FortiNAC is Fortinet’s network access control solution that enhances the Fortinet Security Fabric with visibility, control, and automated response for everything that connects to the network. With FortiNAC, you can implement microsegmentation policies and change configurations on switches and wireless products from 95 vendors. FortiNAC is available with the following FortiCare offerings:

**FortiCare Services**

As a customer’s business rapidly evolves, advancing its security capabilities is critical as well. Often, the customer does not have expertise within their organization to deploy, operate, and maintain these new capabilities or are up against tight deadlines to implement change. Fortinet understands this challenge and helps thousands of organizations every year tackle this problem with FortiCare Services. Fortinet’s experts provide accelerated implementation of the customer’s technology, reliable assistance through advanced support, and proactive care to ensure the customer’s success with Fortinet investment. No matter the size or location of the customer’s organization, Fortinet is ready to provide the customer with an elevated experience to help them achieve their business goals with superior security and performance.

**FortiCare Support**

A FortiCare Support contract entitles the customer not only to receive updates to the FortiNAC firmware, but also receive the following important feeds:

- **Network device database update**: FortiNAC supports more than 2400 switching, wireless, or firewall devices on the market. As new devices release, FortiNAC’s network device database should be updated to reflect these new models. The weekly update from the FortiNAC team keeps the customer’s deployment up to date.

- **FortiGuard IoT Service**: a method that FortiNAC has to identify devices is to use the cloud lookup service that FortiGuard Labs hosts. A FortiCare Support contract entitles the customer to use that service at no additional cost, giving them access to a database of millions of devices.
# PRODUCT OFFERINGS

<table>
<thead>
<tr>
<th>Feature</th>
<th>BASE</th>
<th>PLUS</th>
<th>PRO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Discovery</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Rogue Identification</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Device Profiling and Classification</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Visibility</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced Visibility</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MDM Integration</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Persistent Agent</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Endpoint</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Access Policies</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IoT Onboarding with Sponsor</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Rogue Device Detection and Restriction</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Firewall Segmentation</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>MAC Address Bypass</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Full RADIUS (EAP)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>BYOD/Onboarding</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Guest Management</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Endpoint Compliance</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Automation/Control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Captive Portal</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Incident Response</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Correlation</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Extensible Actions and Audit Trail</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Alert Criticality and Routing</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Guided Triage Workflows</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Integrations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound Security Events</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Outbound Security Events</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>REST API</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customizable Reports</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
### ORDERING INFORMATION

<table>
<thead>
<tr>
<th></th>
<th>BASE</th>
<th>PLUS</th>
<th>PRO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perpetual Licenses</strong>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100 Endpoints</td>
<td>LIC-FNAC-BASE-100</td>
<td>LIC-FNAC-PLUS-100</td>
<td>LIC-FNAC-PRO-100</td>
</tr>
<tr>
<td>1000 Endpoints</td>
<td>LIC-FNAC-BASE-1K</td>
<td>LIC-FNAC-PLUS-1K</td>
<td>LIC-FNAC-PRO-1K</td>
</tr>
<tr>
<td>10000 Endpoints</td>
<td>LIC-FNAC-BASE-10K</td>
<td>LIC-FNAC-PLUS-10K</td>
<td>LIC-FNAC-PRO-10K</td>
</tr>
<tr>
<td><strong>Subscription Licenses</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25 Endpoints</td>
<td>FC1-10-FNAC1-213-01-DD</td>
<td>FC1-10-FNAC1-213-01-DD</td>
<td>FC2-10-FNAC1-209-01-DD</td>
</tr>
<tr>
<td>500 Endpoints</td>
<td>FC2-10-FNAC1-213-01-DD</td>
<td>FC2-10-FNAC1-209-01-DD</td>
<td>FC3-10-FNAC1-209-01-DD</td>
</tr>
<tr>
<td>2000 Endpoints</td>
<td>Coming Soon</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10000 Endpoints</td>
<td>FC3-10-FNAC1-213-01-DD</td>
<td>FC3-10-FNAC1-213-01-DD</td>
<td>FC4-10-FNAC1-209-01-DD</td>
</tr>
</tbody>
</table>

#### Hardware Appliances

**SMB (up to 2000 network ports)**
- FC-10-NC500-247-02-DD
- FC-10-NC500-247-02-DD
- FC-10-NC500-247-02-DD

**Mid Enterprises (up to 15000 network ports)**
- FC-10-NC600-247-02-DD
- FC-10-NC600-247-02-DD
- FC-10-NC600-247-02-DD

**Large Enterprises (up to 25000 network ports)**
- FC-10-NC700-247-02-DD
- FC-10-NC700-247-02-DD
- FC-10-NC700-247-02-DD

