COMGUARD
communication security

WALLIX Bastion

Spravovat privilegované přístupy nikdy nebylo tak snadné

Lukáš Babčický | Vendor Manager

Data Breach Investigations Report 2021, Verizon – Privilege Misuse

Frequency	265 incidents, 222 with confirmed data disclosure
Threat Actors	Internal (99%), Multiple (9%), External (8%), Partner (2%) (breaches)
Actor Motives	Financial (64%), Fun (17%), Grudge (14%), Espionage (9%), Convenience (3%), Ideology (1%) (breaches)
Data Compromised	Personal (64%), Other (35%), Medical (27%), Internal (19%) (breaches)

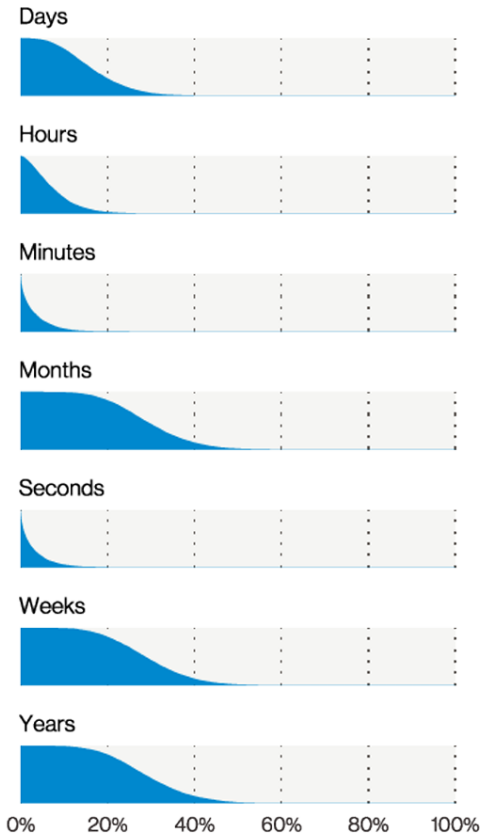


Figure 70. Discovery timeline in Privilege Misuse breaches (n=22)

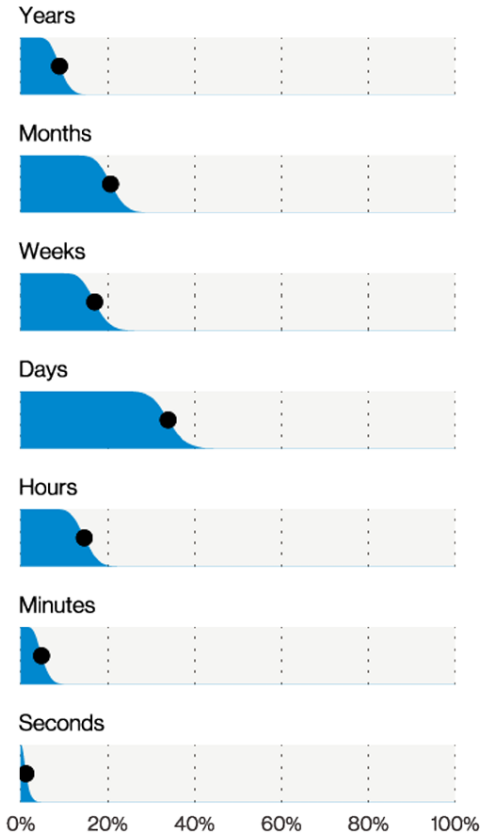


Figure 71. Discovery timeline in 2021 breaches (n=195)

Zero Trust přístup

- „Never trust, always verify“
    - Nevkládáme důvěru uživatelům, zařízením ani aplikacím, bez ohledu na umístění
    - Prosazení MFA jako standardu
    - Důsledné řízení a monitoring

Just in time access (JIT)

- Časové ohraničení udělení privilegií, upřesnění kontextu, schvalovací procesy

Princip nejnižších oprávnění

- Odebrání přebytečných privilegií na nejnižší nezbytnou míru

WALLIX
CYBERSECURITY SIMPLIFIED

- Francouzská společnost s mezinárodní působností
- 18 let působnosti na trhu
- Evropský leader v oblasti PAM

Source: Gartner (July 2021)

