diverse Environments

With the power of micro-segmentation and Zero Trust policies, FortiNAC allows for configuration changes on switches and wireless products from an extended range of vendors. It amplifies the reach of the Security Fabric across multi-cloud, hybrid IT, and heterogeneous environments, implementing “never trust, always verify” principles.

Automated Responsiveness

FortiNAC reacts to network events in real-time to contain threats before they spread, utilizing a broad and customizable set of automation policies. Leveraging AI, these policies can instantly trigger configuration changes and remediation actions when targeted behavior or anomalies are observed, aligning with the Zero Trust model's dynamic and proactive approach.

Next-Gen FortiNAC-F

FortiNAC introduces the Next-Gen FortiNAC-F OS with hardened virtual and physical appliances that increase security and compliance capabilities. Following the tradition of providing the reliable platforms of Fortinet, the new FortiNAC-F will extend the performance capability and introduce new features.

Highlights

Granular Device Visibility

The essence of securing a dynamic, ever-evolving network lies in comprehending its makeup. FortiNAC leverages AI and machine learning from FortiGuard Security Services, goes beyond merely “seeing” everything on the network—it comprehends and analyzes. It scans your network to discover every user, application, and device. Using a variety of techniques—it profiles each element based on observed behavior, real-time threat intelligence, as well as tapping into FortiGuard IoT Services, a cloud-based database for identification lookups.

Scanning can be active or passive, utilizing permanent agents, dissolvable agents, or agentless approaches. Moreover, FortiNAC can evaluate a device against pre-approved profiles, noting any discrepancies or software updates required to patch vulnerabilities. With FortiNAC, the network isn't just known—it's understood, assessed, and continually monitored.

Besides recognizing the entire network, FortiNAC's advanced visibility incorporates passive traffic analysis, leveraging Fortinet FortiGate appliances as sensors to identify anomalous behavior patterns. These patterns can indicate a potential compromise, triggering real-time alerts for the SOC team and aligning with the proactive threat containment approach integral to the Zero Trust model.



FortiNAC 21 Profiling Methods for Device Classification



Highlights



Network Security and Intelligent Segmentation

After successful classification of devices and user identification, FortiNAC now integrates advanced segmentation techniques to ensure only authorized users and devices have access to requisite resources, thus preventing unauthorized intrusion. Through its progressive role-based network access control, FortiNAC allows for strategic network segmentation by logically grouping similar data and applications, limiting access to a particular set of users or devices. This strategy effectively confines a compromised device, thereby inhibiting its ability to traverse the network and inflict damage on other resources. FortiNAC not only fortifies the protection of sensitive data and vital assets but also ensures adherence to internal, industrial, and government regulations and mandates.



Device Integrity Verification and Malware Prevention

FortiNAC emphasizes on the importance of device integrity prior to network connection, significantly reducing the risk and potential spread of malicious software. As a device attempts to join or re-join the network, FortiNAC assesses its configuration for compliance. Any non-compliant configuration is promptly managed; for instance, the device may be allocated to an isolated or restricted access VLAN, devoid of any access to corporate resources. This feature has become increasingly relevant with the rise of IoT devices and remote work trends, ensuring a secure and controlled network environment.



Intelligent Monitoring and Automated Reaction

FortiNAC proactively supervises the network continuously, examining endpoints to verify their compliance with predefined profiles. Leveraging modern security tactics, FortiNAC rescreens devices to prevent any possible bypassing of network access security via MAC-address spoofing. Further, FortiNAC is equipped to identify irregularities in traffic patterns, a vital feature considering the growing complexities in network usage patterns with the rise of cloud and edge computing. This passive anomaly detection function operates symbiotically with FortiGate appliances. Upon recognizing a compromised or susceptible endpoint as a potential risk, FortiNAC promptly instigates an automated reaction, quarantining the endpoint in real-time, furthering its commitment to maintaining a secure and controlled network environment.

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.

