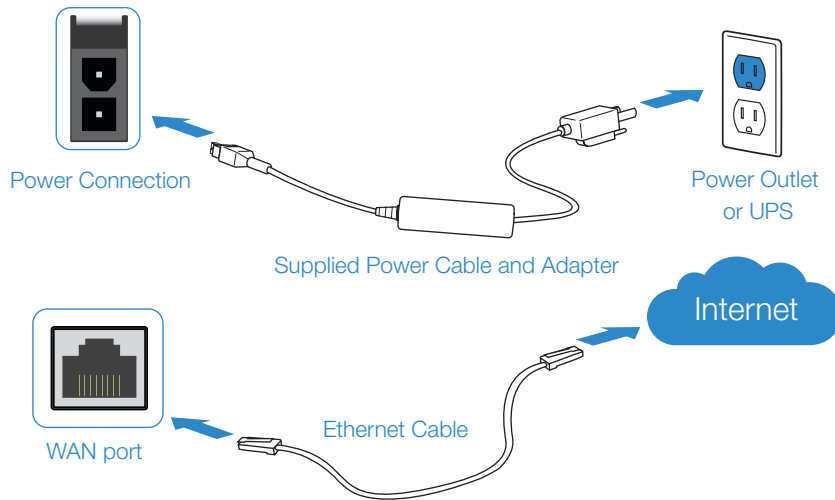


# Installation

Your FortiGate/FortiWiFi includes a wall mount kit and connection cables. Desktop installation, rack mount and slide-rail kits are also available.

## Basic Connections



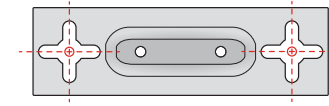
1. Plug in your device to power outlet using the provided power adapter & cable
2. Connect a WAN port to the internet using the supplied Ethernet cable

**Note:** We recommend connecting your FortiGate to an uninterruptible power supply (UPS) in case of a power outage

**Optional:** The FortiGate/FortiWiFi 80F/81F Series have optional dual DC inputs for failover redundancy. If both DC inputs are used, only one is active. If the active DC input fails, the second input will be active.

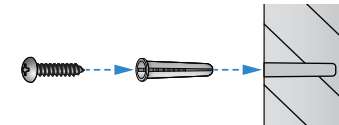
## Wall Mount Option

1. Mark the location of the holes using the mounting bracket

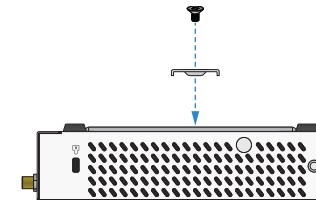


2. Drill holes for the anchors

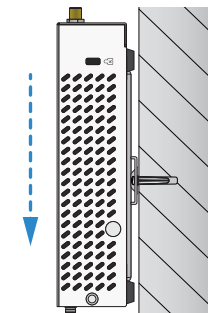
3. Insert the anchors and then screw in the screws with 2mm exposed



4. Fasten the mounting bracket



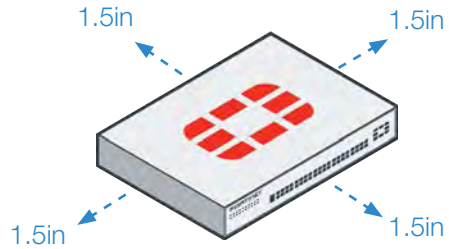
5. Position the device and slide into place



6. Plug the provided power cable into the rear of the unit and then into a grounded electrical outlet or separate power source

## Desktop Option

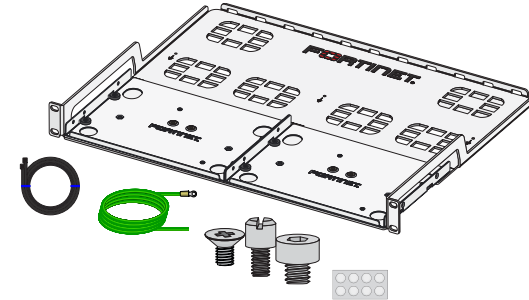
1. Place the unit on a flat, clean and stable surface
2. Ensure there is at least 1.5in of clearance for adequate airflow



3. Plug the provided power cable into the rear of the unit and then into a grounded electrical outlet or separate power source
- 

## Rack/Rail Mount Option

Fortinet carries a variety of standard and custom rack and rail mount accessories, including a rack mount tray kit, SP-RACKTRAY-02.



