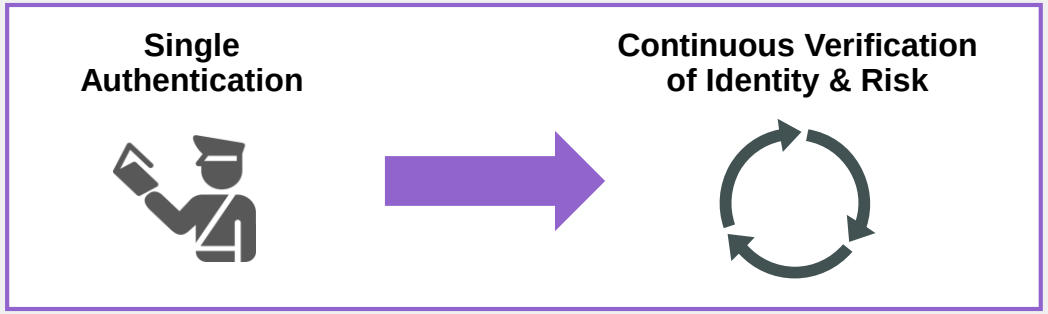
Improve Application Access and Security With Fortinet Zero Trust Network Access

Madalin Vasile
Sr. Manager Systems Engineering

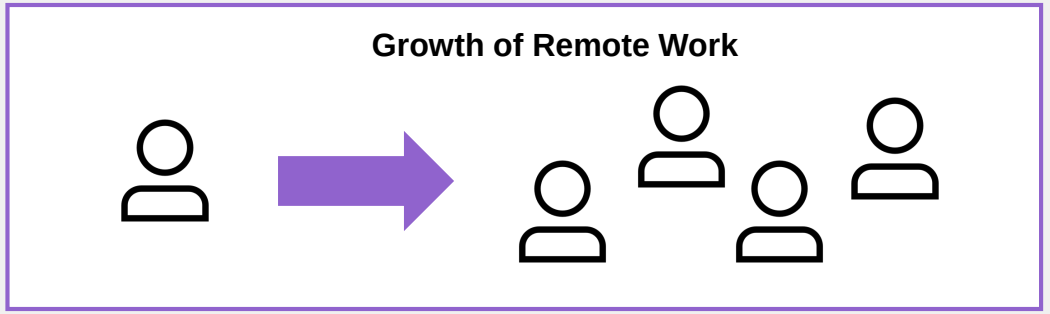
Agenda

- What is Zero Trust?
- Where is ZTNA in the Fortinet Security Fabric?
- Why do customers care about ZTNA?
- What is ZTNA?
- How does ZTNA work?
- Fortinet ZTNA’s Advantages
- What do you need to deploy ZTNA?

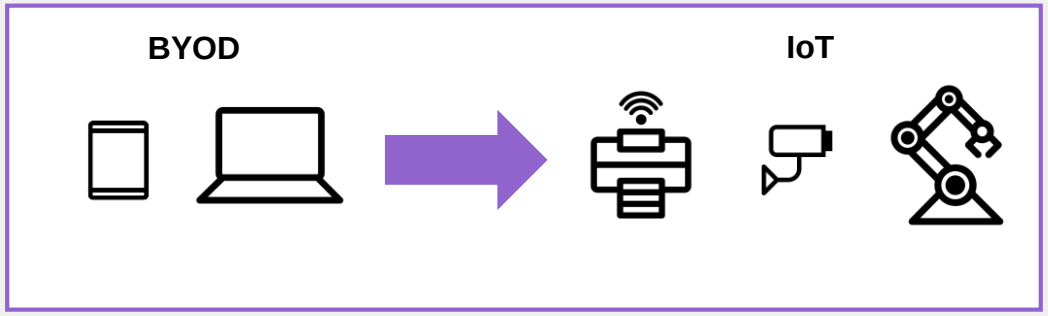
Enterprise Access Trends



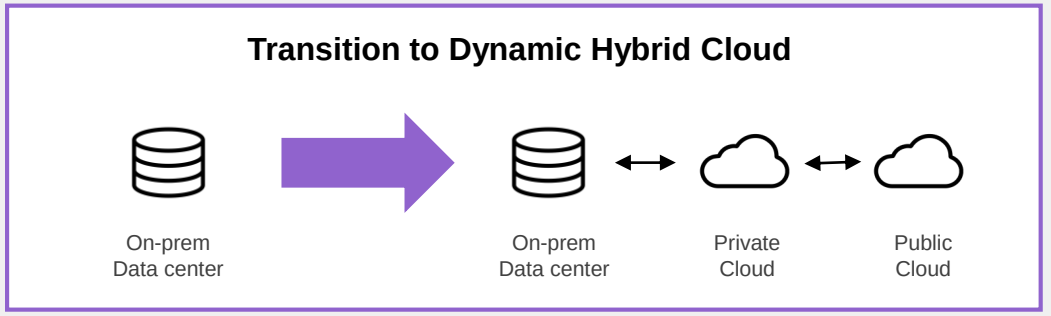
By 2024, 70% of application access will use MFA, up from 10% today[1]



