Portfolio řešení a služeb

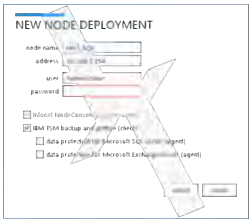
Flexibilní ochrana dat do každé firmy

TSMbox

Obchodně důležitá data, mnoho souborů s nabídkami, technickými detaily výrobků i kód aplikací. To vše jsou důležitá aktiva společnosti. Na těchto aktivech stojí Váš obchodní úspěch. A přesto ne každý a ne zcela věnuje pozornost ochraně dat, která jsou pro společnost důležitá a kritická.

Nabízíme kompletní a flexibilní řešení pro ochranu vašich dat. Jsme připraveni postavit řešení, které naplní očekávání od malých společností až po ty velké. Cílem je škálovatelné, spolehlivé, rozšiřitelné a cenově přijatelné řešení adekvátní vašim potřebám.

- flexibilní financování a cena řešení (CAPEX, OPEX, služba)
- jasné a predikovatelné náklady na vlastnictví (typicky 3 leté TCO)
- možnost vzdáleného dohledu řešení
- snadná rozšiřitelnost za předem daných podmínek
- žádné skryté náklady



Základem naší nabídky je tzv. „zálohovací appliance" - připravený TSMbox, který obsahuje potřebný hardware (server, diskové kapacity, případně páskovou mechaniku) a i veškerý software. Tento box vám přivezeme, zapojíme, provedeme základní nastavení a zaškolení a druhý den již můžete zálohovat svá důležitá data. Opravdovou lahůdkou pak jsou náklady na implementaci/ uvedení řešení do provozu, které jsou v řádu jednotek dnů a jsou v ceně zálohovacího zařízení

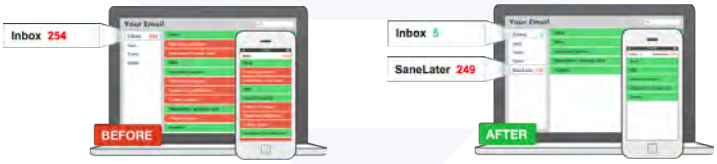
- zcela nové vlastní uživatelské rozhraní (GUI)
- automatizovaná vzdálená instalace a konfigurace klientů
- umožňuje zahájit obnovu během minut
- integrovaná deduplikace dat na straně serveru i klienta

Více informací také na www.tsmbox.cz

Příčetný a přehledný mailbox

SaneBox

Podle posledních studií průměrný zaměstnanec věnuje týdně 9 hodin (23%) čtením a odpovídáním na e-maily, místo toho aby se soustředil na práci. E-mailové přetížení je digitální epidemie. Podle interních statistik SaneBox z analýzy miliard e-mailových zpráv si méně než polovina e-mailů zaslouží okamžitou pozornost.



SaneBox determinuje a neustále se sám učí označovat důležité e-maily na základě Vašich akcí s e-maily (odesílatel, přečtení / nepřečtení, doba od příchodu zprávy do přečtení / smazání / přesunutí, apod.) Vliv má i propojení se sociálními sítěmi a dlouhodobé statistiky. Poté SaneBox přesune nedůležité e-maily z hlavního adresáře doručené pošty do jiný pro tyto účely vytvořených adresářů (SaneLater, SaneNews, atd). Sami systém učíte pouhým přetažením e-mail zprávy v případě jejího chybného zařazení. O veškerých přesunech a zpracování se dozvíte z jednoduché a přehledné zprávy zaslané každý den.

- propracovaný systém notifikací (pokud adresát neodpověděl)
- účinný antispamový systém
- integrace se službou Dropbox, Box a IBM SmartCloud Storage
- chytré dashboardy při celofiremním nasazení

Obrovskou výhodou cloudové služby a přístupu pomocí protokolu IMAP je, že čistý a příčetný mailbox máte k dispozici na libovolném zařízení. Při přístupu např. z chytrého telefonu už se nemusíte na relativně malém displeji probírat desítkami nedůležitých zpráv, ale ve svém inboxu máte pouze to podstatné!

