Ray Security

WHITE PAPER

Ray Security

Not All Data Is Created Equal

Jan 13, 2025

Ray Security

Ray Security Benefits

- → Reduce **data attack surface** by 90% within weeks
- → Get most value from a classification project in weeks, not years
- → Achieve over 90% data-level ransomware resilience, even when hackers bypass the traditional defenses
- → Remove unused access permissions across your entire data estate, both on-premise and in the cloud

Jan 13, 2025

TABLE OF CONTENTS

INTRODUCTION

Data leaks pose a significant risk for every organization, overshadowing external security breaches. Hope and personal responsibility alone are insufficient to safeguard your organization. Ray Security provides full data inventory and can help dramatically reduce your data attack surface, help with much better ransomware resilience, and give you an unprecedented view of your data behavior.

NOT ALL DATA IS CREATED EQUAL

The Ray Approach

How often have you heard that most enterprises possess far more data than they realize? They need help knowing where it's stored, who has access to it, whether it's secure, and whose personal information it contains.

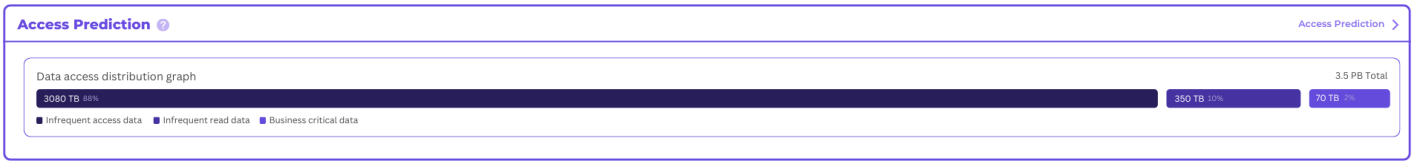
We get it.

Even today, there's no comprehensive solution to protect and manage data security across hybrid, on-prem, and cloud environments. No answer covers end-to-end security, permissions, resilience, full ransomware protection, and automation. It's simply too complex—until now.

Introducing Ray's Preemptive Data Security

By leveraging proprietary time-series analysis, Ray predicts which data will likely be accessed. This predictive approach enables focused, high-granularity protection for frequently accessed data while ensuring rapid protection for data that remains dormant.

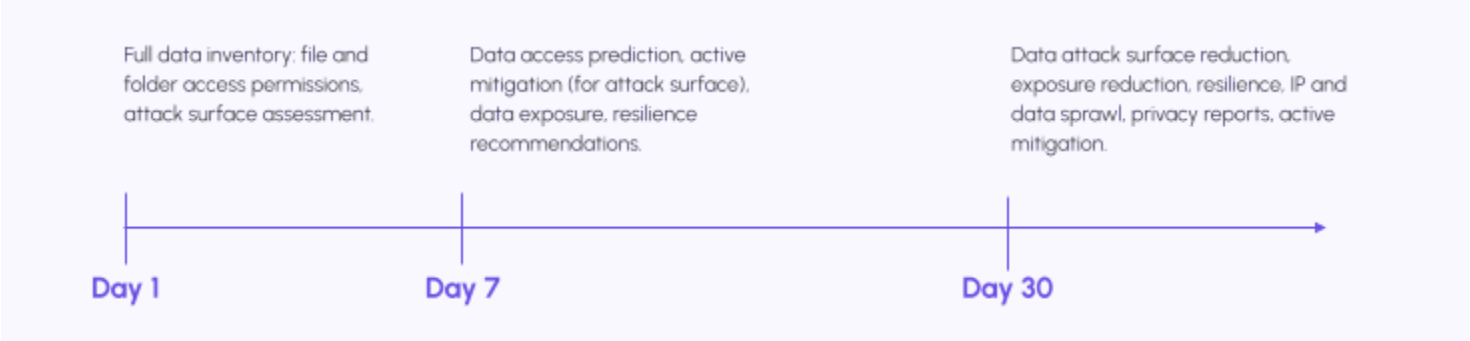
Ray Security was founded on the principle that not all data is created equal. The reality is that, at any given moment, we only use a fraction of the data available to us, and enterprises utilize just a portion of their overall data. The question then becomes: who benefits from the fact that the majority of the data - which you won't be accessing soon - is available? It's not you. The answer is simple: the attacker. In fact, on any given day, over 90% of the data in a typical enterprise is not accessed, which makes it beneficial only for malicious actors. It may not be the exact data daily, but it's the same percentage.



Preemptive Data Security Benefits

- ➔ Reduce your data attack surface in weeks
- ➔ Remediate overexposure
- ➔ Prioritize data classification projects to complete 80% of the needed job done in weeks, not years
- ➔ Dramatically faster data recovery after a ransomware attack: achieve over 90% data-level ransomware resilience (encryption and exfiltration), even when hackers bypass traditional defenses
- ➔ Easily protect sensitivities and comply with regulation

Deployment Timeline



Data Privacy

- When scanning data it's always important to make sure your data is safe and secured. Ray Security uses a wide range of protection mechanisms to make sure your data is never compromised nor is it exposed, even to the Ray Security system:
  - By default, the system only scans metadata, not file/DB contents.
  - Optionally, filenames and paths can be tokenized to prevent them from being exposed.
- For Data Classification use case:
  - The user needs to explicitly request the system to classify the data and examine data contents.
  - The user can limit the scope of data where classification happens.
  - The user can pause the system at any time.
  - No sensitive data is saved anywhere.

  the system has two modes to classify the data:

- Fast classification (on-prem) based on RegEx. Data sent to the backend does not contain any sensitive data.
- Deep classification (backend) that's deep, AI-based, and has data classification baked in. In this case, data is encrypted in transit and is never saved permanently so that no piece of sensitive data is present once the extraction of sensitive data is completed.
- In both cases, Ray Security's system only contains the notion of whether or not sensitive data is present (yes/no), not the data itself.

