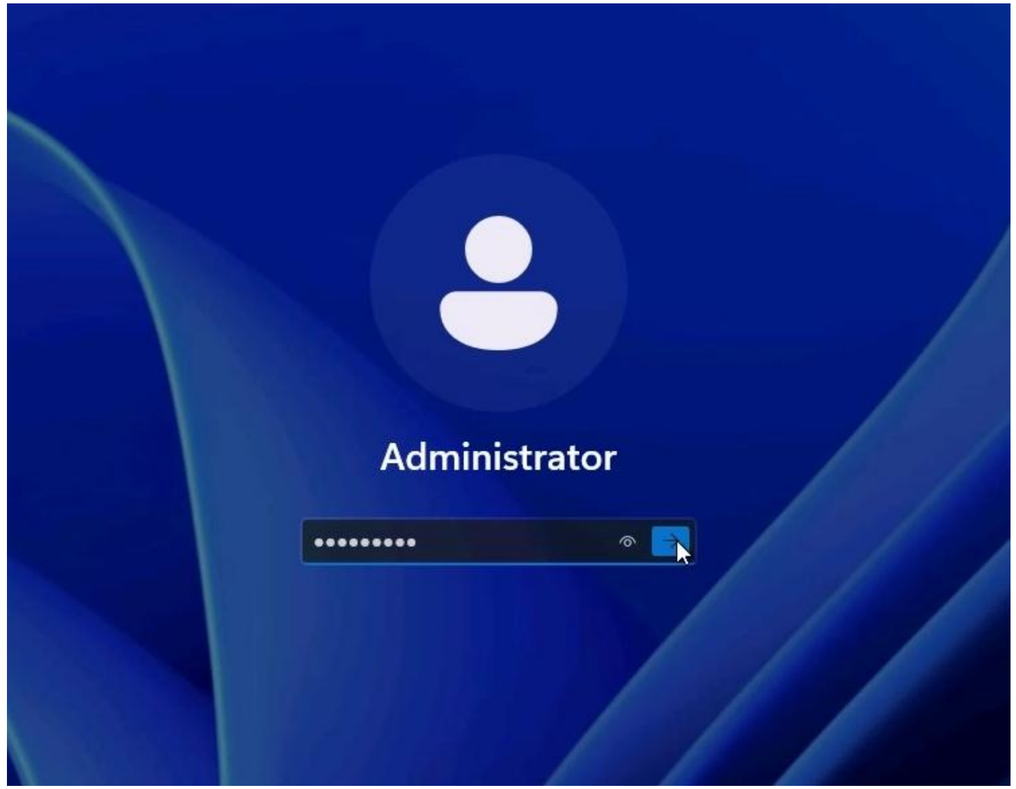
A1 ICT Distribucija

Kako upravljanjem privilegiranih pristopa do veće kibernetičke sigurnosti?

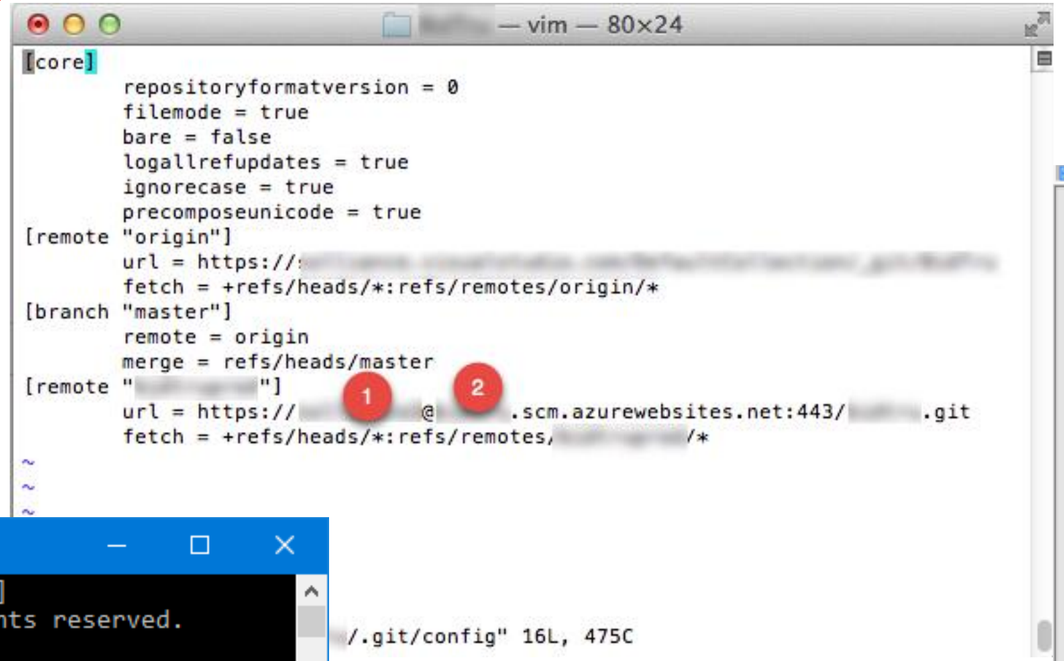
Marko Kašić, Lead ICT Engineer, A1 Slovenija

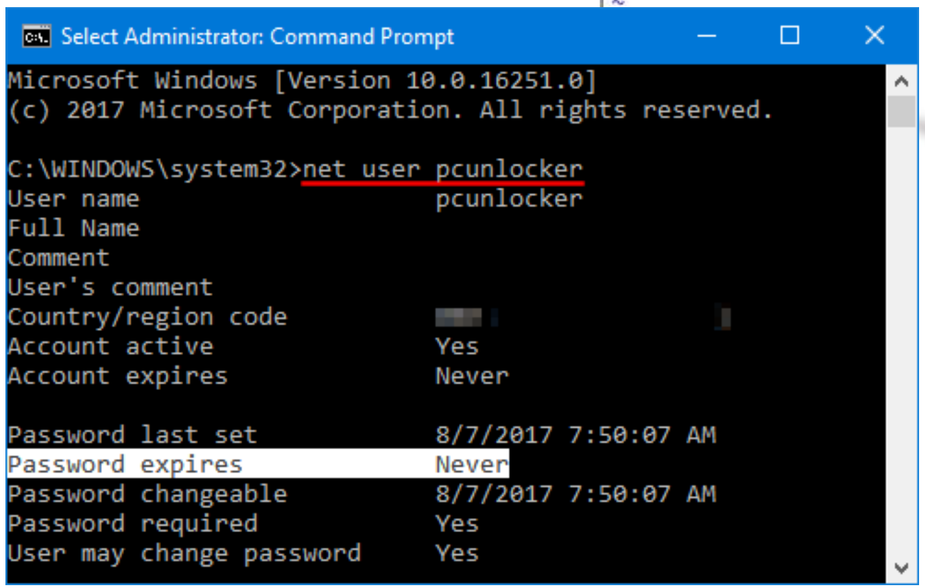
wallix

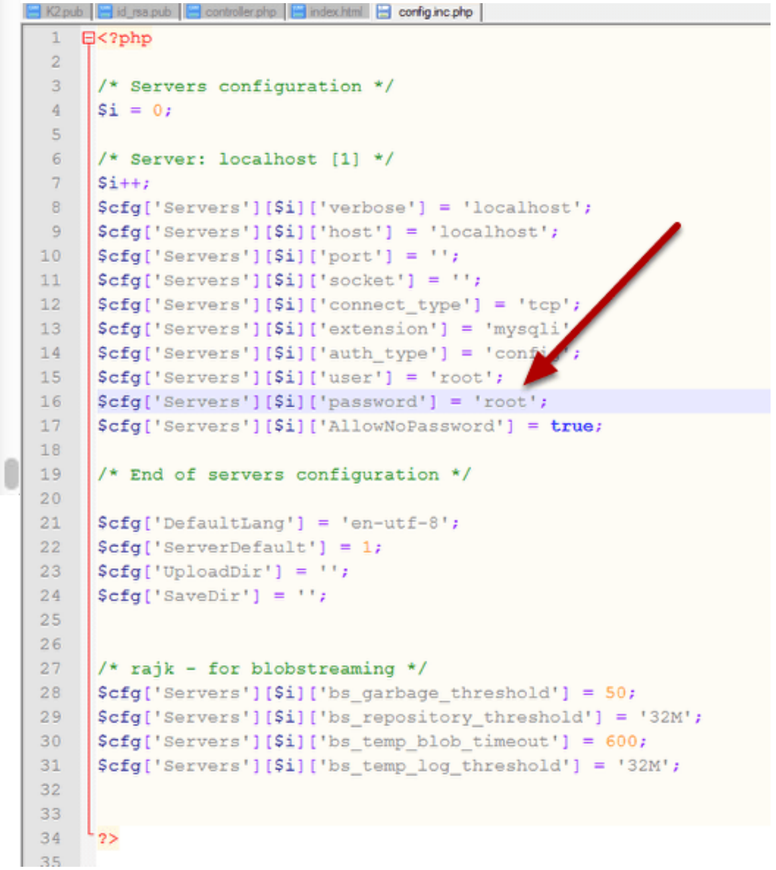
Nadzor privilegiranih računa



Nadzor privilegiranih računa







Nadzor privilegiranih računa

Trendovi koji potiču potrebu za kibernetičkom sigurnošću

- UPRAVLJANJE RIZICIMA

✓ Cyber napadi
✓ Reputacija
✓ Intelektualno vlasništvo
✓ Strateška sredstva

- COMPLIANCE

✓ Regulative i industrijski / državni standardi,…
  - GDPR,
  - NIS
  - PCI-DSS
  - HIPPA / HDS
  - ISO-27001
  - …

