safetica

Váš průvodce komplexní DLP strategií: procesy, nástroje a dodavatelé

2026

Obsah

Váš průvodce komplexní DLP strategií: procesy, nástroje a dodavatelé

Prevence ztráty dat (Data Loss Prevention – DLP) existuje již od počátku 21. století. Byla průkopnicky rozvíjena řadou startupů, které se zaměřovaly především na síťové kontroly sloužící k blokování úniků dat na perimetru.

Mnoho prvních uživatelů nasadilo DLP jako základní prvek své kyberbezpečnostní strategie, často společně s firewally a systémy pro detekci průniků, aby mohli vynucovat politiky nad daty v pohybu.

Přístup k DLP se však od těchto počátků bohužel změnil. Regulace, jako je GDPR v roce 2018 a CCPA v roce 2020, vyžadovaly přísnější nakládání s daty a přiměly organizace využívat DLP spíše pro auditní stopy a reportování než pro čistou prevenci hrozeb. Pokuty za nedodržení byly vysoké a nekompromisní.

Jakmile se však soulad s předpisy stane důležitějším než řízení rizik, priority se **rozcházejí**. Tento vývoj způsobil, že se DLP v mnoha případech stalo pouze „checkboxovým“ cvičením pro splnění compliance požadavků.

Dalším problémem je, že rané formy DLP, které se silně opíraly o statická pravidla a data v klidu, jednoduše nebyly schopny reagovat na nové obchodní reality. Bezpečnostní profesionálové se ocitli v začarovaném kruhu: implementovali nejlepší dostupná řešení, ale přesto čelili pokutám za úniky dat, protože tehdejší technologie DLP ještě nebyla dostatečně vyspělá.

V dnešní době je možné řídit rizika a zároveň udržet soulad s předpisy, pokud je použit správný systém. DLP se v průběhu let výrazně vyvinulo a organizace by měly znovu posoudit své potřeby v oblasti DLP i to, jak by měla moderní DLP řešení vypadat. Klíčem je využít systém, který byl od základu navržen s ohledem na obě tyto potřeby.

Moderní DLP využívá behaviorální analytiku k detekci anomálií, čímž se liší od starších systémů založených na pravidlech, které často generují vysoký počet falešných poplachů.

Globální objem dat dosáhl ohromujících hodnot a bude dále růst s tím, jak se svět stává stále více závislým na digitálních datech. Vše od smluv po dokumentaci se přesouvá online, což výrazně zvyšuje potenciální riziko ztráty dat.

Vedoucí pracovníci v oblasti bezpečnosti musí vyhodnotit stávající nasazení ve světle těchto změn a odstranit mezery v ochraně. To zahrnuje mapování datových ekosystémů, identifikaci bodů vystavení, provádění hodnocení rizik se zaměřením na vysoce hodnotná aktiva, zapojení chování uživatelů do vynucování politik a integraci všeho do jednoho systému, který nepřetržitě monitoruje data v klidu i v pohybu.

Pokud to zní jako hodně práce, tak ano. Ale s moderním a komplexním DLP řešením je to možné.

Příprava na tuto novou realitu vyžaduje pochopení nového prostředí rizik, nástrojů a procesů, které by měla organizace zvážit, a také způsobu, jak přistupovat k dodavatelům.

Zvažte například fakt, že **70 % ztrát dat vzniká na endpointu**, což naznačuje, kde by měla být soustředěna většina ochranných opatření. Zjednodušená odpověď „zaměřme se na endpointy“ však opomíjí komplexní povahu ukládání a přenosu dat. I když ke ztrátám dat nejčastěji dochází na koncových zařízeních, kompromitace, která ke ztrátě vede, zde obvykle nezačíná ani nekončí – často má původ jinde.

Tento příklad jasně ukazuje, proč musí bezpečnostní profesionálové přehodnotit své stávající DLP postupy a zároveň vybírat nástroje, které poskytují kontextové informace.

Ochrana založená na kontextu vyžaduje přehled napříč sítí, cloudovými aplikacemi i chováním uživatelů – nikoli pouze na úrovni endpointu. Tento průvodce se zaměří na nové prostředí DLP, podobu efektivního DLP a na to, jak se stát informovanějším kupujícím při výběru DLP dodavatelů.