USE CASES

FULL DATA INVENTORY

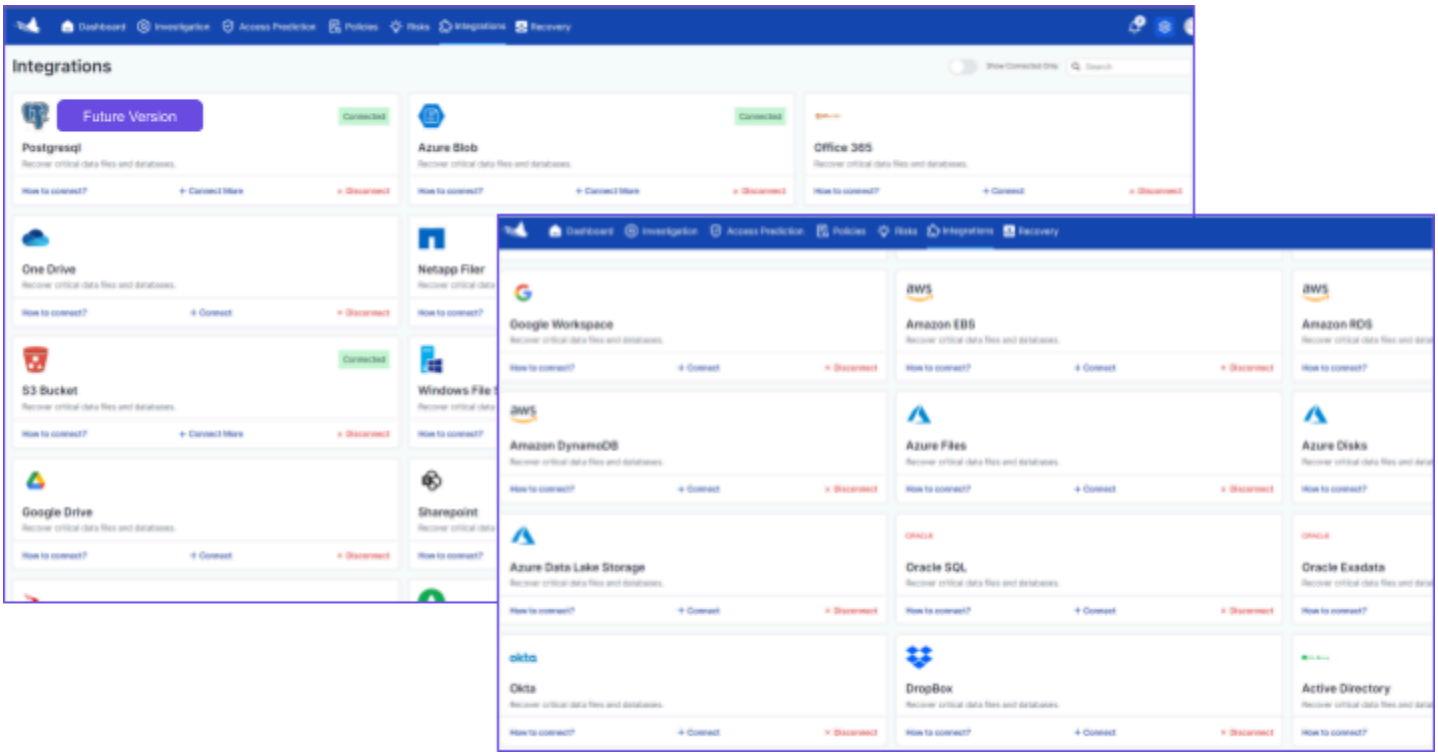
Ray Security provides comprehensive visibility across the entire data inventory. Ray Security ensures no data remains unseen by integrating various data sources, including Windows/Linux operating systems, enterprise storage solutions, and cloud platforms like SharePoint, Google Drive, and Amazon S3. The system's ability to collect metadata such as file names, locations, origins, and access history, combined with advanced machine learning algorithms, enables precise monitoring and analysis of data access patterns. This ensures that organizations can accurately identify critical data, understand usage patterns, and safeguard sensitive information. As a fully managed SaaS offering, Ray Security eliminates the need for complex deployments and ongoing maintenance.

Single Pane Of Glass

Ray's system is deployed as a complete SaaS solution (no deployment) or on-prem (in which case no data leaves your organization).

The system integrates with various data sources to provide unified discovery, management, and protection capabilities across multiple platforms. Whether it's cloud storage, databases, or on-premise servers, Ray can protect critical data files and databases across:

- **Databases:** Postgresql, Oracle SQL, MongoDB, Snowflake, Amazon RDS, Google Cloud SQL, DynamoDB, and more.
- **Cloud Storage:** Azure Blob, S3 Buckets, OneDrive, Google Drive, and Dropbox.
- **File Systems:** NetApp Filer, Windows File Server, AWS EFS, Google Cloud Filestore, Azure Files.
- **Enterprise Applications:** Office 365, Google Workspace, SharePoint.
- Backup Solutions: Rubrik, Veeam, Dell EMC.
- **Security Tools:** CrowdStrike Falcon, Palo Alto, Okta, Active Directory.



Ray leverages these integrations to enable easy data inventory, protection, and even recovery, providing rapid access to business-critical files across all connected systems. Through unified management, administrators can easily match the protection level to the data criticality throughout these sources, ensuring data protection and business continuity. Additionally, Ray's predictive analytics ensures that critical data is protected before it is accessed, further optimizing resilience.

Consistent Data Security Policy

Securing data across diverse and fragmented infrastructures is inherently challenging due to the overwhelming volume of data and the lack of coordination between security features across different data stores. Each data repository operates with its unique security configurations, making centralized governance nearly impossible without additional tools. Ray Security addresses this complexity with a unified platform offering a single pane of glass for managing security policies. This approach allows organizations to enforce consistent data security policies across all their systems. For example, administrators can automate the removal of unused read permissions for data that has been dormant for extended periods. Ray's system interprets and applies such policies uniquely for each data store, ensuring compliance with the store's specific requirements while

maintaining overarching security goals. This harmonized framework reduces complexity, enhances efficiency, and fortifies data protection across the enterprise.

