WALLIX
CYBERSECURITY SIMPLIFIED

The European cybersecurity leader providing Identity and Access Security solutions for a secure digital future

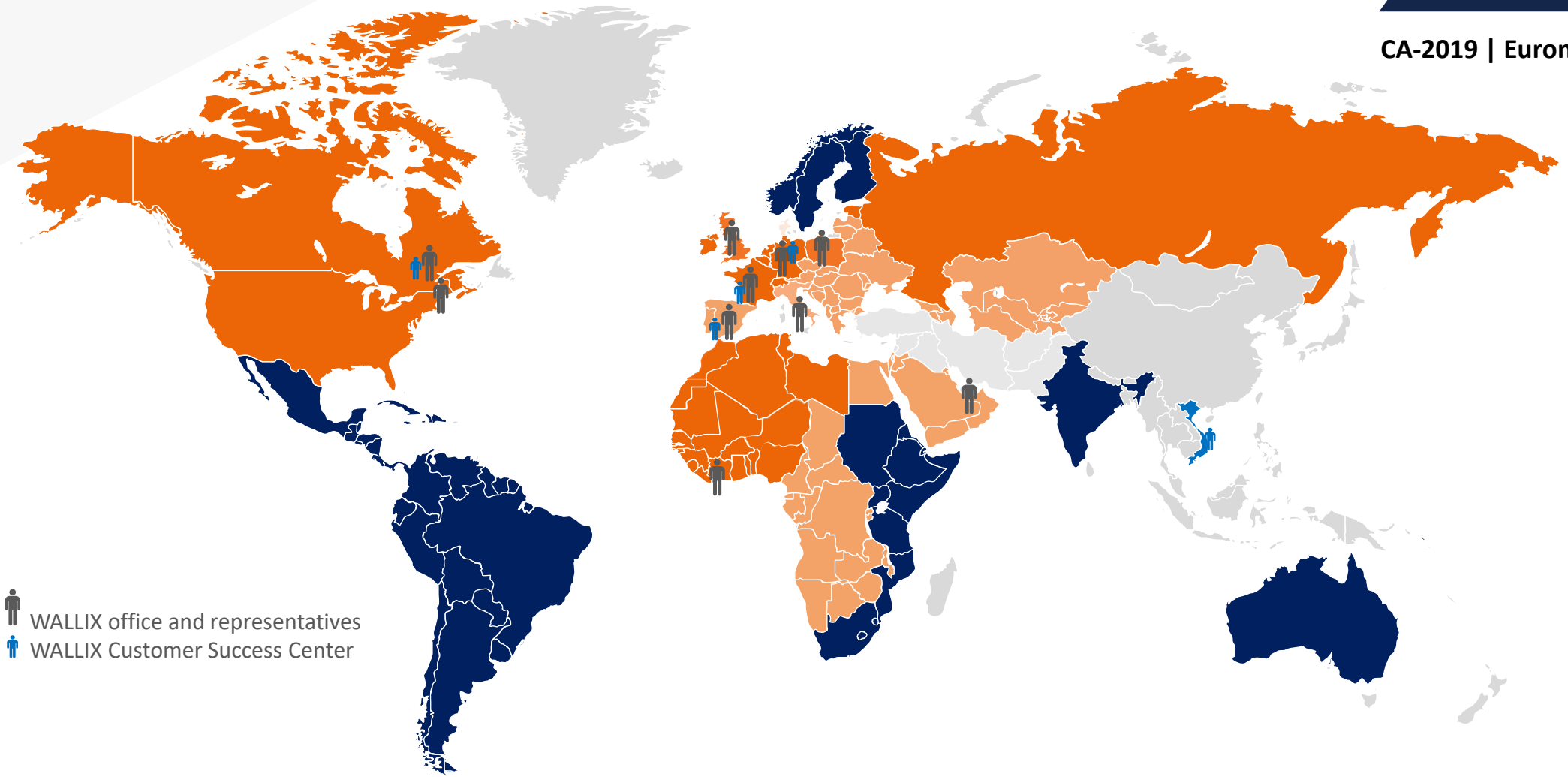
WALLIX
CYBERSECURITY SIMPLIFIED

www.wallix.com

WALLIX at a glance

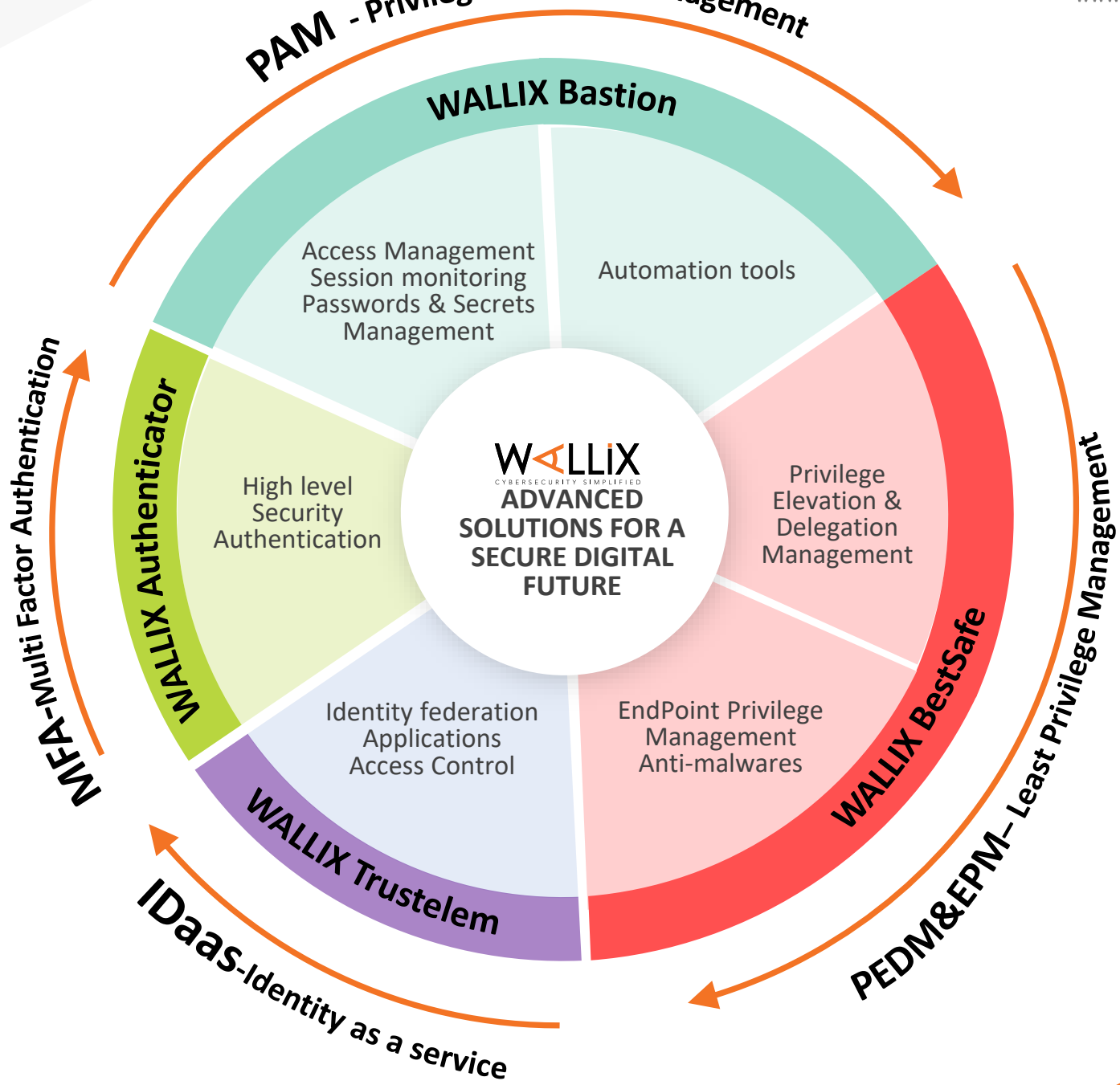
Employees	Customers		Partners
170 +	1200 +	16.7M€	170 +

CA-2019 | Euronext



WALLIX office and representatives
WALLIX Customer Success Center

ALLIX
EURONEXT
GROWTH


PAM - Privileged Access Management
WALLIX Bastion
Access Management
Session monitoring
Passwords & Secrets
Management
Automation tools
WALLIX Authenticator
High level
Security
Authentication
WALLIX
CYBERSECURITY SIMPLIFIED
ADVANCED
SOLUTIONS FOR A
SECURE DIGITAL
FUTURE
Privilege
Elevation &
Delegation
Management
WALLIX BestSafe
Identity federation
Applications
Access Control
EndPoint Privilege
Management
Anti-malwares
WALLIX Trustelem
MFA-Multi Factor Authentication
IDaas-Identity as a service
PEDM&EPM– Least Privilege Management

4 good reasons to implement a PAM solution

External service providers

I have no visibility on what my providers are doing on the infrastructure

Many people access servers, devices and applications: I do not know who has access to what, when or how

I must control these accesses and change external provider if I need to

How can I ensure full access control? How can I find the origin of the problem? Who is responsible?