- MIGRACIJA U CLOUD

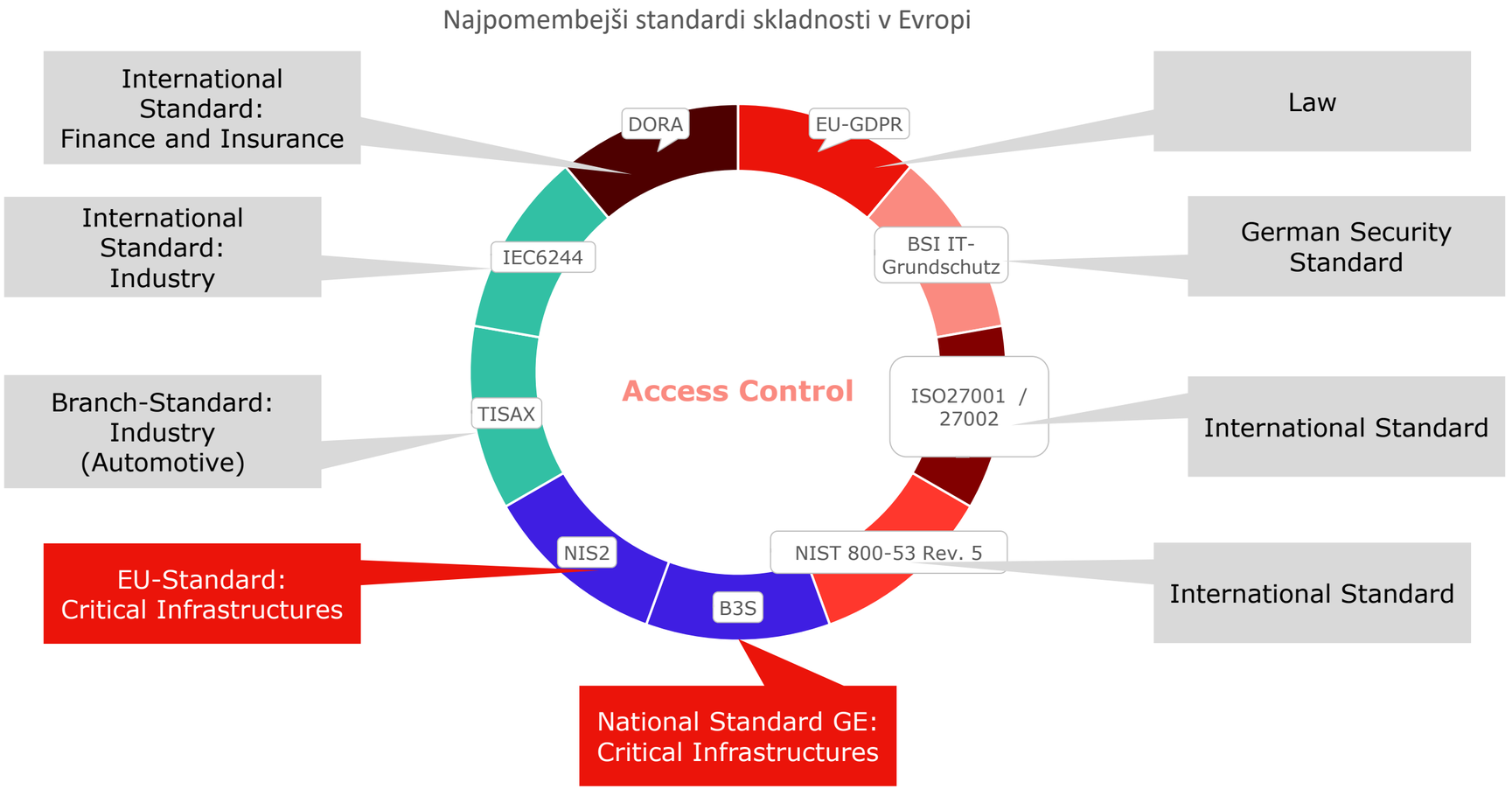
✓ Tehnička kompleksnost
✓ Migracija u javni cloud / hibrid

- DIGITALNA TRANSFORMACIJA

✓ Širenje Dev Ops
✓ Iz IT u OT i IoT mreže
✓ Mobilnost
✓ Interoperabilnost
✓ Eksplozija rasti broja uređaja


A1
80%
cyber napada iskorištava privilegirane račune

Regulative i standardi



Kontrola pristupa ima ključnu ulogu u svim standardima, čime se osigurava integritet podataka i ograničava pristup kritičnim podacima i sustavima.

NIS2

- **(44)** | CSIRT-ovi bi trebali imati mogućnost na zahtjev ključnog ili važnog subjekta pratiti imovinu subjekta s internetskim sučeljem, kako u fizičkim prostorima tako i izvan njih, kako bi utvrdili i razumjeli ukupne organizacijske rizike subjekta u pogledu novootkrivenih slučajeva ugrožavanja lanaca opskrbe ili kritičnih ranjivosti te upravljali njima. Subjekt bi trebalo poticati da obavijesti CSIRT o tome ima li **povlašteno upravljačko sučelje** jer bi to moglo utjecati na brzinu poduzimanja mjera ublažavanja.

- **(49)** | Politikama o kiberhigijeni pružaju se temelji za zaštitu infrastruktura mrežnih i informacijskih sustava, sigurnost hardvera, softvera i internetskih aplikacija te poslovnih podataka ili podataka krajnjih korisnika na koje se subjekti oslanjaju. Politike o kiberhigijeni sastoje se od zajedničkog temeljnog skupa praksi koje uključuju ažuriranja softvera i hardvera, **promjene lozinki**, upravljanje novim instalacijama, **ograničenje računa za pristup na razini administratora** i sigurnosno kopiranje podataka, te se njima omogućuje stvaranje proaktivnog okvira za pripravnost i opću sigurnost u slučaju incidenata ili kiberprijetnji. ENISA bi trebala pratiti i analizirati politike država članica u području kiberhigijene.

NIS2

- **(89)** | Ključni i važni subjekti bi trebali usvojiti **niz osnovnih praksi računalne kiberhigijene**, kao što su načela nultog povjerenja, ažuriranja softvera, konfiguracija uređaja, segmentacija mreže, **upravljanje identitetima i pristupom** ili informiranje korisnika, organizirati osposobljavanje svojeg osoblja i podizati razinu osviještenosti u području kiberprijetnji, phishinga ili tehnika društvenog inženjeringa. Nadalje, ti subjekti bi trebali procijeniti vlastite kibersigurnosne sposobnosti i, ako je prikladno, integrirati tehnologije kojima se jača kibersigurnost, kao što su umjetna inteligencija ili sustavi strojnog učenja u cilju jačanja svojih sposobnosti i zaštite mrežnih i informacijskih sustava.

Privileged Access Management (PAM)

