Zero Trust Network Access (ZTNA)

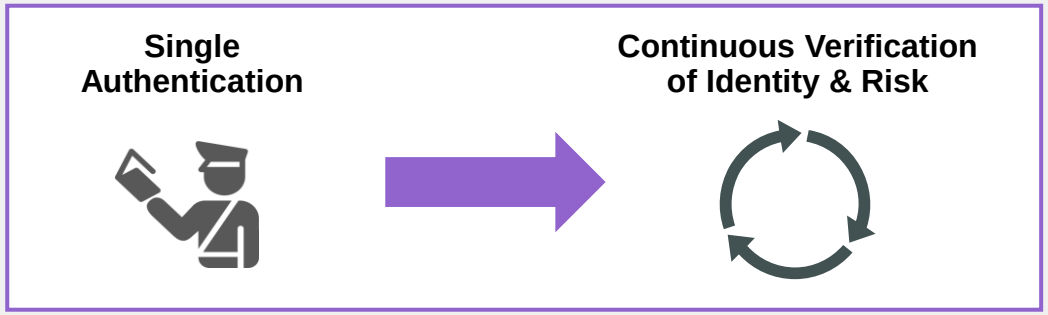
The Evolution of Remote Access to Applications

„never trust, always verify“

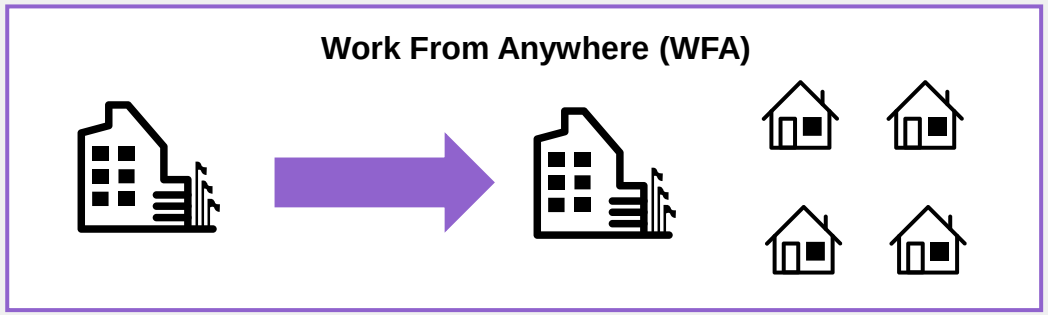
Herbert Teibler : Systems Engineer Austria
NSE7, CCIE #9928

Why do we need ZTNA?

