Fortinet FortiPAM

Thomas Hans

Senior Systems Engineer

KBC Forum 2023

Agenda

- **Privileged Access Management** (PAM)
- **FortiPAM Solution Overview**
- **Key Functions**
- **Feature Deeper Dive**
- **Competitive Advantages**
- **Resources**

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Vorstellung

Thomas Hans
Sr. Channel Systems Engineer

E: thans@fortinet.com
M: +49 170 57 90 180
Feldbergstrasse 35 | 60323 Frankfurt | GER
Home Office Standort Bielefeld

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Securing people, devices, and data everywhere.

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our security solutions are among the most deployed, most patented, and most validated in the industry.

Global Customer Base **680,000+** Customers	2022 Billings **$5.59B+** *(as of Dec 31, 2022)*	Market Capitalization **$59.38B** *(as of June 30, 2023)*
Broad, Integrated Portfolio of **50+** Enterprise Cybersecurity Products	Strong Analyst Validation **41** Enterprise Analyst Report Inclusions	Vertical Integration **$1B+** Investment in ASIC Design & Development

FORTINET

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500**

Member of: **2022 Dow Jones Sustainability World and North America Indices**

Security Investment Grade Rating: **BBB+ Baa1**

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

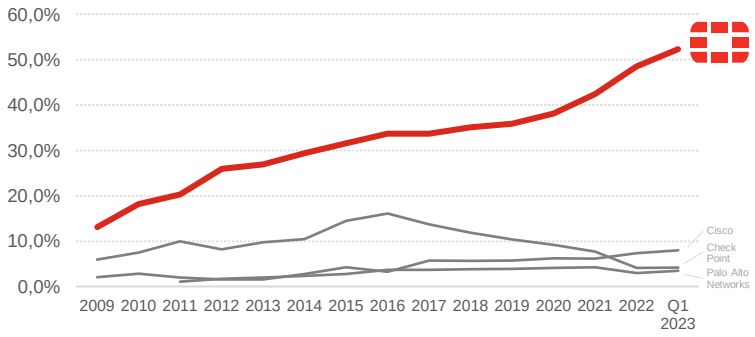
Investing in Innovation for Our Customers

Strong investment in our supply chain

~50%

of All Next-Gen Firewall Shipments &
#1 in revenue market share

Global Firewall Shipments



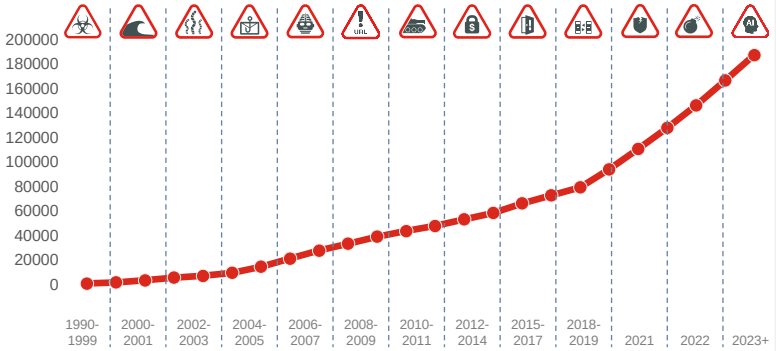
Source: IDC Quarterly Security Appliance Tracker 2023Q1 (based on shipments of Firewall + UTM appliances)

Investment in scale of threat intelligence and AI/ML

100+B

global security events analyzed per day

Advanced Threats – Global CVE

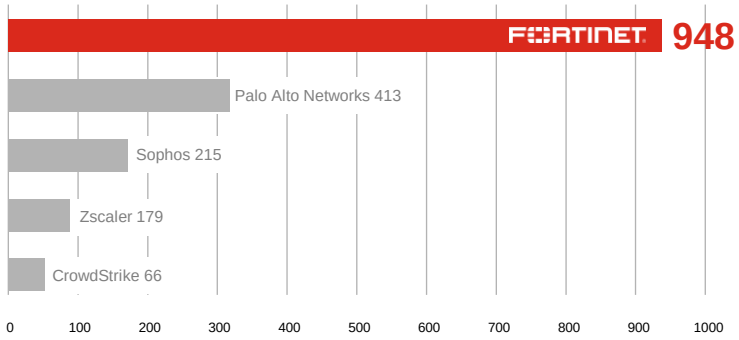


Organic R&D investment across our portfolio

1,285

Global Industry Patents

U.S. Patents



Source: U.S. Patent Office, as of June 30, 2023

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Privileged Access Management (PAM)

FortiPAM

2008 „Netzwerk Kidnapper“

heise online heise+ Jetzt 1 Monat gratis testen

IT Wissen Mobiles Security Developer Entertainment Netzpolitik

TOPTHEMEN:

APPLE KÜNSTLICHE INTELLIGENZ ASTRONOMIE WINDOWS ENERGIE E-I

OPEN SOURCE PODCASTS

"Netzwerk-Kidnapper" von San Francisco muss sich vor Gericht verantworten

Dem Netzwerkadministrator, der Router und Switches des städtischen Kommunikationsnetzes von San Francisco so manipuliert hatte, dass niemand außer ihm mehr darauf zugreifen konnte, drohen bei einer Verurteilung mehrere Jahre Haft.

Lesezeit: 2 Min. In Pocket speichern

29.12.2008 16:46 Uhr

Von Peter-Michael Ziegler

heise online heise+ Jetzt 1 Monat gratis testen

IT Wissen Mobiles Security Developer Entertainment Netzpolitik

TOPTHEMEN:

APPLE KÜNSTLICHE INTELLIGENZ ASTRONOMIE WINDOWS ENERGIE E

OPEN SOURCE PODCASTS

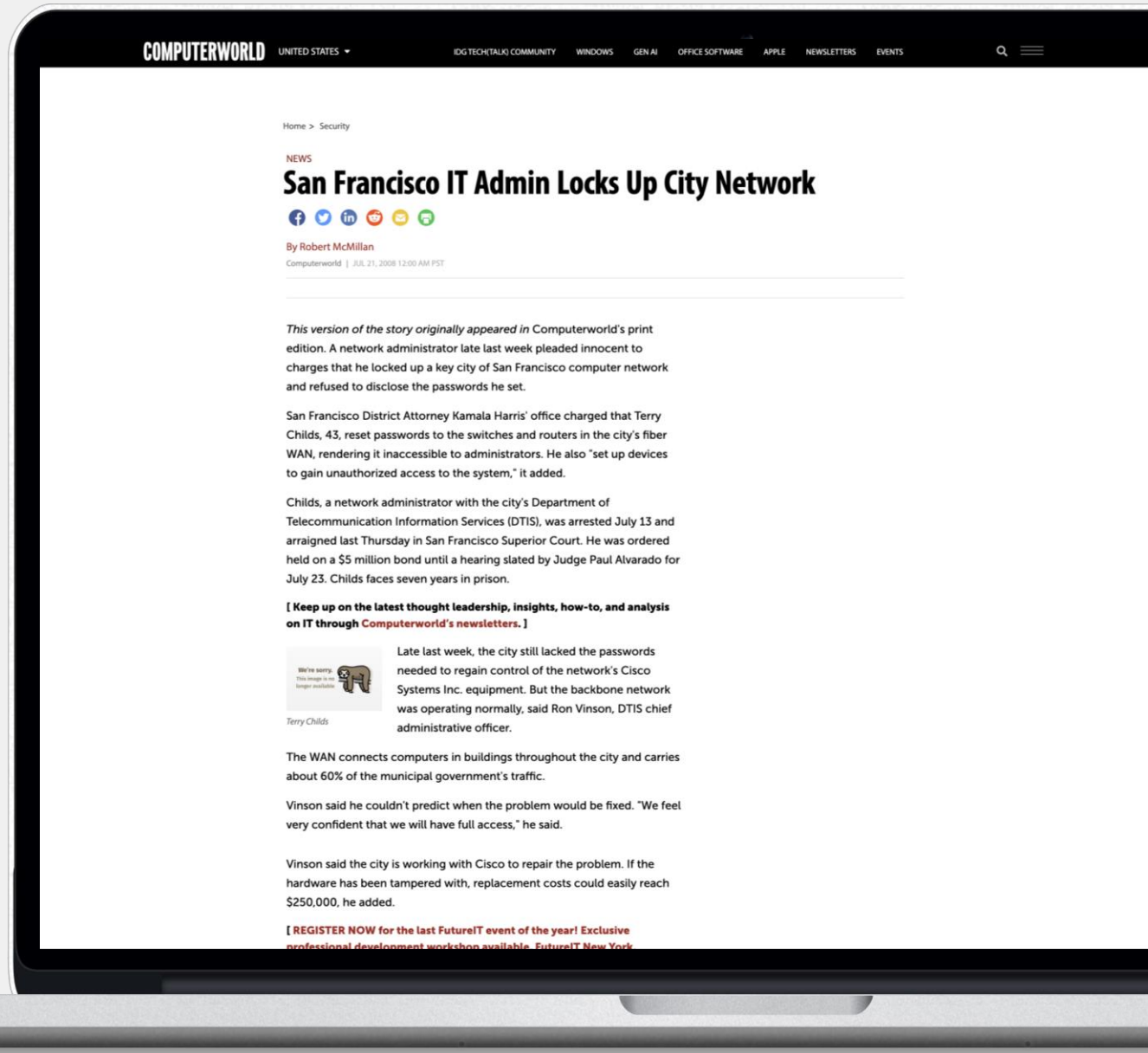
"Netzwerk-Kidnapper" von San Francisco schuldig gesprochen

