

WHITE PAPER

De ce aveți nevoie de un model de securitate centrat pe informații?
"Suficient de bun" nu este suficient de bun.

Symantec DLP protecția datelor acolo unde contează!

TABLE OF CONTENTS

Introducere

Tehnologii Protecție Date

Microsoft

Symantec

Criterii DLP

Complet

Politici

Practic

Informativ

Cost Redus

Concluzie

Introducere

Acest document este destinat proprietarilor de date: persoane fizice, directori financiari, DPO, manageri HR, specialiști PR, manageri de risc și conformitate și specialiști responsabili cu protecția datelor critice din organizații. Acest document conține informații care pot fi folosite și pentru specialiști în următoarele domenii: informații, comunicații și implementarea de soluții pentru protecția datelor. Acest document recomandă organizațiilor să evalueze soluțiile de protecție a datelor luând în considerare costul total de proprietate, nu doar prețul de achiziție și ghidază cititorul prin factorii relevanți în acest proces de evaluare.

Tehnologii Protecție Date

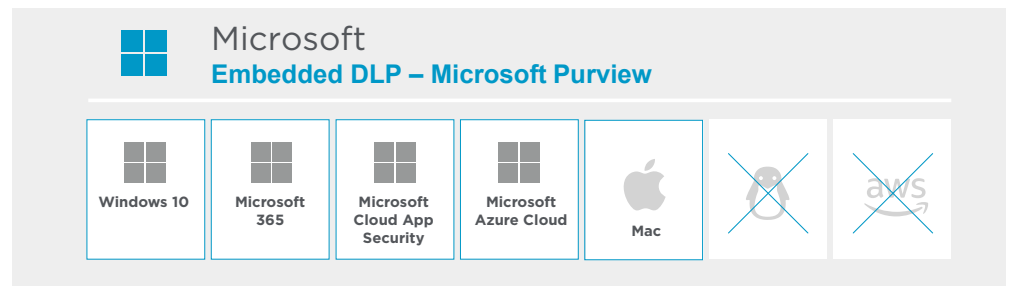
Microsoft și Symantec oferă soluții (DLP), dar fiecare companie are obiective diferite când vine vorba de protecția datelor. Diferențele între soluții sunt foarte mari, una fiind o soluție de tip "este adecvată" în timp ce cealaltă este o soluție de tip "Enterprise".

Această lucrare Symantec se bazează pe în alegerea soluției Microsoft din aprilie 2023.

Microsoft

Microsoft încorporează capacități de protecție a datelor în soluțiile sale precum: Windows 10, Microsoft (anterior Office) 365, Microsoft Cloud App Security (MCAS) și Azure. Microsoft numește aceste capacități Microsoft Purview Information Protection.

Această abordare Microsoft oferă protecție de bază pentru conținutul nestructurat creat predominant folosind instrumente Microsoft, cu un anumit suport pentru formate de fișiere non-Microsoft. Este o alegere acceptabilă pentru utilizatorii DLP ale căror date sensibile sunt păstrate în întregime în mediile Microsoft, și pentru organizațiile non-Enterprise pentru care pierderea datelor nu este preocupare.



Symantec

Symantec/Broadcom® oferă un portofoliu de soluții special construite pentru protejarea endpoint-urilor, datelor locale și datelor din Cloud, ce se integrează cu produse de tip: gateway web, e-mail, aplicații cloud, SaaS și IaaS pentru extinderea protecției de tip DLP.

