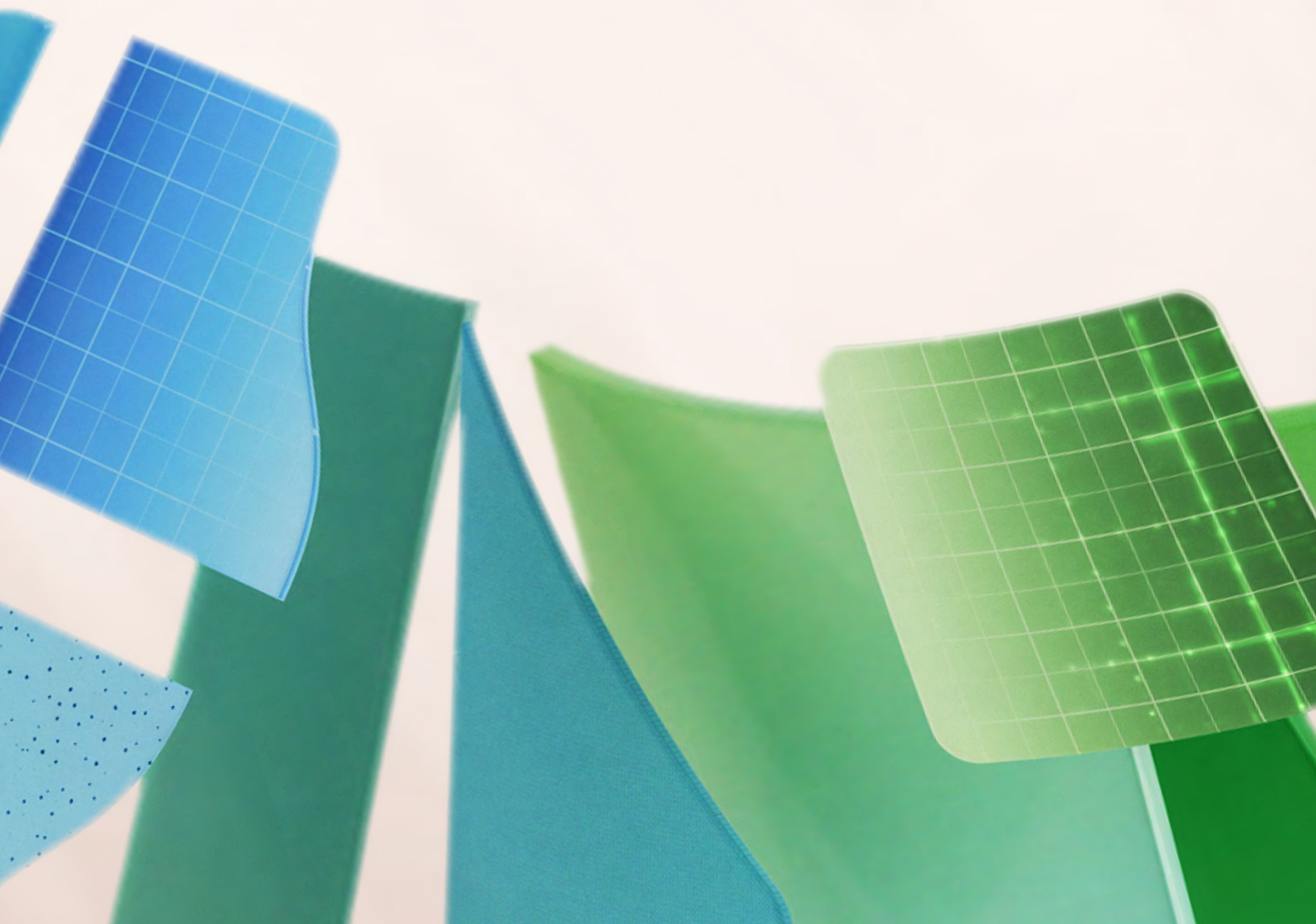


Data pod kontrolou

Ovládnutí řízení dat pro úspěch s AI



Obsah

Úvod

Řízení dat je základem bezpečného zavedení AI

Generativní AI slibuje transformaci firem – ale realizace takového potenciálu závisí na kvalitě a dostupnosti firemních dat.

