Virtualios infrastruktūros sauga

Virtualių darbo vietų infrastruktūros (VDI) sauga

Virtuali darbo vieta

Virtuali darbo vieta - tai virtuali mašina, kuri pateikiama organizacijos darbuotojui.

Virtuali darbo vieta pasiekiama per klientinę programą, kuri pateikia darbo vietos vaizdą, leidžia naudotis periferiniais įrenginiais.

Pagrindiniai virtualių darbo vietų infrastruktūros tiekėjai:

Citrix, Microsoft, VMware.

Virtualių darbo vietų sprendimai: VDI, DaaS, Microsoft Remote Desktop Services (RDS).

Virtuali darbo vieta

Virtualių darbo vietų tipai

- Dedikuota darbo vieta (persistent desktop)
- Migruojanti darbo vieta (nonpersistent desktop).

Dedikuota darbo vieta – tai unikalus OS ir programų rinkinys skirtas konkrečiam vartotojui. Problema – tokio tipo VDI reikalauja daugiau saugyklos vietos.

Migruojanti darbo vieta sukuriama ir priskiriama vartotojui iš standartino *image* jungimosi metu ir grąžinama atgal į grupę (pool) vartotojui baigus darbą.

Kas yra VDI?

VDI (virtual desktop infrastructure) – tai virtualių darbo vietų technologija, kuri leidžia darbo vietas sukurti duomenų centre (on-premises) ir jas pateikti vartotojui, centralizuotai valdyti ir administruoti**.**

Privalumai:

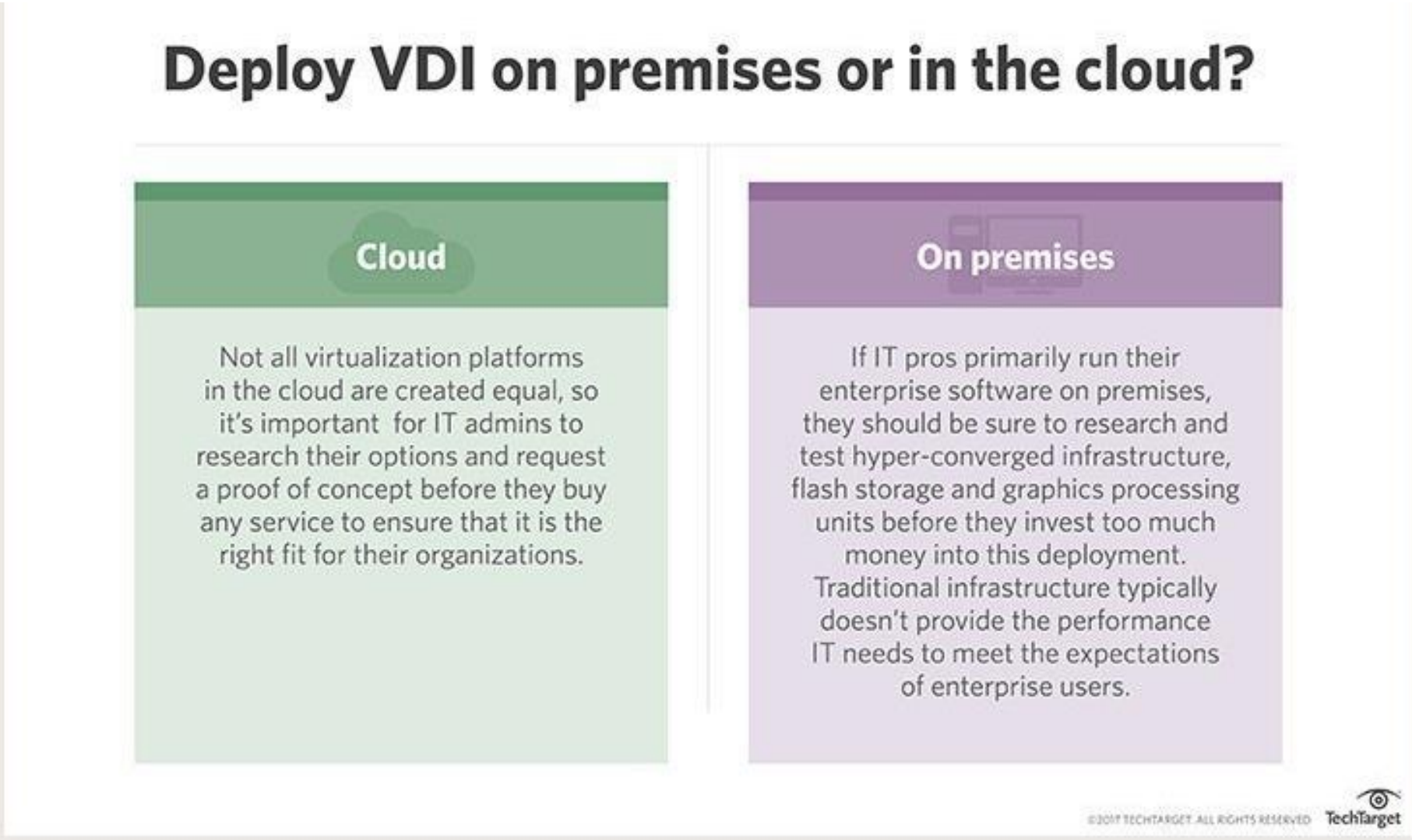
- Darbo vietų duomenų izoliavimas ir sauga
- Negendanti aparatūrinė dalis (virtuali)
- Dinamiškai plečiami, mažinami resursai
- Centralizuotas valdymas, administravimas
- Nuotolinis prisijungimas per daug protokolų (RDP, VNC, ssh)
- Greitas programų instaliavimas
- Storas, plonas klientas prisijungimui