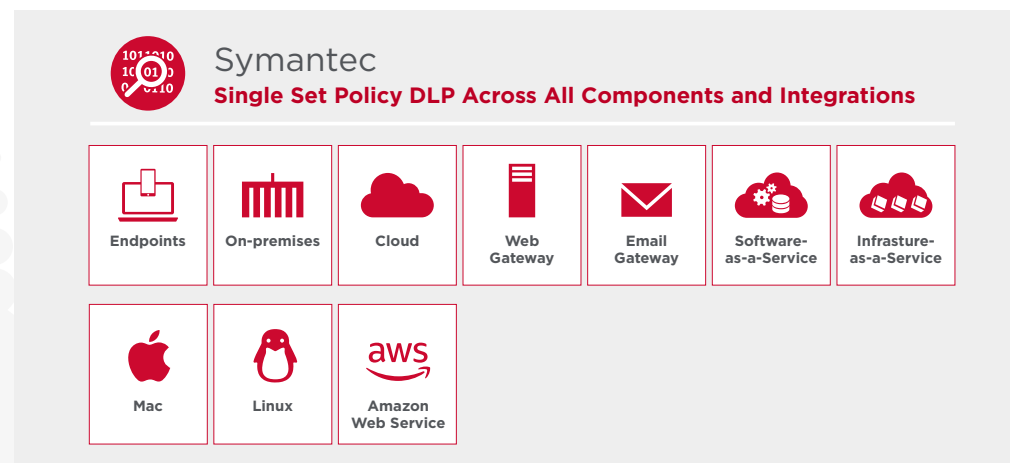
Symantec DLP este o soluție de protecție a datelor pentru date: în uz, în mișcare sau în repaus de pe orice mediu.

Symantec® DLP protejează: date, aplicații, fișiere, imagini și date structurate în medii Microsoft și non-Microsoft,

Symantec DLP aplică un singur set de politici pentru toate componentele și integrările.

Symantec DLP a fost conceput și adoptat pe scară largă de întreprinderile mari deoarece oferă o soluție completă bazată pe gestionarea riscului și satisface nevoile organizațiilor ce pun accent pe protejarea datelor.

Symantec DLP este o soluție de protecție a datelor pentru date: în uz, în mișcare sau în repaus de pe orice mediu.



Capabilitati DLP

Solutiile DLP de nivel Enterprise trebuie sa aiba urmatoarele capabilitati:

	Complet Protejeaza toate informațiile sensibile, indiferent cât de vechi, oriunde sunt stocate și oricum sunt transmise
	Politici Aplică în mod consecvent fiecare cerință de reglementare, standard industrial și politic organizațional pentru toate aplicațiile, dispozitivele și mediile acoperite
	Practic Conectează procesele de configurare și gestionare la procesele operaționale stabilite pentru a economisi timp, bani și personal
	Informativ Furnizează date complete contextuale în cazul evenimentelor de exfiltrare de date și încălcări ale politicilor implementate pentru determinarea răspunsului adecvat în cazul unui eveniment.
	Cost Redus Costul soluției DLP nu va îngunchia o organizație și va genera valoarea prin standardele implementate de protecție a datelor.

Aplicarea acestor criterii soluțiilor Microsoft și Symantec în următoarele secțiuni ilustrează diferența dintre cele două soluții.



Complet

Cea mai importantă decizie în alegerea unei soluții DLP este:

Acoperire completa:

- Ce date veți proteja sau, invers, ce date sunteți pregătiți să treceți cu vederea?

Soluția DLP va descoperi și proteja toate datele din infrastructura unei Organizații?

- Ce servere, puncte finale, magazine de date etc. veți scana pentru sensibile informații?
- Ce tipuri și ce dimensiuni vor avea fișierele?
- Veți include în soluția DLP date structurate și nestructurate?
- Ce se întâmplă cu formatele învechite precum Lotus 1-2-3, WordStar sau Microsoft Works?

- Ați luat în considerare imaginile și atașamentele de e-mail?

A doua parte a acoperirii implică monitorizarea:

- Ce cîmpuri de date, medii și puncte finale veți monitoriza pentru prevenirea scurgerilor de date?

În concordanță cu filozofia Microsoft de protejare a datelor, Microsoft Purview Information Protection identifică și monitorizează un mic subset de informații sensibile pe care organizațiile trebuie să le protejeze. Abordarea Symantec independent de furnizor aplică politici consecvente de protecție a datelor pentru întreaga gamă de date ale companiei.

