COMGUARD

cyber security masters

# Proaktivní ochrana před zneužitím privilegovaných účtů

Petr Konečný| Senior Account Manager

19. 9. 2024

## Compliance

NIS2

Potřeba vyhovět Zákonu o kybernetické bezpečnosti

Interní směrnice a pravidla

COMGUARD

| Bezpečnostní opatření poskytovatele regulované služby | | |
|---|---|---|
| | **v režimu vyšších povinností** | **v režimu nižších povinností** |
| organizační opatření | § 4 Systém řízení bezpečnosti informací | § 4 Zajišťování kybernetické bezpečnosti |
| | § 5 Povinnosti Vrcholného vedení | § 5 Povinnosti vrcholného vedení |
| | § 6 Bezpečnostní role | |
| | § 7 Řízení bezpečnostní politiky a bezpečnostní dokumentace | |
| | § 8 Řízení aktiv | |
| | § 9 Řízení rizik | |
| | § 10 Řízení dodavatelů | |
| | § 11 Bezpečnost lidských zdrojů | § 6 Bezpečnost lidských zdrojů |
| | § 12 Řízení změn | |
| | § 13 Akvizice, vývoj a údržba | |
| | § 14 Řízení přístupu | § 8 Řízení přístupu |
| | § 15 Zvládání kybernetických bezpečnostních událostí a incidentů | § 11 Řešení kybernetických bezpečnostních incidentů |
| | § 16 Řízení kontinuity činností | § 7 Řízení kontinuity činností |
| | § 17 Audit kybernetické bezpečnosti | |
| technická opatření | § 18 Fyzická bezpečnost | |
| | § 19 Bezpečnost komunikačních sítí | § 12 Bezpečnost komunikačních sítí |
| | § 20 Správa a ověřování identit | § 9 Řízení identit a jejich oprávnění |
| | § 21 Řízení přístupových oprávnění | § 18 Řízení přístupových oprávnění |
| | § 22 Detekce kybernetických bezpečnostních událostí | § 10 Detekce a zaznamenávání kybernetických bezpečnostních událostí |
| | § 23 Zaznamenávání událostí | |
| | § 24 Vyhodnocování kybernetických bezpečnostních událostí | |
| | § 25 Aplikační bezpečnost | § 13 Aplikační bezpečnost |
| | § 26 Kryptografické algoritmy | § 14 Kryptografické algoritmy |
| | § 27 Zajišťování dostupnosti regulované služby | |
| | § 28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv | |

## NIS2: § 20 - Správa a ověřování identit / § 21 – Řízení přístupových oprávnění

- Povinná osoba používá nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv regulované služby. Nástroj zajišťuje:
  - ověření identity před zahájením jejich aktivit,
  - opětovné ověření identity po stanovené době nečinnosti,
  - centralizovanou správu identit s ohledem na vazby mezi aktivy.
- Povinná osoba pro ověření identity administrátorů, uživatelů a technických aktiv využívá autentizační mechanizmus, který je založený na **vícefaktorové autentizaci** s nejméně dvěma různými typy faktorů.

## NIS2: § 14 - Řízení přístupu

Povinná osoba dále v rámci řízení přístupu k aktivům:

- omezí přidělování administrátorských a privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce

COMGUARD

## Compliance

NIS2

Potřeba vyhovět Zákonu o kybernetické bezpečnosti

Interní směrnice a pravidla

## Administrátorská hesla

Nevhodné nakládání s credentials – Nešifrované dokumenty, post-it lístečky

Chybějící efektivní, standardizovaný přístup ke správě přihlašovacích údajů

Sdílené účty typu Admin & Root již nadále nejsou přípustné

## Řešení incidentů

Privilegovaný účet mnohdy vázaný na aktivum, ne uživatele

Nedaří se dohledat původ a okolnosti incidentů

Nevíme, kdo prováděl daný servisní úkon

## Externí poskytovatelé služeb

Chybí mi přehled o činnostech externistů v mé infrastruktuře

Nevíme, kdo má přístup ke kterým zařízením, na jakou dobu a za jakých okolností

Máme zájem tyto přístupy kontrolovat

COMGUARD

## Zero Trust – Never trust, always verify

- Nevkládáme důvěru uživatelům, zařízením, aplikacím ani souborům, bez ohledu na umístění
    - Multifaktorová autentizace jako standard, důsledná identifikace, kontrola souborů, kontrola rolí
- Důsledné řízení a monitoring privilegovaných přístupů
    - Podklady pro dohledatelnost původu relací se sdíleným účtem (Admin, root)

