Securing Critical Assets with FortiPAM

Marcus Moerke – Systems Engineer

What is PAM?

Privileged Access Management (PAM)

is a cybersecurity strategy meant to secure and monitor access to critical assets such as firewalls, servers, OT or cloud infrastructure. It ensures only authorized users can perform sensitive tasks such as configuration and maintenance while preventing unauthorized access to sensitive information.

Manage Privileged Access

Ensure only authorized users have access

Manage Privileged Credentials

Store credentials securely and automatically create and rotate passwords

Monitor and Record Sessions

Post session audit and ability to terminate sessions in real-time

FortiPAM Use Cases

Attack Mitigation

- Mitigate external attacks
- Prevent lateral spread

Threat Prevention

Prevent insider threat

- Many cyber attacks are perpetrated by users who had been given privileged access to an organization's IT system

Access Control

Control third-party access

- Organizations routinely outsource operations to external service providers
- Audit usage for billing purposes.

Compliance

- Meet Cybersecurity Insurance requirements
- Achieve compliance

Visibility

- Provide visibility and management of access to critical assets

FortiPAM Features

FortiPAM Key Functions

Providing credential vault

- End users does not know or see the credentials
- Reduces the risk of credentials leaking

No sensitive data left on end-user computer
Automatic password changing

Only authorized users can access specific resources

- Least privilege access based on roles (Standard User, Administrator, Custom)
- Secret permission control
- Administrator defined policy and permission

ZTNA Controls
Hierarchical approval system
Control of risky commands

Session activity surveillance

- Session list monitoring
- Session recording
- Over the shoulder monitoring Roadmap
- Post session audit

