COHESITY

EINKAUFSLEITFADEN

MIT DER RICHTIGEN DSPM-LÖSUNG DURCH DATEN UND KI-RISIKEN NAVIGIEREN

Zusammenfassung

Sensible Daten sind jetzt über Ihre Cloud-Plattformen, SaaS, Datenbanken, Backups, hybride Infrastruktur, NAS und mehr verteilt. Sie haben wahrscheinlich bereits mehr Daten, als Sie leicht verwalten können. Es ist jedoch schwer zu verstehen, wo Ihre sensibelsten Daten gespeichert sind, wie umfassend sie offengelegt werden, wer Zugriff auf sie hat und ob dieser Zugriff angemessen ist.

Dies führt zu einer perfekten Kombination, um das Geschäftsrisiko auf Vorstandsebene erheblich zu erhöhen. Und die Herausforderung wächst: Auch wenn Menschen weiterhin auf diese Daten zugreifen, sie verändern und verschieben, bringen KI-Agenten neue und wachsende Risiken mit sich.

Diese Sicherheits- und Schutzlücken sind der Grund, warum Datensicherheitslagen-Management (Data Security Posture Management, DSPM) für moderne Führungskräfte in Unternehmen zu einer strategischen Priorität geworden ist.

89 % **der Sicherheitsverantwortlichen geben an, dass der Status quo der Datensicherheit in ihrem Unternehmen ein Problem darstellt.**

39 % **der Sicherheitsverantwortlichen geben an, dass Legacy-Technologien für die aktuellen Anforderungen unzureichend sind.**

60 % **der Unternehmen fehlt die Transparenz über mindestens die Hälfte ihres Datenbestands.[1]**

[1]Omdia-Whitepaper: Cyber-Resilienz mit zielführender Datenintelligenz erreichen

Eine moderne DSPM-Lösung sollte Ihnen helfen, weit mehr zu tun als nur Daten zu inventarisieren. Sie sollte Ihnen helfen, Risiken aktiv zu reduzieren, die Cyber-Resilienz zu stärken und kritische Fragen während der Reaktion auf Vorfälle, bei Sicherheitsübungen oder Audits zu beantworten:

- Wo und was sind unsere sensiblen Daten?
- Wer oder was hat Zugriff darauf?
- Was sollten wir zuerst regeln?
- Wie reduzieren wir Risiken, ohne die Geschäftsinnovation und das Wachstum zu verlangsamen?
- Sind die Daten geschützt und können sie schnell, sicher und regelkonform wiederhergestellt werden?

Für Sicherheitsverantwortliche bedeutet dies, von Transparenz zu zielführender Risikoreduzierung überzugehen – sowohl vor als auch nach einem Angriff.

Dieser Leitfaden richtet sich an Teams, die DSPM-Lösungen evaluieren, damit Sie die richtige für Ihre Anforderungen auswählen können.

Dateninventarisierung ist nicht alles.

Die eigentliche Kauffrage ist nicht, ob eine Lösung Ihnen zeigen kann, wo sich die Daten befinden. Es geht darum, ob die Lösung erkennen und aufzeigen kann, *warum* ein hohes Risiko besteht und was Sie jetzt tun können, um dieses Risiko zu beheben.

Was DSPM löst

Einer der häufigsten Fehler, den Organisationen bei der Bewertung von DSPM machen, ist, es wie ein einfaches Discovery-Tool zu behandeln. Bei einer DSPM-Lösung geht es um weit mehr als nur um Transparenz. Die richtige Lösung sollte Ihnen helfen, Probleme im Zusammenhang mit der Datenrisikolage zu lösen.

