Microsoft

6 steg för en holistisk säkerhetsstrategi med Microsoft 365

Innehållsförteckning

6 steg för en holistisk säkerhetsstrategi med Microsoft 365

Att skydda sina data och system är högsta prioritet för dagens företag och organisationer. En utmaning som blir svårare för varje dag i takt med att attackerna blir mer sofistikerade och medarbetarna använder allt fler olika enheter och program. I dag flödar data in och ut i verksamheten på långt fler sätt än för bara några år sedan.

Dagens chefer måste balansera de här utmaningarna mot behovet av samarbete, innovation och tillväxt. Det behövs en mångsidig syn på säkerheten och metoder som skyddar alla slutpunkter, snabbt kan identifiera tidiga tecken på intrång och kan reagera innan skadan inträffar. Oavsett hur starkt försvar du har så räcker det inte längre med preventiva åtgärder. Du behöver även vara redo för ”förmodade intrång” och ha metoder för identifiering och svarsåtgärder.

De flesta CISO:er (Chief Information Security Officer) har nu riskhantering som ett ansvarsområde. Där ingår att minimera potentiella skador från allt mer sofistikerade attacker samtidigt som färre medarbetare måste skydda allt fler användare, enheter, program, data och infrastrukturdelar.

Dagens CISO:er behöver ett flexibelt ramverk för säkerheten, anpassat till dagens digitala arbetssätt samt en heltäckande strategi som är inbyggd i teknik, processer och utbildning. I den här e-boken berättar vi om strategier och beprövade metoder från CISO:er som genom att se säkerhet som en av företagets hörnstenar säkerställt framgångar för affärerna.

> *Du måste hela tiden vara förberedd. Och det innebär även att du hela tiden måste tänka på säkerheten i driften.*
>
> **Satya Nadella,**
> *Microsoft CEO*

Microsoft 365 Enterprise är en komplett och intelligent lösning som inkluderar Office 365, Windows 10 Enterprise och Enterprise Mobility + Security, så att alla medarbetare kan vara kreativa och samarbeta säkert.

Microsoft 365 har inbyggda säkerhetslösningar från tredje part för skräppost, kryptering, hantering av mobila enheter och andra utmaningar. I Microsoft Intelligent Security Graph används avancerad analys på de miljarder med hotsignaler vi tar emot i våra produkter, såsom Exchange, Windows och Azure. Det här gör att vi kan leverera djupare insikter som gör att din organisation snabbt kan identifiera och reagera på attacker. Den här typen av säkerhet används på alla nivåer i Microsoft 365 – både fysiskt och i nätverket, infrastrukturen och programmen. Det gör att du kan skydda dina medarbetare, era data och enheter utan att störa produktiviteten.

01 Integrering och snabba motåtgärder

Hotaktörerna har utvecklats och gått från tillfälliga "smash-and-grab"-attacker till att försöka ta sig in i system och bli kvar där en längre tid. Angriparna använder sig nu av en mängd olika tillvägagångssätt och allt fler verktyg och tekniker: att stjäla inloggningsuppgifter, installera skadlig programvara som undgår upptäckt genom att radera sig själv, modifiera interna processer och dirigera om nätverksdata, bedrägerier på sociala medier och direktangrepp på enskilda anställdas mobiltelefoner och privata enheter.

Dagens företag och organisationer använder så klart allt fler säkerhetsverktyg som svar på de här hoten. De här lösningarna är ofta inriktade på ett visst problem och fungerar sällan tillsammans. Många använder inköpta instrumentpaneler, konsoler och loggar. Eftersom lösningarna inte är integrerade blir det svårt att få en helhetsbild av systemet och att snabbt kunna prioritera olika hot. Det blir dessutom ännu svårare om det gäller resurser både i molnet och lokalt. Allt det här gör att en attack kan förbli oupptäckt i omkring 140 dagar.[1]

[1] "Threat Landscape: By the Numbers." FireEye. 2016.
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Infographic-mtrends2016.pdf

En genomsnittlig stor organisation använder 75 olika säkerhetsprodukter.[2]