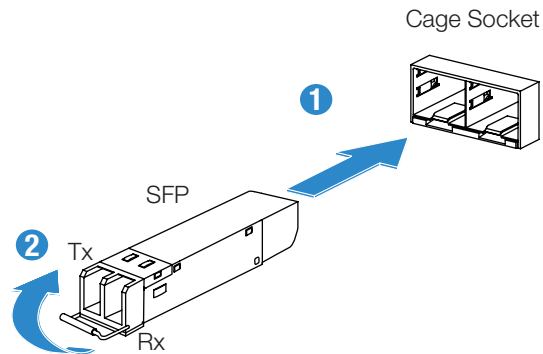
SP-RACKTRAY-02

**Ordering:** Contact Fortinet to order brackets, rail slide kits, rack mount kits and other accessories, such as a console cable

## SFP Ports

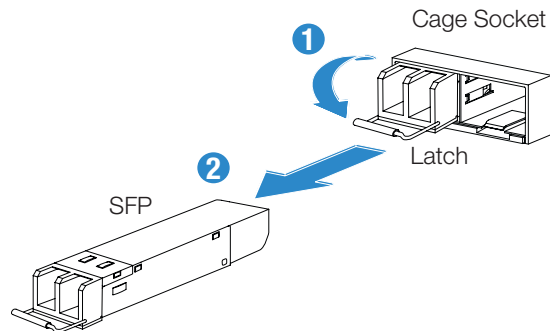
To install the SFP transceivers

1. Slide the SFP into the cage socket until it clicks into place
2. Lift the latch to lock the SFP



To remove the SFP transceivers

1. Lower the latch to unlock the SFP
2. Carefully pull the SFP out of the cage socket



For additional info on SFP's, visit:

[support.fortinet.com](https://support.fortinet.com)

## Setup Options

Set up your device locally or on the cloud. Choose one of the following options to complete your setup, then configure your device.



### A GUI

An **easy-to-use GUI**, compatible with most web browsers. To minimize scrolling, the screen resolution should be at least 1280 x 1024 pixels.



### B FortiGate Cloud

FortiGate Cloud is a **cloud-based** infrastructure management solution and log retention service. It provides **centralized reporting**, **traffic analysis**, **configuration management**, and **log retention** without the need for additional hardware and software.



### C FortiExplorer

FortiExplorer for iOS is a **user-friendly iOS application** that helps you **configure**, **manage**, and **monitor** appliances. FortiExplorer rapidly provisions, deploys, and monitors Security Fabric components such as **FortiGate**, **FortiWiFi**, and **FortiAP** devices.



### D Command Line Interface (CLI)

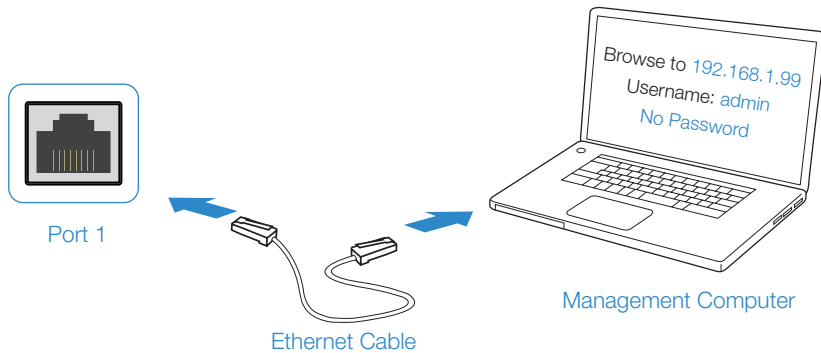
An alternate configuration tool from the web-based manager that uses a **terminal emulation** application to **type commands** or upload batches of commands from a text file or **configuration script**. Requires a console cable (available for purchase).

