VARONIS

BÍLÁ KNIHA

7 osvědčených způsobů ochrany dat nejenom v Office 365

Jak získat jednotný přehled o nestrukturovaných datech uložených lokálně i v cloudu a kontrolu nad nimi.

Obsah

Zabezpečení dat v komplexním hybridním světě 3

Vzestup „temných“ dat 4

Zabezpečení dat není dobrovolné 5

Jen cloudová bezpečnost nestačí 6

Posílení cloudové bezpečnosti s produkty Varonis 9

1. Jednotná kontrola nad lokálními daty a daty v Office 365 10

2. Plná viditelnost oprávnění a jejich správa 11

3. Rozpoznávání citlivých údajů 12

4. Komplexní audity a monitoring 13

5. Pokročilá detekce hrozeb (UEBA) 14

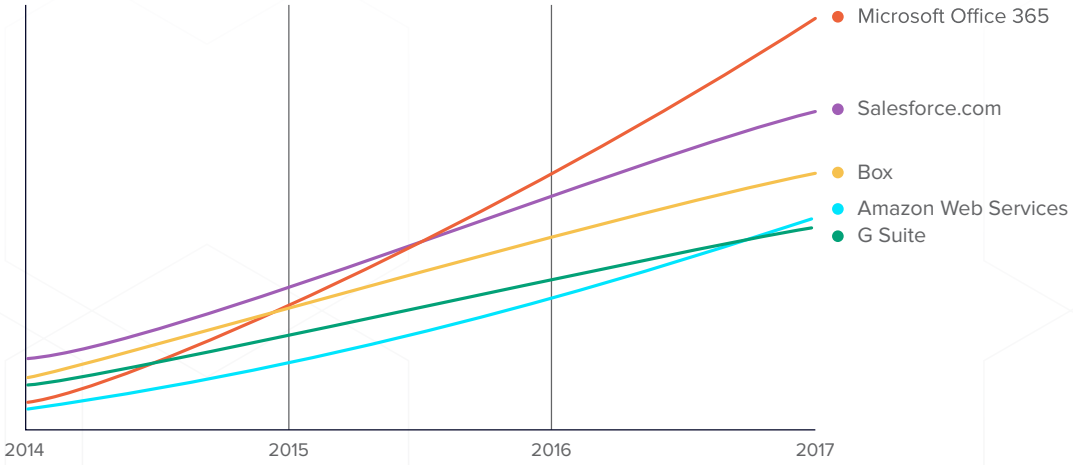
6. Odstraňování rizik a automatizace na principu nejmenších možných oprávnění 15

7. Řízení přístupu na bázi vlastnictví dat 16

Nechte si vypracovat vlastní posudek rizik v Office 365 17

Zabezpečení dat v komplexním hybridním světě

Jsme svědky globálního posunu od čistě lokální infrastruktury IT k hybridním prostředím. Mnohé podniky přesouvají části své infrastruktury pro e-maily a sdílení souborů do cloudu, kde je jasnou jedničkou na trhu systém Microsoft Office 365.



▲ Source: Okta Businesses @ Work, January 2017

Používání Office 365 spolu s podnikovými datovými sklady způsobuje pro zabezpečení a řízení dat obtíže, které je v éře obrovských úniků dat a přísné ochrany soukromí nutno řešit.

Lídři v oboru zabezpečení a omezování rizika by měli pro všechny své lokální i cloudové datové sklady zavádět konzistentní a udržitelné způsoby řízení datové bezpečnosti a využívat osvědčené postupy.

V tomto dokumentu se zabýváme následujícími tématy:

- Vzestup „temných“ dat
- Proč jen cloudová bezpečnost nestačí
- Posílení zabezpečení Office 365 s produkty Varonis 365

Vzestup „temných“ dat

Odhaduje se, že za posledních 25 let utratily společnosti miliardy, možná dokonce biliony za přesun téměř všech analogových informací do digitální podoby. Citlivá data nyní najdete v soukromých datových centrech, veřejných cloudech i v poštovních schránkách. Mnohé podniky podcenily s tím související rizika. Soustředily se na zvyšování produktivity, aniž by se zajímaly o zabezpečení dat před hackery, zlovolnými zaměstnanci nebo třeba nepřátelskými státy.