Ein Netzwerkadministrator, der im Sommer 2008 weltweit für Schlagzeilen sorgte, weil er zentrale Komponenten des städtischen Kommunikationsnetzes so manipuliert hatte, dass außer ihm niemand mehr darauf zugreifen konnte, ist am Dienstag schuldig gesprochen worden. Die Jury sparte aber auch nicht mit Kritik an seinen Vorgesetzten.

Lesezeit: 3 Min. In Pocket speichern 171

28.04.2010 15:00 Uhr

Von Peter-Michael Ziegler

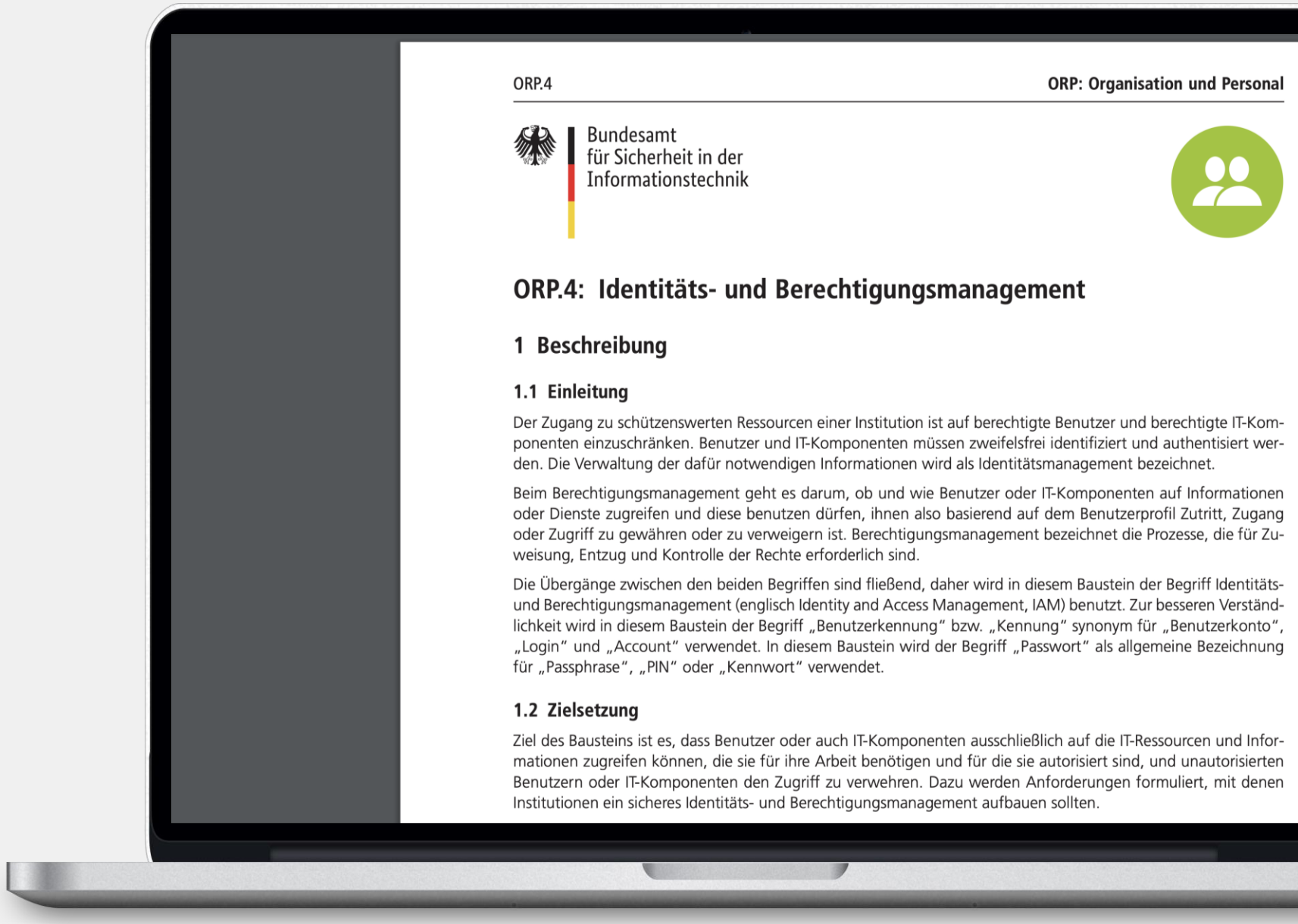


© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM

BSI IT Grundschutz

ORP.4 & OPS.1.1.2



[Quelle: BSI]

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Privileged Access

Privileged Access is access to privileged accounts by privileged users (e.g., IT Managers and System Administrators)

Privileged Account

A **privileged account** is any account that exposes resources, information and operations beyond those of standard, non-privileged accounts. Privileged accounts can be associated with human identities or machine identities.

Privileged User

A **privileged user** is any user currently having access to a privileged account.

Risk Factor

Because of their access to elevated capabilities, privileged users and privileged accounts pose considerably **larger risks** than non-privileged accounts / non-privileged users.

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

What is Privileged Access Management (PAM)?

- PAM is a cybersecurity strategy that helps protect organizations against cyberthreats by adding layers of protection to reduce the attack surface and mitigate risk of data breaches
- Involves people, processes, and technology
- Uses principle of least privilege
  - Limits the number of users that can access privileged accounts
  - users are assigned only the minimum level of access required to perform their job function
- Provides for vaulting of credentials
- Monitors, records, detects, and prevents unauthorized privileged access to critical resources
- Gives visibility into who is using privileged accounts and what they are doing
- BSI ORP.4 & OPS.1.1.2

Areas of PAM Use Cases

Five Primary Use Case Areas

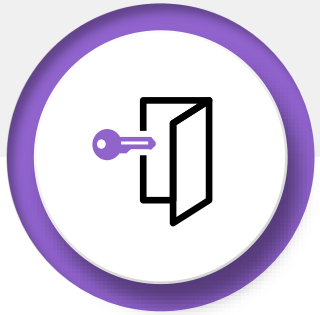
Attack Mitigation

- Mitigate external attacks

Threat Prevention

Prevent insider threat

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



Access Control

Control third-party access

- Organizations routinely outsource operations to external service providers
- Majority of these have been victims of a security breach
- Some major security breaches were attributed to an external service provider
- Contractor Access