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



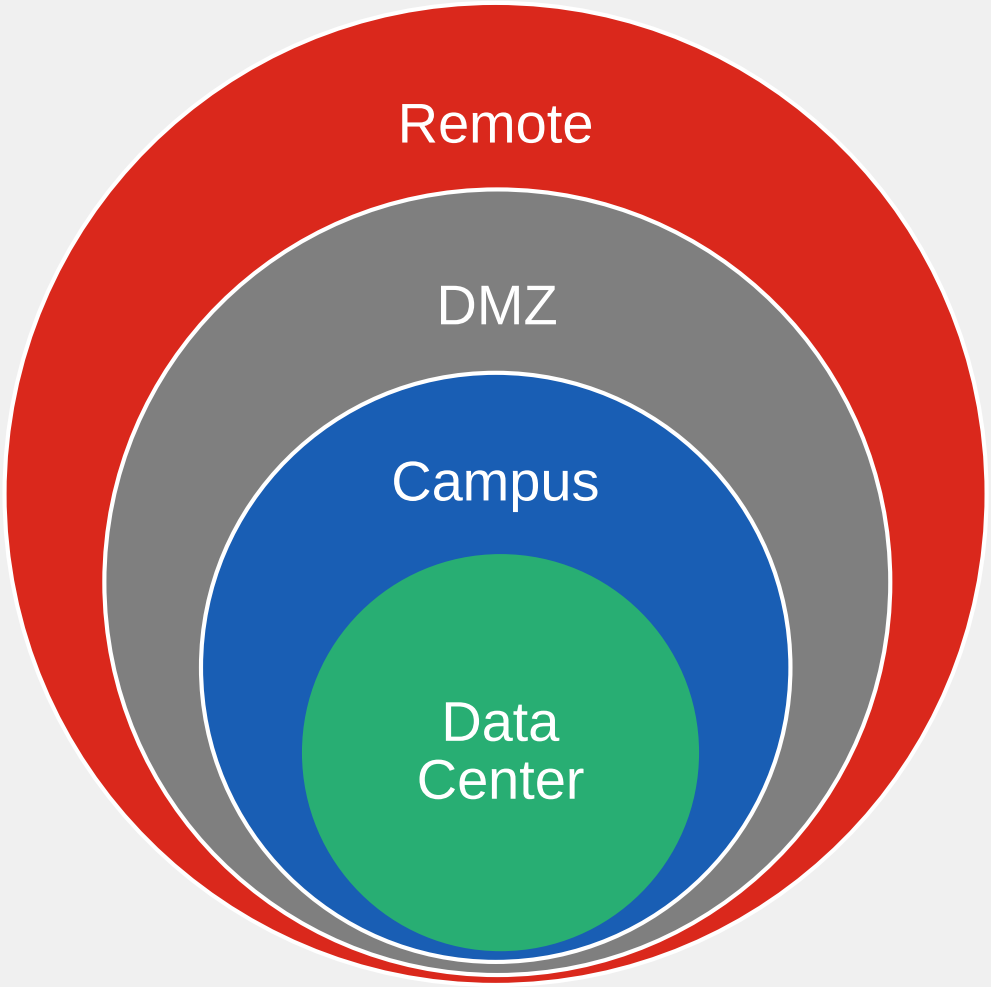
By 2025, there will be **12B** installed IoT devices[3]