Organizace, které samy upřednostňují silnou pozici v řízení dat, získávají s AI konkurenční výhodu. Řízení dat pomáhá zajistit, že data, na která se dotazuje AI a která AI generuje, jsou správná, bezpečná, řízená a v souladu s předpisy.

Kvalita a dostupnost dat:

Systémy AI spoléhají na velké, vysoce kvalitní datové sady, s nimiž poskytují nejlepší možnou odpověď se správným kontextem z jedinečných pracovních postupů vaší organizace. Vyšší kvalita dat vede k efektivnějším poznatkům a predikcím AI.

Dodržování předpisů: Silné řízení dat zajišťuje dodržování regulačních požadavků, což snižuje riziko právních problémů a pokut.

Zabezpečení: Správné popisování a řízení dat chrání citlivé informace před neoprávněným přístupem, nevhodným sdílením a úniky.

Důvěra: Spolehlivé řízení dat vytváří důvěru zúčastněných stran ve výstupy AI, což podporuje širší zavedení a podporu iniciativ AI.

Tato elektronická kniha představuje stěžejní postupy řízení dat, které připravují organizaci na AI. Zabývá se způsoby, jak stanovit robustní standardy kvality dat, zajistit dodržování regulačních požadavků a implementovat ochranu dat a bezpečnostní opatření. Ať už jde o ochranu informací z citlivé schůzky před externím sdílením, nebo obranu před únikem dat, dozvíte se strategie, jak vybudovat důvěru v systémy AI a zajistit snadnou přístupnost dat, ze kterých vyplynou prakticky využitelné poznatky. Zavedením těchto postupů může vaše organizace využít plný potenciál AI k průběžným inovacím a jako konkurenční výhodu.

Případy použití generativní AI

Urychlení komunikace: Rychleji můžete vytvářet koncepty přizpůsobeného obsahu, což uvolní čas na budování vztahů a spolupráci.

Zlepšení efektivity: Zkraťte dobu věnovanou rutinním úkolům, zvýšte produktivitu a ušetřete náklady.

Podpora inovací: Pomozte vzniku nápadů a návrhů na nové produkty a služby.

Přizpůsobení zákaznických prostředí: Přizpůsobte obsah a doporučení na míru a podpořte tak věrnost a zapojení.

Posílení řízení dat pro transformaci AI

Všechny firmy mají zásady a procesy, kterými se řídí používání dat. Rámce řízení dat mívají různou vyspělost a ucelenost, ale jen některé z nich jsou plně optimalizované pro AI. Mnoho osvědčených postupů při řízení dat zůstává stejných, například zajištění přesnosti a konzistence dat, ale jiné aspekty je zapotřebí upravit, aby bylo možné naplno využít investice do AI. Pojdme se podívat na několik zásadních oblastí.

Viditelnost dat

Podrobné znalosti toku dat v systémech AI umožňují najít a zmírnit neoprávněné nebo nevhodné používání. Tato informovanost pomáhá podporovat zabezpečení a dodržování předpisů, čímž se chrání citlivá data, s nimiž se dá maximalizovat hodnota AI.

Obvyklé řízení dat se zaměřovalo na znalost, kde se data nacházejí, a na řízení přístupu. AI se však stále více začleňuje do firemního provozu, proto musí řízení dat udržovat krok s měnícími se požadavky na zabezpečení.

Například při uvádění značně citlivého produktu teď musí řízení zahrnovat i správu obsahu generovaného AI. Musí se zajistit, že dokumenty, komunikace a poznatky související s projektem, které AI vytváří, jsou v bezpečí. To znamená implementovat ochranné mechanismy, aby jen autorizovaní členové týmu měli přístup k AI a mohli ji využívat k analýze nebo vytváření souhrnů informací o projektu.

Kromě toho můžou organizace správou zpracovávání dat a objemů úložiště lépe řídit provozní náklady související s AI.