Hier sind fünf Probleme, bei deren Lösung Ihnen Ihr DSPM helfen sollte:

Problem	Wie DSPM es löst
Ich weiß nicht, wo sich meine sensiblen Daten befinden.	Viele Organisationen können nicht mit Sicherheit beantworten, wo sich ihre wertvollsten oder streng reglementierten Daten in Cloud-, SaaS- und Hybrid-Umgebungen befinden. Warum ist das der Status quo? Traditionelle Datensicherheits-Tools sind auf bestimmte Datentypen, bestimmte Bereitstellungsmodelle oder spezifische Anwendungsfälle beschränkt. Selbst wenn sie über einen gewissen Bestand verfügen, ist dieser häufig unvollständig, veraltet oder vom Risikokontext abgekoppelt. Um mit dem Datenvolumen und der zunehmenden Datenflut Schritt zu halten, ist eine moderne, cloudnative Architektur erforderlich.
Ich weiß nicht, wer oder was auf meine Daten zugreift (oder zugreifen kann).	Ein durchschnittlicher Mitarbeiter nutzt täglich etwa 36 Cloud-Dienste, verteilt auf mehr als 200 Tools für die Zusammenarbeit. Sensible Informationen verbreiten sich über verschiedene Plattformen hinweg und werden häufig außerhalb etablierter Governance-Kontrollen geteilt. Sensible Daten werden noch riskanter, wenn sie übermäßig offengelegt, mit zu weitreichenden Berechtigungen versehen, zu breit geteilt, am falschen Ort gespeichert oder für mehr Identitäten (und nichtmenschliche) zugänglich sind als beabsichtigt. Ihre DSPM-Lösung sollte Ihnen helfen zu verstehen, welche Daten gefährdet sind – nicht nur, welche Daten einer Klassifizierungsrichtlinie entsprechen.
Ich weiß nicht, welche Datenrisiken ich zuerst zur Behebung priorisieren sollte.	Die meisten Unternehmensumgebungen enthalten große Mengen sensibler Daten. Allerdings bergen nicht alle Datenrisiken die gleiche Dringlichkeit. Teams benötigen eine Möglichkeit, Hintergrundrauschen von relevanter Exposition zu unterscheiden. Die richtige Lösung sollte Ihnen helfen, sich auf die Probleme mit den größten potenziellen geschäftlichen Auswirkungen zu konzentrieren – basierend auf Sensibilität, Zugriff, Exposition, Umgebung und erlerntem Geschäftskontext.
Ich kann Datenrisiken nicht schnell oder automatisch beheben.	Datenkontext – in Kombination mit tiefer Integration über die gesamte Security-Toolchain hinweg – ist entscheidend, um die MTTR (Mean Time To Respond) bei der Behebung von Daten mit hohem Risiko zu reduzieren. Traditionelle Methoden der Datensicherheit stützen sich stark auf Muster und Tags und überfluten Teams mit lautstarken Warnmeldungen, denen es oft an Glaubwürdigkeit mangelt. DSPM-Lösungen sollten Maßnahmen vorantreiben. Ergebnisse sollten verständlich, zuweisbar und nachverfolgbar sein. Sicherheits- und IT-Teams sollten in der Lage sein, zuversichtlich darauf zu reagieren.
Wenn ich Daten wiederherstellen muss, ist es langsam, riskant und kostspielig.	Sekundärdaten (wie z. B. Backups) sind entscheidend, wenn es um die Reaktion und Wiederherstellung nach Vorfällen geht. Diese Daten können auch Risiken und potenzielle Compliance-Verstöße mit sich bringen, die es zu beheben gilt. Moderne DSPM-Lösungen sollten die Ergebnisse der Cyber-Resilienz stärken und Datenintelligenz bereitstellen, um die Anwendung der richtigen Schutzstufen sicherzustellen. Sensible Daten sollten bei der Reaktion auf Vorfälle priorisiert und regelkonform wiederhergestellt werden.

Was „gut“ bedeutet

Bevor Sie Hersteller bewerten, müssen Sie entscheiden, was „gut“ überhaupt bedeutet. Hier sind fünf Bereiche, in denen eine moderne DSPM-Lösung überzeugen sollte:

Schnell bereitstellen und nahtlos ohne Grenzen skalieren

Gute Erkennungsfunktionen sollten Ihnen helfen, schnell einen umfassenderen Überblick über Ihre Exposition zu gewinnen, ohne dass ein langer, aufwändiger Implementierungszyklus erforderlich ist, bevor ein Nutzen entsteht.

