AppSentinels

AppSentinels
DATA PROTECTION
Capabilities

We are in the era of unprecedented connectivity and data growth. Data is getting created as well as shared at the fastest pace ever. Organizations are adding new APIs to facilitate faster exchange of data. For security leaders and practitioners, this presents new and daunting challenges with massive volume of data and new pathways to oversee, new threats to stay ahead of, and regulatory complexities to navigate. Security leaders must maintain visibility of data, manage user access to data, and enforce strong security and privacy controls. DLP, DSPM and DDR etc are few technologies to address the challenges related to data visibility & protection. This guide provides insights for security leaders while they evaluate right technology for data-security and highlights how AppSentinels API Security platform complements these tools to provide critical controls needed to protect organizations against data breaches and exfiltration.

Foundations

Let's start by looking at few underlying basics of all Data Security technologies:

1. Data Discovery

Where is my data? Discover data across structured & unstructured data stores like databases, storage blobs, drives/files, data-processing-pipelines etc. The discovery should be continuous and cover all kind of environments including cloud, on-prem and hybrid.

2. Data Classification & Risk Assessment

What data is critical from risk perspective? Identify critical sensitive business and personal data and the risk is represents for the organization. Organizations can decide what data is critical to be secured vs data that is 'okay' to lose!

3. Data Access Privilege Management

Who has access to the data? Check for access privileges and permissions to the users & roles in the organization. With respect to the data in question and its associated risk, identifies misconfigurations in the configured access permissions like is data store publicly accessible, is un-encrypted or with weak encryption, backup not kept securely etc. Also checks for over-privileged access rights to users or roles.

This is mostly focused on the Internal User activity.

4. Data Access Monitoring

Monitors who's accessing the data at various time. Performs analytics to identify any anomalous pattern of access. It monitors files access, emails, databases, backups, snapshots etc.

Security Products Offering Data Security

Over the years, multiple security products have tried to solve the problem. However, no single technology or product have solved it holistically. Let's briefly look at these technologies:

1. Data Leak Prevention (DLPs)

- These were the first breed of product initially built around mid/late 2000's.
- Focus was to prevent data exfiltration from Endpoints.
- Provide controlled access to USBs, network-filesystems, emails, clipboards, screenshot/recordings, backups etc.
- Had immature data classification technology and suffered from lots of false positives.
- Were tough to configure & manage and were mostly deployed in monitoring mode.

2. DAM (Database Access Monitoring)

- Primarily meant to monitor and control access to the database(s).
- Built on top of role-based database access control to DB tables.
- Provide granular controls to specific rows & columns of database tables to specific users/roles.

3. DSPM (Data Security Posture Management)

- New gen products built over last 4-5 years. Has better data discovery & classification. Assign labels and helps simplify DLP policy enforcement.
- Support single & multi-cloud, hybrid and On-Prem environments though capabilities in hybrid/on-prem environments are limited.
- Find risky misconfigurations like overprovisioned access permissions, entitlements, group memberships, data-storage without encryption, data-movement without strong encryption etc.
- Monitor access to data including activities like backups, snapshots, emails, access via encrypted channels etc.
- Focus on insider threats (internal users) and depend mostly on anomaly-based detection.

Limitation of data-security technologies

While data-security products are good in discovery, classification & risk assessment of data-at-rest, capabilities for data-in-motion are limited. It's well known that APIs are the preferred pathways of exchanging data today. Unfortunately, **data-security products are blind to your application APIs. They don't understand deeper context of the APIs – the users calling the APIs and operations they are performing including any sensitive data access via the APIs. For these products, API is a legitimate access to the data by the application**. They don't know if a rouge user is manipulating APIs and accessing someone else data or exfiltrating any data!

Let's understand this limitation with an example -

Optus Breach – a data breach via APIs Limitation of DSPM Technologies

In Sept 2022, second largest telecom service provider in Australia suffered a major data-breach. Personal information including credit-card numbers of close to 10 million customers comprising a third of Australia's population was leaked due to an API flaw. This was equivalent of around 90% of the customer-base of Optus. There was an unauthenticated API that can be called by any user. Further, the API also had a BOLA vulnerability where a user can manipulate and pass someone's phone-number, and the API would return the personal details of the owner of that phone-number to the caller. A single API resulted in the massive data-breach. Unfortunately, such APIs exist in all organizations. This incident resulted in class-action lawsuit against the company, regulatory fines and loss of trust customers. One estimate put the cost to Optus at A$140 million including replacement of the lost official documents and credits it had to provide to affected customers.

Similar breaches were disclosed by LinkedIn (2021), Meta (2019), Twitter (2019, 2020 & 2022).

How AppSentinels can help?

AppSentinels is a development to production full-life cycle API security platform that helps organizations in **SHIFT-LEFT by helping developers build secure APIs faster** and **PROTECT-RIGHT by helping security teams protect applications against run-time business-logic API attacks**. The platform builds deep white-box understanding of the Application behavior including various user journeys and business logic graphs and uses this insight to:

- It discovers all APIs in real-time including shadow/unused/orphaned/public-internal/sensitive/privilege APIs, discovers PII/Sensitive data in the APIs as well as provide real-time risk score of the APIs.
- It blocks zero-day API attacks and API abuses to protect applications from breaches, frauds and data loss.
- It provides pin-pointed remediation to developers to fix API vulnerabilities and insights to security teams to protect applications against run-time attacks promptly and precisely.

The platform supports all kinds of applications and onboards any application in minutes.

The platform monitors each API, user activity and understands if the operation and the data being accessed is authorized or not. It knows if a user is trying to manipulate an API and trying to exfiltrate data.

Summary

APIs are the pipelines to access data. A security leader can't secure its data without securing the pipelines used to access the data. Unfortunately, APIs are the blind spots of all data-security products. This is where AppSentinels comes in as it has complete understanding of APIs and the data being accessed through the APIs. AppSentinels bring complete visibility, and provides critical controls to security leaders to stop data exfiltration via APIs, data-scraping attempts etc.

Contact AppSentinels to discovery more about your APIs -
contact@appsentinels.ai | www.appsentinels.ai