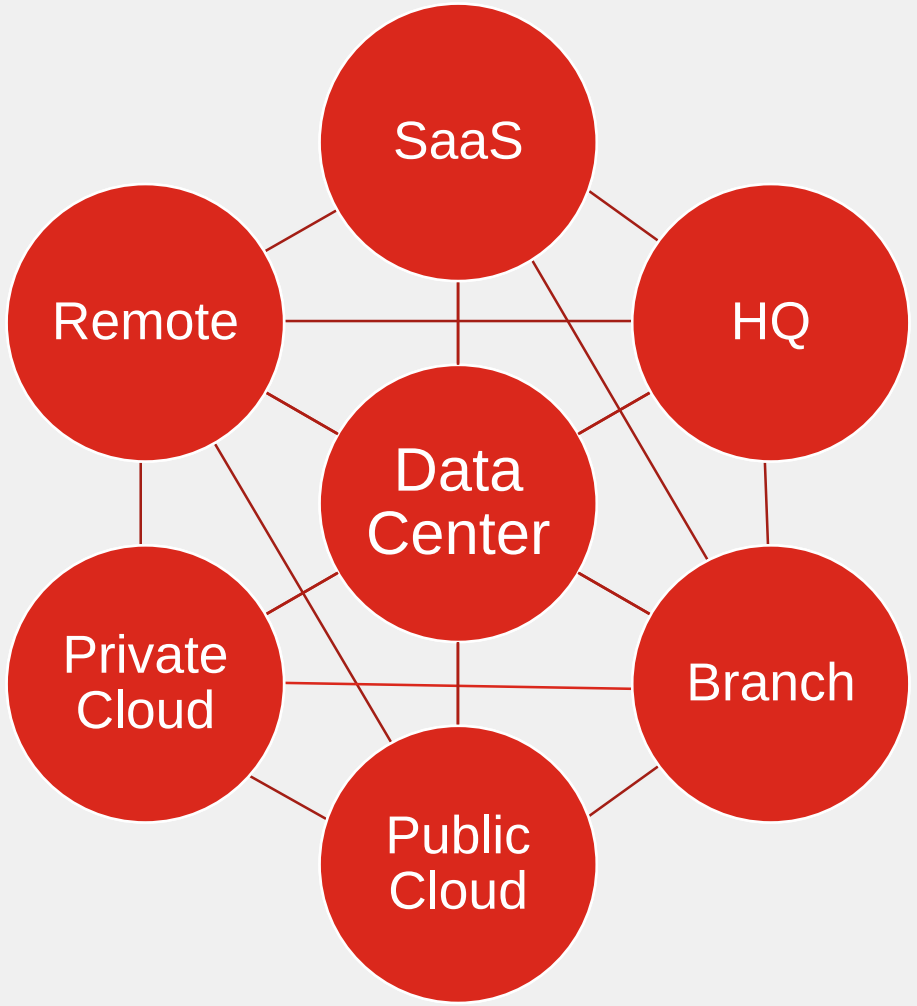


Since nearly every organization needs it, hybrid IT use-case requirements have become more common among Gartner clients.[4]