VDI trūkumai

- Kainos, susijusios su VDI kūrimu, sunkiai kontroliuojamos ir dažnai viršija numatytus biudžetus.
- Virtualios darbo vietos prieiga ir darbo greitis priklauso nuo tinklo pralaidumo.
- Dirbant su grafinėmis programomis (graphic intensive), reikalaujančiomis grafinio procesoriaus GPU, dažnai būna problemų.
- Yra licenzijų, kurios pririšamos prie konkrečių HW ID, todėl nepavyksta naudoti migruojančių virtualių darbo vietų.

PCoIP *on the central source, compresses, encrypts and rapidly transports image pixels to PCoIP end-user devices. They in turn decrypt, decompress and display the image on a screen.*

VDI ar DaaS


Deploy VDI on premises or in the cloud?
Cloud
Not all virtualization platforms in the cloud are created equal, so it's important for IT admins to research their options and request a proof of concept before they buy any service to ensure that it is the right fit for their organizations.
On premises
If IT pros primarily run their enterprise software on premises, they should be sure to research and test hyper-converged infrastructure, flash storage and graphics processing units before they invest too much money into this deployment. Traditional infrastructure typically doesn't provide the performance IT needs to meet the expectations of enterprise users.
©2017 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

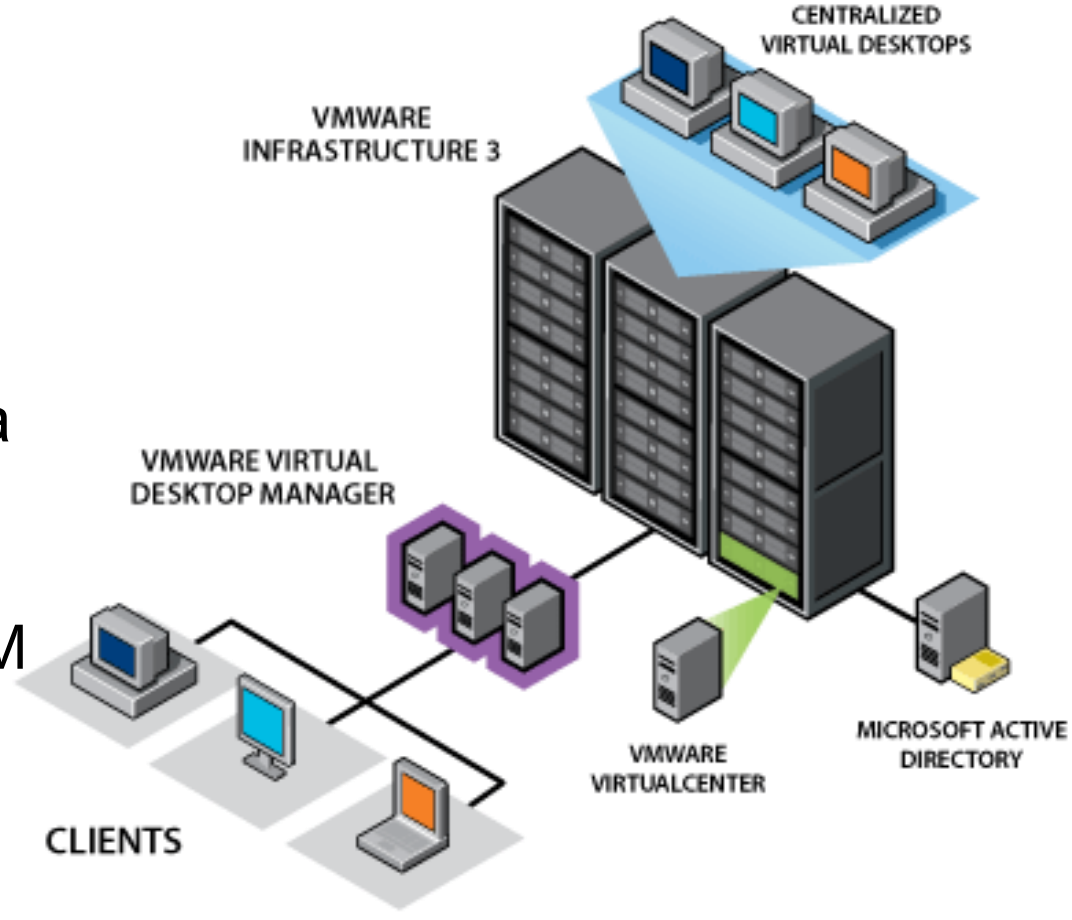
VDI komponentai

VDI sudaro:

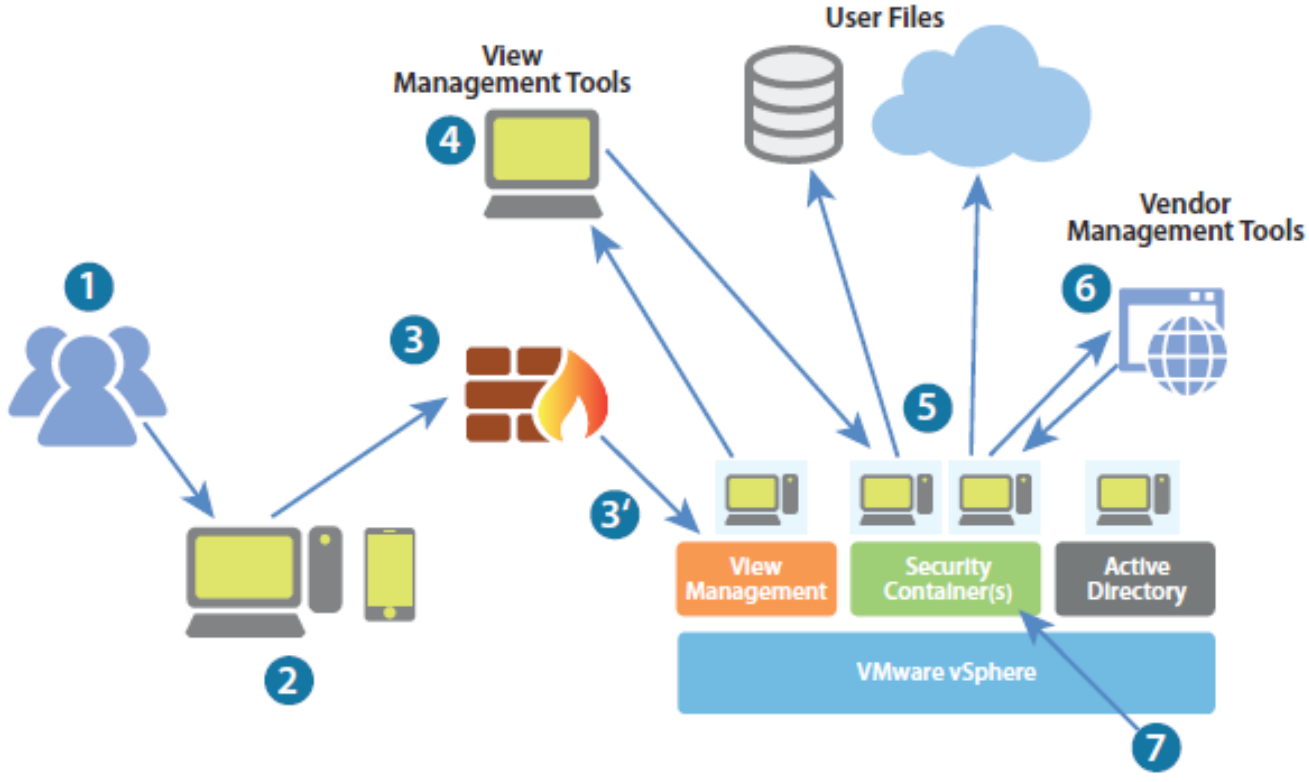
- Klientas
- Apsaugos serveris
- Sujungimų brokeris
- Virtuali darbo vieta
- Tapatybės valdymo sistema