Comparatie între Soluțiile Microsoft și Symantec

Acoperire	Microsoft	Symantec
Medii		
Servere și Medii De Stocare On Prem	Scanare Limitată	Scanare de până la 2 TB Ora
Stocare IaaS Cloud	AWS, S3 buckets, Google	AWS, S3 buckets, Google
Web Gateways,	Nu	Da
Email Archive și Atasamente	Microsoft 365	Microsoft 365, Gmail, și mai multe
Medii de Stocare atasate de Endpoint	Nu	Da
Stocare "Bring Your Own" Device	Nu	Da
Inspectie de Continut	Nu	Peste 200 de aplicații suportate
Sisteme De Operare și Software		
OS	Windows 10, 11, și ultimele trei versiuni de MAC	Suporta versiunile anterioare de Windows plus MAC și Linux
Web Browsers	Chrome, Firefox, Edge, Safari, etc.	Chrome, Firefox, Edge, Safari, etc.
Baze de Date: Oracle, MS SQL, IBM Db2, etc.	Da	Da
Vectori Exfiltrare		
Upload către Web sau Cloud	Da	Da
Copy Clipboard	Da	Da
Copiere către medii de stocare (USB)	Da	Da
Print	Da	Da
Imagini : Print Screen, Photo, Scan, etc.	Nu	Da
Caracteristici Fisiere		
Tipuri Fisiere: Prezente, Legacy și care nu mai sunt suportate	Sub 50 de tipuri de fisiere	Peste 375 de tipuri de fisiere
Fisiere Mari și Atasamente	Nu	Da
Scanare		
Continuu	Da, dar cu SLA mai lung	Da
Exhaustive	No	Da

^b Analysis based on the Symantec understanding of Microsoft product capabilities as of April 2023.

Politicile stabilesc ce va căuta și proteja o soluție DLP



Politicile

Politicile stabilesc ce va căuta și proteja o soluție DLP. Politicile sunt determinate în primul rând de reglementările și standardele pe care organizația dorește să le respecte. Soluțiile DLP pot include politici predefinite precum politici de tip US Regulatory Enforcement sau General Data Protection Regulation.

Dar politicile predefinite nu vor examina dacă organizația va respecta standarde customizate ce pot fi mai complexe sau mai simple decât politicile predefinite în soluții.

La fel cum reglementările și standardele se aplică întregii organizații, politicile de protecție a datelor trebuie să fie și ele consecvente indiferent de infrastructura unei organizații. Soluțiile DLP eficiente ar trebui să se adapteze și să permită extinderea politicilor, luând în considerare atât contextul, cât și conținutul. De asemenea, soluția DLP trebuie să se adapteze folosind tehnologii precum AI sau analiza comportamentului cu scopul prevenirii breșelor de date. Aceste tehnici sunt deosebit de importante atunci când utilizatorii pot accesa date în cloud-ul public din orice locație. Evaluarea atât a riscului pe care îl reprezintă utilizatorul cât și a sensibilității datelor permit crearea de controale eficiente ce vor reduce riscul unei breșe.

La fel cum reglementările și standardele se aplică întregii organizații, politicile de protecție a datelor trebuie să fie și ele consecvente indiferent de infrastructura unei organizații

Politicile	Microsoft	Symantec
Granularitate		
Combinatii Logice (And, OR)	Da	Da
Limite, excepții, praguri, acceptate, de exemplu numărul de SSN?	Da	Da
Identical Policy Framework		
On-Premises și Cloud	Nu	Da
Email	Nu	Da
Web Applications	Nu	Da
Secure Web Gateways, Mirror Gateways, etc.	Nu	Da
Politicile Customizabile și Predefinite		
Politicile Predefinite	Da	Da
Politicile Predefinite Pot Fi Customizate	Da	Da
Politicile Customizate Create de laZero	Da	Da
Politicile Ce Pot Folosi AI	Da	Da
Analiza Comportament și Context		
DLP Bazat pe Context	Da	Da
User Behavior (UEBA) Analytics	Da	Da

Symantec DLP automatizează procesele cât mai mult posibil, și integrează luarea deciziilor administrative în fluxurile de lucru stabilite.



Practice

Conștientizarea excepțiilor politicii DLP nu este suficientă. Organizațiile trebuie, de asemenea, să reacționeze pentru a remedia orice daune și să prevină viitoare incidente sau alarme false. Integrarea răspunsului la incident, remedierea, și alte acțiuni în fluxurile de lucru practice pot face diferența între un program de protecție a datelor care funcționează fără probleme și eficient și un program reactiv, costisitor și, în cele din urmă, nesustenabil. Microsoft și Symantec au fiecare abordări diferite. Symantec DLP automatizează procesele cât mai mult posibil, și integrează luarea deciziilor administrative în fluxurile de lucru stabilite.