Admin Passwords

Post-it notes multiply on computer screens or on the desks or in unsecured Excel file

Passwords are handled chaotically. Sometimes, they are only in the admin's head

Generic accounts (Admin & Root) are not longer an option

What is the best way to handle user authentication?

When an incident happens

Origin of an incident and traceability of actions

The customer database crashed after a support intervention from an external provider during a major upgrade

We cannot establish responsibilities or find evidence!

Where did the problem come from? Can we review what happened? How can we determine the origin of the problem?

IT teams turnover

One of my admins is leaving the company

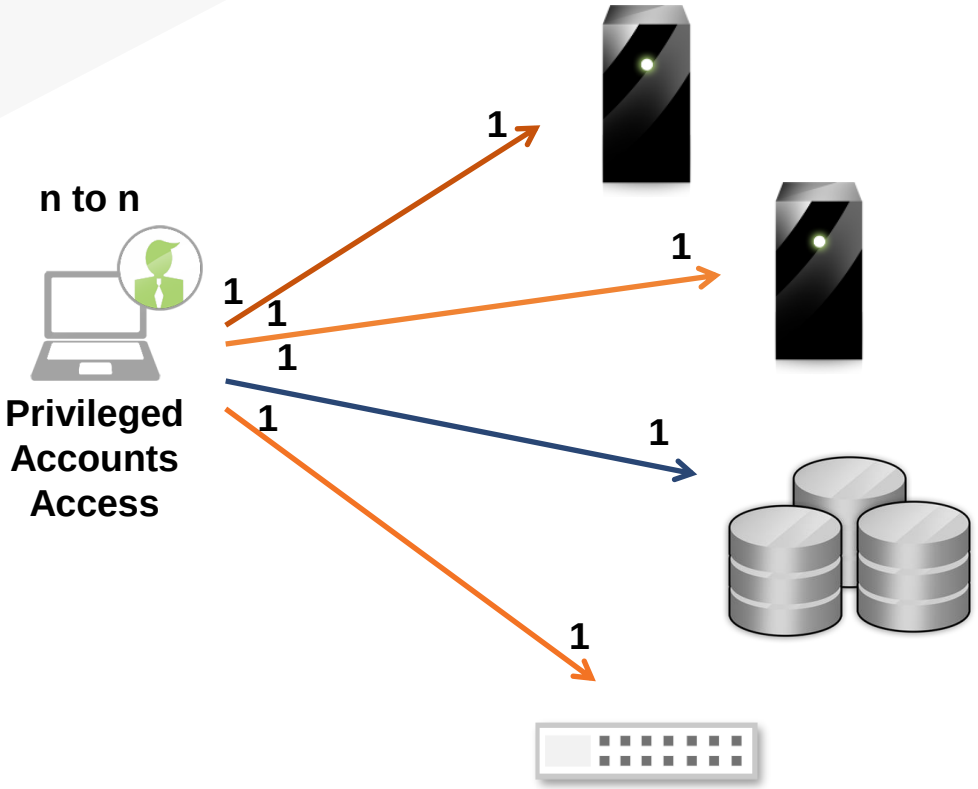
His/her access rights must be listed, deactivated and modified for every device

These changes must be communicated internally

How can I make sure he/she will no longer be able to access to the information system?

