securonix

Securonix + Snowflake

Erkennung von und Reaktion auf Bedrohungen in der ganzen Cloud

Herausforderungen für die Sicherheit von Big Data

Mit der Verlagerung von Unternehmensdaten in die Cloud reichen herkömmliche SIEM-Lösungen angesichts des Umfangs und der Komplexität der Sicherheitsdaten nicht mehr aus. Die sich daraus ergebenden Einschränkungen und Transparenzlücken erschweren die wirksame Erkennung von und Reaktion auf Bedrohungen. Erste Versuche, dieses Problem zu lösen, scheiterten an der Übernahme, Anreicherung und Formatierung der Daten und deren Umwandlung in für Analysten nutzbare Anwendungsfälle.

Cloud-Datenplattformen sind zwar für kosteneffiziente Analysen in großem Maßstab ausgelegt, verfügen aber weder über Sicherheitsintegrationen noch über vordefinierte Analysen, wie sie die Sicherheitsteams benötigen.

Die Lösung: Securonix + Snowflake

In einer aufregenden neuen Partnerschaft entwickelten Securonix und Snowflake eine Lösung mit geteilter Architektur, die es Kunden ermöglicht, Securonix-Analysen neben ihrer bestehenden Snowflake Data Cloud Platform zu nutzen. Durch die gemeinsame Lösung können Snowflake-Kunden ihre Daten in ihrer Snowflake-Implementierung belassen und gleichzeitig zur Verbesserung der Sicherheitstransparenz, für Analysen und die datenbasierte Reaktion auf Vorfälle Securonix Next-Gen SIEM nutzen.

Im Gegensatz zu herkömmlichen SIEM-Lösungen mit einem Datenverbrauchsmodell ermöglicht dieser hybride Ansatz die optimale Bereitstellung von Daten, Diensten und Anwendungen zwischen der Snowflake Data Cloud und der Cloud-nativen Infrastruktur von Securonix. Durch die gemeinsame Lösung können Unternehmen ihre gesamten Unternehmens- und Sicherheitsdaten an einem einzigen Ort konsolidieren und die Vorteile moderner Analysen für Erkennung und Reaktion nutzen.

Vorteile der Lösung

Eine einzige Referenzquelle

Alle Protokolle, Assets und Konfigurationen werden gemeinsam analysiert, gegenseitige Abschottungen werden beseitigt, die Komplexität wird reduziert.

Transparente Preisgestaltung und Kosteneinsparungen

Erschwingliche Preise für Speicher und sekundengenaue Abrechnung der Rechenleistung senken die SIEM-Kosten. Bezahlen Sie Snowflake direkt, damit die Kosten für die Datenübernahme nicht in die Höhe schnellen.

Schnellere Erkennung und Reaktion auf Bedrohungen

Die zentralisierte Securonix Next-Gen SIEM-Lösung fasst Untersuchungen zusammen und fungiert als Erweiterung der Snowflake Data Cloud des Kunden.

Kunden können die einstufige Architektur von Snowflake für kosteneffiziente und unbegrenzte Cloud-Speicherung mit einer flexiblen Archivierungsrichtlinie nutzen, die innerhalb des Unternehmens kontrolliert wird. Die Rechenleistung ist praktisch unbegrenzt und kann bei Bedarf für schnelle Untersuchungen selbst über Terabyte und Petabyte von Daten skaliert werden. Durch die verbrauchsabhängige Preisgestaltung von Snowflake brauchen Sie zudem nur für genutzte Ressourcen zu bezahlen, was insgesamt zu deutlichen Kosteneinsparungen führt.

Details zur Bereitstellungsarchitektur

- Securonix hostet für die Lösung zentrale SIEM-Anwendungsdienste, Überwachung, Microservices und Disaster Recovery.
- Das bestehende Snowflake-Konto des Kunden erhält normalisierte und angereicherte Sicherheitsdaten.
- Vorhandene Ressourcen der Snowflake Data Cloud werden als unbegrenzter Speicherplatz genutzt, um Abfragen von der Securonix-Konsole aus durchzuführen.
- Geschäftsdatensätze aus dem Snowflake-Konto des Kunden können davon unabhängig geladen und mit Sicherheitsdaten zur Kontextanreicherung kombiniert werden.
- Der Kunde ist Eigentümer aller gesammelten Protokolldaten und kann sie für Anwendungsfälle nutzen, die über SIEM hinausgehen, z. B. zur Beobachtung von Betriebsabläufen, für Sicherheitsmetriken und zur Validierung von Kontrollen.

Erkennung und Reaktion mit Securonix + Snowflake

Im Gegensatz zu herkömmlichen Datenverbrauchsmodellen ist bei diesem gemeinsamen Bereitstellungsmodell Securonix Next-Gen SIEM eine nahtlose Erweiterung der Snowflake-Cloud-Umgebung des Kunden. Alle Sicherheitsprotokolle werden an einem Ort gespeichert und analysiert, was eine schnellere Erkennung und Reaktion auf Bedrohungen in der Umgebung des Kunden ermöglicht. Unternehmen können mit Securonix und Snowflake vollständige Transparenz, verwertbare Erkenntnisse, eine bessere Automatisierung und erhebliche Einsparungen erzielen.

Wenn Sie weitere Informationen über Securonix und Snowflake wünschen, vereinbaren Sie bitte einen Termin für eine Demo unter: **www.securonix.com/request-a-demo**

securonix