1. Connect **port 1** to the **Management Computer** using the supplied **Ethernet cable**

2. Enable **DHCP** or set the Management Computer's **IP** and **subnet** to:

**Static IP Address:** 192.168.1.1  
**Subnet Mask:** 255.255.255.0

3. Visit **192.168.1.99** in a web browser



4. Log in with username **admin** and **no password**

The screenshot shows a login interface with a green header. It contains two input fields: 'Username' and 'Password'. Below the fields is a green 'Login' button.

5. When prompted to register, enter your **Fortinet credentials**

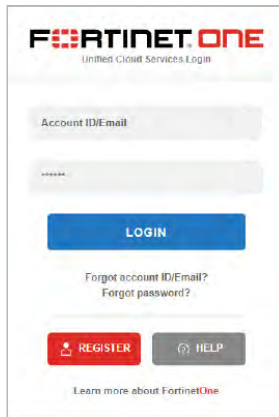
The screenshot shows a 'FortiCare Registration Required' dialog box. It displays the Serial Number 'FG800D3915800295' and offers 'Login' and 'Create Account' actions. There are input fields for Email, Password, Country, and Reseller, along with a 'Forgot your password?' link and 'OK' and 'Cancel' buttons.

6. The **FortiCare Support Status** in the FortiOS License Information widget will change to **Registered**

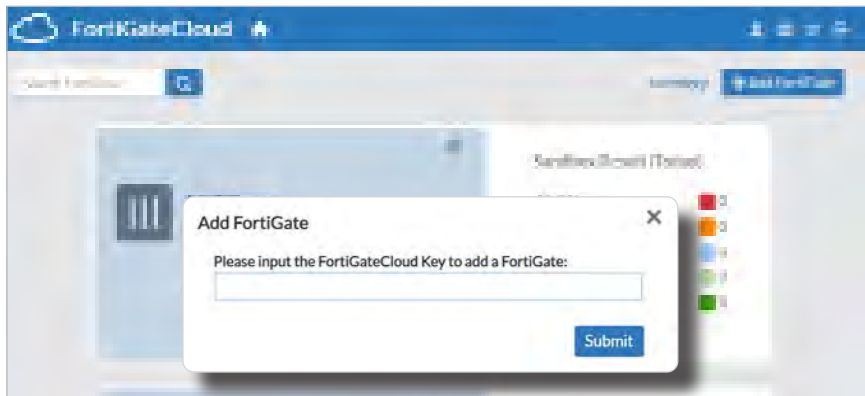
The screenshot shows the 'License Information' widget in FortiOS. It contains a table with columns for 'Entitlement' and 'Status'. The 'FortiCare Support' row is highlighted with a red box and shows a status of 'Registered' with a green checkmark.

Entitlement	Status
FortiCare Support	Registered
Enhanced Support	8x5 support - expires on 2020/03/08
Virtual Machine	Valid - expires on 2020/03/06
Allocated vCPUs	25% 1 / 4
Allocated RAM	1002 MiB
Firmware & General Updates	Licensed - expires on 2020/03/08
Application Control Signatures	Version 6.00741
Device & OS Identification	Version 1.00084
Internet Service Database Definitions	Version 7.00109
Intrusion Prevention	Licensed - expires on 2020/03/08
IPS Definitions	Version 6.00741
IPS Engine	Version 5.00031
Malicious URLs	Version 2.00430
Botnet IPs	Version 1.00000