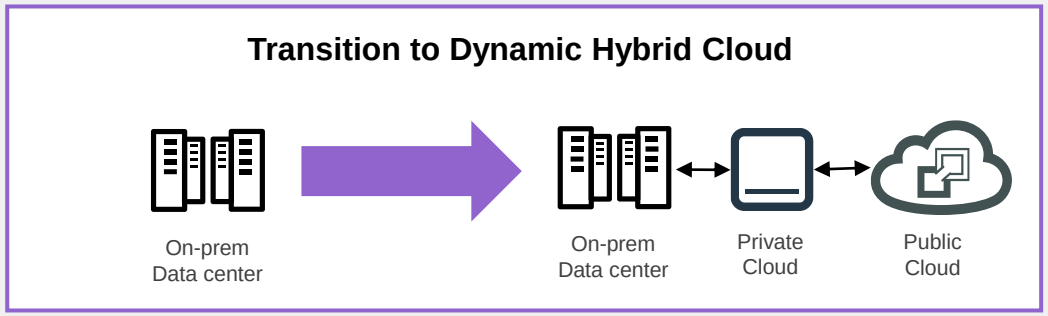
Enterprise Access Trends



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



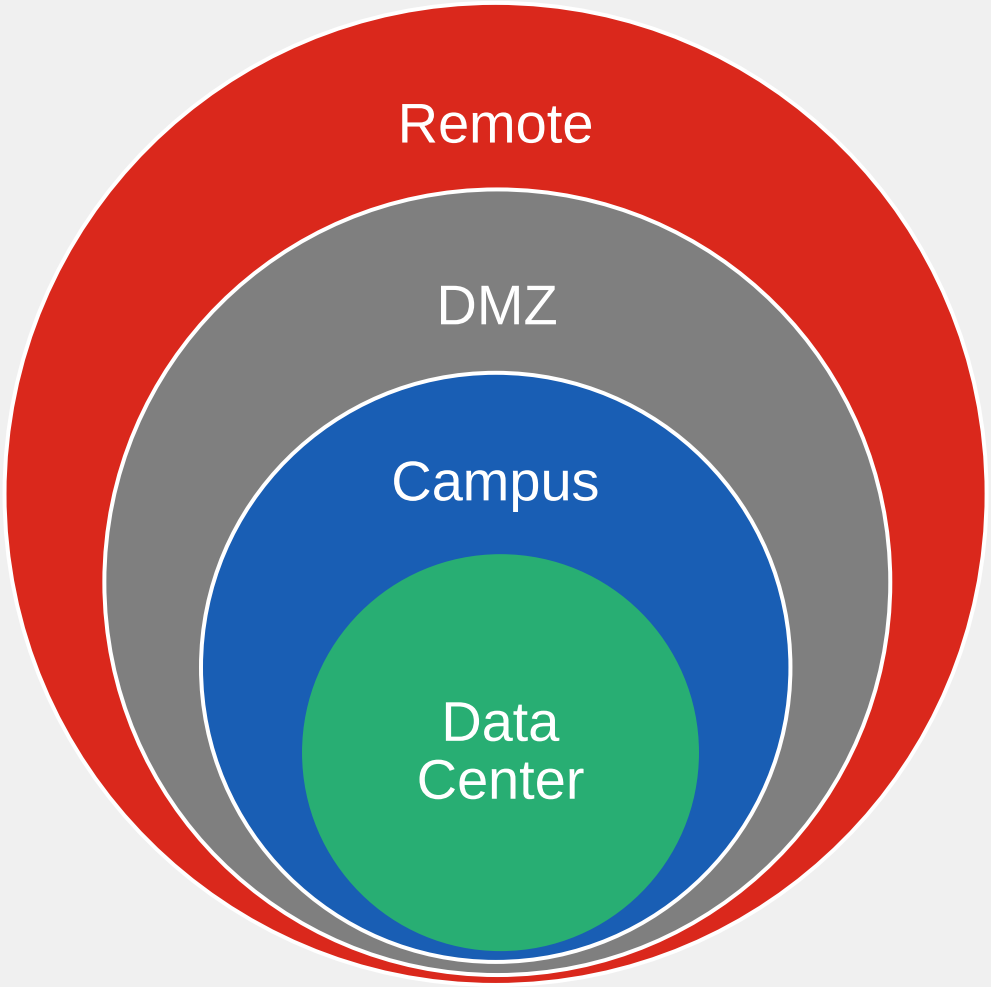
Workforce shifts from 4% teleworking to 30% teleworking by end of 2021[2]

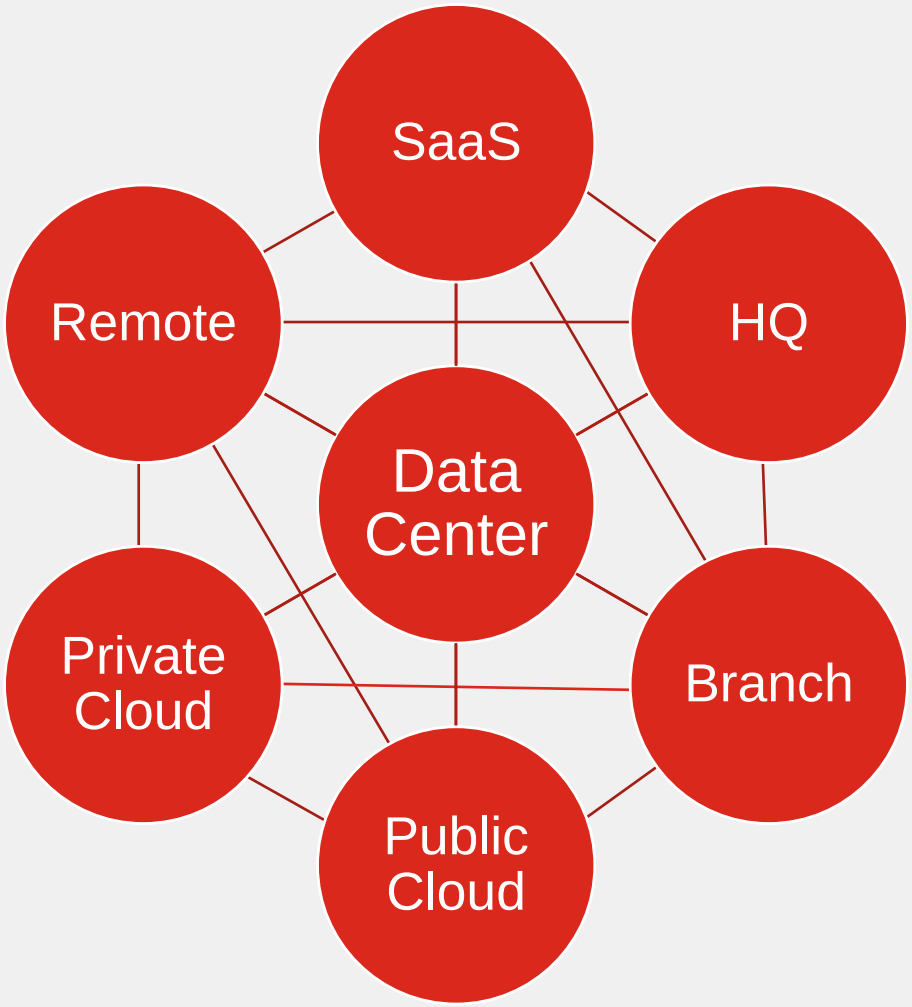


Since nearly every organization needs it, hybrid IT use-case requirements have become more common among Gartner clients.[4]

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

Architectures Change





What is ZTNA?

