

Technická opatření pro plnění požadavků GDPR

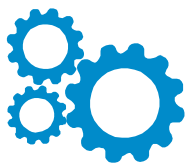
Bezpečnost v souladu s regulací EU

Ondřej Číž
ociz@vmware.com

vmware®

© 2015 VMware Inc. All rights reserved.

Průzkum - metodika



Metodika

CATI telefonické dotazování
průměrná délka cca 10 minut



Cílová skupina

Osoby, které mají ve firmě na starosti osobní data a jejich bezpečnost
Typicky IT, právní, HR oddělení
Firmy nad 100 zaměstnanců



Vzorek

151 za obě země dohromady
60 % ČR, 40 % Slovensko

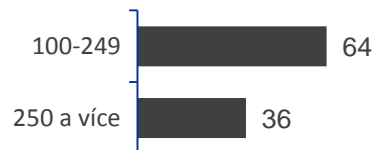


Sběr dat

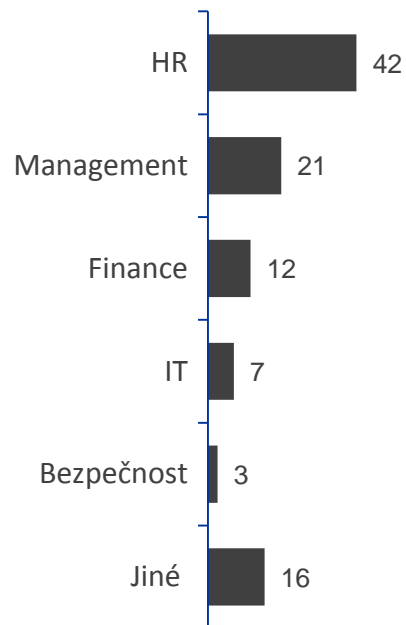
27.2. – 7.3.2017

Průzkum – Struktura vzorků

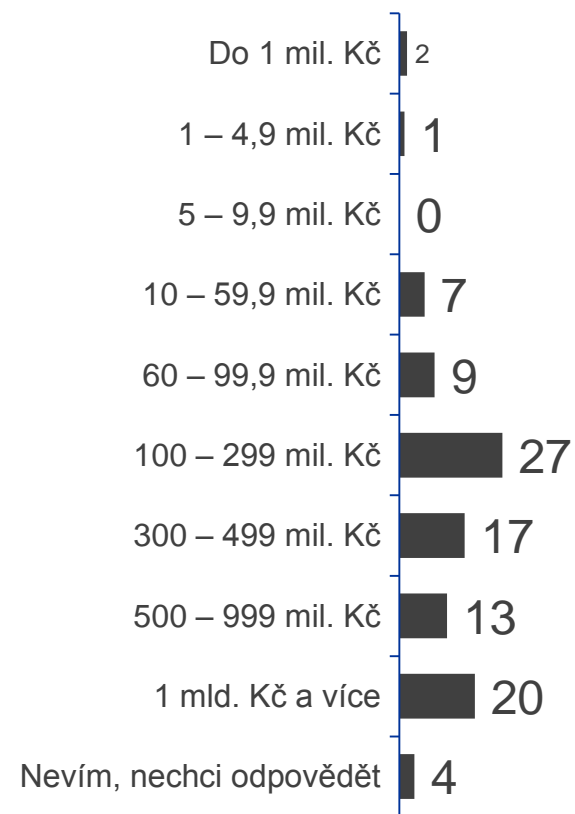
Počet
zaměstnanců



Oddělení
v rámci firmy

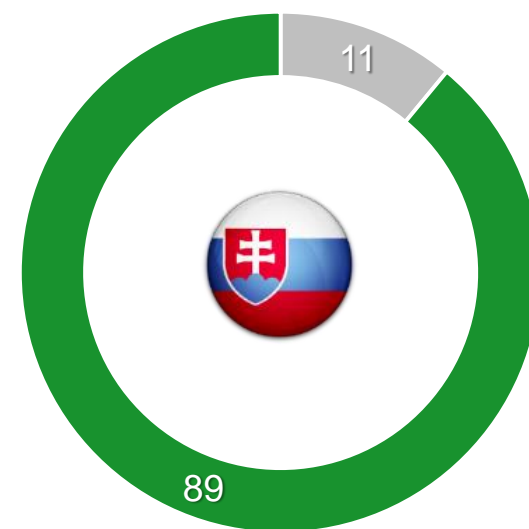
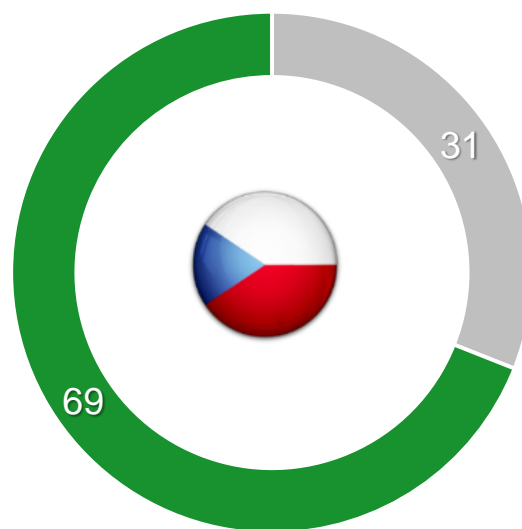
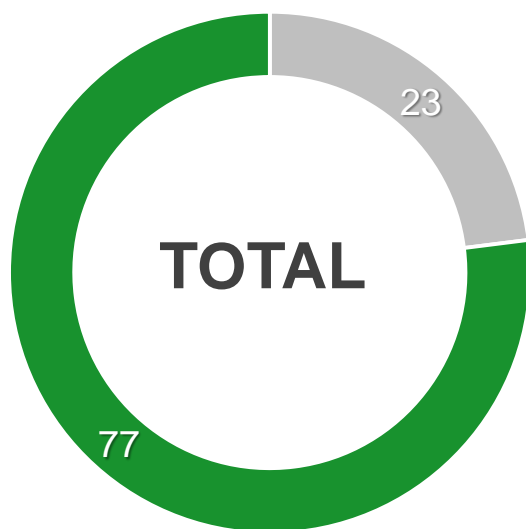


Obrat firmy



Průzkum – Jsou firmy obeznámeny s GDPR?

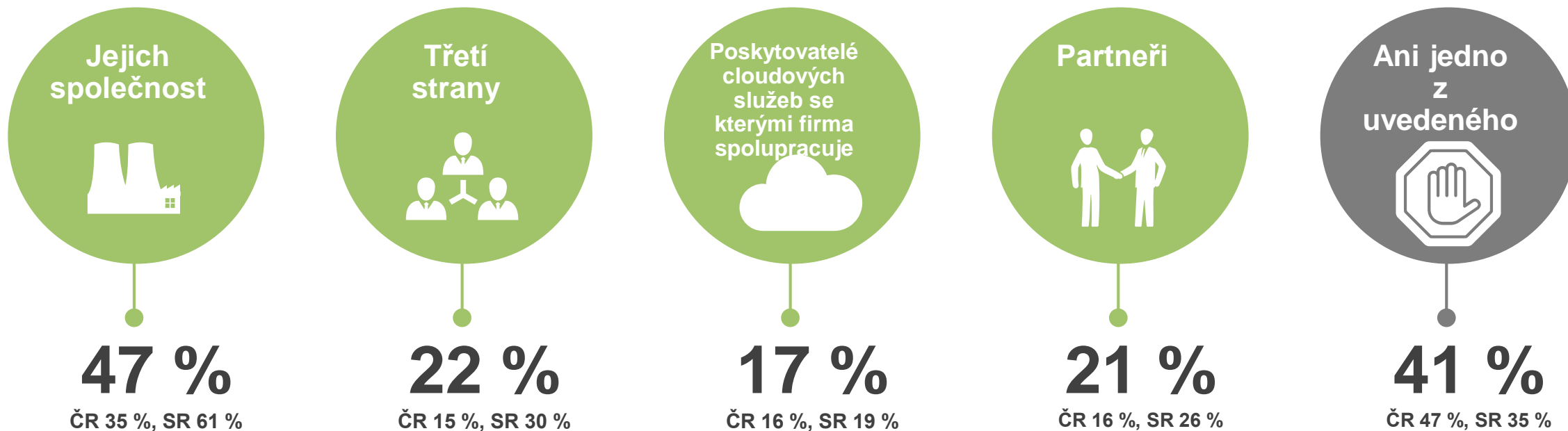
■ Ano ■ Ne



v %

Průzkum – Právo být zapomenut

Mají firmy adekvátní procesy a technologie, aby právo „být zapomenut“ mohli uplatnit:



VMware NSX adresuje následující GDPR oblasti

- Článek 18 – Pravo omezení procesů
- Článek 24 – Zodpovědnost regulátora
- Článek 25 – Ochrana dat návrhem řešení a vlastnostmi
- Článek 26 – Součinnost regulátora
- Článek 32 – Zabezpečení procesů
- Článek 35 – Ochrana dat a posouzení případných dopadů

VMware NSX adresuje následující GDPR oblasti

GDPR článek	VMware
Článek 18	NSX Distributed firewall, NSX Service composer, NSX Logical switches, NSX Guest introspection, NSX Network extensibility
Článek 24	NSX Application rule manager, NSX Endpoint monitoring, vRealize network insight, vRealize operations , vRealize log insight
Článek 25	NSX Endpoint monitoring, NSX Service composer, NSX Guest introspection, vSphere, vShield endpoint
Článek 26	NSX Distributed firewall, vRealize network insight
Článek 32	NSX Service composer, NSX Edge services gateway, vSphere, vCenter, Data protection, vSphere replication, vRealize network insight, Site recovery manager
Článek 35	NSX Application rule manager, vRealize network insight, vRealize log insight

Klasifikace dat v aplikacích

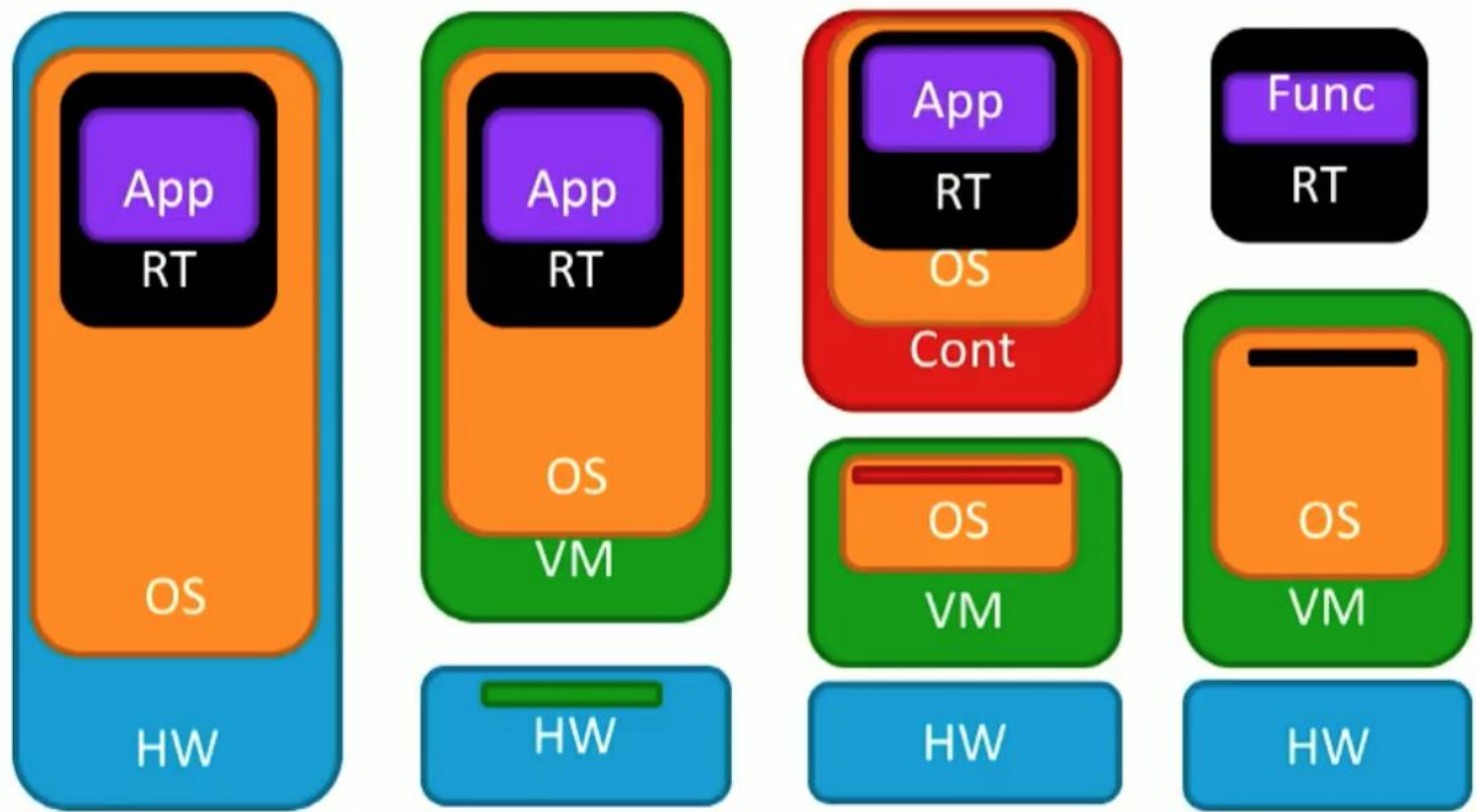
Adaptivní a inteligentní skupiny, integrace s DLP