1. Log in to [forticloud.com](http://forticloud.com) using your Fortinet credentials



2. Click **Add FortiGate** and enter the **Cloud Key** located on the **sticker** on your device

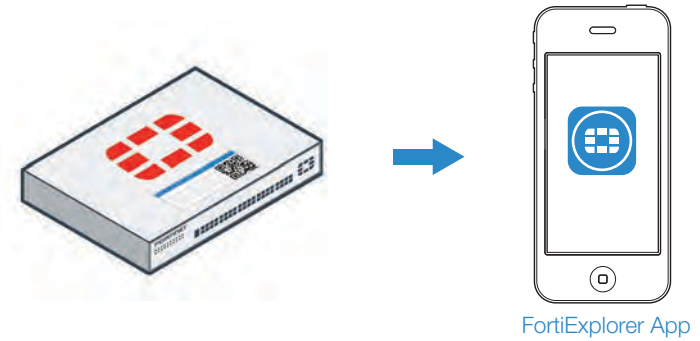


3. You can now manage your device from the cloud

**Note:** To get a [Fortinet account](http://support.fortinet.com), register at [support.fortinet.com](http://support.fortinet.com)

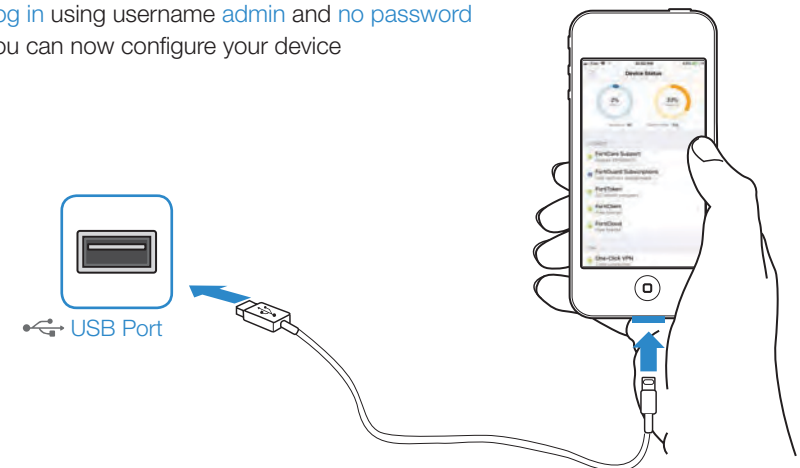
### 1 Cloud Key Setup

1. **Download** and launch the [FortiExplorer iOS App](#)
2. Tap **Devices**, then tap **Add**
3. Select **FortiGate Cloud** and log in using your [Fortinet credentials](#)
4. **Scan** the **QR code** on the Cloud Key
5. **Log in** to your device using username **admin** and **no password**
6. You can now configure your device

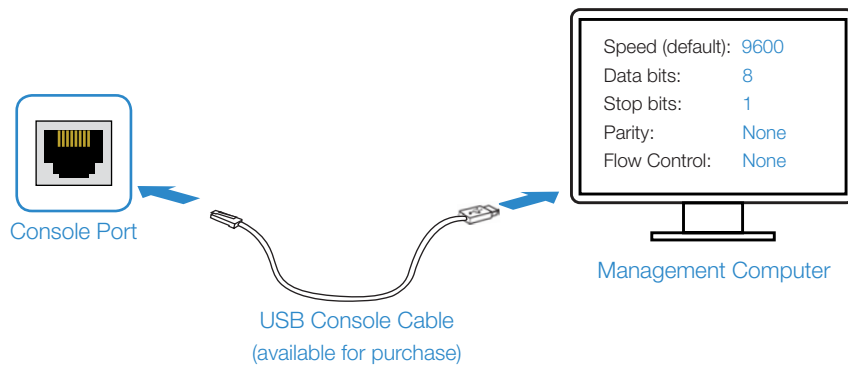


### 2 USB Setup

1. **Download** and launch the [FortiExplorer iOS App](#)
2. Connect your **Apple Lightning to USB cable** to the FortiGate/FortiWiFi **USB port**
3. **Tap** your device when it appears in [FortiExplorer](#)
4. **Log in** using username **admin** and **no password**
5. You can now configure your device