Produktai:

- VMware Horizon View, VDM
- Microsoft VDI
- Citrix XenDesktop



Prisijungimų scenarijus



1-2 End User Authentication
3 - Untrusted to Trusted Connection
4 - Provisioning Desktop
5 - User Data
6 - Uninformed Management Tools

Sujungimų brokeris (VDM)

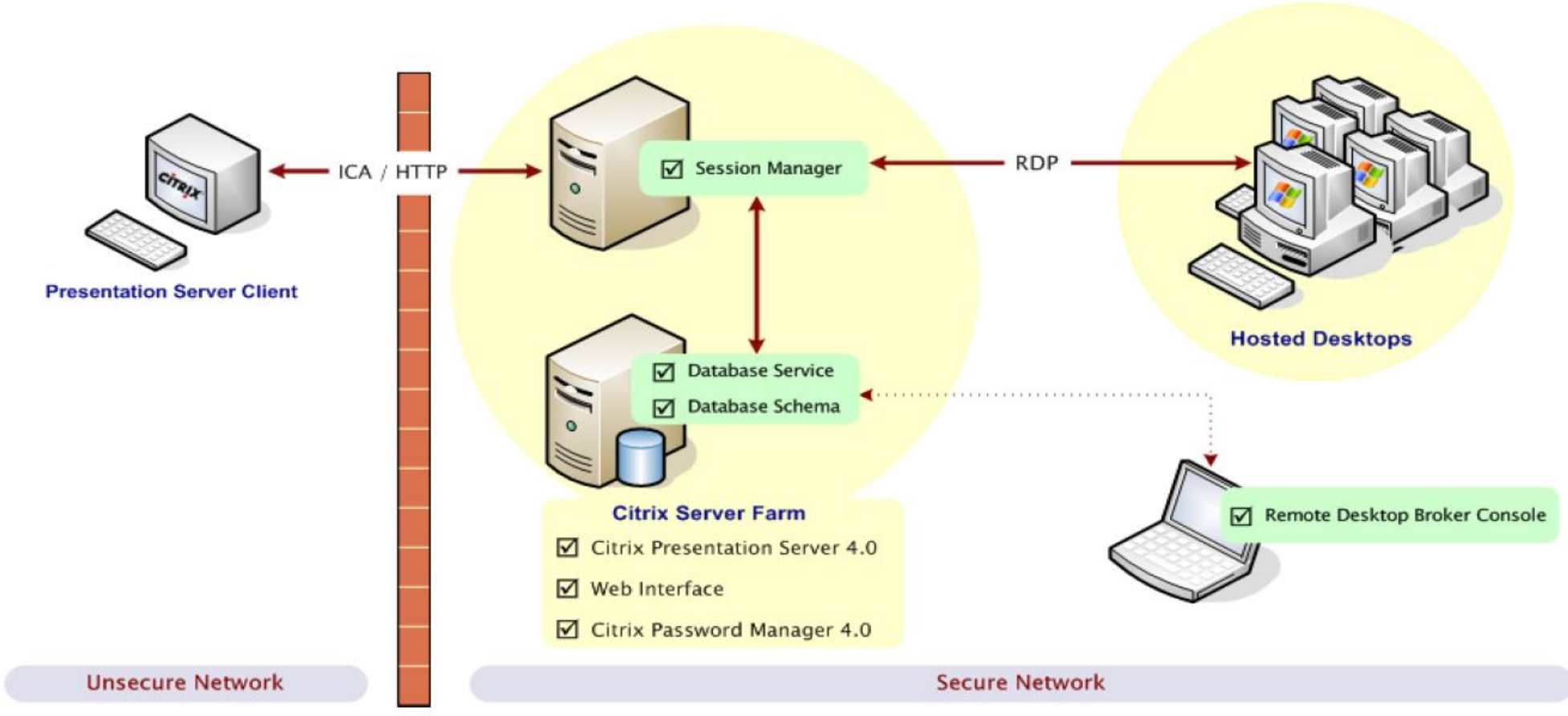
Sujungimų brokeris (connection broker) – tai serveris, kurio paskirtis priskirti vartotojui darbo vietą (VM), pagal atitinkamus nustatymus: pastovi, migruojanti.
VMware Horizon View – VMware VDM valdytojo pavadinimas.
Desktop broker – Citrix Presentation Server.