Management and Workflow	Microsoft	Symantec
Politici		
Un set de politici pentru toate aplicațiile, platformele și mediile	Nu	Da
Consol unic de management pentru DLP end-to-end	Nu	Da
Alerte		
Notificări Automate	Da	Da
Blocare automată la punctele de ieșire	Selectiv	Da
Remedierea incidentelor de nivel scăzut de către proprietarii de date	Nu	Da
Prioritizare		
Contextul complet de alertă pe o singură pagină	Nu	Da
Instrumente pentru gestionarea alarmelor false	Nu	Da

Politici: Politicile Microsoft de protecție a datelor sunt gestionate individual pentru fiecare aplicație, platformă sau mediu. De exemplu, chiar dacă MCAS protejează mai multe aplicații cloud diferite, politicile sunt administrate separat pentru fiecare.

Symantec DLP aplică un singur set de politici în toate infrastructura: medii cloud, inclusiv punctele finale ale acestora și punctele de ieșire web și e-mail, și le gestionează dintr-o singură consolă administrativă.

Alerte: excepțiile politicii DLP declanșează alerte, care pot să apară sau nu la nivelul incidentelor acționabile. Răspunsul la alertă vă spune cât de mult lucrează Soluția DLP pentru a le confirma, prioritiza și escala, și cum o mare parte din acestea va reveni personalului administrativ. Răspunsurile automate pot varia de la avertismentele pop-up ale utilizatorilor la criptarea fișierelor transferate. Traficul de rețea este de obicei redirecționat sau blocat la punctele de ieșire din rețea sau la transferul de e-mail.

Alertele Microsoft blochează traficul selectiv, de exemplu, numai către Azure. În datele proprietarii nu pot repara ei înșiși incidentele de nivel scăzut, crescând sarcina asupra echipelor administrative.

În Symantec DLP, alertele blochează exfiltrarea datelor la fiecare punct de ieșire și utilizatorii pot remedia incidentele de nivel scăzut fără a implica administratorii de protecție a datelor.

Stabilirea priorităților: stabilirea care alerte constituie incidente acționabile, necesită judecată umană și context iar contextul lipsește pur și simplu în soluția Microsoft DLP:

- Care politică a fost încălcată ?
- Ce activitate a cauzat încălcarea?
- Ce conținut a fost implicat?
- Ce fișier a fost implicat și unde se află ?
- Ce utilizator a fost implicat; pe cine suni?
- Numele măștii, aplicația, atributele Active Directory și multe altele.

Symantec oferă aceste informații contextuale și multe altele pe un singur ecran, gata pentru escaladare și răspuns efectiv.

Soluțiile de protecție a datelor sunt reglate în mod deliberat pentru a declanșa alerte pentru a reduce riscul apariției unei breșe de date. Majoritatea alertelor din viaa reală vor fi alarme false declanșate prin activități inofensive. Fără o metodă eficientă de a le face față, alarmele false vor copleși rapid personalul de conducere și vor crea stimulente pentru a face sistemul mai puțin sensibil. Microsoft nu oferă instrumente de gestionare pentru alarme false sau prioritizarea incidentelor; Symantec este dezvoltat pe această bază.

Escaladare și raportare: Majoritatea organizațiilor mari au deja instrumente pentru escaladarea și raportarea incidentelor; ServiceNow este o soluție de vârf.

Integrarea cu un sistem consacrat de identificare a problemelor simplifică foarte mult generarea de răspunsuri la incidente și reduce sarcinile de lucru. Microsoft nu oferă integrare;

Symantec include și integrare cu ServiceNow.

Informativ

Informațiile sunt esențiale pentru gestionarea și rafinarea politicilor cât și pentru generarea de răspunsuri automate și umane la alerte. Informațiile contextuale ajută foarte mult în acest domeniu.

- Determinați amploarea a unei breșe pentru a: reduce timpul de așteptare, efectua activități de recuperare, efectua acțiuni de tip "public relations" și efectua despăgubiri.
- Reconstruiți șirul de evenimente care au precedat breșa, pentru îmbunătățirea politicilor implementate și prevenirea unei alte breșe.
- Efectuați analize criminalistice cu mult înaintea unei breșe, pentru a identifica modele de comportament suspecte și posibili utilizatori rău intenționați.
- Documentați încălcarea, antecedentele acesteia și măsurile de remediere pentru a asigura autoritățile că totul este în ordine.