Komplexní portfolio interoperatibilních řešení

- Samostatně funkční a vysoce škálovatelné komponenty
- Možnost postupného deploymentu
- Uživatelská přívětivost ruku v ruce s zabezpečením bez kompromisů
    - Nevyžaduje výrazné zásahy do infrastruktury a změny stávajících workflows

- **PAM**
  - Bastion Session Manager
  - Bastion Password Manager
  - Access Manager

- **IDaaS (Identity as a service)**
  - Trustelem

- **MFA**
  - Authenticator

- **EPM (Endpoint Privilege Management)**
- **PEDM (Privilege Elevation and Delegation Management)**
  - BestSafe

SSO vstupní brána

- Obstarání autentizace a poskytnutí přístupu k cílovým aktivům
  - Podpora MFA
- Spolupracuje se zabezpečeným úložištěm přihlašovacích údajů
- Umožňuje nastavení rozšířených přístupových pravidel
  - Časové rámce, schvalovací procesy

SSO vstupní brána

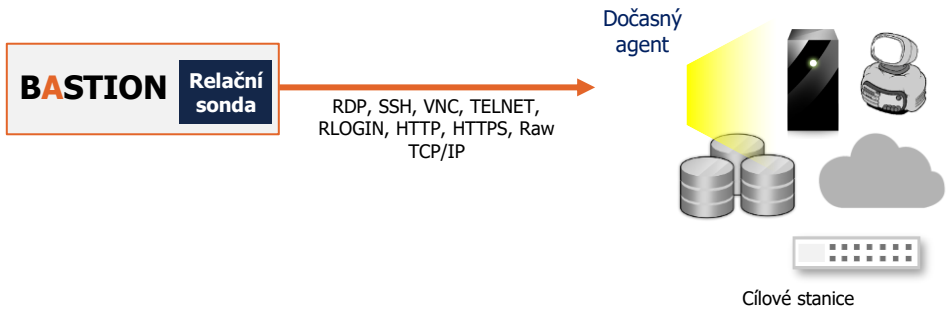
- Obstarání autentizace a poskytnutí přístupu k cílovým aktivům
  - Podpora MFA
- Spolupracuje se zabezpečeným úložištěm přihlašovacích údajů
- Umožňuje nastavení rozšířených přístupových pravidel
  - Časové rámce, schvalovací procesy

Monitoring uživatelských aktivit

- Sledování či sdílení relace
- Monitoring aktivit
- Detekce nežádoucího chování
- Podpora ICAP pro kontrolu souborů
  - DLP
  - Antimalware

Audit a dohledatelnost

- Pořízení nepozměnitelného záznamu a logování relací
- Obohacení nahrávky o metadata z **relační sondy**



Správa a rotace credentials

- Spolupráce s Password Vaultem (AES256 Encrypted)
- Management hesel a SSH klíčů

Cílové stanice

Password Manager umožňuje:

- Automatizaci rotace hesel
- Definici jejich formátu / komplexity
- Výměnu po časovém úseku
- Výměnu po využití

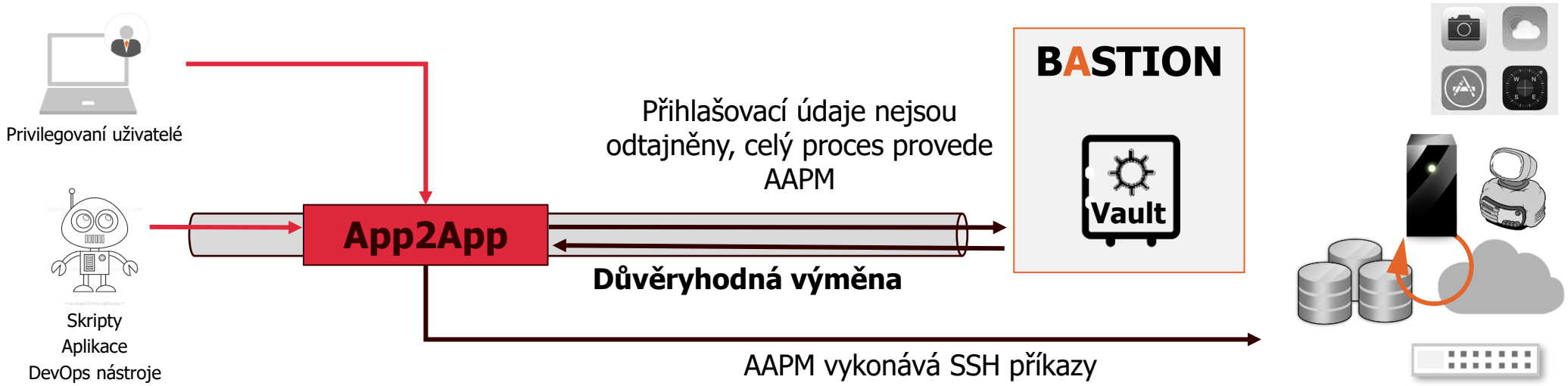
- Check-In / Check-Out proces
- Breaking Glass mechanismus