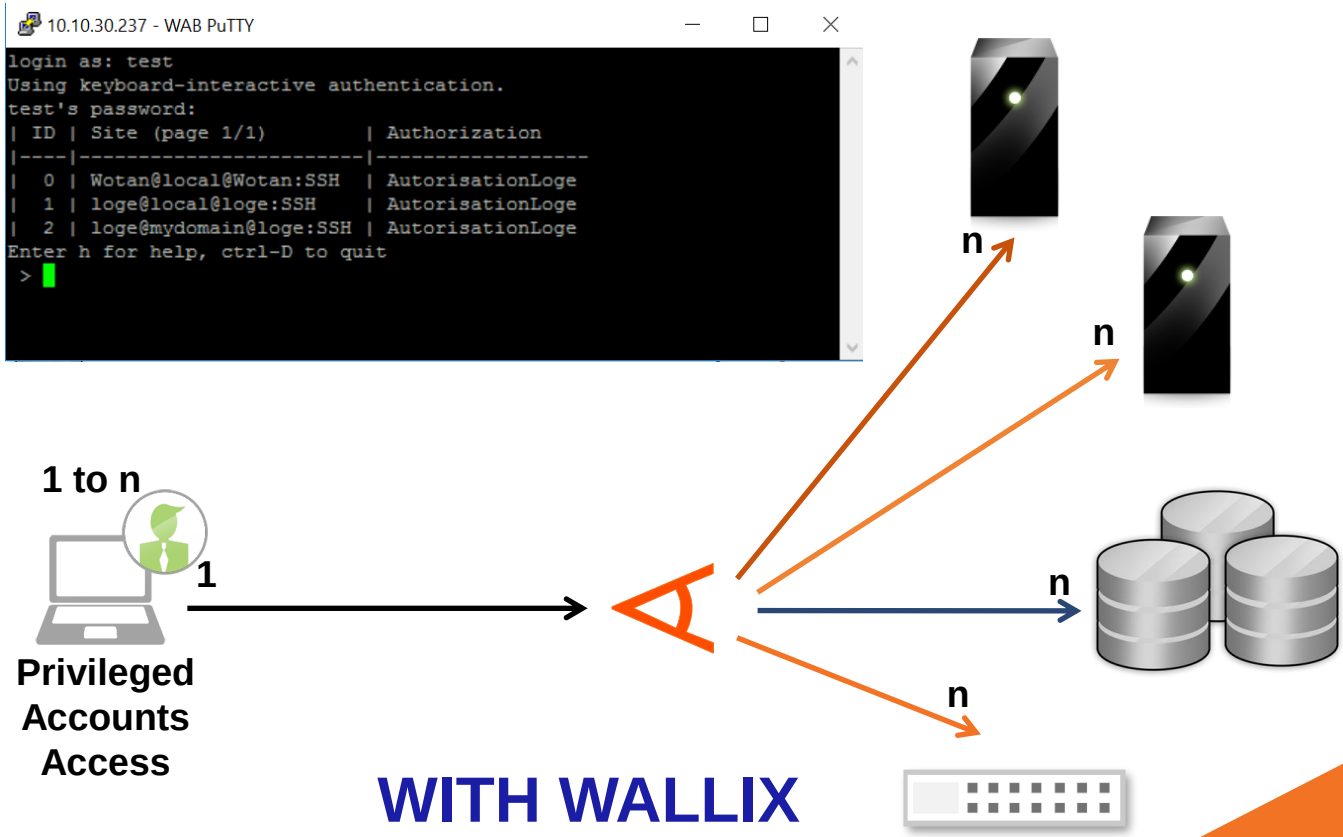
WALLIX in the middle

- N accounts to N resources
- Direct access to resources



WITHOUT WALLIX

- Bridging 1 accounts to N resources
- No knowledges of passwords on resources



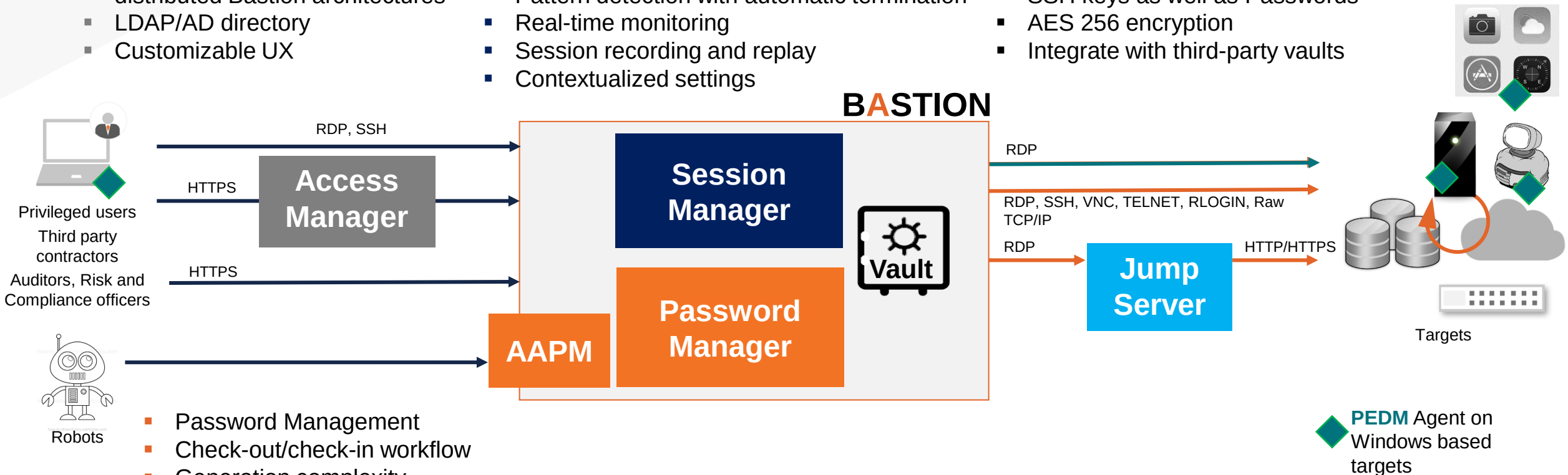
WITH WALLIX

WALLIX Bastion Key Architecture and Functionalities

- Web console to access and audit distributed Bastion architectures
- LDAP/AD directory
- Customizable UX

- Privileged accounts mgt & governance
- Pattern detection with automatic termination
- Real-time monitoring
- Session recording and replay
- Contextualized settings

- Vault to store passwords
- SSH keys as well as Passwords
- AES 256 encryption
- Integrate with third-party vaults



- Password Management
- Check-out/check-in workflow
- Generation complexity
- App2App Password Mgt

PEDM Agent on Windows based targets

Certified by **ANSSI**
French cybersecurity compliance body

Deployment options

- 3 – layer architecture to provide scalability
  - Bastion Access Manager farms
  - Bastion Clusters
  - Jump Server Clusters

- Speed up configuration
  - Import/Export capabilities
  - REST API

Bastion Administrator

- Sizing VM

Maximum number of registered devices	Number of concurrent sessions (RDP[1] / SSH)	Number of CPUs	GHz to reserve	Memory (GB) to reserve
50	2 / 20	2	6	4
200	16 / 50	6	15	8
600	25 / 100	8	20	16
1000	80 / 200	16	40	16
2000	160 / 400	16	42	16

Access without WALLIX PAM

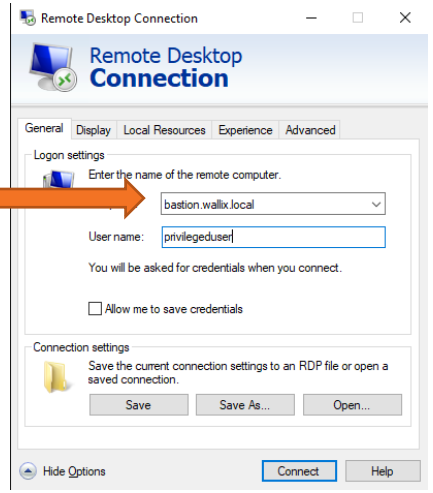
- Direct connection to target system using mstsc

No PROXY – no access control
No network separation
No monitorig
No historical data
No recording

Access to corporate resources via WALLIX PAM

- Mitigating risk od sharing privileged user's password

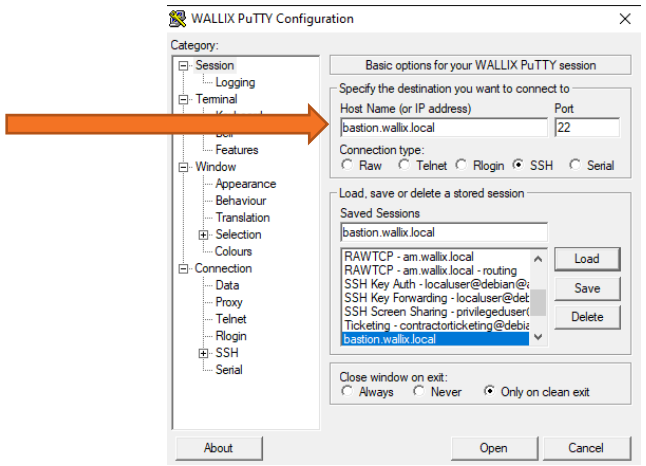
WALLIX Bastion instead of target system



Native SSH client access with WALLIX

- Using native PuTTY client

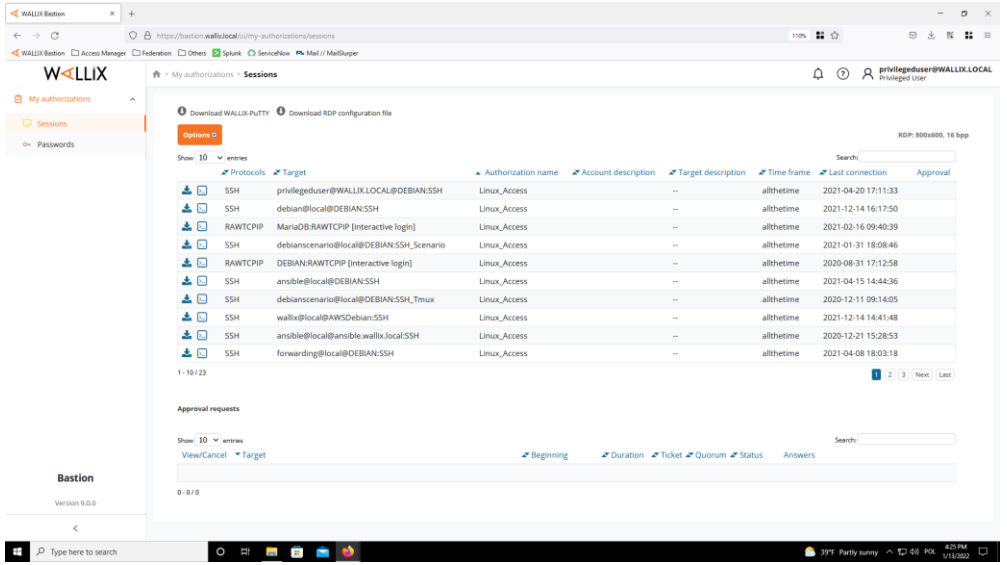
WALLIX Bastion instead of target system



UAC based access

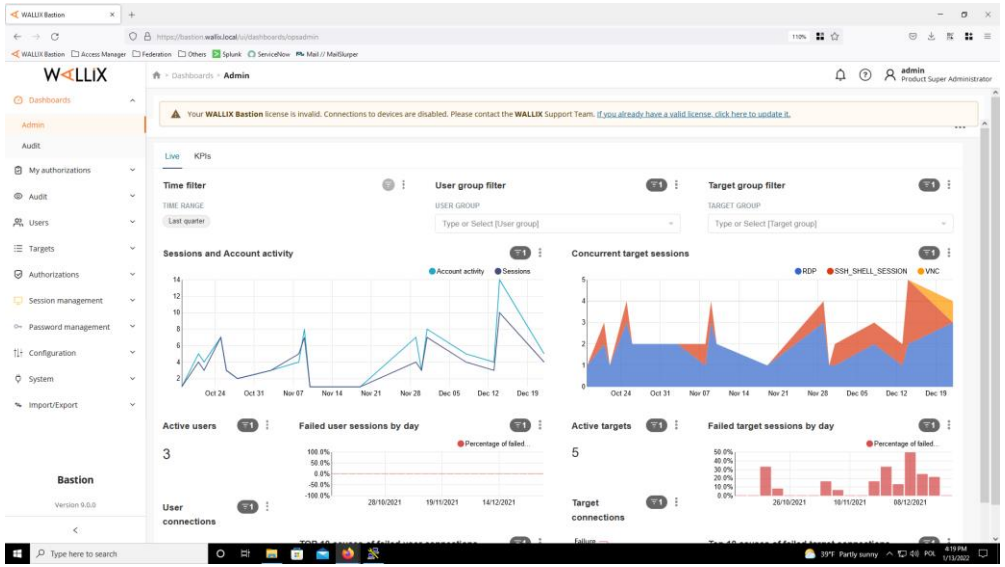
- Standard users profiles
  - USER
  - ADMINISTRATOR