Typy údajů

- Obecné
- Organizační
- Citlivé

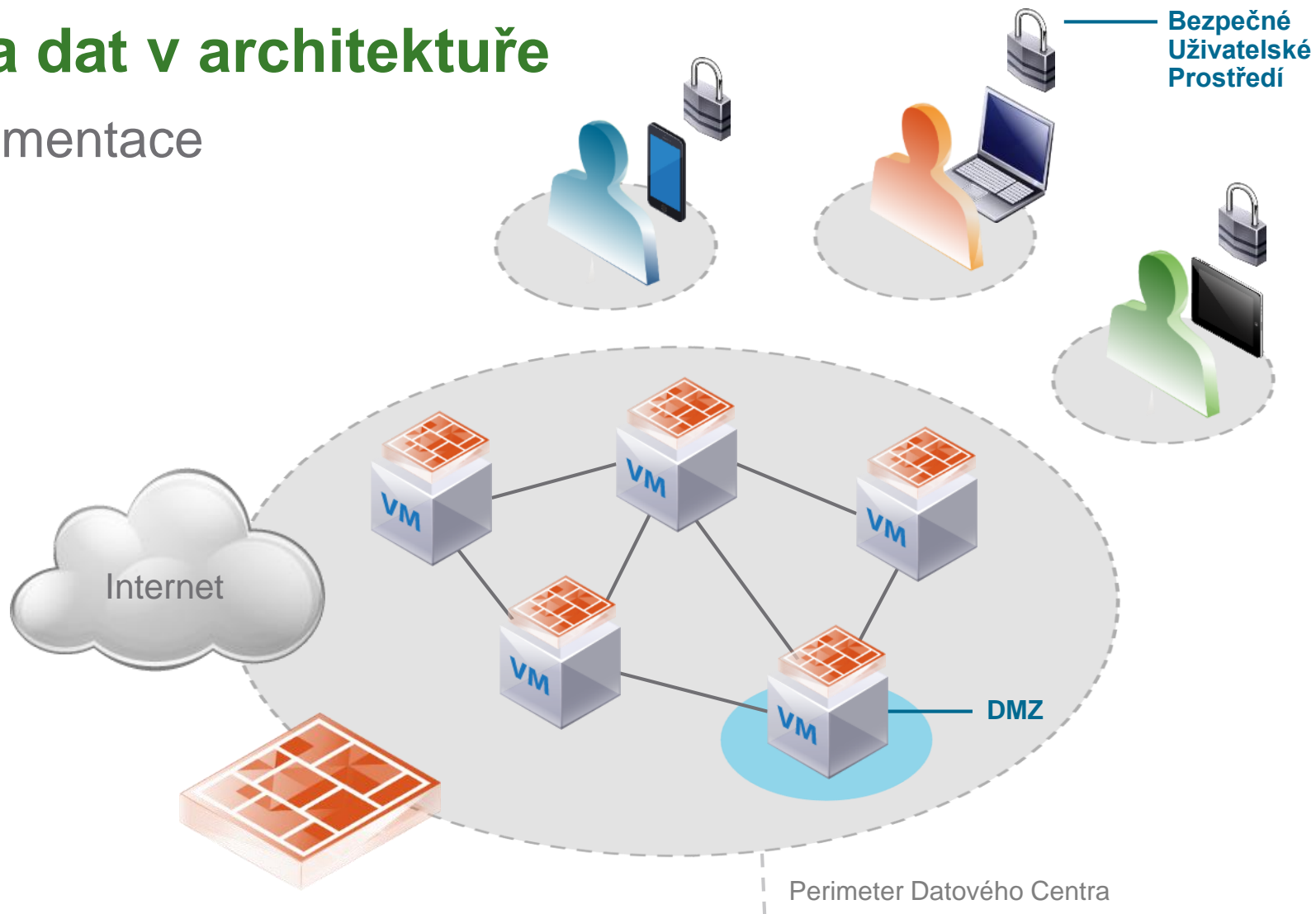
Typy aplikací

- App/HW Server
- App/VM Server
- Kontajner/VM
- Serverless



Ochrana dat v architektuře

Mikro-segmentace



Přidaná hodnota

Bezpečné prostředí uživatele, jednoznačná identifikace nezávislá na zařízení, ochrana nezávislá na typu aplikace.