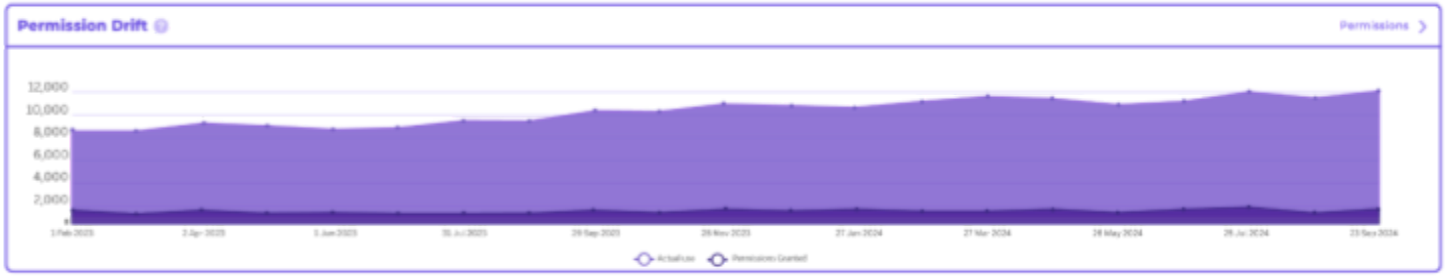
RANSOMWARE RESILIENCE

Exfiltration Resilience And Minimizing Potential Damage

Ray Security's advanced time-series, proprietary AI analysis minimizes the risk of data exfiltration through its advanced access management and monitoring systems. The system continuously monitors file access patterns, identifying and responding to over 90% of unusual activity (thus, virtually almost every intruder will be noted). By dynamically adjusting its prediction and requiring multi-factor authentication (MFA) for access to critical data, Ray reduces the attack surface and limits the potential damage caused by unauthorized access.

Data Breach/Leak Resilience

Ray Security's approach to data breach and leak prevention is rooted in its comprehensive data classification and monitoring capabilities. The system predicts future data usage based on importance and urgency, ensuring that critical information is given the highest level of protection. Near-Real-time data access monitoring and automated response mechanisms, such as alerts, MFA, or user session termination, provide an additional layer of



defense against data breaches and leaks. Unlike other solutions, and as noted earlier, this is orchestrated across the entire data estate, making data breach/leak prevention much more straightforward.

Software-Defined Data Immutability, Encryption Resilience, and Faster Recovery

Ray Security introduces a revolutionary approach to data protection by enabling dynamic management of write permissions, a feature that significantly enhances data resilience. Unlike read permissions, write permissions are rarely necessary for most users in day-to-day operations. Restricting write permissions has minimal impact on user functionality since users can always create copies of the data for their workflows. However, this strategic restriction delivers a profound security advantage: over 90% data immutability is achieved, eliminating the need for additional hardware or specialized devices, as competing solutions require.

This level of immutability drastically reduces the risk of unauthorized changes or encryption, effectively shrinking the attack surface for ransomware and other encryption-based threats. Furthermore, Ray Security seamlessly integrates with existing backup solutions, leveraging its advanced analytics to identify and prioritize restoring critical data. Organizations can ensure a swift and efficient recovery process by focusing on data that directly impacts revenue generation. Simultaneously, Ray's immutability measures safeguard less critical data, offering a dual-layered defense strategy combining prevention and recovery.

This combination of in-place immutability and targeted recovery optimization gives organizations a powerful, cost-effective means to protect their data assets. It mitigates the risk of data loss or corruption and ensures that recovery efforts are strategically aligned with business priorities, maximizing operational continuity and resilience.