Změna v prostředí DLP

Rozsah míst, kde se nacházejí data organizace, se dramaticky rozšířil. Širší využívání SaaS nástrojů a třetích stran než kdy dříve způsobuje, že data přirozeně směřují do cloudu. To vede k datovému rozptylu a vzniku ROT dat (redundantních, zastaralých nebo

triviálních), což často znamená, že organizace mají příliš mnoho dat na příliš mnoha místech.

Tento problém je ještě výraznější v hybridních prostředích, zejména pokud se aktiva neustále přesouvají z on-premise do cloudu. Tato migrace vystavuje data novým rizikům a protože cloudoví poskytovatelé zajišťují úložiště, zatímco odpovědnost za bezpečnostní konfigurace zůstává na organizacích, přenášejí nezabezpečení poskytovatelé cloudových úložišť většinu rizika právě na organizace.

Dodavatelé, SaaS a široký ekosystém třetích stran

Organizace zvýšily svou závislost na externích dodavatelích – průměrná firma používá 106 SaaS aplikací v roce 2024. Velké podniky v průměru využívají 131 SaaS nástrojů. A to jsou pouze SaaS aplikace, bez započtení dalších dodavatelů.

Dodavatelé mají často přístup k citlivým datům, což vytváří potenciální body úniku, pokud nemají přísné kontroly. I když týmy obvykle přístup dodavatelů auditují, nejednotné standardy napříč partnery komplikují vynucování politik. Rozšířené využívání SaaS a rychlá implementace navíc znamenají, že SaaS dodavatelé mohou být onboardováni během několika dní, aniž by o tom bezpečnostní tým věděl nebo je stihl řádně prověřit.

Open-source kód a IDE

Open-source vývojová prostředí představují další rizikovou oblast. Open-source komponenty mohou obsahovat známé i neznámé zranitelnosti. Pokud jsou tyto komponenty použity ve vývojových nebo produkčních systémech, útočníci je mohou zneužít k získání neoprávněného přístupu a potenciální exfiltraci dat.

Rozsáhlá studie rozšíření pro VS Code zjistila, že více než 2 000 rozšíření (přibližně 8,5 % všech rozšíření) je náchylných k úniku dat. Tyto open-source komponenty jsou

obzvlášť rizikové, protože jejich povaha umožňuje útočníkům snadno vyvíjet exploity nebo útoky cílené právě na ně. Identifikací široce používané komponenty mohou útočníci zasáhnout tisíce společností prostřednictvím jediné zranitelnosti.

Politiky vzdálené a hybridní práce

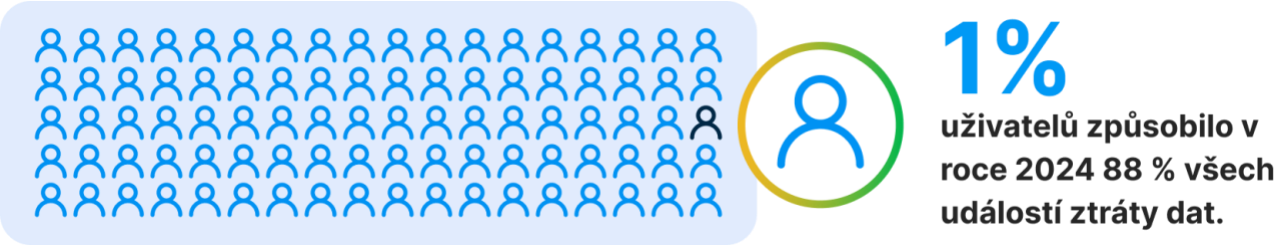
Politiky vzdálené a hybridní práce decentralizovaly přístup k datům. Zaměstnanci přistupují k systémům z různých míst a zařízení, což zvyšuje riziko na úrovni endpointů. Více lokalit a globální pracovní síla navíc fragmentují správu dat a dále přispívají k jejich rozptylu.

Široce distribuovaná pracovní síla může být také noční můrou z hlediska compliance. Různé země mají odlišné zákony týkající se ukládání a zpracování dat, což vede ke komplikacím při přístupu k datům z jiných jurisdikcí.

Různé týmy mohou preferovat různé nástroje pro spolupráci, například WhatsApp v LATAM oproti Slacku nebo Teams v USA, což komplikuje standardizovaný DLP proces i celkovou viditelnost dat.

Tyto faktory činí DLP ještě složitějším, než již bylo, a vedou k situaci, kdy **více než 50 % firem zaznamenalo narušení provozu** v důsledku ztráty dat, zatímco pouze 35 % uvádí, že má „vyspělý“ DLP program.