Den traditionella metoden är att korrelera information från en mängd olika verktyg med hjälp av SIEM-lösningar (Security Information and Event Management). För detekteringen krävs dock fortfarande att IT bearbetar loggar och data för att sedan prioritera och undersöka incidenter. Insamlingen och sammanställningen av data är komplicerad, och eftersom det inte ges någon enhetlig vy blir det svårare med motåtgärder och administration. Allt eftersom det blivit viktigare med snabb detektering och snabba motåtgärder så har följande regelverk växt fram:

- Skaffa dig en helhetsbild av hela nätverket, inklusive moln- och hybridmiljöer.
- Skapa ett ekosystem med säkerhetsprodukter och plattformar som kan integreras med varandra och ger insikter från en mängd olika plattformar.
- Samarbeta med teknikleverantörer som är aktiva och delar information inom säkerhetsbranschen.
- Kombinera datainsikter med information från säkerhetsanalytiker, forskare och hotjägare så att du kan bedöma och prioritera händelser ännu snabbare.

[2] Enligt Balaji Yelamanchili, Executive Vice President och General Manager för Enterprise Security Business, Symantec, som citeras i: Symantec. "Symantec Introduces New Era of Advanced Threat Protection." 27 oktober 2015. https://www.symantec.com/en/in/about/newsroom/press-releases/2015/symantec_1027_01

Microsofts lösningar för säkerhetshantering

Microsoft 365 ger dig insyn i och kontroll över din säkerhet, tack vare helhetssynen på säkerhet som omfattar allt från skydd vid ytterdörren och att skydda era data var de än är, till att identifiera och åtgärda attacker. Det här gör att du kan minska antalet verktyg som används samtidigt som era säkerhetsspecialister har den flexibilitet och frihet som behövs för att hantera specifika arbetsbelastningar.

Viktiga punkter

- **Bristen på integrering mellan olika säkerhetsprodukter gör det svårt för IT-avdelningen att snabbt kunna identifiera och åtgärda olika hot.**
- **Välj produkter som är utformade för att integreras med andra.**

02

Behovet av säkerhetskontroller när antalet slutpunkter bara växer

Företag idag vet att dataintrång kan vara mycket kostsamma, samtidigt som det fortfarande är en stor utmaning att implementera tillräckligt med säkerhetskontroller för att få den insyn som behövs i hot och attacker. Dessutom måste de förhålla sig till en konsumentcentrerad IT-miljö där användarna inte längre bara jobbar på företagets hårt kontrollerade enheter, utan även förväntar sig att kunna arbeta var de än befinner sig oavsett enhet eller plattform. Och oavsett om IT godkänt just den lösningen eller ej.

Identitetsbaserade säkerhetsstrategier handlar om att knyta åtkomst till identiteter, så att organisationer kan sluta fokusera på enheter och tillämpa kontroller baserat på roll och behov, oavsett hur användaren ansluter. Autentiseringen och hanteringen av användare när de ansluter till företagstillgångar gör även att organisationer kan skydda sina data oavsett var de lagras, hur de används eller vilka de delas med.

Vi vill även ta upp två andra tekniker: IAM-lösningar (Identity and Access Management) och DLP-lösningar (Data Loss Prevention) inom mobilappshantering. Både minskar risken genom att åtkomsten till program och data skyddas både i företagsresurser och i molnet. IAM kan göra att användarna slipper hantera olika inloggningsuppgifter och att de får en enda identitet för åtkomst till både molnbaserade och lokala resurser. Molnbaserade IAM-system kan även omfatta hotinformation och analys från teknikleverantören så att du enkelt kan se onormala inloggningsbeteenden och vidta lämpliga åtgärder.

MFA (Multi-factor authentication) är ytterligare ett skyddslager där användarna både måste visa upp någonting de känner till (sitt lösenord) och någonting de har (sekundär autentisering via en enhet, fingeravtryck

eller ansiktsigenkänning). Andra kraftfulla metoder kan vara att basera åtkomst på användarrisk, enhetsrisk, programrisk eller platsrisk. Med de här funktionerna kan du automatiskt tillåta, neka eller begära MFA från en användare i realtid baserat på de principer du ställer in, så att säkerheten stärks vid organisationens ytterdörr.

I de här moderna verktygen får du även tillgång till förebyggande slutpunktssäkerhet. De bästa lösningarna hjälper dig att kryptera enheter på alla nivåer, från maskinvara till program, och de ger en heltäckande insyn i olika attacker. De mer avancerade verktygen har dessutom ett skyddslager som träder i kraft efter ett eventuellt intrång, som innehåller förslag på motåtgärder och insikter i liknande attacker samt inbyggda verktyg som snabbt kan blockera eller radera företagsdata, eller sätta dem i karantän.