Why Ray Security Ransomware Resilience Is Better

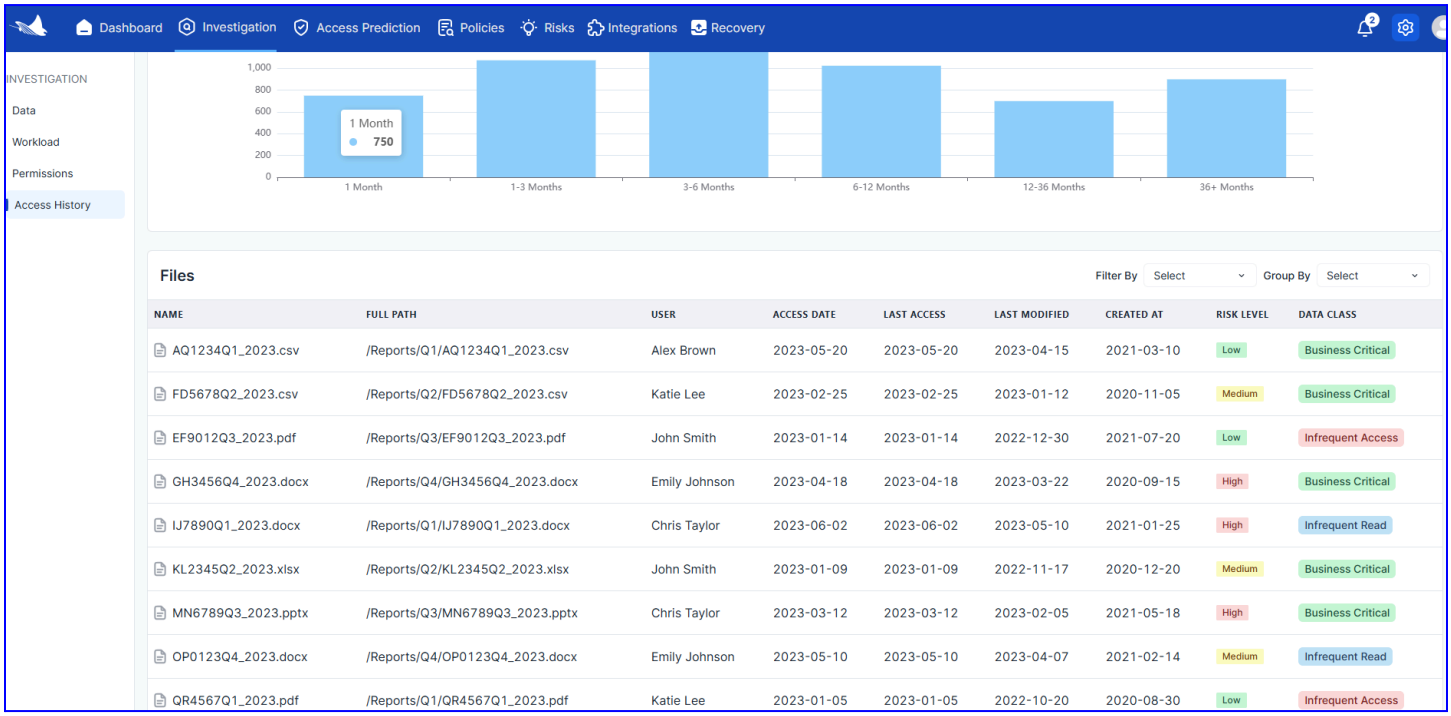
		Ray Security	Legacy Security Platforms	DSPMs	EDRs and Specialty EDRs	Backup
Encryption Blast Radius Reduction And Resilience	Encryption prevention[1] (actively stop encryption)	✅[2]	❌	❌	✅	❌
	Encryption resilience (reduce blast radius to a minimum and provide fast recovery for the rest)	✅[3]	❌	❌	✅[4]	❌
	Fast recovery	✅[5]	❌	❌	❌	🟨[6]
	Reliable restore	✅	❌	❌	❌	❌
	Non-encrypted backup	✅	❌	❌	❌	🟨[7]
Exfiltration Blast Radius Reduction And Resilience	Exfiltration resilience (reduce blast radius by removing unneeded permissions)	✅	✅[8]	❌	✅	❌
	Exfiltration prevention (reduce blast radius by removing unneeded permissions)	✅	❌	❌	✅	❌
	Mitigation by sensitive data mapping	✅	✅	✅	❌	❌
Protected Infra	Endpoint	❌	❌	❌	✅	❌
	Central data stores (on-prem and cloud)	✅	✅	✅	❌	✅
	Data pipelines	✅	❌	❌	❌	❌
Efficiency	Unified Actionable Data Security Policy	✅	❌	❌	✅	❌

[1] Suspicious activity identification (mass read/write, irregular connections, and more - depending on the technology)
[2] Depending on policies in place and infrastructure capabilities. In typical scenarios ~90% of the data is protected from encryption with self-access governance, activity governance and automatic permission management. The protected data automatically changes daily by prediction.
[3] By protection 90%-95% of the data from encryption
[4] Some vendors provide the ability to decrypt certain strains of ransomware.
[5] Ray provides fast, simple, statistically
[6] Vendor specific
[7] Vendor specific
[8] Manual effort required

DATA ACCESS GOVERNANCE

Ray integrates with data access logs and event logs, allowing you complete visibility of the access patterns to your data. This includes common use cases such as:

- Who accessed/accesses what
- What is/is not accessed
- Which data is not used / not expected to be used soon
- Which permissions are not used / not expected to be used
- Data "heatmap": which data is more frequently used and by whom
- Least privileges analysis



NAME	FULL PATH	USER	ACCESS DATE	LAST ACCESS	LAST MODIFIED	CREATED AT	RISK LEVEL	DATA CLASS
AQ1234Q1_2023.csv	/Reports/Q1/AQ1234Q1_2023.csv	Alex Brown	2023-05-20	2023-05-20	2023-04-15	2021-03-10	Low	Business Critical
FD5678Q2_2023.csv	/Reports/Q2/FD5678Q2_2023.csv	Katie Lee	2023-02-25	2023-02-25	2023-01-12	2020-11-05	Medium	Business Critical
EF9012Q3_2023.pdf	/Reports/Q3/EF9012Q3_2023.pdf	John Smith	2023-01-14	2023-01-14	2022-12-30	2021-07-20	Low	Infrequent Access
GH3456Q4_2023.docx	/Reports/Q4/GH3456Q4_2023.docx	Emily Johnson	2023-04-18	2023-04-18	2023-03-22	2020-09-15	High	Business Critical
IJ7890Q1_2023.docx	/Reports/Q1/IJ7890Q1_2023.docx	Chris Taylor	2023-06-02	2023-06-02	2023-05-10	2021-01-25	High	Infrequent Read
KL2345Q2_2023.xlsx	/Reports/Q2/KL2345Q2_2023.xlsx	John Smith	2023-01-09	2023-01-09	2022-11-17	2020-12-20	Medium	Business Critical
MN6789Q3_2023.pptx	/Reports/Q3/MN6789Q3_2023.pptx	Chris Taylor	2023-03-12	2023-03-12	2023-02-05	2021-05-18	High	Business Critical
OP0123Q4_2023.docx	/Reports/Q4/OP0123Q4_2023.docx	Emily Johnson	2023-05-10	2023-05-10	2023-04-07	2021-02-14	Medium	Infrequent Read
QR4567Q1_2023.pdf	/Reports/Q1/QR4567Q1_2023.pdf	Katie Lee	2023-01-05	2023-01-05	2022-10-20	2020-08-30	Low	Infrequent Access

BREACH RESILIENCE AND PERMISSION MANAGEMENT

Ray analyses permissions associated with your data to provide a complete map of who can access what data. This allows you to identify overly accessible data and gaps. The system provides a unified dashboard, or "single pane of glass", simplifying permission reduction and least privilege. This centralized view allows administrators to easily track, audit, and modify permissions, ensuring compliance with least privilege principles while maintaining streamlined control over data access.