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’

Zero Trust Concepts

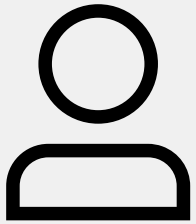
Zero Trust	What is it?	A philosophy for only trusting a user or device after explicitly confirming their identity and status. It focuses on users, devices, and the specific resources being accessed, utilizing segmentation and zones of control.
Zero Trust Architectures	Strategy:	Systematic approach to replace implicit trust with explicit trust after verification. Requires multiple technologies to address user, device, network, and cloud resource protection. Proposed architectures:
		• NIST SP 800-207 Zero Trust Architecture: NGFW, IAM, **ZTNA**, micro-segmentation
		• Forrester Zero Trust Edge: NGFW, SD-WAN, CASB, SWG, **ZTNA**
		• Gartner Secure Access Service Edge (SASE): SD-WAN, FWaaS, SWG, CASB, **ZTNA**
Zero Trust Initiatives	Specific Projects:	• Remote Access / Work From Anywhere
		• Network Segmentation
		• Micro-Segmentation
Zero Trust Technologies	Features/ Products:	• FortiClient / **Zero Trust Network Access (ZTNA**)
		• FortiPolicy (ShieldX- micro-segmentation)
		• FortiAuthenticator/ FortiToken /RBAC
		• FortiNAC / FortiLink NAC

Zero Trust in Business words

1. **Prioritize business needs over technology**: It is important that organizations do not view Zero Trust adoption as a technology initiative that is about replacing technology. Rather, it should support key business initiatives in a way that makes the organization more secure, flexible and resilient to change.
2. **Consensus on the need for Zero Trust**: Not only the cybersecurity team needs to be involved, but also the IT department, the helpdesk, the end users and other business stakeholders.
3. **Iterative and incremental approach**: Start with low-risk goals, such as a low-risk user population and/or set of applications, to minimize the potential for operational impact and implement lessons learned along the way. Ultimately, you can apply these insights to the company's most valuable "crown jewels" – the business-critical applications and data.

ZTNA Business Drivers in detail

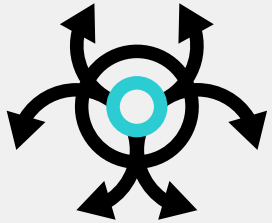
Work From Anywhere (WFA)