Organisationen sollten mit einer kontinuierlichen Überprüfung von Hunderten von Petabyte rechnen, ohne dass dies die Leistung beeinträchtigt. Der richtige Hersteller bietet umfassende Unterstützung in wichtigen Umgebungen, einschließlich Cloud-Datenspeichern, SaaS-Apps, Dateisystemen und gegebenenfalls On-Premise-Datenbanken.

Schwachstellen sollten durch genaue Erfassung und Klassifizierung eliminierbar sein

Eine gründliche Erkennung hilft zu verhindern, dass minderwertige Ergebnisse jedes nachgelagerte Ergebnis beeinträchtigen. Wenn das DSPM-Tool kritische Orte übersieht, sensible Informationen falsch klassifiziert oder zu viel manuelle Feinabstimmung erfordert, werden die Ergebnisse weniger hilfreich oder sogar irrelevant sein.

Die richtige DSPM-Lösung deckt Schwachstellen auf, indem sie sich an Ihre Umgebung anpasst und Daten automatisch klassifiziert (einschließlich IP und Daten, die für Ihr Unternehmen einzigartig wichtig sind).

Echte Risiken priorisieren und nicht nur so tun als bo

Die Zeit ist wertvoll; kein Team kann alles auf einmal beheben. Eine starke DSPM-Lösung kombiniert Expositionen und Kontext, um sich auf die größten Gefahren zu konzentrieren. Sie sollte Risiken durch hochsensible Daten mit breiter Exposition priorisieren.

Dies erfordert fortgeschrittene Fähigkeiten, um Datensensitivität, Geschäftszweck, Identitäten, Zugriffsaktivitäten und Exposition zu korrelieren, sodass reale Geschäftsrisiken sichtbar werden.

Behebung in großem Maßstab automatisieren

Moderne DSPMs müssen die Exposition von Organisationen nicht nur beobachten, sondern auch verringern. Organisationen sollten nach DSPMs suchen, die sofort einsatzbereite Behebungsmaßnahmen bereitstellen. So bieten führende Lösungen beispielsweise One-click-Kontrollen für Zugriffsentzug, Maskierung von Daten, Aktivierung von vordefinierten Workflows und Weiterleitung von Problemen direkt an die zuständigen Personen – mit den notwendigen Informationen für eine rasche Lösung.

Dies ist besonders wichtig im Unternehmensmaßstab, wenn viele Teams beteiligt sind. Sicherheitsteams identifizieren das Problem oft, aber die Behebung kann von verschiedenen Gruppen wie Speicheradministratoren, Datenverantwortlichen, Identity-Teams oder Business-Stakeholdern abhängen. Je klarer eine Lösung diese Weiterleitung unterstützt, desto wahrscheinlicher ist es, dass sie zu sinnvollen Ergebnissen führt, die Ihre Sicherheitslage verbessern.

Sicherheit vor und nach Vorfällen stärken

Wir haben bereits die proaktive Risikoreduzierung behandelt, bevor es zu einer Sicherheitsverletzung kommt. Die richtige DSPM-Lösung kann auch die Datenintelligenz und den Kontext bereitstellen, die zur Stärkung von Wiederherstellungsmaßnahmen erforderlich sind, und sicherstellen, dass Sicherheits- und Datenschutzteams verstehen, wo sich sensible Daten befinden, welche Assets am kritischsten sind und ob die angemessenen Schutzmaßnahmen auf die wichtigsten Assets der Organisation angewendet wurden.

Mit einem klaren Überblick über sensible und geschäftskritische Daten sollte Ihr DSPM die Datenschutzstrategien, die die Cyber-Resilienz untermauern, beeinflussen und verbessern. Dies wird Ihnen helfen, die wichtigsten Daten während der Wiederherstellung zu priorisieren, die Reaktion auf Vorfälle mit besserem Kontext zu beschleunigen sowie Kosten und Komplexität zu reduzieren, indem veraltete, redundante oder geringwertige Daten identifiziert und eliminiert werden.

Das Ergebnis ist eine kontinuierliche Feedback-Schleife zwischen Sichtbarkeit, Schutz, Reaktion und Wiederherstellung. Mit der richtigen DSPM-Lösung sollten Sie in der Lage sein, diese Funktionen zu verbinden, sodass Sie von isolierten Sicherheitsmaßnahmen zu einer ganzheitlicheren, durchgängigen Datensicherheits- und Cyber-Resilienz-Strategie übergehen können.