Elastic Permissions

Moreover, Ray can dynamically adjust data permissions based on real-time usage patterns, ensuring that only the necessary identities can access the data when required. This automated, usage-based approach provides better security by monitoring, alerting, and minimizing unnecessary access.

Ray Security's elastic permissions system combines permission management with data access history. This dynamically alerts or even adjusts access permissions based on real-time analysis of usage patterns. By reducing unnecessary permissions, Ray Security minimizes the attack surface, particularly for infrequently accessed, sensitive, regulated, or any combination of these. To ensure no additional work is put on the CISO team, the system provides self-service break-glass mechanisms to allow users to grant themselves access with an MFA and similar means with which the system integrates.

Better Data Access Permissions

Traditional data access permissions are outdated—limited to basic read, write, and a few sub-categories, they are inconsistently applied across infrastructures, creating complexity and increasing security risks. Ray Security transforms this outdated paradigm with a unified management platform that simplifies and standardizes permissions across all systems, ensuring consistency and control. But Ray doesn't stop there. It goes beyond traditional models to introduce an innovative meta-layer that revolutionizes access control.

Key features of Ray's advanced permissions include:

- **Record-Limited Access:** Restrict users to a specific number of records and receive alerts on potential over-access, enabling proactive monitoring and control.

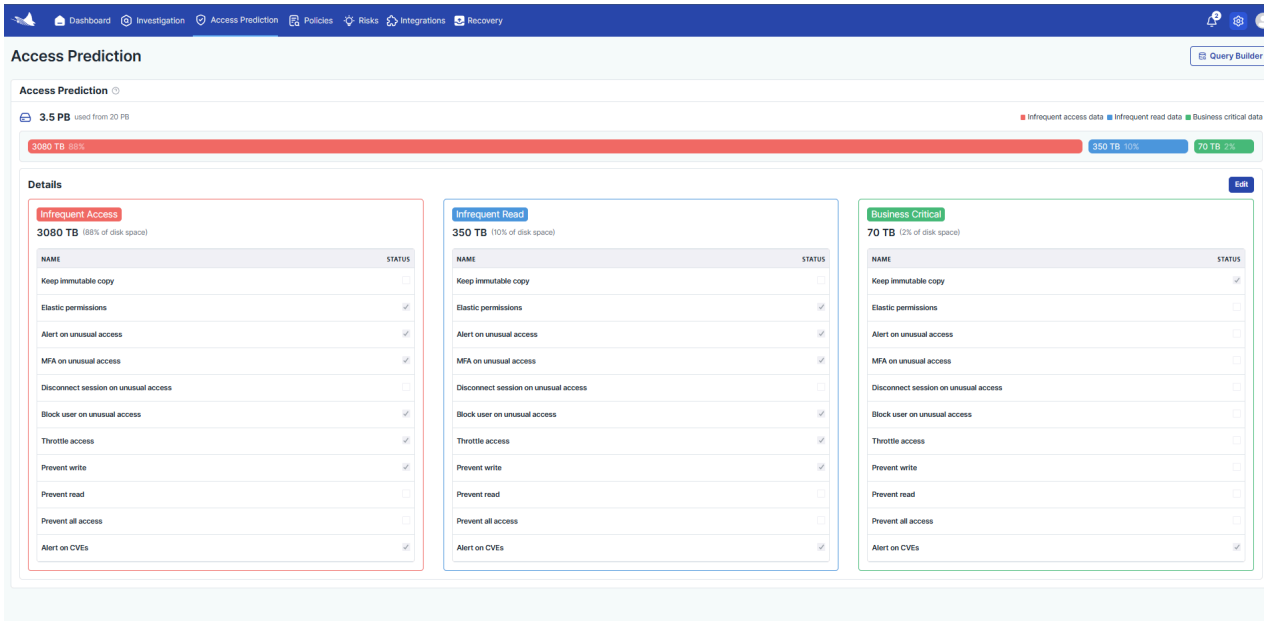
- **Modified File Access:** Grant access to customized versions of files as determined by external engines, ensuring data relevance and security.
- **Time-Bound Permissions:** Allow read or write access for a defined period, minimizing exposure while maintaining operational flexibility.

Implications for Read vs. Write Permissions

The introduction of these advanced capabilities has unique implications for read and write permissions. Traditionally, write permissions pose a greater security risk, as unauthorized write access can lead to data corruption, ransomware attacks, or accidental overwrites. By implementing time-bound and modified access controls, Ray Security ensures that write permissions are granted only when necessary, significantly reducing the likelihood of unauthorized or inadvertent data modifications.

However, read permissions, often considered less risky, also demand careful oversight in today's data landscape. Unrestricted read access can lead to data exfiltration, intellectual property theft, or unauthorized insights into sensitive operations. Ray's record-limited access introduces a groundbreaking layer of control for read permissions, enabling organizations to limit exposure while maintaining operational needs. For example, a user accessing sensitive data can be restricted to a small subset of records, reducing the risk of large-scale data leaks without hampering productivity.

By differentiating and enhancing how read and write permissions are managed, Ray Security bridges critical gaps in traditional access control systems. This dual-layered approach allows organizations to address both immediate security needs and long-term governance goals, creating a robust framework for modern data protection. These innovations don't just mitigate risks—they redefine how permissions align with organizational priorities.