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

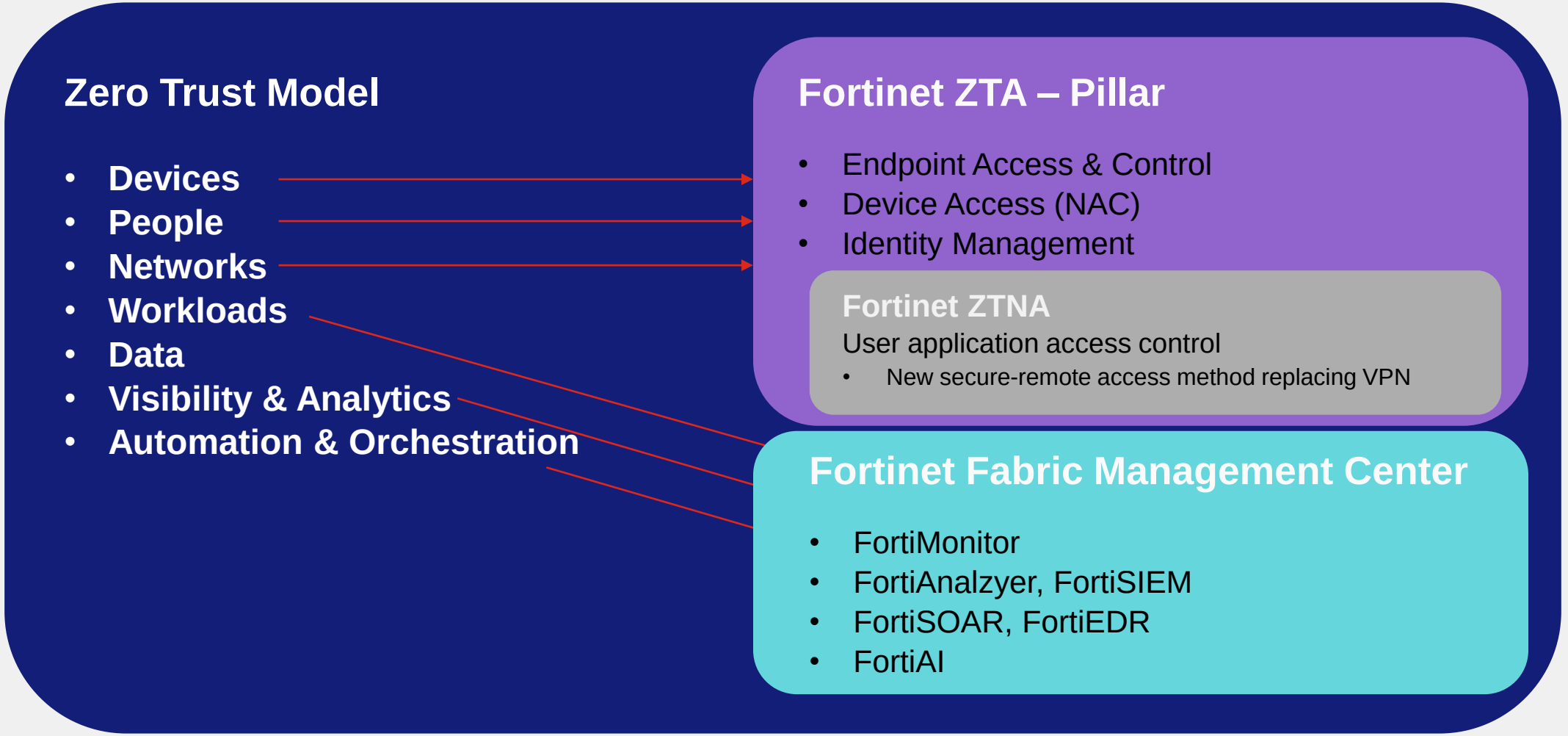
For users and devices

- 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’

Fortinet ZTA, FMC and ZTNA in Context



Fortinet Security Fabric

Broad

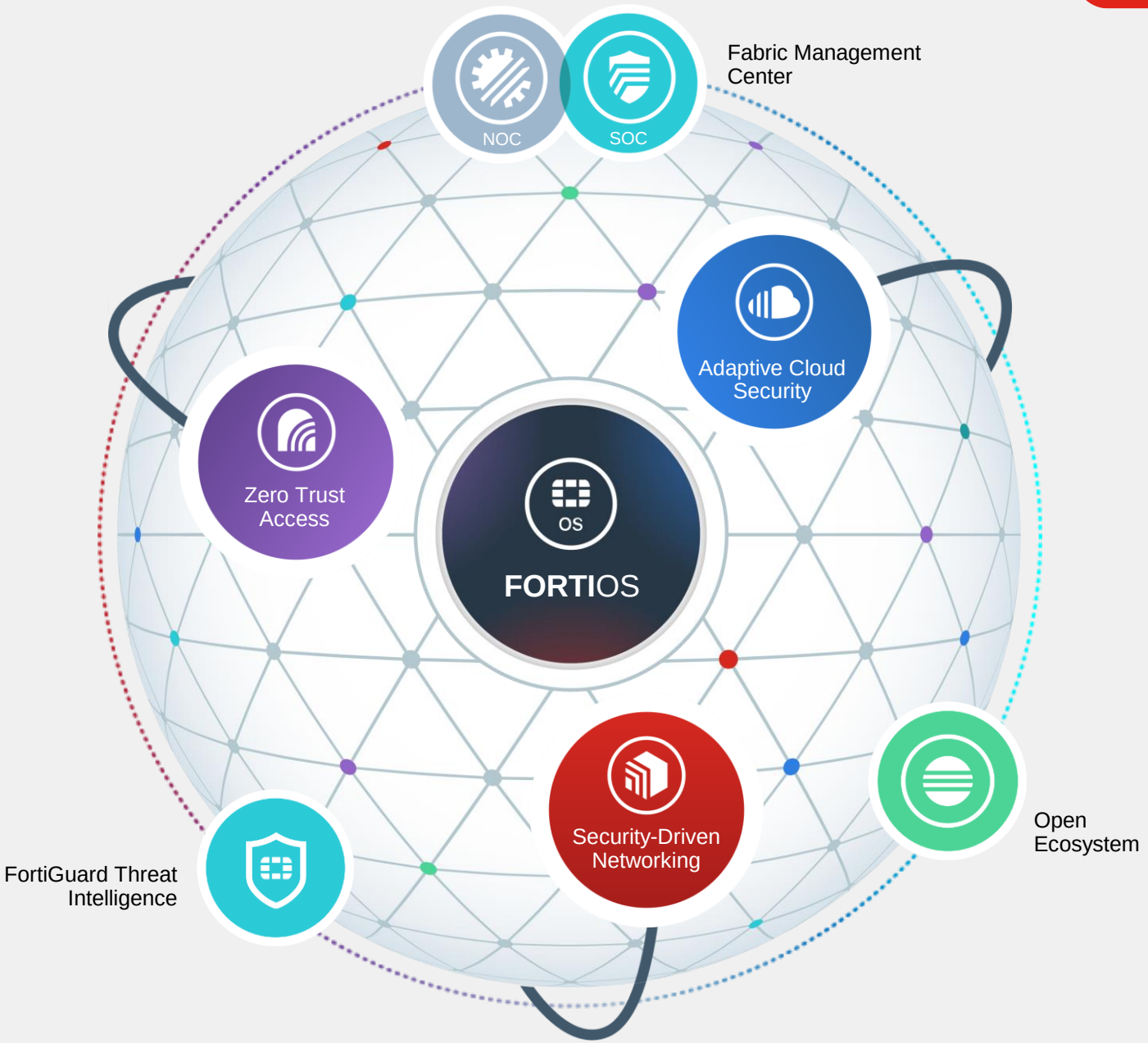
visibility and protection of the entire digital attack surface to better manage risk

