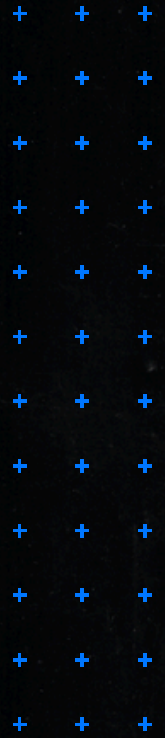




# DATA SECURITY PLATFORM BUYER'S GUIDE



+ + +

# INTRODUCTION

+ + +

+ + +

Data is an enterprise's most valuable — and vulnerable asset. In 2024, the No. 1 consequence of cyberattacks was data exfiltration.

+ + +

+ + +

While organizations have endpoint and perimeter security, traditional “castle-wall” security strategies fall short when it comes to securing data. Most cyberattacks use techniques that bypass perimeter security, like social engineering and password sprays. Once in the environment, bad actors overwhelmingly target data.

+ + +

+ + +

+ + +

+ + +

Increasing data volumes, more attack vectors, and new risks from generative AI all make data security challenging. To address these challenges, enterprises are turning to Data Security Platforms to secure sensitive data and prevent breaches.

+ + +

+ + +

+ + +

## THE RISE OF THE DATA SECURITY PLATFORM

Traditionally, data security approaches have been fragmented. Key capabilities like data loss prevention, access governance, and threat detection have been spread across disparate tools. Now, enterprises are turning to Data Security Platforms to secure sensitive data, create operational efficiencies, and remove the manual burden of managing numerous tools and solutions.

*“Organizations have traditionally tackled [data security] via ‘point’ solutions — individual applications or solutions — for data loss prevention (DLP), governance, data protection, encryption, and threat detection. However, as data volumes and complexity continue to grow, so does the complexity of managing multiple solutions, further increasing costs and risks to a business’s data assets.”*

— GigaOm Radar for Data Security Platforms 2024

The Data Security Platform market is crowded with solutions that seem to take a platform approach on the surface but fail to effectively secure data. This guide aims to help you better understand Data Security Platforms and avoid common mistakes when selecting one.

+ + +

+ + +

+ + +

+ + +

+ + +

+ + +

+ + +

+ + +

+ + +

+ + +

+ + +

+ + +

# Three evaluation tips for CISOs

Below are three of the top tips for CISOs evaluating a Data Security Platform:

## 1. RUN A PROOF-OF-CONCEPT (POC)

The golden rule when evaluating any new technology is to validate claims with a POC. Vendors who refuse to do a POC should raise red flags. Try to do a proof-of-concept on production systems or sandboxes that mimic your production environment. POCs are important for understanding the scale and accuracy of a DSP.

## 2. READ REAL CUSTOMER REVIEWS

Be careful judging vendors based on awards and press, many of which are pay-to-play. Look for validated reviews from trusted sources like Gartner and Forrester. Ask to speak directly to reference customers and make sure they have customer case studies on their website.

## 3. ASK FOR A SAMPLE RISK ASSESSMENT

Ask to see an anonymized risk report from a real customer. This can help you understand if the vendor offers the level of granularity and depth you're after. Sample reports can help you determine if a POC is worthwhile.



# Not all Data Security Platforms are created equal.

The sheer number of offerings in the security space makes it difficult to distinguish what is and isn't an effective approach to data security. Below, we've listed some of these technologies that, on the surface, may seem to offer data security but ultimately don't provide the completeness of a Data Security Platform.

## PERIMETER-ONLY-SECURITY

Every organization has perimeter security tools like an EDR, firewalls, and a SIEM. While these tools are important for an overall security strategy, it is a mistake to think they are enough to secure your data.

Most data breaches completely bypass the perimeter, including [the No. 1 cause of cyberattacks](#): compromised identity. When an identity is compromised, the perimeter essentially becomes non-existent.

Some tools might seem like they secure data, like cloud security posture management (CSPM) or cloud-native application protection platforms (CNAPP). In actuality, these tools aren't a substitute for a Data Security Platform. An effective Data Security Platform secures the data itself and the tools in place to prevent data breaches and detect threats.