Dashboard
Investigation
Access Prediction
Policies
Risks
Integrations
Recovery
Access Prediction
Query Builder
Access Prediction
3.5 PB used from 20 PB
Infrequent access data
Infrequent read data
Business critical data
3080 TB 88%
350 TB 10%
70 TB 2%
Details
Edit
Infrequent Access
3080 TB (88% of disk space)
NAME
STATUS
Keep immutable copy
Elastic permissions
Alert on unusual access
MFA on unusual access
Disconnect session on unusual access
Block user on unusual access
Throttle access
Prevent write
Prevent read
Prevent all access
Alert on CVEs
Infrequent Read
350 TB (10% of disk space)
NAME
STATUS
Keep immutable copy
Elastic permissions
Alert on unusual access
MFA on unusual access
Disconnect session on unusual access
Block user on unusual access
Throttle access
Prevent write
Prevent read
Prevent all access
Alert on CVEs
Business Critical
70 TB (2% of disk space)
NAME
STATUS
Keep immutable copy
Elastic permissions
Alert on unusual access
MFA on unusual access
Disconnect session on unusual access
Block user on unusual access
Throttle access
Prevent write
Prevent read
Prevent all access
Alert on CVEs

Why Ray Security Breach Prevention And Data Access Governance Is Better

		Ray Security	Legacy Security Platforms	DSPMs	Traditional Privacy Platforms
Permission management	Overly permissive data analysis	✅	✅	🟨	🟨
	Remediation actions	✅	❌	❌	🟨
Data Access Governance	Past data usage analysis	✅	✅	🟨	🟨
	Audit logs				
	Automatic least privileges[9]	✅	❌	❌	❌
	Future data usage prediction	✅	❌	❌	❌
Efficiency and Productivity	Unified data security policy	✅	❌	❌	❌
	Automatic data security policy (prediction based)	✅	❌	❌	❌
	Full coverage (cloud and on-prem)	✅	❌	❌	✅
	Fast time to value	✅	❌	❌[10]	❌

[9] Automatically match permissions to use

[10] Integration is easy, but the number of alerts is overwhelming

DATA CLASSIFICATION

Ray Security effectively uses advanced machine learning and natural language processing (NLP) to identify and categorize sensitive information. It analyzes file and database content to assign labels, enforce security controls, and identify PII, business-critical data, and regulatory-sensitive information.

What sets Ray apart are two key concepts:

a. Prioritized classification
b. Classification and permission integrated

By monitoring access rights and identifying over-privileged users, Ray ensures security controls align with data classification and exposure risks, preventing unauthorized access and streamlining compliance.

How The Ray's Approach Stands Out

Traditional data classification projects often take years to complete or incur significant costs. These efforts introduce risks of project mismanagement, excessive managerial attention, and lack of control over prioritization, leaving critical data unclassified and vulnerable for long periods. Ray Security addresses these challenges with an efficient, focused approach. As in real life, most of your data doesn't generate revenue at any point and, hence, does not need to be exposed for no reason. It makes sense to start with your code-red data. Don't just start classifying from an arbitrary data source the security team selects. Instead, take a conscious approach and let the system automatically decide where to start for you: start from the data that must be exposed while reducing the exposure to the still-unclassified data with more straightforward tools Ray provides.

The idea is simple:

- Start with identifying the data that you absolutely need to expose (that you need for the day to day operations).
- Protect unclassified data with reduced permissions or monitoring to minimize exposure.
- Dynamically classify data upon access for just-in-time security.
- Scale classification efforts based on available resources to balance priorities and reduce overhead.

- Constantly and dynamically monitor and limit user access to unclassified data by capping access to a small number of records, providing unmatched control and reducing exposure risks.

Ray's strategy secures both classified and unclassified data, mitigates the risks associated with traditional classification projects, and enables organizations to achieve robust protection without unnecessary complexity or delays.

Classify Proprietary Information

Ray Security's AI-based technology provides unprecedented accuracy in document classification. The system does not only rely on the usual LLM-based technique. It also learns directly from your data, based on your specific examples and training, to reach a resolution that is hard to get elsewhere. This allows you to classify proprietary information with greater accuracy and much better context and business results.

Protect Your Secret Information, PIIs, And Sensitive Data.

Classifying your data is essential for identifying document types, personal information, and business-critical data. Integrating data classification allows you to gain visibility into your data landscape, ensure compliance, and improve risk accuracy. With "efficient security," you can protect sensitive data dynamically, providing focused security measures precisely when and where they're needed, minimizing risk.

But Don't The GDPR, CCPA, And The Like Require Me To Classify All My Data?

While some do, others don't, however, you cannot classify everything on day one, so it's better to:

- Protect data in more than one measure even while the classification process is ongoing
- Control classification order and priorities

Don't Boil The Ocean

Ray Security prevents you from trying to boil the ocean: first, use the Ray Security prediction module to secure all the data where no access is expected. This allows you to focus your classification efforts on the most critical data - typically, 5% of the overall data.

In recent years, there has been a tendency to classify all data, but this approach can often be counterproductive. Protecting sensitive data is often easier when you don't even know it's there. It's more efficient to apply the

highest possible level of protection to all unneeded data and classify just in time rather than classifying everything and overwhelming teams with endless alerts.

Why Ray Security Classification Is Better

		Ray Security	Legacy Security Platforms	Traditional Privacy Platforms	Traditional DSPMs
Productivity	Prioritized Classification (Prediction-Based Or Policy-Based)	✅	❌	❌	❌
	Actionability	✅	❌	❌	❌
	Security Integrated (Permissions, Access Governance)	✅	✅	❌	❌
	Short Time To Value	✅	❌	❌	Partial
Classification Flexibility	Complex Classification	✅	❌	❌	❌
	PII And Regex	✅	✅	✅	✅
Coverage	On-Prem + Cloud	✅	Partial Cloud	✅	❌
	Structured + Unstructured	✅	❌	✅	✅
Compliance	Compliance	✅ Fast	Complex	✅	✅ Gazillion Alerts

DATA GOVERNANCE

Ray Security's data analytics capabilities enable organizations to gain deep insights into their data usage and security posture. The system's comprehensive querying capabilities allow you to obtain immediate, accurate, actionable insights about your data—all in one place.