Proč efektivní DLP vyžaduje úplnou viditelnost



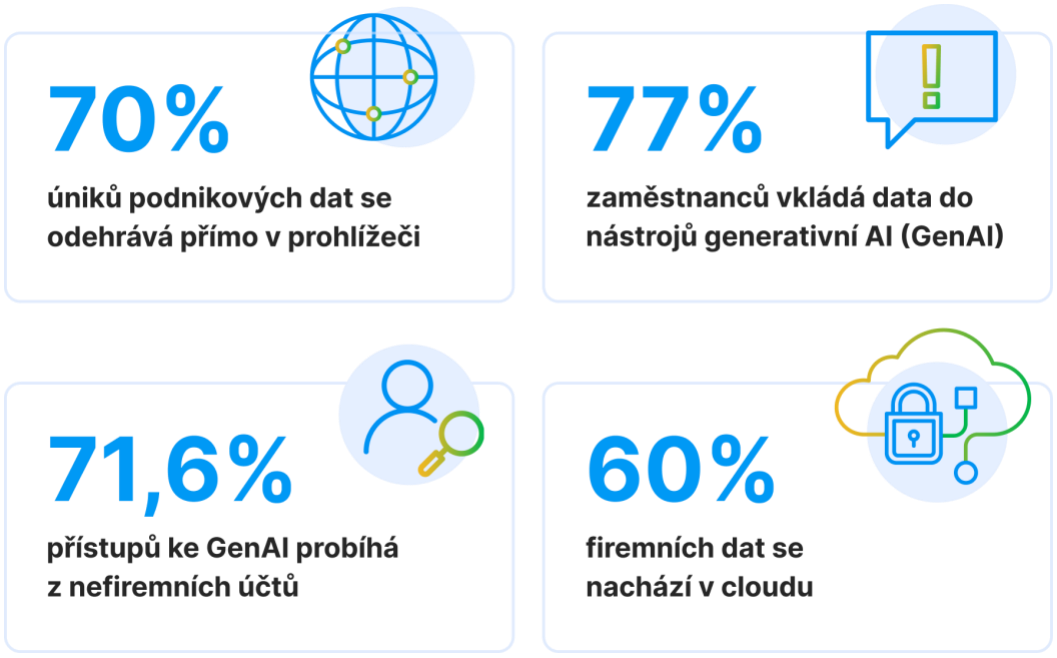
88 % všech incidentů ztráty dat v roce 2024 bylo způsobeno 1 % uživatelů, což podtrhuje, jak zásadní je zabezpečit *každé* zařízení a *každý* potenciální bod ztráty. Útočníkovi stačí jediná slabina, aby získal dostatečný přístup a způsobil významné škody.

Viditelnost je obtížná v roztříštěném datovém prostředí

S ohledem na nové datové prostředí je tvrzení, že viditelnost představuje obtížnou a komplexní výzvu, spíše slabým vyjádřením. Data dnes existují napříč endpointy, SaaS aplikacemi, IaaS platformami, nástroji třetích stran, kolaboračními platformami, osobními zařízeními, více zařízeními vlastněnými zaměstnanci, IoT zařízeními a cloudovými úložišti.

Tradiční nástroje založené na perimetru nedokážou konzistentně sledovat ani vynucovat politiky napříč všemi těmito vrstvami. Zaměstnanci navíc mohou používat neautorizované služby ke sdílení souborů nebo ke zjednodušení práce, často bez vědomí IT oddělení.

Statistiky týkající se nedostatečné viditelnosti organizací jsou velmi výmluvné.



Bezpečnostní oddělení nebyla původně navržena tak, aby sledovala data v prostředích, ve kterých dnes fungují, a s adaptací na tuto novou realitu mají značné potíže. Viditelnost selhává, protože nástroje nejsou integrovány, data nemají jasně vymezené hranice a většina klasifikace je povrchní. To, co je často považováno za „klasifikaci“, je ve skutečnosti jen shoda klíčových slov nebo jednorázové označení souboru jako „důvěrný“ s předpokladem, že takový zůstane i po zkopírování nebo sdílení.

I při velmi kvalitní klasifikaci může být prosazování správné datové hygieny obtížné. V mnoha organizacích je samotná datová vrstva roztříštěná a oddělená od systémů, které ji mají sledovat. Dokud bezpečnostní profesionálové nepřehodnotí, kde a jak monitorují používání dat, komplexní viditelnost bude nadále selhávat.