## ECOSYSTEM-SPECIFIC TOOLS

Nearly every platform comes with native security tools, including AWS, Microsoft, and Salesforce. While these native tools can be a starting place, they aren't a replacement for a Data Security Platform.

The first and most obvious shortcoming is that native tools don't extend across your environment. Suppose you rely on Amazon Macie to secure data in S3, for example. In that case, you will need additional resources to manage the native tools in Box, Google Drive, Microsoft 365, Salesforce, and more. In contrast, a Data Security Platform provides one central place to manage data security across your entire environment.

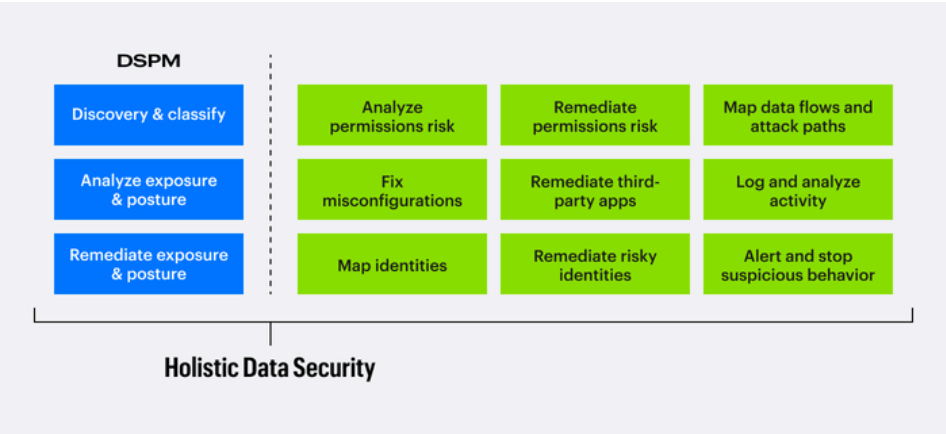
+ + +  
 + + +  
 + + +  
 + + +  
 + + +  
 + + +  
 + + +  
 + + +  
 + + +  
 + + +  
 + + +

Native tools come with complex configurations and require a good deal of manual effort. Each platform demand deep expertise and meticulous management. Most enterprises simply don't have the resources and expertise to manage these native tools to their fullest. As a result, misconfigurations are common — opening the door for a data breach. An effective Data Security Platform simplifies data security, detecting and fixing misconfigurations without requiring specialization or additional resources.

### DATA SECURITY SOLUTION

Numerous solutions claim to be a Data Security Platform — or could be confused for one. This is especially common with [data security posture management \(DSPM\)](#). These tools claim to secure data but are geared toward discovery and classification with surface-level posture capabilities.

While [data discovery and classification](#) are important parts of a Data Security Platform, they don't prevent data breaches. These tools cannot analyze permissions risks, remediate identity issues — the top cause of data breaches — alert on suspicious behavior, and more. The hard work of securing data falls on your team, and as a result, DSPM projects fail.



*DSPM stops short of securing data, leaving the hard work to security teams*

DSPM solutions are also most often focused on IaaS without the ability to cover data centers. This creates gaps in your approach to data security. An effective Data Security Platform goes beyond data discovery and classification to secure data and cover all critical data sources.







# Top five things to look for in a Data Security Platform

DSPs have emerged to address the challenge of securing large amounts of data in complex environments. These platforms seek to combine disparate capabilities into a single solution to help organizations streamline and scale data security. That said, not all DSPs have the capabilities needed to secure data and prevent data breaches. Below are five key requirements for an effective DSP.

## 1. Deep visibility






Deep visibility is the foundation for data security. An effective Data Security Platform delivers deep visibility into data, including sensitivity, permissions, identity, and activity.

Many data security solutions rely on sampling and periodic scans to scale data discovery. This is a mistake. Data exfiltration happens fast, and even a small amount of exposed sensitive data can lead to a serious data breach. An effective Data Security Platform should provide a complete and real-time view of your critical data.

An effective Data Security Platform must also go beyond classification to analyze configurations, data access activity, identity, and permissions. Without this context, it's impossible to know whether sensitive data is exposed or at risk.