VDM komponentai:

- Serveris
- Klientas (fizinėje darbo vietoje)
- Agentas (virtualioje darbo vietoje)

Galima naudoti SSO, jei visoms virtualios darbo vietų mašinoms naudojamas MS AD.

Sujungimų brokeris



Grėsmės prisijungiant

Galimos saugumo grėsmės

- Vartotojo duomenų perėmimas
- Vartotojo sesijos perėmimas (hijacking)
- Nepasirašyto sertifikato naudojimas
- Nesaugūs įrenginiai darbo vietoje (flash, CD, DVD)

Sprendimai

- Dviejų lygių autentifikacija (smart card, eToken, biometriniai sensoriai, RSA ir t.t.)
- Pažeidžiamumų monitoringas, portų skenavimas, analizė
- Duomenų šifravimas ir ribojimas prie duomenų prieigos

VDI saugos aspektai

Tarp VDI kliento (host) ir VMware VDM relalizuojama SSL tunelį.

Tarp VDM ir ESX nenaudojamas SSL, todėl jungiantis per pvz. RDP, nenaudojamas joks šifravimas šioje atkarpoje.

VDI realizuota USB raktų palaikymas, kas sukelia grėsmes duomenų saugumui (pvz. neleistinos kopijos) ir KPK.

Didinant saugumą galima dviejų lygių autentifikacijos mechanizmą t.y. be AD (kas įprastai naudojama VDI), dar papildomai naudojat RSA Autentification Manager.

RDP ir PCoIP

VM grafinio vaizdo siuntimui, naudojami PCoIP (PC-over-IP) arba Microsoft RDP (Remote Desktop Protocol).

Vartotojui galima nustatyti, kurį protokolą jis naudos arba nustatyti leisti pasirinkti prisijungimo metu.

RDP palaiko:

- Teksto ir sisteminių objektų (failų, katalogų) *copy and paste* tarp lokalios sistemos ir View desktop.
- 32-bit spalvas
- 128-bit encryption.

PCoIP

PCoIP – tai *remote display protocol*.

PC over IP naudoja UDP ir perduoda suspaustą, šifruotą (AES 128-bit) vaizdą (bitmap) į nuotolinį klientą. Tolesnis perdavimas vyksta tik tuomet, kai pakeičiamas vaizdas ir perduodami tik pasikeitusios vaizdo vietos.

PCoIP gali dirbti su *sunkia* 3D grafika nedidinant kliento CPU apkrovos.

Tinklo apkrova mažinama iki 75% lyginant su RDP.

Klientui pakanka kompiuterio 800MHz su SSE2.

Pažeidžiamumai išskiriant VM

Galimos grėsmės

- VM apkrėstas virusais
- Trūksta OS programinės įrangos atnaujinimų

Sprendimai

- Sukurti saugią tinklo zoną, atskirą nuo valdymo tinklo
- Naudoti automatinius įrankius pvz. vCenter Configuration, kuris tikrina VM patch lygį
- Naudoti MS WSUS atnaujinimų valdymui
- Naudoti VM‘uose antivirusines programas

VM klonavimas

VM diegimas paprastai atliekamas naudojant VM šabloną t.y. klonuojant (naudojamas Desktop Composer).

Siekiant taupyti vietą klonuojant tikslinga naudoti surištus klonus (linked clones) t.y. saugoti tik atskirų VM pakeitimus, o ne visus pilnus VM.

Realizacijos ypatumai: turi būti atskirta OS ir vartotojo duomenys.

Saugos aspektai:

- Išgadintas tėvinis VM (base image)
- Apkrėstas tėvinis VM naudojant KPK
- Kas įvyks, jei tėvinio VM diskas bus defragmentuotas?