Konsolidace zabezpečení dat je samostatnou výzvou

DLP je efektivní pouze tehdy, pokud pokrývá veškerá data organizace, což je při fragmentovaném úložišti obtížné a vede k neúplné ochraně.

Moderní podniky trpí datovým rozptylem v důsledku výše popsaných problémů. Datová aktiva jsou stále více rozprostřena napříč mnoha systémy a úložišti. Tradiční DLP řešení byla navržena pro starší, jednodušší infrastruktury, jako jsou on-premise servery, spravované endpointy a podnikové sítě. Jak se práce přesunula do SaaS aplikací, cloudových úložišť, nástrojů v prohlížeči, hybridních cloudů a vzdáleného režimu, tyto původní předpoklady přestaly platit.

V důsledku této změny se dnes velká část citlivých dat nachází nebo pohybuje v kanálech, které tradiční DLP nedokáže monitorovat. Zaměstnanci například používají SaaS aplikace nebo webové nástroje k úpravám, nahrávání nebo sdílení citlivých souborů. Starší DLP řešení umístěná pouze na hranicích endpointů tyto kanály často zcela přehlížejí.

Tato fragmentace vytváří slepá místa, kde může docházet k únikům dat mimo dosah tradičního DLP. Výsledkem jsou částečné implementace DLP – například pouze na endpointech nebo on-premise systémech. Není proto překvapivé, že to vede jen k částečné ochraně a nutí bezpečnostní lídry hledat komplexnější řešení, pokud si tyto limity vůbec dokážou uvědomit.

Řízení interních rizik

Řízení interních rizik (Insider Risk Management – IRM) je klíčovým rozšířením každé komplexní DLP strategie. Na rozdíl od externích hrozeb pochází interní rizika od osob, které již mají přístup k interním systémům nebo přihlašovacím údajům. Patří sem zaměstnanci, dodavatelé i partneři – a to jak v případě úmyslného jednání, tak i nedbalosti.

Lidský faktor dominuje událostem ztráty dat. Podle zprávy Verizon 2024 Data Breach Investigations Report, **68 % narušení dat zahrnuje nemaliciózní lidský prvek**, například podlehnutí sociálnímu inženýrství.

IRM je nezbytným rozšířením rozsahu DLP. DLP bez povědomí o interních rizicích nezohledňuje nejčastější příčiny úniku dat. Komplexní DLP strategie musí zahrnovat nástroje a procesy schopné rychle identifikovat a řešit interní rizika.

Na co se zaměřit pro efektivní DLP: Procesní průvodce

Efektivní DLP začíná správnou prioritizací – bez ní jsou snahy příliš široké a rozmělněné.

> „Organizace si často myslí, že zabezpečení dat pomocí DLP řešení je jen otázkou konfigurace nástroje," říká Ján Lakatoš, Director of Product ve společnosti Safetica. „Ve skutečnosti jde o zavedení zcela nového bezpečnostního procesu do pracovního prostředí a hledání rovnováhy mezi přísnou bezpečností a podporou byznysu. Dosáhnout této rovnováhy je téměř nemožné, protože do hry vstupuje příliš mnoho proměnných."

Začněte viditelností

Viditelnost je základem každé efektivní DLP strategie. Bez ní organizace nedokážou zjistit, kde se citlivá data nacházejí, jak se pohybují ani kdo s nimi pracuje.

Efektivní viditelnost vyžaduje průběžné objevování dat napříč všemi prostředími. Musí být také navázána na identitu – tedy spojovat přístup k datům s konkrétními uživateli a zařízeními. To je klíčové jak pro vynucování politik v reálném čase, tak pro vyšetřování po incidentech.

Žádný DLP systém nemůže aplikovat kontroly ani detekovat zneužití, pokud nejprve neví, jaká data existují a kde jsou uložena.

Implementujte efektivní monitoring

Jakmile je zajištěna viditelnost, monitoring umožňuje sledovat přístup k datům a jejich pohyb v reálném čase. Bez monitoringu zůstává viditelnost pasivní – užitečná pro audity, nikoli však pro prevenci nebo detekci incidentů.

Efektivní monitoring zachycuje nejen to, kde se data nacházejí, ale i jejich chování. Určuje, *kdo* k nim přistupoval, *jaké* akce prováděl a zda tyto akce odpovídají firemním politikám. V ideálním případě by měl monitoring pokrývat autorizované i neautorizované nástroje, včetně SaaS platforem a nástrojů v prohlížeči.

