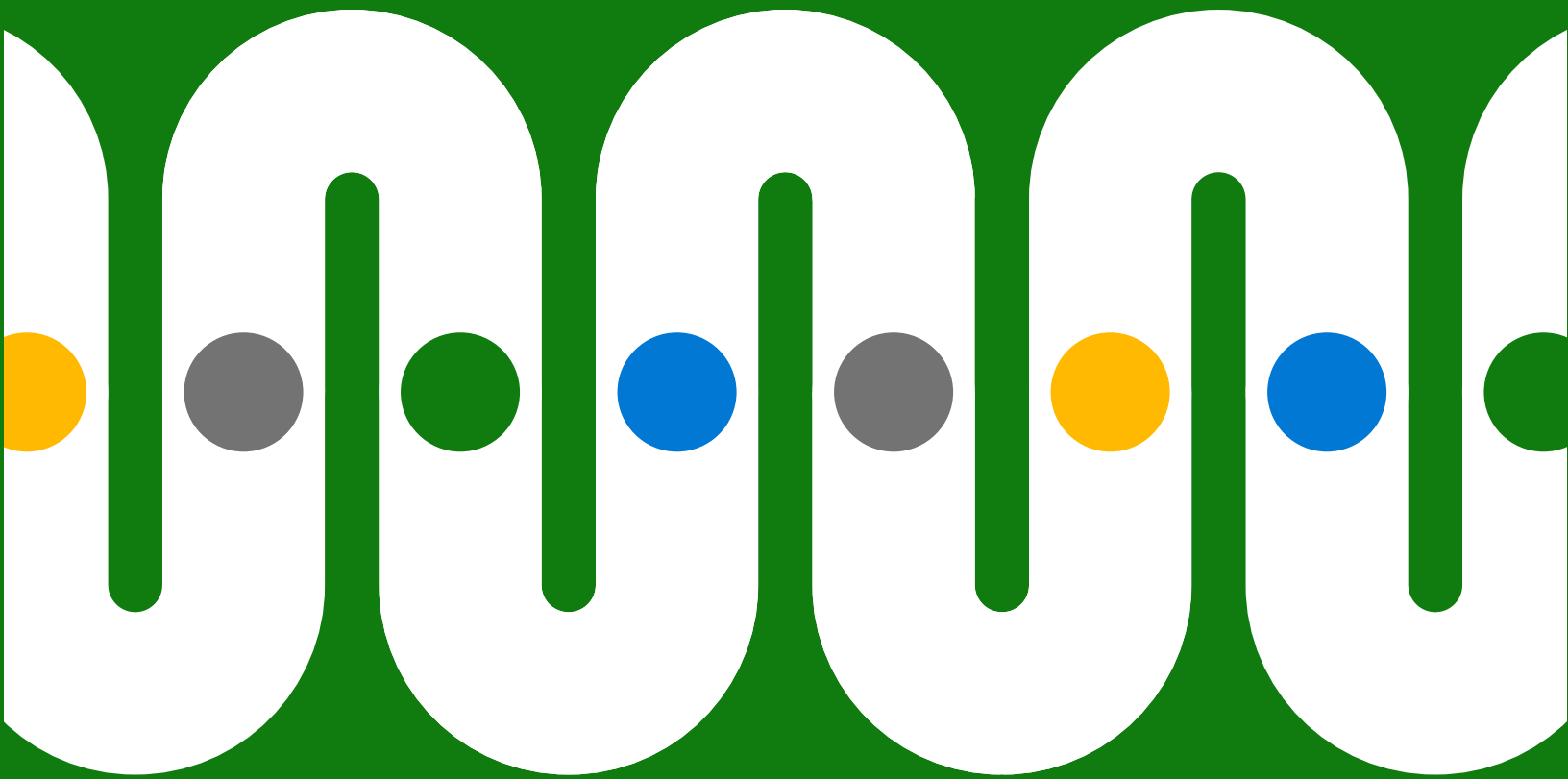
Microsoft Security

3 kroky ke komplexní ochraně vašich dat



Obsah

Průzkum provedený mezi pracovníky s rozhodovací pravomocí v oblasti dodržování předpisů ukázal, že 95 % z nich dělají starosti výzvy spojené s ochranou dat.[2]

Úvod

Hybridní práce vede k tomu, že organizace výrazně zvyšují svou digitální stopu, která nyní výrazně překračuje tradiční kanceláře.