Compliance

- Achieve compliance
- Obtain cybersecurity insurance

Visibility

- Provide visibility and management of cloud systems and services

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM

Solution Overview

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
- Post session audit

Keystroke monitoring
Video recording

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

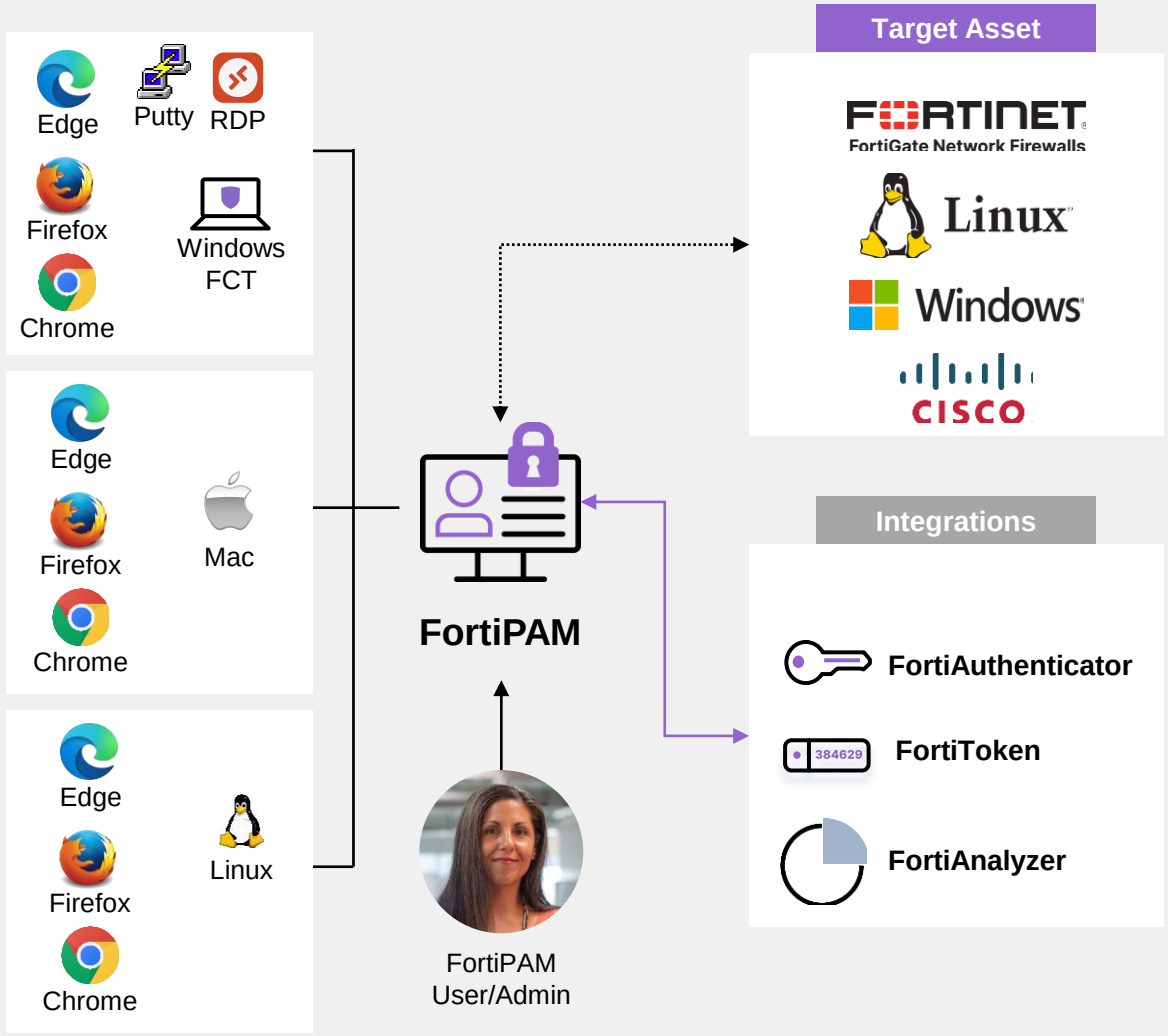
FortiPAM Solution Components

FortiPAM server (mandatory)

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

FortiClient / Web Extension(optional)

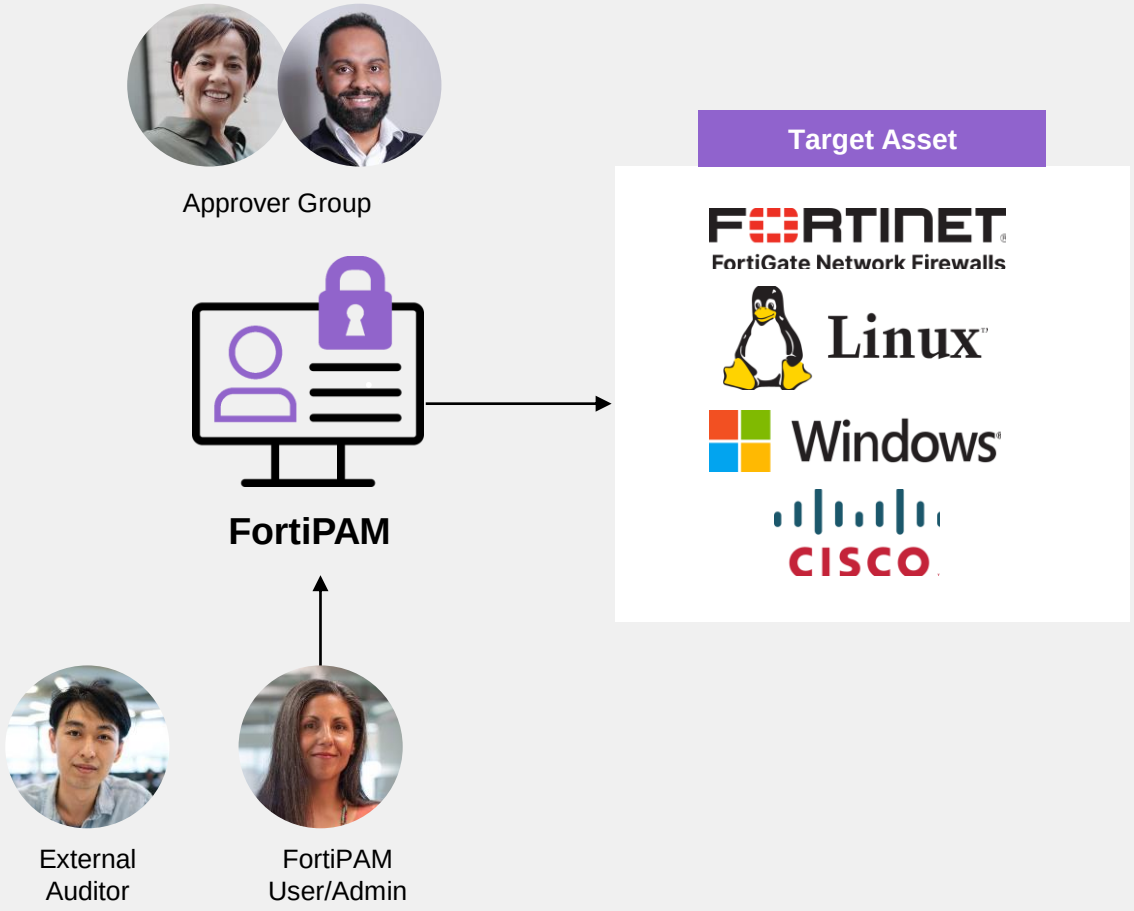
- FortiVRS – Video Recording Service
- FortiTCS – ZTNA Service
- Privileged Access Agent / Web browser Extension/Password filler (Chrome, Edge, Firefox)



© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM Key Functions

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



© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM

Concepts & Features

FortiPAM User Management

User Authentication Methods

- Local User
- Remote User: RADIUS Server
- Remote User: AD/LDAP Server
- Remote User: SAML IdP

Strong Security

- MFA Methods:
  - Native - FTM OTP, Email/SMS OTP
  - FortiToken Cloud – multiple MFA methods, Adaptive Auth
  - FortiAuthenticator - multiple MFA methods, Adaptive Auth, FIDO