Here are three questions to ask when evaluating the level of visibility that a platform provides:

- Is data classification complete, or does it rely on sampling?
- Is data classification real-time, or does it rely on periodic scans?
- Does the platform analyze activity, identity, and permissions?

| 29,648 events on sensitive data ▾   |                    | 18 alerted events ▾ | 1,719 events by admin accounts ▲ |                 |
|---|--------------------|---------------------|----------------------------------|-----------------|
| Platform  | Event type         | Object name         | Is sensitive?                    | Account type    |
|  | file modified      | HOW_TO_DECRYPT.txt  | ✓                                | Admin           |
|  | share link created | Bonus.xlsl          | ✓                                | Executive       |
|  | file deleted       | Product_SKUs.pptx   |                                  | User            |
|  | client DNS request | mega.co.nz          |                                  | Admin           |
|  | authentication     | corp.local          |                                  | Service account |

## VARONIS OFFERS DEEP VISIBILITY INTO SENSITIVE DATA.

Varonis provides a complete, real-time view of sensitive data, including activity, identity, and permissions. Varonis scans multi- petabyte customer environments top-to-bottom without relying on sampling. Classifications are always current, and every change or addition is tracked to provide an up-to-date understanding of risk.

## 2. Automated remediation

Manually fixing security issues doesn't scale in complex environments with huge volumes of data, permissions, and configurations to manage.

An effective Data Security Platform should automatically remediate issues and enforce policies. Some data security solutions claim to provide automated remediation, but their capabilities are limited to creating support tickets or suggesting actions. An effective Data Security Platform should be able to automatically take steps to improve data security like right-sizing permissions and enforcing MFA directly — with minimal effort from your team.

Below are some questions to ask Data Security Platform vendors about automated remediation:

- What specific data risks can be remediated?
- Can automations be executed natively?
- Are changes committed to the target platform?



*“You want your Data Security Platform to enforce policies that secure your data while enabling data use with minimal friction. Success here will pave the way for generating greater value from your investment in a Data Security Platform as you expand your use of the full breadth of capabilities within the offering.”*

— Forrester

| Policies                         |             |  |                                   |
|----------------------------------|-------------|--|-----------------------------------|
| Name                             | Category    | Event type                                       | State                             |
| Remove collaboration links       | Remediation | <a href="#">remove collaboration links</a>       | <input type="checkbox"/> Disabled |
| Remove links                     | Remediation | <a href="#">remove collaboration links</a>       | <input type="checkbox"/> Disabled |
| Remove stale collaboration links | Remediation | <a href="#">remove stale collaboration links</a> | <input type="checkbox"/> Disabled |
| Remove stale membership links    | Remediation | <a href="#">remove collaboration links</a>       | <input type="checkbox"/> Disabled |
| Remove stale permissions         | Remediation | <a href="#">remove stale permissions</a>         | <input type="checkbox"/> Disabled |

**VARONIS CONTINUOUSLY AND AUTOMATICALLY REMEDIATES DATA SECURITY RISKS.**

Varonis can automatically remediate numerous issues that, if left unaddressed, put data at risk. This includes eliminating risky permissions, fixing misconfigurations, and more without manual effort. Varonis comes with ready-made remediation policies that you can personalize for your organization.



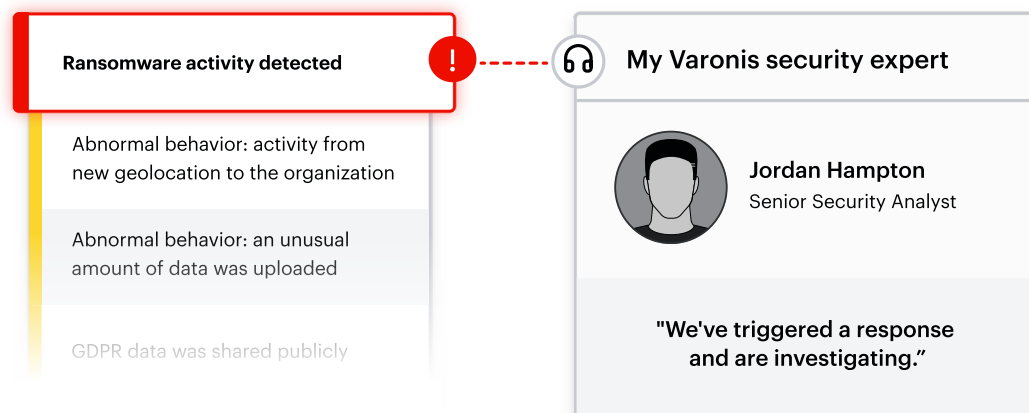
### 3. Proactive threat detection and incident response

Data exfiltration is the No. 1 consequence of a cyberattack. Even with the right perimeter and posture security protection, bad actors and rogue insiders can enter your environment and target sensitive data.