Množství dat raketově rostlo a informační bezpečnost zaostávala. V téměř každém datovém skladu lze najít široce dostupné a přitom kriticky důležité informace. Škody, které tím nepřímo vznikly, se projevily prostřednictvím katastrofických úniků dat ve společnostech Sony, Equifas, federálním úřadu pro personalistiku USA (Office of Personnel Management, OPM) a v Demokratickém národním výboru (DNC).

A rozvoj hybridních cloudových prostředí riziko bezpečnostních incidentů ještě posílil. Jak uvádí společnost Gartner:

> Sklady nestrukturovaných dat v organizacích trpí chronicky nedostatečným managementem a přílišnou přístupností. Vzhledem k postupnému zavádění cloudových úložišť a platforem pro spolupráci v posledních letech je řešení této situace ještě složitější.[1]

Něco se muselo změnit.

[1] Gartner: „Získejte znovu kontrolu nad přístupem ke svým úložištím nestrukturovaných dat v cloudu i lokálně“ (Regain Control of Access to Your Unstructured Data Repositories On-Premises and in the Cloud), Marc-Antoine Meunier, David Anthony Mahdi, 12. dubna 2017

Zabezpečení dat není dobrovolné

Aby se nestaly další obětí, začínají organizace na situaci reagovat a snaží se osvětlit svá „temná data“. Pravidelně posuzují riziko spojené s daty, požadují od dodavatelů systémů Saas/IaaS komplexnější bezpečnostní funkce a mezery vyplňují řešeními od jiných dodavatelů.
Mnoho z těchto nezávislých řešení je však přinejlepším jen částečnou odpovědí a jejich nasazení může zbytečně zvětšit složitost, což má negativní vliv na bezpečnost.

Vzhledem k pohybům dat mezi lokálními úložišti a cloudy, jako je Office 365, je v oblasti IT nutno umět odpovědět na základní otázky bezpečnosti dat týkající se jejich zabezpečení a vhodného využití.

[2] Glosář Gartner, https://www.gartner.com/it-glossary/dark-data

Jen cloudová bezpečnost nestačí

Existují bezpečnostní řešení zaměřená na cloud, která se na některé z těchto otázek snaží odpovědět a vyřešit některé ze souvisejících bezpečnostních problémů.

Oblíbenou kategorií cloudových produktů je například zabezpečené zprostředkování přístupu do cloudu (CASB), které pomáhá potlačit neoprávněné využívání cloudových služeb (stínové IT), blokovat přístup k nepovoleným cloudovým aplikacím a zamezit externímu sdílení dat, u nichž není sdílení povoleno. Obvykle pracují mezi uživateli a cloudovými službami a fungují jako přesměrování a/nebo reverzní proxy server.

Ačkoli jde o užitečné funkce, jsou čistě cloudová řešení slepá vůči lokální infrastruktuře, převážně slepá vůči hybridním infrastrukturám a postrádají pokročilé bezpečnostní funkce, na které si podniky zvykly u špičkových produktů pro audit a ochranu dat.

Hlavní problémy CASB popsala společnost Gartner ve zprávě „Produkty CASB nesmí tvořit ostrovy datové bezpečnosti“ (CASBs Must Not Be Data Security Islands) (duben 2017):

- Mnohé produkty CASB jsou schopny provádět kontrolu DLP, kontrolu obsahu však ještě neprovádějí tak důkladně jako komplexní podniková řešení DLP a DCAP.
- Funkce DLP a SCAP v produktech CASB mají v současnosti omezenou flexibilitu z hlediska cloudových aplikací, uniformity zásad a propojení s jinými produkty pro zabezpečení dat.
- Omezené propojení s jinými podnikovými produkty DCAP může vést k nedůslednému a nespolehlivému uplatňování zásad a nejednotným přehledům.

