

Zálohovat umí ledaskdo,
ale zkoušeli jste někdy ze
zálohy obnovit systémy tak,
aby fungovaly?

Prianto Group



**Hungary,
Czech,
Slovakia,
Adriatics**
2017

Canada
Moncton
2019

USA
Miami
2021

Romania
2021

Poland
Krakow
2014

France
Paris
2017

Austria
Vienna
2019

Turkey
Istanbul
2021

- Založena v r. 2009
- Obrat v r. 2021 100+ M Euro
- Zaměstnanců v r. 2022: 150
- Website: www.prianto-group.com
- 100% distribuce
(bez přímého prodeje KZ)
- Headquarter v Mnichově
- Aktuálně 18 poboček v Evropě a Severní Americe

Na ISSS stánek č.2, 1. patro levé předsálí

Chce to změnu

Nová filozofie ochrany dat a aplikací před všemi možnými útoky (zvenku i zevnitř) říká, že vyrobit totálně „neprůstřelnou“ ochranu **reálně nelze**.

Přijměme to jako fakt – dříve či později bude potřeba celý systém či alespoň nějakou jeho část obnovit.

Správný plán obnovy navíc musí projít auditem.

Trocha statistiky

V roce 2020 čelilo 69 % organizací útoku ransomwarem.

Pouze 8 % z těch, které zaplatily výkupné, získalo všechna svá data zpět.

Průměrná doba odstávky v důsledku útoku ransomwaru je 21 dní.

Průměrné náklady na nápravu jednoho ransomwarového útoku činí 1,85 milionu dolarů.

V roce 2020 činily celkové náklady na škody z ransomware 20,8 miliard USD - jen pro americké zdravotnické organizace!

Active Directory jako základ bezpečného a funkčního IS

Bez ohledu na složitost IS nebo obor působnosti subjektu, se všechny nitky ICT potkávají v jednom „středobodu“ – tím je Active Directory. Tam se nastavují práva a přístupy jednotlivých uživatelů (osob i aplikací), tam se vytvářejí pravidla pro skupiny, v AD se rozhoduje, kdo je běžný uživatel i kdo má více pravomocí...

Bez dobře nastaveného AD mohou být investice do dalších nástrojů, nejen z oblasti bezpečnosti, jen penězi vyhozenými z okna.

Proč mají firmy IT (informační technologie, ne oddělení)?

Na základě získaných, přijatých a vyhodnocených informací činí uživatelé/firmy/společnosti rozhodnutí, která komunikují dalším článkům/členům interního či externího dodavatelsko-odběratelského řetězce, za účelem podporovat a rozvíjet primární aktivitu zaměstnávajícího subjektu.

Proč dávat do souvislosti AD a bezpečnost?