Kvalita dat

AI zvyšuje důležitost velmi kvalitních dat, protože jejich nízká kvalita má přímý vliv na výsledky AI. Při zavádění nástrojů s AI, které se mají dotazovat na firemní data, je nutné zajistit, že jsou data aktuální a důvěryhodná. Zrovna tak důležité je porozumět původu a kvalitě dat, která vaše týmy používají k vytváření svých vlastních modelů a aplikací s AI. Pravidelné audity dat, přísné ověřovací procesy a aktivní správa pomáhají zajistit integritu dat. Když se organizace budou soustředit na tyto oblasti, můžou s AI dosáhnout spolehlivých výsledků, které podpoří lepší rozhodování a inovace.

Správa uživatelů

S AI uživatelé pracují s daty sofistikovanými způsoby. Komunikují se systémy AI, jako je Microsoft 365 Copilot, prostřednictvím výzev v přirozeném jazyce. Když bude mít AI zavedeny ochrany a oprávnění, může získávat přístup k relevantnímu kontextu z dat – například souborů, chatů a e-mailů – spolu s externími zdroji prostřednictvím modulů plug-in a následně vygenerovat odpověď.

Je nezbytně důležité monitorovat data používaná v těchto procesech, aby bylo jisté, že AI bude poskytovat správné odpovědi zakládající se na skutečnostech. Zajištění transparentnosti prostřednictvím poznámek pod čarou nebo odkazů na původní zdroje pomáhá uživatelům ověřovat informace, snížit riziko zneužití dat a ověřovat dodržování regulačních předpisů.

Dodržování předpisů a eDiscovery

Příchod AI přináší nové problémy s dodržováním předpisů a eDiscovery (zpracovávání dat pro právní případy), obzvláště při správě dat generovaných AI a přizpůsobování se měnícím se zákonným požadavkům. Aktualizace rámců řízení dat tak, aby řešily tyto problémy, znamená vyvinout zásady zabývající se obsahem vygenerovaným AI, které například zajistí sledování, kategorizaci a bezpečné ukládání dokumentů nebo komunikace vytvořených AI. Může být například zapotřebí aktualizovat zásady, aby e-maily nebo zprávy generované AI byly označeny a správně archivovány pro budoucí potřebu.

Zlepšení schopností eDiscovery by znamenalo integrovat nástroje s AI, které dokáží vyhledávat a identifikovat obsah generovaný AI na nejrozličnějších platformách. Například během právního vyšetřování musí nástroje eDiscovery dokázat najít a získat konkrétní dokumenty generované AI, shrnout příslušnou komunikaci a poskytovat srozumitelné záznamy pro audit, které prokáží dodržování předpisů. Aktualizací těchto schopností můžou organizace lépe spravovat data během právních auditů a šetření, čímž se zajistí, že všechny relevantní informace vygenerované AI budou přístupné a obhajitelné u soudu.

Zabezpečení dat

Zabezpečení provozu řízeného AI by mělo zahrnovat principy Zero Trust (nulové důvěry) na úrovni identit, což minimalizuje riziko neoprávněného přístupu. Pravidelné aktualizace koncových bodů, včetně zařízení a aplikací, omezují nedostatky v zabezpečení, kterých by šlo zneužít. Povědomí o nástrojích s generativní AI, které se v organizaci používají, umožňuje blokovat neschválené nebo nezabezpečené aplikace, což pak na oplátku brání možnému narušení zabezpečení. Když se omezí přístup k nástrojům s AI a datům jen na důvěryhodný personál, můžou organizace dosáhnout větší integrity dat a chránit své operace AI před možnými hrozbami.



Co je Zero Trust (nulová důvěra)?

Zero Trust (nulová důvěra) je model zabezpečení, který se zaměřuje na ověřování každého požadavku, jako by přišel z nedůvěryhodné sítě. Namísto předpokladu, že všichni za firemním firewallem jsou v bezpečí, tento přístup zavádí princip „nikdy nedůvěřuj, vždy ověřuj“.

Principy Zero Trust (nulová důvěra)

Explicitní ověřování: Požadavky vždy ověřujte a schvalujte na základě všech dostupných datových bodů.

Použití přístupu s nejnižšími možnými oprávněními: Omezte přístup uživatelů zásadami „just-in-time“ a „just-enough-access“ (JIT/JEA), adaptivními zásadami založenými na riziku a ochranou dat.

Předpoklad narušení: Omezte škody, spravujte přístup, zajistěte šifrování a používejte data, s nimiž detekujete hrozby a posílíte obranu.