## Just in Time přístup

- Oprávnění udělujeme pouze v případě aktuální potřeby
- Lze vyžádat kontext žádosti o udělení přístupu

## POLP – Principle of least privileges

- Ideálně udělujeme nejnižší míru oprávnění potřebnou k výkonu práce
- Oprávnění je možné dočasně eskalovat po schválení

wallix

- Francouzská společnost s mezinárodní působnosti
- Leader v oblasti PIM / PAM
- Silné zaměření na OT security

**KUPPINGERCOLE**

**Leader 2020-2022**

**FROST & SULLIVAN**

V roce 2022 byl PAM4ALL vyhodnocen jako nejlepší dostupné PAM řešení s ohledy na flexibilitu, jednoduchost a cenu.

**2022 Customer Value Leadership Award**

Gartner

Velmi rychlý posun na **globálního Leadera** v roce 2022

2022 SPARK MATRIX LEADER

**QUADRANT KNOWLEDGE SOLUTIONS**

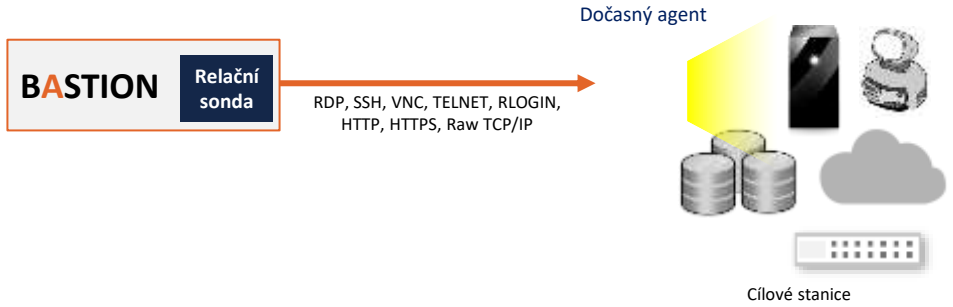
**Leader** v prvním vydání Spark Matrix PAM

COMGUARD

# Session Manager

## Správa vzdálených přístupů

- Spolupracuje se zabezpečeným úložištěm přihlašovacích údajů
- Obstará autentizaci a poskytne přístup k spravovaným aktivům
  - Podpora vícefaktorové autentizace
- Umožňuje nastavení rozšířených přístupových pravidel
  - Časové rámce, schvalovací procesy
- Podpora ICAP pro kontrolu souborů – DLP, AV




## Řízení uživatelských aktivit

- Umožňuje v reálném čase:
  - Sledovat a sdílet relaci
  - Upozornit na nepovolené akce a příkazy
  - Detekovat anomálie (blacklistované příkazy) a následně ukončit relaci

## Dohledatelnost a audit

- Pořizuje nepozměnitelné záznamy a loguje uskutečněné relace
  - Bohatá metadata díky **relační sondě**
  - Možnost přehrání záznamu relace
  - Záznam všech aktivit včetně management konzolí a webových aplikací