USER



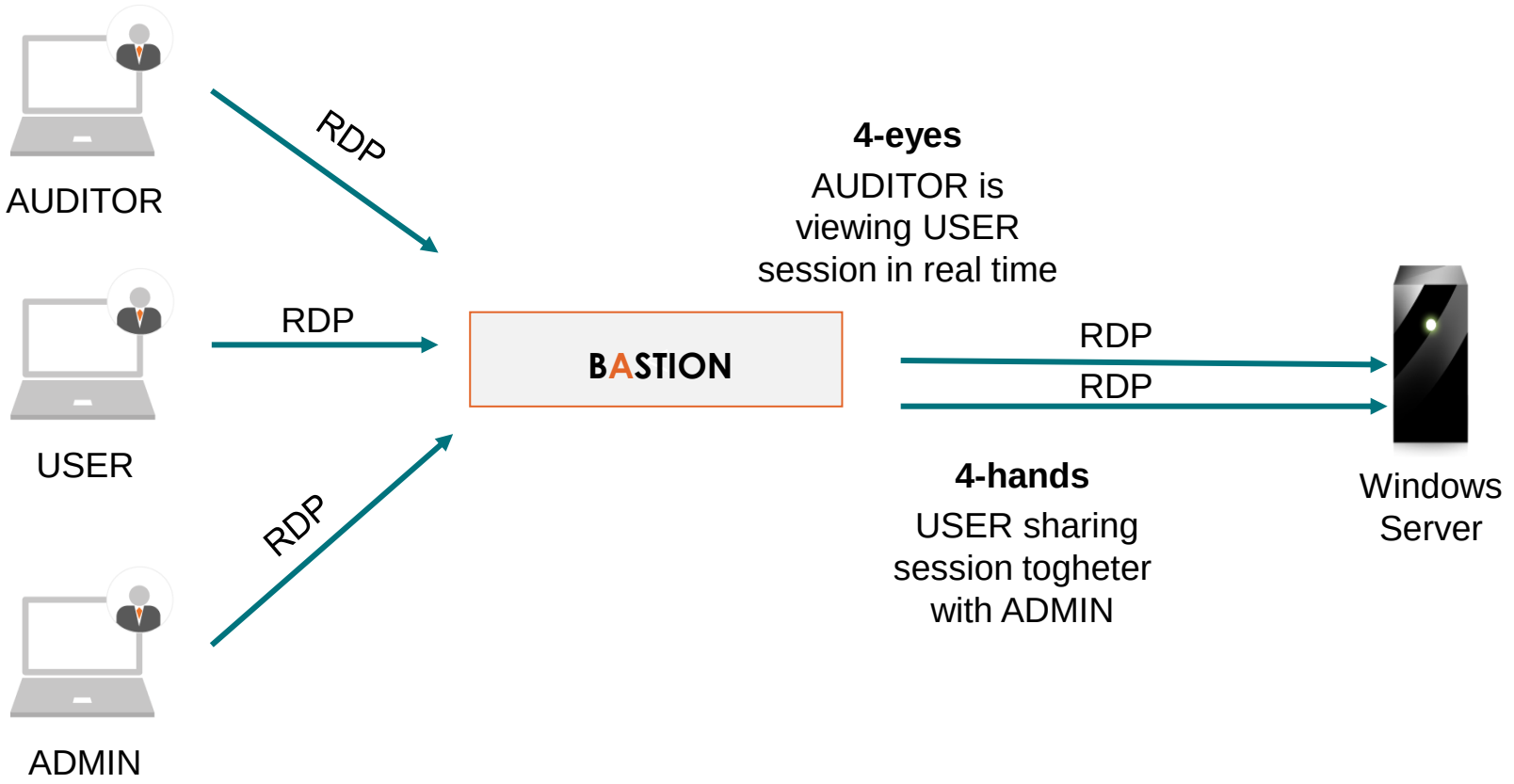
BASTION

ADMIN



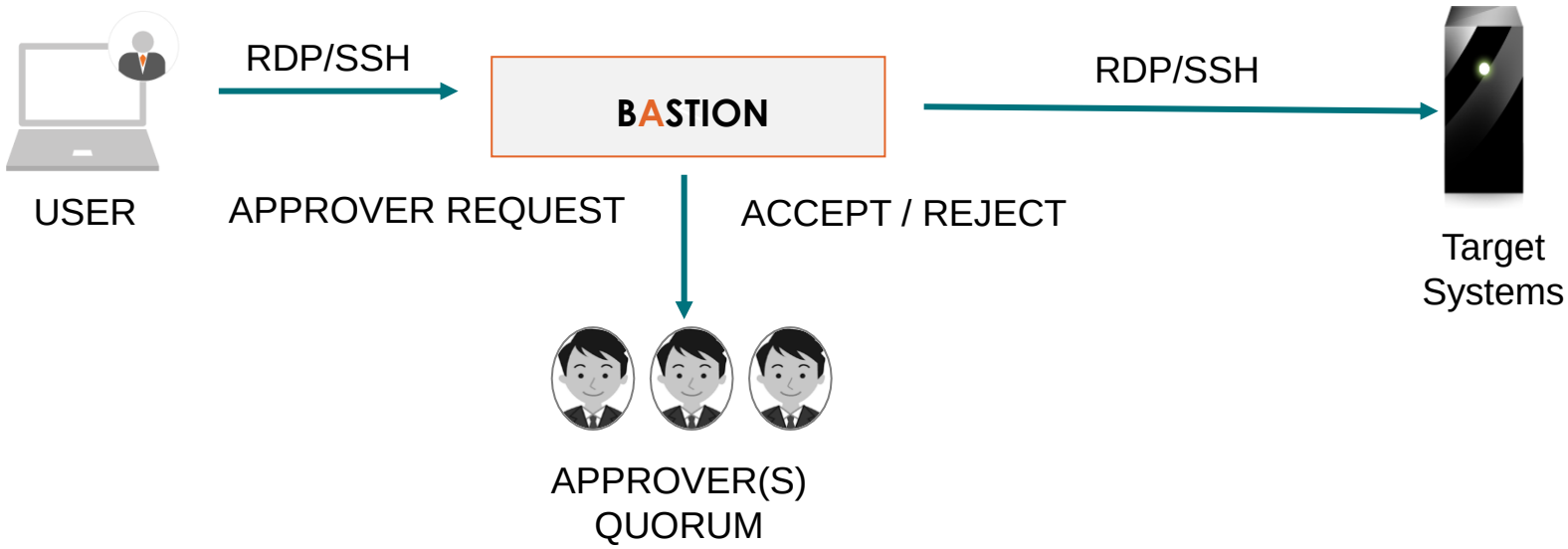
Audit data

- Viewing recorded session
- 4-eyes
- 4-hands



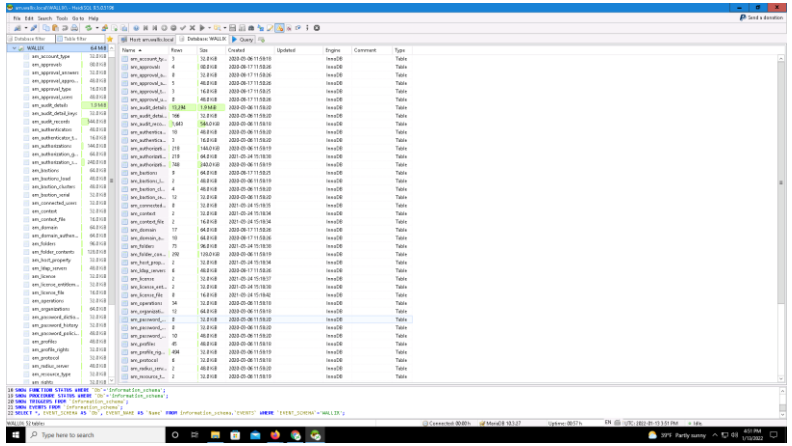
Workflow approval mechanism

- Access for critical resources for defind time

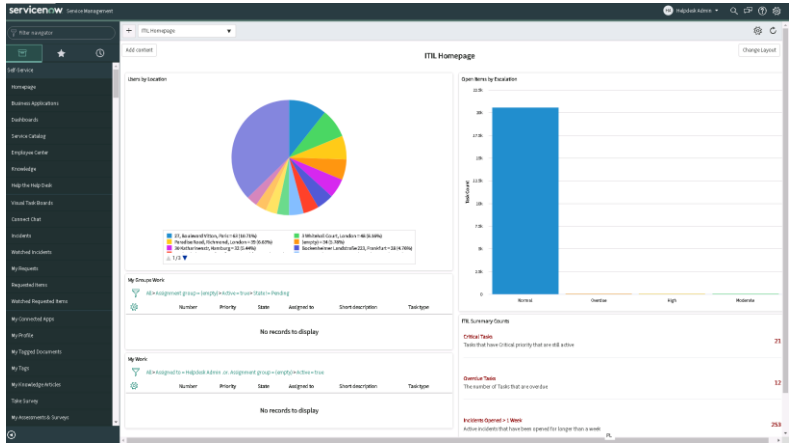


Access & monitoring Application profile

- Monitoring Apps profiles
- Web App access with credentials automation injection