Hersteller-Bewertungskit

Kritische Fragen, die Sie Herstellern stellen sollten

Die folgenden Fragen helfen Ihnen, Ihre engere Auswahl an DSPM-Produkten zu bewerten.

Zur Erkennung und Abdeckung:

- Welche Cloud-, SaaS-, KI-, Datenbank- und Hybrid-Umgebungen unterstützen Sie heute?
- Wie identifizieren und klassifizieren Sie sensible Daten über verschiedene Datentypen hinweg? Wie lange dauert das normalerweise?
- Wie gehen Sie mit strukturierten und unstrukturierten Daten um? Haben Sie bessere Unterstützung für die einen oder die anderen?
- Welcher Grad an Feinabstimmung ist erforderlich, bevor die Ergebnisse verwendbar sind?
- Wie helfen Sie Ihren Kunden, die Sicherheit frühzeitig zu überprüfen und Vertrauen aufzubauen?

Zu Exposition und Zugriffskontrollen:

- Wie stellen Sie fest, ob sensible Daten übermäßig offengelegt sind? Können Sie zeigen, welche Identitäten, Gruppen oder Benutzer Zugriff auf sensible Daten haben?
- Wie identifizieren Sie weitreichenden, übermäßigen oder riskanten Zugriff?
- Wie verknüpfen Sie den Zugriffskontext mit der Datensensitivität?
- Können Sie verhindern, dass sensible Daten in KI-Modelle und -Systeme eingegeben werden oder diese verlassen?
- Können Sie darlegen, wie Ihre Lösung die Bereiche mit dem höchsten Risiko aufzeigt?

Zur Risikopriorisierung und Behebung:

- Wie stufen Sie Erkenntnisse ein oder priorisieren sie? Welche Faktoren beeinflussen den Schweregrad oder die Risikobewertung?
- Können Sie zeigen, wie Teams von vielen Erkenntnissen zu einem überschaubaren Aktionsplan gelangen?
- Wie leitet Ihre Lösung die Behebung an?
- Können Ergebnisse den richtigen Teams oder Verantwortlichen zugewiesen werden?
- Können Erkenntnisse nahtlos an Datenschutzplattformen übermittelt werden und bessere Sicherheits- und Wiederherstellungsergebnisse liefern?

Zeit bis zur Wertschöpfung und Bereitstellung:

- Was erfordert die anfängliche Bereitstellung von unserem Team?
- Wie schnell können wir nützliche Erkenntnisse erwarten?
- Wie sollte Erfolg in den ersten 30, 60 und 90 Tagen aussehen?

Warnsignale, auf die Sie achten sollten

Eingeschränkte Transparenz hinsichtlich des Zugriffsrisikos

Der Zugriff auf sensible Daten ist das größte Risiko. Wenn ein Hersteller nicht klar aufzeigen kann, wer (oder was) auf Daten zugreifen kann und welche Risiken bestehen, ist das eine gravierende Einschränkung.

Ergebnisse sind nicht mit dem individuellen Geschäftsrisiko und Kontext verknüpft

Jedes Unternehmen ist anders. Das Risiko, das von sensiblen Daten oder offengelegtem geistigem Eigentum ausgeht, kann je nach dem variieren, was für diese Organisation wichtig ist. Ergebnisse sollten auf erlerntem Kontext und Klassifikatoren basieren, um genaue Empfehlungen zur Risikobehebung zu liefern.

Unfähigkeit, das Datenrisiko mit Ergebnissen der Cyber-Resilienz zu verknüpfen

Die Optimierung der Daten- und KI-Risikoposition ist entscheidend für die Cyber-Resilienz. Datenintelligenz sollte genutzt werden, um proaktive Datensicherheit zu unterstützen und bessere Wiederherstellungsergebnisse zu ermöglichen. Ergebnisse sollten nicht isoliert behandelt werden, zumal die Behebung häufig funktionsübergreifende Teams einbezieht.

