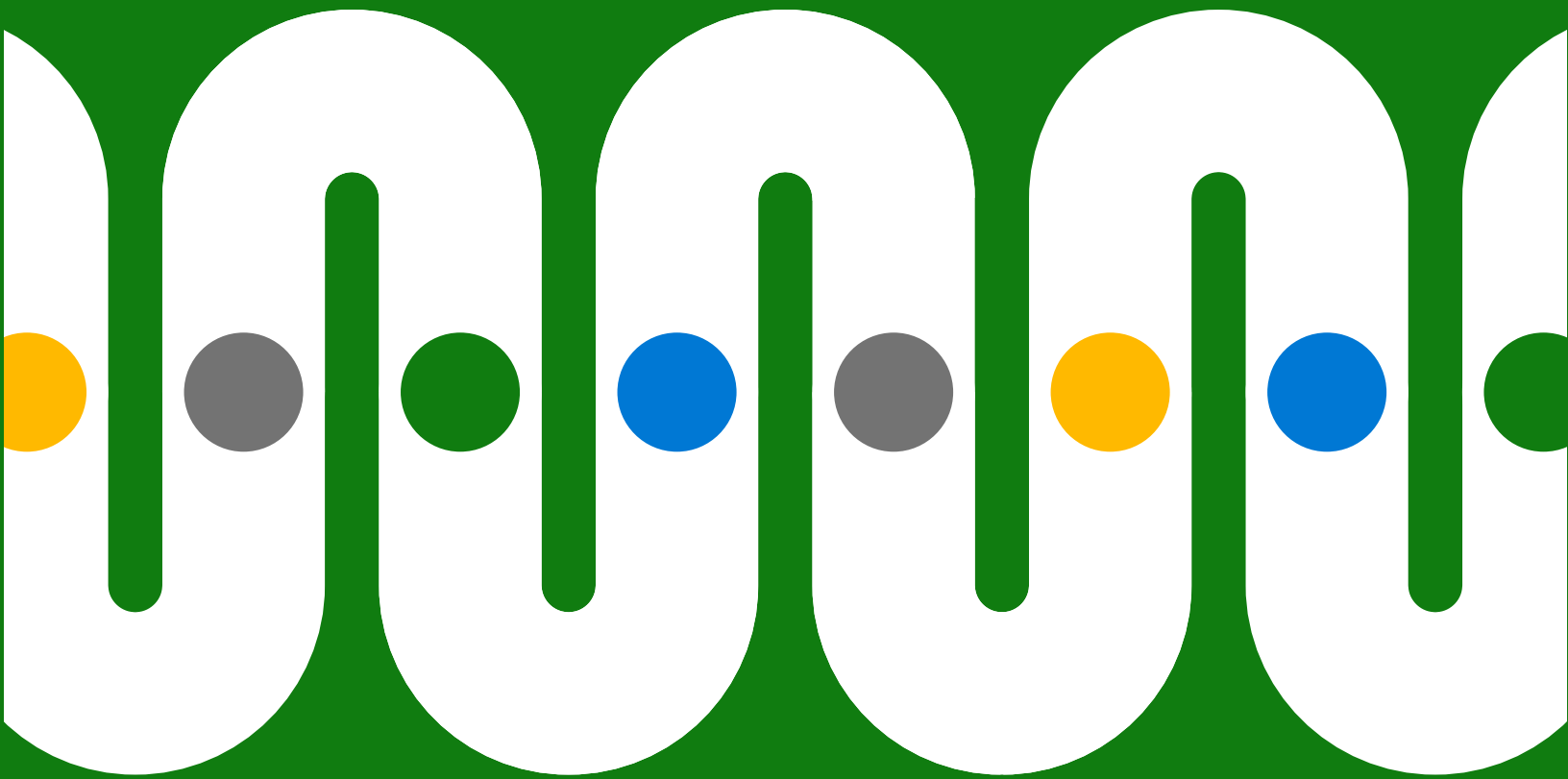
Microsoft Security

Tre steg för att skydda dina data under hela livscykeln



Innehåll

En undersökning av beslutsfattare inom regelefterlevnad visade att 95 procent var bekymrade över problem med dataskyddet.[2]

Inledning

Organisationer har upplevt en enorm ökning av sitt digitala fotavtryck på grund av hybridarbetet, som sträcker sig långt utanför det traditionella kontoret.

Det har lett till större datafragmentering och mer exfiltrering – där allt kompliceras genom alltfler appar, enheter och platser. Många medarbetare har också bytt roller i sitt sökande efter ett mer givande och flexibelt arbete. Detta har gjort utmaningarna ännu större, vilket skapar nya blinda fläckar inom dataegendomar som ständigt växer.[1]

Alla dessa faktorer har inneburit att CIO:er och CISO:er fått ompröva sin syn på informationsskydd. I en återkommande undersökning som genomförs i USA av över 500 beslutsfattare inom regelefterlevnad var nästan alla (95 procent) bekymrade över problem med dataskyddet.[2]

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

[2] En undersökning genomförd av Vital Findings i september 2021 av 512 beslutsfattare i USA inom regelefterlevnad, på uppdrag av Microsoft.