Keystroke, mouse events monitoring
Video recording

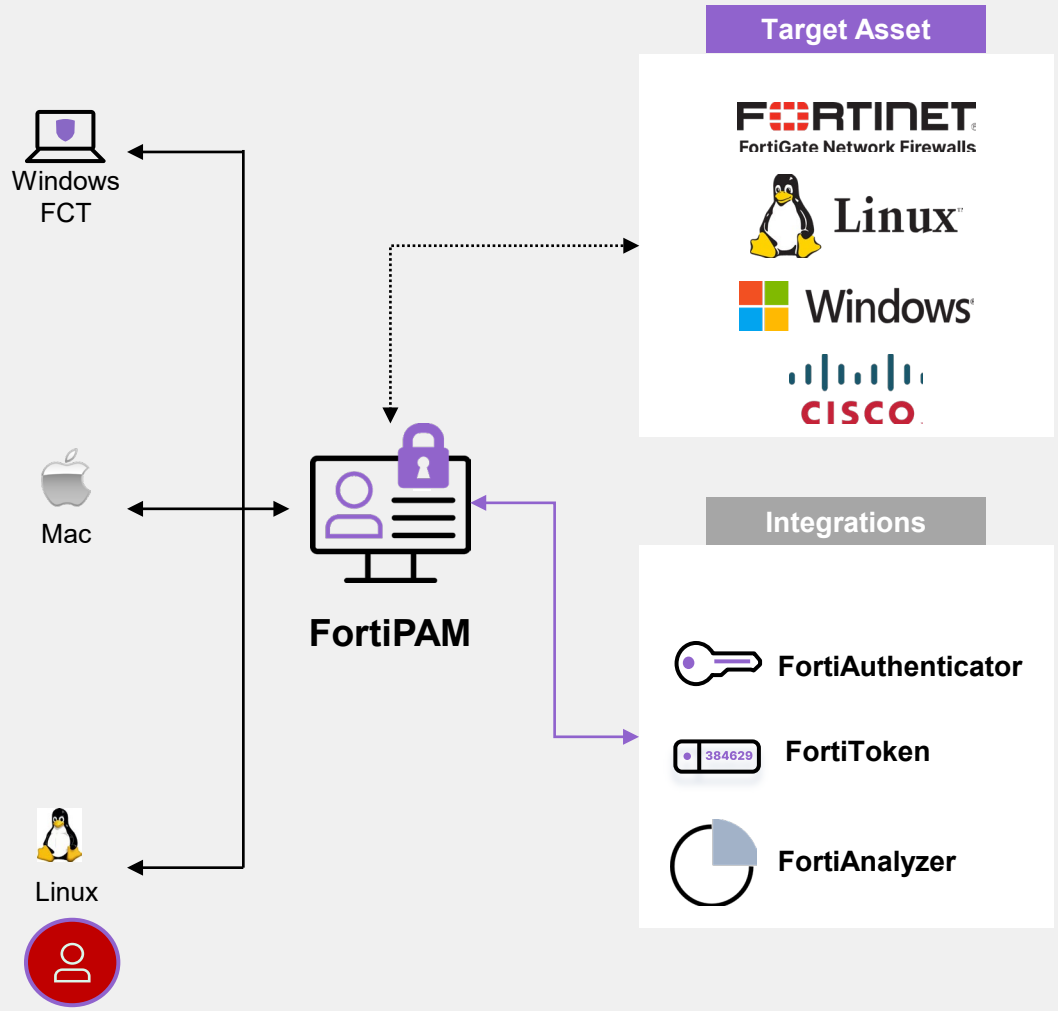
FortiPAM Solution Components

FortiPAM server

- FortiOS/FortiProxy platform and framework
- GUI
- Backend application

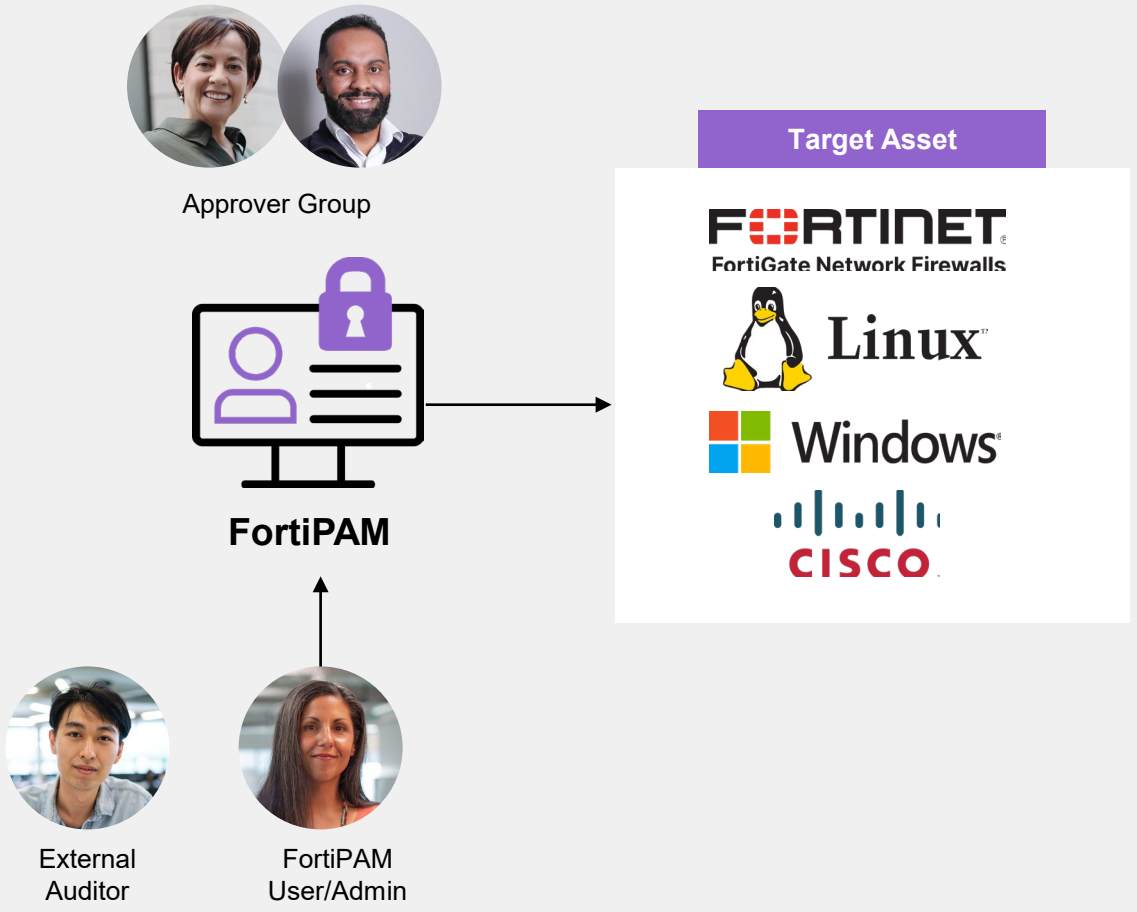
FortiClient

- FortiVRS – Video Recording Service
- FortiTCS – ZTNA Service
- Web Extension (Chrome, Edge, Firefox)



FortiPAM Key Functions

- Hierarchical approval
- Session Surveillance and Audit
- Scheduled credential changing
- Secret check-out/check-in



Asset Access Monitoring

User Monitor

- Logged in user
- Keyboard/mouse activity logging

Active Sessions

- Sessions currently being proxied to critical asset
- Active viewing with session termination capability

Secret Video

- View logs of video recordings
- Playback recordings from the log viewer

FortiPAM Advantages

- Why FortiPAM is growing as fast as it is

Unique Security

- ZTNA
- Anti-Virus
- DLP

Ease of Use

- Core PAM capabilities
- Quick to deploy and use
- Flexible options: appliance, VM, cloud