COST REDUCTION AND LIFECYCLE MANAGEMENT

Knowing which data is likely to be accessed shortly allows Ray to optimize resource allocation, focusing storage and management costs on that specific subset of data that needs to be quickly available, tiering off and proactively back-hydrating data as predicted. Ray can avoid unnecessary costs for securing dormant or infrequently accessed data by predicting future access patterns. This targeted approach reduces storage, processing, and security expenses.

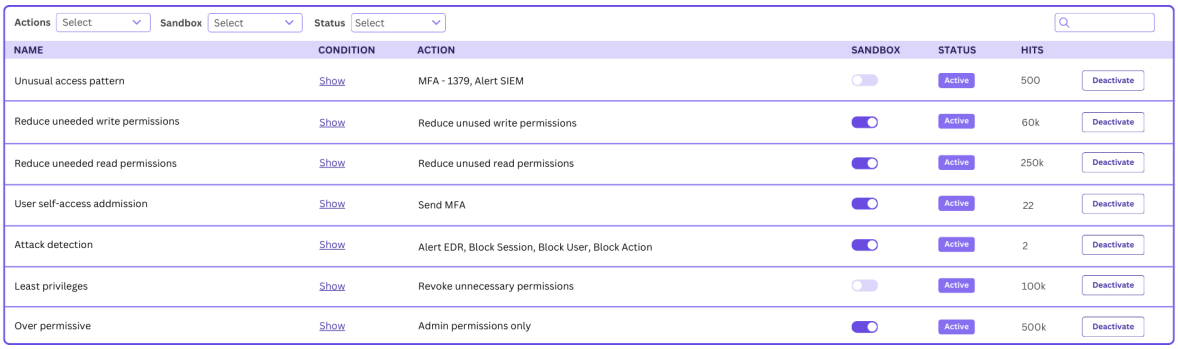
		Ray Security	Legacy Security Platforms	IT Data Movers
Productivity	Move with confidence (Prediction-Based data management)	✅	❌	❌
	Dynamic move (Move data between tiers based on access likelihood)	✅	❌	❌
	Gradual access retirement (First remove access, then tier internally, then tier off)	✅	🟨	❌
	Fast time to value	✅	❌	❌
Efficiency	Use existing infrastructure	✅	❌	❌
Compliance	Move with compliance	✅	🟨[11]	🟨[12]

[11] Multi-step: classify the data, filter the list and move it (sometimes with a different tool)
[12] Multi-step: classify the data, filter the list and move it (sometimes with a different tool)

DATA GOVERNANCE FOR AI AND CO-PILOT

The last few years have brought a surge of tools for reading, manipulating, and exposing enterprise data in new, innovative ways—GenAI-based systems, chatbots, and more. This has raised a new question: Which data is accessible to AI tools, what does it contain, and how can they control what they have access to?

On the one hand, you want your co-pilot to give good answers. On the other hand, you don't want it to expose all of your data to everybody. How do you manage the data it sees, ensure its integrity, and keep your secrets protected? Ray Security's next-gen analysis helps manage the attack surface of your personal, sensitive, or secret information while responsibly and controllably utilizing the latest chat technology.