Tento vývoj vede k větší fragmentaci a exfiltraci dat – to vše je dále komplikováno rychlým nárůstem množství různých aplikací, zařízení a lokalit. Mnozí pracovníci také mění svou roli při hledání většího naplnění nebo větší flexibility, což tyto výzvy dále komplikuje a vytváří nová slepá místa v rámci neustále se rozrůstajícího množství dat.[1]

CIO a CISO musí kvůli všem těmto faktorům přehodnocovat svůj přístup k ochraně dat. V rámci průzkumu, jehož se zúčastnilo více než 500 amerických pracovníků s rozhodovací pravomocí v oblasti dodržování předpisů, téměř všichni (95 %) uvedli, že jim dělají starosti výzvy spojené s ochranou dat.[2]

[1] „How Microsoft can help reduce insider risk during the Great Reshuffle, Alym Rayani", Microsoft Security. 28. února 2022.

[2] „Průzkum mezi 512 americkými pracovníky s rozhodovací pravomocí v oblasti dodržování předpisů ze září 2021 zadaný společností Microsoft u společnosti Vital Findings".

Týmy v oblasti IT a zabezpečení hledají lepší způsoby správy celého životního cyklu dat napříč více cloudy, hybridními cloudy a místními prostředími. Tento komplexní přístup zahrnuje tři klíčové kroky:

Krok 1: Identifikace dat

Stanovení, kde se vaše data nachází, o jaký druh dat se jedná a jak se tato data používají nebo sdílejí

Krok 2: Kategorizace dat

Kategorizace a označení dat tak, abyste věděli, jaké zásady a postupy pro zmírňování rizik máte použít

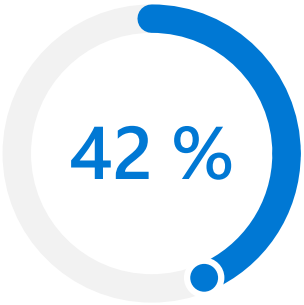
Step 3: Ochrana před únikem informací

Dosažení rovnováhy mezi snižováním rizik a flexibilitou pro vaše pracovníky prostřednictvím inteligentní detekce a řízení

Cíl tohoto přístupu? Uzavření mezer a minimalizace rizik, aniž by docházelo k omezení produktivity.

Krok 1

Identifikace dat



42 % organizací na otázku, jak velká část jejich dat je „temná“, uvedlo, že se jedná alespoň o polovinu.[3]

Tato „skrytá“ data mohou mít spoustu podob od e-mailových příloh a nahrávek hovorů se zákazníky až po protokoly strojů a videozáznamy.

Pokud svá data nedokážete identifikovat – nevíte, kde se nacházejí, o jaký druh dat se jedná nebo jak jsou používána a sdílena – nemůžete na ně aplikovat správné zásady a správnou úroveň ochrany.

Moderní organizace neustále generují obrovské množství dat. Nejedná se jen o dokumenty, e-maily a zprávy, ale o vše od záběrů z bezpečnostních kamer až po údaje o poloze. Množství dat je dále umocněno jejich šířením v různých aplikacích, zařízeních a úložištích, a to jak na pracovištích, tak v cloudu.

Identifikovat všechna tato data může být obtížné a 42 % organizací tvrdí, že alespoň polovina jejich dat připadá na „temná data“.[3] Jedná se o informace, které jsou sice shromážděné, ale jsou neznámé nebo nevyužité pro obchodní účely. Někdy se data změní na temná, když pracovník, který je vytvořil, přejde na jiný projekt nebo do jiné role. Často také jednoduše neexistují žádné systémy, které by data v okamžiku jejich vytvoření nebo úpravy identifikovaly.