Additional Native Security Measures

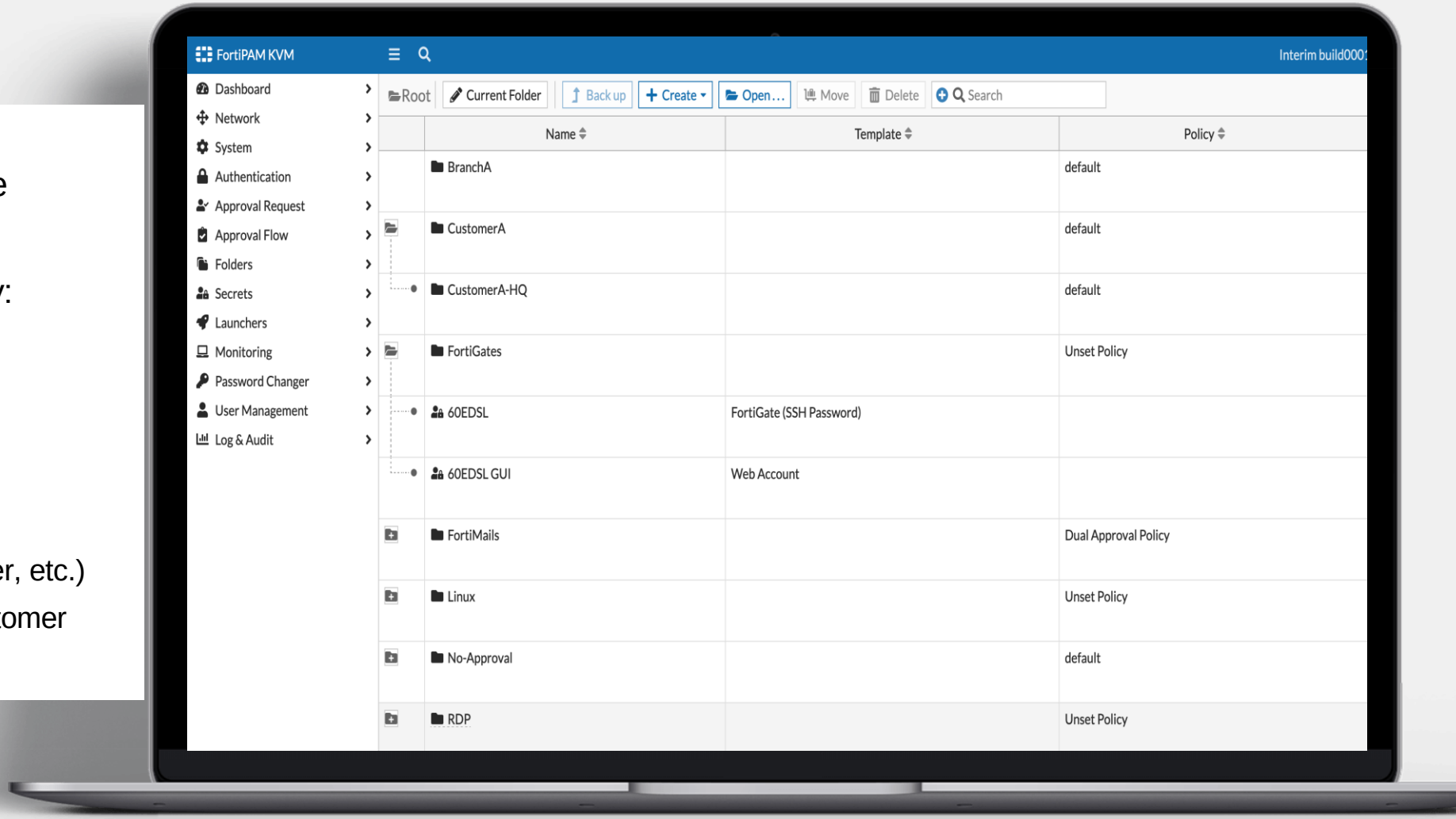
- Source IP Check
- Schedule to limit access
- ZTNA control (required FortiClient ZTNA agent

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Folder Management

Hierarchical containers used to organize secrets

- Folders can be used to organize and manage the secrets
- Folders can organize secrets by:
  - customer
  - region
  - site
  - department
  - type of target (FortiGate, web server, Linux server, etc.)
  - whatever makes sense for the customer



© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Folders

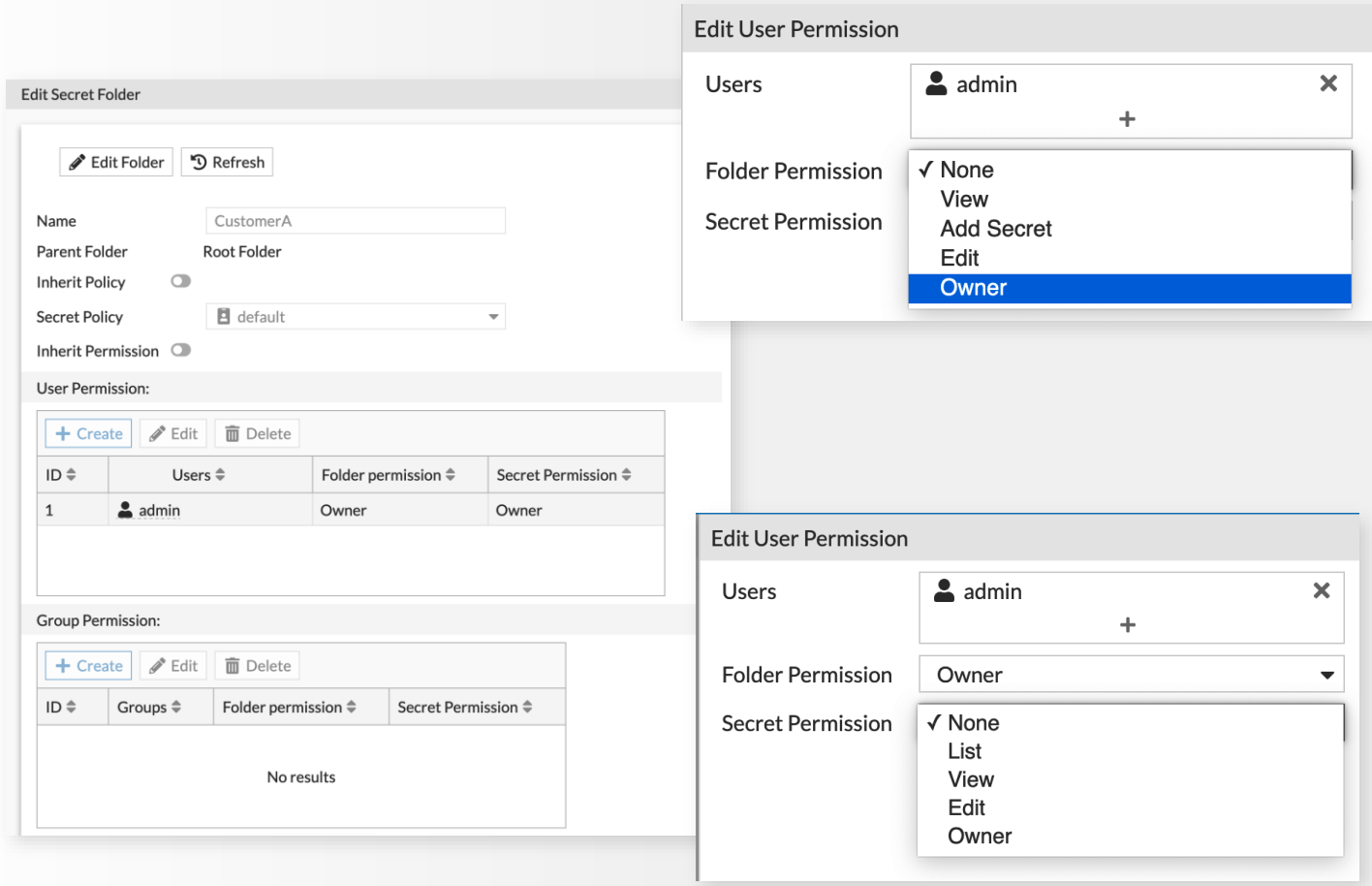
Permissions control who can access folders and secrets