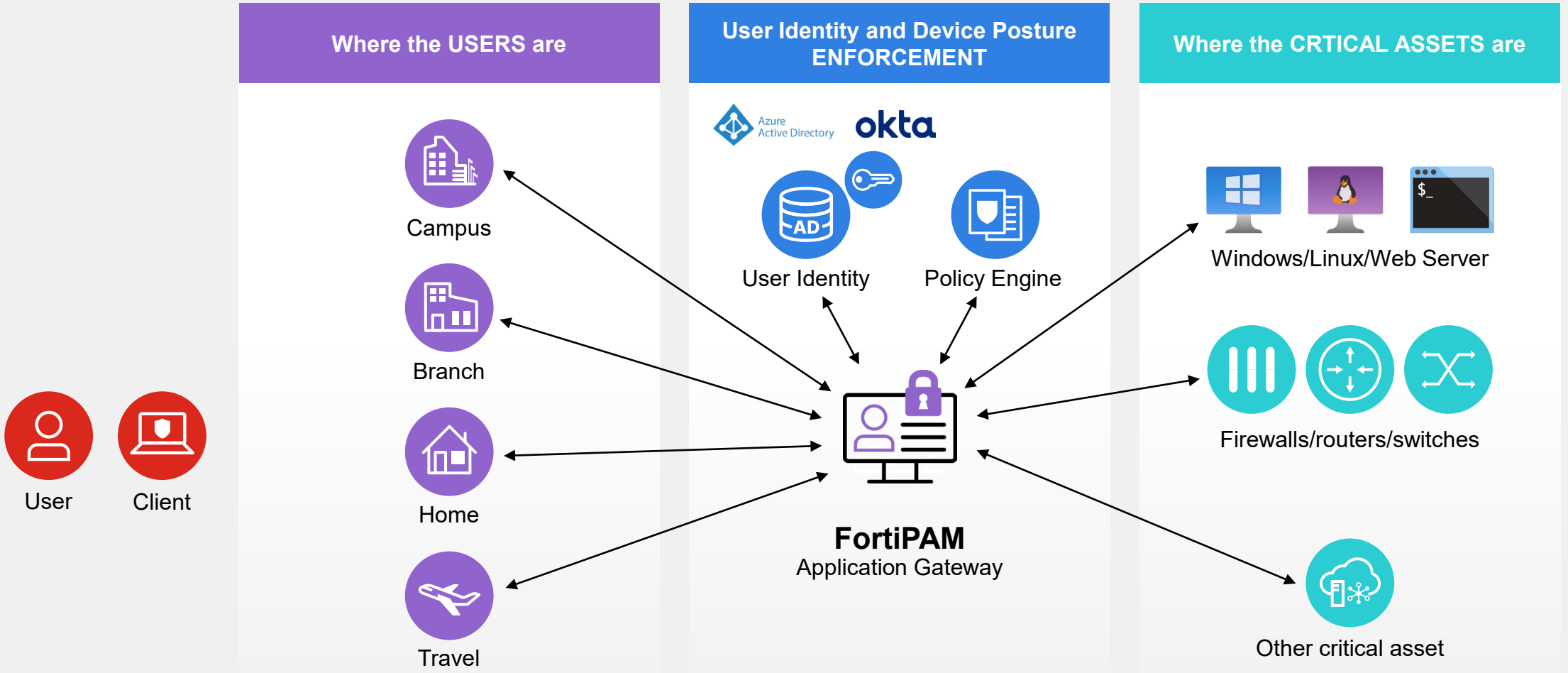
Value

- No hidden costs for additional features
- Established vendors charging way too much

