Ray Security

WHITE PAPER

Ray Security

Not All Data is Created Equal

Ray Security

WHITE PAPER

NOT ALL DATA IS BORN EQUAL

Ray Security Benefits

- → Reduce data attack surface by 90% within weeks
- → Complete a classification project in weeks instead of years
- → Achieve 98% 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

INTRODUCTION

For every organization, data leaks pose a significant risk, 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 into your data behavior.

NOT ALL DATA WAS CREATED EQUAL

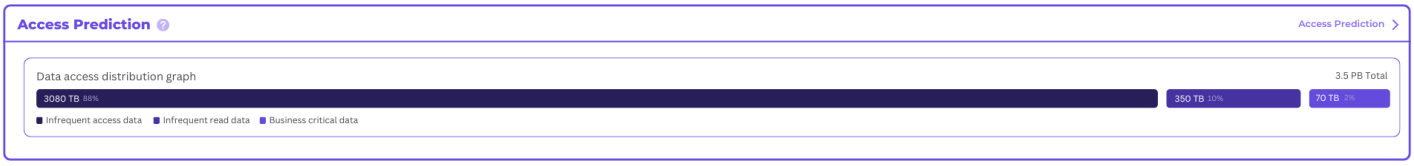
The Ray Approach

How many times have you heard that most enterprises possess far more data than they realize? That they struggle to know 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 single 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 is likely to be accessed. This predictive approach enables focused, high-granularity protection for frequently accessed data, while ensuring rapid protection for data that remains dormant.

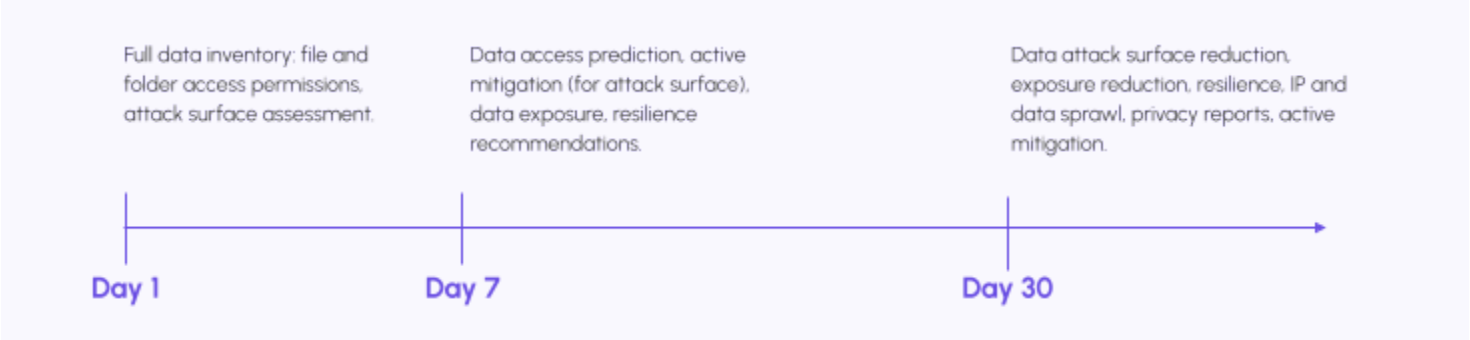
Ray Security was founded on the principle that not all data is created equal. The reality is that, at any given moment, we only use a fraction of the data available to us, and enterprises utilize just a portion of their overall data. The question then becomes: who benefits from the fact that the majority of the data - to which you won't

be accessing soon - is available? It's obviously not you. The answer is simple: the attacker. In fact, at 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 same data everyday, but it's the same percentage.

Preemptive Data Security Benefits

- ➔ Reduce your data attack surface in weeks
- ➔ Complete data classification projects in weeks instead of years
- ➔ Achieve 98% ransomware resilience, even when hackers bypass traditional defenses
- ➔ Recover from a ransomware attack in hours, not days
- ➔ Are you confident you know where all your sensitive documents are? Or has something been overlooked?

Deployment Timeline



USE CASES

FULL DATA INVENTORY

Ray Security provides comprehensive visibility across the entire data inventory. Ray ensures no data remains unseen by integrating with 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.