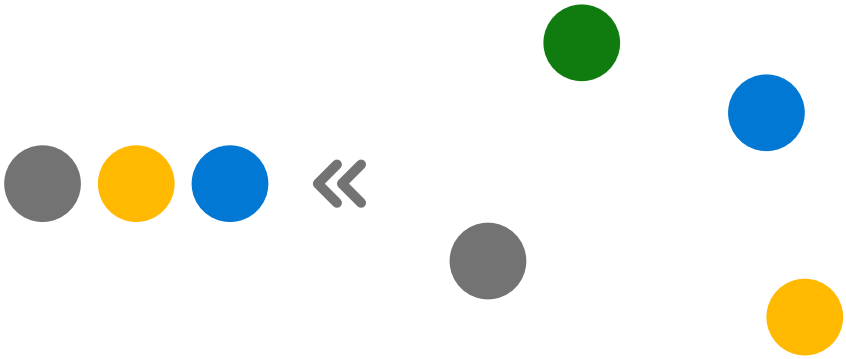
[3] Zpráva „2022 State of Data Governance and Empowerment Report“, Enterprise Strategy Group. Červenec 2022.

Chcete si vybudovat komplexní pracovní postup pro objevování dat na jedné platformě?

Seznamte se s objevováním dat ve službě Microsoft Purview na adrese **Microsoft.com**.

Tato výzva bude stále výraznější. Očekává se, že se množství nově vytvořených, zachycených, replikovaných a spotřebovaných dat do roku 2026 více než dvojnásobí, protože podniková data rostou více než dvakrát rychleji než data spotřebitelů.[4]

Umělá inteligence (AI) a strojové učení (ML) mohou pomoci s rozpoznáním citlivých dat, jako jsou e-mailové adresy, údaje o zdravotním stavu, čísla kreditních karet nebo duševní vlastnictví, a automaticky je kategorizovat. Umělá inteligence a strojové učení mohou také zvýšit přesnost kategorizace a zpětně data kontrolovat. Tyto identifikační procesy mohou zahrnout veškerá vaše data a mohou zachovávat, shromažďovat, analyzovat, přezkoumávat a exportovat obsah všude, kde se nachází, v libovolných cloudech.



[4] „Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth“, John Rydning, IDC. Květen 2022.

Krok 2

Kategorizace dat

Kategorizace a zásady musí data sledovat na jejich cestě společností.

Pokud například pracovník zkopíruje čísla kreditních karet z dokumentu Microsoft Word do Excelu, měly by se zásady a kategorizace automaticky použít na oba dokumenty.

Řádná kategorizace dat vám pomůže určit správné zásady a správné způsoby omezování rizik, které zajistí, aby jednotlivé typy dat nebyly neúmyslně či záměrně zneužity nebo aby k nim neměly přístup osoby bez náležitého oprávnění. Šifrování a vodoznak mohou data ochránit ještě výrazněji – to platí pro uložená data, přenášená data i právě používaná data.

Kategorizace a zásady však musí být na příslušná data navázány během celé jejich cesty organizací. Zásady označování a ochrany se nemohou omezovat na jednotlivé dokumenty, musí zahrnovat celý digitální majetek – od lokálních úložišť po cloudová, od aplikací typu SaaS (software jako služba) po aplikace v operačním systému.

Tradiční přístupy ke kategorizaci vyžadují rozsáhlou ruční práci, což s sebou nese riziko chyb nebo neúmyslného přehlédnutí kritických dat. Vestavěné a trénovatelné kategorizační nástroje mohou přispět k automatizaci tohoto procesu a správci mohou prostřednictvím integrovaného řešení centrálně spravovat zásady ve všech systémech.

Chcete lépe spravovat a chránit citlivá data v rámci celého svého prostředí?

Seznamte se s kategorizací a ochranou dat ve službě Microsoft Purview na adrese **Microsoft.com**.

Krok 3

Ochrana před únikem informací

Zásady DLP mohou zabránit akcím, které nejsou v souladu s předpisy.

Pokud se například zaměstnanec pokusí stáhnout tabulku s čísly kreditních karet na jednotku flash nebo ji nahrát do cloudového úložiště, mohou zásady DLP tuto aktivitu identifikovat jako porušení předpisů a zakázat ji.