Produkty CASB mají pro podnikovou strategii zabezpečení dat svoji hodnotu, samy o sobě však nezajišťují takové pokrytí, aby mohly sloužit jako primární řešení zabezpečení dat pro Office 365. A samozřejmě nabízejí pouze částečné pokrytí v hybridních prostředích.

Někteří dodavatelé cloudových aplikací začali jako alternativu nebo doplněk k produktům CASB nabízet vlastní bezpečnostní funkce. Například Microsoft má v systému Office 365 nativní bezpečnostní funkce. Analytici i bezpečnostní odborníci se však shodují, že aby bylo dosaženo maximálního přehledu a ochrany, je vhodné doplnit nativní funkce produktů Microsoft o produkty třetí strany.

Není překvapivé, že to platí zejména pro hybridní prostředí.

> Lídři na poli bezpečnosti IT by měly pochopit, že aby byly nové funkce pro zabezpečení dat plně využity, měly by být používány jako součást důkladně definované strategie řízení datové bezpečnosti, která pokrývá cloudová i lokálně uložená data.

Zpráva společnosti Gartner: Produkty CASB nesmí tvořit ostrovy datové bezpečnosti, duben 2017

Posílení cloudové bezpečnosti s produkty Varonis

Izolované bezpečnostní nástroje, které vyplňují malé mezery, mohou být nákladné a jejich použití zkomplikuje infrastrukturu a zvětší riziko. Společnost Varonis nahrazuje tradičně nesourodé bezpečnostní nástroje jediným řešením, které bezpečnostním týmům umožňuje centrálně organizovat řízení datové bezpečnosti a jednotně uplatňovat zásady v celé řadě různých datových skladů, lokálně i v cloudu.

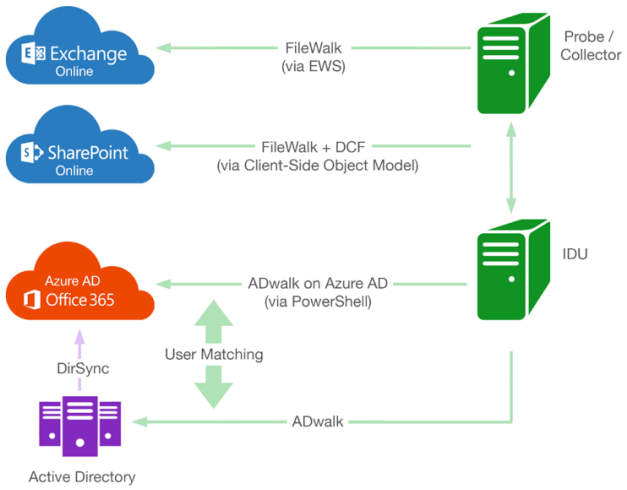
Níže uvádíme sedm jedinečných vlastností, které podtrhují, jak platforma Varonis Data Security posiluje vestavěné bezpečnostní funkce Office 365.

1. Jednotná kontrola nad lokálními daty a daty v Office 365
2. Plná viditelnost oprávnění a jejich správa
3. Rozpoznávání citlivých údajů
4. Komplexní audity a monitoring
5. Pokročilá detekce hrozeb (UEBA)
6. Odstraňování rizik a automatizace na principu nejmenších možných oprávnění
7. Řízení přístupu na bázi vlastnictví dat

1 Jednotná kontrola nad lokálními daty a daty v Office 365

Podle strategických odhadů společnosti Gartner „bude v roce 2020 více než 85 % společností upřednostňujících ve své strategii cloud nadále hostovat aplikace kriticky důležité pro jejich provoz v prostředích tradičních datových center.“ [3]

Vzhledem k tomu, že lví podíl nestrukturovaných dat je stále uložen lokálně, trpí nativní bezpečnostní nástroje v Office 365 zjevnou zásadní nevýhodou: nemohou zajistit jednotné řízení pro lokální a cloudová data. Kvůli tomu je v hybridních prostředích potřeba zdvojovat postupy, aplikace, upozornění a přehledy.