Users Access unaffected by Location

Improved User Experience

Ransomware Attacks



Granular Application Access

Reduced Attack Surface

Cloud Journey

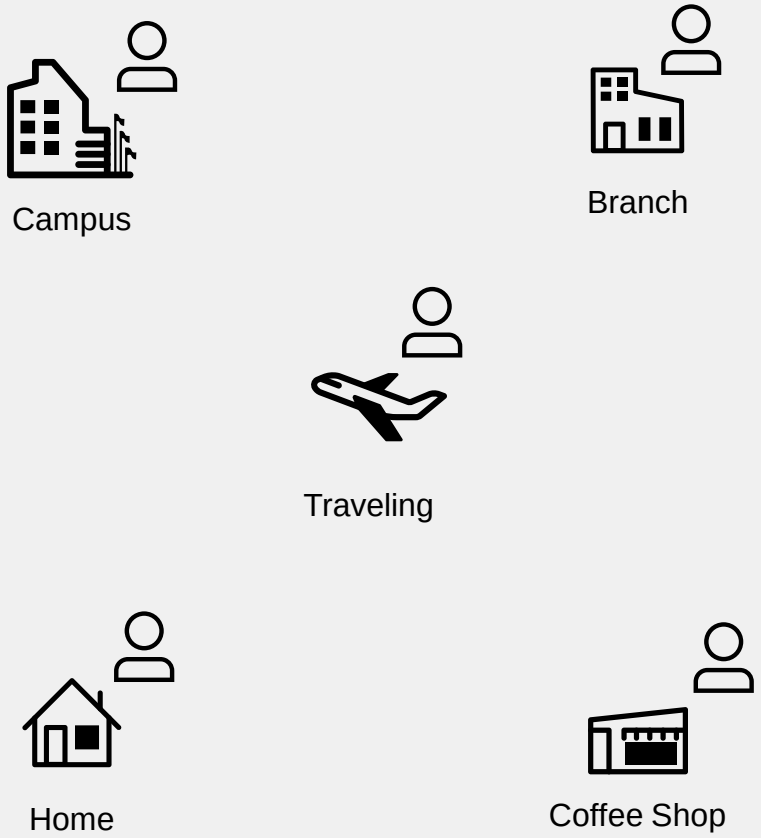
Applications unaffected by Location

Flexible Administration

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



Reducing the Attack Surface

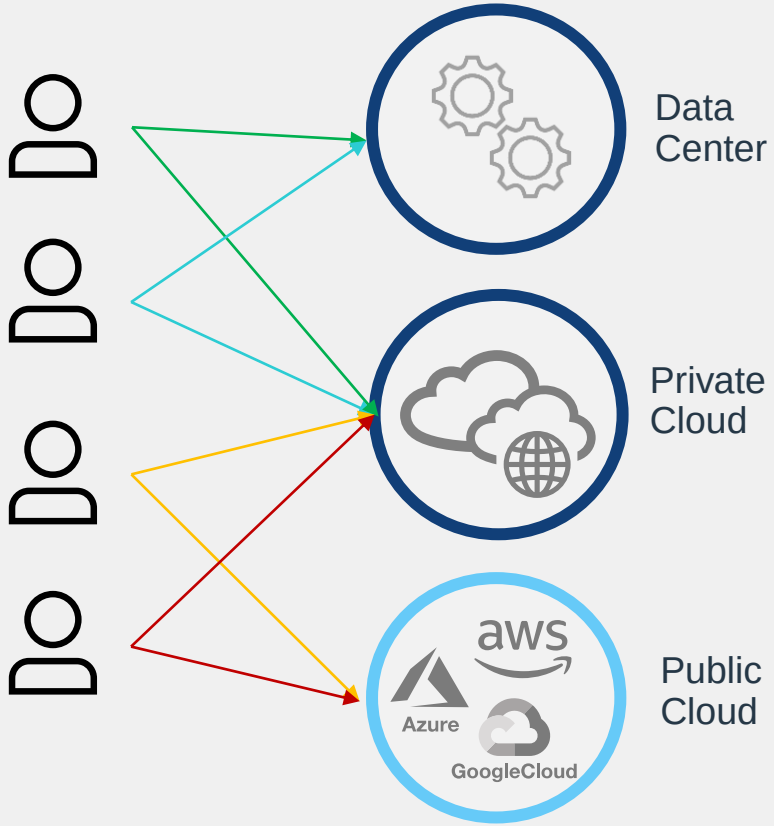
Granular Control to Applications

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

Supporting the Cloud Journey

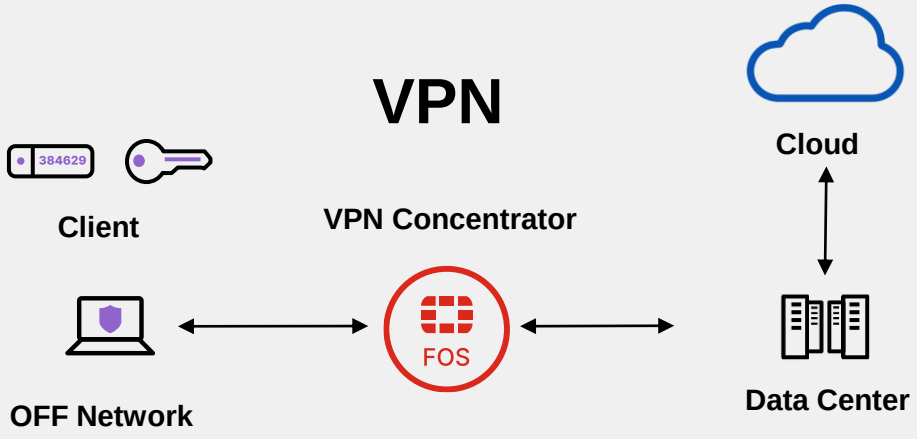
Controlling access to hybrid cloud architecture

