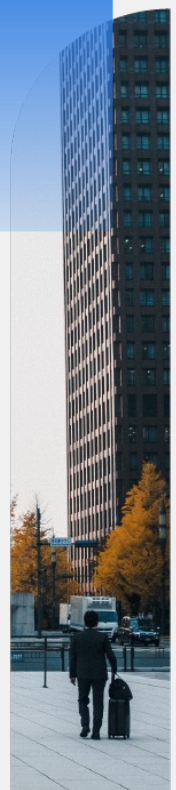
# Zero Trust Network Access (ZTNA)

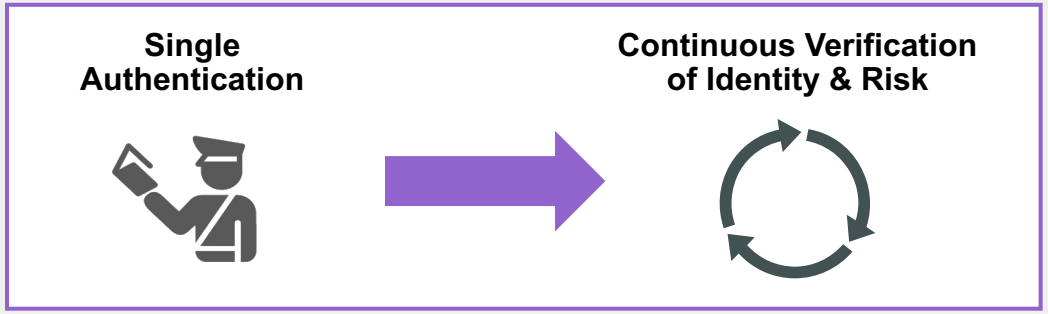
The Evolution of Remote Access to Applications



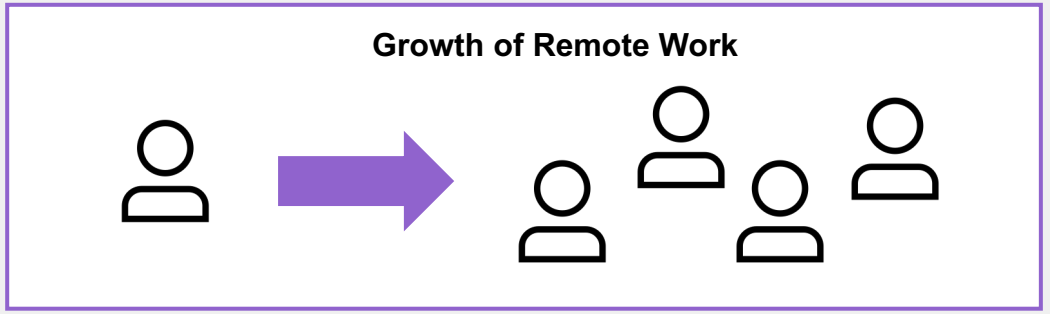
# ZTNA Agenda

- Zero Trust Basics
- Business Drivers
- Technology Overview
- Education Baseline
  - VPN
  - ZTNA
- Fortinet Solution Overview
- Summary

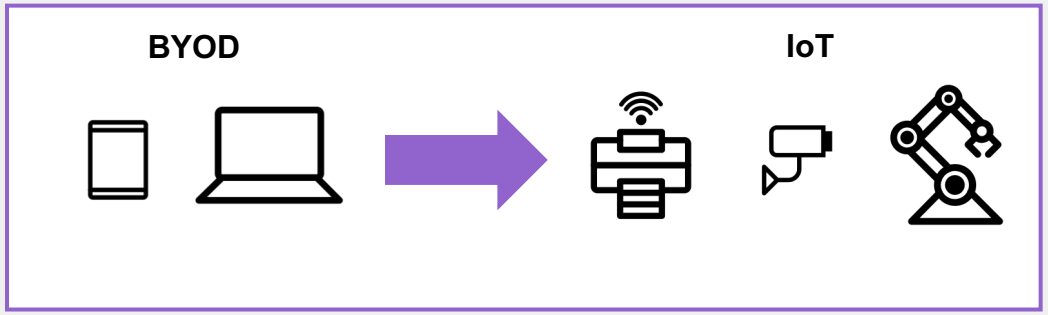
# Enterprise Access Trends



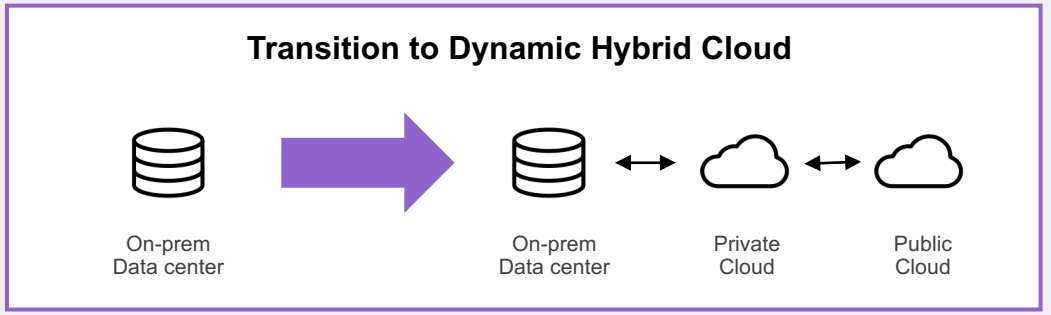

By 2024, 70% of application access will use MFA, up from 10% today[1]




Workforce shifts from 4% teleworking to 30% teleworking by end of 2021[2]