## D CLI



1. Connect the [Console Port](#) with a [console cable](#) to the [Management Computer](#)
2. Start a [terminal program](#) on the [Management Computer](#) and select an available [COM Port](#) using the following default settings:

**Baud rate:** 9600  
**Data bits:** 8  
**Parity:** None  
**Stop bits:** 1  
**Flow control:** None

3. Log in using username [admin](#) and [no password](#)
4. You can now configure your device

```
FortiGate # ?
config      Configure object.
get         Get dynamic and system information.
show       Show configuration.
diagnose   Diagnose facility.
execute    Execute static commands.
exit       Exit the CLI.

FortiGate # config ?
alertemail Alert email configuration.
antivirus  AntiVirus configuration.
application Application control configuration.
client-reputation Client reputation tracking configuration
dlp        DLP configuration.
endpoint-control Endpoint control configuration.
firewall   Firewall configuration.
ftp-proxy  FTP proxy configuration.
gui        GUI configuration.
icap       ICAP client configuration.
imp2p      IM & P2P policy configuration.
ips        IPS configuration.
--More--
```

**Note:** Type [?](#) for a [list of commands](#). Type a command with [?](#), such as [config ?](#) to list the options. For advanced options, visit [support.fortinet.com](#)

## Resources

Refer to the following resources to continue your FortiGate setup.

### FortiGate Documentation Library

Up-to-date hardware and software guides

<https://docs.fortinet.com/fortigate>

### Fortinet Customer Service & Support

Access knowledge bases, resource libraries and contact support

<https://support.fortinet.com/>

### Fortinet Video Tutorials

FortiOS Tips, Web GUI tutorials, SD-WAN tricks and more

<http://video.fortinet.com>

### FortiGuard Labs

Discover FortiGuard's Zero-Day Research, Weekly Threat Briefs and Threat Lookups

<https://fortiguard.com/>

### FortiGate Cloud

Analyze centralized reporting, traffic analysis, configuration management and logs

<https://forticloud.com>

## Register for Free Licenses & Services

Simplify and leverage provisioning, management, and analytics with FortiGate Cloud's centralized administration. Extend online logs and analysis to 1 full year with a subscription.

### FortiGate Cloud 7 Days of Data Retention

Make remote access simple. Use [yourcompany.fortiddns.com](https://yourcompany.fortiddns.com) instead of a hard-to-remember IP address.

### Fortinet DDNS Service



Enable two-factor authentication for remote access using mobile devices. Available for iOS and Android devices. Get extra tokens from your Fortinet reseller.

### 2 FortiToken Mobile Licenses

## Services with FortiCare Subscriptions

Global 24/7 support for your Fortinet hardware & software

Get the latest product security updates and features. Stay with us and see the product evolve.

### Firmware Updates

Use cellphone technology as backup Internet connection. We are always adding support for new third party 3G/4G+ devices.

### USB Modem Database Updates

Set up policies and track activities based on geography. Your **FortiGate** will intelligently identify where an IP is originated or destined.

### Geo-IP Database Updates

Create policies to allow, deny, or restrict access to applications or entire categories of applications. You can use application control to keep malicious, risky, and unwanted applications out of your network.

### Application Control Database Updates

Identify device type and OS information. Great for organizations who want to enforce device-based policies so that employees can bring in their devices.

### Device Signatures Database Updates

Internet service database objects consist of IP addresses, port numbers, and protocols used by Internet services. Simplify the management and control of cloud-based applications.