FortiNAC

Dashboard

Users & Hosts

FortiGate Sessions

10.14.14.1@nec.ac

Users & Hosts

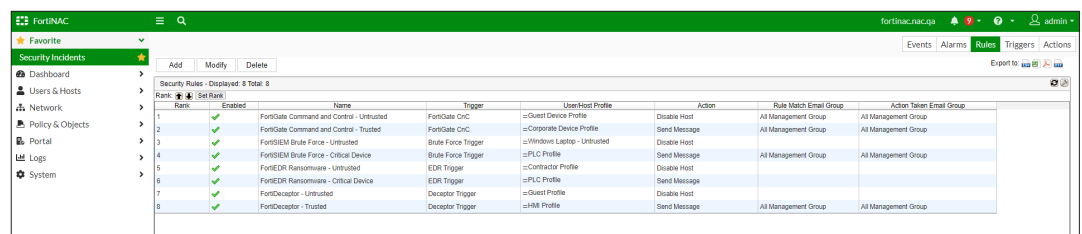
FortiGate Sessions

	Firewall	Source	Protocol	Source Address	Source MAC Address	Source Port	Destination Address	Destination Port	Added Date
Administrators	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	56921	8.8.8.8	53	2023/07/28 12:13:12
Guests & Contractors	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64909	104.117.233.39	443	2023/07/28 12:13:12
Account Requests	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64911	51.105.71.137	443	2023/07/28 12:13:12
Registration Requests	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64912	20.189.173.4	443	2023/07/28 12:13:12
User Accounts	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64908	20.125.63.4	443	2023/07/28 12:13:12
Hosts	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	61335	8.8.8.8	53	2023/07/28 12:13:12
Adapters	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	56220	8.8.8.8	53	2023/07/28 12:13:12
Applications	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64914	204.79.197.239	443	2023/07/28 12:21:49
Endpoint Fingerprints	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	62066	8.8.8.8	53	2023/07/28 12:21:49
Profiled Devices	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	58963	8.8.8.8	53	2023/07/28 12:21:49
Device Profiling Rules	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	50252	8.8.8.8	53	2023/07/28 12:21:49
FortiGate Sessions	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	51513	8.8.8.8	53	2023/07/28 12:23:41
Locate Hosts	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	57210	8.8.4.4	443	2023/07/28 12:23:41
Manage Hosts and Ports	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64919	142.250.188.3	443	2023/07/28 12:23:41
Send Message	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64920	142.251.46.227	443	2023/07/28 12:23:41
Network	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64928	142.251.46.226	443	2023/07/28 12:23:41
Policy & Objects	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	55942	142.250.189.170	443	2023/07/28 12:23:41
Portal	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64922	142.250.189.238	443	2023/07/28 12:23:41
Logs	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	51058	142.250.191.74	443	2023/07/28 12:23:41
System	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	59218	142.250.188.14	443	2023/07/28 12:23:41
	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	63289	142.251.46.195	443	2023/07/28 12:23:41
	192.168.1.1	Firewall	udp	10.10.16.11	00:50:56:85:D9:13	62575	8.8.8.8	53	2023/07/28 12:23:41
	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64929	142.250.188.14	443	2023/07/28 12:23:41
	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64917	142.250.189.238	443	2023/07/28 12:23:41
	192.168.1.1	Firewall	tcp	10.10.16.11	00:50:56:85:D9:13	64925	142.250.189.170	443	2023/07/28 12:23:41

FortiNAC 21 Profiling Methods for Device Classification

Security Fabric Integrations

FortiNAC integrates with multiple Fortinet products such as FortiGate, FortiSIEM, FortiAnalyzer, FortiEDR, FortiDeceptor, FortiClient EMS, FortiLAN Cloud, FortiSwitch, FortiAP, and FortiExtender. The security rules are triggered by syslog/snmp messages from the other Fortinet products as shown below.