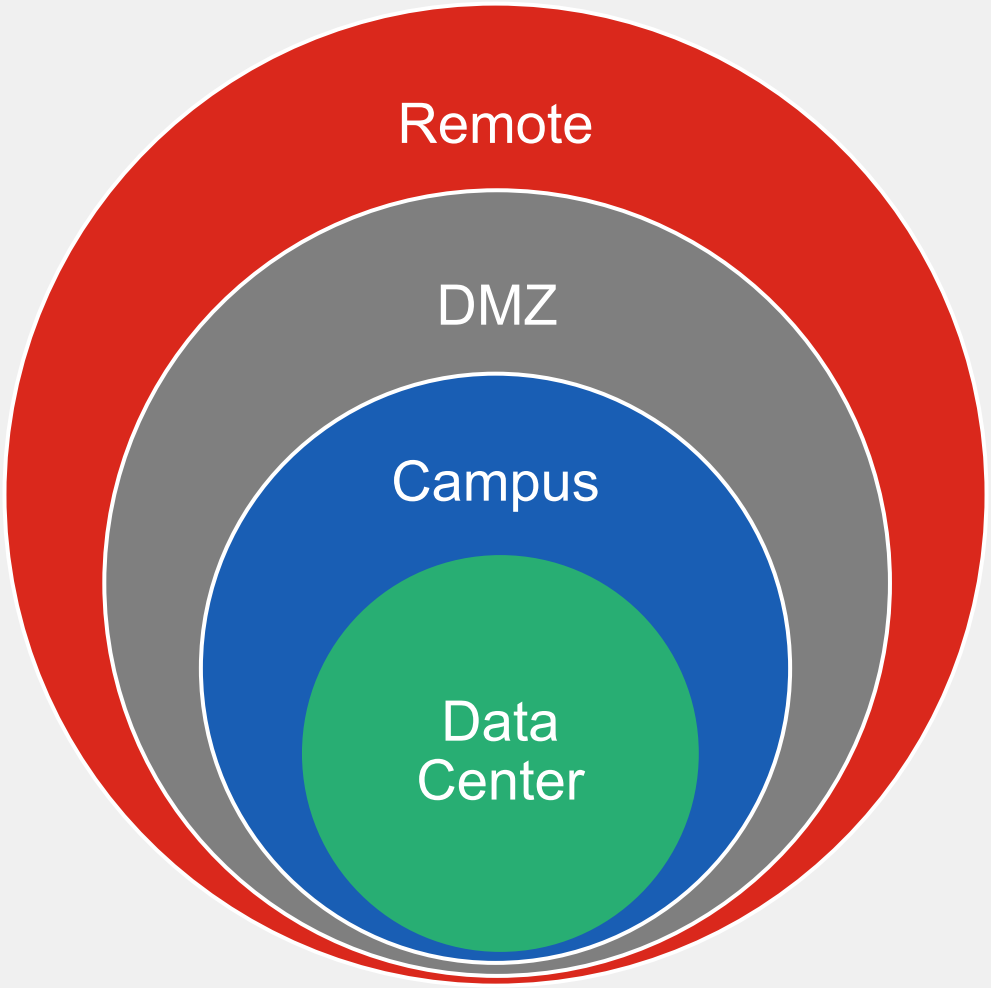

By 2025, there will be **12B** installed IoT devices[3]

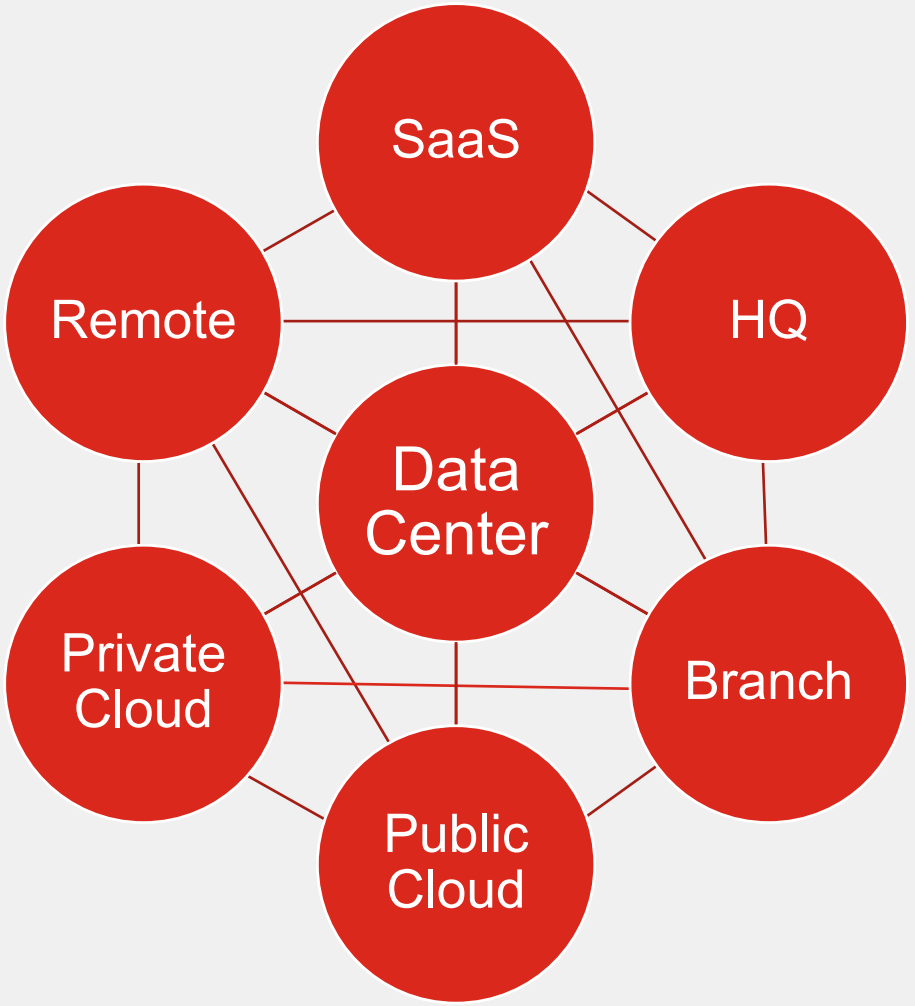



Since nearly every organization needs it, hybrid IT use-case requirements have become more common among Gartner clients.[4]

1 Gartner Magic Quadrant for Access Management, 12 August 2019
2 Global Workplace Analytics
3 Gartner IoT Forecast
4 Gartner Magic Quadrant for Public Cloud Managed Services, 4 May 2020

# Architectures Change



# Zero Trust Principles

What is zero trust?  Zero Trust is a philosophy around how to grant users access to resources.  It's not a product or a project, but a new mindset about how to organize and provision resources.

- Verify
  - Authenticate and verify– on an ongoing basis

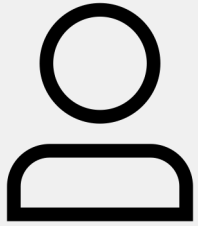
- Give minimal access
  - Segment the network to create small zones of control
  - Control access to applications, data, resources
  - Grant least privilege access based on need or role

- Assume Breach
  - Plan as if attackers are inside and outside the network
  - Forget the concept of a "trusted zone", e.g., 'in the office'

# ZTNA Business Drivers

# ZTNA Business Drivers

## Work From Anywhere (WFA)



Users Access unaffected by Location

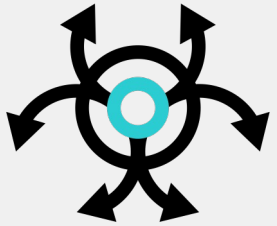
Improved User Experience

## Cloud Journey

Applications unaffected by Location

Flexible Administration

## Ransomware Attacks



Granular Application Access

Reduced Attack Surface

# Supporting Work From Anywhere (WFA)

## A better user experience

- Access from in or out of Office
- Automatic secure tunnels to applications
- SSO Supported
- No need to know applications location