Role správy dat v transformaci AI: Původ, kvalita a spolehlivost

Když organizace zavádějí AI, která má pomáhat s obchodním rozhodováním, musejí zajistit, že tyto systémy dokáží poskytovat správné a spolehlivé výsledky. AI musí poskytovat odpovědi, které se zakládají na datech, jsou dostupné, konzistentní a dobře zdokumentované.

Správa dat podporuje důvěryhodnou AI tím, že zavádí zásady řízení, které sledují původ dat, kontrolují jejich kvalitu a zajišťují jejich spolehlivost a přesnost. Tyto postupy utvářejí základ pro systémy AI, které přinášejí spolehlivé poznatky a umožňují se rozhodovat na základě informací a s jistotou.

Rodokmen dat: Porozumění původu a změnám informací

Rodokmen dat sleduje, kudy v organizaci se přenášejí data. Dokumentuje původ, transformace a cíle dat. Pro firmy založené na AI je pochopení rodokmenu dat stěžejní hned z několika důvodů:

- **Transparentnost:** Informace o tom, odkud data pocházejí a jak se mění, pomáhají potvrdit přesnost výstupů generovaných AI a zajišťují dodržování regulačních předpisů tím, že je z nich zřetelná historie dat.
- **Sledovatelnost:** Rodokmen dat umožňuje organizacím vystopovat chyby nebo nekonzistence zpět k jejich zdroji, což zjednodušuje řešení problémů a opravu dat.
- **Analýza dopadů:** Srozumění s tím, jak se data využívají v nástrojích s generativní AI, pomáhá posoudit možný dopad změn ve zdrojích dat nebo metodách zpracovávání na přesnost výstupů a hospodářské výsledky.

Kvalita dat: Kvalita určuje hodnotu odpovědí AI

Kvalita dat má přímý vliv na spolehlivost výstupů AI. Vysoce kvalitní data poskytují modelům AI kontext, s nimiž můžou poskytovat správné a hodnotné reakce na vstupy uživatelů. Mezi hlavní aspekty kvality dat patří:

- **Přesnost:** Data musí správně korelovat se skutečným stavem.
- **Úplnost:** Všechna potřebná data musí být tam, kde jsou očekávána, a žádná nesmí chybět.
- **Konzistence:** Data musí být konzistentní ve všech systémech i v průběhu času.
- **Aktuálnost:** Data musí být aktuální a dostupná ve chvíli, kdy je jich zapotřebí.

Spolehlivost dat: Zajištění důvěryhodných dat

Spolehlivost dat znamená, že data konzistentně splňují standardy kvality a jsou k dispozici ve chvíli, kdy je to třeba. Ve firmách založených na AI jsou spolehlivá data stěžejní při utvrzování důvěry v nástroje AI a v rozhodnutí, která se na informacích z nich zakládají. K zajištění spolehlivosti dat patří:

- **Redundance dat:** Implementace zálohovacích systémů, které předcházejí ztrátě a zvyšují dostupnost.
- **Pravidelné zálohy:** Časté vytváření záloh pro ochranu před poškozením nebo ztrátou dat.
- **Monitorování a upozornění:** Nastavení monitorovacích systémů pro detekci a upozornění zúčastněných stran na problémy s daty v reálném čase.
- **Plány obnovení po havárii:** Vývoj a testování plánů, které rychle obnoví data a provoz po narušení.

Vztah mezi řízením, zabezpečením a odpovědnou AI

Řízení dat a zabezpečení společně utvářejí základ pro odpovědné používání AI. Vysoce kvalitní zabezpečená data zajišťují, že AI bude fungovat eticky a efektivně. K hlavním oblastem, které je zapotřebí vyhodnotit, patří klasifikace dat, řízení přístupu, šifrování, reakce na incidenty a dodržování regulačních předpisů.

Kategorizace dat

Klasifikace dat je stěžejní součástí při stanovování, jak nástroje s AI mají zpracovávat citlivé informace. Obvykle jsou data a schůzky klasifikovány jako obecné, důvěrné nebo vysoce důvěrné. Správná klasifikace zajišťuje, že AI bude mít přístup jen ke vhodným informacím. Sníží se tím riziko odhalení citlivých dat neautorizovaným uživatelům.