Pažeidžiamumai vart.duomenys

Galimos saugumo grėsmės

- Matomi duomenys
- Duomenų nutekėjimas
- Duomenys įrašomi į USB nešiojamą įrenginį
- Vienu metu paleidžiami darbai pagal tvarkaraštį (pvz. virusų skenavimas)

Sprendimai

- Duomenų šifravimas
- VM tinkamas konfigūravimas specialiais įrankiais – pvz. vCenter Configuration Manager

VC apsauga

VDI administratorius – tai tam tikra VI vartotojo rolė. Jis turi prieigą prie VC, tačiau jis neturi turėti VC administratoriaus teisių.

Rekomenduojama riboti VDI administratoriaus teises:

- Apibrėžti resursų rinkinį, kurį jis gali administruoti
- Apibrėžti veiksmus:
  - Įjungti/išjungti
  - Pridėti/išmesti diską
  - Modifikuoti nustatymus
  - Kurti VM iš šablono
  - Priskirti VM apibrėžtam resursų rinkiniui (pool)

Offline VM

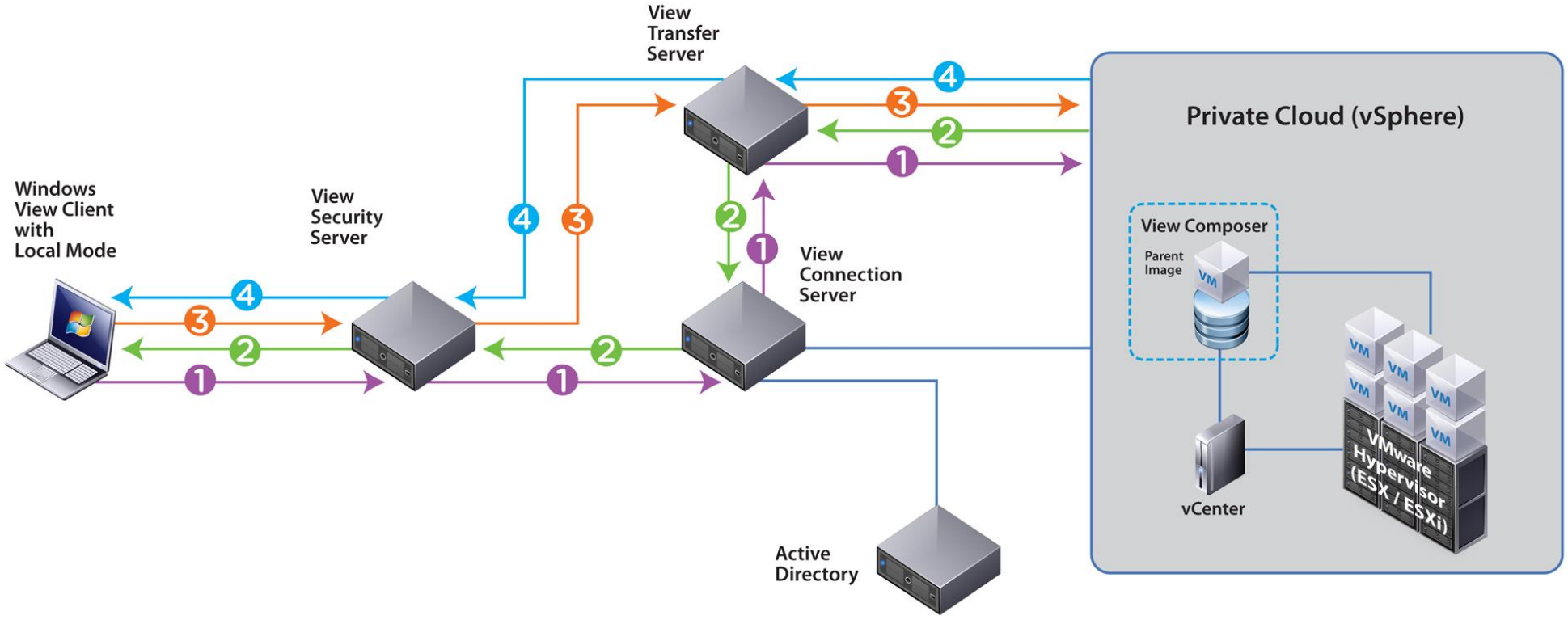
Norint suteikti galimybę VDI vartotojams dirbti vietose, kur nėra tinklo naudojama offline kliento technologija:

- VMware Ace (iki 2011 m.)
- Horizon View with Local mode

Veikimo principas:

1. Padaroma VM kopija lokaliame kompiuteryje.
2. Duomenys šifruojami ir nustatomi max naudojimo laikas offline rėžime (po to prieiga draudžiama).
3. Prisijungus prie tinklo įvyksta sinchronizacija ir *delta* duomenys ir nustatymai persiunčiami į VDI.