Campus

Branch

Traveling

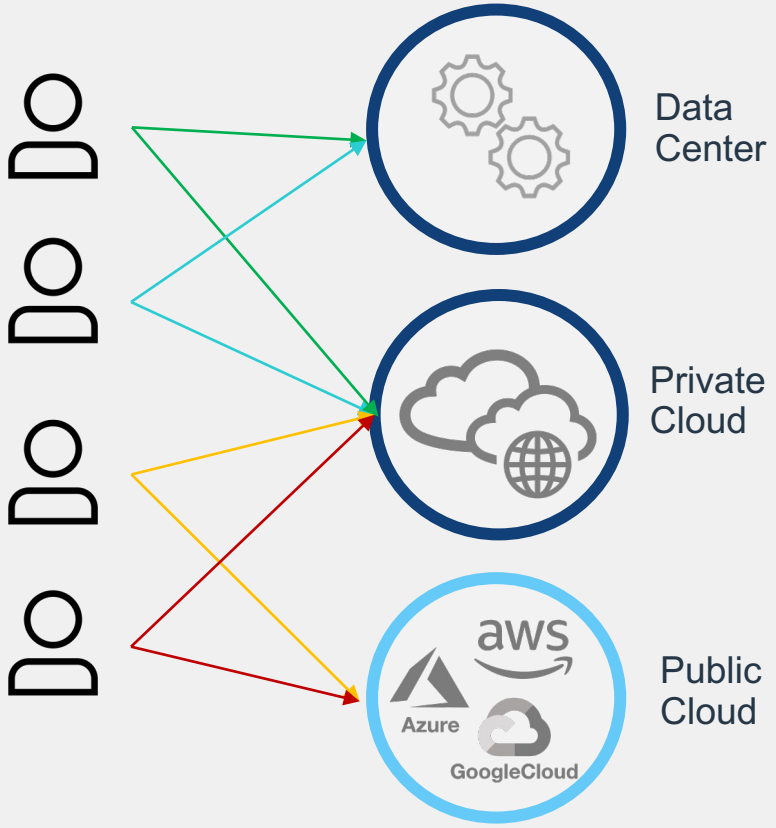
Home

Coffee Shop

# Supporting the Cloud Journey

## Controlling access to hybrid cloud architecture

- Applications located anywhere
- Centrally managed across on-prem or remote enforcement points
- User groups enable bulk configuration
  - Granular modifications available



# Reducing the Attack Surface

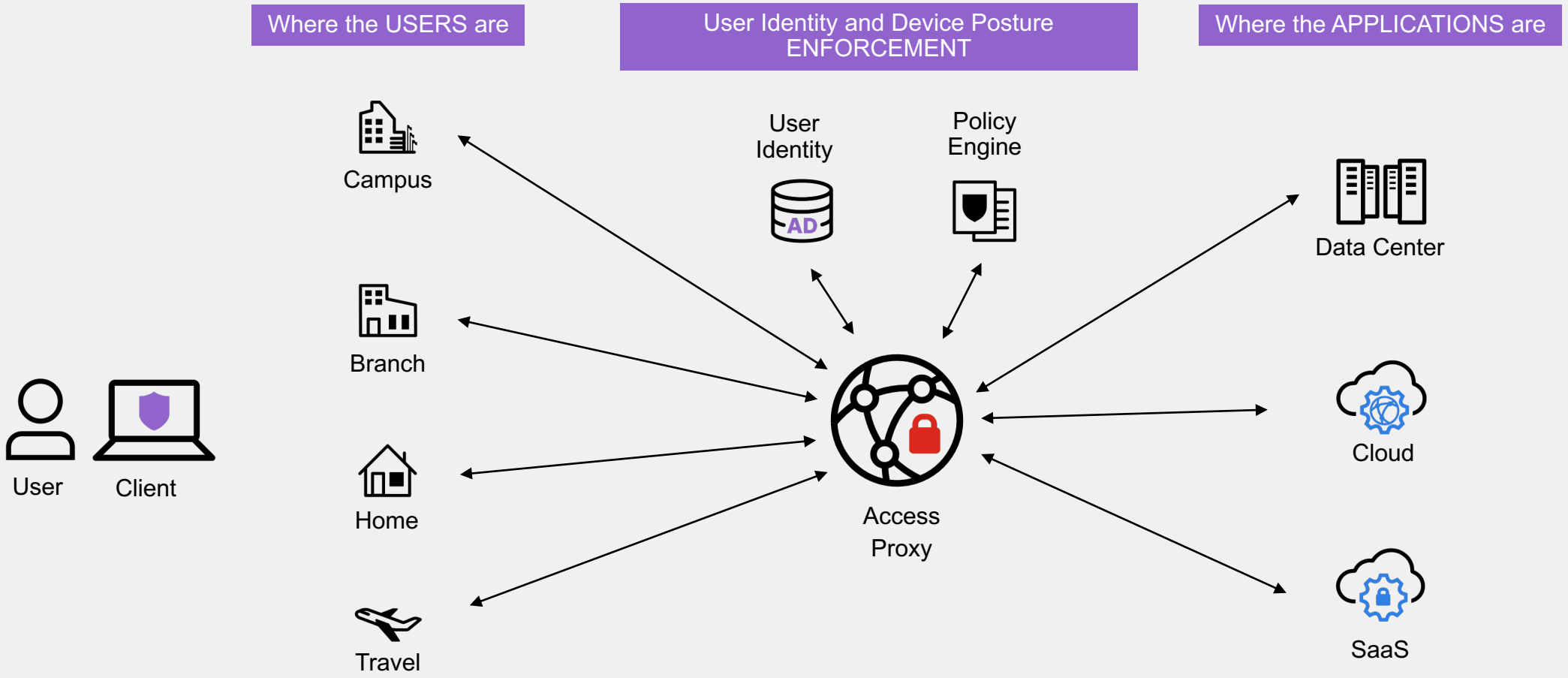
Granular Control to Applications

- User Identity Authenticated per connection 
- Strong Authentication (MFA) & Single Sign-on (SSO) Supported 
- Device Identity verified per session 
- Device Posture verified per session 
- User access allowed only to necessary applications and data 
- Applications hidden from Internet behind Access Proxy 

# ZTNA Technology

# ZNTA Elements

The components of a client-based ZTNA solution



# Evolution of VPN tunnels

Bringing Zero Trust principles to remote access = ZTNA

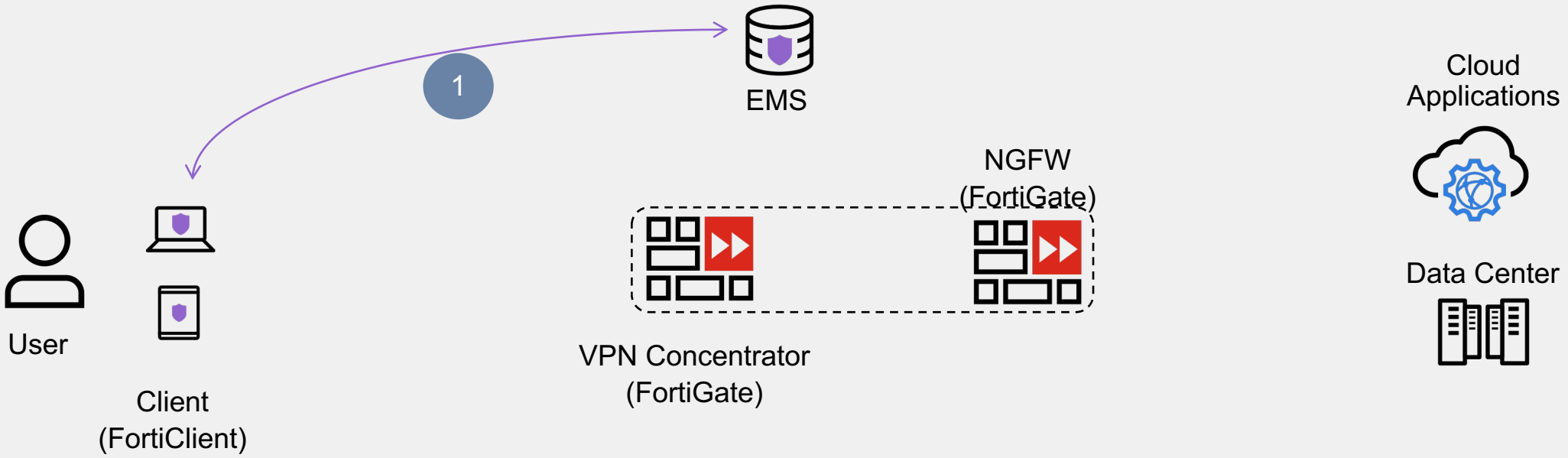
- Ongoing verification
  - Per connection user identity checks, with SSO support
  - Per session device identity check
  - Per session device posture checks (OS version, A/V status, vulnerability assessment)
- More granular control
  - Access granted only to specific application
  - No more broad VPN access to the network
- Easier user experience
  - Auto-initiates secure tunnel when user accesses applications
  - Same experience on and off-net