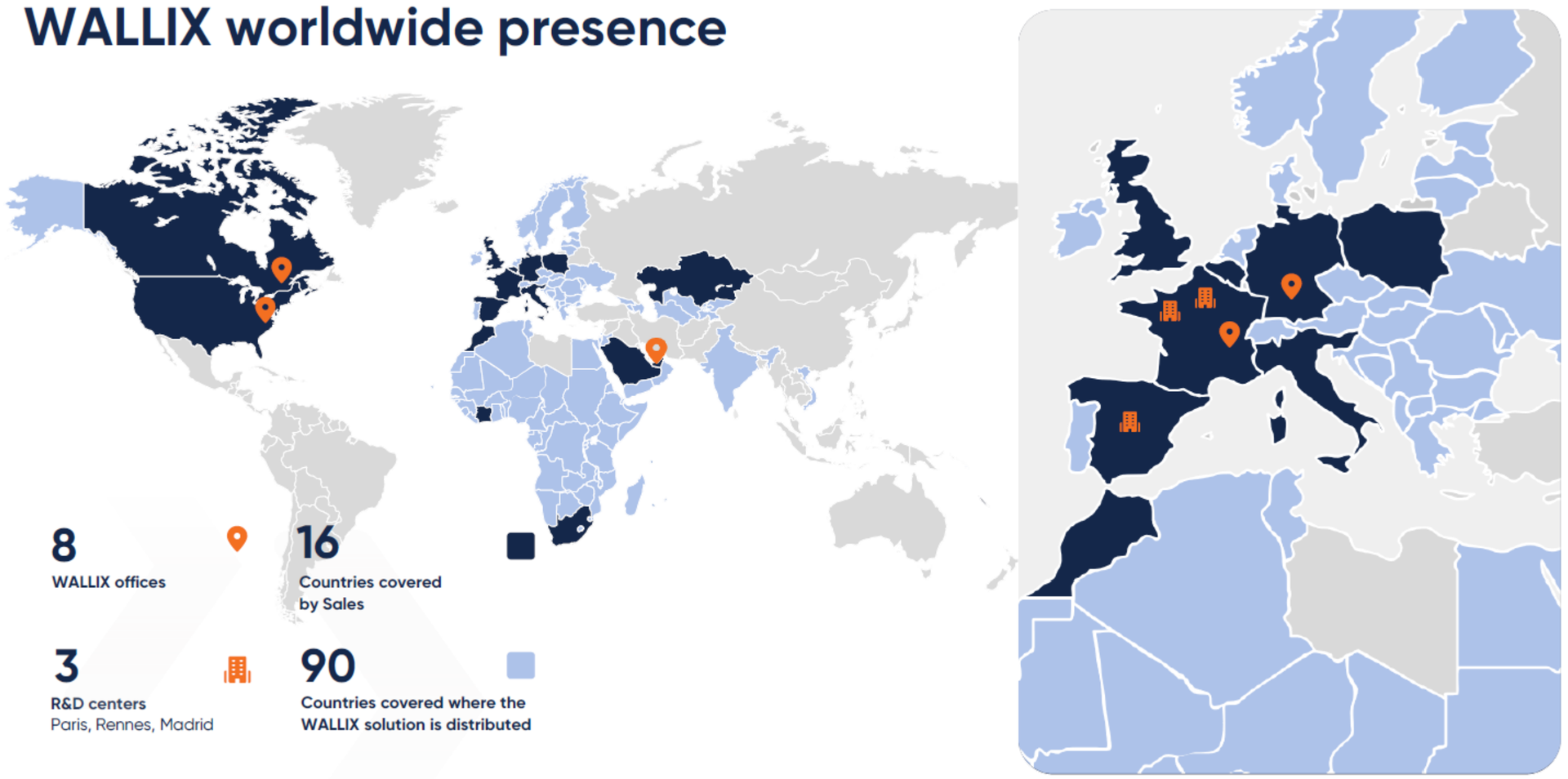
A1 ICT Distribucija

Wallix

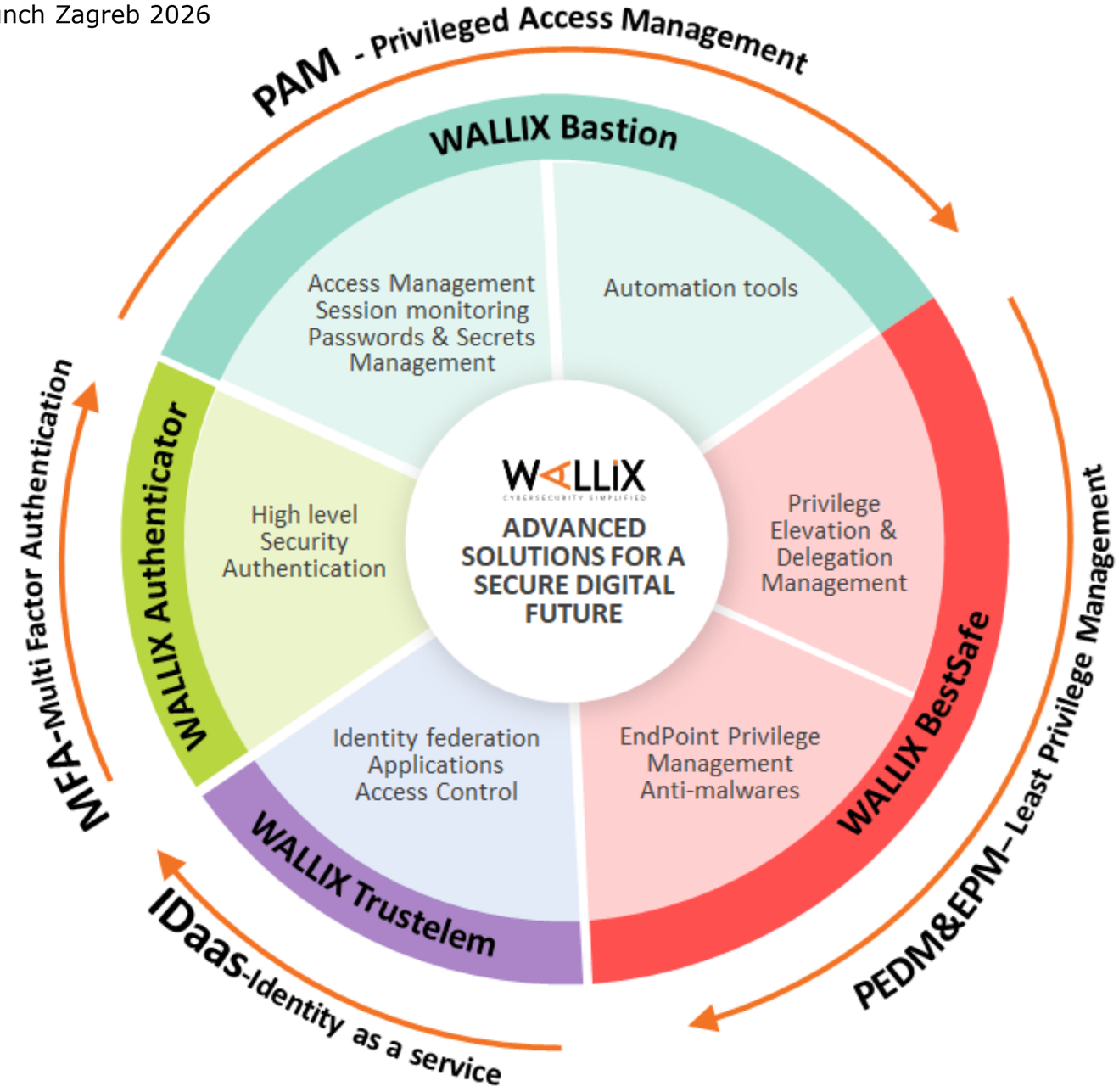
Wallix

BITNI PODACI

- 3000+ klienata
- 300+ partnera
- 90 država



Wallix


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
MFA-Multi Factor Authentication
Identity federation
Applications
Access Control
EndPoint Privilege Management
Anti-malwares
WALLIX Trustelem
IDaas-Identity as a service
PEDM&EPM– Least Privilege Management

WALLIX Bastion

Jednostavno rješenje za zaštitu privilegiranog pristupa kritičnim uređajima, čime se smanjuje sigurnosni rizik i usklađuje s regulatornim zahtjevima