### Internet Service Database Updates



## Fortinet Bundled Services with FortiCare

Fortinet Bundled Services	360 Protection	Enterprise Protection	UTM	Threat Protection
FortiCare	ASE	24x7	24x7	24x7
FortiGuard App Control Service	✓	✓	✓	✓
FortiGuard IPS Service	✓	✓	✓	✓
FortiGuard Advanced Malware Protection (AMP)	✓	✓	✓	✓
FortiGuard Web Filtering Service	✓	✓	✓	
FortiGuard Anti-Spam Service	✓	✓	✓	
FortiGuard Security Rating Service	✓	✓		
FortiGuard Industrial Service	✓	✓		
FortiCASB SaaS-only Service	✓	✓		
FortiConverter Service	✓			
SD-WAN Cloud Assisted Monitoring	✓			
SD-WAN Overlay Controller VPN Service	✓			
FortiAnalyzer Cloud	✓			
FortiManager Cloud	✓			

# The Fortinet Security Fabric

## Broad

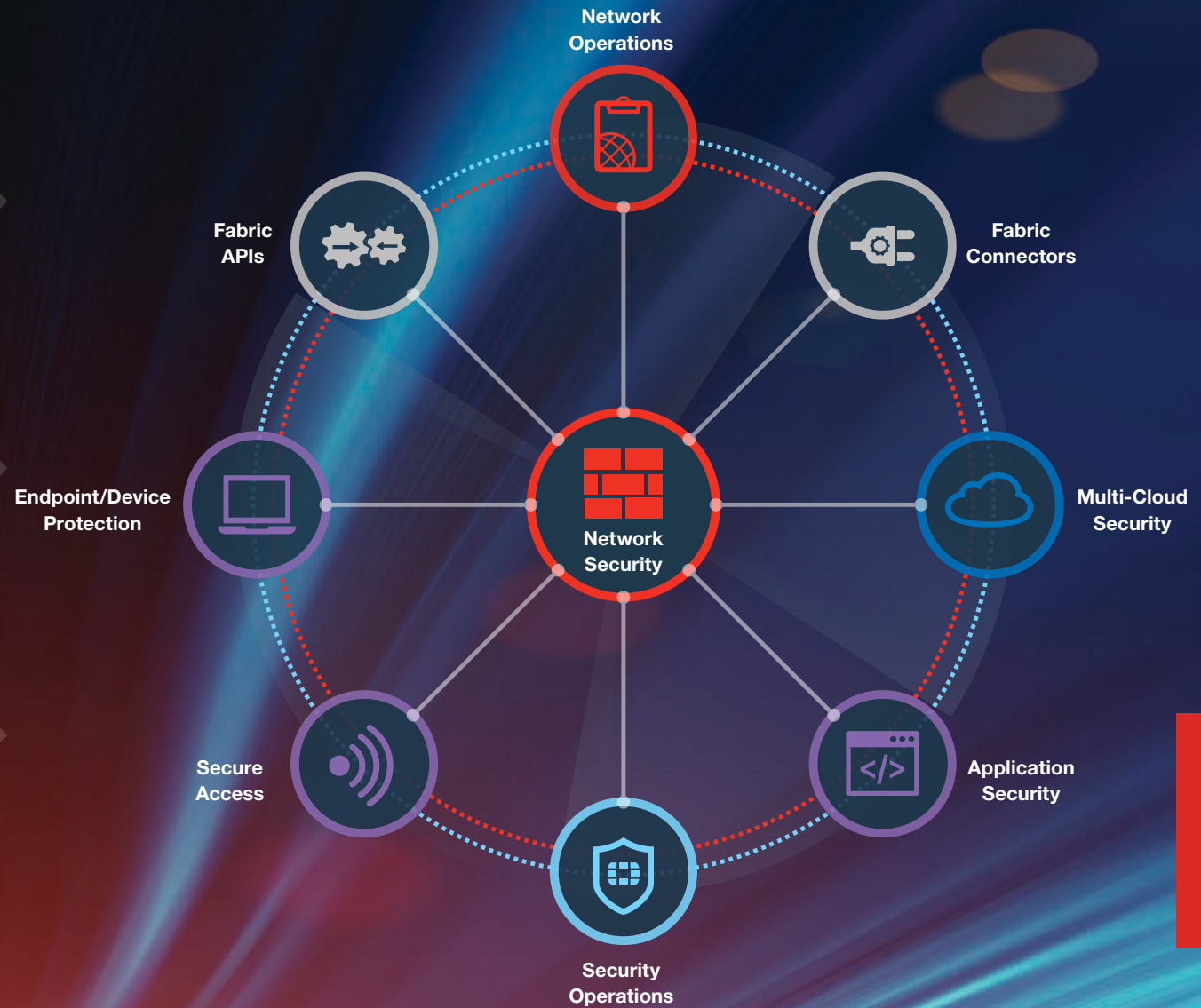
Visibility of the entire digital attack surface