# VPN Basics

So we can understand why ZTNA is better

# Virtual Private Networking (VPN) Technology

## Client Configuration



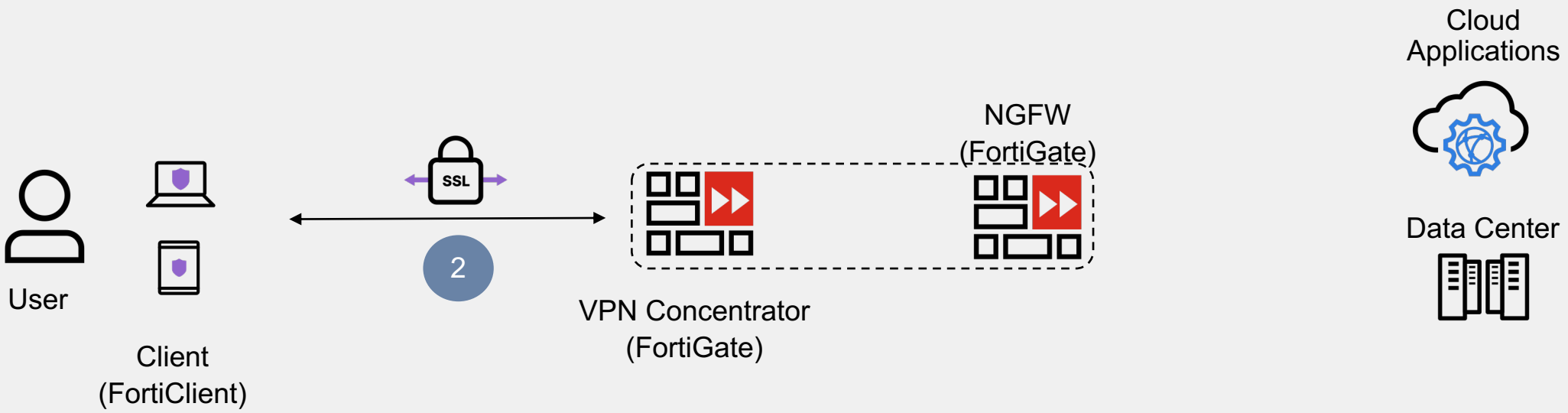

**What's happening?**

FortiClient connects to EMS for configuration

- Where to connect VPN tunnel

# Virtual Private Networking (VPN) Technology

## Tunnel launched

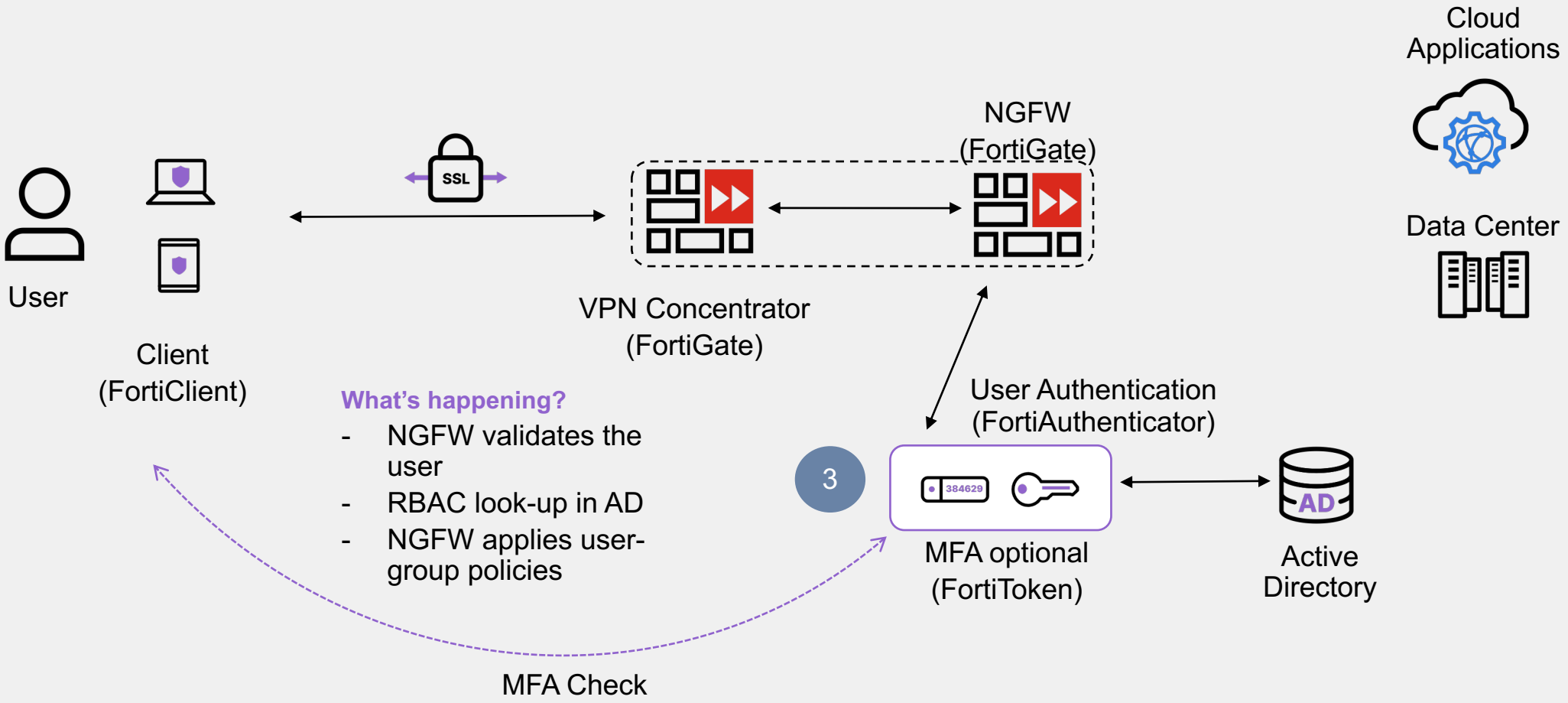



What's happening?