Microsoft 365 fungerar tillsammans med den befintliga infrastrukturen och samlar IT-hanteringen av användare, enheter, appar, data och tjänster, så att din IT-avdelning kan minska antalet lösningar som används och spara pengar. Dessutom finns det stöd för hybridmiljöer så att du kan integrera molnbaserade och lokala lösningar.

Cyber Defense Operations Center: Så skyddar Microsoft sin plattform

I Microsoft Cyber Defense Operations Center (CDOC) samlas säkerhetsexperter från hela företaget för att skydda, identifiera och åtgärda säkerhetshot mot vår infrastruktur och våra tjänster i realtid.

Med en enklare och smartare säkerhetshantering får du insyn i och kontroll över din säkerhet

Nyckeln till framgång för en CISO handlar inte om att ha en enda konsol för allt, utan om integrering där den gör nytta. Du behöver inte alla punktlösningar för hantering av datapunkter när du ska skydda slutanvändarnas enheter och det växande nätverket. Med Microsoft 365 får du en intelligent säkerhetshantering med specialiserade kontroller som utgår från behoven hos dina säkerhetsteam, insyn där du behöver den och vägledning kring hur du kan stärka organisationens säkerhet. På så sätt kan du både ta del av den flexibilitet och frihet som behövs när du ska hantera säkerheten med inbyggda kontroller, och dra nytta av vår säkerhetsinformation och vägledning så att du kan stärka din säkerhet och skydda organisationen mot olika hot.

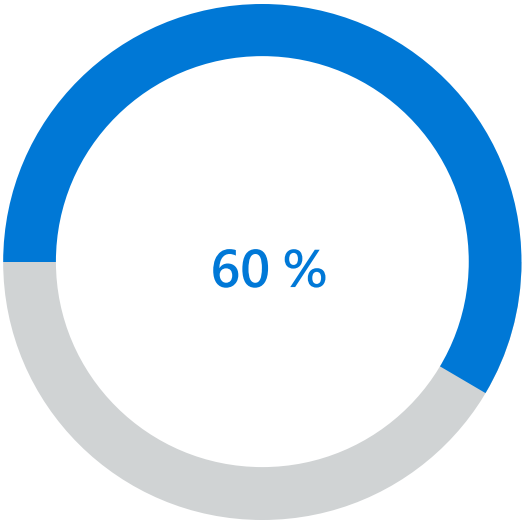
- Förstå ert säkerhetslandskap: ta reda på mer om det aktuella säkerhetstillståndet och riskerna för olika resurser i organisationen, så att du kan identifiera olika hot och åtgärda dem effektivt.

- Definiera vilken nivå av dataskydd ni behöver: skapa och anpassa konsekventa säkerhetsprinciper och aktivera kontroller som behövs i en intelligent säkerhetshantering.

- Håll dig uppdaterad med säkerhetsinformation: använd interna analyser, rekommendationer och vägledning till att stärka organisationens säkerhet.

Förbättra säkerheten med identitets- och åtkomstkontroller

Microsofts lösningar för identitets- och åtkomsthantering hjälper dig att skydda användarnas identiteter och styra åtkomsten till värdefulla resurser utifrån användarnas risknivå. Microsoft 365 Enterprise har skydd för identiteter (Windows Hello, Touch ID, Credential Guard, Conditional Access, Azure Active Directory), appar och data (Office DLP, Azure Information Protection, Cloud App Security) samt enheter (Device Guard, Intune).



60 procent av alla intrång beror på en utsatt slutpunkt.[3]

Microsofts lösningar för identitets- och åtkomsthantering

Lägg fokus på att skydda identiteter och information. Microsofts lösningar för identitets- och åtkomsthantering hjälper dig att skydda användarnas identiteter och åtkomsten till appar och data, samtidigt som våra lösningar för informationsskydd hjälper dig att skydda företagets information, var den än befinner sig, även när den förflyttas.

Viktiga punkter

- Upprätta kontroller för identitets- och åtkomsthantering
- 60 procent av alla intrång beror på en utsatt slutpunkt.[3]
- Med en identitetsinriktad säkerhetsstrategi flyttas fokus från att hålla reda på ett växande antal slutpunkter till att hantera användningen av företagsdata.
- De mer robusta slutpunktsskydden ger även insikter kring angriparens teknik efter ett eventuellt intrång.