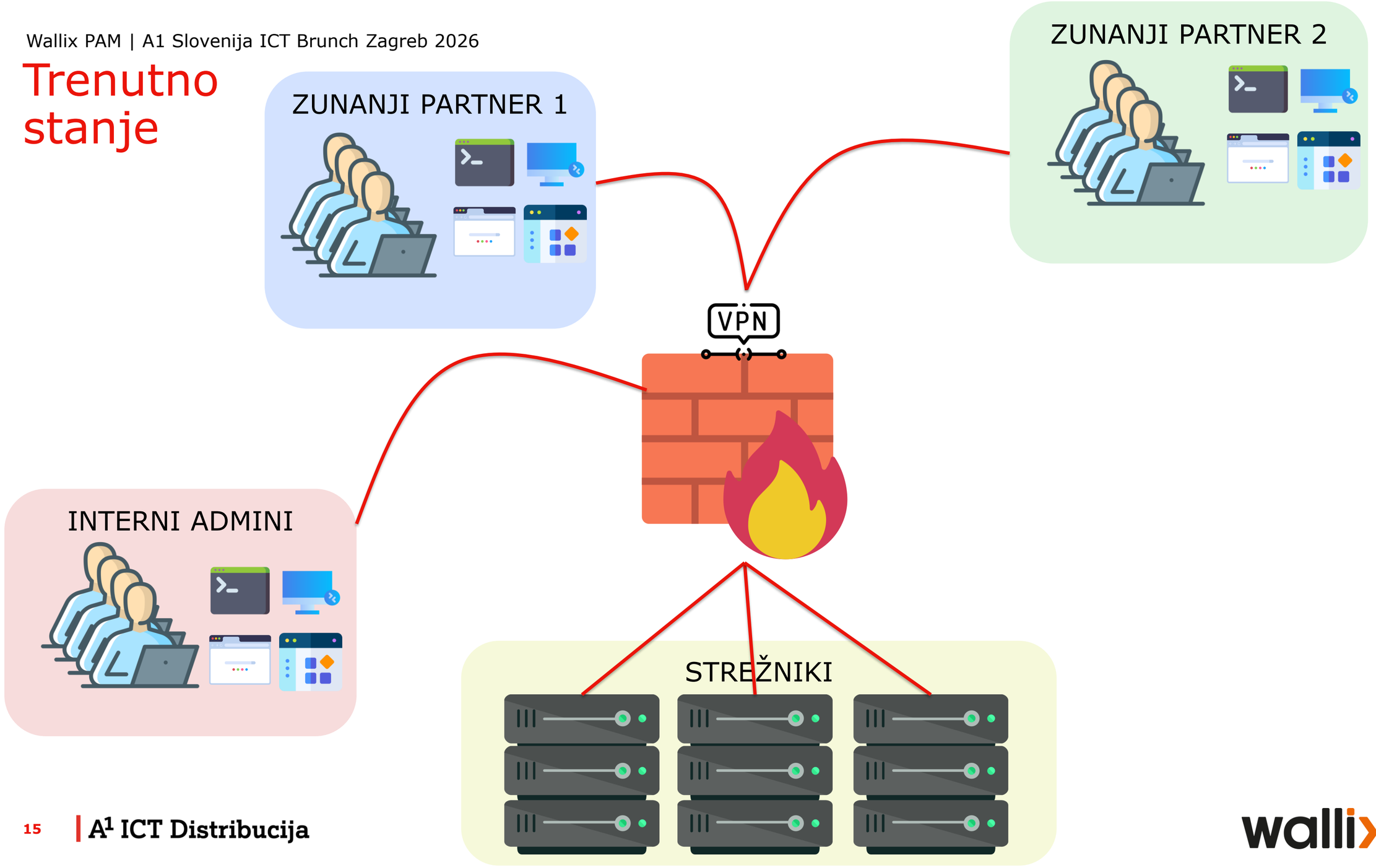
Zaštita udaljenog pristupa

Zaštita od unutarnjih prijetnji

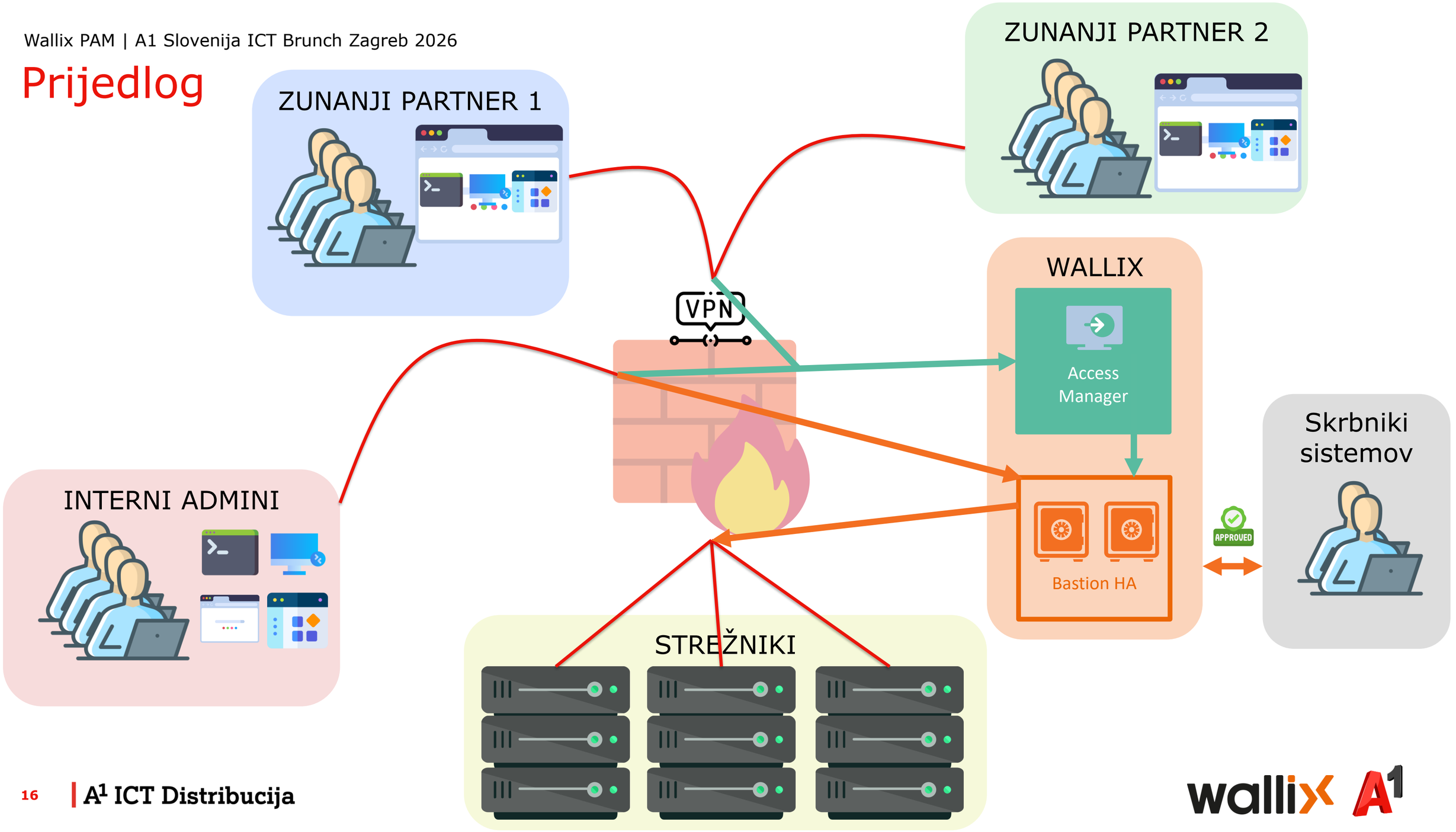
Zaštita za DevOps

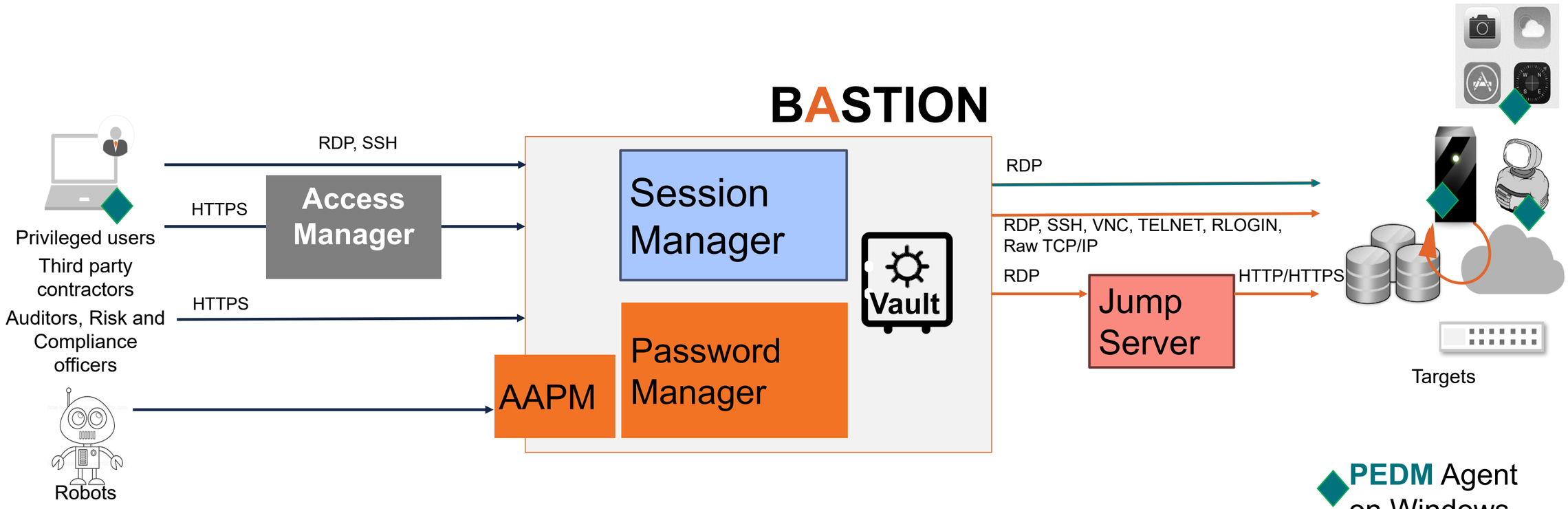
Sigurnost u OT okruženju

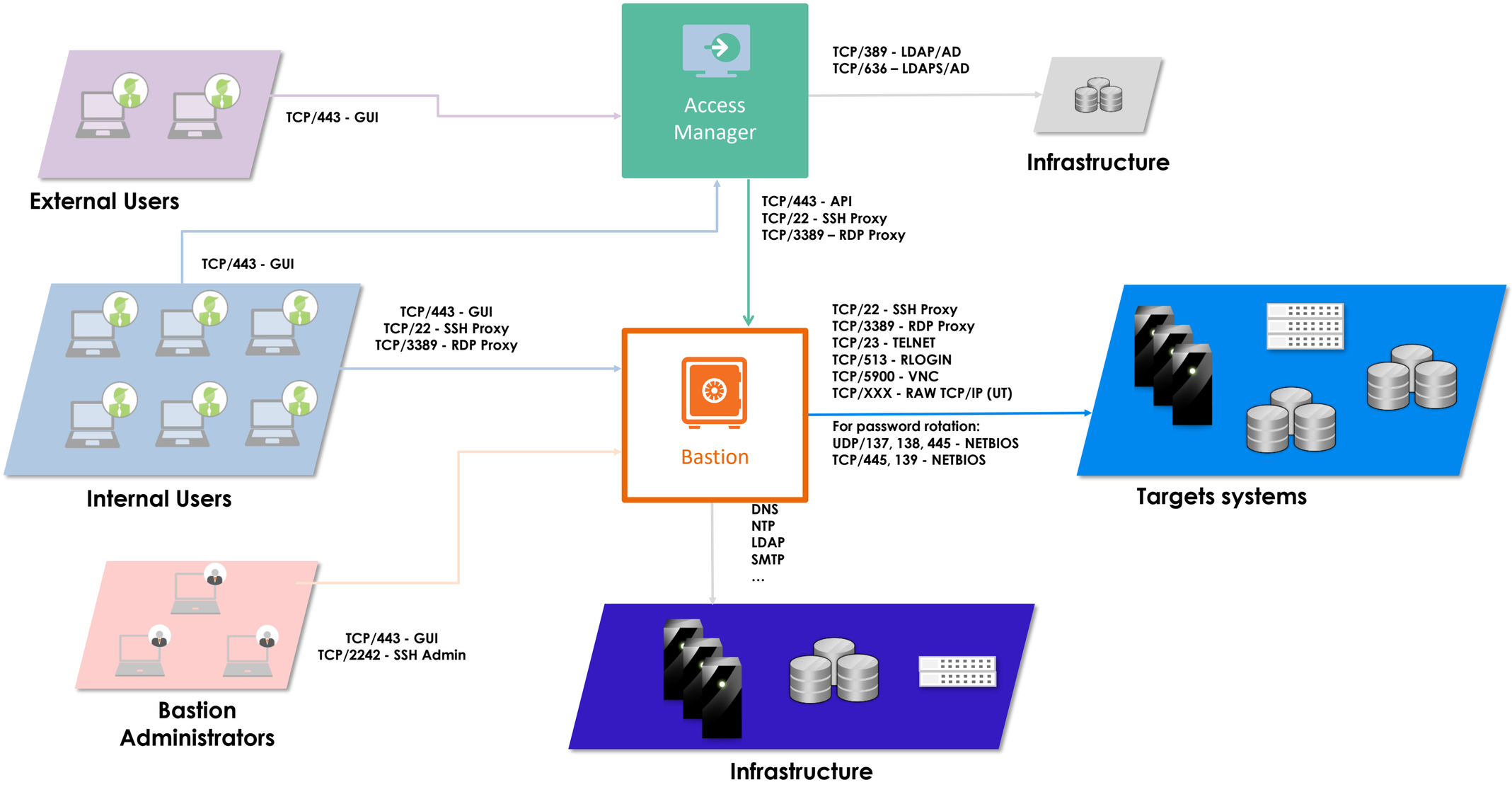
Trenutno stanje



Prijedlog


ZUNANJI PARTNER 1
ZUNANJI PARTNER 2
VPN
WALLIX
Access Manager
Bastion HA
APPROVED
Skrbniki sistemov
INTERNI ADMINI
STREŽNIKI


BASTION
RDP, SSH
HTTPS
Access Manager
Privileged users
Third party contractors
HTTPS
Auditors, Risk and Compliance officers
Robots
Session Manager
Password Manager
AAPM
Vault
RDP
RDP, SSH, VNC, TELNET, RLOGIN, Raw TCP/IP
RDP
Jump Server
HTTP/HTTPS
Targets
PEDM Agent on Windows based targets


Access Manager
TCP/389 - LDAP/AD
TCP/636 – LDAPS/AD
Infrastructure
External Users
TCP/443 - GUI
TCP/443 - API
TCP/22 - SSH Proxy
TCP/3389 – RDP Proxy
TCP/443 - GUI
Internal Users
TCP/443 - GUI
TCP/22 - SSH Proxy
TCP/3389 - RDP Proxy
Bastion
TCP/22 - SSH Proxy
TCP/3389 - RDP Proxy
TCP/23 - TELNET
TCP/513 - RLOGIN
TCP/5900 - VNC
TCP/XXX - RAW TCP/IP (UT)
For password rotation:
UDP/137, 138, 445 - NETBIOS
TCP/445, 139 - NETBIOS
Targets systems
DNS
NTP
LDAP
SMTP
...
Bastion Administrators
TCP/443 - GUI
TCP/2242 - SSH Admin
Infrastructure

Wallix v regiji

- Klijenti v **različitim sektorima**
  - Energetika
  - Financije
  - Zdravstvo
  - Državne institucije
  - Proizvodnja
  - …

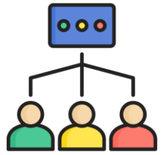
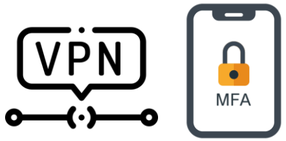
- Iskusni, stručni i certificirani partneri u regiji
  - Prve implementacije **u 2016**

- A1 Slovenija **distributer godine** za CEE regiju 2022. in 2023.