- End users initiates a VPN tunnel
- Client connects to VPN concentrator

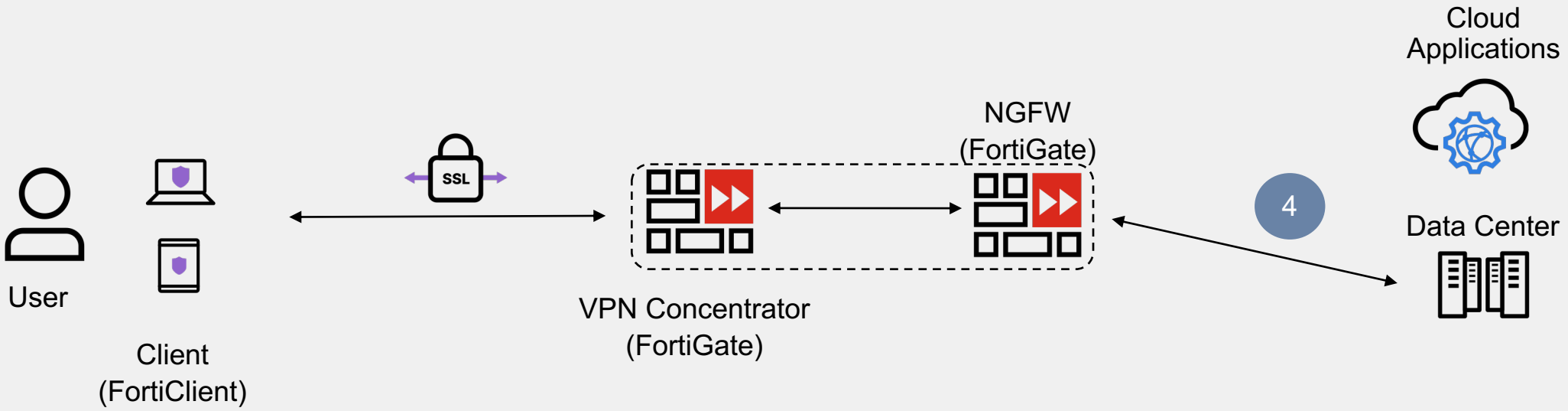
# Virtual Private Networking (VPN) Technology

## User Verified; Optional Multi Factor Authentication (MFA)



# Virtual Private Networking (VPN) Technology

## Network Access Granted

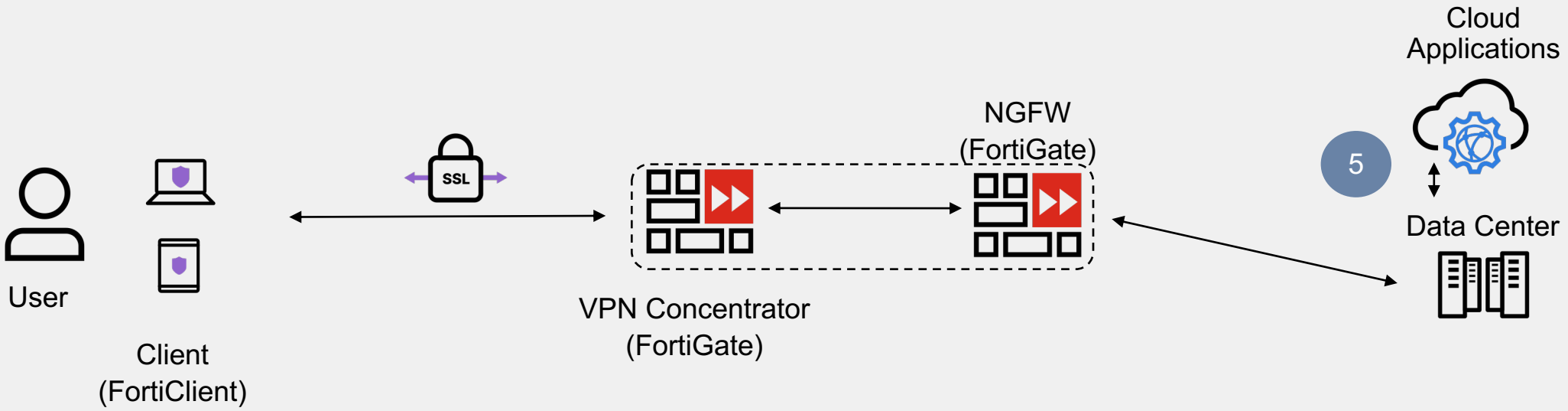



**What's happening?**

- NGFW allows the user access to the network

# Virtual Private Networking (VPN) Technology

## Access to Cloud-based Resources




**What's happening?**

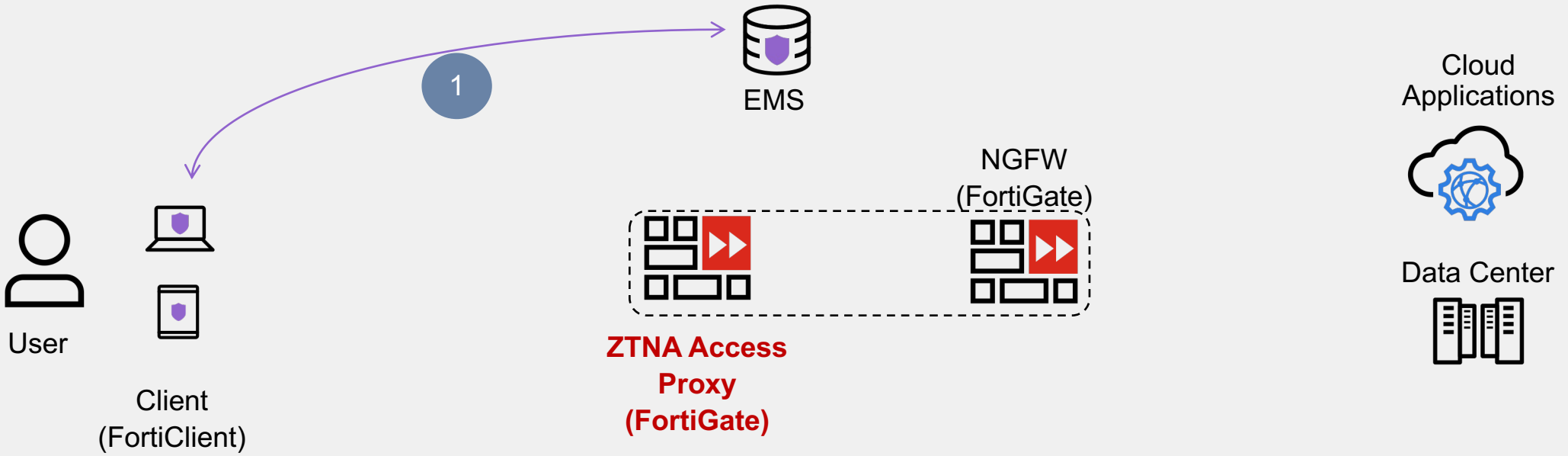
- Traffic to the Cloud travels through the data center