Nativní podpora rotace hesel na systémech:

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

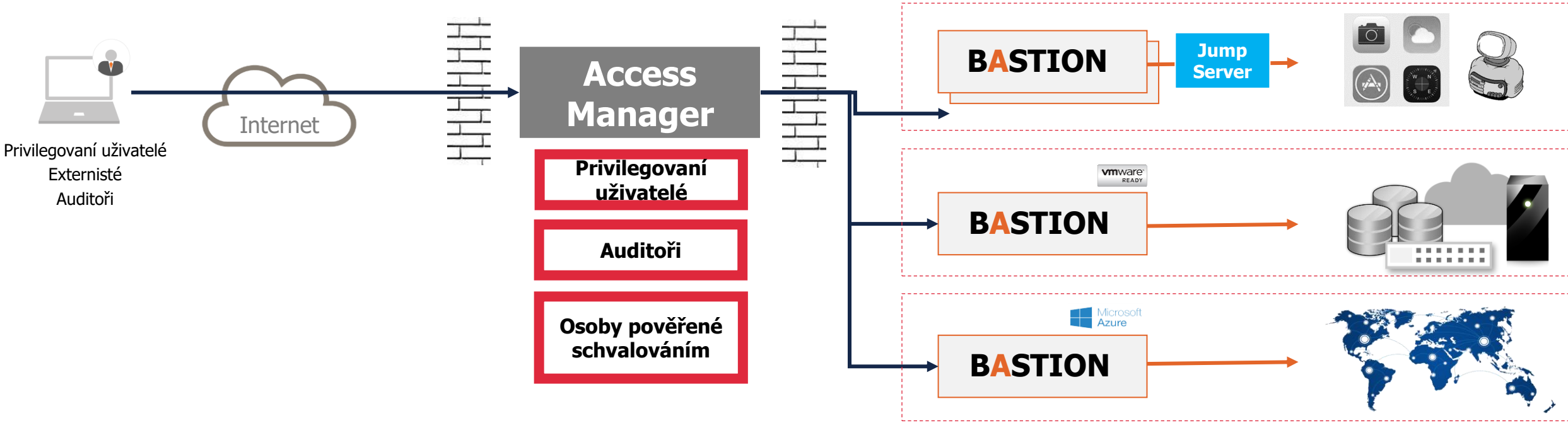
Application to Application Password Management

- Řešení pro zabezpečení přihlašovacích údajů u automatizovaných úkonů – DevOps či skripty
- Efektivní náhrada hardcoded hesel
- AAPM vyzvedne credentials z Vaultu a provede úkon definovaný skriptem



HTML5 vstupní brána k Bastionu

- SSO prostředí pro více instancí PAM
- Jednotný bod pro auditing
- Přístup k PM i SM
- Přizpůsobitelné rozhraní



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.