[3] Ibid. Reed, 2017.

03 Hastighet och flexibilitet bland dagens hot

Hackare vet att alla organisationer har flera olika ingångar. De använder nätfiske, skadlig programvara och spionprogram, säkerhetsluckor i webbläsare och programvara, borttappade och stulna enheter, social manupilation och andra taktiker för att ta sig igenom din säkerhet. Du behöver hela tiden vara vaksam om du ska kunna ha överblick över de hot du känner till och samtidigt identifiera framtida svagheter.

Vissa verktyg kan hjälpa dig med en kontinuerlig säkerhet, men ibland kan det vara bättre med ett bredare angreppssätt. I traditionella verktyg ligger fokus på förebyggande funktioner, men det räcker inte längre idag. Organisationer måste förutsätta att intrång antingen redan har inträffat eller kommer att inträffa snart. Sedan måste de hitta sätt att avsevärt minska tiden det tar att identifiera ett sådant intrång och åtgärda det.

Den genomsnittliga stora organisationen måste hantera 17 000 varningar om skadlig programvara varje vecka.[4]

[4] Ponemon Institute. "The Cost of Malware Containment." Sponsored by Damballa. 2015. https://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

I många säkerhetsprogram används inbyggda analys- och maskininlärningsfunktioner till att ge insikter kring incidenter samt vilka aktiviteter och åtgärder angriparna utförde. Det här är dock fortfarande en analys av tidigare skeenden som kanske inte gör identifiering och återställning snabbare i framtiden. De mer avancerade säkerhets- och analyslösningarna använder sig av sådana insikter och agerar automatiskt för att förhindra och åtgärda liknande intrång, vilket minskar tiden till skademinimering avsevärt. Bakom de här lösningarna ligger en enorm mängd signaler och information, och när de kombineras med expertisen och kompetensen hos mänskliga experter kan de här lösningarna vara kraftfulla verktyg även mot snabba hotaktörer.

Säkerhetschefer bör samarbeta med ledningen och styrelsen om att etablera en acceptabel risknivå, och sedan balansera den mot säkerhetsbudgeten. Det finns ingen lösning som passar alla organisationer, men med ett riskhanteringsperspektiv kan du få hjälp att avgöra hur och var du ska investera enligt just din organisations behov.

Microsofts lösningar för skydd mot hot

Skydda er mot avancerade hot och återställ snabbt efter en attack.

Microsoft anser att skydd mot hot handlar om att organisationer själva ska kunna skydda sig mot avancerade cyberattacker. Dessutom ska de kunna få lösningar som identifierar misstänkta beteenden inom organisationen. Eftersom ingen säkerhetslösning heller är 100 % effektiv måste det finnas processer och verktyg för att snabbt kunna reagera på hot, minimera skador och begränsa effekterna av en attack.

Microsoft lösningar för skydd mot hot är en kombination av traditionella metoder som antivirus, och nya innovationer som UEBA (user and entity behavior analytics) och EDR (endpoint detection and response). Microsoft investerar både i att förebygga attacker samt att identifiera och åtgärda attacker när de har inträffat.

Viktiga punkter

- **Tänk på säkerheten som att du förutsätter ett intrång.**
- **Välj lösningar som minimerar tiden det tar att identifiera och åtgärda ett intrång.**
- **Använd riskhanteringsanalys till att avgöra var du ska investera.**

04 En säker flytt till molnet

Varje organisation har sin egen resa mot molnet. Krav på regelefterlevnad, lokala föreskrifter och andra utmaningar i migreringen innebär att alla organisationer inte är redo att flytta kritiska arbetsbelastningar till molnet.

Att flytta till molnet behöver inte innebära att ni helt lämnar befintliga system och processer. I en helt integrerad IT-hybridmiljö blir molnet en förlängning av ert datacenter och de principer ni använder för att styra det. Med en hybridstrategi för molnet får säkerhetschefer dessutom ett kontrollerat sätt att flytta till molnet. De kan flytta affärsfunktioner först när de känner sig säkra på att tjänsten erbjuder tillräcklig kontroll.