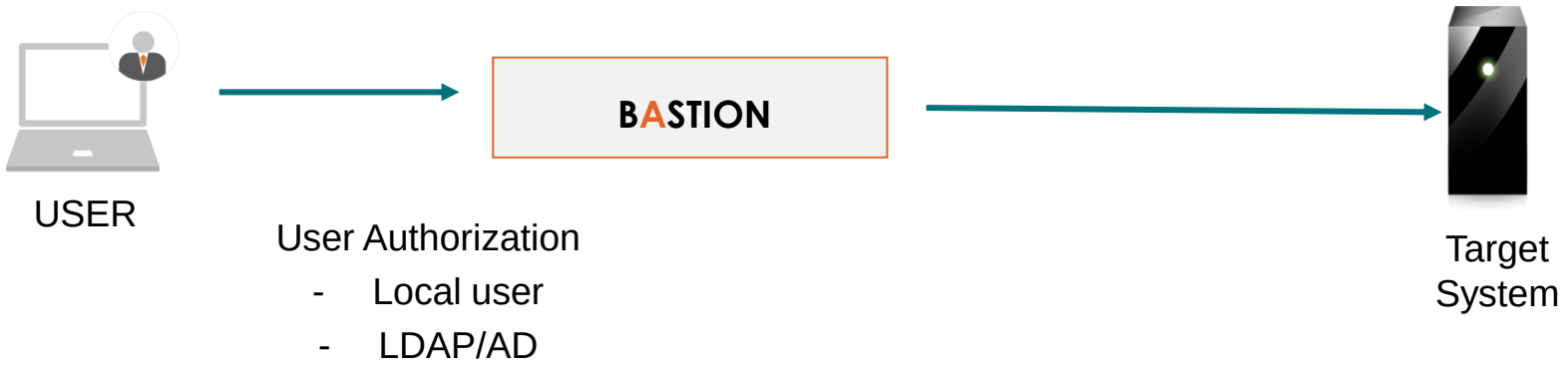
HeidiSQL



Web App

Authorization methods on Primary connection

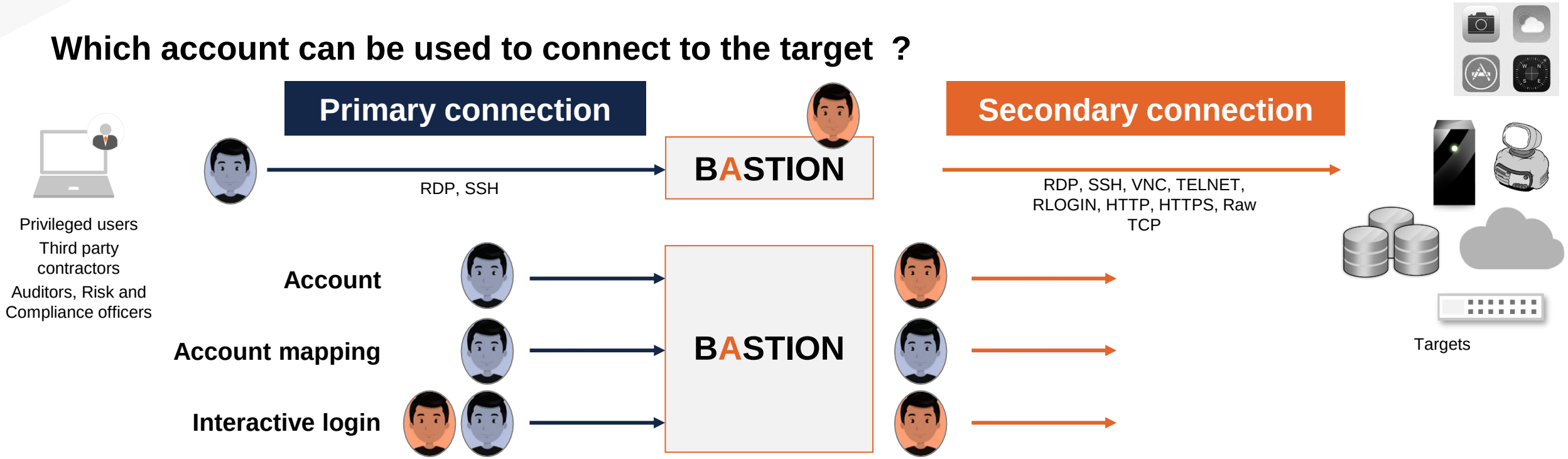
- Local users
- LDAP/AD



Supported login mechanism on Secondary connection

- Accont
- Account mapping
- Interactive

Which account can be used to connect to the target ?



Password Manager

Securing passwords in a certified vault, hiding, revealing, changing or generating target passwords

Targets

- Bastion Vault, the credentials' secured storage
  - SSH key as well as Password
  - Password encryption using AES 256

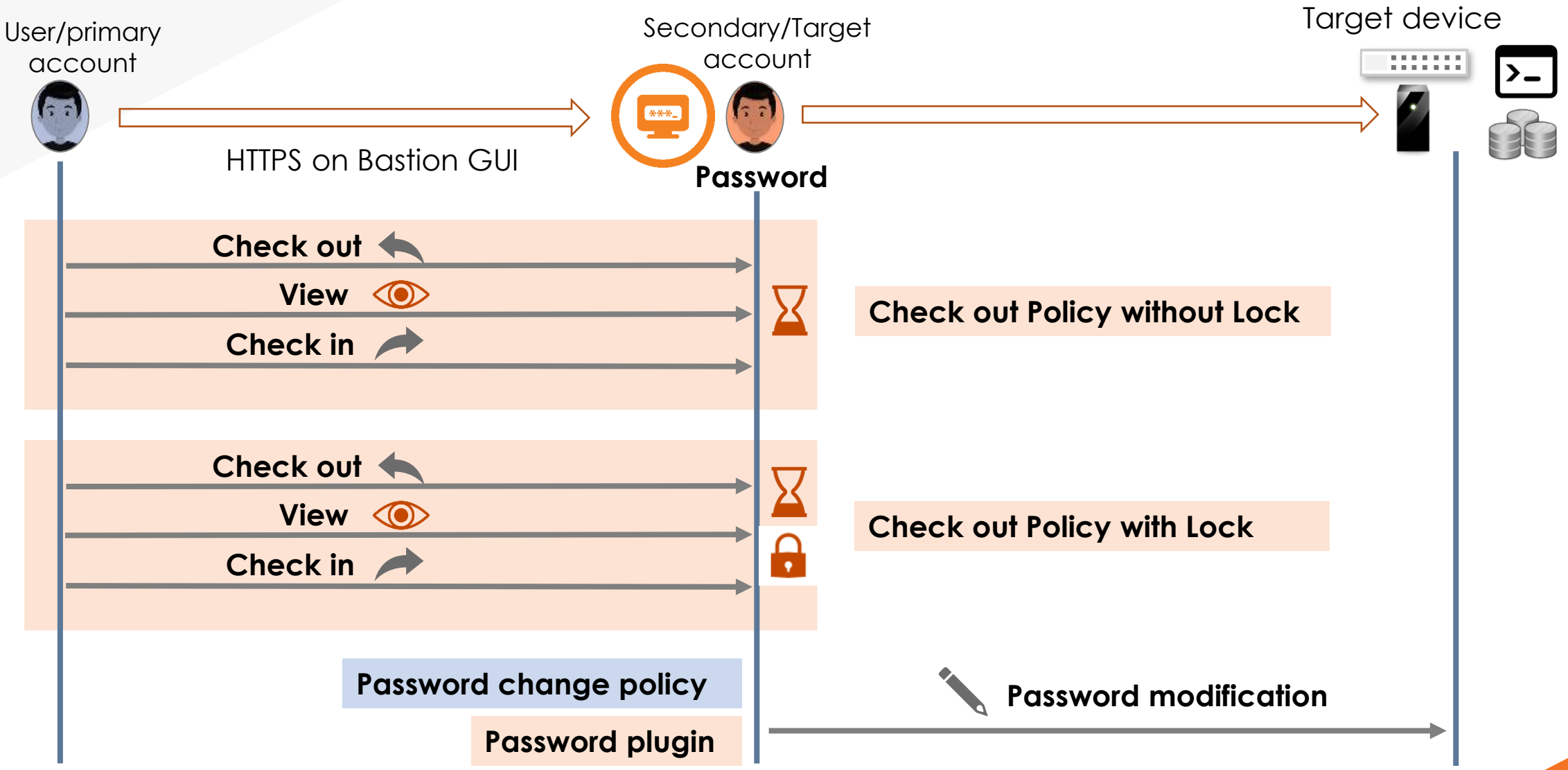
- Password Management capabilities
  - Automatic or on-demand password rotation
  - Check-out/check-in workflow
  - Password complexity generation
  - App2App Password Management
  - Breaking glass