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	=Unknown Laptop - Untrusted	Disable Host	All Management Group	All Management Group
4	✓	FortiSIEM Brute Force - Critical Device	Brute Force Trigger	=PLC Profile	Send Message	All Management Group	All Management Group
5	✓	FortiEDR Ransomware - Untrusted	EDR Trigger	=Contractor Profile	Disable Host	All Management Group	All Management Group
6	✓	FortiEDR Ransomware - Critical Device	EDR Trigger	=PLC Profile	Send Message	All Management Group	All Management Group
7	✓	FortiDeceptor - Untrusted	Deceptor Trigger	=Guest Profile	Disable Host	All Management Group	All Management Group
8	✓	FortiDeceptor - Trusted	Deceptor Trigger	=HR Profile	Send Message	All Management Group	All Management Group

FortiNAC Security Rules



FortiNAC Device and Network View

Status	Host Status	IP Address	Physical Address	Location	Vendor Name	Access Value	Connected Container	Rule Name
		10.10.12.18	00:50:56:B5:A4:89	OMA_OOSG_USER_4510_1 Gi/17	VMware, Inc.	71	Omaha	Central - Windows
		10.10.12.22	00:50:56:B5:A4:90	OMA_OOSG_USER_4510_1 Gi/3	VMware, Inc.	71	Omaha	Central - Windows
		10.10.16.22	00:50:56:B5:A4:95	OMA_OOSG_USER_4510_1 Gi/5	VMware, Inc.	71	Omaha	Cisco IP Phone
		10.10.16.88	00:70:56:B5:A2:88	OMA_OOSG_WEST_USER_4510_1 Gi/22	Dell, Inc.	71	Omaha	Cisco IP Phone
		10.10.16.71	00:70:56:B5:A2:86	OMA_OOSG_WEST_USER_4510_1 Gi/22	Dell, Inc.	71	Omaha	Cisco IP Phone
		10.10.16.52	00:70:56:B5:A2:52	OMA_OOSG_WEST_USER_4510_1 Gi/24	Dell, Inc.	71	Omaha	Cisco IP Phone
		10.10.24.28	00:50:56:B5:A6:66	OMA_OOSG_USER_4510_1 Gi/5	VMware, Inc.	159	Omaha	Avaya IP Phone
		10.10.114.28	00:50:56:B5:B2:50	OMA_OOSG_EAST_USER_4507_1 Gi2/43	VMware, Inc.	159	Omaha	Avaya IP Phone
		10.10.114.152	00:70:56:B5:A2:C2	OMA_OOSG_WEST_USER_4510_1 Gi/24	Dell, Inc.	159	Omaha	Cisco IP Phone
		10.10.114.12	00:70:56:B5:A2:D2	OMA_OOSG_WEST_USER_4510_1 Gi/24	Dell, Inc.	159	Omaha	Cisco IP Phone
		10.10.114.18	00:50:56:B5:B2:55	OMA_OOSG_EAST_USER_4507_1 Gi2/43	VMware, Inc.	15	Omaha	Avaya IP Phone
		10.10.14.18	00:50:56:B5:B2:04	OMA_OOSG_EAST_USER_4507_1 Gi2/43	VMware, Inc.	15	Omaha	Avaya IP Phone
		10.10.14.20	00:50:56:B5:B2:14	OMA_OOSG_EAST_USER_4507_1 Gi2/43	VMware, Inc.	15	Omaha	Avaya IP Phone
		10.10.160.30	00:50:56:B5:C2:56	OMA_OOSG_EAST_USER_4507_1 Gi2/42	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.28	00:50:56:B5:C2:58	OMA_OOSG_EAST_USER_4507_1 Gi2/44	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.70	00:50:56:B5:C2:70	OMA_OOSG_EAST_USER_4507_1 Gi2/44	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.72	00:50:56:B5:C2:70	OMA_OOSG_EAST_USER_4507_1 Gi2/36	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.78	00:50:56:B5:B2:A0	OMA_OOSG_EAST_USER_4507_1 Gi2/35	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.34	00:50:56:B5:B2:34	OMA_OOSG_EAST_USER_4507_1 Gi2/26	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.104.28	00:50:56:B5:A5:95	OMA_OOSG_USER_4510_1 Gi/5	VMware, Inc.	127	Omaha	Cisco IP Phone
		10.10.14.28	00:50:56:B5:A6:95	OMA_OOSG_USER_4510_1 Gi/5	VMware, Inc.	127	Omaha	Cisco IP Phone
		10.10.127.34	00:70:56:B5:B2:34	OMA_OOSG_WEST_USER_4522_1 Gi3/16	Dell, Inc.	127	Omaha	Cisco IP Phone
		10.10.127.44	00:70:56:B5:B2:44	OMA_OOSG_WEST_USER_4522_1 Gi3/16	Dell, Inc.	127	Omaha	Cisco IP Phone
		10.10.127.124	00:70:56:B5:B2:84	OMA_OOSG_WEST_USER_4522_1 Gi3/16	Dell, Inc.	127	Omaha	Cisco IP Phone