Integrated

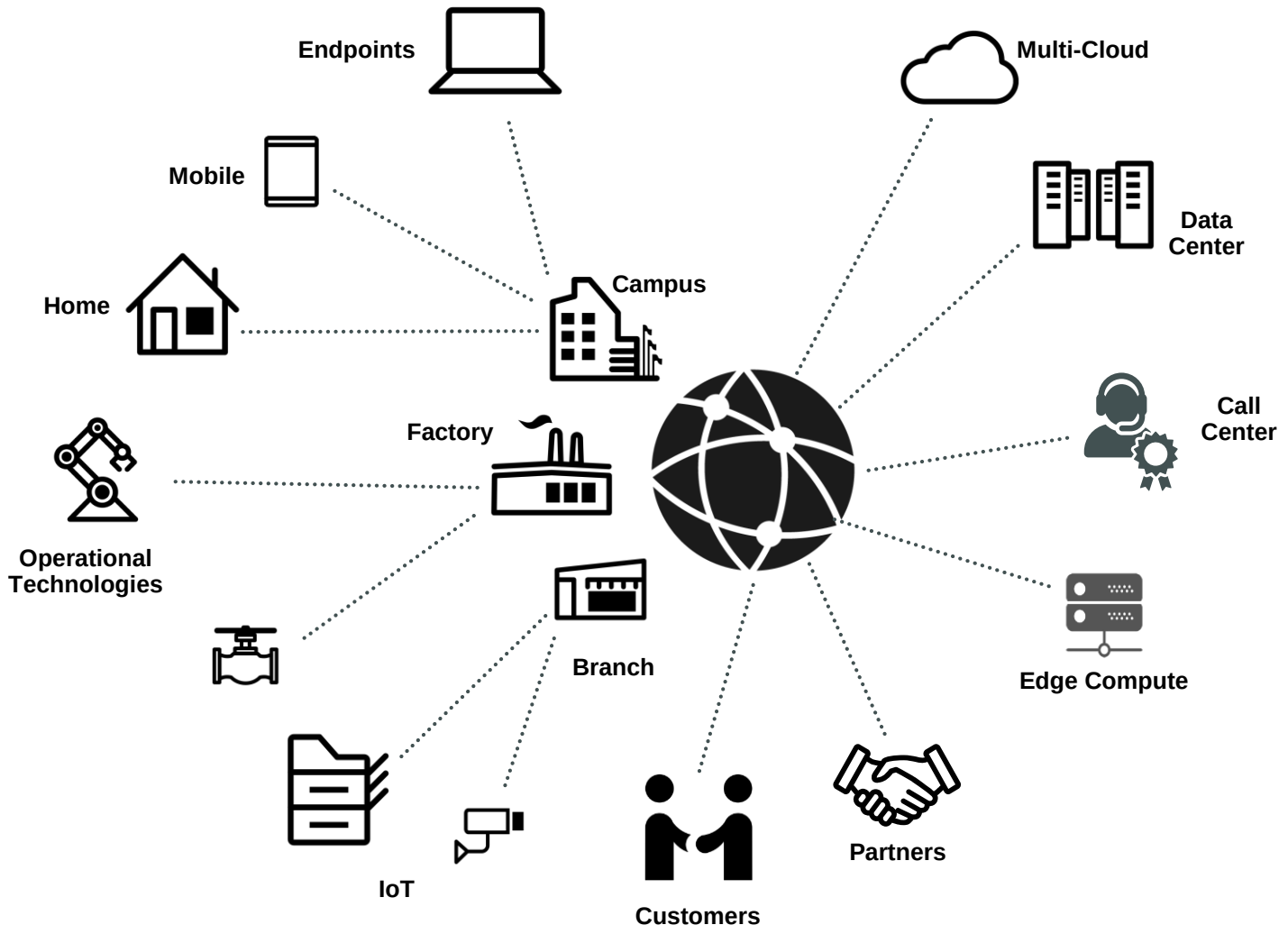
solution that reduces management complexity and shares threat intelligence

Automated

self-healing networks with AI-driven security for fast and efficient operations



Zero Trust Access



Knowing and Controlling Everyone and Everything on and off the Network

Ensures consistent security policy across the network, the cloud, and off-network

Zero Trust Access Shift

<2021

Zero Trust Access
Users & Device Access

Identity & Access Management (IAM)