Bastion Administrator

Plugin based architecture to easily support password change and rotation

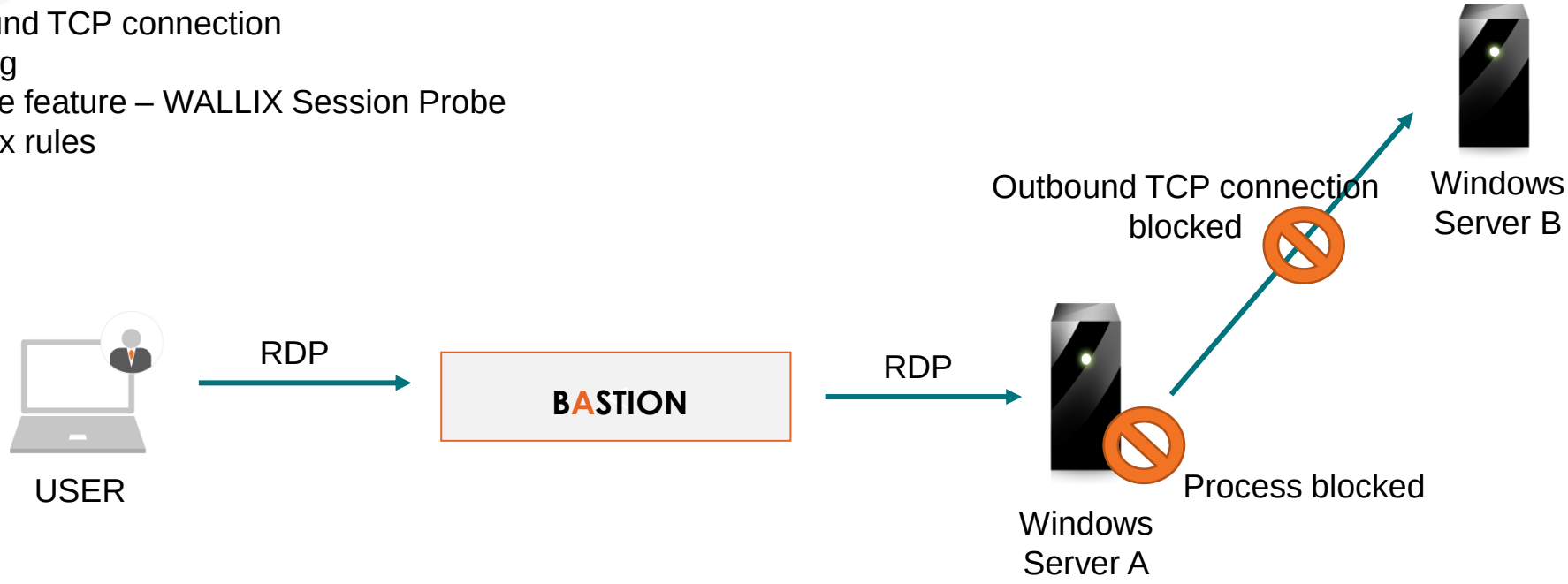
Juniper SRX	Windows	LDAP	MySQL
IBM 3270	Cisco	Linux	SQL Server
Palo Alto PA-500	Oracle	Fortinet FortiGate	Teradata

Password Manager capabilities: Check-out/in workflow



Blocking unwanted process or behavior

- Blocking outbound TCP connection
- Process blocking
- Based on unique feature – WALLIX Session Probe
- Based on RegEx rules

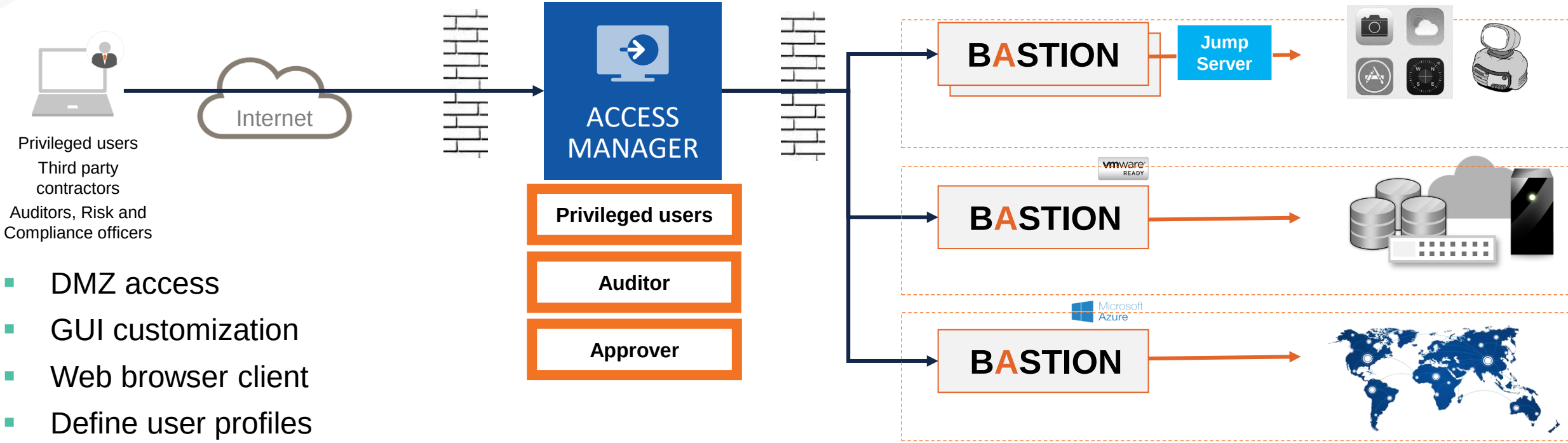


Access Manager - secure remote access without VPN

A unique interface to access several Bastion instances

- Multi-bastion architecture with organization of users/domains groups

Single sign-on via Access Manager to your Bastion farm embedding RDP & SSH clients



- DMZ access
- GUI customization
- Web browser client
- Define user profiles
- Manage approval

WALLIX BestSafe - PEDM

- Implement the Principle of Least Privilege without impacting productivity
- Effectve anti-ransomware solution: detects in real time when a process intends to perform an encryption operation before it is carried out
- Real-time monitoring of applications: monitoring access to disk, to the registry, to the network and actions like creating new processes or local user account
- Control access to resources by applicaiton: blocking of all outgoing connections of a cetain application regardless of the user's credentials

- Increases system security by reducing administrator's rights to the bare minimum needed to address their tasks
- Enriched metadata, thanks to the BestSafe PEDM agent controlled by session probe, thus enhancing the traceability functionality of the Bastion