0% 136 Updated: 16:21:25

FortiNAC Adapter View

Physical Address	Device Type	Operating System	IP Address	Host Name	Vendor	Vendor OUI	Source	Rule Name	Device Registered
52:54:00:06:D5:B4	Network	FortiSwitch		S108DVUKOKBLFH25		52:54:00	DHCPv4		
00:50:56:B5:B1:5D	Linux	Fedora based			VMware, Inc.	00:50:56	DHCPv4		
00:50:56:B5:B1:5D	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:75:63	Network	FortiSwitch		S108DVHU33XFNZ99		00:50:56	DHCPv4		
00:50:56:B5:75:63	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:59:0B	Network	FortiSwitch		S108DVJ37QBQYD5		00:50:56	DHCPv4		
00:50:56:B5:59:0B	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:0C:29:78:CF:F7	Windows	Windows 10		DESKTOP-OSNODRU	VMware, Inc.	00:0C:29	DHCPv4		
00:0C:29:78:CF:F7	Windows	Windows 10		DESKTOP-OSNODRU	VMware, Inc.	00:0C:29	DHCPv6		
00:0C:29:78:CF:F7	Server	Windows			VMware, Inc.	00:0C:29	FortiGuard		
00:50:56:B5:6B:BF	Network	FortiSwitch		S108DVQWQKDYA85		00:50:56	DHCPv4		
00:50:56:B5:6B:BF	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:D6:DB	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:3E:D2	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:77:C0	Network	FortiSwitch		S108DVKA2W5EVD06		00:50:56	DHCPv4		
00:50:56:B5:77:C0	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:4A:ED	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:76:06	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		
00:50:56:B5:61:2B	Network	FortiSwitch		S108DVS4ACRXH9D		00:50:56	DHCPv4		
00:50:56:B5:61:2B	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		

0% 244 Updated: 16:23:07

FortiNAC New Endpoint Fingerprints View

Third Party Ecosystem 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

- More than 3000 devices with unique MIB OIDs
 - More than 2000 models including switches, access points, and network controllers
 - More than 90 vendors in networking, security, and communication industries
- with the following vendor and models as examples*.

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, Microsoft Entra ID 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, Armis, Claroty

* 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

Straight Forward Deployment with Seamless Integration

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 on-premise and cloud environments or as hardware appliances, the supported list of hypervisors and Cloud Marketplaces are as:

Hypervisors	Cloud Marketplace
Broadcom VMWare	Microsoft Azure
Microsoft Hyper-V	Amazon AWS
Nutanix	Google GCP
Linux KVM	Oracle OCI
	Alibaba Cloud

The Application and Control Servers can be deployed in a variety of sizes, depending on the number of managed endpoints they need to support. FortiNAC is ideal for supporting 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.