User Authentication

VPN Tunnel

Remote Access

Network Access Control (NAC)

Device Access

With 7.0

Zero Trust Access
Users & Device Access

Identity & Access Management (IAM)

User Authentication

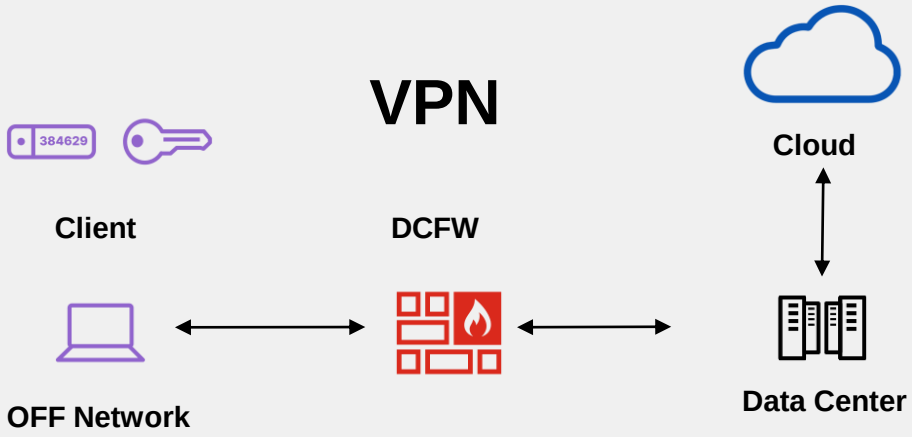
Zero Trust Network Access (ZTNA)

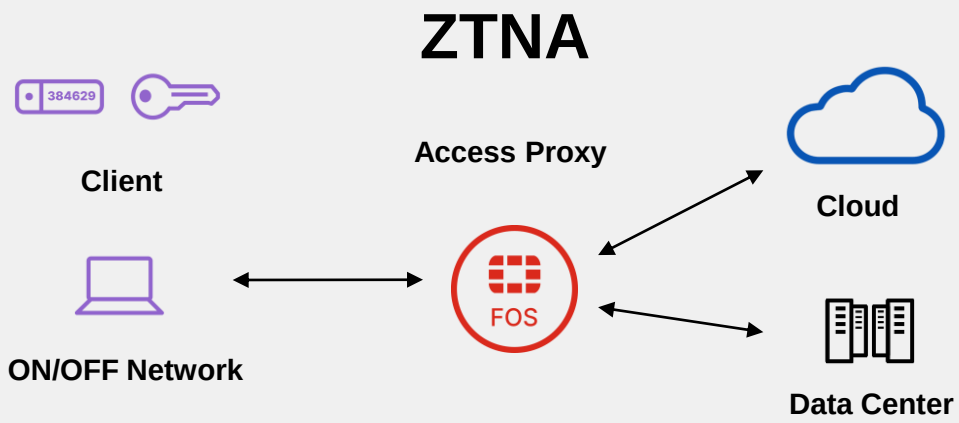
Application Access

Network Access Control (NAC)

Device Access

Evolution from Traditional VPN to ZTNA



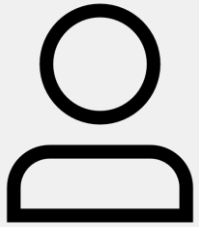


- One Time Trust Check
- Access Entire Network
- Generic Rule Set

- Continuous Trust Check
- Access Specific Applications
- User Contextual Rule Set