90%

Of companies use on-premises AD

10 Billion

On-prem AD authentications per day

95 Million

AD authentications are under attack daily

2.5 Million

Additional O365 users each month

47%

YoY revenue growth for Office 365

75%

Of enterprises with more than 500 employees sync on prem. AD to Azure AD

700 Million

Azure AD accounts

1.3 Billion

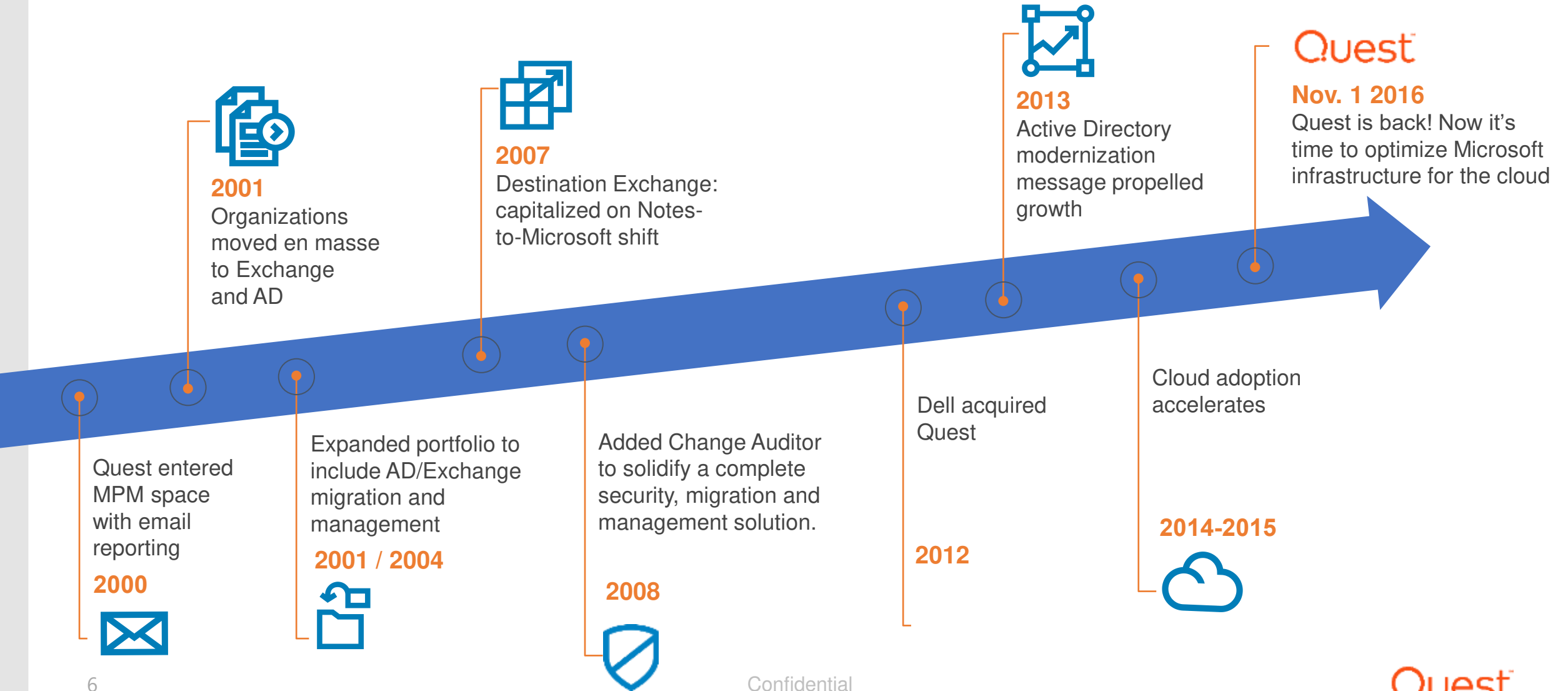
MS cloud login attempts per day

10 Million

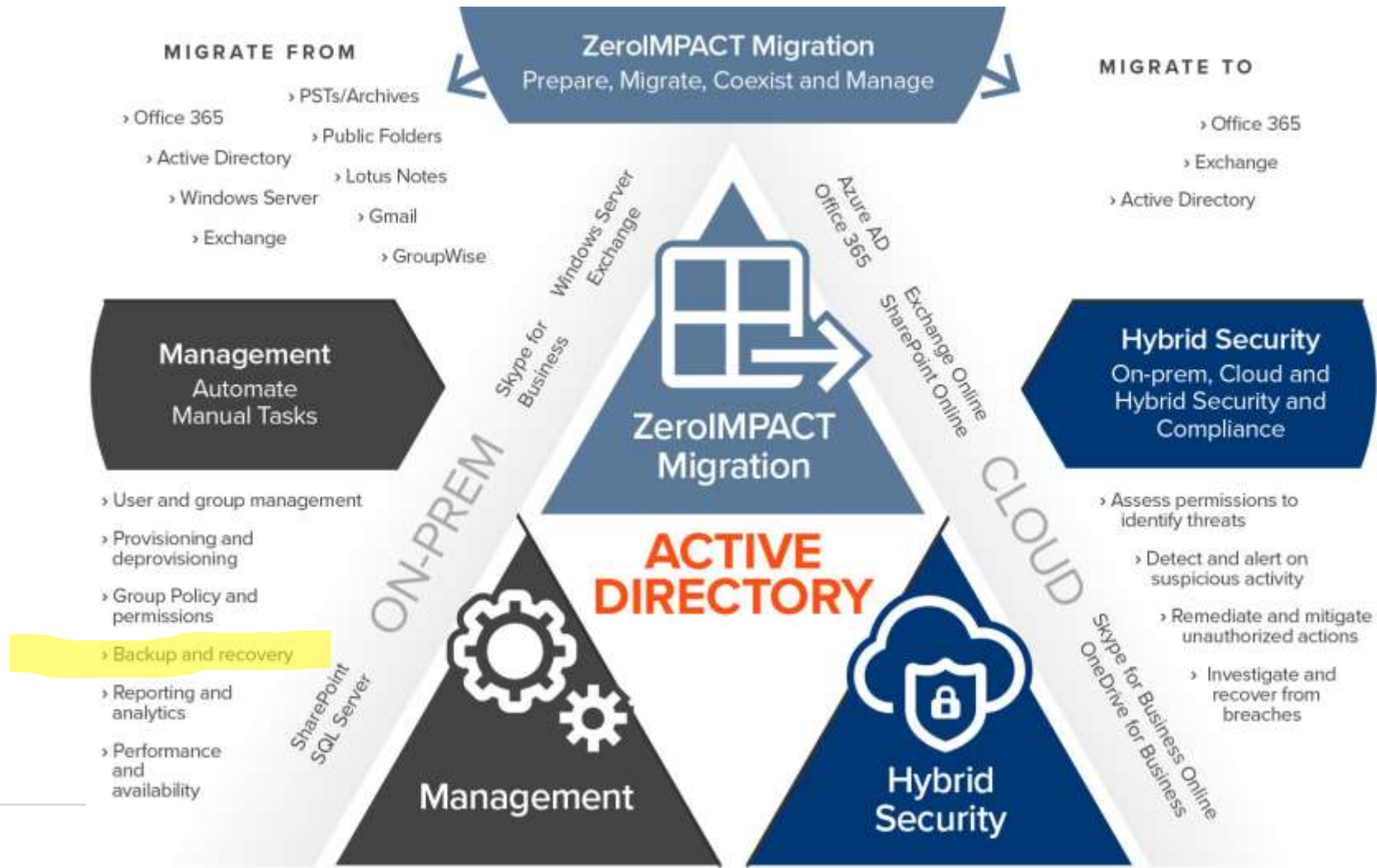
Daily MS Cloud logins are cyber-attacks



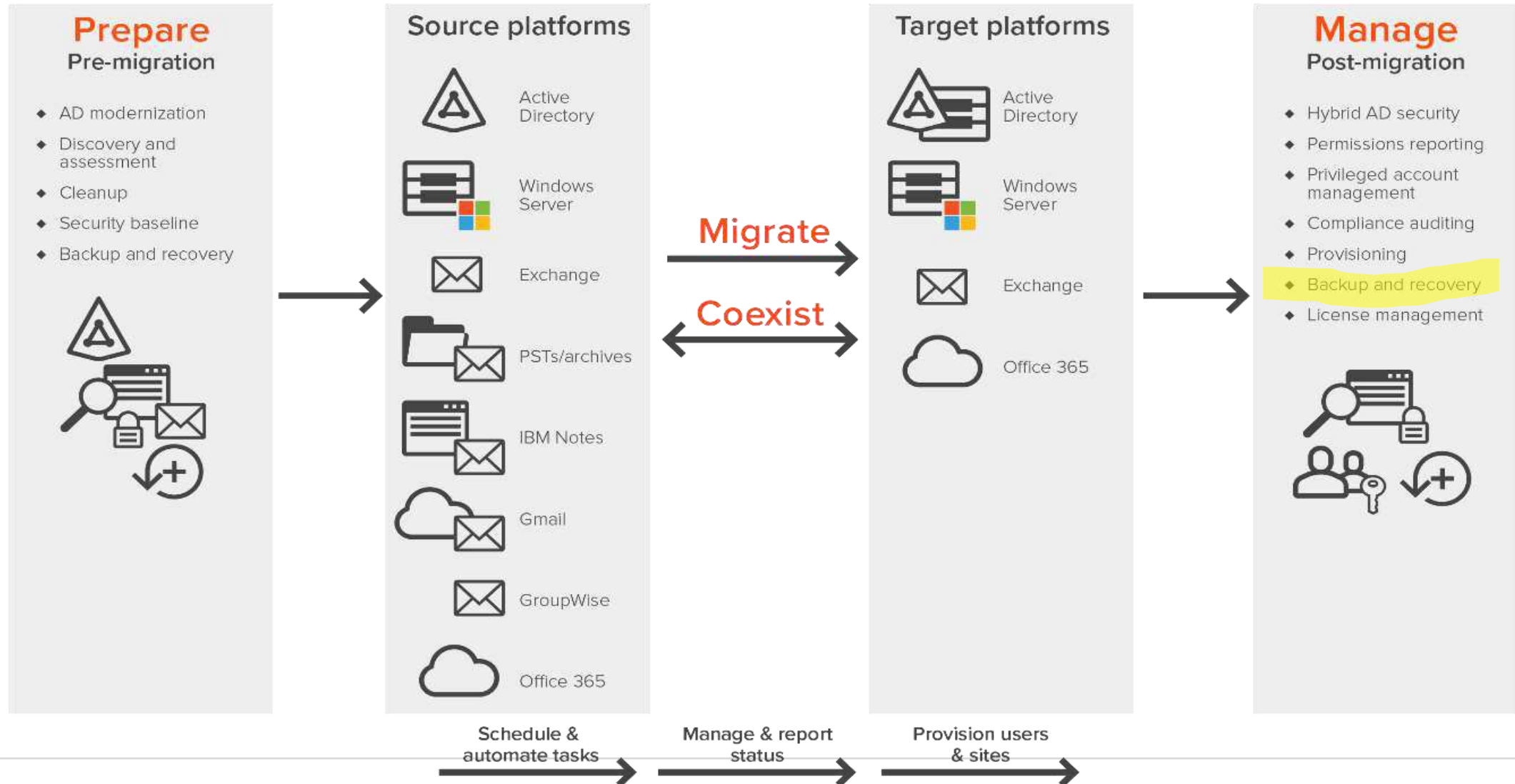
je jedním z TOP3 MS partnerů na světě – o Active Directory ví všechno...



Vše se „točí“ kolem Active Directory Úkoly: přesunout, zabezpečit, řídit a spravovat...



ZeroIMPACT migration solutions



Recovery Manager

Záloha a obnova Active Directory

- Rychle
- Efektivně
- Komplexně
- Již během implementace vzniká plán obnovy AD s konkrétními údaji.
- Testování a simulace obnovy po každé změně prostředí = plán obnovy vždy aktuální.
- Plán obnovy připravený pro audit.



Děkuji za pozornost

Tomáš Poslušný

Sales Manager

PRIANTO

Mobil: +420 605 232 939

e-mail: tomas.poslusny@prianto.com

Prianto CZ, V Olšínách 75, 100 00 Praha 10 - Strašnice

www.prianto.com

Na ISSS stánek č.2, 1. patro levé předsálí