Der Wert hängt von übermäßigem manuellem Aufwand ab

Ein Produkt, das umfangreiche Feinabstimmung, Interpretation oder die Gestaltung von Kundenprozessen erfordert, kann laufende Betriebskosten und die Komplexität erhöhen.

Herstellervergleichstabelle

Verwenden Sie diese Tabelle, um Hersteller nebeneinander anhand der Kernfunktionen zu vergleichen, die für eine effektive DSPM-Strategie erforderlich sind. Wenn Sie jede Zeile durchgehen, berücksichtigen Sie nicht nur, ob eine Funktion vorhanden ist, sondern auch, wie gut sie in der Praxis umgesetzt wird*.

Um Herstellervergleiche konsistenter und objektiver zu gestalten, kann jede Fähigkeit anhand eines einfachen Bewertungsmodells von 0 bis 5 bewertet werden. Dieser Ansatz hilft Teams dabei, über einen einfachen Checklistenvergleich hinauszugehen und die relative Stärke, den Reifegrad sowie die praktische Anwendbarkeit der einzelnen Funktionen zu bewerten. Eine höhere Punktzahl sollte darauf hindeuten, dass die Funktion nicht nur verfügbar, sondern auch unternehmenstauglich, betriebseffizient und nachweislich in der Lage ist, in großem Maßstab einen Mehrwert zu liefern.

Bewertung	Definition
5	Erstklassige Fähigkeit, die vollständig bereitgestellt wird sowie hochautomatisiert, skalierbar und gut integriert ist
4	Starke Fähigkeit mit solider Funktionalität und geringfügigen Lücken
3	Angemessene Fähigkeit, die die grundlegenden Anforderungen erfüllt, jedoch Einschränkungen in Tiefe, Skalierung oder Nutzung aufweist
2	Grundlegende oder teilweise Unterstützung mit deutlichen Lücken, manuellem Aufwand oder eingeschränkter Anwendbarkeit
1	Minimale Fähigkeit, Funktionalität im Frühstadium oder stark eingeschränkte Unterstützung
0	Nicht unterstützt oder keine aussagekräftigen Nachweise vorgelegt

Kategorie	Hersteller 1	Hersteller 2	Hersteller 3	Notizen
Cloudnative Architektur für eine schnelle und agentenlose Bereitstellung				
Kontinuierliche Datenentdeckung in großem Maßstab und hoher Geschwindigkeit				
KI-gestützte Datenklassifizierung				
Datenkontextualisierung				
Zuordnung von Risiken zu Vorschriften				
Anpassungsfähige Zugriffskontrollen und Durchsetzung				
Echtzeit-Erkennung von Daten und Reaktionen				
Kontextbezogene Warnmeldungen				
Integrierte Workflows zur Behebung				
Nahtlose Integration mit Datenschutzplattformen				
Gesamt				

** Die Bewertungen sollten sich auf das derzeit allgemein verfügbare Angebot stützen, nicht auf Angaben aus der Entwicklungsplanung. Jede Bewertung sollte anhand von Produktdemos, Kundenreferenzen, Dokumentation, Bereitstellungsanforderungen und einem Nachweis der Integrationstiefe validiert werden.*

Das Endergebnis

Die Auswahl einer DSPM-Lösung ist mehr als die einfache Entscheidung für das richtige Tool. Das Risiko ist dafür zu hoch. Daten vermehren sich weiterhin und breiten sich in alarmierendem Tempo aus, und manuelle Ansätze oder Legacy-Technologie können nicht Schritt halten. Die richtige DSPM-Lösung hilft Ihnen dabei, Klarheit zu schaffen, Ihre Teams fokussiert zu halten, Risiken zu minimieren und sowohl die Datensicherheit als auch die Cyber-Resilienz zu stärken. Diese Lösung wird sich langfristig auszahlen, da sie Ihnen dabei hilft, die Daten zu schützen und abzusichern, die KI-Modelle, -Systeme und -Agenten untermauern.

Erfahren Sie mehr über unsere DSPM-Lösung und wie sie Ihre Daten- und KI-Risikoposition optimieren kann. Oder kontaktieren Sie uns noch heute.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500066-001-EN 4-2026