An effective Data Security Platform should be able to detect suspicious activity and respond to threats. Proactive threat detection and incident response are a crucial part of data security.

Below are some questions to ask Data Security Platform vendors about threat detection and response:

- Does the platform alert you to anomalies and suspicious behavior?
- Does the platform provider offer support for incident response and investigations?
- Does the platform provide a searchable audit trail for investigations?



#### **VARONIS STOPS DATA BREACHES.**

Varonis monitors for suspicious behavior in real time. Hundreds of expert-built threat models automatically detect anomalies, alerting you to unusual file access activity, email send/receive actions, permissions changes, geo-hopping, and much more.

Varonis also offers [Managed Data Detection and Response \(MDDR\)](#), the industry's first managed service dedicated to stopping threats at the data level.

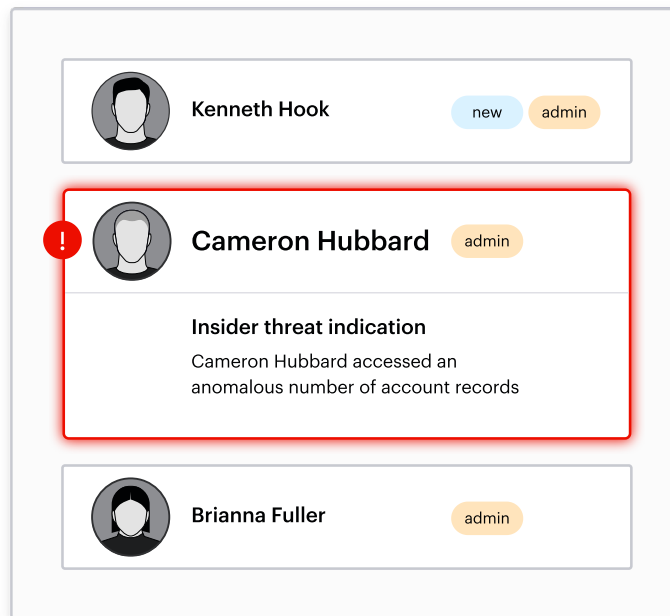
## 4. AI Security

The widespread use of AI will only increase the amount of data breaches. There is no way around it. AI copilots, agents, and infrastructure each introduce unique data security challenges and increase the likelihood of data breaches.

For example, copilots make it easy for bad actors to exploit high-risk permissions to access sensitive data, and model poisoning makes it even more important to secure sensitive training data. In each case, data is at the heart of the risk.

An effective Data Security Platform must address the numerous risks that come with AI. Below are some questions to ask Data Security Platform vendors about AI security:

- How does your platform ensure the safe use of AI copilots and agents?
- How does your platform safeguard AI training data?
- Can your platform ensure that AI isn't accessing sensitive data?



### VARONIS LEADS IN AI SECURITY.

Varonis leads in AI security with capabilities to prevent the misuse of AI applications and safeguard sensitive data. Varonis offers [the industry's first data security solution for Microsoft 365 Copilot](#) and has a wide range of AI security capabilities for other copilots, LLMs, and gen AI tools.