Monitoring musí být kontextový – pouhá informace, že byl soubor otevřen, nestačí. Systém by měl zaznamenat, kdo k němu přistoupil, odkud, z jakého zařízení a zda byl sdílen nebo exfiltrován. Tento kontext je zásadní pro detekci rizik, protože umožňuje pokročilým DLP nástrojům identifikovat kompromitace nebo interní útoky na základě anomálního chování, nikoli jen podle statických pravidel či podpisů.

Bez kontinuálního, vícevrstvého monitoringu nemohou DLP kontroly reagovat na reálné hrozby ani dynamicky vynucovat politiky.

Upřednostněte konsolidaci a zjednodušenou datovou architekturu

Fragmentovaná prostředí vytvářejí slepá místa a zpomalují reakční časy, což činí konsolidaci nezbytnou. Jednotná datová architektura poskytuje jasný přehled o všech interakcích s daty, zvyšuje přesnost detekce a snižuje počet potenciálních bodů selhání.

Existence více pravidel napříč platformami pro klasifikaci dat nebo retenční politiky – případně rozdílné politiky napříč databázemi a prostředími – vede ke konfliktům. Konsolidace a standardizace zajišťují jednotné uplatňování pravidel a odstraňují konfigurační mezery.

Výsledkem je rychlejší reakce na incidenty, protože existuje jediné místo pro kontrolu logů a úpravu kontrol. Konsolidace by měla zahrnovat také audit, který ověří, že data nejsou uložena ve veřejně dostupných nebo nezabezpečených databázích a že nebyla opomenuta žádná místa, kde by se data mohla nacházet. Prioritou by mělo být omezení rozptýlených zdrojů dat na jeden autoritativní zdroj, aby bylo možné jednat rychle a s jasným přehledem o situaci.

Nepřetěžujte svůj tým

Složitost dodavatelů a příliš mnoho nástrojů výrazně zvyšují riziko ztráty dat. Starší nástroje ztěžují implementaci efektivního DLP, což je důvod, proč **78 % organizací** mělo v roce 2024 problémy s DLP nástroji.

Nejde jen o organizaci, ale i o tým. Nedostatek personálu a mezery v dovednostech jsou běžné. Téměř všichni CISOs uvádějí, že jejich týmy jsou poddimenzované, a **90 % odborníků na kyberbezpečnost** hlásí nedostatek potřebných dovedností. Přesto mnoho bezpečnostních lídrů reaguje snahou přidat další nástroje.

To vede k vyhoření týmu a nadměrné složitosti, která snižuje efektivitu. Zaměřte se raději na automatizaci rutinních úloh a omezte nástrojový chaos pouze na nezbytné integrace. Tím zvýšíte kapacitu bez přetížení.

Nepřidávejte další komplexitu do již přetíženého týmu.

Úvod do DLP nástrojů

Na trhu existuje mnoho DLP nástrojů a je úkolem bezpečnostního lídra být informovaným zákazníkem. Jinak hrozí, že pořídíte řešení, které nebude vhodné pro vaši organizaci, tým ani rizikový profil.

Ne všechny nástroje jsou stejné a ne všechny slouží všem organizacím. Bezpečnostní lídři by měli hledat nástroje, které podporují proaktivní přístup a odpovídají prioritám definovaným v rámci DLP strategie.

Níže uvádíme přehled typů nástrojů, které vám pomohou vybudovat efektivní DLP technologický stack.

Nástroje pro objevování a klasifikaci dat

Nástroje pro objevování a klasifikaci dat prohledávají data organizace, zjišťují, kde jsou informace uloženy, a třídí je do smysluplných kategorií. Jejich hlavním cílem je zviditelnit skrytá data napříč všemi lokacemi (cloud, on-premise, třetí strany) a správně je označit, aby na ně bylo možné aplikovat odpovídající ochranu.

Tyto nástroje analyzují počítače, servery, cloudová úložiště, e-mailové systémy, sdílené složky a někdy i staré archivy. Identifikují zákaznické záznamy, platební údaje, osobní identifikátory, interní dokumenty a duševní vlastnictví.

Po identifikaci aplikují jasná označení, která umožňují automatické vynucování bezpečnostních pravidel, například blokování stahování nebo zabránění externímu sdílení.

MDM (správa mobilních zařízení)
Nástroje pro správu mobilních zařízení (MDM) vytvářejí kontrolované prostředí pro každý telefon, tablet nebo notebook, který pracuje s firemními daty.