## PEDM / EPM

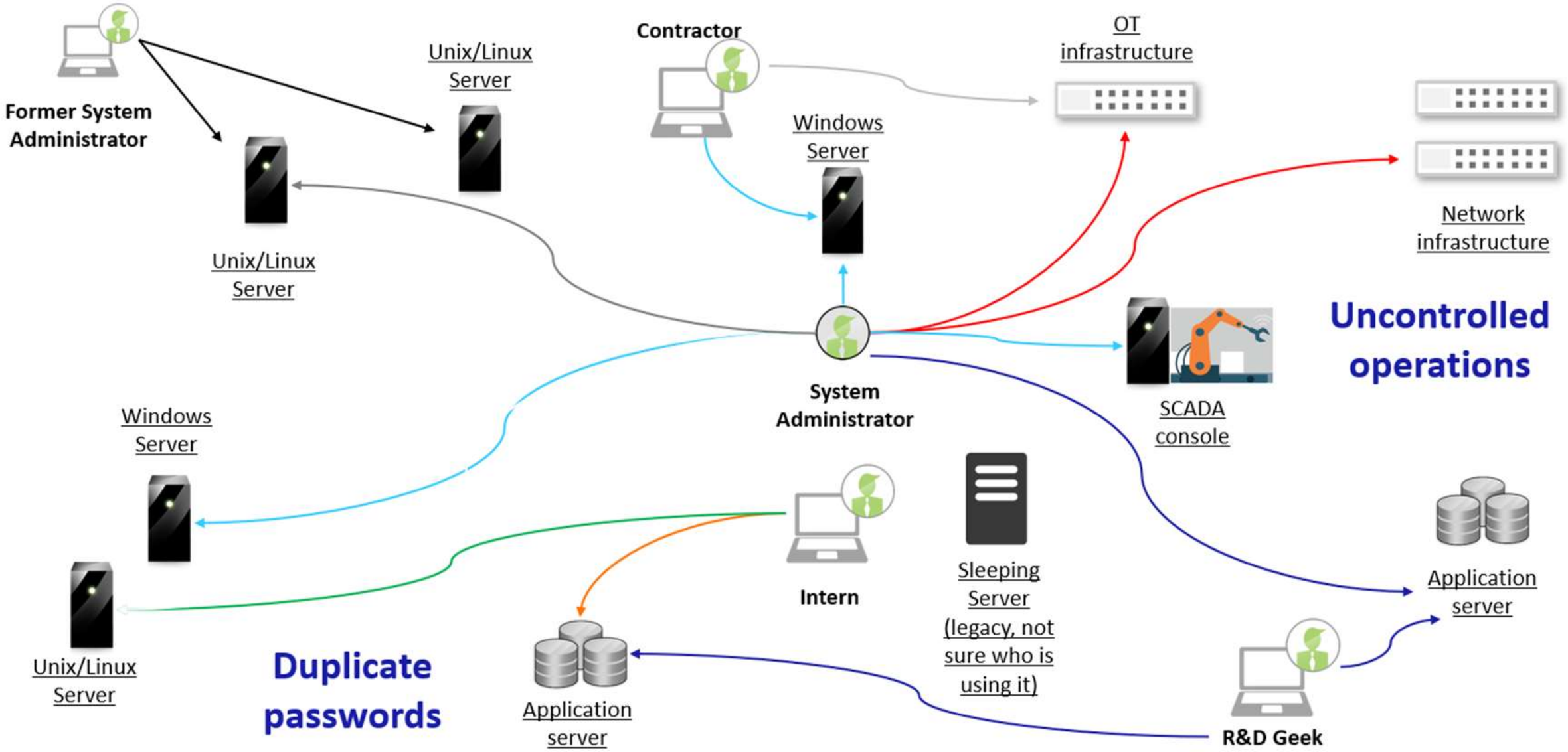
**Prosazení principu nejnižších privilegií bez dopadu na produktivitu**

- Využitelné jako komponenta PAM ekosystému nebo standalone nástroj

- Granulární definice oprávnění v kontextu uživatelů / aplikací
- Umožňuje plošně odebrat uživatelům administrátorská oprávnění
  - Náhrada ve formě udělení oprávnění aplikacím / procesům