Contextul complet oferit de soluțiile Symantec DLP prin alerte și jurnale complete pot face diferența în reducerea riscului apariției unei breșe de date.



Cost Redus

Determinarea costului total de proprietate (TCO) este o sarcină complexă, iar costurile licențelor software sunt doar începutul. O soluție DLP nu ar trebui evaluată numai pe baza costului, ci pe baza calculului risc/beneficii.

Pretul unei soluții DLP include costurile soluției de bază DLP sau ale setului de caracteristici. În Microsoft Purview Information Protection, aceste costuri depind de: aplicație, platformă sau mediu; Symantec oferă costuri mult mai simple de calculat.

-Perpetual sau Subscripție

-Upgrade-uri

-Costuri Suport Furnizor

De asemenea trebuie incluse în costul total și golurile pe care o soluție DLP nu le acoperă precum:

-Platforme și medii critice non-Microsoft

-Vectori de exfiltrare cu risc ridicat: imprimante, unități USB,

-Fișiere .txt, imagini

- Shadow IT: telefoane, dispozitive BYO, aplicații web etc.

-Canale web, cum ar fi Secure Web Gateways, on-premise și în cloud - Gateway-uri de e-mail, on-premises și în cloud

- Cloud-Access Security Brokers (CASB)

- Canale pentru carantina traficului suspect

- Portaluri Zero Trust Network Access

- Soluții personalizate pentru protejarea proprietăților intelectuale

-Costurile de suport, upgrade și întreținere

Considerațiile privind costurile de personal includ personal pentru implementarea, integrarea și gestionarea soluțiilor de bază și de completare a golurilor și pentru a efectua sarcini administrative acolo unde soluțiile automate nu sunt disponibile:

- Costuri pentru angajarea, instruirea și întreținerea unei forțe de muncă foarte mobile, solicitate, prime salariale pentru angajații cu înaltă calificare pentru scripturile necesare sau integrări personalizate

- Taxe de servicii și consultanță

- Personal pentru a răspunde la alerte cu informații contextuale slabe și pentru a gestiona alarmele false

- Personal pentru: descoperirea manuală, managementul politicilor, prioritizarea proceselor de escaladare

- Personal pentru a îndeplini cerințele de conformitate și raportare

- Personal pentru administrarea și gestionarea mai multor console, platforme și instrumente

Costurile de tip "Downstream" includ costurile operaționale directe și indirecte ale unei soluții DLP suboptimale:

-Ineficiențe din soluția DLP de a acoperi toate zonele expuse.

-Impactul asupra eficienței utilizatorilor finali, inclusiv răspunsurile la alarmele false

- Impactul volumului de muncă asociat proceselor manuale și alertele ce pot avea efect asupra moralului operațiunilor de securitate.

-Impactul asupra cifrei de afaceri

SYMANTEC DLP OFER SOLUȚIE COMPLETĂ BAZAT PE RISC CARE RĂSPUNDE NECESITĂȚILOR ORGANIZAȚIILOR DE NIVEL ENTERPRISE

Concluzie

Microsoft Purview Information Protection oferă soluții de tip DLP de bază într-o gamă largă de produse și servicii populare. Organizațiile care au nevoie de o soluție DLP avansată vor achiziționa o soluție care satisface următoarele criterii:

- **Completa:** identifică și monitorizează informațiile sensibile indiferent de format pe orice mediu de stocare și vector de exfiltrare.
- **Politici:** Soluția va folosi singur set de politici granulare ce pot atinge majoritatea cerințelor de reglementare existente: industrial, sănătate, financiar, guvernamental.
- **Practica:** Soluția trebuie să includă capacități precum: politici, alerte, procese, prioritizarea/escaladarea și raportarea pentru a economisi resurse financiare și umane.
- **Informații:** Soluția trebuie să furnizeze context complet când apare un eveniment pentru ca echipele de securitate să poată genera un răspuns adecvat.
- **Cost Redus:** Soluția trebuie să aibă un cost direct proportional cu beneficiile pe care le aduce într-o organizație.