Molntjänstmodeller påverkar hur tjänsteleverantörer och kunder fördelar ansvaret sinsemellan. Det här innebär att CISO:er måste ta ställning i ett antal frågor när det gäller att ge upp en del av kontrollen i de lokala lösningarna för att kunna ta del av den starkare säkerheten hos en molnleverantör.

”Offentliga molnleverantörer kan erbjuda bättre säkerhet än vad ett litet eller till och med stort företag kan uppnå. Detta tack vare de investeringar som molnleverantören gör i att bygga upp och underhålla sin molninfrastruktur.”[5]

Tumregeln när det gäller säkerhet i molnet är ett delat ansvar. Molnleverantörer måste ha en förstklassig säkerhet och kryptering, men kunderna måste se till att de tjänster som köps in faktiskt är säkra, och att de säkerhetsprinciper som behövs även förlängs till de nya molnresurserna. Sök insyn när du planerar en molnmigrering: leverantörerna bör publicera detaljerad information om säkerhet, sekretess och regelefterlevnad i sina tjänster. De bör även producera granskningsrapporter och andra material som verifierar utfästelserna och hjälper dig att förstå var deras ansvar slutar och ditt eget börjar.

[5] Trotter, Paul. “Top Cloud Security Fears & How the C-Suite Is Tackling Them.” 20 maj 2015. http://www.cio.com/article/2924390/cloud-security/top-cloud-security-fears-and-how-the-c- suite-is-tackling-them.html

Frågor till din molnleverantör

Att bedöma olika molnleverantörer handlar inte bara om att välja en tjänst, utan vem ni betror era data med. Här är några viktiga frågor kring säkerhet och åtkomstkontroll:

- ✓ Skyddas mina data med stark säkerhet och förstklassig teknik?
- ✓ Använder ni er av designbaserad säkerhet och har vi kontroll över våra data i företagsmolnet?
- ✓ Investerar ni i robusta och innovativa efterlevnadsprocesser så att min organisation kan uppfylla våra efterlevnadskrav?
- ✓ Var lagras mina data, vem har tillgång till dem och varför?
- ✓ Utsätter sig molnleverantören för årliga granskningar av tredje part?
- ✓ Kommer molnleverantören att motsätta sig alla förfrågningar om spridning av kundernas personliga data som inte är juridiskt bindande? Följer molnleverantören gällande standarder för efterlevnad och regelverk i olika länder och på olika platser?

Det betrodda molnet

Individer och företag använder bara den teknik de kan lita på. Du kan flytta till molnet säkert när du har tillräcklig kunskap om din molnleverantörs säkerhet, sekretess, regelefterlevnad och transparens. Microsofts molntjänster är uppbyggda kring de här fyra principerna, och "Trusted Cloud Initiative" främjar en uppsättning riktlinjer, krav och processer som gör att vi kan erbjuda ett rigoröst stöd inom teknik, juridik och regelefterlevnad för våra molntjänster.

Nå avkastning snabbare med Microsofts molntjänster och FastTrack

FastTrack har redan hjälpt fler än 40 000 kunder att maximera avkastningen på sin investering, distribuera snabbare och underlätta införandet.

- Migrera e-post, innehåll och aktivera Microsoft 365-tjänster, inklusive vägledning kring bedömningar och åtgärder som hjälper dig att förbereda din infrastruktur för molnet
- Distribuera och hantera enheter säkert, inklusive enheter som kör Microsoft 365
- Gör företaget effektivare och uppmuntra medarbetarna att jobba på ett nytt, mer digitalt sätt.

Via programmet Fast Track erbjuder Microsofts ingenjörer er hjälp att migrera till molnet i er egen takt, och sätter er i kontakt med kvalificerade partnerföretag om ni behöver ytterligare tjänster.

Viktiga punkter

- Att flytta till molnet behöver inte innebära att du helt lämnar befintliga system och processer.
- Ett hybridmoln är ett kontrollerat sätt att migrera till molnet.
- När du utvärderar olika molnleverantörer bör du se till att de följer internationella standarder.
- Leta efter leverantörer som publicerar detaljerad information kring hur de driver sina tjänster och hanterar data.