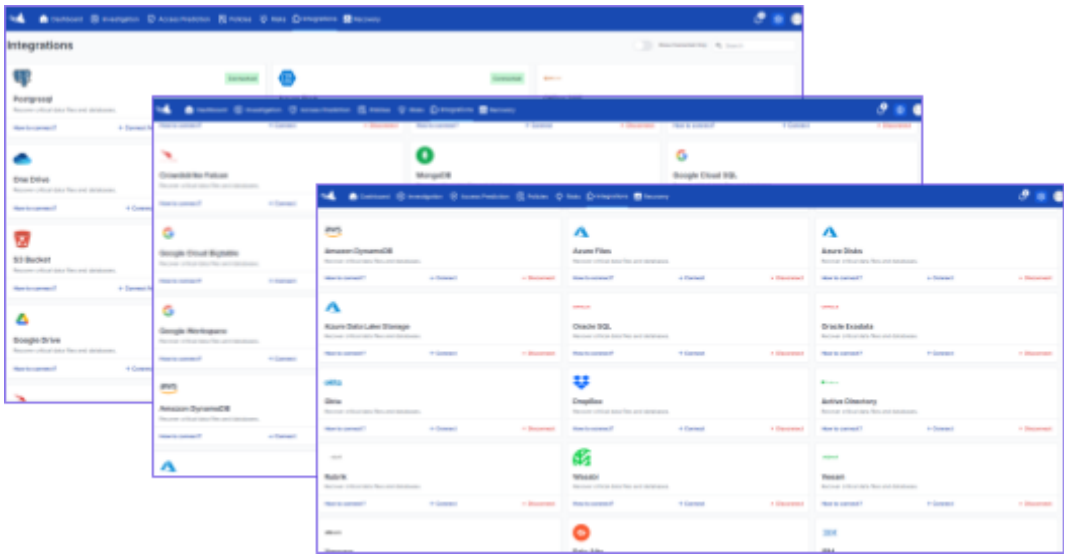
Seamless Integration

Ray's system integrates seamlessly with various data sources to provide robust recovery and management capabilities across various platforms. Whether it's cloud storage, databases, or on-premise servers, Ray can recover 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 seamless data recovery, providing rapid access to business-critical files across all connected systems. Through unified management, administrators can easily initiate recovery processes from any of 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 recovery processes.



RANSOMWARE RESILIENCE

Exfiltration Resilience And Minimizing Potential Damage

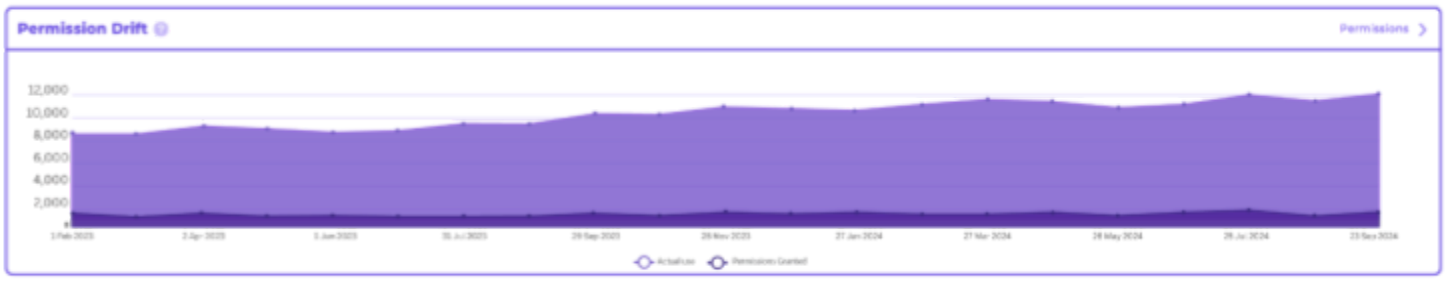
Ray Security's advanced time-series, proprietary AI analysis minimizes the risk of data exfiltration through its advanced access management and monitoring systems. The system continuously monitors file access patterns, identifying and responding to 95% of unusual activity (thus, in practice, almost every 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. Real-time monitoring of data access and automated response mechanisms, such as MFA or user session termination, provide an additional layer of defense against data breaches and leaks. Unlike other solutions, and as noted earlier, this works in an orchestrated manner across the entire data estate, making data breach/leak prevention much simpler.

Encryption Resilience For Faster Recovery

Ray Security's ransomware protection begins with reducing the attack surface. But this is not everything: Ray focuses you to just the data that you need for a quick restoration in the case of a ransomware attack, allowing you to better protect against an encryption event. It shows clearly what's the data that needs to be accessible at any point in time and lets you focus your attention and efforts towards creating a fast recovery plan to just this data, while simplifying recovery efforts dramatically in case of an attack.