Inheriting Policy

- Inherit Policy - **Enabled**:
  Subfolder uses same policy
  of parent folder
- Inherit Policy - **Disabled**:
  Choose any pre-configured policy
  for the folder

Permission

- User and Group level setting
- Can be inherited from higher level folder
- Can be configured explicitly
  - Folder Permission: view, add, edit, owner
  - Secret permission: list, view, edit, owner

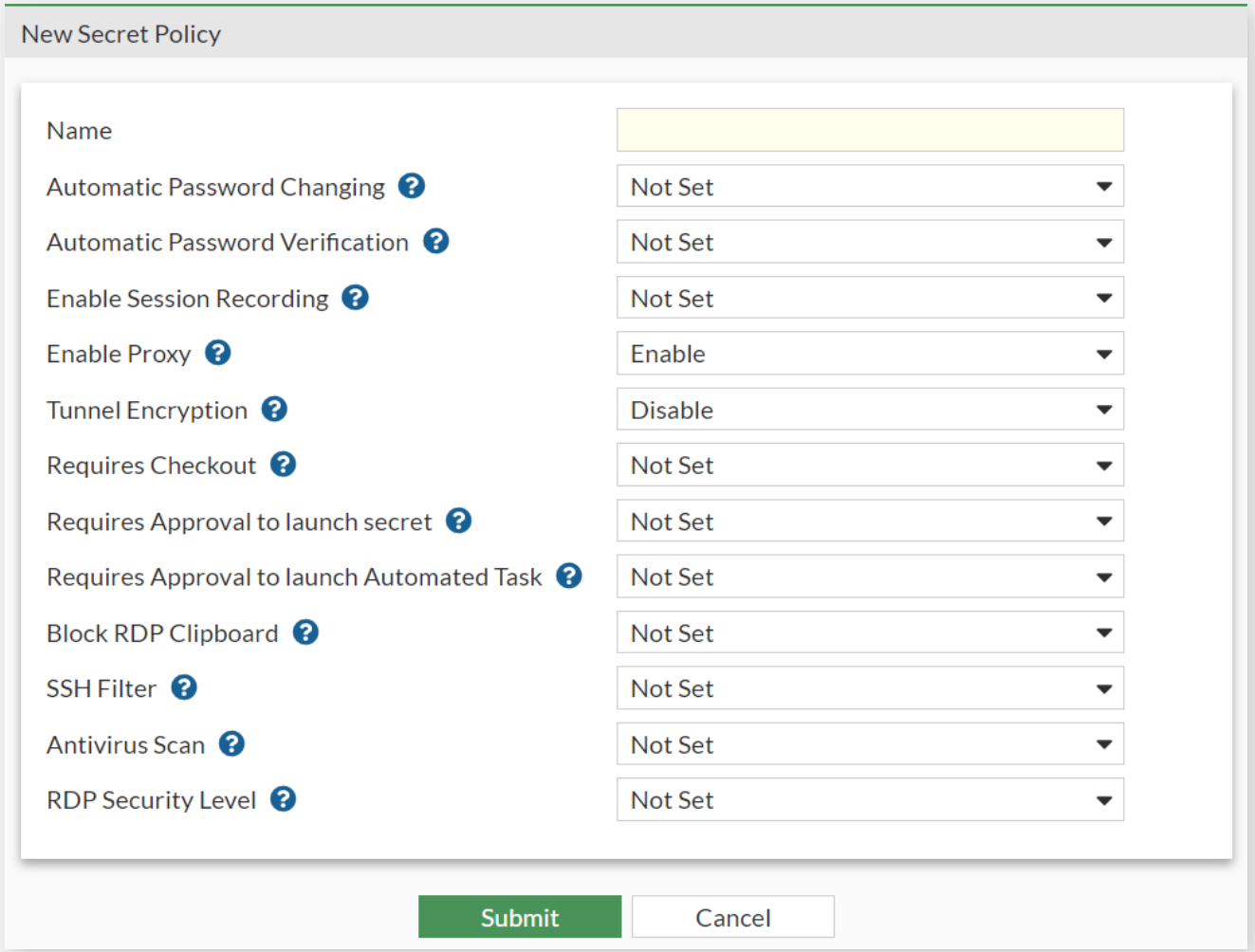


© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Secret Policies

Policy allows you to pre-configure the settings for a secret

- Automatic Password Changing
- Automatic Password Verification
- Enable Session Recording
- Enable Proxy
- Tunnel Encryption
- Requires Checkout
- Requires Approval to Launch Secret
- Requires Approval to Launch Job
- Antivirus Scan
- RDP Security Level
- Block RDP Clipboard
- SSH Filter prevents certain commands from running on an SSH terminal



© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Secret Launchers

A secret *launcher* starts applications on end-user devices and automatically logs on target server using credentials stored in the FPAM secret.

Supported Target Server Types

SSH Servers
- Password mode
- Key mode

RDP Servers
- Windows Servers and Workstations, Linux RDP
- AD Account, Windows local Account

VNC Servers
- General VNC Server (Windows, Linux)
- Mac OS VNC Server

Network Devices
- Cisco ISO: “User Mode” and “Enable Mode”
- FortiOS
- Custom (e.g., for Juniper)

Web Apps
- AWS
- VSphere
- FortiOS Admin
- GUI
- etc.

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FPAM Native and Web-based Secret Launchers

Default Native app launchers

- Putty
- WINSCP
- Remote Desktop
- MSTSC
- VNC viewer
- TightVNC

Default Web-based launchers

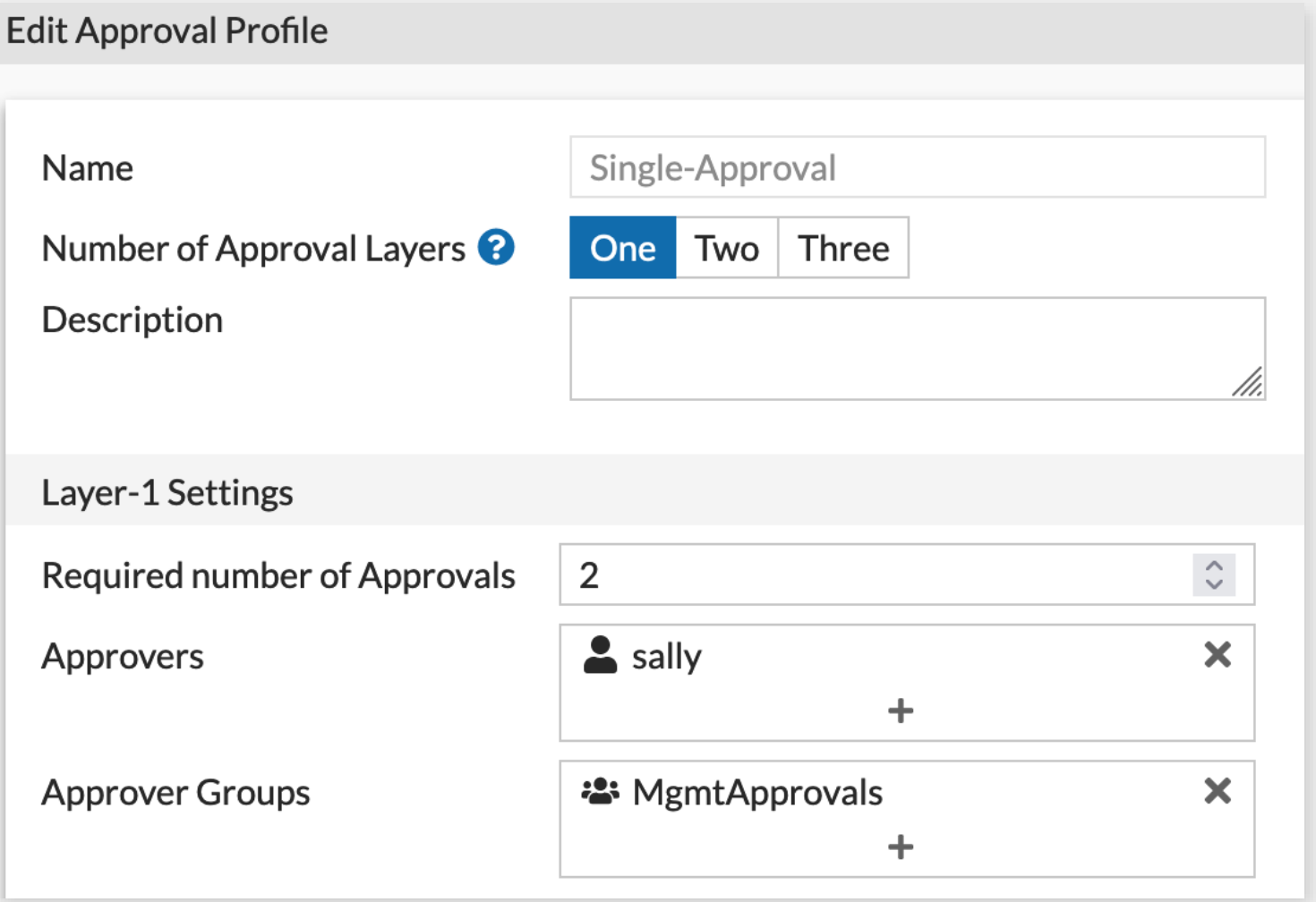
- Web-SSH
- Web-RDP
- Web-VNC
- Web-SFTP
- Web-SMB