05 Riskerna med skugg-IT

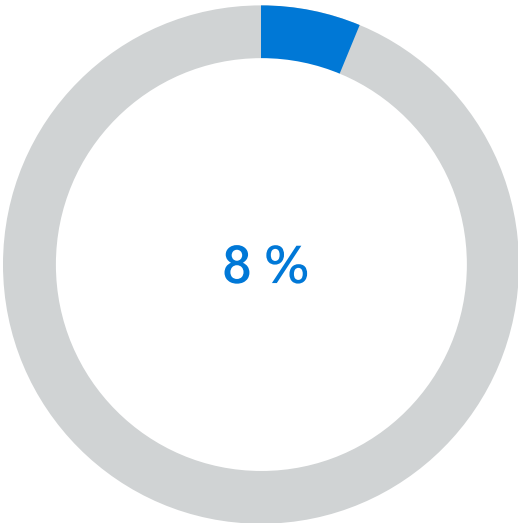
Även om din organisation inte använder molnbaserade lösningar så gör förmodligen dina anställda det. Den här trenden, som även kallas för skugg-IT, är mycket större än de flesta vet om. Faktum är att bara åtta av alla företag känner till omfattningen på sin skugg-IT,[6] och att antalet molntjänster som anställda på företag använder snabbt håller på att passera IT-avdelningarnas uppskattningar.

> *2022 kommer en tredjedel av alla framgångsrika attacker mot företag att göras via skugg-IT-resurser.*[7]
>
> Gartner's Top 10 Security Predictions 2016

Skugg-IT utsätter din organisation för enorma risker inom IT- och programhantering, säkerhet och regelefterlevnad.

[6] "Cloud Adoption Practices & Priorities Survey Report." Cloud Security Alliance. Januari 2015. https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf

[7] Gartner, Smarter With Gartner "Gartner's Top 10 Security Predictions 2016." 15 juni 2016. http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/



Endast 8 procent av alla företag känner till omfattningen av skugg-IT inom organisationen.[12]

Slutanvändare godkänner ofta regler och villkor utan att läsa dem, och utan att egentligen förstå vad det är de ger åtkomst till. Traditionella säkerhetslösningar för nätverk är inte utformade för att skydda data i SaaS-appar, och ger inte IT-avdelningen insyn i hur de anställda använder molnet.

Samtidigt är det ingen bra lösning att helt blockera skugg-IT, de anställda hittar alltid nya sätt att komma runt olika begränsningar. Onödigt stela kontroller motverkar innovation, står i konflikt med oplanerade och utmanande teknikkrav, hindrar produktiviteten och kan minska engagemanget och öka omsättningen hos den mest kompetenta medarbetaren.

I slutänden måste vi alla acceptera att skugg-IT är ett nytt normaltillstånd. När du låter slutanvändare och grupper använda de molnprogram de föredrar i sitt arbete ökar produktiviteten och innovationen främjas. Det första steget när det gäller att hantera riskerna och att underlätta den digitala transformationen som redan pågår på ditt företag är att skaffa insyn, kontroll och skydd mot hot i SaaS-skuggappar.

CASB:er (Cloud access security brokers) kan ge organisationer en detaljerad bild av hur medarbetarna använder molnet:

- Vilka molnappar använder de anställda?
- Vilka risker innebär de här apparna för organisationen?
- Hur används de här programmen?
- Vilken typ av data skickas till och delas från de här programmen?
- Hur ser trafiken ut när det gäller upp-/nedladdning?
- Förekommer det avvikelser i användarnas beteende, som omöjliga förflyttningar, misslyckade inloggningsförsök eller misstänkta IP-adresser?

Med bättre insyn i och kontroll över de här apparna och tjänsterna kan säkerhetschefer ta fram och genomdriva mer rimliga och effektiva SaaS-principer utan att tumma på den säkerhet och regelefterlevnad som organisationen behöver.

Microsofts lösningar för informationsskydd

Din organisation kan använda molnet utan att utsätta känsliga data för risker. Med Microsofts lösningar för informationsskydd får du den insyn du behöver, och du kan utöka dina säkerhetsprinciper till molnet. Med Microsoft Cloud App Security får du hjälp att:

- Upptäcka och bedöma risker: identifiera molnappar i nätverket, få insyn i skugg-IT och få riskbedömningar och kontinuerlig analys.

- Styra åtkomsten i realtid: hantera och begränsa åtkomsten till molnappar utifrån tillstånd och sessionskontext, inklusive användarens identitet, enhet och plats.