- U 2024. i 2025. godini uspješno realizirana **2 top projekta u CEE regiji** (financijski sektor)

Tipični zahtjevi

- Mogućnost uvida u aktivne i povijesne sesije 
- Obvezno odobrenje svakog pristupa kritičnim sustavima 

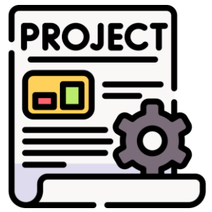
- Integracija s postojećim korisnicima u Microsoft Active Directoryju 
- MFA sustav, ako ne postoji (+ VPN) 

- Osiguravanje usklađenosti sa zakonodavstvom, standardima i regulativom 
- Zaštita privilegiranih računa od naprednih napada i zloupotrebe kroz lanac opskrbe 

Implementacija

- **Ukupno sa lokalnim partnerom**
  - Certificirani stručnjaki
  - Povjerenje u partnere temeljeno na dobrom iskustvu

- **Tipičan projekt**
  - Priprava popisa standardnih pristupa
  - Implementacija sustava Wallix Bastion u visokoj dostupnosti (HA)
  - Implementacija sustava Wallix Access Manager za internetski/web pristup
  - Uspostava sinkronizacije s internim sustavima (Aktivni imenik – Microsoft AD)
  - Uvoz popisa svih sustava za pristup
  - Validacija svih scenarija pristupa i implementacija procesa odobrenja
  - Provedba edukacije i prijenos znanja za napredno korištenje
  - **Veličina: 200 sustava i 50 privilegiranih korisnika**



Koristi implementacije

- Nadzor svih pristupa privilegiranih korisnika **na jednom mjestu** (bilježenje svih pristupa i njihovih aktivnosti)

- Zaštita sustava od kibernetičkih napada **kroz lanac opskrbe**

- **Optimizacija rada administratora** sustava zahvaljujući procesu odobrenja svakog pristupa

- Implementacijom je osigurana **usklađenost s internim i vanjskim regulativama** (NIS2, ZinfV-1, GDPR, ISO/IEC 27000, …)

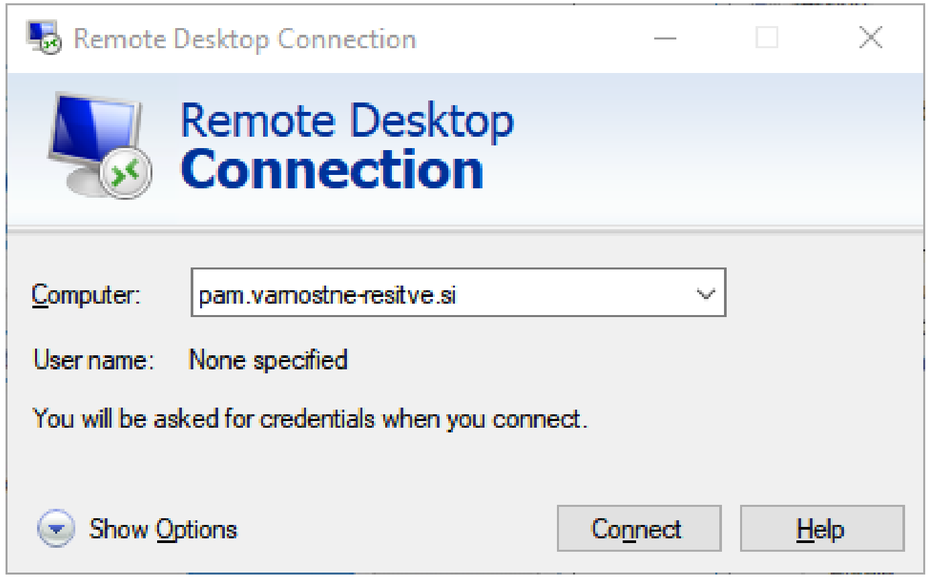
- **Samostalno upravljanje sustavom**

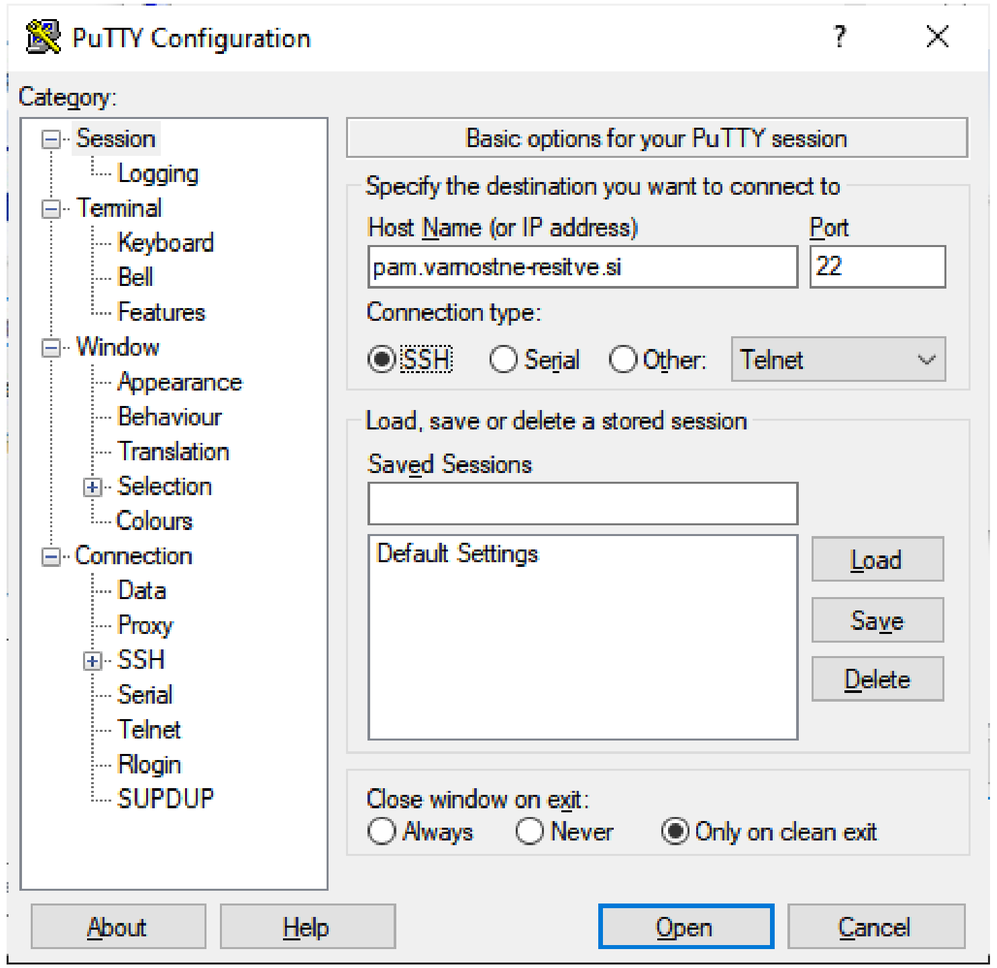
- **Lokalni partner na raspolaganju** za veće zahvate (npr. nadogradnja sustava)

.

Wallix PAM u praksi

A1 ICT Distribucija


Remote Desktop Connection
Remote Desktop
Connection
Computer:
pam.varnostne-resitve.si
User name:
None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
pam.varnostne-resitve.si
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel

Authorization	Target ?	Protocol
Interactive	Interactive@TestnoOkolje:RDP	RDP
MarkoAdmin	Skruju@local@Windows-10:RDP	RDP
MarkoAdmin	administrator@local@WinSrv2019_FSPM:RDP	RDP
MarkoAdmin	administrator@local@WinSrv2022Lic:RDP	RDP
MarkoAdmin	administrator@local@WinSrv_DC01:RDP	RDP
MarkoAdmin	administrator@local@WinSrv_Suite:RDP	RDP
MarkoAdmin	administrator@local@WinSrv_prtg:RDP	RDP
MarkoAdmin	ict.local\administrator@ict.local@WinSrv2016:RDP	RDP
MarkoAdmin	ict.local\administrator@local@WinSrv2019_FSPM:RDP	RDP
MarkoAdmin	ict.local\administrator@local@WinSrv_DC01:RDP	RDP
MarkoAdmin	ict.local\administrator@local@WinSrv_Suite:RDP	RDP
MarkoAdmin	ict.local\administrator@local@WinSrv_prtg:RDP	RDP
MarkoAdmin	ict2\ictadministrator@local@WinSrv2012Ess:RDP	RDP
MarkoAdmin	rds@local@RDS_Debian:RDP	RDP