Custom Native Launchers can also be configured in FPAM

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Approvals

- If a secret is configured with an approval policy, approval must be granted before a user may access that secret
- Hierarchical - up to 3 tiers of approval
- Minimum number of approvals may be required for each layer of approval
- Both users and groups may be selected as approvers

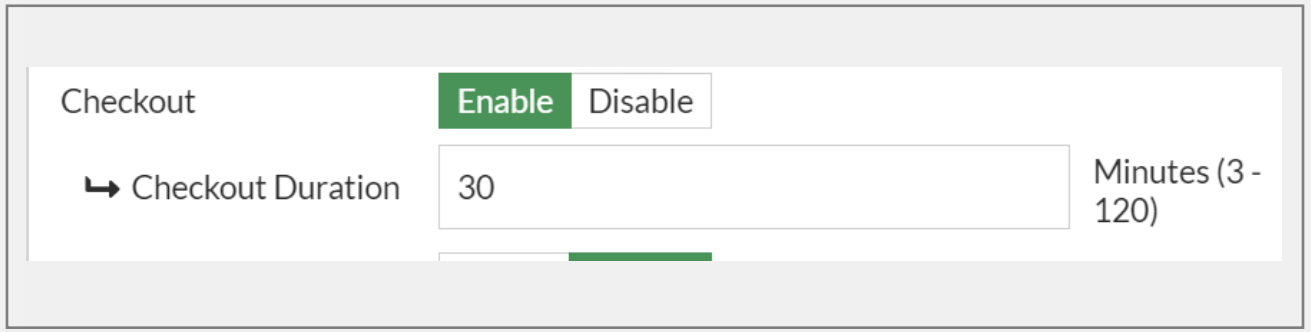


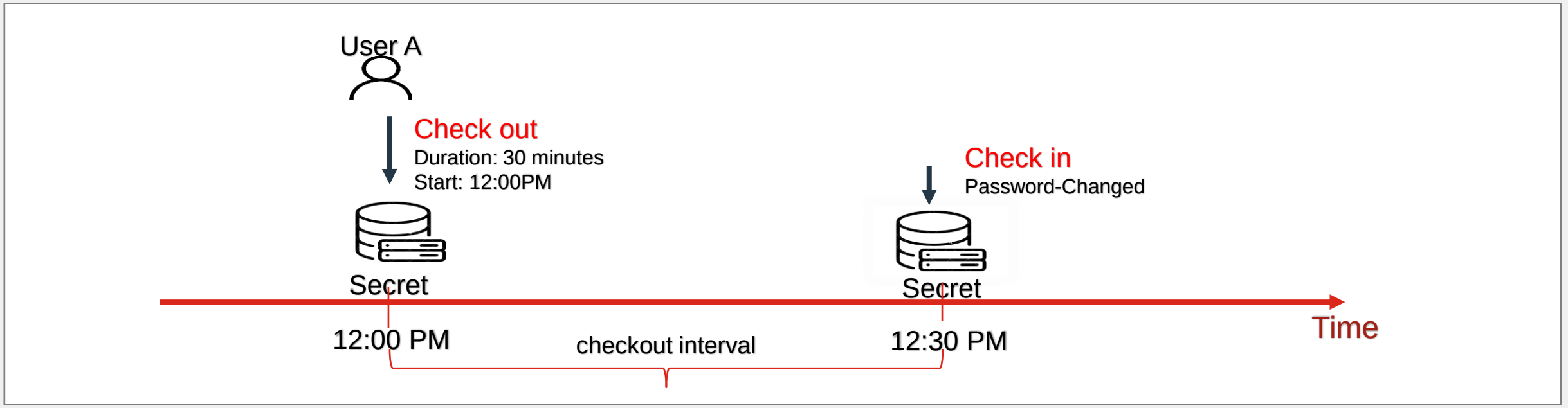
© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Secret Check out and Check in

The checkout feature allows users in FortiPAM to have exclusive access to a secret for a limited time.

- Secret owner or admin enables check out feature
- Only User A can launch the secret during checkout interval unless user A checks in manually





© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Password-Changer

For automatic or on-demand password rotation

Built-In Password Changers

- Active Directory LDAP
- Open LDAPS
- SMB
- SSH with Key
- SSH with Password

Break Glass (Emergency Account)

FortiPAM provides “Break Glass” feature for emergency and disaster recovery. When an FPA admin user activates Break Glass mode, they can bypass normal access controls and procedures to access all folders, secrets, and secret requests. This admin user can launch any secret.

- FPAM user requests a "break glass" checkout to immediately access an account that they are not otherwise authorized to access.
- If configured, email notification is sent to the "Emergency Account Manager" when "break glass" checkout is requested,
- There is no approval needed nor can the process be stopped.
- The checked-out break glass session is recorded for audit purposes by default.
- FPAM has a configurable setting to disable recording requirement (in case PAM user does not or cannot use the recording agent
- FPAM alerts the administrator(s) when an emergency account is activated.

FPAM will use push to FTM for notifications of Break Glass event. ROADMAP

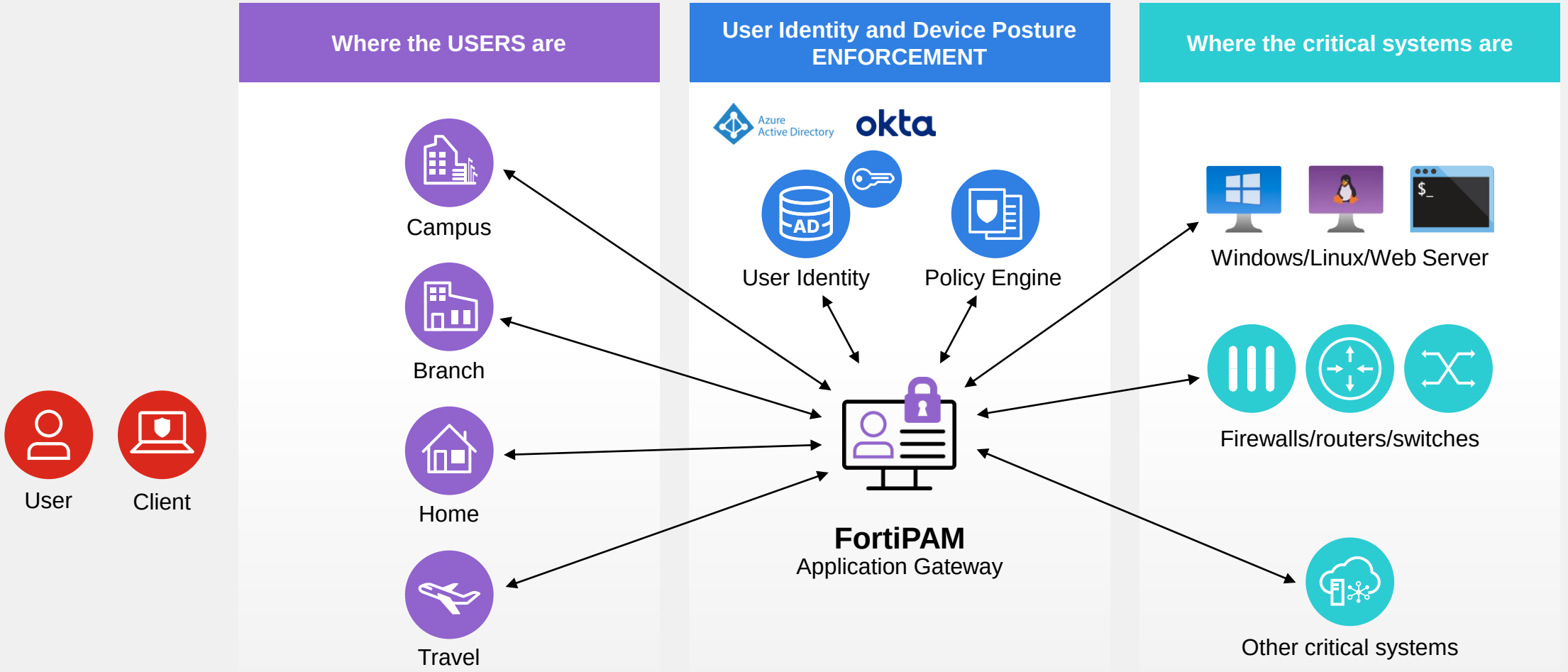
© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM

Feature deep dive

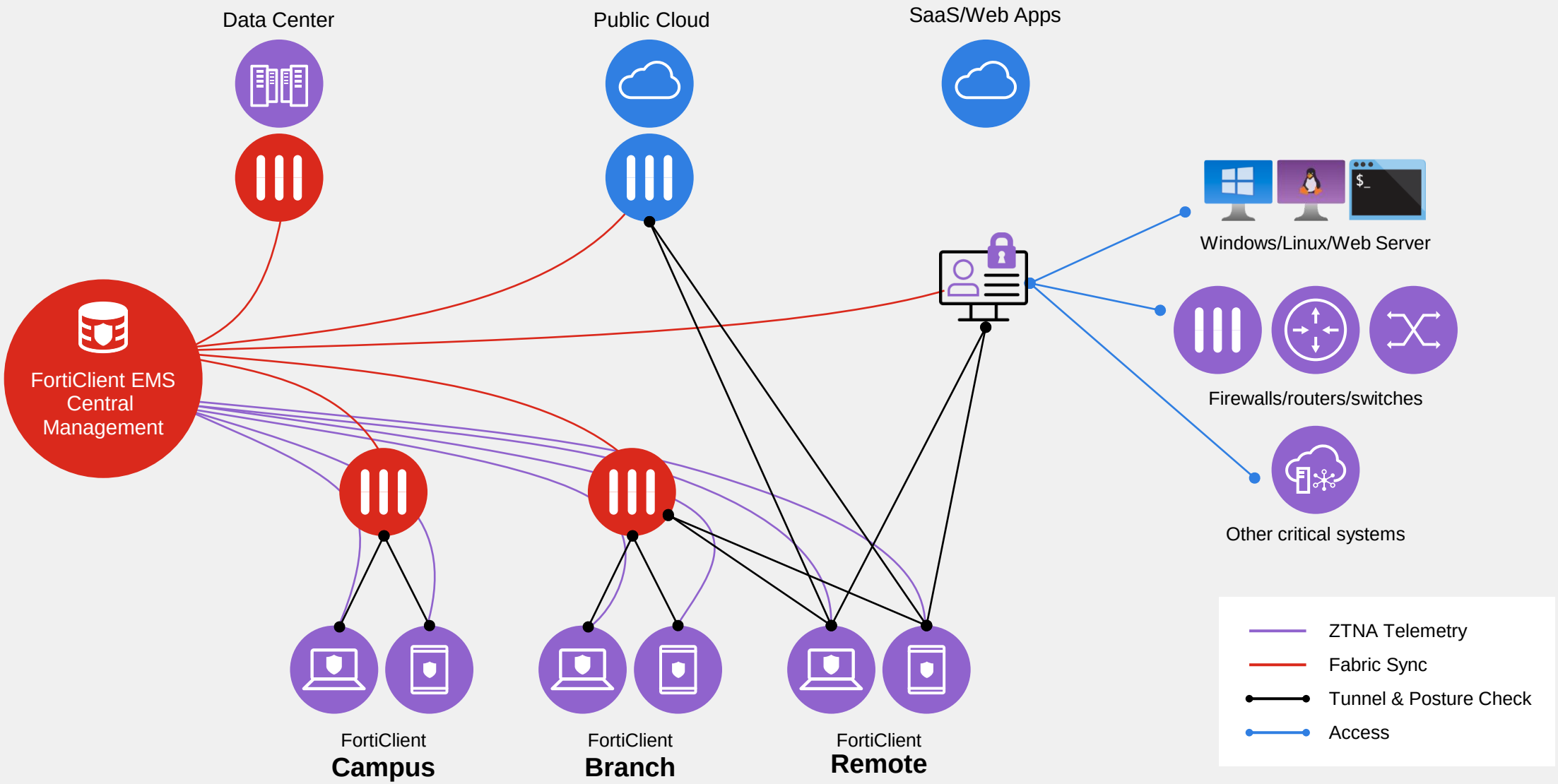
ZTNA Elements – FortiPAM as Application Gateway

The components of a client-based ZTNA solution



© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM ZTNA Process in a Fortinet Security Fabric



© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM Features

Secure File Transfer, Securing Secrets and Monitoring

Secure File Transfer

Protocols

- WinSCP
- SMB

AntiVirus Scan performed by FPAM protects against malware infected files

- uploaded from the user's endpoint
- downloaded to user's endpoint

Securing Secrets in FortiPAM

- TPM in Hardware Models
- vTPM in Virtual Machine

Monitoring

Command trace feature:
Limited to SSH access (RDP not supported because client-side RDP is image based)

Monitor Users

- Monitor logged in Users
- Force logoff of logged in users

Monitor Secrets In Use

- Monitor Active Session
- Terminate Active Session

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM Features

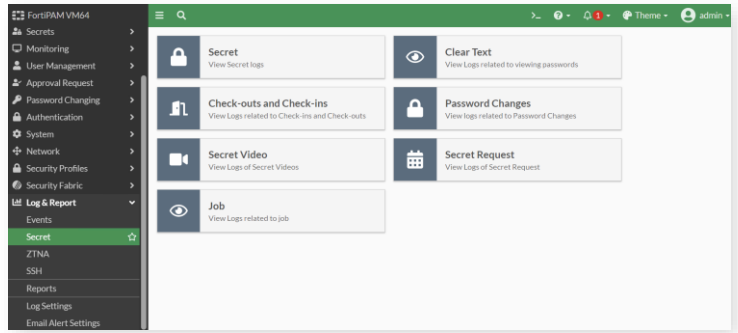
Video Recording and Logs

Video Recording

- **Target server sessions are recorded according to secret policy**
  - FortiClient PAM agent
  - Web Extension
- **User keyboard or mouse click activity detected by FortiClient agent (roadmap)**
  - logged and combined with video recording
  - jump to the corresponding video from the mouse click event
- **Video storage globally configured for max after which session is terminated**
- **Video retention policy in system setting**
  - rolling storage, retention time depends on disk size
  - can be disabled via secret policy
  - can also be configured for manual deletion

Logs

- **Events**
  - HA
  - System
  - User
- **Secret Logs**
  - Secret access
  - Clear-text password viewing
  - Check in/out
  - Password Changes



- **Secret Video**
  - Video recorded sessions are logged
  - Recordings can be played from the log viewer

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Feature / Agent Summary

1. No agent/Extension (Win, Linux, Mac)
   - Web SSH, Web RDP, Web VNC, Web SFTP,…
2. Extension only (Windows, Linux, Mac - Chrome preferred)