**Management Appliance (optional unlimited network ports)**
- FC-10-NC500-247-02-DD
- FC-10-NC500-247-02-DD
- FC-10-NC500-247-02-DD

#### Virtual Appliances

**SMB (up to 2000 network ports)**
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD

**Mid Enterprises (up to 15000 network ports)**
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD

**Large Enterprises (up to 25000 network ports)**
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD

**Management Appliance (optional unlimited network ports)**
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD
- FC-10-FNVX-200-02-DD

### Hardware Product

**FortiNAC 500, Network Control and Application Server with RAID and Redundant Power Supplies, for up to 2,000 total ports**
- FNC-CA-500C
- FNC-CA-600C
- FNC-CA-700C
- FNC-M-550C

**FortiNAC 600, High Performance Network Control and Application Server with RAID and Redundant Power Supplies, for up to 15,000 total ports**
- FNC-CA-500C
- FNC-CA-600C
- FNC-CA-700C

**FortiNAC 700, Ultra High Performance Network Control and Application Server with RAID and Redundant Power Supplies, for up to 25,000 total ports**
- FNC-CA-500C
- FNC-CA-600C
- FNC-CA-700C
- FNC-M-550C

**FortiNAC Manager 550, Network Manager with RAID and Redundant Power Supplies**
- FNC-CA-500C
- FNC-CA-600C
- FNC-CA-700C
- FNC-M-550C

### Virtual Appliance

**FortiNAC Control and Application VM Server (VMware/ Hyper-V/AWS/Azure/KVM)**
- FNC-CAX-VM
- FNC-MX-VM

**FortiNAC Manager VM Server (VMware or Hyper-V)**
- FNC-CAX-VM
- FNC-MX-VM

### FortiCare Support for FortiNAC Perpetual Licenses

**License Model**
- 24x7 FortiCare Contract (100 Endpoints) for FortiNAC BASE deployments
- FC1-10-FNAC0-240-02-DD
- FC2-10-FNAC0-240-02-DD
- FC3-10-FNAC0-240-02-DD
BILL OF MATERIAL EXERCISES

Exercise 1
A manufacturing customer is interested in NAC for their factory in twelve cities across the U.S. They are interested in visibility only of the network, their PLC controllers and devices, and any computers connected to their manufacturing environment. The customer knows they have many unmanaged hubs and switches they must replace over time but do not know where they exist. The customer is focused on cloud-based solutions in two Azure datacenters and all twelve sites have robust connectivity to Azure. The customer's infrastructure is all Cisco hardened switches and a FortiGate firewall at the edge. Meraki APs provide wireless. Customer estimates about 8400 active devices across all twelve sites and wants a single pane of glass to manage NAC. The customer has capital expense money in this year's budget but wants a 3 year cost. Their partner will provide the installation services.

The customer needs the following bill of material (BoM):

High availability (HA) FortiNAC control application VM, one VM in each data center with FortiCare for 36 months:
2x FNC-CAX-VM
2x FC-10-FNVXA-248-02-36
8400 FortiNAC base license with FortiCare for 36 months:
8x LIC-FNAC-BASE-1K
4x LIC-FNAC-BASE-100
84x FC1-10-FNAC0-240-02-36

Exercise 2
A medium-sized global bottle manufacturing company is concerned about IoT creep in their manufacturing networks and recently had a ransomware breach in their European office due to a third party contractor that brought malware into their system. They are going all-in on Fortinet's Security Fabric solution. The U.S. account manager is working with their counterparts in EMEA and APAC to develop a solution that each region locally manages (Americas, EMEA, and APAC) but delivers reporting at a global level. The customer is purchasing FortiGates, FortiEDR, FortiClient EMS, and FortiSIEM in addition to FortiNAC. They want integration across all products. They found their old SIEM solution notified them of the breach, but they did not see the alerts until it was too late. Security automation is of the utmost desire. The customer has plenty of capital expenses but wants 24 month costs to align with their global strategic finance partnerships. The partner did an assessment and determined about 3000 licenses and 2000 ports consumed equally between regions would be needed and the customer will run in their own datacenters in each region but wants an all-hardware appliance solution with HA and next day RMA services and needs budgeting for three years of FortiCare. Their partner will provide the installation services.