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



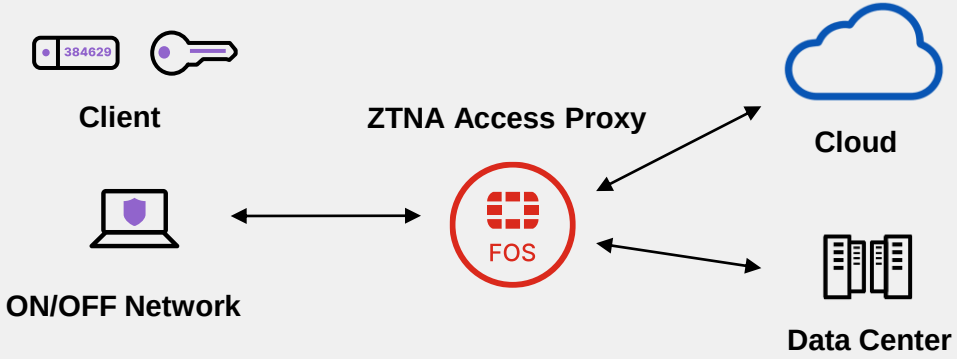
Evolution from Traditional VPN to ZTNA

VPN



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

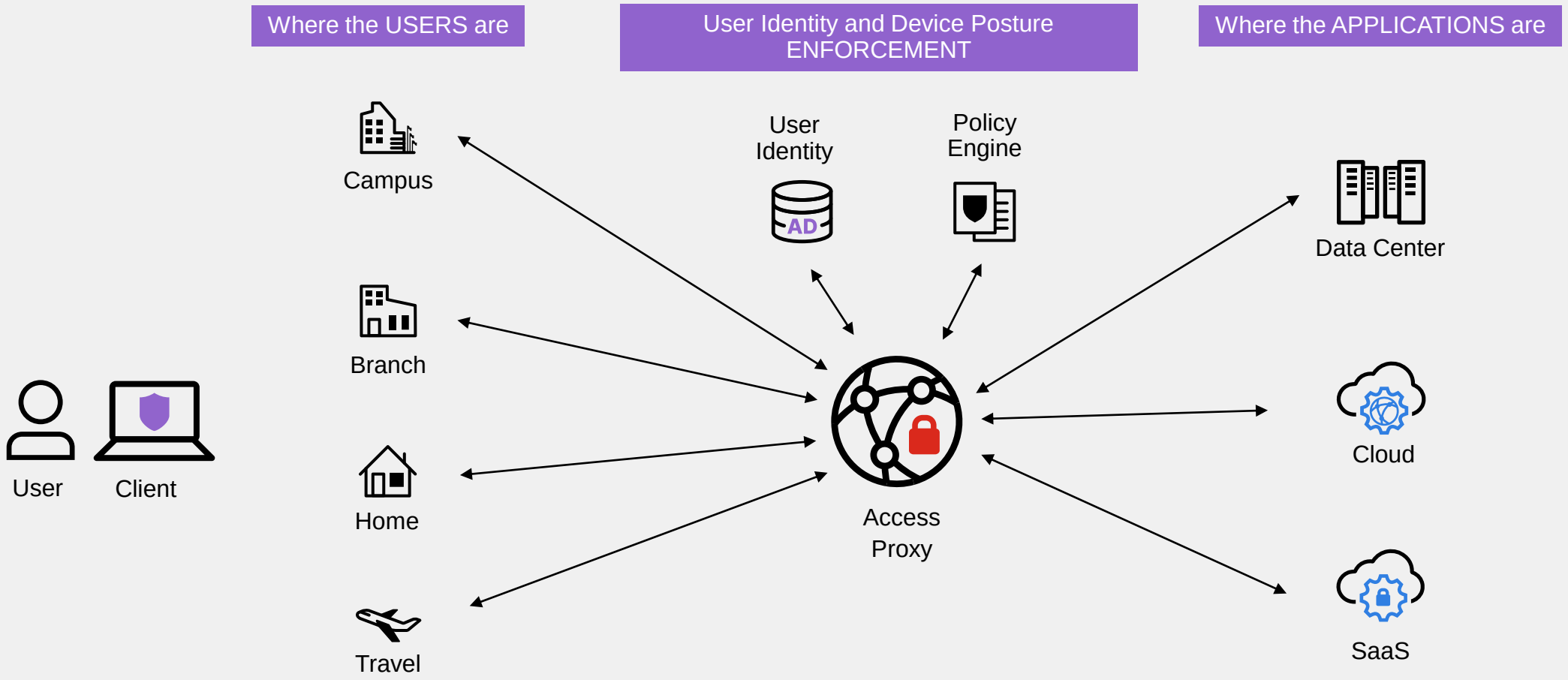
ZTNA



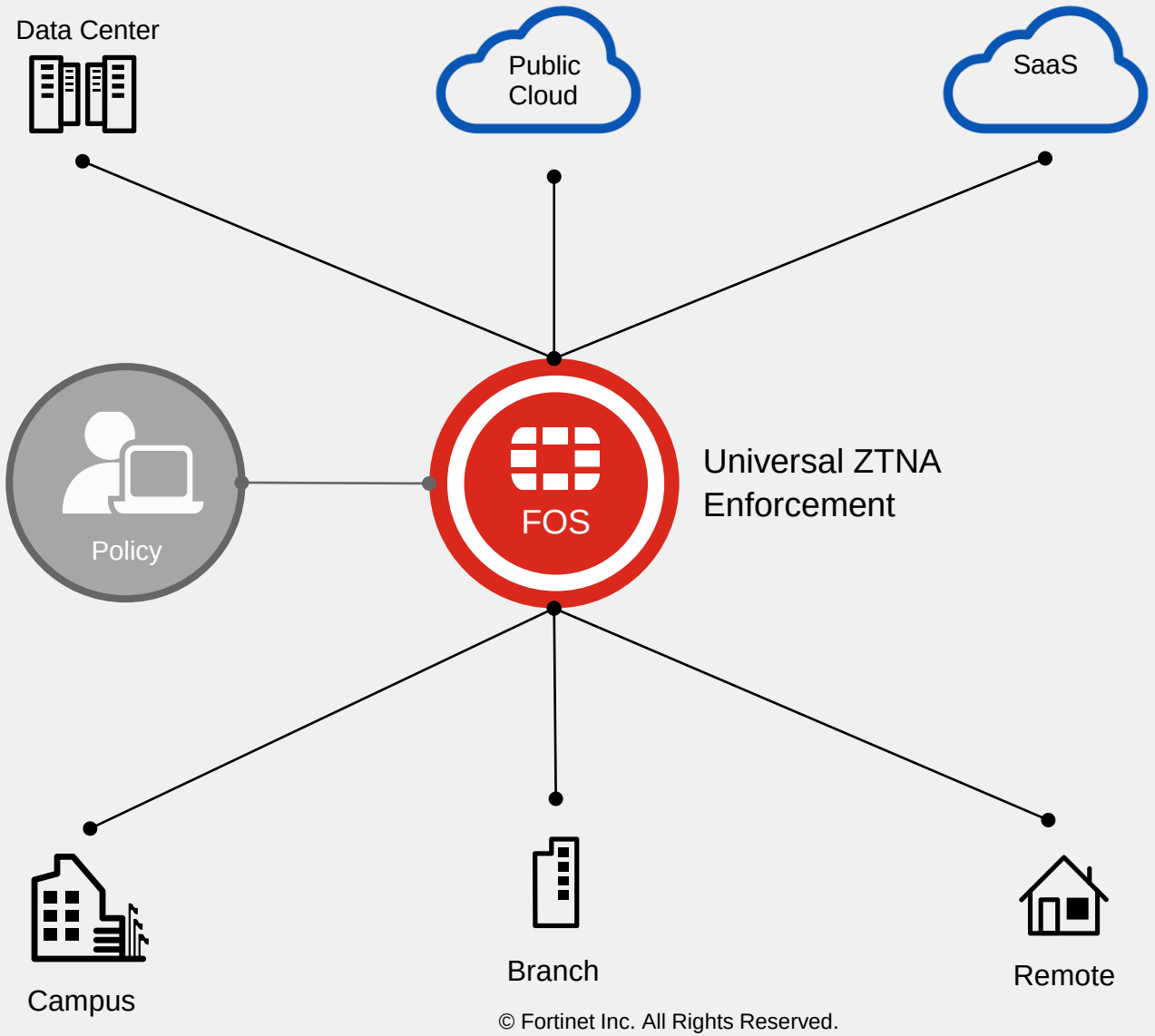
- Continuous Trust Check
- Access Specific Application
- User Contextual Rule Set