sl-SI

◀◀ ◀ 1 /1 ▶ ▶▶

Logout Connect

Information

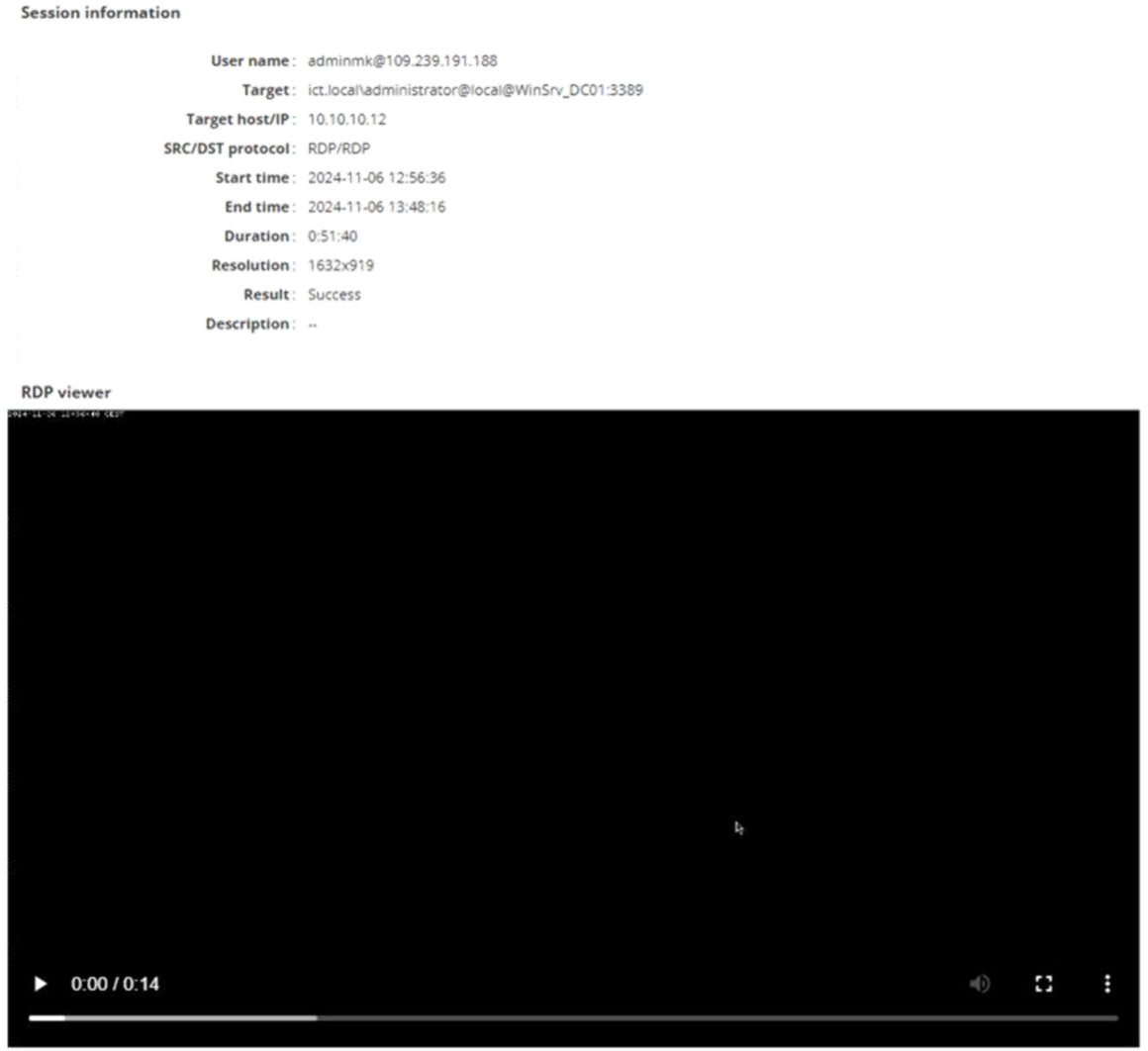
You are hereby informed and acknowledge that your actions may be recorded, retained and audited in accordance with your organization security policy.
Please contact your WALLIX Bastion administrator for further information.

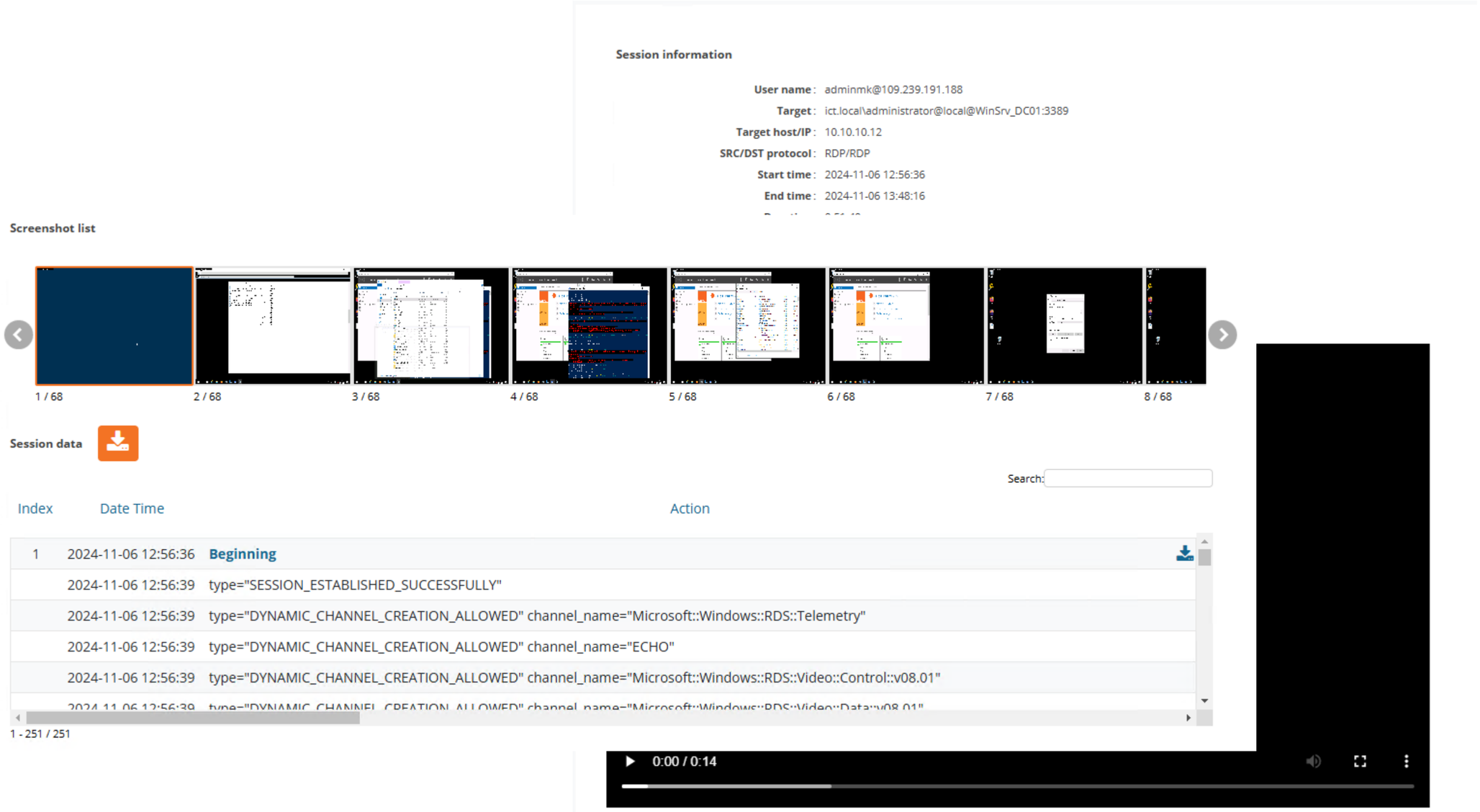
OK Refused

```
Keyboard-interactive authentication prompts from server:
End of keyboard-interactive prompts from server
| ID | Site (page 1/1)              | Authorization
|----|------------------------------|---------------
|  0 | admin@local@FW:SSH           | CLI
|  1 | admin@local@FW:SSH           | MarkoAdmin
|  2 | rds@local@RDS_Debian:SSH     | MarkoAdmin
|  3 | Interactive@TestnoOkolje:SSH | Interactive
|  4 | Interactive@TestnoOkolje:SSH | MarkoAdmin
Enter h for help, ctrl-D to quit
 > 1
Selected target: admin@local@FW:SSH
Account successfully checked out

You are hereby informed and acknowledge that your actions may be recorded, retained and audited in accordance with your organization security policy.
Please contact your WALLIX Bastion administrator for further information.

Last login: Mon Oct 14 14:57:36 2024 from 109.239.191.188
```