The customer needs the following BoM:

1x HA Cluster of FNAC Manager
2x FNC-M-550C
2x FC-10-NC550-247-02-36
2x FC-10-NC550-210-02-36

3x HA Clusters of FNAC Control and Application
6x FNC-CA-500C
6x FC-10-NC500-247-02-36
6x FC-10-NC500-210-02-36

3000 Subscription Pro licenses
4x FC3-10-FNAC1-209-01-24
BILL OF MATERIAL EXERCISES

Exercise 3
A transportation company with trains operating between 700 stations in the regions has always deployed FortiNAC for visibility of all their connected devices at each station and for control of the device access to the network. They have bought the Plus license. As they are getting mature in their security journey, they are ready to take a step further. They not only want visibility and access control but automated response and remediation as well so they can take action quickly and more effectively toward security risks and reduce the manual process by IT teams. The customer has six regional data centers and two core data centers. All the management plane is in the core data centers in HA and the control network services are distributed between the six regional data centers. The administrative center has around 2000 employees. The partner has provided the assessment and the customer environment is based on 4500 connected devices between LAN and wireless, 7500 IoT devices, and they want to provide a guest network for up to 1000 connected devices. The customer is looking for HA in all regional and core sites with a year of FortiCare.

The customer needs the following BoM:

HA cluster of FortiNAC Manager VM for the core data center with FortiCare for 12 months:
- 2x FNC-MX-VM
- 2x FC-10-FNVXVM-248-02-12

HA clusters of FortiNAC CA VM for each regional data center with FortiCare for 12 months:
- 12x FNC-CAX-VM
- 12x FC-10-FNVXA-248-02-12

13000 FortiNAC Plus license with FortiCare for 12 months:
- 3x LIC-FNAC-PLUS-1K
- 1x LIC-FNAC-PLUS-10K
- 130x FC2-10-FNAC0-240-02-12

Exercise 4
A retail company has 1700 stores nationwide. They deployed FortiNAC CA VM at one data center to manage ten store locations as the first trial phase with roughly 1000 devices to support. They like the way FortiNAC provides them with the instant device and user visibilities. Now, they are ready to expand the deployment into all 1700 stores including 170000 devices to cover with a Plus FortiCare license of 12 months. The stores have the reliable FortiGate SD-WAN solution to provide the data connection with two data centers. The customer wants to have the hardware-based offering with the HA cluster.

The customer needs the following BoM:

HA cluster of FortiNAC Manager hardware-based with FortiCare for 12 months:
- 2x FNC-M-550C
- 2x FC-10-NC550-247-02-12
- 2x FC-10-NC550-210-02-12

HA clusters of FortiNAC CA 700C large deployment unit for up to 25000 total ports for each regional data center with FortiCare for 12 months:
- 14x FNC-CA-700C
- 14x FC-10-NC700-247-02-12
- 14x FC-10-NC550-210-02-12

170000 FortiNAC Plus licenses with FortiCare for 12 months:
- 3x LIC-FNAC-PLUS-50K
- 2x LIC-FNAC-PLUS-10K
- 1700x FC2-10-FNAC0-240-02-12
VIRTUAL APPLIANCES

Fortinet has introduced a new generation of FortiNAC virtual appliances that come with new features, such as the following:

- New FortiNAC operating system
- New internal database
- Cloud deployment enhancements
- New UI workflows of policy creation for:
  - EasyConnect
  - Endpoint compliance
  - Network access policy
  - Authentication policy
  - Captive web portals
  - User host profiles

The SKUs for the next generation of FortiNAC VMs are available for Control and Application and Manager. The customer can choose the new SKU schema as follows:

<table>
<thead>
<tr>
<th>FORTINAC CONTROL AND APPLICATION</th>
<th>FORTINAC MANAGER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Old</td>
</tr>
<tr>
<td>VM Server</td>
<td>FNC-CA-VM</td>
</tr>
<tr>
<td>FortiCare</td>
<td>FC-10-NCVCA-248-02-DD</td>
</tr>
</tbody>
</table>

1. Customers can still buy the current VM in the following cases:
   - Expansion of their current deployment
   - New deployment where the current VM’s capabilities are satisfactory
   - If they want a combination of hardware appliances and virtual appliances to have the same underlying software infrastructure (operating system and database) across the deployment

2. All new customers should consider next-generation VM only.