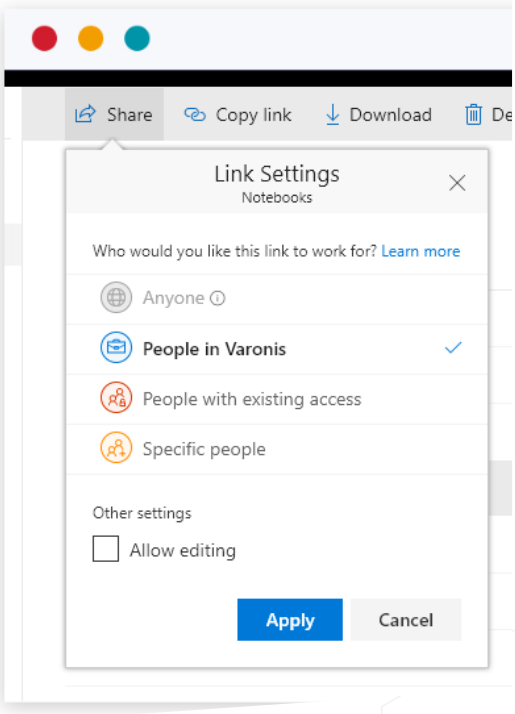
Varonis je jednotná bezpečnostní platforma pro lokální i cloudová data. Pomáhá zajistit, aby v každém okamžiku měli k datům přístup pouze ti lidé, kteří jej mít mají. Veškerá manipulace je sledována a na neoprávněnou činnost je upozorněno.

- **Nevyžaduje instalaci žádných rozhraní**
- **Události shromažďuje pomocí oficiálního rozhraní API od Microsoftu**
- **Blesková instalace**

[3] Gartner, tržní trendy: Postavte se do čela trhu lokálních řešení a zaměřte se na vlastnosti, které jsou pro jeho rozhodování podstatné

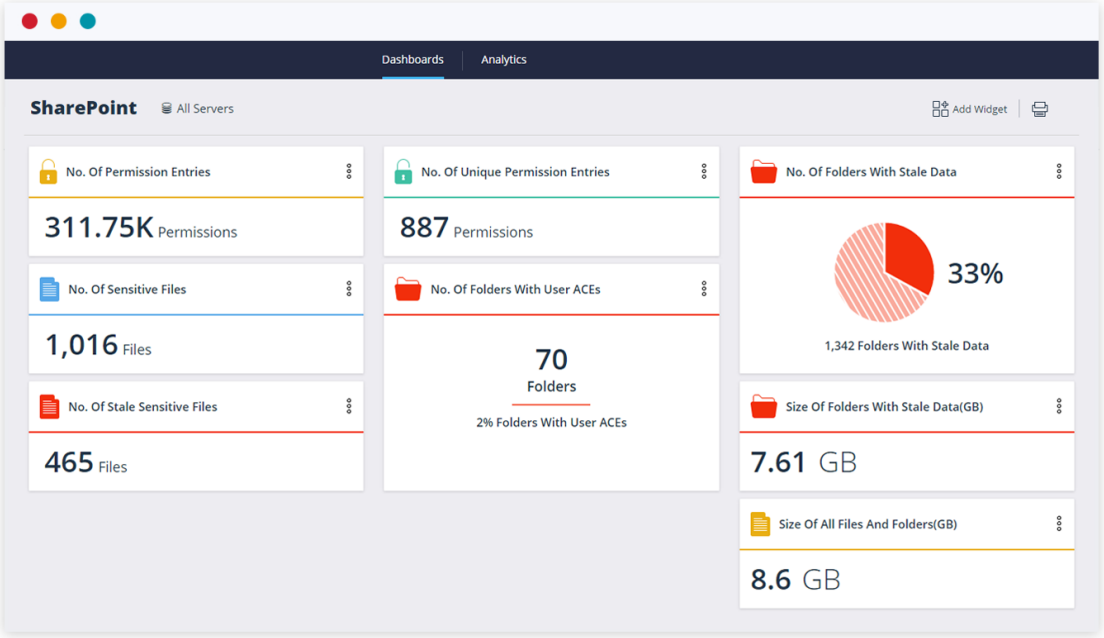
2 Plná viditelnost oprávnění a jejich správa