   FortiPAM only features +
   - Video recording
   - Direct Web browsing with pwd filler
3. Standalone PAM FortiClient (Windows only)

   FortiPAM password filler features +
   - Instant video uploading
   - Native programs: putty, VNC viewer, Winscp
4. Standard FortiClient with PAM (Windows only)

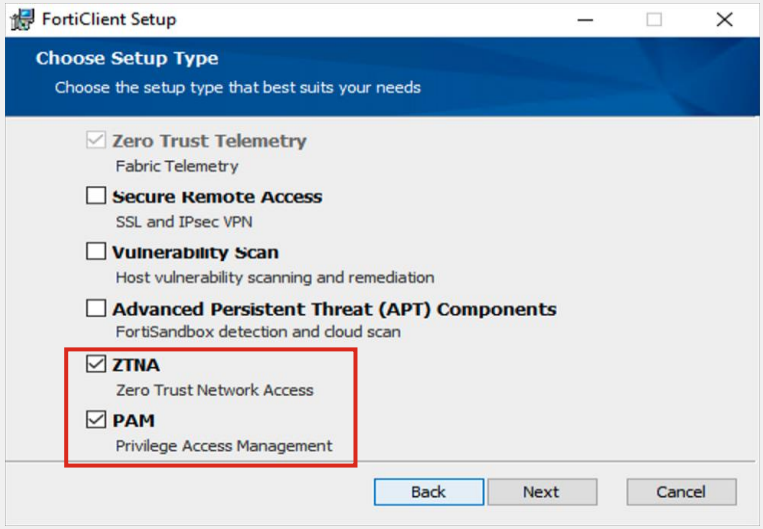
   Standalone PAM FortiClient features +
   - Possible to combine with VPN, SSOMA, ZTNA

Features	Extension Only	Standalone PAM Installer	Standard FortiClient	No Agent or Extension
Windows OS client endpoint (Chrome, Edge, FF*)	Y	Y	Y	Y
Linux OS client endpoint (Chrome, Edge, FF*)	Y	N	N	Y
MacOS client endpoint (Chrome, Edge, FF*)	Y	N	N	Y
ZTNA client endpoint	N	N	Y	N
Web SSH, RDP, VNC, SFTP,SMBA (web launchers are available only in proxy mode; credential protected in PAM)	Y	Y	Y	Y
Proxy mode Web browsing (credential sent to extension with permission protection)	N	Y	Y	N
Direct mode web browsing (credential sent to extension with permission protection)	Y	Y	Y	N
Video recording	Y	Y	Y	N
Instant video uploading	N	Y	Y	N
Native program Putty key/password, mstsc, vncviewer, winscp proxy mode (credential protected in PAM)	N	Y	Y	N
Native program Putty password, mstsc direct mode (credential delivered to FortiClient with permission protection)	N	Y	Y	N

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Licensing: FortiClient & EMS

- Windows only (ask for Linux / Mac)
- Dedicated free standalone FortiClient with PAM function
  - Does NOT require EMS
  - Can NOT be combined with other FCT standalone versions and can only be used for FortiPAM
    - **FortiPAM standalone + (SSOMA) standalone on roadmap**
- Licensed FortiClient with PAM function activated
  - Uses existing EMS licenses - no additional license required
  - Additional SSL VPN, ZTNA, SSOMA functions can also be activated.
  - Recommended deployment
  - FCT and EMS 7.2.0 or later required



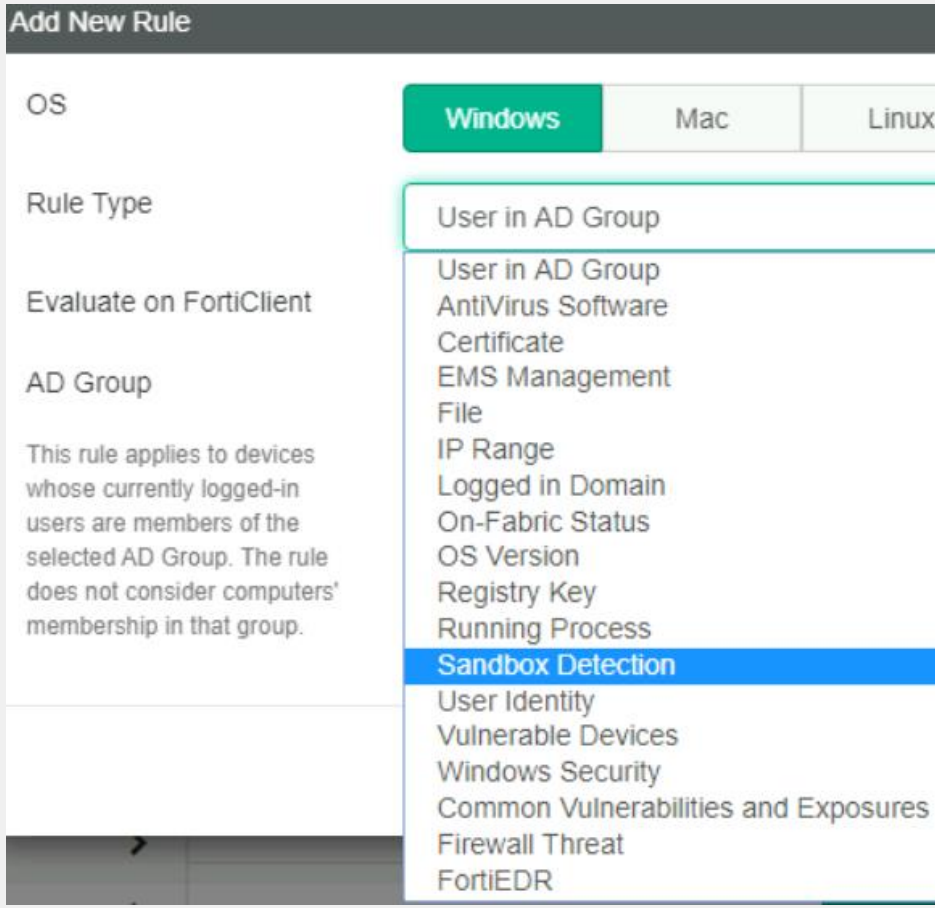
Endpoint-based Licenses - EPP/APT (On Premise Deployments)	FC1-10-EMS04-429-01-DD	FortiClient EPP/APT Subscription for 25 endpoints, Includes VPN/ZTNA Agent, EPP/APT, on-prem EMS with FortiCare Premium.

FortiPAM

Competitive advantage, Roadmap & Resources

Strengths vs competition

- Leverages FOS code base
  - GUI / logs / debugs
- Integrates fully with the Fortinet Fabric
  - LDAP/RADIUS/SAML remote user database integration for authentication and authorization (via groups)
  - ZTNA support
    - Restrict access based on tags on a per secret basis
    - Validate device posture, etc…
    - Unique in PAM market
  - FAZ & EMS connectors
- Simplicity
  - Licensing
  - Management



© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FortiPAM VM Licenses

- Stackable
- HA A/P cluster needs same licenses on Primary and Secondary
- System limits examples: 10K Folders, 10K secrets (independent of No of users)

SKU	Description
FC1-10-PAVUL-591-02	Subscription for one FortiPAM Virtual Machine seat for between **5 to 9 users**. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license
FC2-10-PAVUL-591-02	Subscription for one FortiPAM Virtual Machine seat for between **10 to 24 users**. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license
FC3-10-PAVUL-591-02	Subscription for one FortiPAM Virtual Machine seat for between **25 to 49 users**. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license
FC4-10-PAVUL-591-02	Subscription for one FortiPAM Virtual Machine seat for between **50 to 99 users**. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license
FC5-10-PAVUL-591-02	Subscription for one FortiPAM Virtual Machine seat for between **100 to 249 users**. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license
FC6-10-PAVUL-591-02	Subscription for one FortiPAM Virtual Machine seat for **250 or more users**. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

Additional Resources

Admin Guide:
https://docs.fortinet.com/product/fortipam/1.0

Datasheet:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortipam.pdf

Ordering Guide:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortipam.pdf

© Fortinet Inc. All Rights Reserved. Proprietary and Confidential.

FORTINET®