Horizon View with Local mode



Veiksmų sekos detalizuotos sekančioje skaidrėje

Horizon View with Local mode

Veiksmų sekų detalizavimas:

1. *View Client with Local Mode* prašo atjungti *offline desktop*. Tada *View Connection Server* prašo *View Transfer Server* užmontuoti saugyklą, kuri turi reikiamą virtualią mašiną.

2. vSphere siunčia saugyklos adresą į *View Transfer Server*, kuris persiunčia adresą *View Client with Local Mode*.

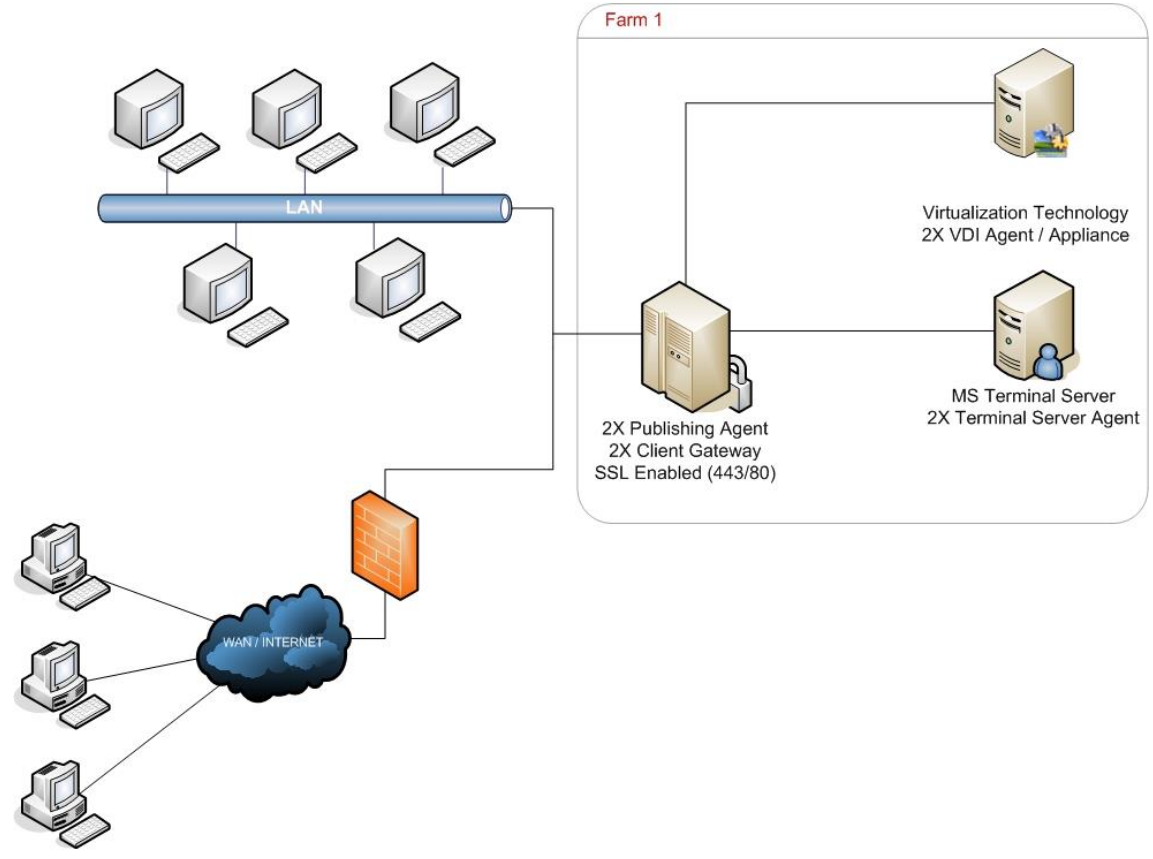
3. View Client with Local Mode pareikalauja *offline desktop* pagal gautą adresą.