N+1 Failover Group

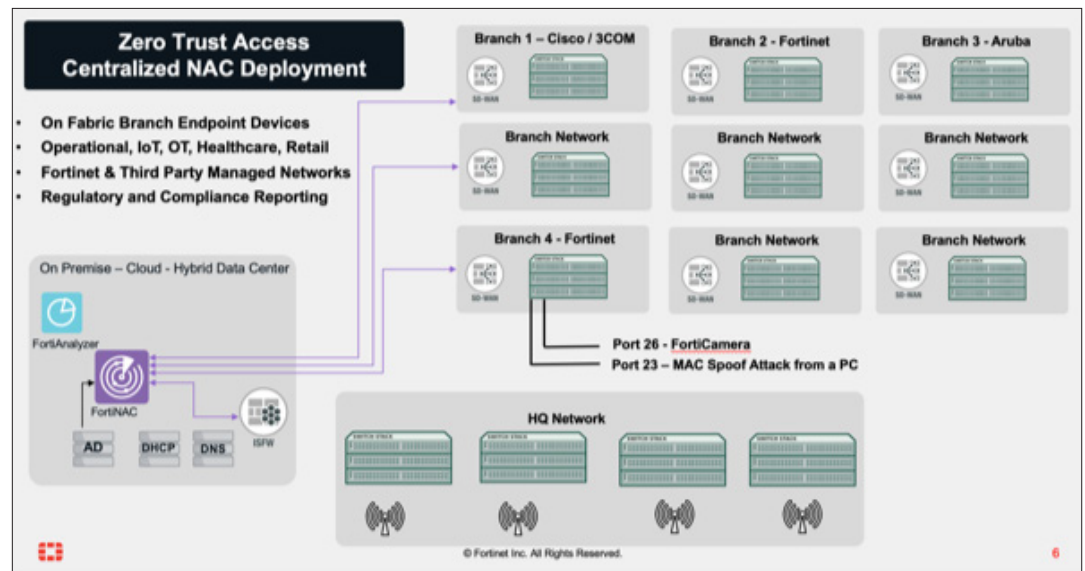
FortiNAC also extend the deployment support to N+1 Failover Group which consist of robust configuration that ensures high availability and redundancy. Can be deployed on shared IP address when all the FortiNAC CAs are in the same subnet for very larger enterprises which are distributed environments. To fully leverage this setup, it's essential to integrate a load balancer to manage traffic distribution and provide automatic failover between the primary and secondary failover group nodes.



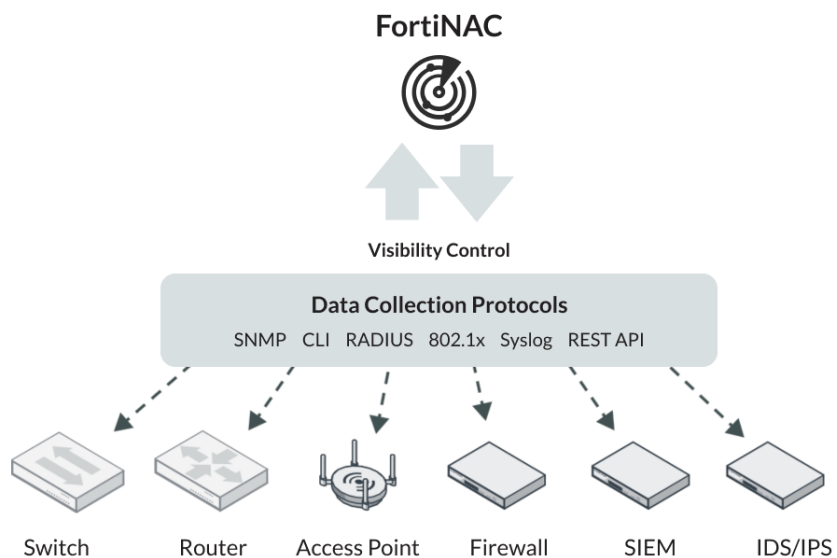
Deployment Options

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.

Plus License

The PLUS license level builds on comprehensive features with enhanced visibility and 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	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓
		Rogue Identification	✓	✓
		Device Profiling and Classification	✓	✓
	Endpoint	Enhanced Visibility	✓	✓
		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