Portfolio řešení a služeb

Správa mobilních zařízení

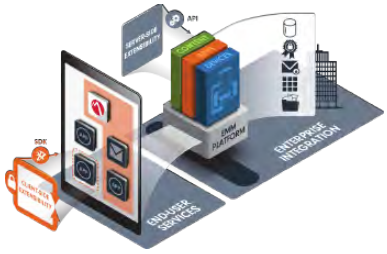
MobileIron

MAKING MOBILE FIRST

Řady IT manažerů již připouštějí, že nová mobilní zařízení v podnicích přestávají mít pod kontrolu a značně nabourávají zažitou firemní IT rutinu. Uživatelé chtějí pracovat s vlastními zařízeními, která chtějí připojit k podnikovým sítím. Je narušena dosavadní podniková homogenita a strategie jednotné mobilní platformy. Ve smartphonech se pospolu ocitají podniková i soukromá data včetně nekontrolovaných a neschválených aplikací, které zejména v případě sociálních sítí mohou šířit informace na všechny světové strany bez omezení. Nekontrolovaný nárůst chytrých zařízení představuje významné bezpečnostní riziko. Koncept BYOD (Bring Your Own Device - Přineste si své zařízení) řeší právě tuto problematiku používání soukromých chytrých zařízení.

Vyjímečná platforma MobileIron velmi efektivně řeší BYOD zabezpečení a správu aplikací, dokumentů a mobilních zařízeních.

- uživatel si může vybrat libovolné zařízení a OS
- definice konfigurace zařízení a zabezpečení
- vysoce zabezpečené oddělení prostoru podnikových dat od soukromých
- bezpečný přístup k firemním službám (intranet, CMS, ...)
- zabezpečený podnikový e-mail
- ... a to vše při zachování komfortu prostředí a veškerých soukromých aplikací



MobileIron dokáže velmi jednoduše rozšířit aplikace na straně klienta (smartphone), nebo na straně serveru. Díky tomu je možné řešení MobileIron integrovat do mnoha dalších řešení aplikací.

- real-time vynucení nastavení politik na zařízení
- jednotné přihlášení neobtěžující uživatele
- šifrování a možnost vzdáleného výmazu podnikového prostoru
- zcela jednoduché a flexibilní způsob licencování

Pokročilé podnikové Wi-Fi

aruba NETWORKS

Provozování Wi-Fi připojení je dnes zcela běžné a je všude. S nástupem obrovského množství chytrých mobilních zařízení došlo k další změně architektury podnikové infrastruktury. Již nestačí na pár místech umístit několik základních přístupových bodů. Potřebujete mít bezpečné, výkonné a funkční a centrálně řízené řešení. Přesně to nabízí technologie ARUBA - nenáročná síť pro náročné zákazníky. Mezi hlavní vlastnosti patří

- vysoký důraz na kvalitu zpracování (doživotní záruka)
- neznatelné náklady na správu sítě
- špičkový fast-roaming
- unikátní funkce Adaptive Radio Management a ClientMatch

Multifunkční vnitřní přístupové body jsou cenově dostupné AP s podporou 802.11 a,b,g,n a samozřejmě i ac. Jsou navržené pro nasazení v prostorách s vysokou hustotou připojovaných zařízení (kanceláře, nemocnice, školy, OC apod.) Ve spolupráci s centralizovanými mobilními Aruba kontrolery (popř. v Instant řešení) poskytují přístupové body zabezpečené, vysokorychlostní síťové služby, které uživatelům vytvoří model síťového přístupu typu „bezdrátově - kde je to možné, kabel – kde je to nutné“.

Klíčem k zajištění výkonu a spolehlivosti srovnatelným s kabelovým připojením jsou unikátní funkce společnosti Aruba - Adaptive Radio Management (ARM), ClientMatch™ a spektrální analýza. Tyto funkce spravují 2,4GHz a 5GHz rádiová pásma tak, aby byl zajištěn maximální poskytovaný výkon klientům při současném omezení případného rádiového rušení.

- automatická detekce útoku na síť a zařízení
- automatická detekce Rogue AP (vlastní AP zaměstnanců)
- spektrální analyzátor v každém AP
- Air Time Fairness - řízení přístupu a šířky pásma