# ZTNA Basics

Same elements but better coordination

# Zero Trust Network Access (ZTNA) Technology

## ZTNA Telemetry



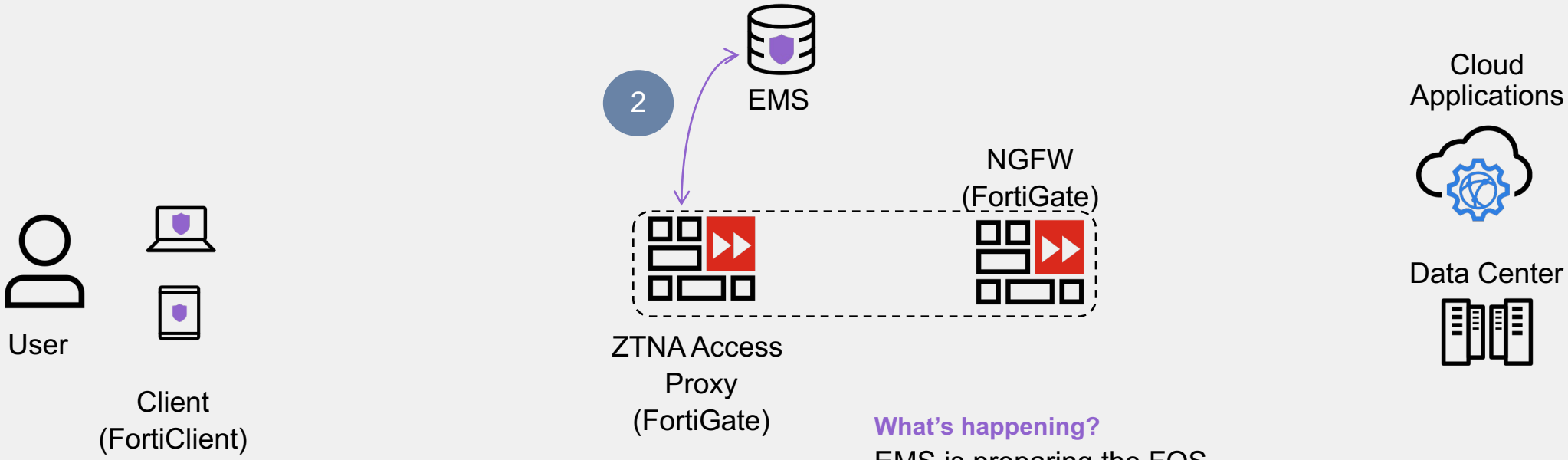

**What's happening?**

FortiClient connects to EMS for configuration:

- Where to connect ZTNA tunnel
- Register device for posture check, provision certificates

# Zero Trust Network Access (ZTNA) Technology

## Fabric Sync



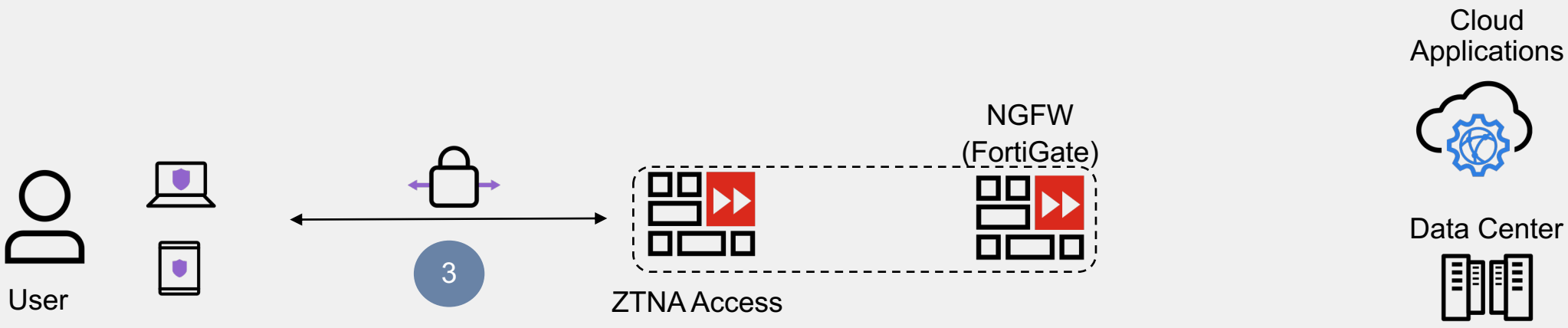

**What's happening?**

EMS is preparing the FOS devices to receive ZTNA tunnels:

- Passing certificates for device identity & posture check
- ZTNA tags added to FortiGate

# Zero Trust Network Access (ZTNA) Technology

## Tunnel and Device Posture Check

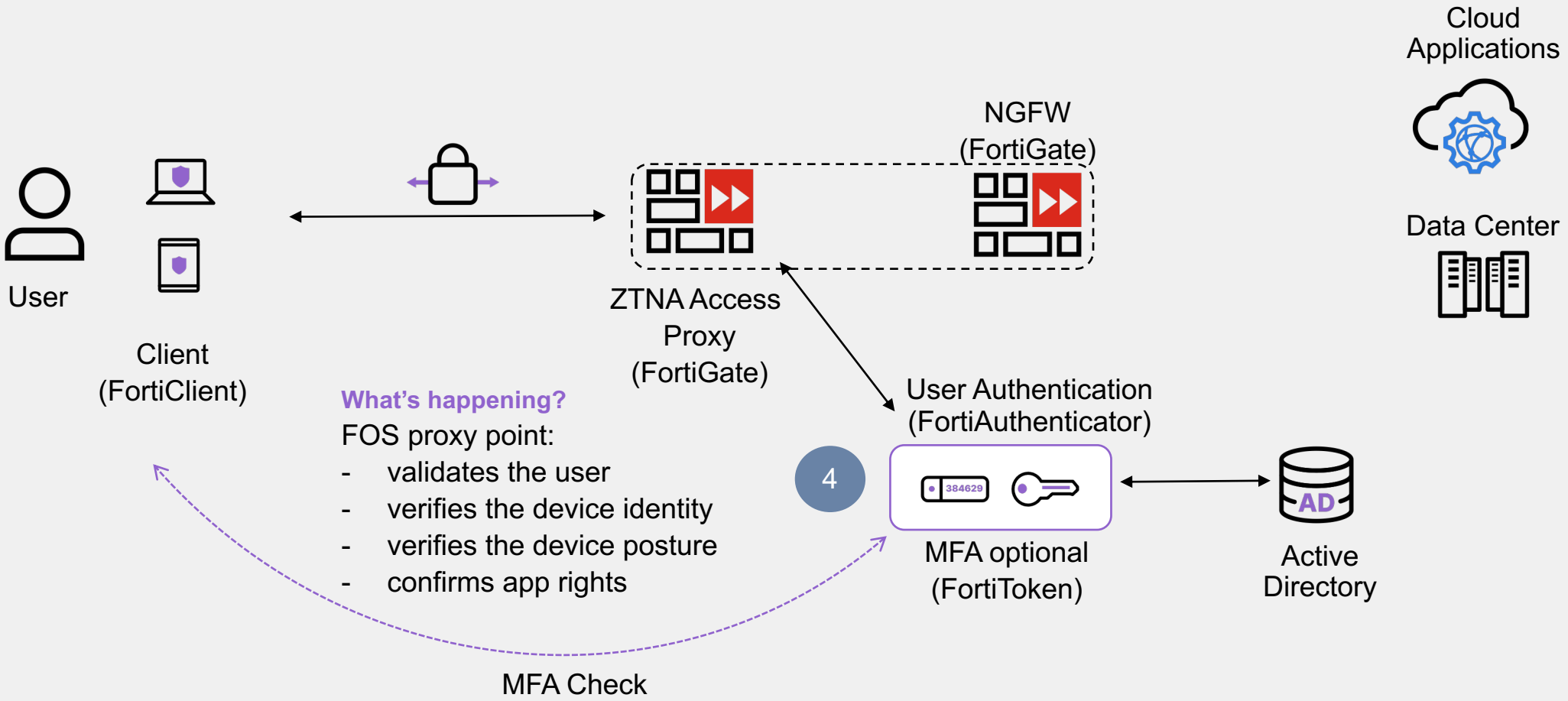



**What's happening?**

When the user opens an app, the ZTNA agent automatically connects to the FOS proxy point