WALLIX Trustelem - IDaaS

Administrators

Users

WALLIX TRUSTELEM

- Azure Active Directory
- Microsoft Active Directory
- G Suite
- LDAP

Identity Sourcing

- Directories
- ID files (csv)
- API
- On the fly through web-forms

User key functions

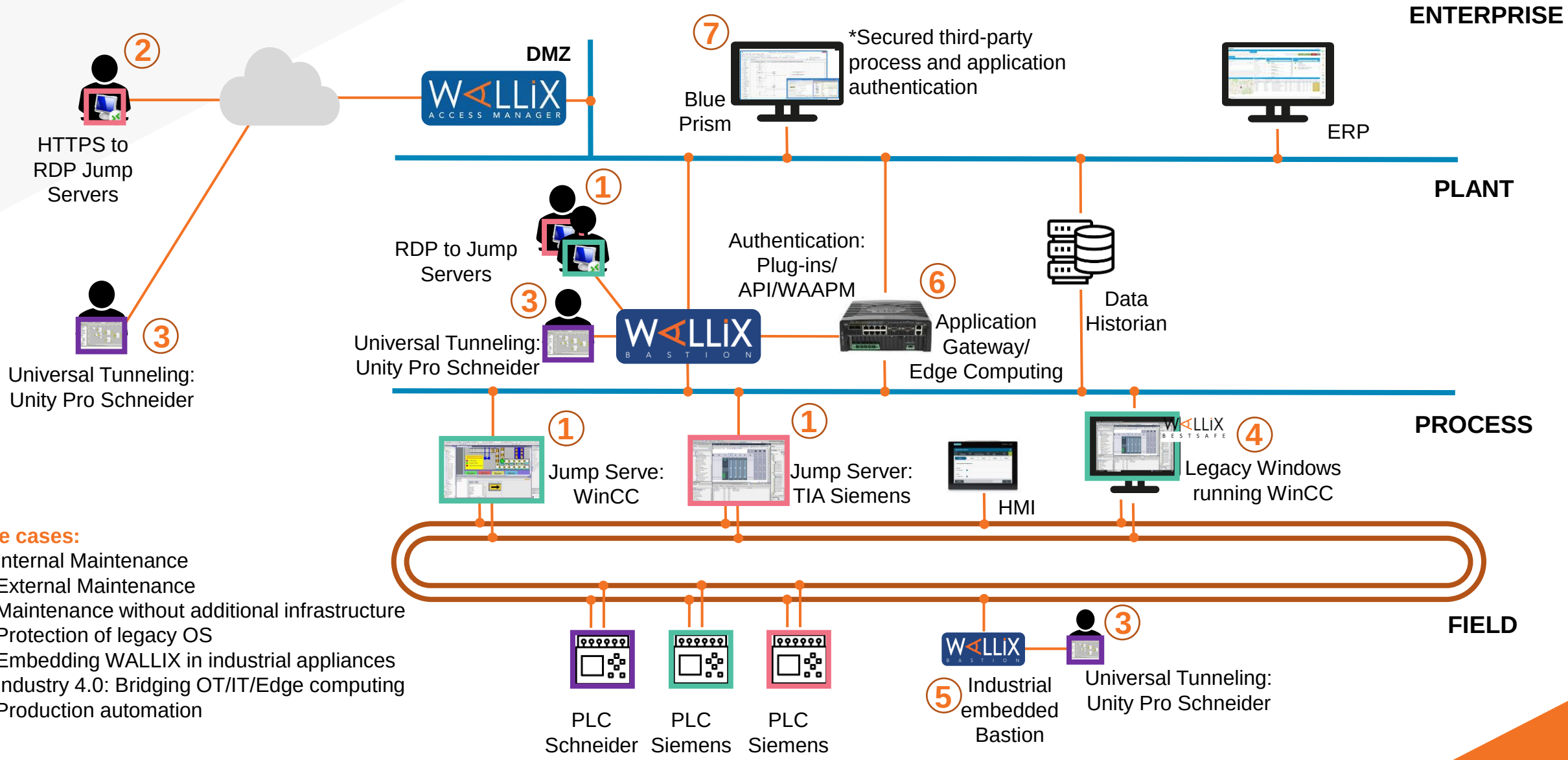
- SSO
- MFA
- Contextual login
- User self-care:
  - MFA enrolment
  - PW reset
- PW reset
- JIT provisioning

Applications access

- How to get access to various applications, through:
  - SAML
  - Open ID connect
  - LDAP

- ownCloud
- Dropbox
- Office 365
- box
- salesforce
- Cisco webex
- Nextcloud
- sage
- Jalios
- SAP ERP
- ZOHO Work · Online
- G Suite
- Jamespot
- WordPress
- ...

WALLIX OT – use cases



Use cases:

1: Internal Maintenance
2: External Maintenance
3: Maintenance without additional infrastructure
4: Protection of legacy OS
5: Embedding WALLIX in industrial appliances
6: Industry 4.0: Bridging OT/IT/Edge computing
7: Production automation

1 Internal Maintenance

Industrial problem to solve:

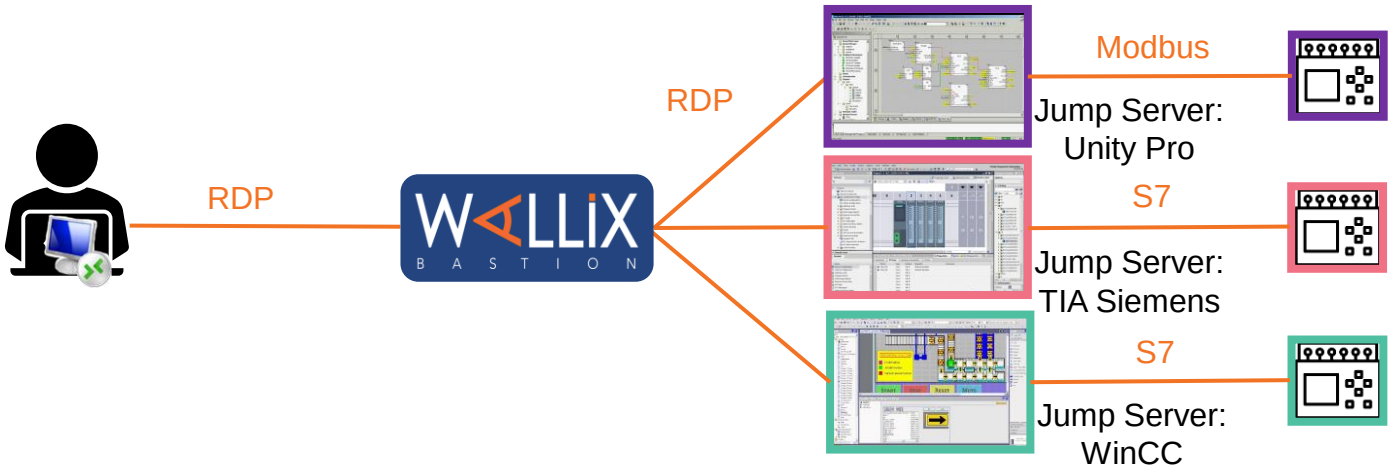
- Traceability of maintenance activity on PLCs.
- Traceability and accountability of privileged Industrial Control System Accounts using automation applications.

Solution:

- WALLIX Bastion to control access and tracking activity of Automation Software running on Jump Servers.

Benefits:

- Accountability of maintainers and traceability of the activity.
- Reduced TCO with a single PAM appliance.
- Enhanced protection with maintainers authentication and account segregation: a maintainer does not know the credentials to authenticate to PLCs.



2 External Maintenance

Industrial problem to solve:

- Lack of internal skills.
- Grant secured access to critical automates from outside of the corporate network.

Solution:

- WALLIX Bastion with the WALLIX Access Manager web portal dedicated to external access.
- Security can be enhanced with native MFA, workflows and ticketing.

Benefits:

- End to end secured access through the internet.
- Reduced TCO with no VPN agents/solution to deploy/maintain.
- Reduced surface attack with use of the HTTPS protocol only.

3 Maintenance without additional infrastructure

Industrial problem to solve:

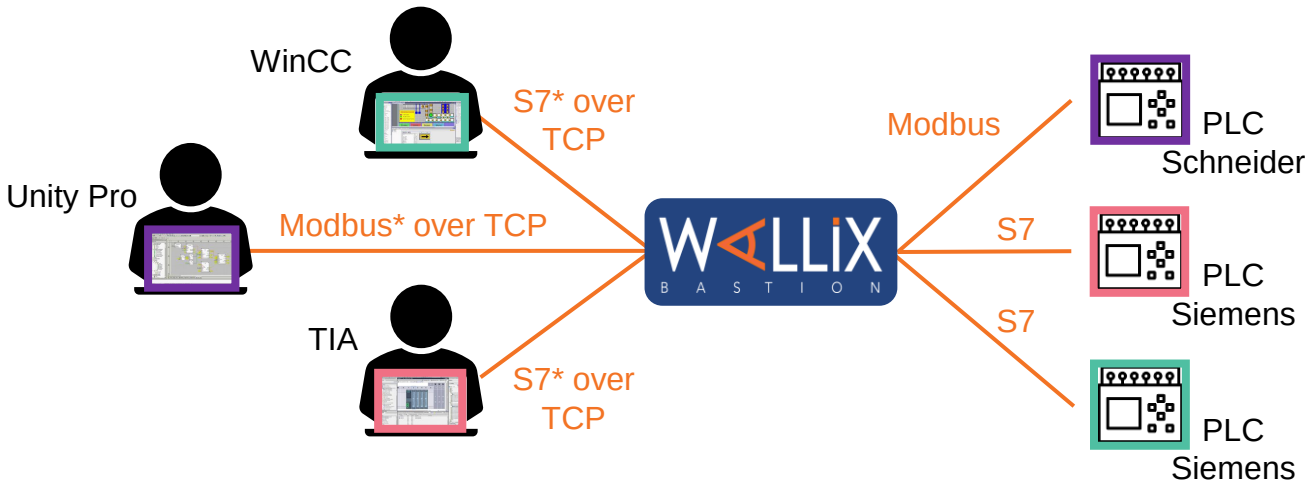
- Run Automation maintenance software on the maintainer PC so that he/she can benefits from dedicated environment/proprietary tools.

Solution:

- WALLIX Universal Tunneling.