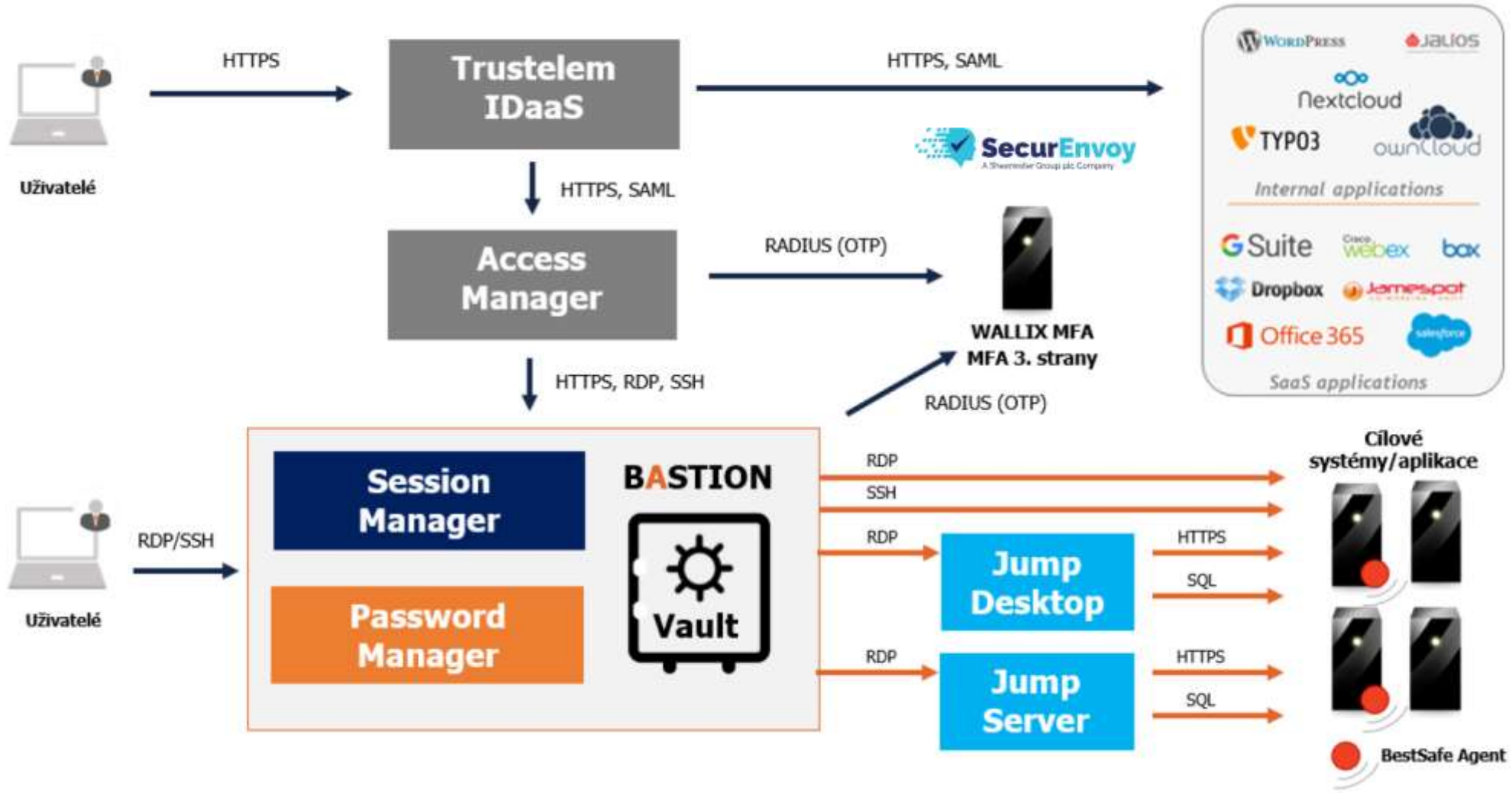
- Efektivní nástroj pro machine hardening účelových PC
- Ochrana proti ransomware blokací CryptoAPI