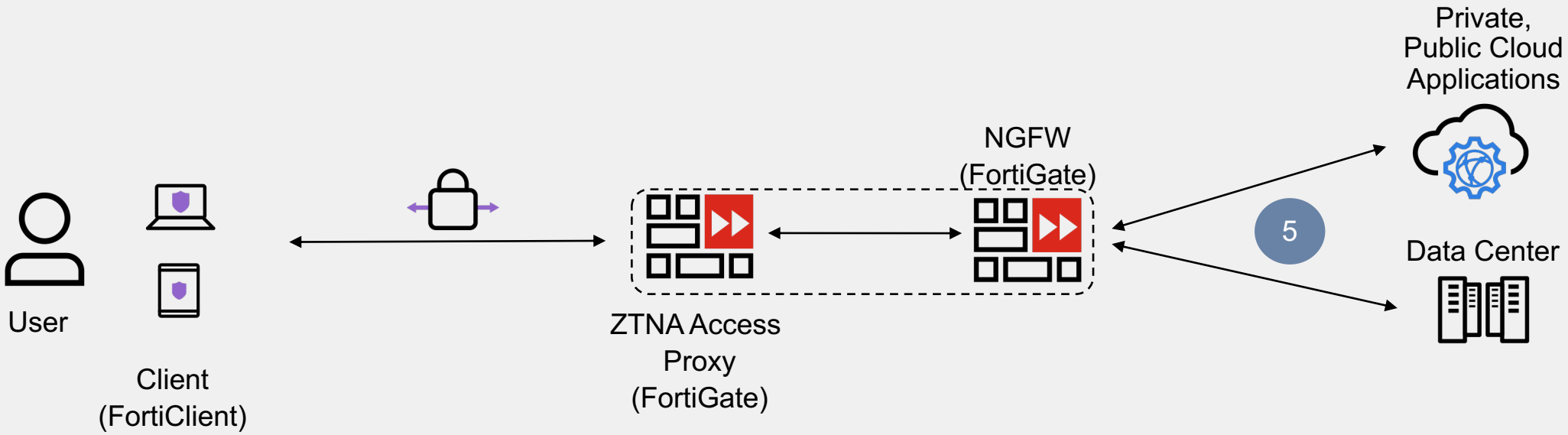
# Zero Trust Network Access (ZTNA) Technology

## Tunnel and Device Posture Check; Optional Multi Factor Authentication (MFA)



# Zero Trust Network Access (ZTNA) Technology

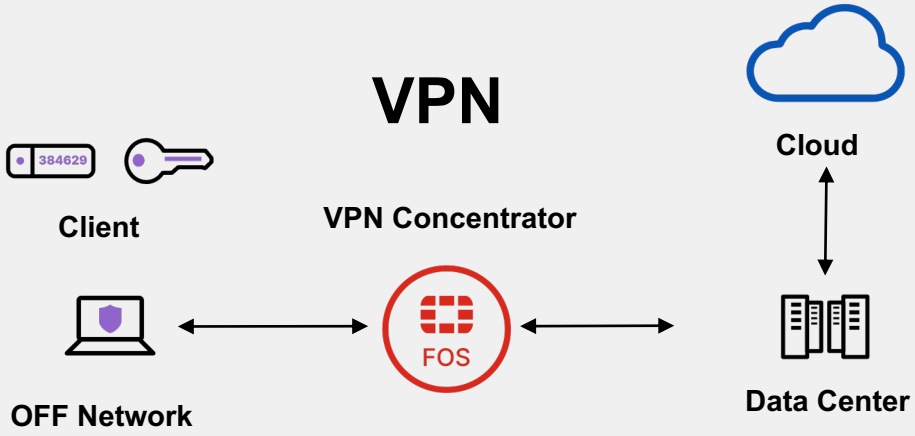
## Application Access Granted




**What's happening?**

FOS proxy point connects to the app, enabling the user to access for that session, no matter where it is

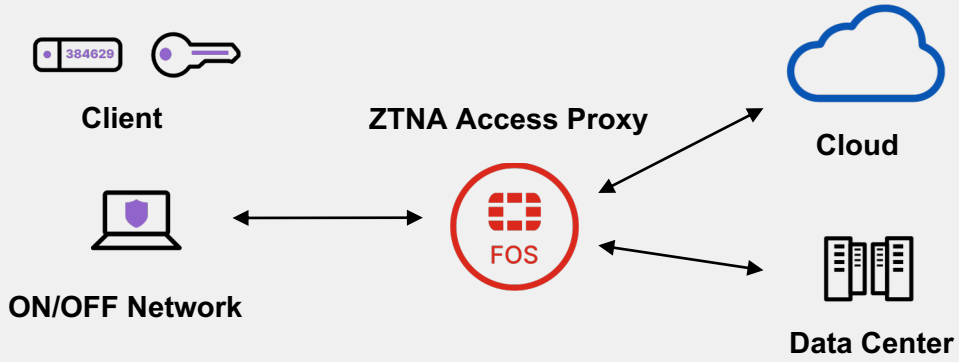
# Evolution from Traditional VPN to ZTNA