	FNC-M-550F	FNC-CA-600F	FNC-CA-500F	FNC-CA-700F
System				
CPU	AMD EPYC 7413 24 Core, 2.65GHz Base Freq.	AMD EPYC 7413 24 Core, 2.65GHz Base Freq.	Intel Xeon E-2278GE 8 Core, 3.3GHz Base Freq.	AMD EPYC 7543P 32 Core, 2.8GHz Base Freq.
Memory	32GB DDR4 memory	32GB DDR4 memory	16GB DDR4 memory	96GB DDR4 memory
Hard Disk	2× 960GB SSDs	2× 960GB SSDs	2× 960GB SSDs	2× 960GB SSDs
BMC	N/A	N/A	N/A	N/A
Network Interface	1x GbE RJ45 and 4× 10GbE SFP+	1x GbE RJ45 and 4× 10GbE SFP+	4x GbE RJ45	1x GbE RJ45 and 4× 10GbE SFP+
RAID Card	N/A	N/A	N/A	N/A
RAID Configuration	Software RAID1	Software RAID1	Software RAID1	Software RAID1
Console Access	RJ45 type COM port for CLI	RJ45 type COM port for CLI	RJ45 type COM port for CLI	RJ45 type COM port for CLI
Form Factor	1U Rack Mount	1U Rack Mount	1U Rack Mount	1U Rack Mount
Dimensions				
Height x Width x Length (inches)	1.73 × 17.20 × 24	1.73 × 17.20 × 24	1.73 × 17.32 × 19.69	1.73 × 17.20 × 24
Height x Width x Length (mm)	44 × 437 × 610	44 × 437 × 610	44 × 440 × 500	44 × 437 × 610
Weight	41 lbs (18.6 kg)	41 lbs (18.6 kg)	32 lbs (14.51 kg)	41 lbs (18.6 kg)
Environment				
Power Supply	Hot Plug, 1+1 Redundant PSU	Hot Plug, 1+1 Redundant PSU	Hot Plug, 1+1 Redundant PSU	Hot Plug, 1+1 Redundant PSU
Input Power	225 watt	225 watt	174 Watt	375 Watt
Input Current	2.3A@100V, 0.94A@240V	2.3A@100V, 0.94A@240V	1.5A@100V; 0.625A@240V	3.75A@100V, 1.57A@240V
Cooling	5x system fans	5x system fans	4x system fans	5x system fans
Panel Display	N/A	N/A	N/A	N/A
Heat Dissipation	767.73 BTU/h	767.73 BTU/h	511.82 BTU/h	1279.553112375 BTU/h
Operation Temperature Range	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature Range	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)
Humidity (Operating)	5% to 90% non-condensing	5% to 90% non-condensing	5% to 90% non-condensing	5% to 90% non-condensing
Humidity (Non-operating)				
Certification				
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), and European Union (CE).			
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), and 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

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



Hardware Server Sizing

Appliance



HARDWARE			
Hardware Server	Type	Target Environment	Capacity ¹
FortiNAC-CA-500F	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 15 000 endpoints
FortiNAC-CA-600F	High Performance Control and Application Server	Medium Environments	Manages up to 30 000 endpoints
FortiNAC-CA-700F	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 50 000 endpoints
FortiNAC-M-550F	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Can manage up to 100 CA servers with latencies up to 600ms in lab environment

¹ Managed Endpoints = Endpoint devices registered, managed, and enforced by FortiNAC.

VM Server Resource Sizing

Virtual



VIRTUAL MACHINE							
VM OS	SKU	Managed Endpoints ¹	Target Environment	CPU Reference	vCPU Qty ²	Memory (GB)	Disk (GB)
FortiNAC-OS	FNC-CAX-VM	Up to 15 000	Small	Intel Xeon E-2278 GE 3.3 GHz 8C/16T	8	16	100
		Up to 30 000	Medium	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100
		Up to 50 000	Large	AMD Milan EPYC 7543P 2.8 GHz 32C/64T	32	96	100
	FNC-MX-VM	Up to 100 CA Servers	Large	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100

¹ Managed Endpoints = total of endpoint devices registered, managed, and enforced.

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.