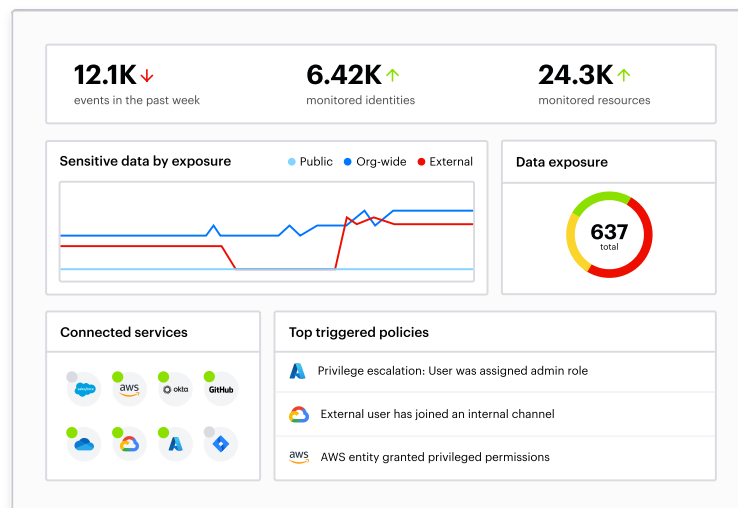
## 5. Coverage for all your critical data

An effective Data Security Platform must secure your critical data wherever it resides. Understand where your mission-critical data lives, prioritize those data stores, and ensure the vendor you select can cover each domain and data type.

While your concern today might be for your data in AWS or Salesforce, your approach to data security shouldn't be fragmented. Critical data resides everywhere, from the Box account used to share information with third-party vendors to the data platform your data analysts use to forecast revenue.

Ask yourself these questions about where your critical data resides:

- Do you have critical data in data stores like AWS, Azure, and Google Cloud?
- Does your organization leverage SaaS apps like Salesforce or Microsoft 365?
- Does your organization use data platforms like Databricks or Snowflake?
- How many SaaS applications in your organization have access to critical data?
- Do you have critical data on-prem?



### VARONIS PROTECTS ENTERPRISE DATA WHERE IT LIVES.

Varonis covers structured, unstructured, and semi-structured data across all three domains. Our platform also maps and monitors attack paths that provide access to data, including directory services (Active Directory, Okta, and Entra ID), network traffic from proxy servers, VPNs, DNS, and firewalls, and API/OAuth connections. Explore [all our coverage](#).

# Ready to secure your data?

The right Data Security Platform can help your company prevent data breaches, investigate incidents quickly, and ensure you're meeting increasingly stringent regulatory requirements.

By focusing on visibility, remediation, and scale, the Varonis Data Security Platform can help you overcome your biggest security risks with virtually no manual effort.

- ✓ Automatically discover and classify all sensitive content
- ✓ Automatically ensure correctly applied labels
- ✓ Automatically enforce least privilege permissions to reduce your exposure
- ✓ Continuously monitor sensitive data and respond to abnormal behavior

## SEE WHAT OTHERS HAVE TO SAY...

Varonis is the leader in data security and is trusted by more than 8,000 organizations to classify and protect their data. Here's what some of our customers said:

**"The transition to Varonis' cloud-native Data Security Platform was completely transparent, smooth, and magical. Varonis forecasts what's involved and what's required, and they helped us make better decisions to bring to our leadership. Having that knowledge is invaluable."**

**Senior Team Member**  
Fortune 500 Company

[Read case study ›](#)

**"Varonis was so easy to use and integrate into our systems that implementing the Data Security Platform just made sense. If they identify a critical risk, they escalate the matter, address it quickly, and give us confidence during the incident management process. They consistently go the extra mile."**

**Cybersecurity Administrator**  
Keeley Companies

[Read case study ›](#)



# YOUR DATA. OUR MISSION.

We hope this guide helps you find a Data Security Platform that can drive the outcomes you're looking for! If you have any questions, don't hesitate to [contact us](#).

## Partner with the leader in data security.

**Gartner**

**#1 DSPM vendor** on  
Gartner Insights

**FORRESTER**

**Leader in Forrester Wave™:**  
Data Security Platforms,  
Q1 2023

**GIGAOM**

**Leader in GigaOm Radar**  
for Data Security Platforms  
(DSPs)

## Reduce your risk without taking any.

Our free Data Risk Assessment takes minutes to set up and delivers immediate value. In less than 24 hours, you'll have a risk-based view of the data that matters most and a clear path to automated data security.

Get a demo at [www.varonis.com/demo](https://www.varonis.com/demo).



### About Varonis

Varonis (Nasdaq: VRNS) is a leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.