One Time Trust Check

Access Network

Generic Rule Set




Continuous Trust Check

Access Specific Application

User Contextual Rule Set

# Fortinet Solution Overview

# Fortinet's ZTNA

## What's it made of? Existing Fortinet Security Fabric Products

**Core Elements**

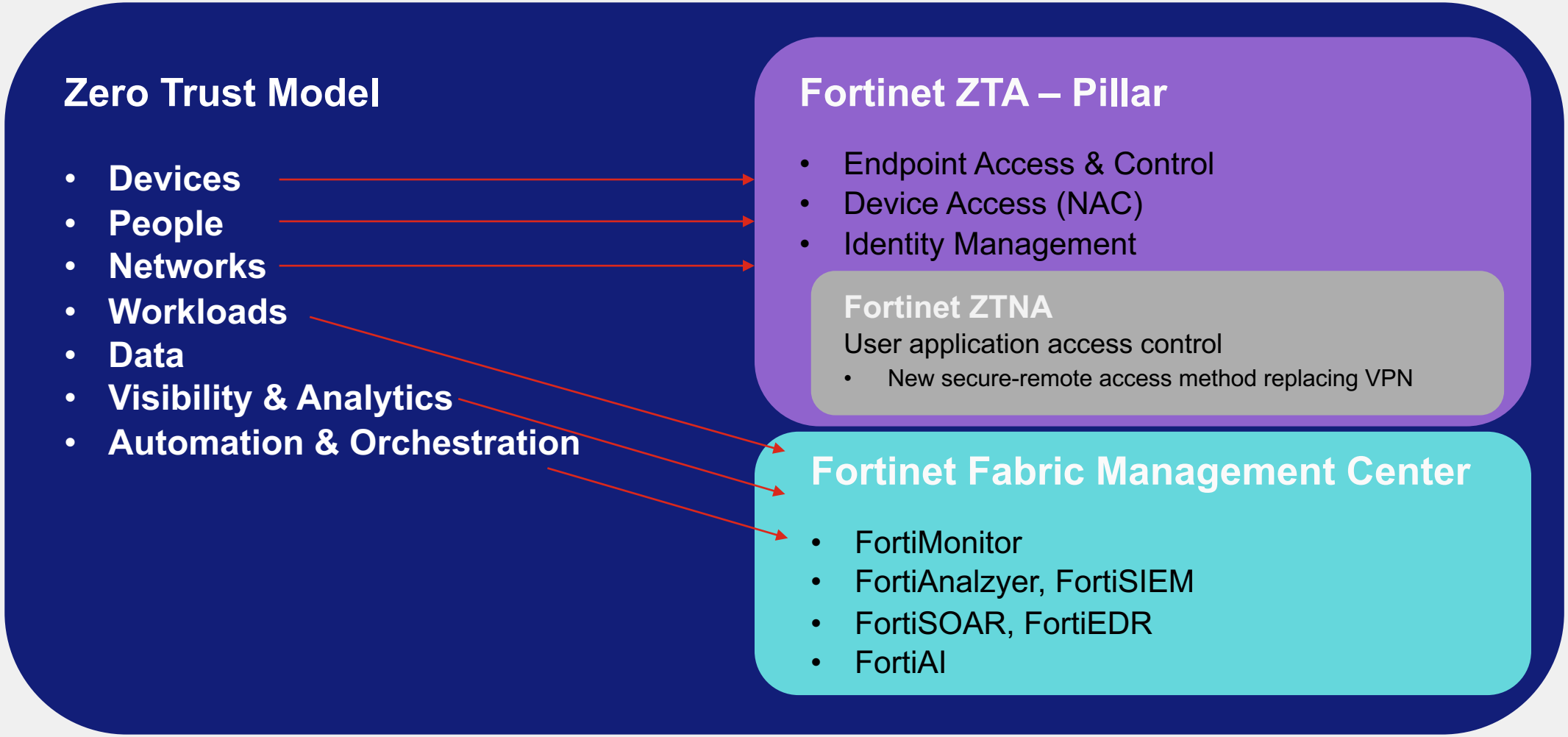
FortiGate

FortiClient / FortiClient EMS

- FortiGate builds the secure tunnel, maintains user group/application access table (FOS 7.0)
- FortiClient EMS configures the ZTNA agent in FortiClient for the secure connection back to the FortiGate (FortiClient 7.0)

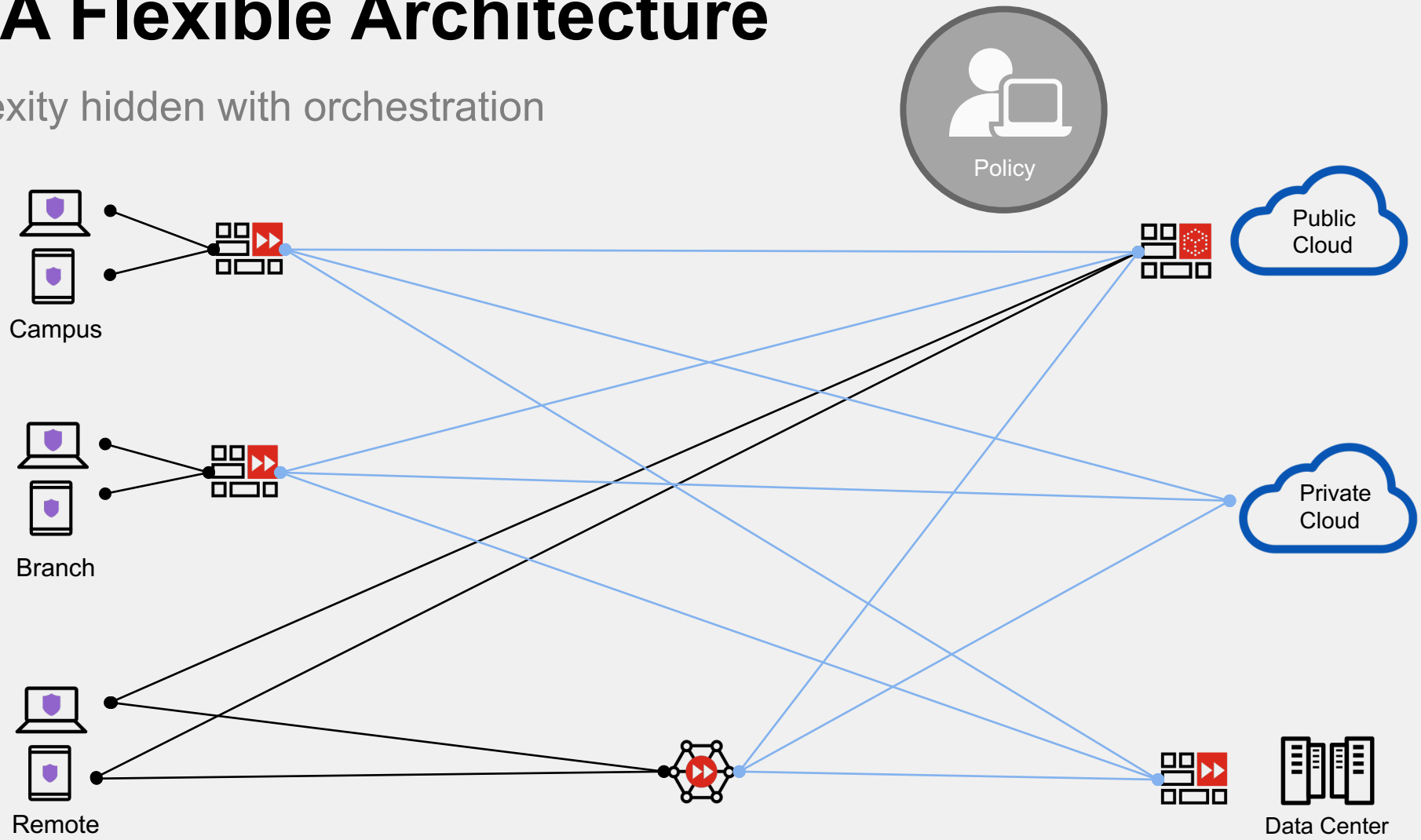
- Authentication Solution
  - FortiAuthenticator, FortiToken or any 3rd party supported by the Security Fabric

# Fortinet ZTA, FMC and ZTNA in Context



# ZTNA Flexible Architecture

Complexity hidden with orchestration




Wherever the user is

Verified user identity, device identity & posture check prior to access

Wherever the application is

# Fortinet ZTNA advantages

## Complete coverage vs. other ZTNA solutions

### Leveraging existing investments in on-prem Firewalls

- Most ZTNA solutions are SASE-only options with expensive charges for company-wide coverage
- Faster access to on-prem applications
- Leverage SD-WAN, SD-Branch capabilities


### Improved Security (“Secure ZTNA”)

- Extend FortiGate protection to wherever you are
- Traffic traversing Industry-leading FortiGate technology
- FortiGuard Labs services

### No Licenses Required

- Simply a feature in FOS & FortiClient to turn on!
- Easy transition from VPN access to ZTNA

# ZTNA Competitive Landscape

## Gartner ZTNA Market Guide

| | | | | |
|---|---|---|---|---|
| **SASE** | Zscaler Private Access (ZPA) | Prisma Access | Netskope Private Access | Forcepoint Private Access |
| **Identity** | Cisco Duo Beyond | BeyondCorp Enterprise | Azure AD Application Proxy | Okta Cloud Identity |
| **Legacy VPN** | AnyConnect | Remote User Secure Access | Global Protect | Pulse SDP |


FORTINET