Performance and Scalability

MANAGED DEVICES, SCALABILITY, GUEST SERVICES, AND PROTOCOLS						
Hardware Server	VM-Small	VM-Medium	VM-Large	FortiNAC-CA-500F	FortiNAC-CA-600F	FortiNAC-CA-700F
Managed Endpoints	15 000	30 000	50 000	15 000	30 000	50 000
Managed FortiGates	2800	4400	5600	3100	4700	6300
FortiGate w/ FortiSwitch (FortiLink)	650 and 650	900 and 900	980 and 980	650 and 650	950 and 900	1100 and 1000
Guest Web Login (Auth / Sec)	35	70	80	100	102	105
Guest Self Registration (Request / Sec)	20	21	22	20	21	22
Netflow (Request / Sec)	400	400	400	400	400	400
Syslog (Request / Sec)	90	90	90	90	90	90
REST API (Request / Sec)	480	480	480	1100	1100	1100

RADIUS PERFORMANCE (REQUEST / SECOND)								
Auth. Outer Method	Auth. Inner Method	Auth Source	VM-Small	VM-Medium	VM-Large	FortiNAC-CA-500F	FortiNAC-CA-600F	FortiNAC-CA-700F
PAP	N/A	Local Database	550	1200	1290	290	900	1050
PAP	N/A	Active Directory	1200	1300	1340	900	1100	1200
PEAP	EAP-GTC	Local Database	270	270	270	230	900	1100
PEAP	EAP-GTC	Active Directory	270	270	270	830	1500	1600
PEAP	EAP-MSCHAPv2	Local Database	300	310	310	900	1400	1500
PEAP	EAP-MSCHAPv2	Active Directory	165	163	194	140	148	152
EAP-TTLS	EAP-GTC	Local Database	340	320	317	230	880	1100
EAP-TTLS	EAP-GTC	Active Directory	321	319	314	850	1700	1800
EAP-TTLS	EAP-MSCHAPv2	Local Database	310	314	310	910	1100	1500
EAP-TTLS	EAP-MSCHAPv2	Active Directory	162	167	179	140	145	150
EAP-TLS	N/A	Local Database	381	352	348	850	1450	1500
EAP-TLS	N/A	Active Directory	372	346	341	850	1450	1500
MAB	N/A	Local Database	536	1724	1676	960	1380	1500

FORTINAC MANAGER		
	FortiNAC-M-550F	FortiNAC-MX-VM
Manager N+1 Failover Group Active Nodes	4	4
Manager N+1 Failover Group Stand-by Units	1	1
Max CA Stand-Alone per Node	100	100
Max CA High-Availability (1+1 Pair) per Node	100	100
Max CA N+1 Failover Group Active per Node	100	100

In the context of max CA capacity for FortiNAC manager, the system counts only active CAs.

Therefore High-Availability 1+1 counts as 1, and an N+1 failover group counts as N, because the standby node only receives health checks.



