

SharePoint a SharePoint Online



Chraňte svá data ve službě SharePoint před nadměrnou přístupností a kybernetickými útoky.

Výzva

SharePoint může být výkonným nástrojem pro spolupráci, ale jeho zabezpečení ve velkém měřítku je velmi obtížné. Se stovkami (možná tisíci) stránek/podstránek/knihoven, přizpůsobitelných úrovní oprávnění, sdílením odkazů a místními uživateli/skupinami, které mohou obsahovat skupiny AD, se odpověď na jednoduchou otázku typu „K jakým datům má kdo přístup?“ stává archeologickým projektem.

Řešení

S Varonis můžete okamžitě vizualizovat a kvantifikovat rizika ve svém prostředí SharePoint bez ohledu na jeho velikost a komplexnost a proaktivně snižovat jejich míru. Varonis odhaluje a klasifikuje citlivé informace, přesně vám ukáže, kdo má k datům přístup, a zaznamená každou jednotlivou akci v podrobné auditní stopě (bez nativního auditu), takže můžete rychle odhalit pokročilé hrozby a vyšetřit incidenty.

„Bez služby Varonis je každé rozhodnutí reaktivní — nástroje Microsoft nenabízejí stejnou úroveň přehledu. S Varonis můžeme přijímat strategická rozhodnutí a proaktivně chránit svá data. Varonis nám přináší konkurenční výhodu.“

CISO,
Obchodník s komoditami v USA

[Přečtěte si případovou studii →](#)

Soubory sdílené
s externími uživateli

42%

Citlivé soubor
sdílené externě

38%

Složky sdílené veřejně

7%

Velikost složek
se zastaralými daty

0.64
GB

Omezte rozsah ohrožení v prostředí SharePoint.

Varonis vám ukáže, kde jsou citlivá data externě přístupná uživatelům typu host nebo všem zaměstnancům a vy tak můžete rychle eliminovat nejkritičtější rizika. Varonis poskytuje intuitivní přehled o účinných oprávněních jakéhokoli uživatele nebo skupiny bez ohledu na zdroj oprávnění. Naše strojové učení analyzuje oprávnění a chování uživatelů a upozorňuje, kde mají uživatelé přístup k datům, která nepoužívají nebo nepotřebují.



Sledujte a prošetřete podezřelé aktivity.

Varonis rozšiřuje vaše zorné pole tím, že uvádí aktivity z prostředí SharePoint a SharePoint Online do kontextu s dalšími aplikacemi M365 a také místními a obvodovými telemetrickými systémy. Naše detekce založené na chování korelují aktivitu v prostředí SharePoint s přihlašovacími chováními, k lokálním archivům a e-mailovou aktivitou a generují přesná upozornění s malým počtem falešných poplachů.

PRÁVNÍ

Doporučení

- ! "#\$% Správce systému ✓
- Margo Conner ✗
- Zara Roberts ✓

Klasifikujte a uzamkněte data ve velkém rozsahu.

Automaticky a přesně klasifikujte citlivá a regulovaná data v prostředí SharePoint pomocí stovek integrovaných zásad, slovníků a pravidel ověřování. Kontrolní panely a přehledy rizik specifické pro SharePoint vám v reálném čase poskytnou informace o stavu rizik a pomohou vám zajistit soulad s příslušnými pravidly a předpisy. Pomocí našeho štítkovače můžete na citlivé soubory aplikovat trvalé štítky MIP pro šifrování, DRM a další.

Provedení operace: Adam Nelson ✕

Služba	Typ	Objekt
	soubor vytvořen	M&A Due Diligence.docx
	soubor vytvořen	G&A Legal Budget.xlsx
	soubor vytvořen	Interesting.txt

Vyzkoušejte Varonis zdarma.

Všechny produkty Varonis lze vyzkoušet zdarma a jsou dodávány s posouzením rizik, které provede bezpečnostní technik. Nejjednodušší způsob jak začít je krátká osobní ukázka a seznamovací rozhovor.

[Kontaktujte nás](#)