IT- och säkerhetsteam vill hitta nya och bättre sätt att hantera hela datalivscykeln i såväl lokala miljöer som flermolns- och hybridmolnsmiljöer. Den här helhetssynen omfattar tre viktiga steg:

Steg 1: Identifiera data

Ta reda på var dina data finns, vilken typ av data det är och hur de används eller delas

Steg 2: Klassificera data

Klassificera och märk dina data så att du vet vilka policyer och riskreducerande åtgärder som ska tillämpas

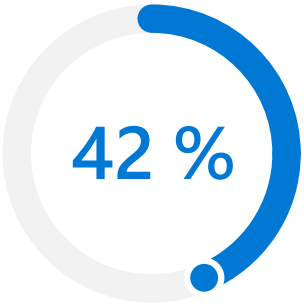
Steg 3: Förhindra dataförluster

Hitta en balans mellan riskreducering och flexibilitet för din personal med intelligent identifiering och kontroll

Vad är målet med denna strategi? Att täppa till luckorna och minimera risken utan att ge avkall på produktiviteten.

Steg 1

Identifiera data



På frågan hur mycket av deras data som är ”mörka”, uppgav 42 procent av organisationerna att det var minst hälften.[3]

Dessa ”dolda” data kan anta många former – från e-postbilagor och kundsamtalsposter till maskinloggar och videofilmer.

Om du inte kan identifiera dina data – var de finns, vilken typ av data det rör sig om eller hur de används eller delas – är det omöjligt att tillämpa rätt policyer eller skydd.

Moderna organisationer genererar kontinuerligt stora mängder data. Det handlar inte bara om dokument, e-postmeddelanden och andra typer av meddelanden, utan allt från säkerhetsmaterial till geolokaliseringsuppgifter. Situationen blir inte bättre av att informationen sprids på appar, enheter och lagring – både lokalt och i molnet.

Det kan vara svårt att identifiera alla dessa data, och 42 procent av organisationerna uppger att minst hälften av deras data är ”mörka”.[3] Det vill säga informationen som samlas in är okänd eller används inte i verksamheten. Ibland blir data mörka när den medarbetare som skapat dem byter projekt eller roll. Ofta finns det helt enkelt inga system för att identifiera data vid tidpunkten då de skapas eller ändras.

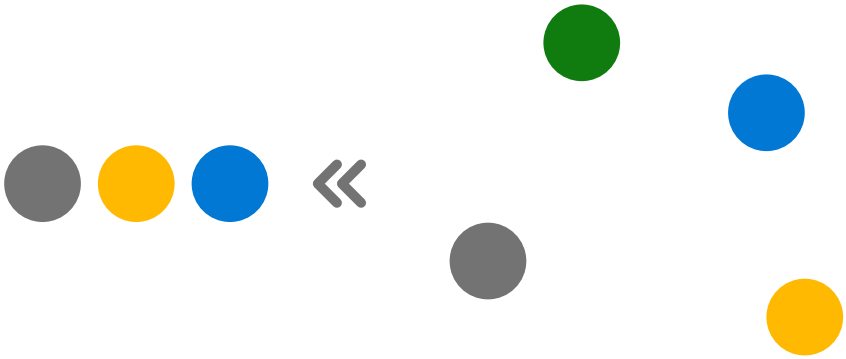
[3] ”2022 State of Data Governance and Empowerment Report”, Enterprise Strategy Group. Juli 2022.

Vill du skapa ett komplett identifieringsarbetsflöde på en och samma plattform?

Läs mer om dataidentifiering i Microsoft Purview på **Microsoft.com**.

Denna utmaning kommer bara bli större. Mängden nya data som skapas, samlas in, replikeras och förbrukas förväntas mer än fördubblas fram till år 2026, och företagsdata växer mer än dubbelt så snabbt som konsumentdata.[4]

Artificiell intelligens (AI) och maskininlärning (ML) kan underlätta genom att de identifierar känsliga data – till exempel e-postadresser, tillståndsdata, kreditkortsnummer eller immateriell egendom – och klassificerar dem automatiskt. AI och ML kan också öka noggrannheten i klassificeringen och granska data retroaktivt. Dessa identifieringsprocesser kan omfatta hela dataegendomen – bevara, samla in, analysera, granska och exportera innehåll var det än finns, i alla moln.



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

Steg 2

Klassificera data

Både klassificeringar och policyer måste följa med när data flyttas.

Säg att en medarbetare kopierar kreditkortsnummer från ett Microsoft Word-dokument till ett Excel-kalkylblad. Då bör klassificeringen och policyerna tillämpas automatiskt på båda dokumenten.