Chybná klasifikace může na druhou stranu vést k tomu, že AI bude zpracovávat data, která by měla být omezena. Výsledkem jsou bezpečnostní incidenty nebo problémy s dodržováním předpisů. Efektivní řízení dat, ať už prostřednictvím automatizovaných nástrojů, nebo zásad pro koncové uživatele, zajišťuje správnou klasifikaci dat, ochranu citlivých informací a podporu schopnosti AI doručovat spolehlivé výstupy přesně podle předpisů.

Řízení přístupu

Toto řízení reguluje, kdo může získat přístup k datům relevantním pro AI a které aplikace nebo identity budou mít oprávnění pracovat s těmito daty. Slabé řízení přístupu může vést k neautorizovanému odhalení citlivých informací, navýšení rizika narušení a ke zneužití.

Řízení dat má stěžejní roli ve vynucování těchto mechanismů, protože omezuje přístup k datům na autorizované zaměstnance a konkrétní aplikace. Tím je zajištěná správná manipulace s citlivými daty. Nejenže se tak chrání integrita dat, ale navíc se tím zajišťuje, že systémy AI budou pracovat se zabezpečenými, důvěryhodnými datovými sadami, což zlepšuje jejich spolehlivost a soulad s předpisy.

Šifrování

Šifrování, kterým se zabezpečují data před zachytáváním a neoprávněnou manipulací, pomáhá zajistit, že nástroje s generativní AI můžou podložit své odpovědi správným kontextem – například daty, soubory, chaty a e-maily souvisejícími s prací – bez rizika úniku dat.

Zásady řízení dat můžou stanovit robustní postupy šifrování, které ochrání data v celém jejich životním cyklu. Tento přístup zajišťuje, že nástroje s AI můžou doručovat spolehlivé odpovědi a zároveň udržovat data v bezpečí a zachovávat důvěryhodnost.

Reakce na incidenty

Citlivá data organizace můžou být odhalena v incidentech, ve kterých figurují nástroje s generativní AI, s nimiž lze získat neautorizovaný přístup k souborům, e-mailům nebo jiným firemním datům, které tyto systémy používají ke generování odpovědí.

V těchto scénářích je zásadní mít k dispozici aktivní plán reakcí na incidenty. Bez takového plánu organizace riskují nejen odhalení citlivých dat, ale také to, že budou spoléhat na kompromitované výstupy z AI. K řízení dat patří generování podrobných protokolů o odpovědích, s nimiž se dají rychle řešit incidenty, minimalizovat jejich dopad a zachovat spolehlivost systému AI.

Dodržování předpisů

Aplikace AI musí dodržovat regulační předpisy, například GDPR nebo CCPA, kterými se řídí ochrana dat a osobních údajů. Jejich nedodržování může vést k nákladným pokutám a narušení důvěry. Kromě toho je nezbytné vědět, kde nástroje s AI zpracovávají data, protože mnoho bezplatných nástrojů může data zpracovávat globálně nebo mimo obvyklá úložiště vaší společnosti. Řízení dat zajišťuje, že aplikace s AI nejenže nevybočí z právního rámce, ale zároveň budou uchovávat data v adekvátních hranicích služeb a odpovídat standardům dodržování předpisů ve vaší organizaci. Tento přístup podporuje etické používání AI a pomáhá vybudovat důvěru v technologii AI.



4

Aktualizace rámce pro řízení dat na podporu zavedení AI

V proměnlivém prostředí AI je důležité identifikovat konkrétní oblasti stávajícího rámce řízení dat, které by mohly vyžadovat větší pozornost. Není zapotřebí přepracovávat celý rámec, můžete se zaměřit na oblasti, které se s největší pravděpodobností změní, a nasměrovat své úsilí tam, kde nejvíce přispěje k hodnotě AI a zajistí, že vaše data zůstanou ochráněna a v bezpečí. Tady je několik zásadních poznatků na zvážení:

Přizpůsobení zásad a postupů

K AI patří nové způsoby shromažďování dat, zpracovávání a používání. Aktualizace zásad pro data dokáže řešit relevantní požadavky na ochranu osobních údajů, dodržování regulačních předpisů a etické používání. Například požadavek na anonymizaci dat v konkrétních případech dokáže ochránit osobní údaje, díky čemuž bude bezpečnější je používat v průběhu životního cyklu AI.