- Skydda din information: få detaljerad kontroll över data och använd inbyggda eller anpassade principer för datadelning och förebyggande av dataförluster.

- Identifiera och skydda mot hot: identifiera riskabel användning och identifiera ovanlig användaraktivitet med Microsofts funktioner för beteendeanalys och identifiering av avvikelser.

Användarna använder ofta appar där känsliga affärs- eller kunddata lagras. Det är viktigt att kunna kontrollera vad som händer efter att data har använts, och att förlänga säkerheten i dina lokala system till molnet där du får bättre insyn, detaljerade kontroller och ett starkare skydd mot hot.

- Våra MAM-funktioner (mobile application management) och principer för appskydd kan hjälpa dig att skydda data på appnivå, till exempel med autentisering på appnivå samt styrning av kopiera/klistra in och spara som.

- Du kan konfigurera dina principer och får en detaljerad kontroll över vad användarna kan göra med de data som används.

- Du kan tillämpa principer för program du vill skydda, oavsett om enheten registreras för hantering, så att du kan skydda företagets information utan att göra intrång i användarens privatliv.

- Du kan kryptera företagsdata i appar med den högsta nivån av enhetskryptering i iOS och Android.
- Du kan även skydda företagets data genom att använda PIN-koder eller inloggningsuppgifter.

Viktiga punkter

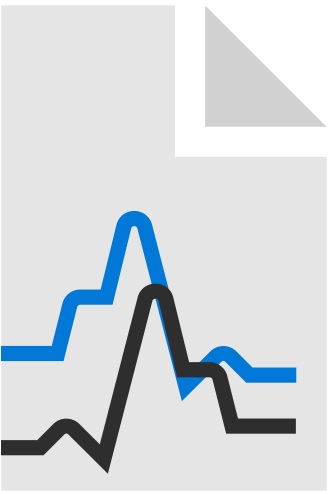
Snarare än att helt blockera skugg-IT bör du leta efter lösningar där du kan övervaka och bedöma risker.

CASB:er kan ge en detaljerad bild av hur de anställda använder molnet.

När du får bättre insyn kan du konfigurera principer som spårar och styr hur de anställda använder de här apparna.

06 Att väga ett heltäckande dataskydd mot produktivitet

Data hamnar i allt större utsträckning utanför din kontroll när de delas mellan anställda, partnerföretag och kunder. Det här ökar produktiviteten och främjar innovation, men om känsliga data hamnar i orätta händer kan det få stora konsekvenser. Säkerhetschefer måste hantera och skydda data som lagras på olika platser och delas över internationella gränser. Organisationer som gör affärer i EU måste prioritera dataskyddet innan den allmänna dataskyddsförordningen träder i kraft den 25 maj 2018. GDPR kommer att innebära stora förändringar i hur företag lagrar och hanterar kunddata, rapporterar intrång, förmedlar principer och investerar i interna resurser.



Dina medarbetare tolererar bara en viss mängd praktiska hinder innan de börjar leta efter sätt att komma runt säkerhetskraven. Att klassificera och kryptera data är det bästa sättet att skydda dem och samtidigt se till att informationen kan användas och delas. Om de anställda förväntas komma ihåg vilka data som måste skyddas och hur de ska klassificeras leder det till fel och förseningar, så det bästa är att klassificera och märka upp data när de skapas. Du kan komma runt den mänskliga faktorn genom att automatisera dataklassificeringen. Verktyg kan lära sig att förstå sammanhang för data, som kreditkortsnummer i en fil, eller hur känsliga data är baserat på var de kommer ifrån. När data har märkts upp kan du automatiskt använda visuella markörer som sidhuvuden, sidfötter och vattenmärken, samt skydd som kryptering, autentisering och åtkomsträttigheter för känsliga data.

Säkerhetsteamet bör också kunna spåra aktiviteten för strikt konfidentiella filer eller affärshemligheter, och neka åtkomst om det behövs. Det här heltäckande skyddet följer med dina data och skyddar dem kontinuerligt, oavsett var de lagras eller vem de delas med.