## Integrated

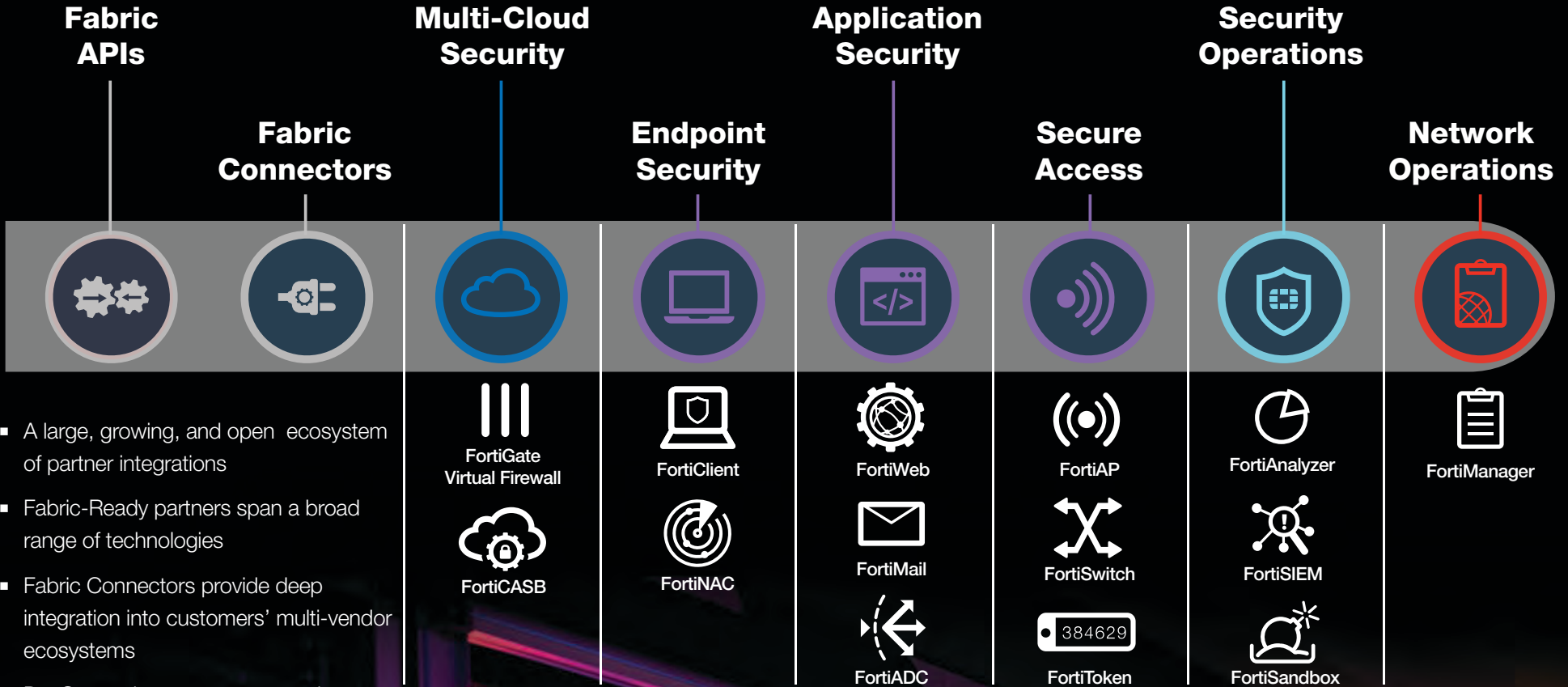
AI-driven breach prevention across all devices, networks, and applications