Benefits:

- Reduced TCO: no need for Jump Servers.
- Traceability of connections.
- Enforced forensic with availability of Session PCAPs.
- Increased efficiency/limited change management: maintainer can work with his/her own environment.

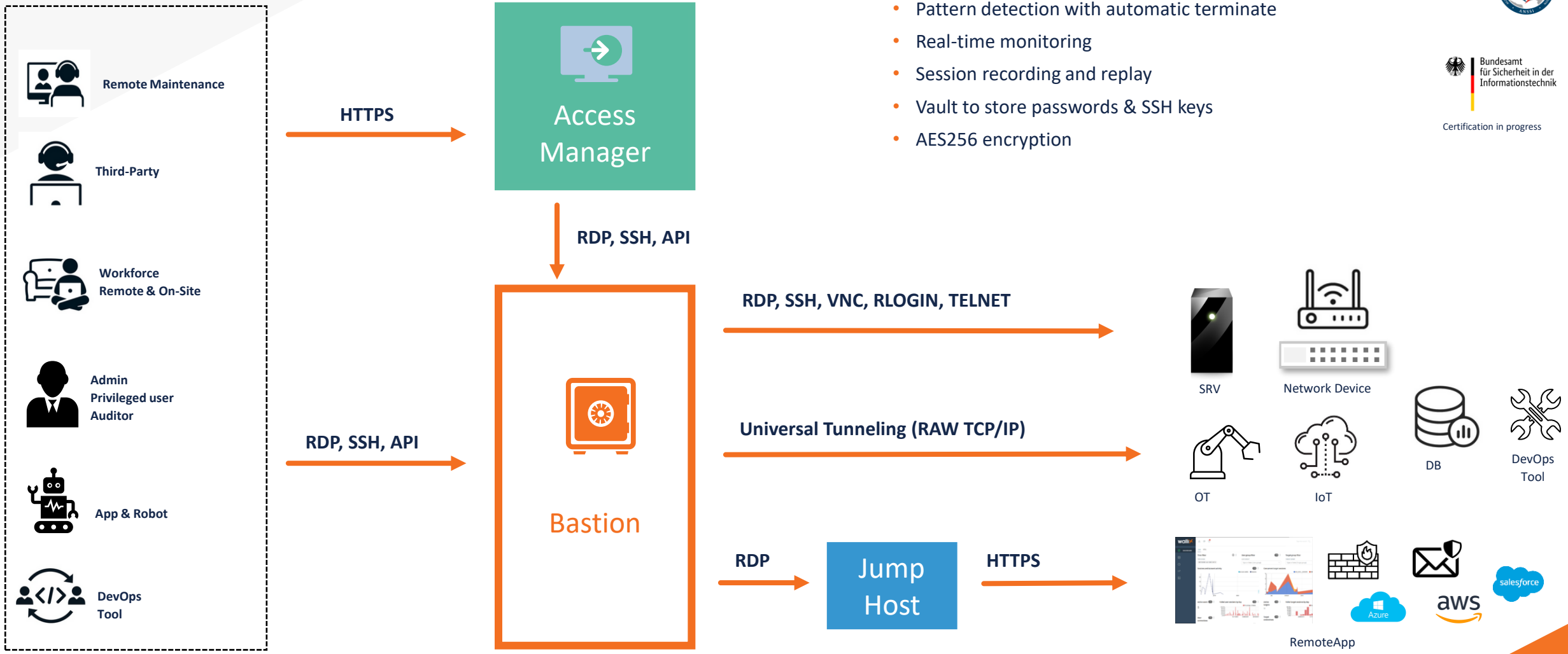


* works with any proprietary protocol that can be encapsulated over TCP

WALLIX PAM: On premise/IaaS

- Privileged access mgt & governance
- LDAP/AD and SAML identity sources
- Pattern detection with automatic terminate
- Real-time monitoring
- Session recording and replay
- Vault to store passwords & SSH keys
- AES256 encryption

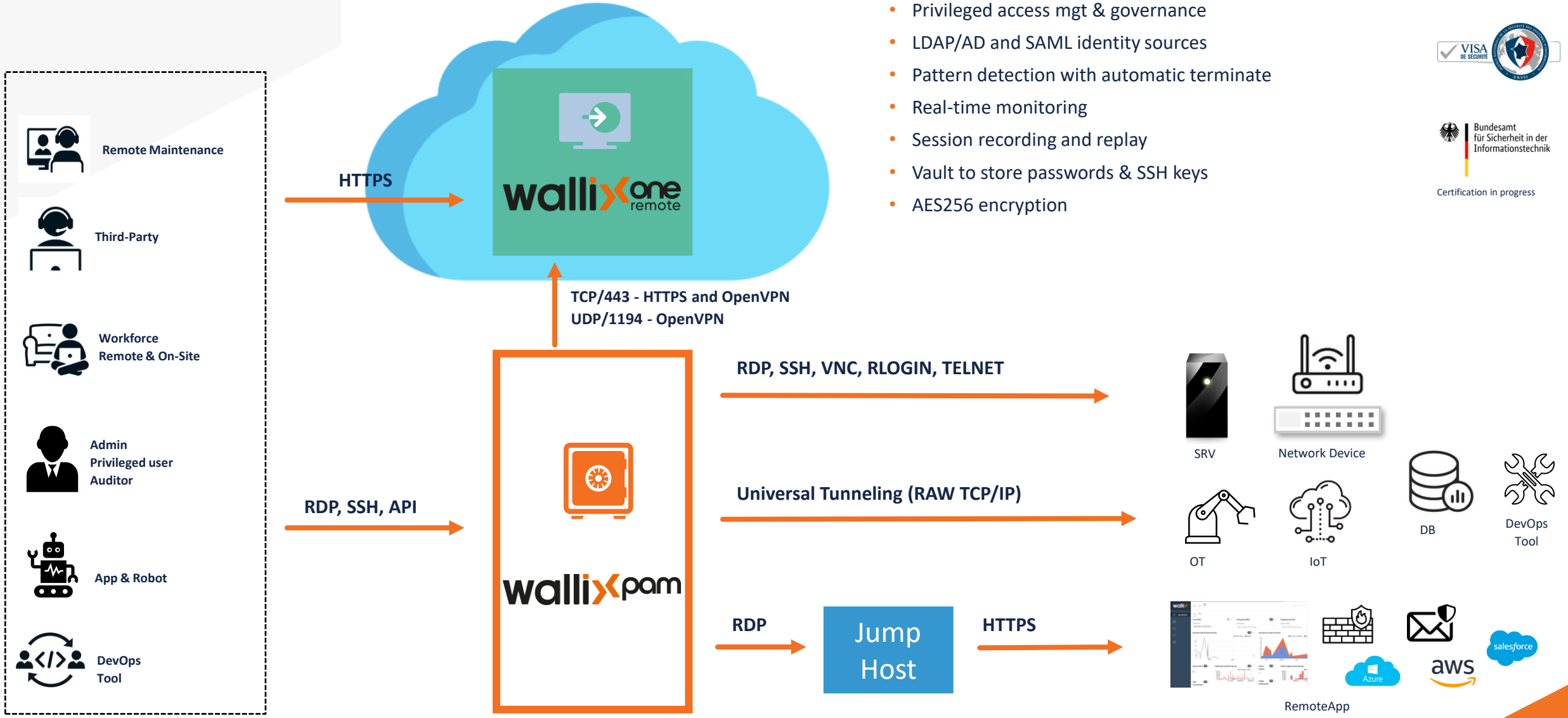
Certification in progress



WALLIX PAM: Hybrid SaaS

- Privileged access mgt & governance
- LDAP/AD and SAML identity sources
- Pattern detection with automatic terminate
- Real-time monitoring
- Session recording and replay
- Vault to store passwords & SSH keys
- AES256 encryption

Certification in progress



WALLIX OnePAM: SaaS

- Privileged access mgt & governance
- LDAP/AD and SAML identity sources
- Pattern detection with automatic terminate
- Real-time monitoring
- Session recording and replay
- Vault to store passwords & SSH keys
- AES256 encryption

Certification in progress

Remote Maintenance

Third-Party

Workforce
Remote & On-Site

Admin
Privileged user
Auditor

App & Robot

DevOps
Tool

HTTPS

RDP, SSH, API

wallix one pam

IPsec Tunnel (Site to Site)
RDP, SSH, Infrastructure … inside

VPN Gateway

To:
- On Premise
- IaaS
- SaaS

SRV

Network Device

OT

IoT

DB

DevOps
Tool

RemoteApp

WALLIX

Thank You

250 bis, rue du Faubourg Saint-Honoré
75008 Paris, France

+33 1 53 42 12 81
info@wallix.com