Role a odpovědnosti

Je nezbytné začlenit připravenost na AI do všech rolí, které se zabývají řízením dat. Zaměstnanci znalí požadavků na data pro AI mohou pracovat jako správci, kteří podpoří kvalitu dat a dodržování předpisů. Spolupráce mezi různými funkčními celky, například týmy pro právní záležitosti, IT a datové vědy, dokáže pomoci efektivněji řešit problémy související s AI.

Prizpůsobení standardům a definicím pro data

Standardizování datových formátů, definic a metrik kvality zjednodušuje implementaci zásad, kterými se řídí používání nástrojů s AI v organizaci. Zřetelné standardy dat usnadňují rozhodování, na základě kterých datových sad můžou nástroje s AI vyvozovat obchodní kontext a která data uživatelé můžou nahrávat k analýze. Tím se zajišťuje, že aplikace s AI používají nejrelevantnější a nejdůvěryhodnější data. To na oplátku zvyšuje jejich efektivitu a zároveň podporuje dodržování předpisů pomocí zásad organizace.

Neustálé zlepšování

Řízení dat je průběžný proces, obzvláště s AI. Pravidelné audity a aktualizace rámce řízení dokáží pomoci přizpůsobit se novému vývoji AI a změnám v regulačních předpisech. Samotná AI se dá používat ke kontrole a vylepšení postupů řízení. Můžou se tak najít nedostatky a navrhnout zlepšení. Takový aktivní přístup vylepšuje dodržování předpisů a efektivitu spolu s tím, jak se AI vyvíjí.

Nástroje a techniky pro efektivní řízení dat

Soulad s obchodními cíli:

Ujistěte se, že vaše strategie řízení dat podporuje cíle organizace. Budete se tak moci lépe rozhodovat a zlepšit efektivitu.

Automatizace rutinních úkolů:

Na opakované úkoly, například klasifikaci dat a řízení přístupu, můžete použít automatizaci, která omezí lidské chyby a zvýší zabezpečení.

Zajištění vysokých standardů přesnosti: Používejte ověřovací a čistící nástroje, které podpoří integritu dat v průběhu času.

Školení uživatelů: Nabízejte školení k nástrojům a postupům řízení dat, aby nedocházelo k nesprávnému zacházení s daty a bylo zajištěno dodržování zásad.

Provádění pravidelných auditů:

Pravidelně kontrolujte postupy s daty a ujišťujte se, že nezůstávají pozadu za změnami v regulačních předpisech a organizaci.

Závěr

Efektivní řízení dat pro přípravu na AI s Microsoftem 365

Odpovědné používání AI vyžaduje robustní řízení dat. Efektivní řízení dat zajišťuje jejich dostupnost, přesnost a zabezpečení, což umožňuje AI doručovat spolehlivé poznatky a podporovat inovace. Upřednostňování kvality dat, dodržování předpisů a zabezpečení vylepšuje funkce AI, podporuje lepší rozhodování a pomáhá udržet si konkurenční výhodu.

Microsoft 365: Podpora připravenosti na AI

Microsoft 365 nabízí špičkové nástroje pro produktivitu s integrovanými nástroji pro klasifikaci, řízení a ochranu dat. Tyto funkce podporují rámec řízení dat, se kterým budete moci, až budete připraveni, snadněji zavést AI s jistotou. Microsoft 365 vám pomůže zajistit:

- **Kvalitu dat:** Podpoří přesnost a spolehlivost pro výstupy AI.
- **Dodržování předpisů:** Dodržuje regulační předpisy a snižuje právní rizika.
- **Zabezpečení Zero Trust (nulová důvěra):** Chrání citlivé informace před neoprávněným přístupem, úniky a kybernetickými hrozbami.

Seznamte se s ucelenými nástroji pro produktivitu vylepšenými o možnosti AI a robustní ochranu, které vaši organizaci pomůžou pracovat efektivně a bezpečně.



Seznamte se s Microsoftem 365