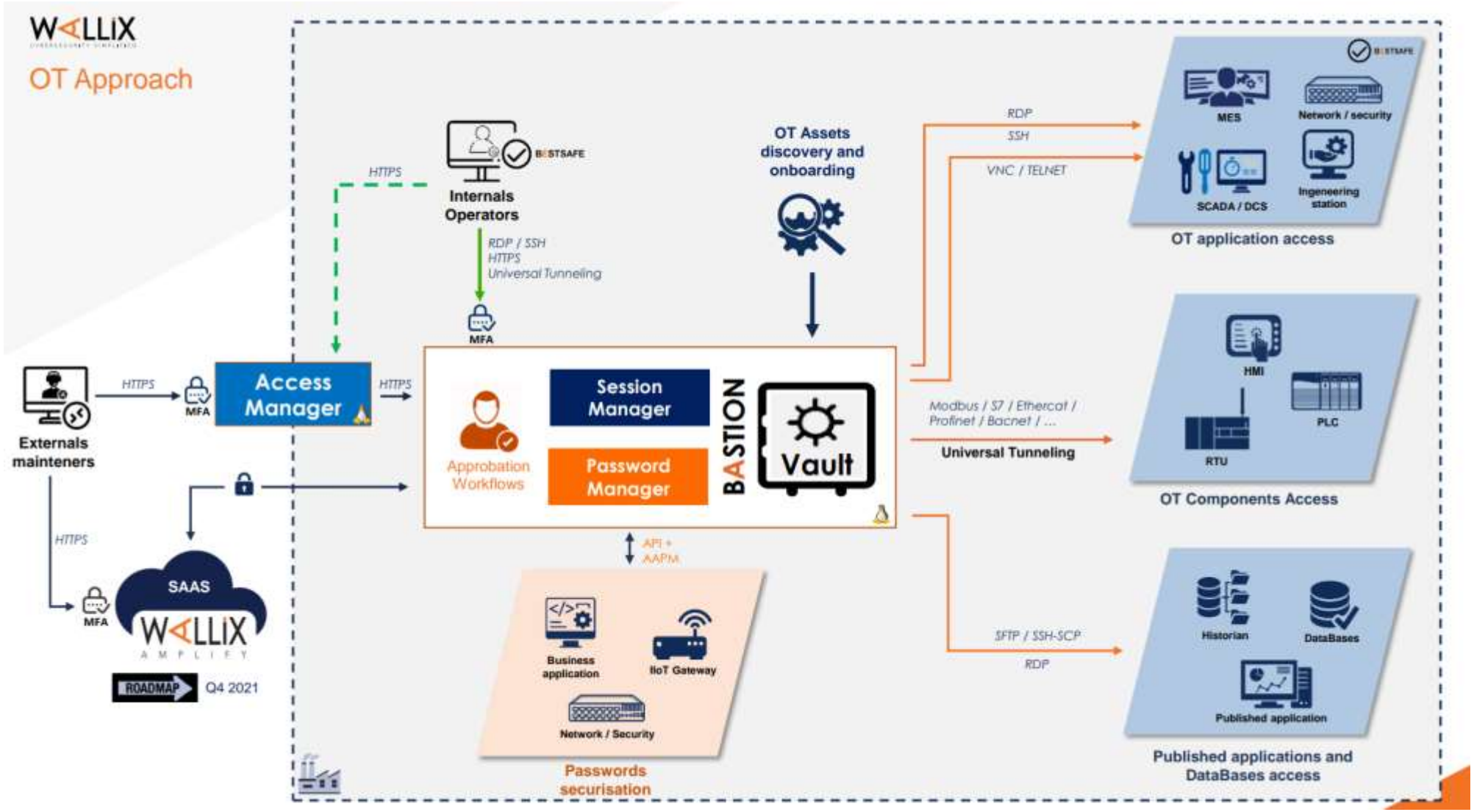
**81% ze 189 kritických zranitelností Microsoft nalezených v roce 2019 bylo možné mitigovat odebráním lokálních administrátorských práv uživatelům.**


Former System Administrator
Unix/Linux Server
Unix/Linux Server
Contractor
Windows Server
OT infrastructure
Network infrastructure
System Administrator
SCADA console
Uncontrolled operations
Windows Server
Unix/Linux Server
Intern
Sleeping Server (legacy, not sure who is using it)
Application server
Duplicate passwords
Application server
R&D Geek

COMGUARD

wallix




WALLIX
OT Approach
HTTPS
BESTSAFE
Internals Operators
RDP / SSH
HTTPS
Universal Tunneling
MFA
OT Assets discovery and onboarding
RDP
SSH
VNC / TELNET
MES
Network / security
SCADA / DCS
Ingeneering station
OT application access
HTTPS
MFA
Access Manager
HTTPS
Externals mainteners
Approbation Workflows
Session Manager
Password Manager
BASTION
Vault
Modbus / S7 / Ethercat / Profinet / Bacnet / ...
Universal Tunneling
HMI
PLC
RTU
OT Components Access
HTTPS
MFA
SAAS
WALLIX AMPLIFY
ROADMAP
Q4 2021
API + AAPM
Business application
IIoT Gateway
Network / Security
Passwords securisation
SFTP / SSH-SCP
RDP
Historian
DataBases
Published application
Published applications and DataBases access

COMGUARD

cyber security masters

# Děkujeme za pozornost!