Ordering Information

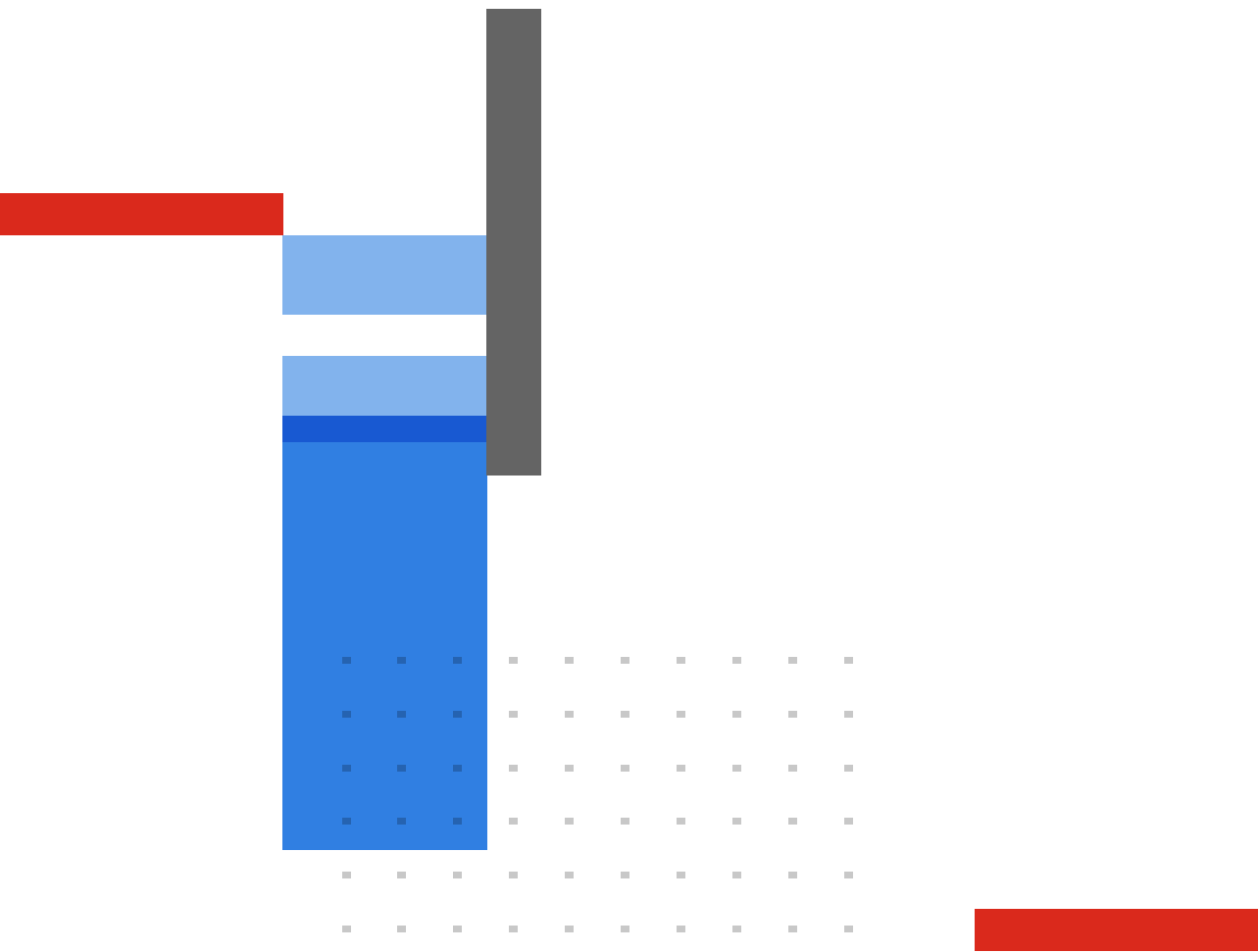
PRODUCT	SKU	DESCRIPTION
Appliances		
FortiNAC-CA-500F	FNC-CA-500F	FortiNAC Network Control and Application Server (F Series).
FortiNAC-CA-600F	FNC-CA-600F	FortiNAC High Performance Network Control and Application Server (F Series).
FortiNAC-CA-700F	FNC-CA-700F	FortiNAC Ultra High Performance Network Control and Application Server (F Series).
FortiNAC-M-550F	FNC-M-550F	FortiNAC Network Manager (F Series).
Virtual Machines		
FortiNAC Control and Application extended VM	FNC-CAX-VM	FortiNAC Control and Application eXtended VM Server (Running FortiNAC-OS).
FortiNAC Manager extended VM	FNC-MX-VM	FortiNAC Manager eXtended VM Server (Running FortiNAC-OS).
Perpetual Licenses		
FortiNAC PLUS License 100	LIC-FNAC-PLUS-100	FortiNAC Perpetual PLUS License for 100 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 1K	LIC-FNAC-PLUS-1K	FortiNAC Perpetual PLUS License for 1K concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 10K	LIC-FNAC-PLUS-10K	FortiNAC Perpetual PLUS License for 10K concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 50K	LIC-FNAC-PLUS-50K	FortiNAC Perpetual PLUS License for 50K concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PRO License 100	LIC-FNAC-PRO-100	FortiNAC Perpetual 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 Perpetual 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 Perpetual 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 Perpetual PRO License for 50K concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.
Subscription Licenses		
FortiNAC Subscription PLUS License	FC5-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 100 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices. MOQ 500
	FC6-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 1000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
	FC7-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 10 000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
	FC8-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 50 000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC Subscription PRO License	FC5-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 100 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response. MOQ 500
	FC6-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 1000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.
	FC7-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 10 000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.
	FC8-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 50 000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.