Chcete inteligentní detekci a kontrolu citlivých informací?

Seznamte se s ochranou před únikem informací ve službě Microsoft Purview na adrese **Microsoft.com**.

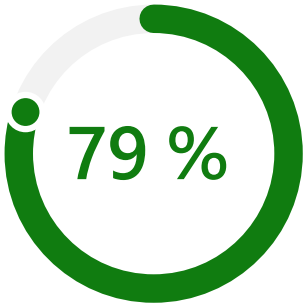
Poté, co svá data identifikujete a kategorizujete, mohou řešení ochrany před únikem informací (DLP) vynutit komplexní zásady ochrany, které dokáží zmírnit hrozby, jako jsou tmavá data a exfiltrace dat, takže současní ani bývalí zaměstnanci nebudou moci sdílet, zpřístupňovat či přenášet citlivá data bez oprávnění, ať již záměrně, nebo neúmyslně.

Inteligentní řešení DLP využívají kontext k dosažení rovnováhy mezi zajišťováním flexibility a blokováním vysoce rizikových akcí. Jednotlivci například budou moci pokračovat v akci poté, co budou upozorněni na potenciální rizika a příslušné zásady. To může přispět k ochraně citlivých dat a současně také ke školení uživatelů, aby lépe porozuměli rizikům.

Řešení DLP mají zásadní význam pro ochranu duševního vlastnictví a dalších kritických podnikových dat, stejně jako pro dodržování předpisů, jako je obecné nařízení o ochraně osobních údajů (GDPR), zákon o přenositelnosti a odpovědnosti zdravotnických informací (HIPAA) a kalifornský zákon o ochraně soukromí spotřebitelů (CCPA).

Komplexní přístup k DLP navíc prosazuje zásady konzistentně v rámci celé organizace, čímž omezuje potenciální zneužití „nejslabších článků" v životním cyklu dat.

Ochranu dat neprovádějte pomocí různých řešení zároveň. Integrujte ji.



Průzkum mezi pracovníky s rozhodovací pravomocí v oblasti dodržování předpisů ukázal, že 79 % z nich zakoupilo více produktů pro dodržování předpisů a ochranu dat.

Většina z nich jich koupila tři nebo více.[5]

Mnoho organizací vyzkoušelo přístup k ochraně informací založený na „postupném doplňování funkcí“, kdy diskrétní části životního cyklu dat spravovaly prostřednictvím několika různých řešení. Týmy zabývající se zabezpečením, správou dat a dodržováním předpisů a právní týmy jsou ale tak nuceny dát dohromady skládačku, která je často neúčinná a která neúměrně zatěžuje zdroje.

„Integrovaný“ přístup může překlenout mezery a spojit identifikaci dat s jejich kategorizací a DLP. Díky integrovanému řešení je jednodušší zásady centrálně spravovat a vynucovat. Zkracuje také dobu potřebnou ke školení uživatelů, kterým se oznámení o zásadách zobrazují známým způsobem, tedy nativně přímo v aplikacích.

[5] „Dotazník z února 2022 mezi 200 americkými pracovníky s rozhodovací -pravomocí v oblasti dodržování předpisů (n = 100 599–999 zaměstnanců, n = 100 1000 a více zaměstnanců) zadaný společností Microsoft u společnosti MDC Research.“

Vestavěné integrované řešení: Microsoft Purview

Microsoft Purview vám pomůže plnit výzvy dnešního decentralizovaného pracoviště s mnoha různými pracovišti. Nabízí ucelenou sadu řešení, která vám pomohou řídit, chránit a spravovat celé vaše datové prostředí.

Jděte za rámec zásad správného řízení.

Další informace o ochraně dat prostřednictvím služby Microsoft Purview >

Zajímá vás určitá konkrétní oblast ochrany dat? Získejte podrobnější informace o tom, jak vám může služba Microsoft Purview pomoci v těchto oblastech:

Objevování dat >

Kategorizace a ochrana dat >

Ochrana před únikem informací >

Microsoft Security