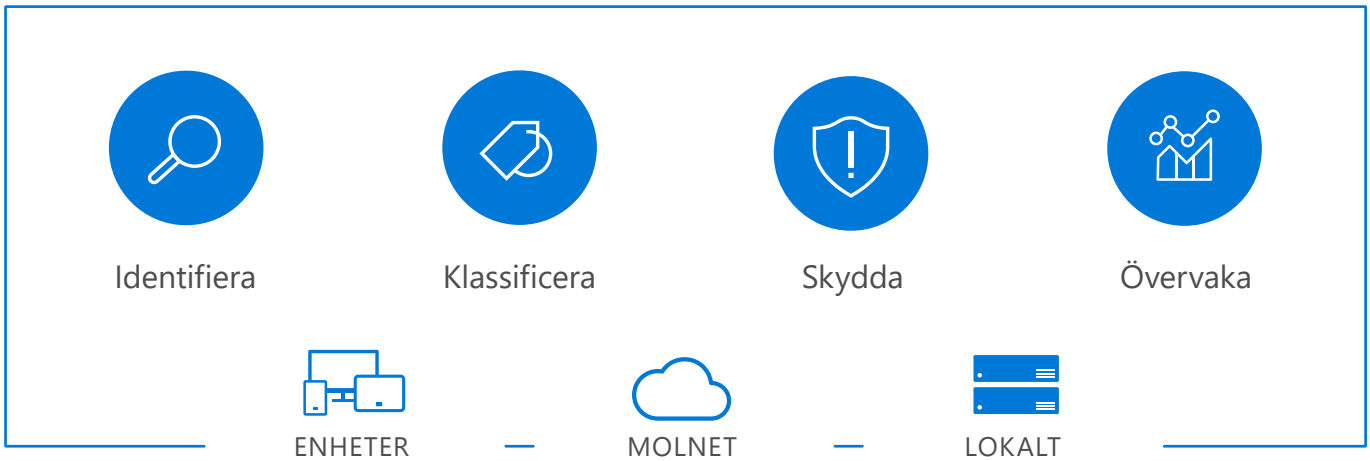
Microsofts lösningar för informationsskydd

Skydda mot läckor och oavsiktlig felhantering var informationen än befinner sig.

Microsofts lösningar för informationsskydd hjälper dig att skydda känsliga data under hela livscykeln – på enheter, i appar, i molntjänster och i lokala system.

Microsofts metod för att kontinuerligt skydda känsliga data under hela livscykeln, både inom och utanför organisationen, handlar om att identifiera, klassificera, skydda och övervaka kritiska data oavsett var de lagras eller skickas. Microsoft 365 har en mer konsekvent och integrerad metod för klassificering, uppmärkning och skydd av data i vår kärnteknik för informationsskydd.

Se diagrammet nedan:



> *Vi måste tänka om när det gäller hur vi skyddar data i den moln- och mobilcentrerade världen. Faktum är att ingen har den expertis, den tid och de resurser som krävs för att göra det här helt på egen hand.*
>
> **Brad Anderson**, *Microsoft Corporate Vice President for Enterprise Mobility*

Viktiga punkter

- **Säkerhetschefer måste fokusera mer på säkerhet på datanivån.**
- **Klassificering och kryptering av data blir allt viktigare. Klassificering och uppmärkning av data ska ske när de skapas, och säkerhetsteamet bör kunna övervaka filanvändningen och vidta snabba åtgärder.**

Samman-fattning

De många olika typerna av cyberhot innebär att du inte längre klarar dig med att lösa bara några säkerhetsutmaningar. Olika lösningar kan fortfarande skydda kritiska slutpunkter, identifiera intrång och begränsa skadeverkningarna, men eftersom dagens cyberhot är ständigt förekommande behöver du ett lika kontinuerligt skydd, och det innebär även en helhetssyn på säkerheten.

Att skydda data och system har nu högsta prioritet oavsett organisation. Varje företag har ett unikt säkerhetsbehov, men utmaningarna är ofta desamma och de måste skydda sina data, anställda och system samtidigt som innovation och tillväxt främjas. Du behöver ett flexibelt ramverk som möjliggör den digitala omvandlingen och som underbyggs av en helhetssyn på säkerheten som är inbyggd i teknik, processer och utbildning. Microsoft 365 Enterprise är en komplett och intelligent lösning som underlättar din digitala omvandling och där funktioner för säkerhet och regelefterlevnad är inbyggda på varje nivå.

Du kan läsa mer om hur Microsoft kan hjälpa dig med en heltäckande säkerhetsstrategi på **startsidan för Microsoft 365.**