IDaaS

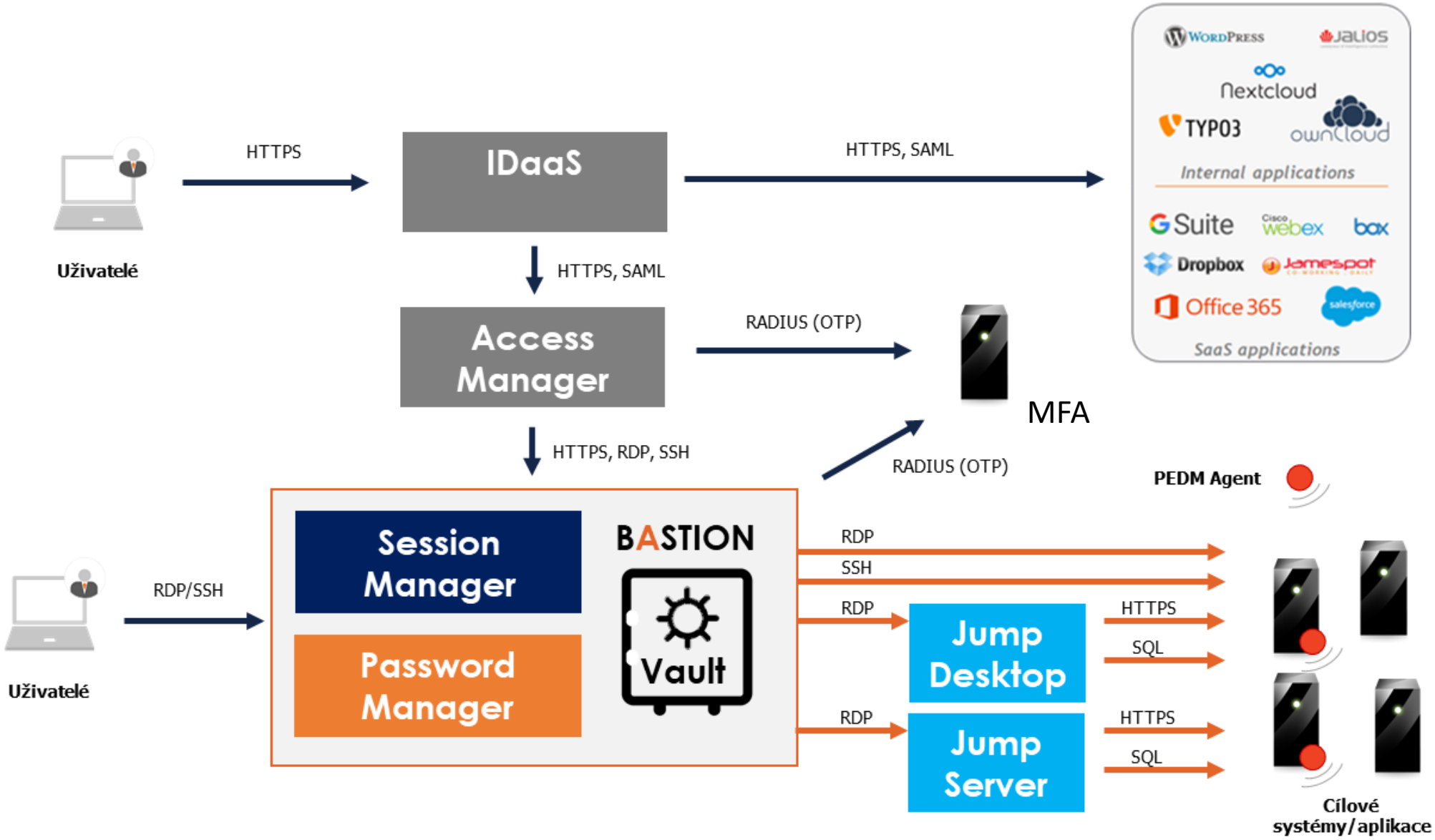
Cloudový identity & Access Management pro webové aplikace

- SSO vstupní brána pro zřízení přístupů
- Náhrada několika různých sad přihlašovacích údajů
- Možnost kontextového MFA

- Integrace s AD / AAD / LDAP / G-Suite
- Podpora SAML 2.0 / OAuth2 / OpenID Connect

- Široká škála předpřipravených integrací

Referenční architektura, nasazení



Škálovatelnost a flexibilita

- Od 10 do desítek tisíc cílů, All-in-one appliance či robustní clustery
- HW, Virtual, Cloud

Modularita

- Oddělené komponenty pro snadné nasazení a výhodné licencování

Jednoduchost

- Snadné nasazení a správa

COMGUARD
communication security

Děkuji za pozornost!

Lukáš Babčický | lukas.babcicky@comguard.cz