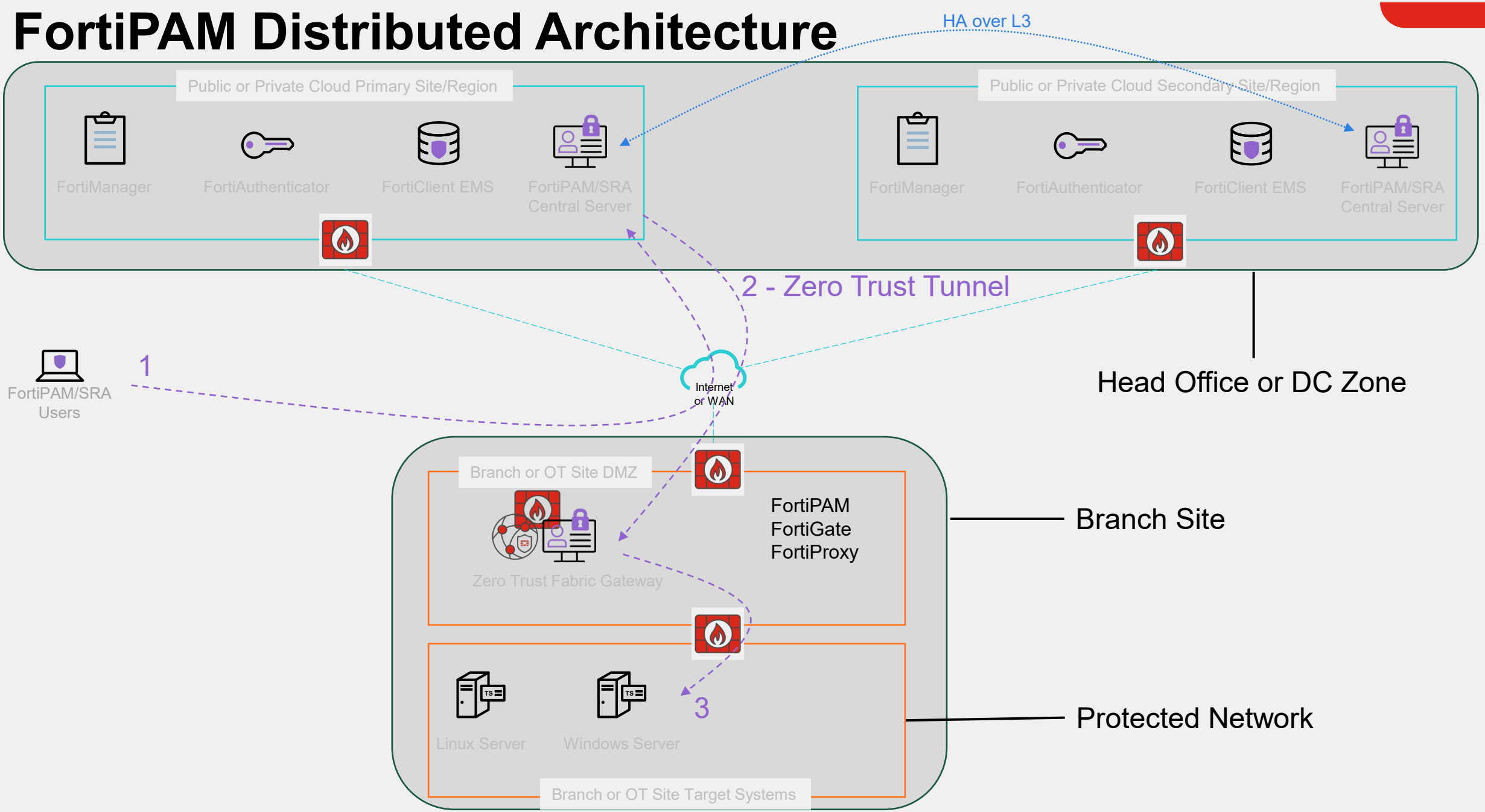
Zero Trust

ZTNA Elements – FortiPAM as Application Gateway

The components of a client-based ZTNA PAM solution

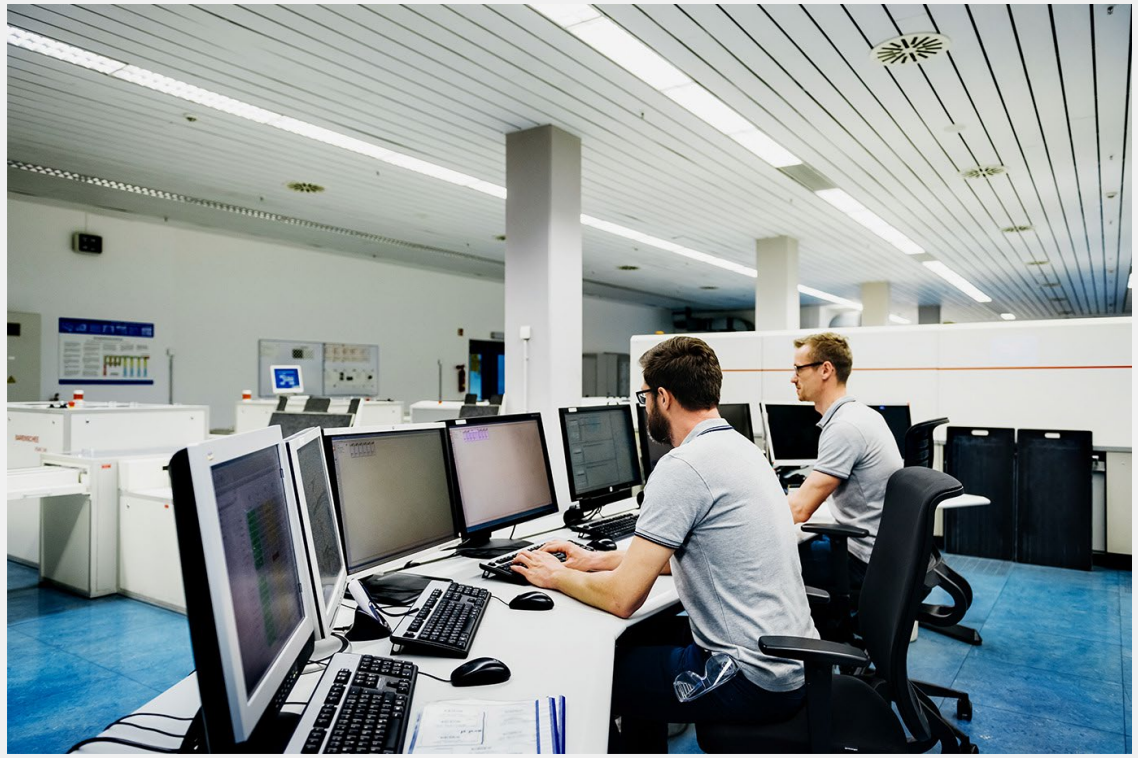


FortiPAM Distributed Architecture



Securing Access to Critical Assets

- Manage Access to Critical Assets
  - Servers, network infrastructure (FortiGate), OT devices
  - Easily provision role-based user access
  - Automatic password changing
- Enhanced Security
  - Control access using ZTNA tags + MFA
  - Scan file uploads for malicious content
  - DLP protection
- Monitor and Audit
  - All sessions recorded for audit purpose
  - Session termination capability
  - Fulfill cybersecurity insurance requirements




FORTINET