4. Virtuali mašina siunčiama į *View Client* per *View Transfer Server.*

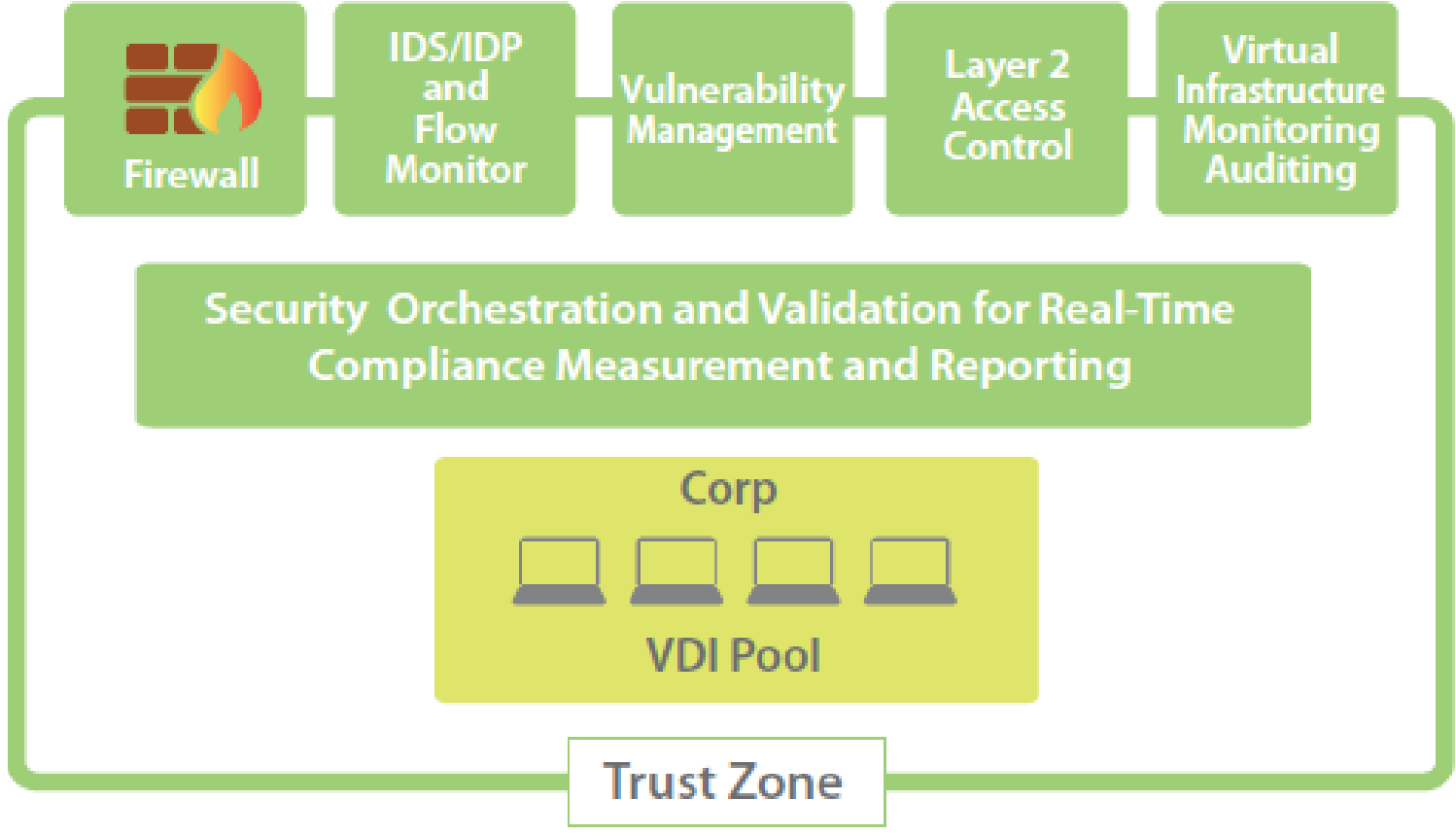
VDI tinklo sauga

VDI tinklo sauga:

- Ryšys tarp išorinių klientų ir VDM šifruotas (SSL)
- Prieigos ribojimams nustatyti patartina naudoti ugniasienes: DMZ ir vidiniame tinkle



VDI tinklo sauga trumpai



VDI sauga trumpai

- Tik autorizuotas prisijungimas prie skirtingų resursų grupių
- Tinklo segmentacija į atskiras saugumo zonas
- Tinklo ir resursų monitoringas
- Tinklo perimetro sauga
- Saugos politikos nustatymas zonoms
- Administravimo išlaidų mažinimas, naudojant automatinius įrankius