5 Best Practices für die Suche nach sensiblen Daten und deren Sicherung

Immer mehr Daten müssen heutzutage an immer mehr Orten gemanagt werden. Deshalb besteht ein wichtiger Schritt bei der Optimierung Ihrer Datenrisikolage darin, herauszufinden, welche Daten sich wo befinden und wie diese richtig gesichert werden können. Befolgen Sie diese 5 Best Practices für die Suche nach sensiblen Daten und deren Sicherung.

1. Ermittlung aller Daten, einschließlich unstrukturierter Daten

Verwenden Sie KI-basierte Klassifizierung, um Daten in Ihrer gesamten IT-Umgebung zu erkennen, einschließlich Dateien, Backups, Archive und Cloud-Umgebungen. Diese proaktive Transparenz wird dazu beitragen, Überraschungen durch die Offenlegung versteckter Kopien und unbekannter Repositorys zu vermeiden.

Warum das wichtig ist:

Blindstellen in Backups, Archiven oder Snapshots können sensible Daten verbergen und den Schaden im Falle einer Sicherheitsverletzung vergrößern.

Vorteile für Sie:

Volle Transparenz hilft Ihnen, die Datenexposition zu reduzieren und Compliance-Lücken zu vermeiden – und zwar vor einem Angriff.

2. Automatisierte, hochpräzise Klassifizierung

Verwenden Sie KI-basiertes Muster-Matching, um Fehlalarme zu reduzieren (bei denen nicht-sensible Daten fälschlicherweise als sensibel eingestuft werden) und kontextbezogene sensible Daten in PII, PHI, PCI, geistigem Eigentum und anderen kritischen Kategorien genauer zu identifizieren.

Warum das wichtig ist:

Die automatisierte Klassifizierung gewährleistet Skalierbarkeit und Konsistenz in wachsenden Datensätzen.

Vorteile für Sie:

Sie sparen Zeit, verbessern die Genauigkeit und skalieren den Schutz Ihrer Daten, ohne zusätzlichen manuellen Arbeitsaufwand.

3. Markierung von Daten mit kontextabhängigen Metadaten

Versehen Sie Ihre sensiblen Daten mit Metadaten wie Klassifizierungsangaben, Standort-Tags und Eigentumsdetails, um eine schnellere Sortierung und eine effektivere Reaktion bei potenziellen Verstößen zu ermöglichen.

Warum das wichtig ist:

Das automatische Markieren sowohl vorhandener als auch neuer Daten mit Metadaten verbessert die Geschwindigkeit und Genauigkeit der Risikobewertung.

Vorteile für Sie:

Mit einem klareren Einblick in das Risiko, können Sie beim Auftreten von Vorfällen schnell und selbstbewusst handeln.

4. Priorisierung von Hochrisikodaten nach Expositionsgrad und Sensitivität

Kennzeichnen Sie sensible Objekte, die als besonders gefährdet gelten (z. B. freigegebene Ordner, Objektspeicher-Bereiche, ungesicherte Sicherungskopien) oder für die Einhaltung von Vorschriften entscheidend sind. Konzentrieren Sie sich bei Ihren Sicherungsmaßnahmen auf die Bereiche mit dem höchsten Risiko.

Warum das wichtig ist:

Da nicht alle Daten das gleiche Risiko aufweisen, sollten sie auf unterschiedliche Weise gesichert werden. Behandeln Sie Ihre Daten wie eine Währung. Einige Daten können den Wert von einem Euro haben, während andere hundert Euro wert sein können.

Vorteile für Sie:

Wenn Sie Ihre Sicherungsmaßnahmen gezielt einsetzen, können Sie die Zeit verkürzen, die Sie für die Reaktion auf Vorfälle aufwenden.

5. Integration der Klassifizierung in die Vorfallsreaktion

Sollte es zu einem Vorfall oder einer Verletzung kommen, können Sie dank Klassifizierungsinformationen direkt bestimmen, welche sensiblen Daten betroffen waren. Außerdem helfen sie Ihnen dabei, regulatorischen Verpflichtungen nachzukommen.

Warum das wichtig ist:

Das Wissen, welche sensiblen Daten betroffen waren, ermöglicht eine schnellere Forensik, genauere Risikobewertungen und eine bessere Compliance-Berichterstattung.

Vorteile für Sie:

Sie können potenzielle Schäden während eines Cyberangriffs bewerten und die regulatorische Berichterstattung problemlos abwickeln.

Wenn Sie diese 5 Best Practices für das Auffinden und Klassifizieren Ihrer sensiblen Daten befolgen, sind Sie auf dem besten Weg, Ihre Datenrisikolage zu optimieren.

Sind Sie bereit, Ihre Datenklassifizierung mit API-gestützten Integrationen weiter zu verbessern? Lesen Sie dazu auch den folgenden Blog: New DSPM integration with Cyera shows the power of open APIs.

COHESITY

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

9100086-001-DE 6-2025