## Automated

Operations, orchestration and response



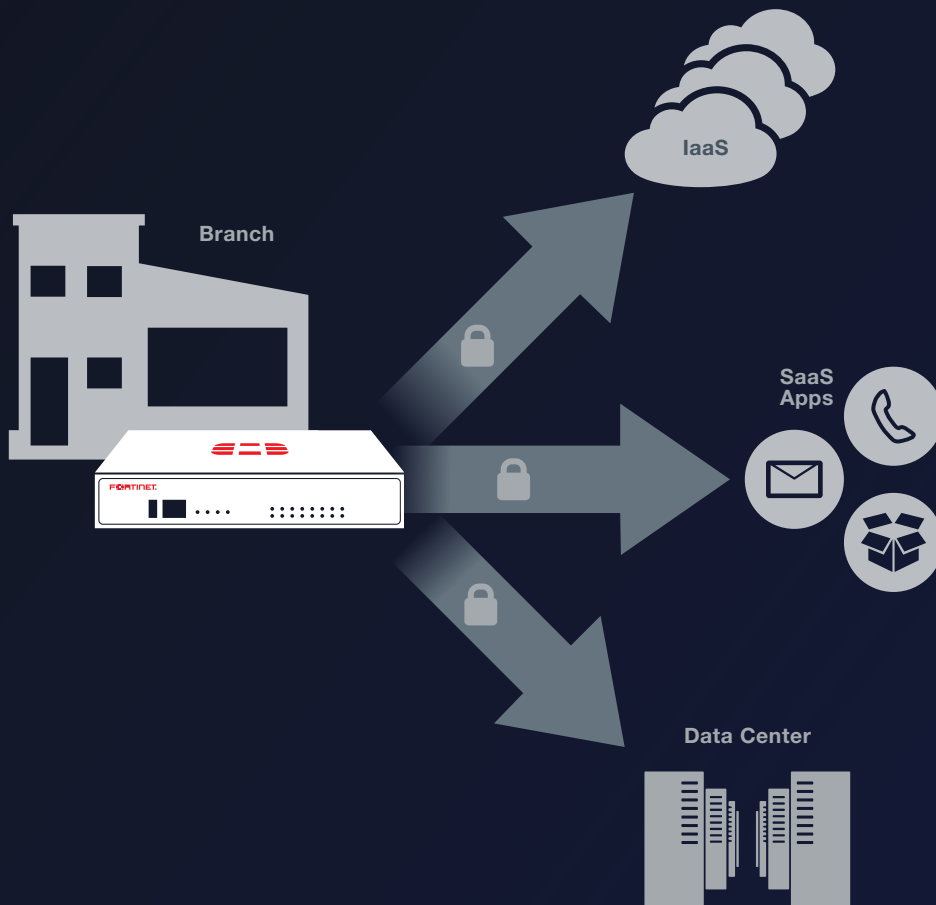
## Other Fabric Solutions



About Fortinet

## Solution Spotlight: Secure SD-WAN

NGFW with built-in, best-of-breed SD-WAN capability enables digital transformation at the enterprise branch.



**SD-WAN** FortiGate 61E

### Products

- FortiGate NGFW (at FortiOS 5.6 & above)
- FortiManager

### Key Features

- Application-aware steering
- Automated WAN path intelligence
- Single-pane-of-glass management with zero-touch provisioning
- SD-WAN features include in base license

### Benefits

- High application performance
- Reduced WAN OPEX
- Safe Internet access for branch sites
- Reduced complexity, easier management



## Fortinet Security Processors

### Specialized chip design delivers more processing power

Fortinet's purpose-built architecture delivers extremely high throughput and exceptionally low latency. These purpose-built security processors radically boost performance and scalability to enable the fastest network security appliances available.

## Most Certified in the Industry

Fortinet is the only network security vendor to earn independent certifications across all core security technologies

Fortinet demonstrates our ability to consolidate multiple security technologies while still meeting the highest standards of performance and accuracy.



About Fortinet