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

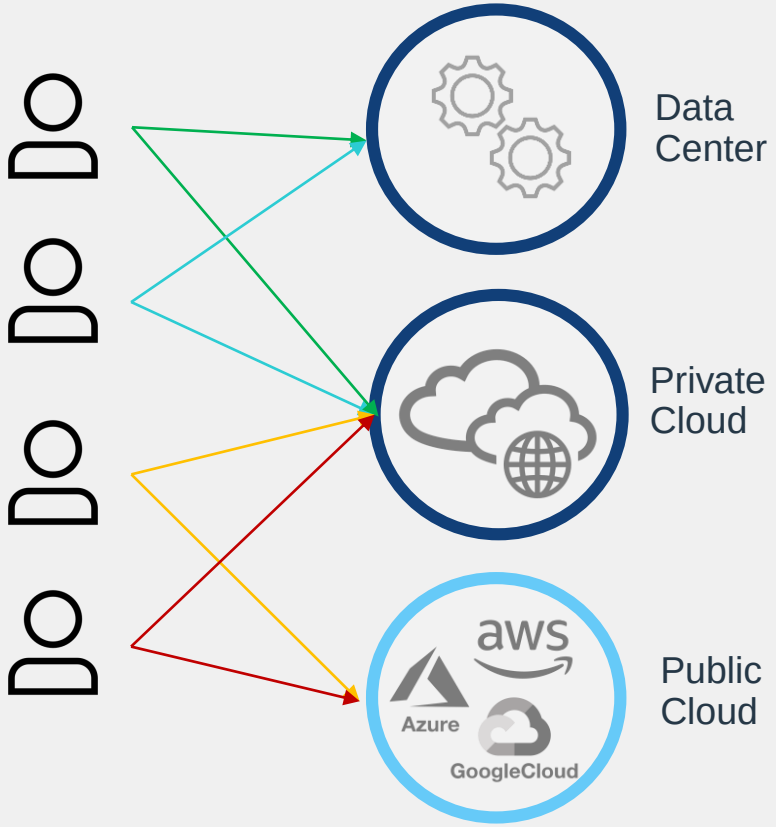
Home

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

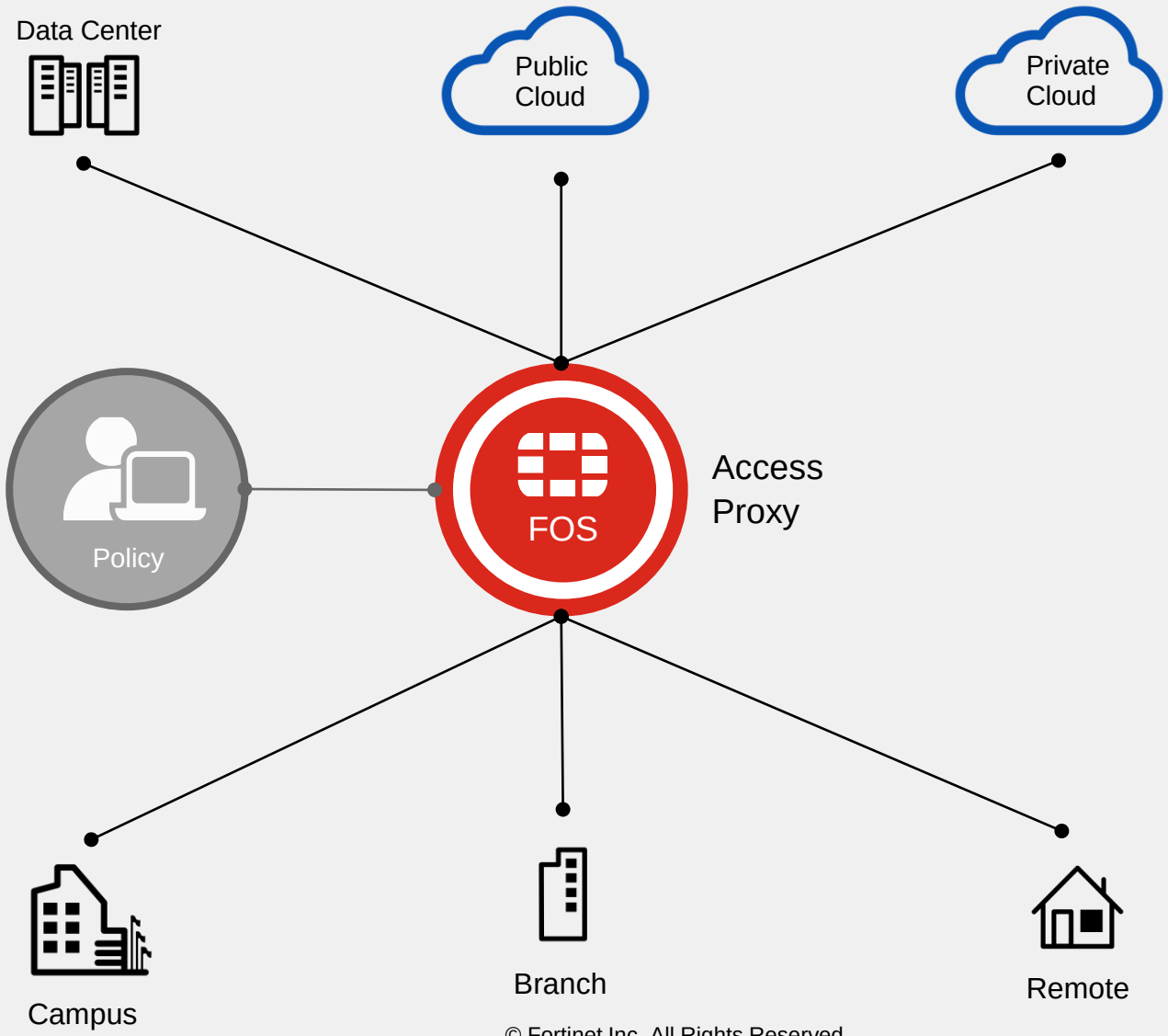


Reducing the Attack Surface

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 Flexible Architecture

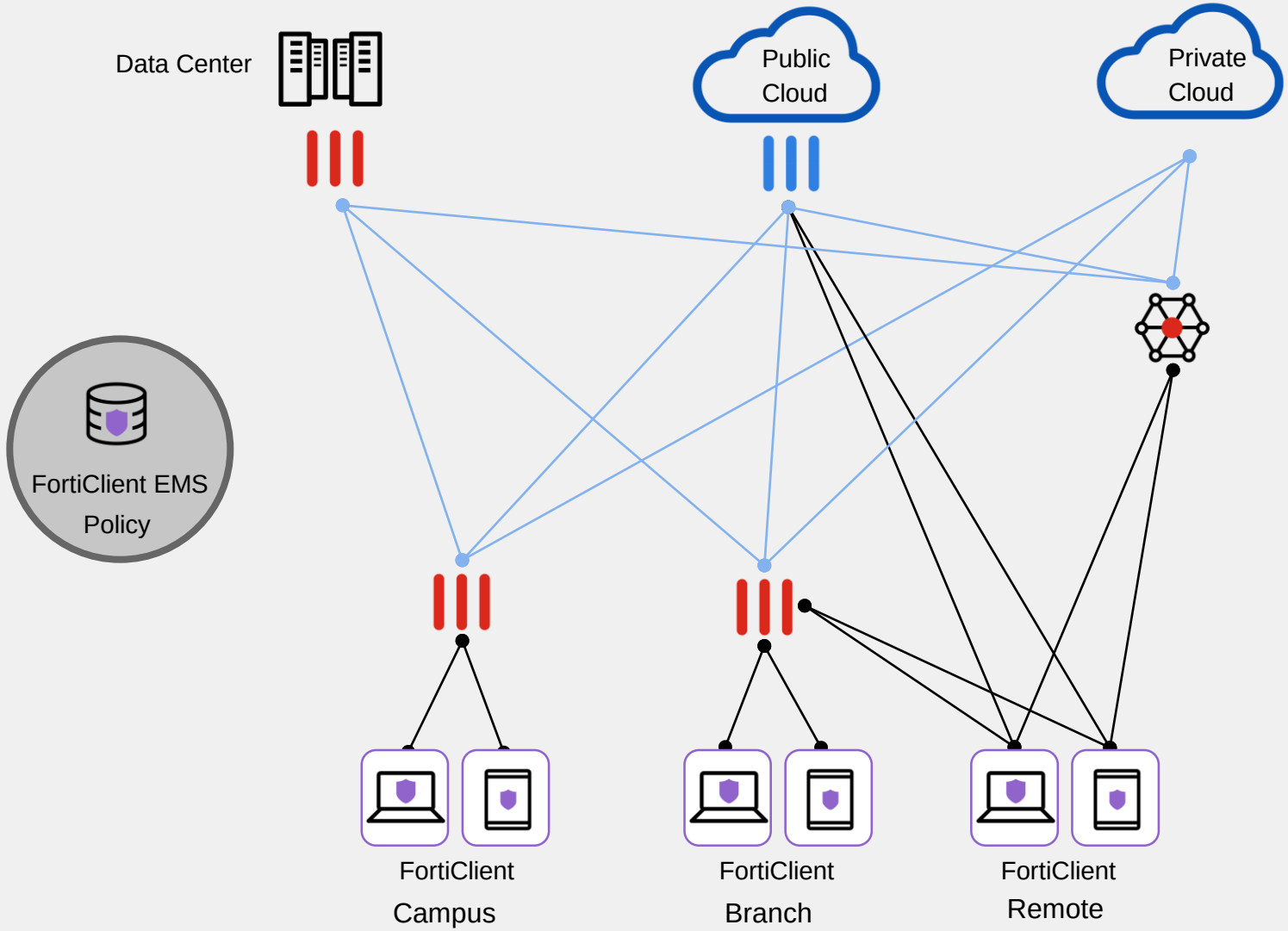


Wherever the application is

Verified user identity and device posture prior to access

Wherever the user is

ZTNA Automatic Secure Connections



Leveraging Existing Infrastructure

Continuous Reassessment & Enforcement

Auto-on secure ZTNA tunnels (HTTPS/SSH)

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 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
  - Leverage SD-WAN, SD-Branch capabilities

- Improved Security (“Secure ZTNA”)
  - Extend FortiGate protection to wherever you are
  - Traffic traversing Industry-leading FortiGate technology

- No Licenses Required
  - Simply a feature in FOS & FortiClient to turn on!

Evolution of VPN tunnels

Bringing Zero Trust principles to remote access

- Ongoing verification
  - Per session user identity checks
  - 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


FORTINET