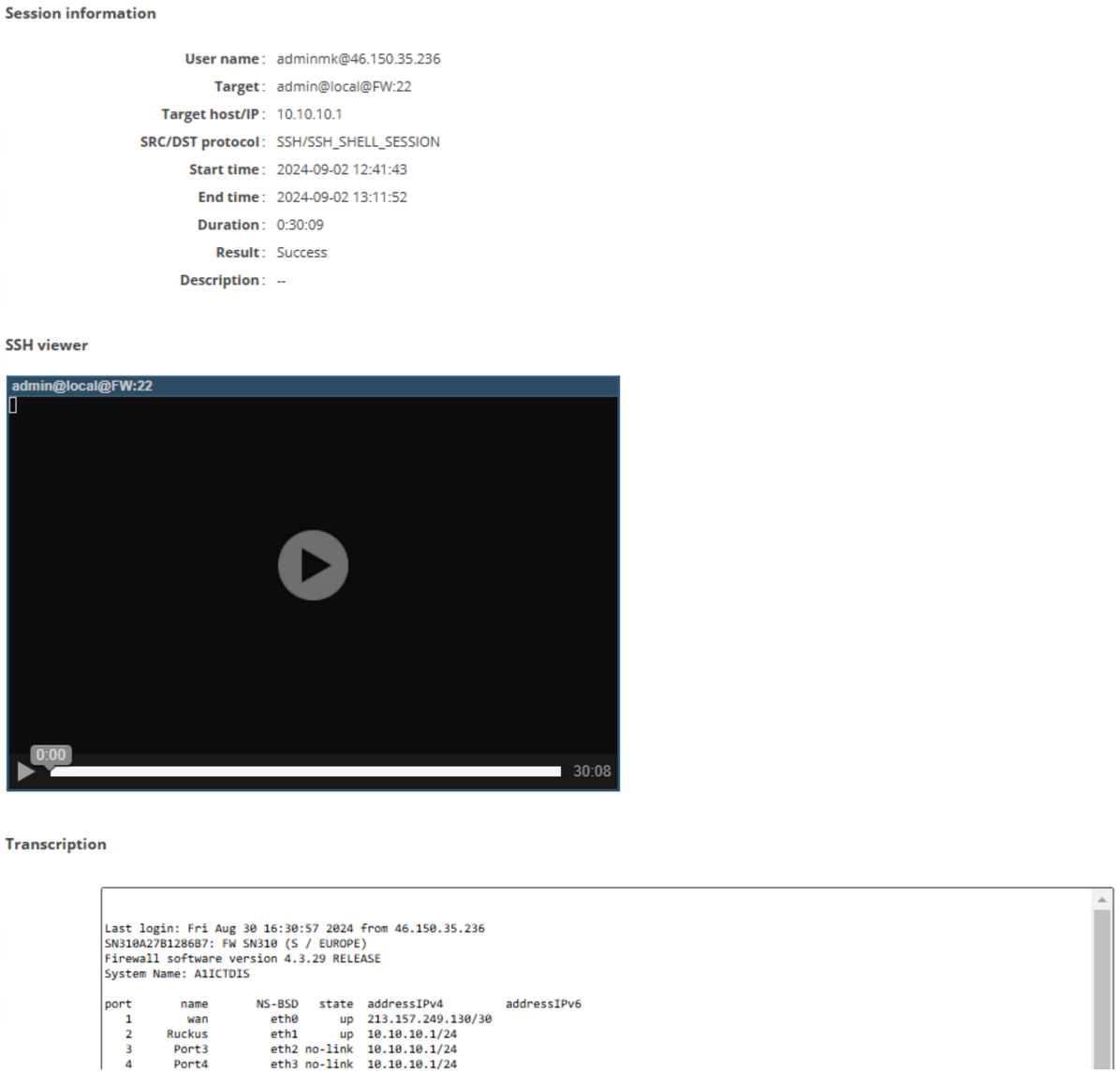
	User	Target	Target host/IP	SRC/DST protocol	Start time	End time	Duration	Size	Result
🔍	adminmk@109.239.191.188	administrator@local@WinSrv2022Lic:3389	10.10.10.15	RDP/RDP	2024-11-06 13:44:23	2024-11-06 13:48:14	00:03:51	707.6 KB	✓
🔍	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_DC01:3389	10.10.10.12	RDP/RDP	2024-11-06 12:56:36	2024-11-06 13:48:16	00:51:40	12.5 MB	✓
🔍	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_DC01:3389	10.10.10.12	RDP/RDP	2024-11-06 10:08:19	2024-11-06 11:37:10	01:28:51	6.2 MB	✓
🔍	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_DC01:3389	10.10.10.12	RDP/RDP	2024-11-04 15:19:19	2024-11-04 16:19:24	01:00:05	1.5 MB	✓
🔍	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_DC01:3389	10.10.10.12	RDP/RDP	2024-11-04 15:18:39	2024-11-04 15:19:21	00:00:42	10.2 KB	✓
	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_Suite:3389	10.10.10.19	RDP/RDP	2024-11-04 15:18:32	2024-11-04 15:18:36	00:00:04	--	⛔
🔍	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_DC01:3389	10.10.10.12	RDP/RDP	2024-11-04 15:13:41	2024-11-04 15:18:05	00:04:24	1.0 MB	✓
	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_DC01:3389	10.10.10.12	RDP/RDP	2024-11-04 15:11:34	2024-11-04 15:12:52	00:01:18	--	✓
🔍	adminmk@109.239.191.188	rds@local@RDS_Debian:3389	10.10.10.42	RDP/RDP	2024-10-28 12:20:48	2024-10-28 15:06:04	02:45:16	--	✓
🔍	adminmk@46.122.102.23	rds@local@RDS_Debian:3389	10.10.10.42	RDP/RDP	2024-10-23 13:12:28	2024-10-23 14:00:57	00:48:29	607.6 MB	✓
🔍	adminmk@109.239.191.188	rds@local@RDS_Debian:3389	10.10.10.42	RDP/RDP	2024-10-23 09:49:01	2024-10-23 12:07:12	02:18:11	--	✓
🔍	adminmk@109.239.191.188	administrator@local@WinSrv2022Lic:3389	10.10.10.15	RDP/RDP	2024-10-21 10:26:01	2024-10-21 12:07:15	01:41:14	583.6 KB	✓
	adminmk@109.239.191.188	administrator@local@WinSrv2022Lic:3389	10.10.10.15	RDP/RDP	2024-10-21 09:51:33	2024-10-21 09:51:37	00:00:04	--	⛔
🔍	adminmk@109.239.191.188	administrator@local@WinSrv2022Lic:3389	10.10.10.15	RDP/RDP	2024-10-21 09:37:59	2024-10-21 09:49:23	00:11:24	3.7 MB	✓
🔍	adminmk@46.150.35.236	ict.local\administrator@local@WinSrv_Suite:3389	10.10.10.19	RDP/RDP	2024-10-15 12:47:51	2024-10-15 14:22:44	01:34:53	3.4 MB	✓
🔍	adminmk@46.150.35.236	ict.local\administrator@local@WinSrv_Suite:3389	10.10.10.19	RDP/RDP	2024-10-15 07:40:28	2024-10-15 09:46:00	02:05:32	3.0 MB	✓
🔍	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_Suite:3389	10.10.10.19	RDP/RDP	2024-10-14 15:03:15	2024-10-14 17:03:35	02:00:20	19.3 MB	✓
🔍	adminmk@109.239.191.187	ict.local\administrator@local@WinSrv_Suite:3389	10.10.10.19	RDP/RDP	2024-10-14 14:44:43	2024-10-14 15:03:18	00:18:35	1.2 MB	✓
🔍	adminmk@109.239.191.188	ict.local\administrator@local@WinSrv_Suite:3389	10.10.10.19	RDP/RDP	2024-10-14 14:31:16	2024-10-14 14:44:46	00:13:30	2.0 MB	✓

- „snemanje“ seje
- Beleženje vnosov tipkovnice
- Beleženje vseh procesov
- Beleženje aktivnih oken uporabnika
- Beleženje izbranih opcij v oknih
- Gesla se NE beležijo



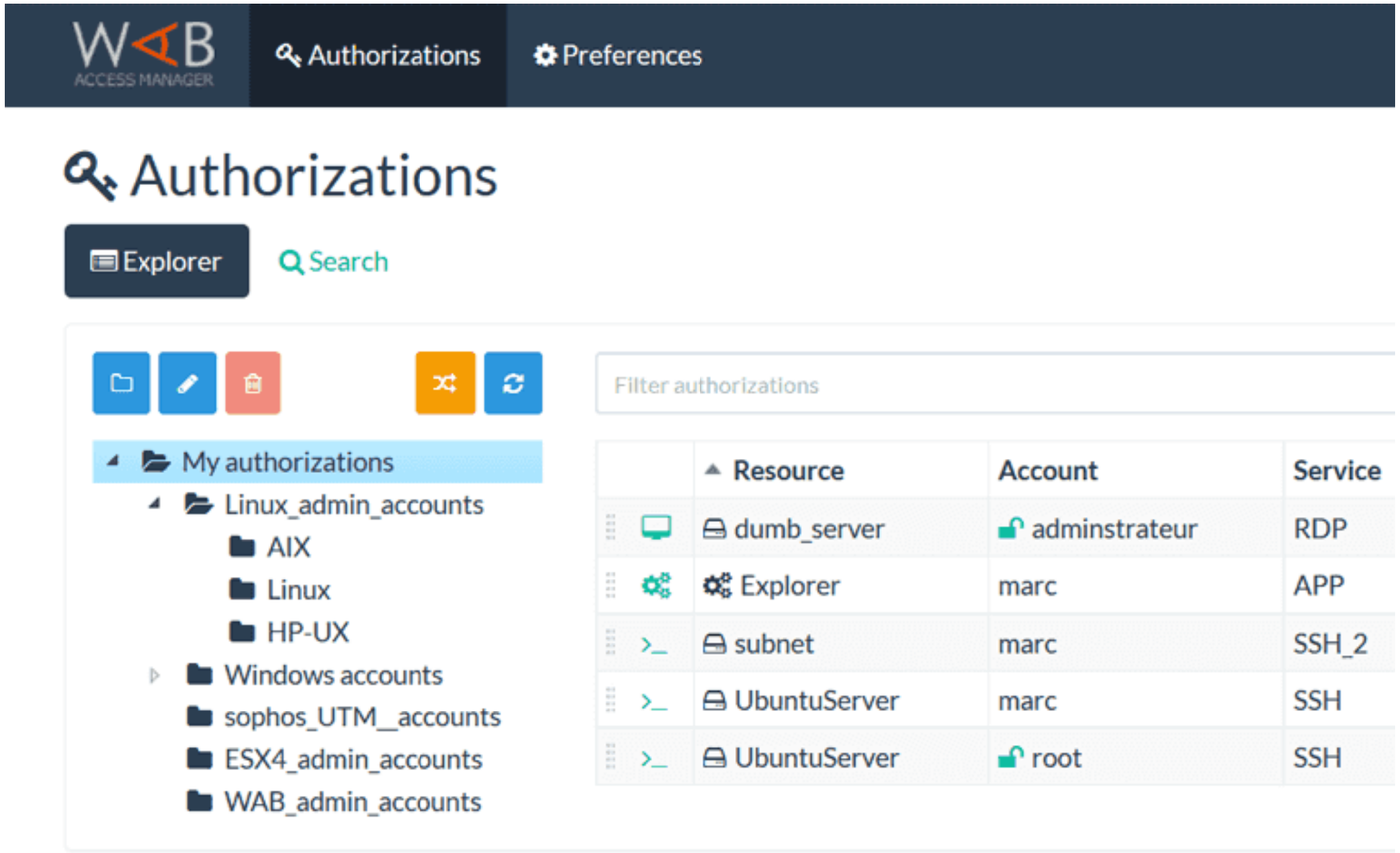

Session information
User name : adminmk@109.239.191.188
Target : ict.local\administrator@local@WinSrv_DC01:3389
Target host/IP : 10.10.10.12
SRC/DST protocol : RDP/RDP
Start time : 2024-11-06 12:56:36
End time : 2024-11-06 13:48:16
Screenshot list
1 / 68
2 / 68
3 / 68
4 / 68
5 / 68
6 / 68
7 / 68
8 / 68
Session data
Search:
Index
Date Time
Action
1 2024-11-06 12:56:36 Beginning
2024-11-06 12:56:39 type="SESSION_ESTABLISHED_SUCCESSFULLY"
2024-11-06 12:56:39 type="DYNAMIC_CHANNEL_CREATION_ALLOWED" channel_name="Microsoft::Windows::RDS::Telemetry"
2024-11-06 12:56:39 type="DYNAMIC_CHANNEL_CREATION_ALLOWED" channel_name="ECHO"
2024-11-06 12:56:39 type="DYNAMIC_CHANNEL_CREATION_ALLOWED" channel_name="Microsoft::Windows::RDS::Video::Control::v08.01"
1 - 251 / 251
0:00 / 0:14