Může být nesmírně náročné či přímo nemožné rychle zjistit, ke kterým složkám OneDrive, webům SharePoint a schránkám Exchange má určitý uživatel nebo skupina přístup. Ještě těžší je najít ohrožená data, složky s citlivými údaji a externě sdílené objekty a odstranit oprávnění, která již nejsou potřebná.



Varonis vám zajistí holistický pohled na data ve všech datových skladech, ať už lokálních nebo v systému Office 365. Během několika sekund tak mohou pracovníci IT vytvořit vizualizaci nebo přehled potenciálního přístupu jakéhokoli uživatele nebo skupiny v Active Directory, Azure AD nebo v lokálním systému, přesně nalézt zbytečně široce přístupná citlivá data a najít účty s příliš širokými oprávněními.

Výkonný systém dokáže v sandboxu simulovat změny v řízení přístupu a v reálném prostředí je použít až tehdy, je-li vše připraveno. Není přitom třeba rozumět všem specifikům modelů oprávnění v Office 365 a lokálních systémech – Varonis nabízí jednotné abstraktní rozhraní pro správu přístupu k datům.



3 Rozpoznávání citlivých údajů

Aby mohli zákazníci Office 365 posoudit riziko, monitorovat hrozby a určit priority nápravy oprávnění, musí zjistit, kde jsou jejich citlivá data uložena. Vestavěná klasifikace od Microsoftu (prostřednictvím Secure Islands a AIP) vyžaduje ruční vytváření pravidel a označování – což může být zvláště v rozsáhlých prostředích velmi náročné – a nepokrývá lokální datové sklady.

Varonis Data Classification Engine klasifikuje citlivá data v úložištích OneDrive a SharePoint Online i v lokálních úložištích. Platforma Varonis umožňuje hladké propojení s AIP a pro nalezená citlivá data poskytuje tolik potřebný kontext. Můžete tak určovat prioritu a úspěšně data chránit, dodržovat předpisy a vyhnout se únikům dat.

Data Classification Engine má celou řadu vestavěných balíčků pravidel podle GDPR, HIPAA, SOX, PCI-DSS atd. Navíc umožňuje vytvářet vlastní pravidla, provádět ověřování pomocí algoritmů, ručně přidělovat příznaky a dokonce automaticky umísťovat do karantény nebo mazat citlivý obsah neodpovídající zásadám.

4 Komplexní audity a monitoring

Ačkoli i v systému Office 365 lze provádět audit chování uživatelů, je obtížné udělat si komplexní obrázek o aktivitě v jednotlivých aplikacích Office 365. To může komplikovat bezpečnostní vyšetřování a zabránit odhalení hrozeb.

Varonis nabízí centralizované audity a upozorňování pro systémy Exchange Online, SharePoint Online a OneDrive. Jednotná auditní stopa umožňuje vyhledávání a kombinuje aktivitu uživatelů Office 365 s lokálními přístupy na zařízení NAS, Active Directory, UNIX, Exchange, ke sdíleným souborům a další.

5 Pokročilá detekce hrozeb (UEBA)

Microsoft nabízí základní (statické) modelování hrozeb, jeho nativní nástroje však postrádají podrobný kontext chování uživatelů napříč všemi produkty a nejsou schopny odhalit podezřelé chování na účtech, k němuž dochází lokálně.

Ačkoli tyto nástroje obsahují určitý počet předpřipravených pravidel, nemohou nahradit dynamickou detekci hrozeb založenou na chování. Postrádají možnost vytvářet pokročilé modely hrozeb a potlačovat falešné poplachy, takže vestavěný engine pro analýzu chování uživatelů (UEBA) v Office 365 pro většinu SOC nestačí.