ZNTA Elements

The components of a client-based ZTNA solution



Universal ZTNA for Flexible Architecture

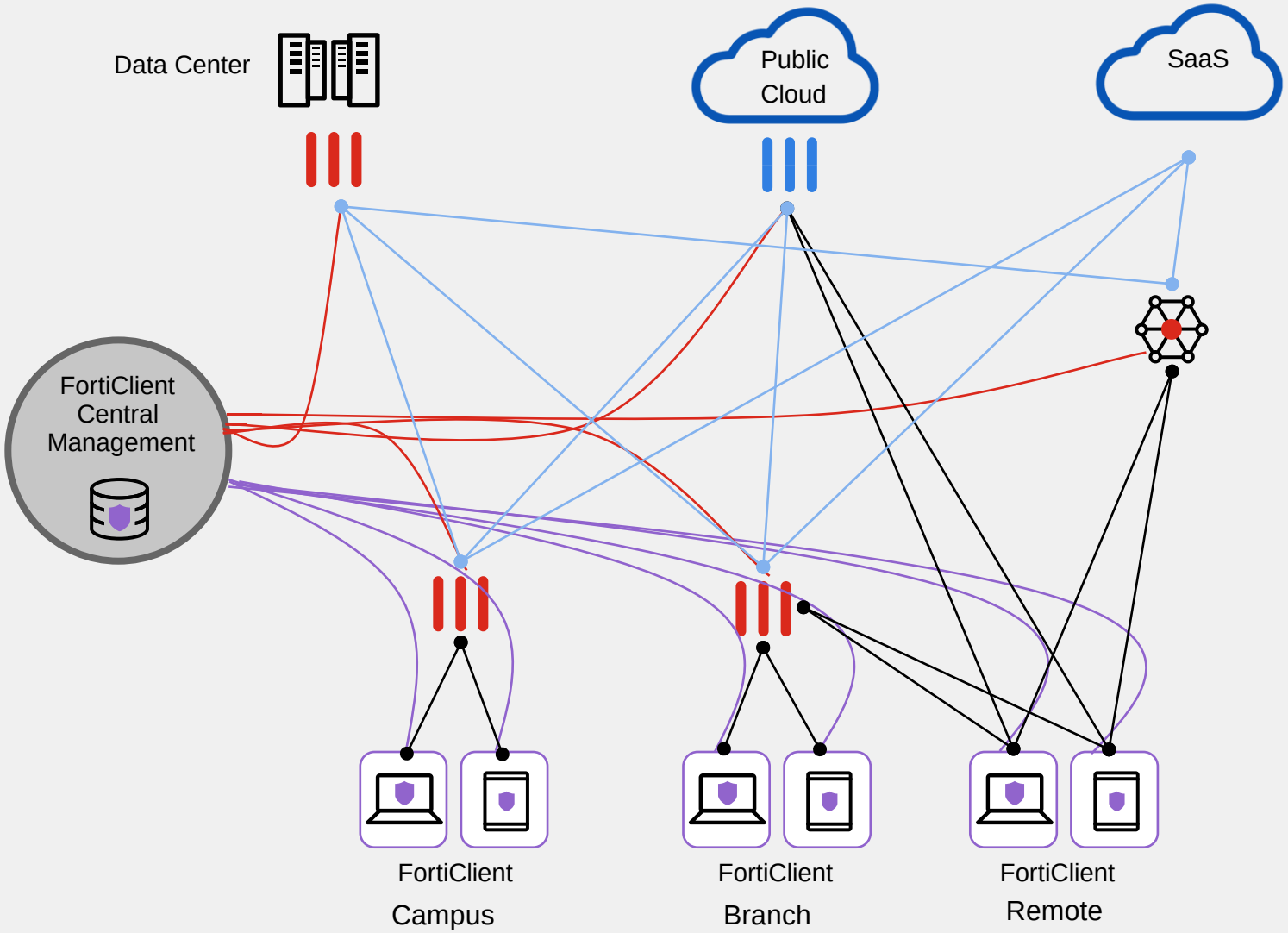


Wherever the application is

Verified user identity and device posture prior to access

Wherever the user is

ZTNA Process, High Level



ZTNA Telemetry

Fabric Sync

Tunnel & Posture Check

Access

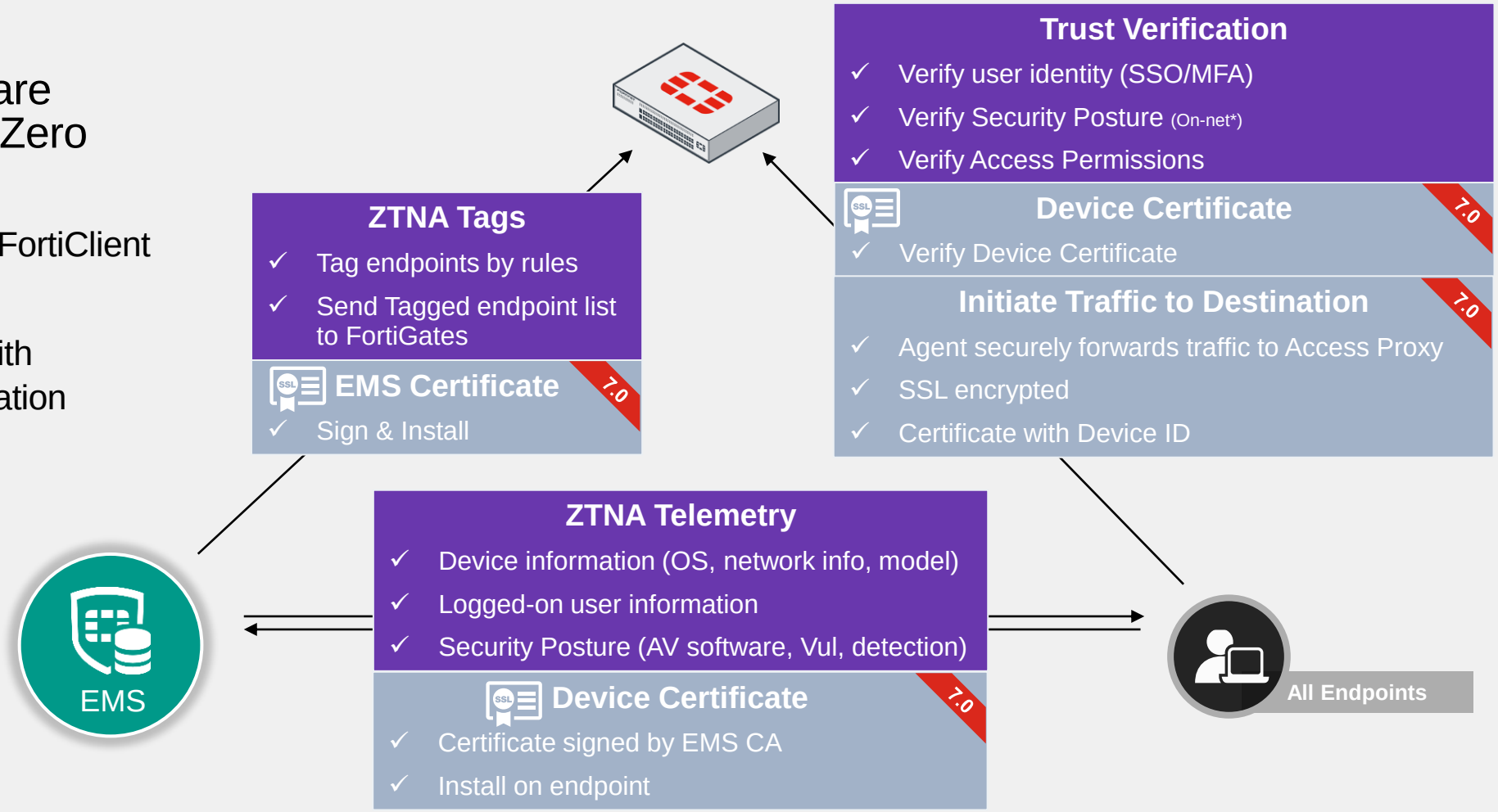
Get a deeper look inside

ZTNA , what's new @ Fortinet

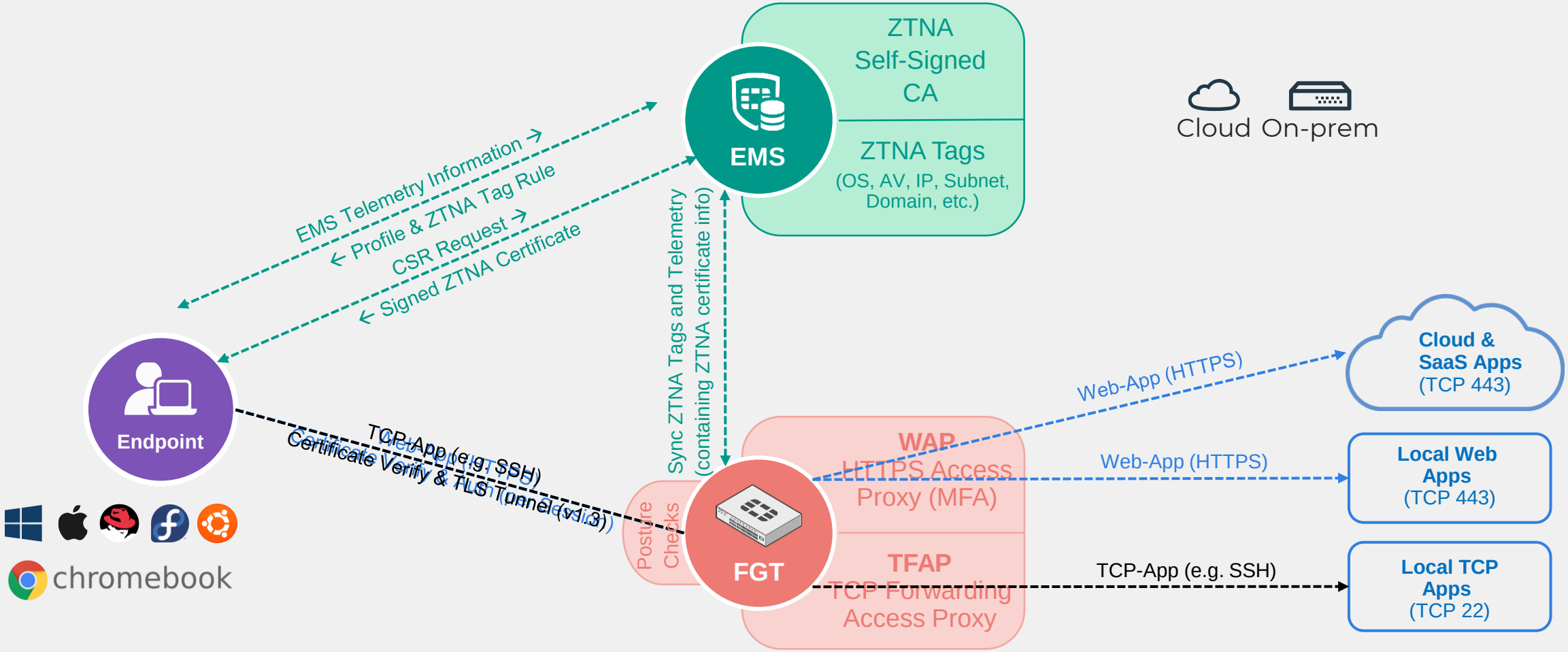
New Zero Trust Solution

Several new features are added to support new Zero Trust solution

- HTTPS access proxy with FortiClient as ZTNA agent
- Support trust verification with certificate-based authentication



What’s happening in the background?



Fortinet’s ZTNA

What’s it made of? Existing Fortinet Security Fabric Products

Core Elements

FortiGate

FortiClient / Central Management

- FortiGate builds the secure tunnel, maintains user group/application access table (FOS 7.0)
- FortiClient Central Management configures the ZTNA agent in FortiClient for the secure connection back to the FortiGate (FortiClient 7.0)
  - FortiClient Central Management: Either FortiClient EMS or FortiClient Cloud
- Authentication Solution
  - FortiAuthenticator, FortiToken or any 3rd party supported by the Security Fabric

Fortinet ZTNA advantages

Convergence of capabilities, Complete coverage, and Cost

- FOS-based ZTNA
  - Leveraging existing investments in FortiGates (lower TCO)
  - Complete WFA coverage, including campus
  - Traffic traversing Industry-leading FortiGate technology
  - Leverage SD-WAN, SD-Branch capabilities

- ZTNA Client also VPN client
  - Transition to ZTNA simplified
  - Shift to ZTNA at customer’s pace

- No Licenses Required (on FortiGate)
  - Simply a feature in FOS & FortiClient, just turn it on!

A recap

Bringing Zero Trust principles to Remote Access

- Ongoing verification of users and devices
  - 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®