- „Snimanje” sesije / Session recording
- Beležnje unosa s tipkovnice (Keylogging)
- Lozinke se NE bilježe
- Cijeli transkript s vremenskim oznakama (Timestamp)

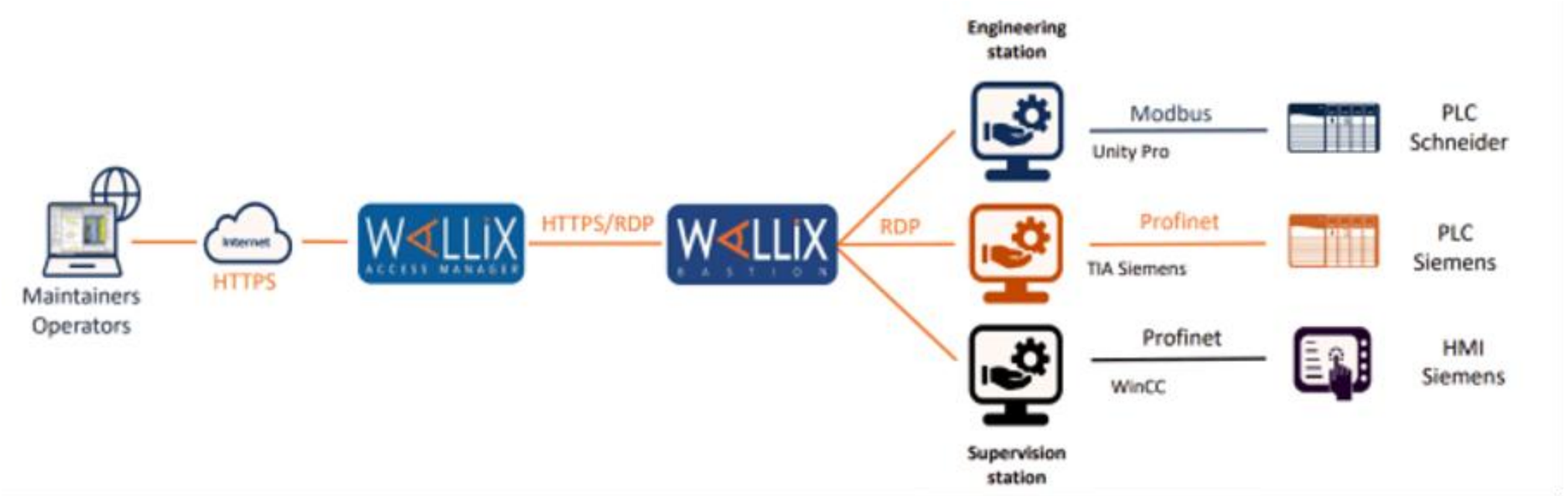


Access Manager

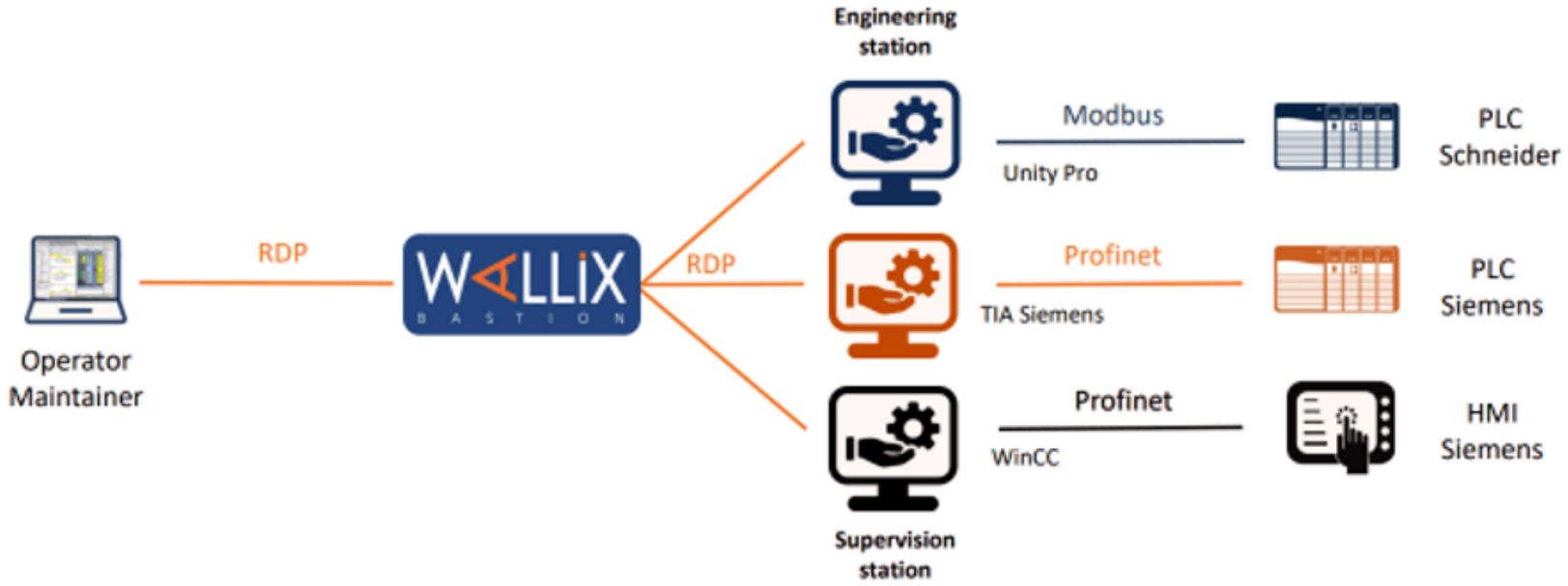
- Pristup putem jedne točke (HTTPS pristup)
- Multi-tenant arhitektura / postavka
- Bez potrebe za klijentom ili agentom (Agentless)



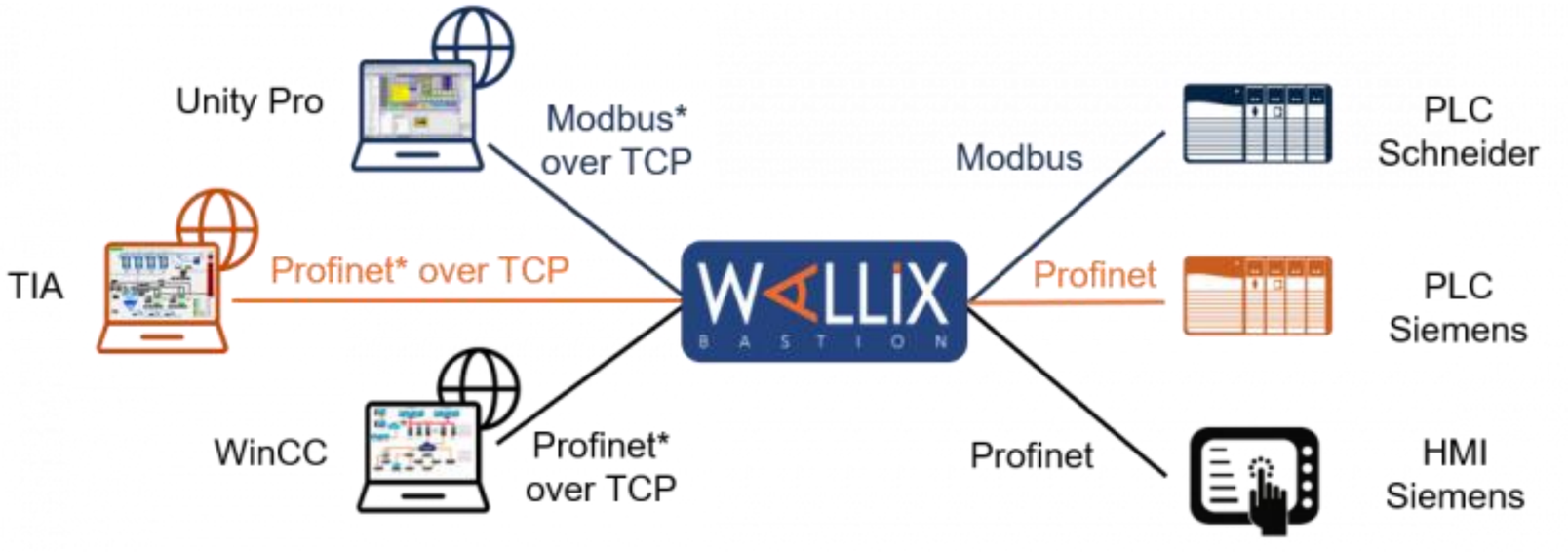
Pristup u OT mreži



Pristup u OT mreži



Pristup u OT mreži



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

Uvjerite se sami

- Več o rešitvi na:
  - https://varnostne-resitve.si/
  - ict-partners@A1.si

Thank you

Marko Kašić

E marko.kasic@A1.si
M +386 40 440 842