Med korrekt dataklassificering kan du fastställa rätt policyer och riskreducerande åtgärder för att säkerställa att olika typer av data inte oavsiktligt eller avsiktligt missbrukas eller används utan behörighet. Kryptering och vattenstämplar kan skydda data ytterligare – oavsett om de är i vila, under överföring eller används.

Men klassificering och policyer måste följa med data när de flyttas i organisationen. Märknings- och skyddspolicyer kan inte begränsas till enskilda dokument, de måste omfatta hela den digitala egendomen – från lokala till molnbaserade lagringsutrymmen, SaaS-appar (programvara som tjänst) och operativsystemspecifika appar.

Traditionella klassificeringsmetoder medför väldigt mycket manuellt arbete, och det finns risk för fel eller oavsiktliga förbiseenden av viktiga data. Inbyggda och träningsbara klassificerare kan underlätta automatiseringen av den här processen, och med en integrerad lösning kan administratörer hantera policyer för alla system från en enda central plats.

Vill du kunna hantera och skydda känsliga data i hela miljön?

Läs mer om dataklassificering och dataskydd i Microsoft Purview på **Microsoft.com**.

Steg 3

Förhindra dataförluster

När du har identifierat och klassificerat dina data kan du använda lösningar för dataförlustskydd (DLP, Data Loss Prevention) för att tillämpa policyer för komplett skydd som mildrar hot som mörka data och datautfiltrering. Nuvarande och tidigare medarbetare kan då inte – avsiktligt eller oavsiktligt – dela, exponera eller överföra känsliga data utan behörighet.

Intelligenta DLP-lösningar använder sammanhanget för att göra en avvägning mellan flexibilitet och att stoppa högriskåtgärder. En person kan till exempel fortsätta med en åtgärd efter att ha blivit påmind om potentiella risker och vilka policyer som tillämpas. På så sätt går det att skydda känsliga data och samtidigt utbilda användarna till att bättre förstå vilka risker som finns.

DLP-lösningar skyddar immateriella rättigheter och andra viktiga affärsdata, samtidigt som de också förbättrar efterlevnaden av förordningar som GDPR (allmänna dataskyddsförordningen), HIPAA (Health Information Portability and Accountability Act) och CCPA (California Consumer Privacy Act).

En heltäckande DLP-metod upprätthåller konsekventa policyer för hela organisationen, vilket skyddar den svagaste länken under hela datalivscykeln.

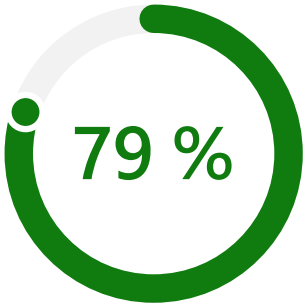
DLP-policyn kan förhindra åtgärder som inte uppfyller kraven på regelefterlevnad.

Om en medarbetare till exempel försöker ladda ned ett kalkylblad med kreditkortsnummer till ett flashminne eller ladda upp det för lagring i molnet, kan DLP-policyn identifiera att aktiviteten bryter mot efterlevnadskraven och stoppa den.

Vill du ha intelligent identifiering och kontroll av känslig information?

Läs mer om dataförlustskydd i Microsoft Purview på **Microsoft.com**.

Klistra inte på dataskyddet på utsidan. Bygg in det.



En undersökning av beslutsfattare inom regelefterlevnad visade att 79 procent hade köpt flera produkter inom regelefterlevnad och dataskydd.

En majoritet hade köpt tre eller fler.[5]

Många organisationer har testat att ”klistra på” informationsskydd, genom att använda flera olika lösningar som hanterar olika faser av datalivscykeln. Men då måste organisationens team som arbetar med säkerhet, datastyrning, regelefterlevnad och juridik tråckla ihop ett lapptäcke som ofta är ineffektivt och tar mycket resurser i anspråk.

Med en ”inbyggd” metod kan du täppa till luckorna genom att samordna dataidentifiering, dataklassificering och DLP. Med en integrerad lösning är det enklare att hantera och genomdriva policyer från en central plats. Det krävs också mindre utbildning av användarna, eftersom de får ta emot policymeddelanden på ett välbekant sätt, inbyggt i apparna.

[5] En undersökning som genomfördes av MDC Research i februari 2022 i USA av 200 beslutsfattare inom regelefterlevnad (n=100 599–999 medarbetare, n=100 1000+ medarbetare), på uppdrag av Microsoft.

En inbyggd, integrerad lösning: Microsoft Purview

Med hjälp av Microsoft Purview kan du möta utmaningarna med dagens decentraliserade och dataintensiva arbetsplatser. Med en omfattande uppsättning lösningar kan du styra, skydda och hantera hela dataegendomen.

Mer än bara styrning.

Läs mer om hur du kan skydda dina data med Microsoft Purview >

Är du intresserad av ett specifikt område inom dataskydd? Få mer detaljerad information om hur Microsoft Purview kan hjälpa dig med följande:

Dataidentifiering >

Dataklassificering och dataskydd >

Skydd mot dataförlust >

Microsoft Security