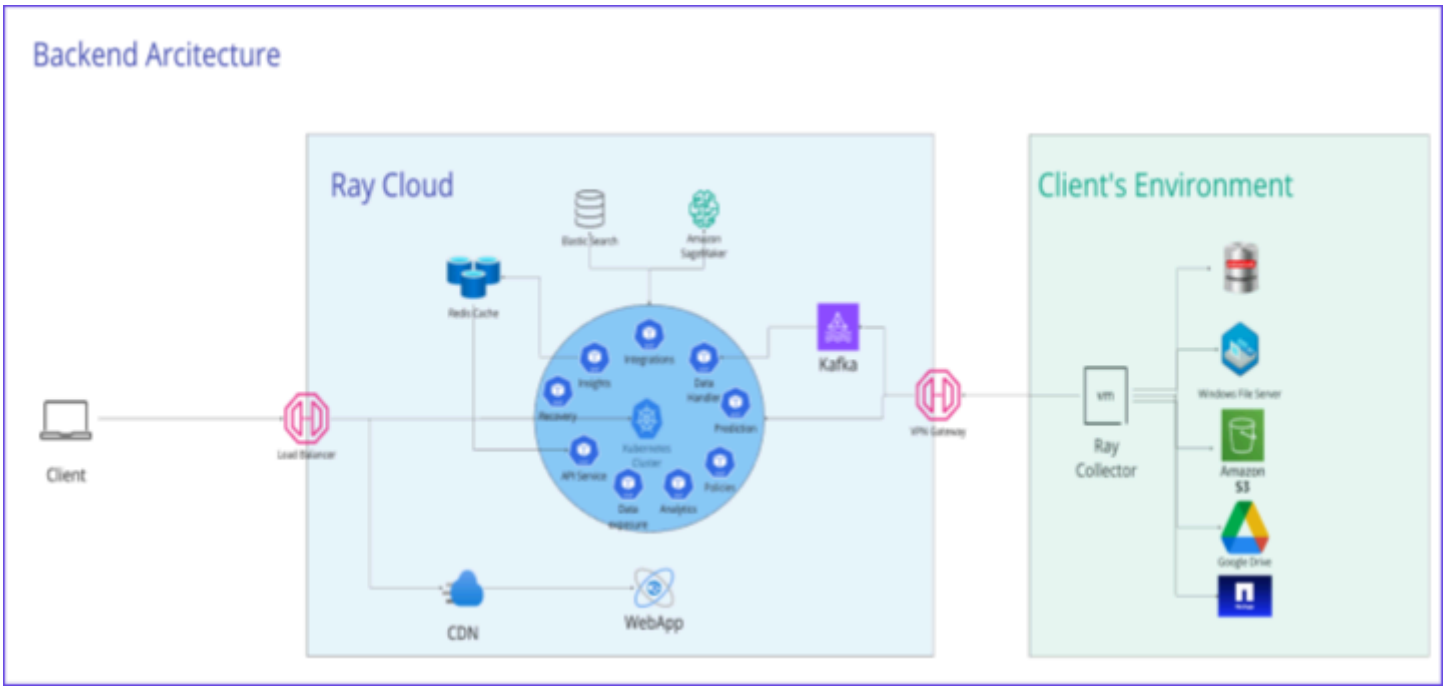
ARCHITECTURE

Components

Virtual Private Network

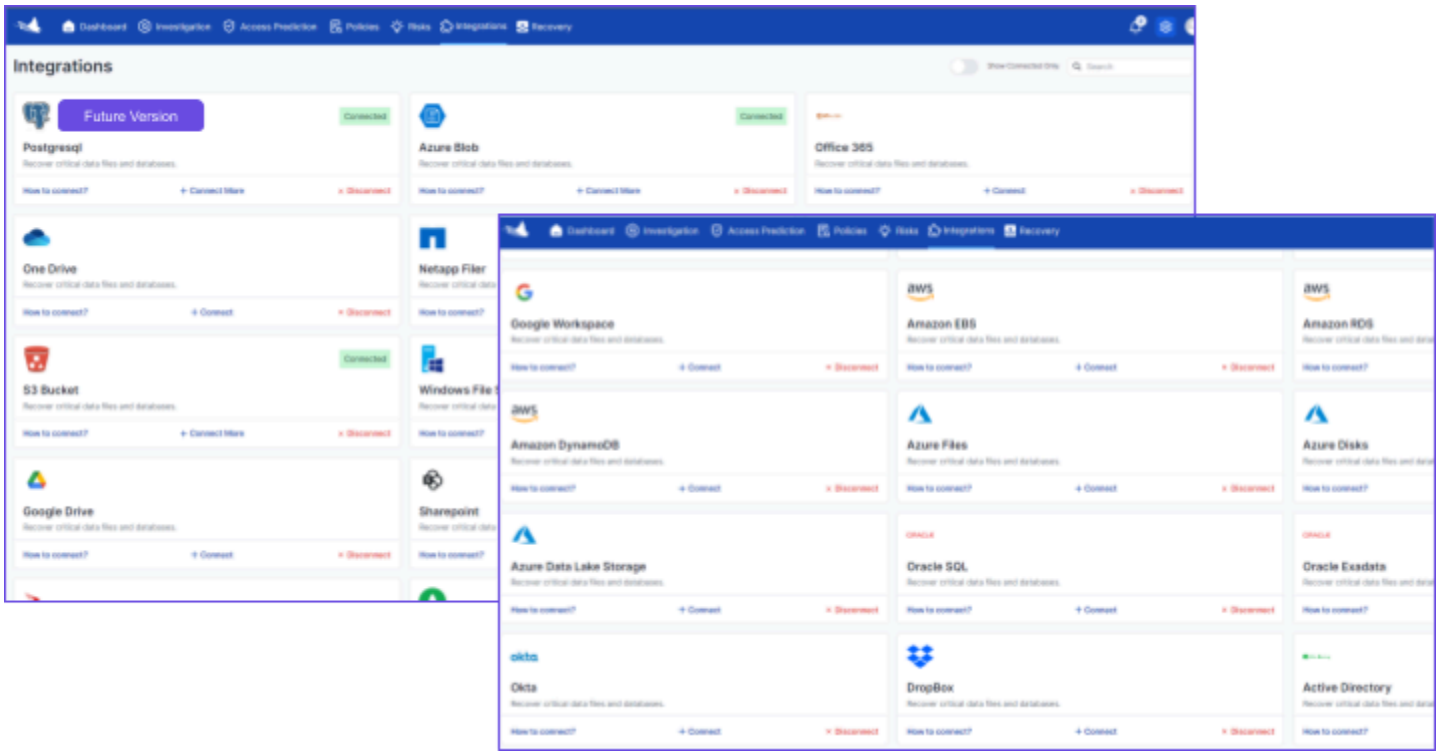
The diagram presented here assumes the customer uses a Private Network to provide a secure and isolated network environment within the Azure/AWS/GCP cloud or On-Premise, allowing resources such as VMs, databases, and applications to communicate privately, securely, and efficiently.

This assumption was made as private networks are a common choice for enterprises. This private network can be replaced with AWS VPC or any private network/On-premise network solution with equivalent features.



Data Source Example: Windows File Server

The diagram presented here assumes the customer has parts of their files on Windows servers. This dictates capabilities and performance and is validated at install time. No assumptions were made on the version. Also, the same architecture applies to different data sources. The screenshots below describe some of the supported data sources:



Ray's Collector

A single VM as presented in the diagram. Its main capabilities are to collect metadata and events, to connect to different types of systems using different protocols and to manage the protection lifecycle.

User Station

The User station presented in the diagram is the client's computers used to log in and use Ray's UI for insights, detections, and management console.

AWS VPC

Ray's Virtual Private Network presents Ray Security AWS-based VPC, used for networking inside the AWS account.

K8S Cluster

This represents the Kubernetes (K8S) cluster used to orchestrate and manage containerized applications within the architecture. This cluster hosts multiple services, such as prevention, detection, and integration services. It ensures scalable deployment and management of the applications, facilitating easy updates, high availability, and fault tolerance.

Prevention Service

A service running within the Kubernetes cluster, designed to identify threats proactively. This service utilizes a combination of rule-based algorithms and AI models to analyze behavioral patterns and file access data.

DB

Centralized database service used to store and manage all data related to user activities, file metadata, event logs, and detection outcomes. This component is crucial for data retention, analysis, and historical threat intelligence.