Přehledná politika

Inteligentní skupiny

Potlačení laterálního pohybu

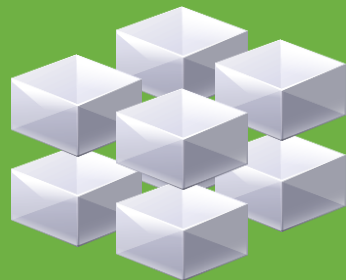
Intelligentní skupiny

Adaptivní, centrálně řízené skupiny

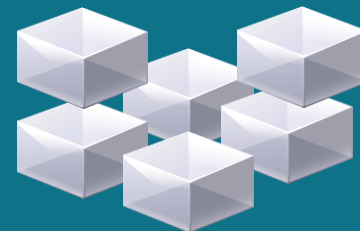
Operační Systém



Jméno Aplikace



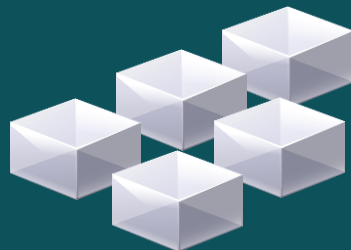
Služba



Aplikační Vrstva



Spĺnění regulace



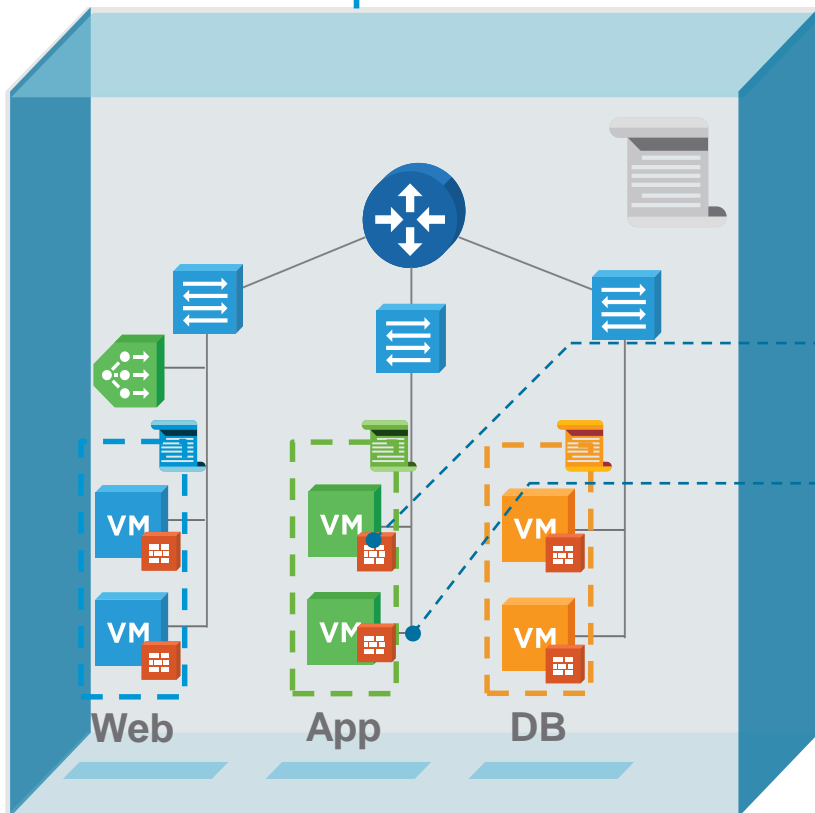
Bezpečnostní
Zóna Modrý



Dosažení souladu s regulací je proces

Vyžaduje flexibilní prostředí

Provozní prostředí

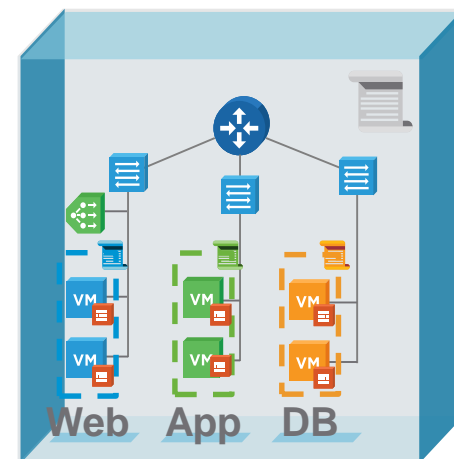


- Bezpečnost

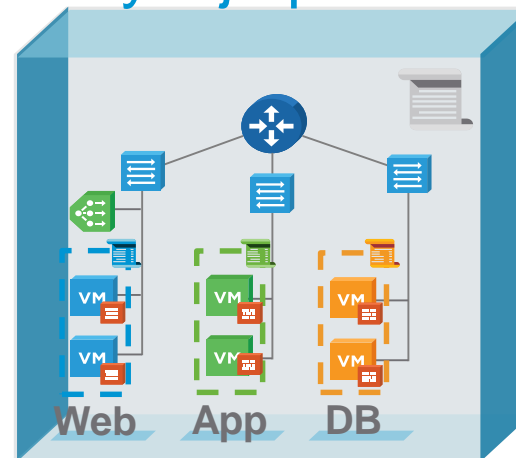
- Nezávislá síť