Varonis analyzuje aktivitu a chování uživatelů v hybridních prostředích a pro každý účet zjišťuje normální chování. Jeho systém Data Security Platform analyzuje události přístupu k datům v kontextu citlivosti dat, oprávnění a metadat z Active Directory, takže zasílaná upozornění jsou přesná a vzniká méně falešných poplachů.

Varonis obsahuje více než 100 modelů hrozeb, takže je schopen upozornit na cokoli od neobvyklé aktivity v e-mailové schránce přes hrozby ze strany vlastních zaměstnanců až po útoky známého ransomwaru. Bezpečnostní týmy mají na výběr, zda budou využívat řídicí panel DatAlert, nebo si nechají zasílat upozornění do integrovaného systému SIEM.

DatAlert je nejčastěji recenzovaný produkt UEBA na serveru Gartner Peer Insights.

Další informace o zkušenostech zákazníků →

Recenze na serveru Gartner Peer Insights představují subjektivní názory jednotlivých koncových uživatelů založené na jejich vlastních zkušenostech. Nevyjadřují názory společnosti Gartner ani jejích spolupracujících subjektů.

6 Odstraňování rizik a automatizace na principu nejmenších možných oprávnění

Microsoft poskytuje omezený přehled o oprávněních a vyhledávání citlivých dat, nepomáhá určovat prioritu nápravy problémů, neumožňuje žádnou simulaci změn a postrádá centralizovaný mechanismus provádění změn členství ve skupinách Azure AD a oprávnění pro kontejnery. Kvůli těmto omezením je velmi obtížné nastolit model nejmenších možných oprávnění a udržovat jej.

Varonis řeší nejprve to, co pro vás představuje největší riziko, ať už dotyčný problém existuje lokálně nebo v Office 365, a umožňuje vám s minimálním úsilím problémy řešit.

Se systémem Varonis mohou zákazníci okamžitě nalézt a chránit citlivý obsah v globálně přístupných sdílených souborech, na webech SharePoint a ve složkách OneDrive – včetně externě sdílených odkazů. Díky možnosti simulovat změny oprávnění ještě před skutečným použitím nových oprávnění vám Varonis pomáhá zjednodušit strukturu oprávnění na všech platformách a odstranit zbytečná oprávnění, aniž by to negativně ovlivnilo uživatele.

7 Řízení přístupu na bázi vlastnictví dat

Pro udržení modelu nejmenších možných oprávnění je velmi důležité zapojit do procesu správy oprávnění i vlastníky dat. Microsoft však neumožňuje vlastníky dat v Office 365 snadno zjistit, ani je nezapojuje do důležitých procesů řízení přístupu, například do kontrol oprávnění.

Varonis určuje pravděpodobné vlastníky dat podle skutečné aktivity uživatelů. Jakmile je vlastník přiřazen, lze automatizovat procesy kontrol a udělování oprávnění. To šetří čas, snižuje zátěž oddělení IT a pomáhá činit v oblasti řízení přístupu viditelně lepší rozhodnutí.

> Dnešní uživatelé si mohou vyžádat přístup k určité skupině a vlastníci dat jsou automaticky zapojeni do rozhodování, zda tento přístup povolit nebo zamítnout, aniž by se na tom museli podílet pracovníci IT. To nejenom celý proces zrychluje, ale pracovníci IT díky tomu mohou věnovat víc času jiným úkolům.

— Serena Lee, starší bezpečnostní analytik, AXA Wealth

> Varonis je fantastické řešení

Gartner peerinsights™

Nechte si vypracovat vlastní posudek rizik v Office 365

Posudek bezpečnosti dat

Získejte svůj rizikový profil, zjistěte, zda jste zranitelní, a napravte skutečné bezpečnostní problémy.

www.varonis.cz

Praktická ukázka

Instalujte systém Varois ve svém vlastním prostředí a zjistěte, jak se ubránit ransomwaru a chránit svá

www.varonis.cz