Tyto nástroje dávají organizacím možnost nastavovat pravidla pro chování zařízení bez ohledu na to, kde se tato zařízení nacházejí. To je zásadní pro prevenci ztráty dat, protože největším rizikem mobilních zařízení je jejich neustálý pohyb a každodenní připojování k různým sítím. Zařízení opouštějí kanceláře, připojují se k nezabezpečeným sítím, mohou se ztratit a ukládají citlivé soubory, které se v případě krádeže zařízení mohou snadno dostat do nepovolaných rukou.

MDM řešení řeší několik problémů najednou, například:

- Zajištění silného zabezpečení každého zařízení na úrovni uzamčené obrazovky
- Oddělení osobního obsahu od pracovního obsahu, aby zaměstnanci mohli zařízení používat bez rizika zpřístupnění firemních souborů
- Kontrola toho, které aplikace mohou otevírat nebo kopírovat pracovní dokumenty
- Sledování zařízení, aby je bylo možné dohledat nebo vzdáleně vymazat
- Umožnění vzdáleného odstranění pracovních dat
- Poskytování centralizovaného přehledu o aktivitě zařízení a včasného varování v případě, že je zařízení (nebo data na něm) ohroženo

Řízení interních rizik (IRM)
Nástroje IRM se zaměřují na prevenci ztráty dat způsobené osobami uvnitř organizace – zaměstnanci, dodavateli a dalšími uživateli s legitimním přístupem k systémům.

Sledují chování, které může vést ke zneužití nebo odcizení dat, například neobvykle velké stahování, pokusy obejít omezení, hromadné kopírování souborů, přístupy v nestandardních časech nebo přesun dat do úložišť mimo kontrolu zaměstnavatele.

Anomální chování nemusí vždy znamenat zlý úmysl, riziko však přetrvává. V nejhorším případě může být účet kompromitován, v lepším případě se data ocitnou mimo dohled organizace. Výsledek je stejný – riziko ztráty dat a narušení bezpečnosti zůstává.

Interní hrozby nemusí být úmyslné a často ani nejsou. Nevinnost nebo špatná bezpečnostní hygiena však nesnižují nutnost tato rizika řešit.

IRM je často vnímáno odděleně od DLP, protože se zaměřuje na lidské chování spíše než na pohyb souborů nebo pravidla zařízení. Ve skutečnosti by však mělo být součástí DLP, protože mnoho incidentů se odehraje i při existenci tradičních kontrol. Kombinací obou přístupů lze dosáhnout výrazně bezpečnějšího prostředí.

Kde mohou dodavatelé pomoci s DLP

Výše uvedené kroky představují pevný základ pro implementaci moderní a efektivní DLP strategie.

> „Je důležité pochopit, jaké jsou cíle a očekávání," říká Miloš Blata, Director of Sales Engineering ve společnosti Safetica. „Jde o klasifikaci dat, ochranu dat, bezpečné kontroly perimetru, zjištění, kde se nacházejí data v klidu, splnění regulatorních požadavků nebo standardů, přehled o tom, co se obecně děje, logování a efektivní správu (ideálně s využitím AI), kombinaci některých z těchto oblastí, nebo vše dohromady? Jakmile je tento ‚nultý krok' jasný, správa DLP konfigurace je mnohem jednodušší."

Při výběru dodavatelů si položte následující otázky:

- Řeší dodavatel klíčovou prioritu uvedenou v tomto průvodci?
- Zvyšuje komplexitu, nebo naopak zlepšuje efektivitu a snižuje provozní zátěž?
- Při zvažování celého rozsahu vaší DLP strategie, jak velkou její část tento dodavatel ovlivňuje? Pokud je tento dopad příliš malý, pravděpodobně budete muset najít další dodavatele.
- Nabízí integrované DLP a IRM v jedné platformě, nebo budete muset spravovat více nástrojů a integrací?

Tyto otázky vám pomohou určit, kteří dodavatelé přinesou vaší organizaci největší přínos.

Při dalším rozvoji DLP strategie nezapomínejte na základy. Dobrá strategie pokrývá všechny aspekty ochrany dat a zároveň zohledňuje nová rizika vyplývající z rozsáhlé digitální stopy i neustále se vyvíjejících interních hrozeb. Silné základy však postačí k tomu, aby se vaše DLP strategie dokázala těmto novým výzvám přizpůsobit. Nejprve je vybudujte – a poté jste připraveni vybrat správné nástroje a dodavatele.