Penetrační test



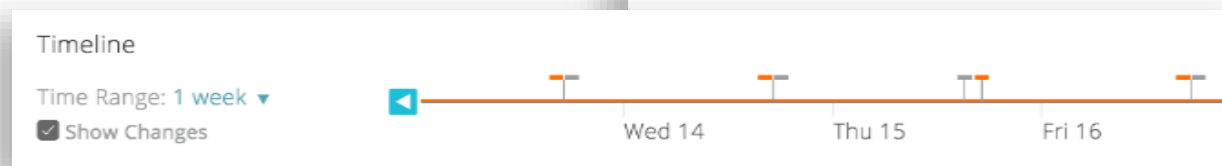
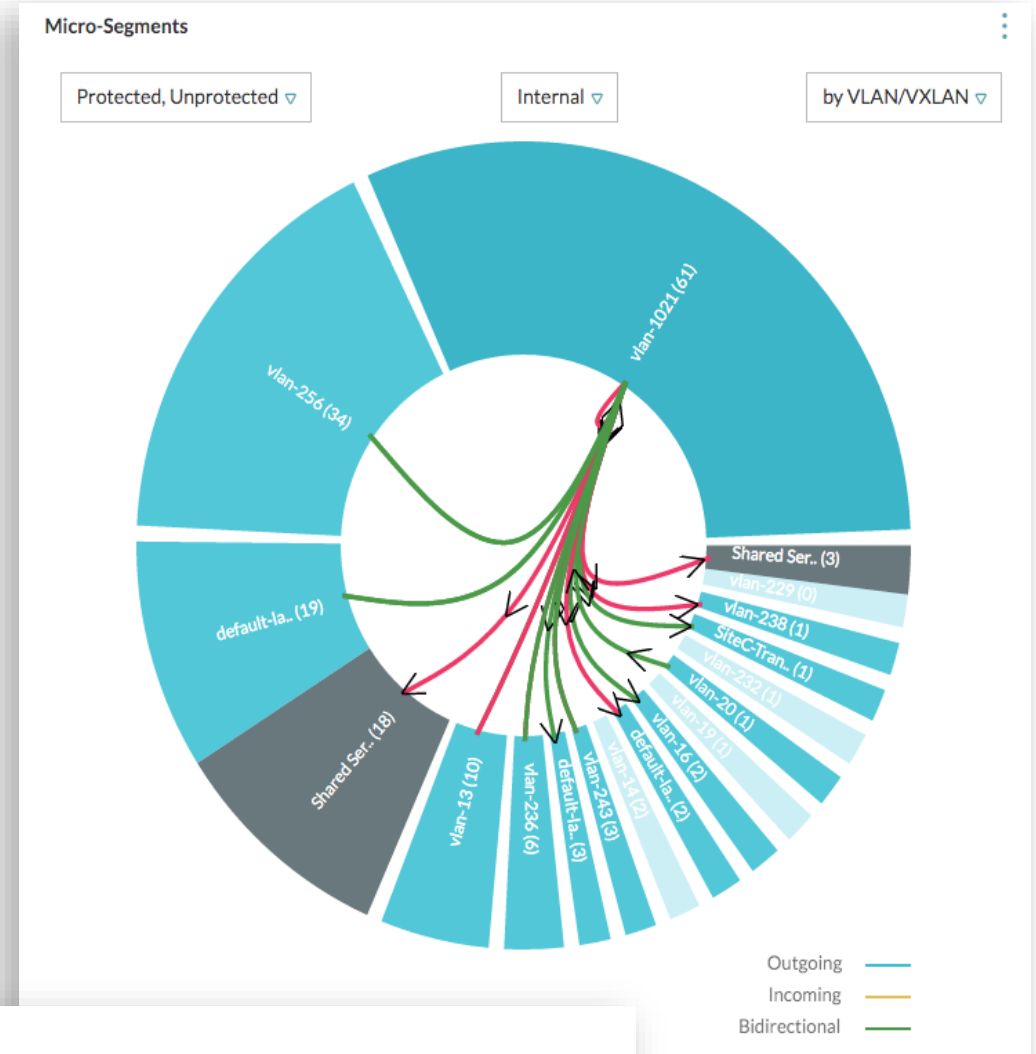
Vývoj aplikace



Monitoring v reálném čase

Data flow analýza, síťový obraz toků

- Real-time analýza datového toku
- Inteligentní skupiny, síťové objekty
- 360° přehled fyzické a virtuální komunikace
- Security analytika
- Snapshot stavu v čase incidentu
- Počáteční assesment

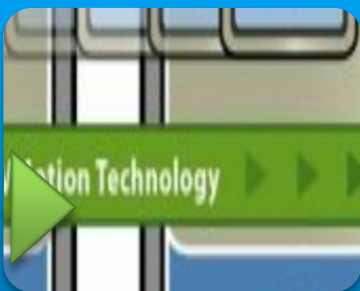


Šifrování dat v klidu a při přenosu



Šifrování dat v klidu

- Asymmetrický klíč je z KMS doručený na host
- Interní klíč (DEK) gereuje host, zašifruje jej klíčem z KMS (KEK)
- I/O operace jsou šifrované transparentně, VMDK a VM soubory
- nové VM, existující VM, existující zašifrované VM



vMotion šifrování dat v pohybu

- Podporuje 3 režimy – nikdy, oportunisticky, vždy
- 256b jednorázový náhodný klíč
- Ochrana proti relay útokům



Šifrování dat v pohybu

- Podpora standardních algoritmů AES-DES, FIPS/CC certified
- Technologie IPsec, L2VPN, L2VPN SSL
- Client SSL VPN

Závěr

- Identifikace osobních dat interním nebo externím DLP
- Segmentace jako základní nástroj prevence laterálního pohybu
- Šifrování citlivých dat v pohyby a klidu
- Monitoring pro forenzní analýzu

Děkuji !