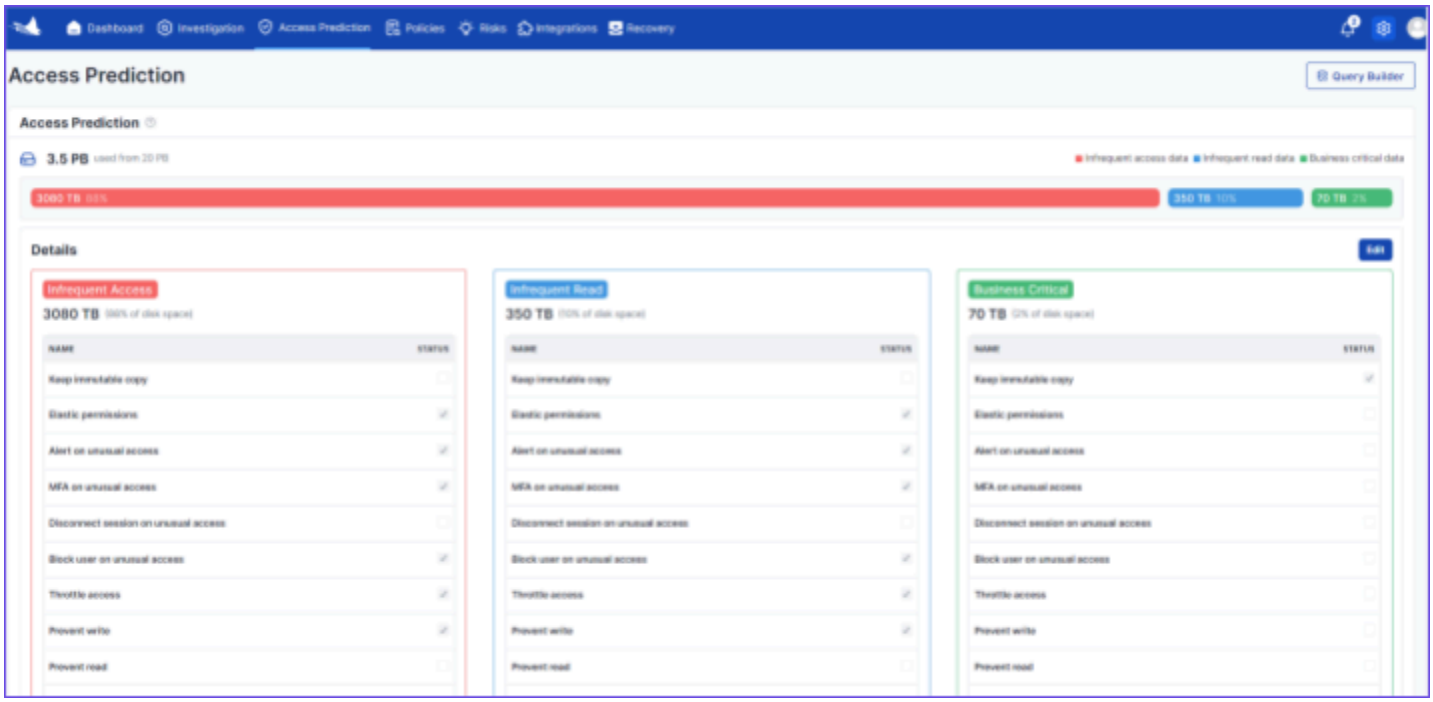


PERMISSION MANAGEMENT

Ray dynamically adjusts file and data permissions based on real-time usage patterns, ensuring that only the necessary personnel have access to the data when it's required. This automated, usage-based approach enhances security by minimizing unnecessary access. Simultaneously, Ray provides a unified dashboard, or "single pane of glass," that simplifies permission reduction and least privilege management. 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

Ray Security's elastic permissions system dynamically adjusts file access permissions based on real-time analysis of usage patterns. This approach minimizes the attack surface by reducing unnecessary permissions, particularly for infrequently accessed files. To ensure no additional work is put on the CISO team, the system provides self service mechanism to allow users to grant themselves access with an MFA and similar means with which the system integrates.



DATA ANALYTICS AND 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 at the same place.

DATA COST REDUCTION

Knowing which data is likely to be accessed in the near future weeks 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. By predicting future access patterns, Ray can avoid unnecessary costs associated with securing dormant or infrequently accessed data. This targeted approach reduces storage, processing, and security expenses.

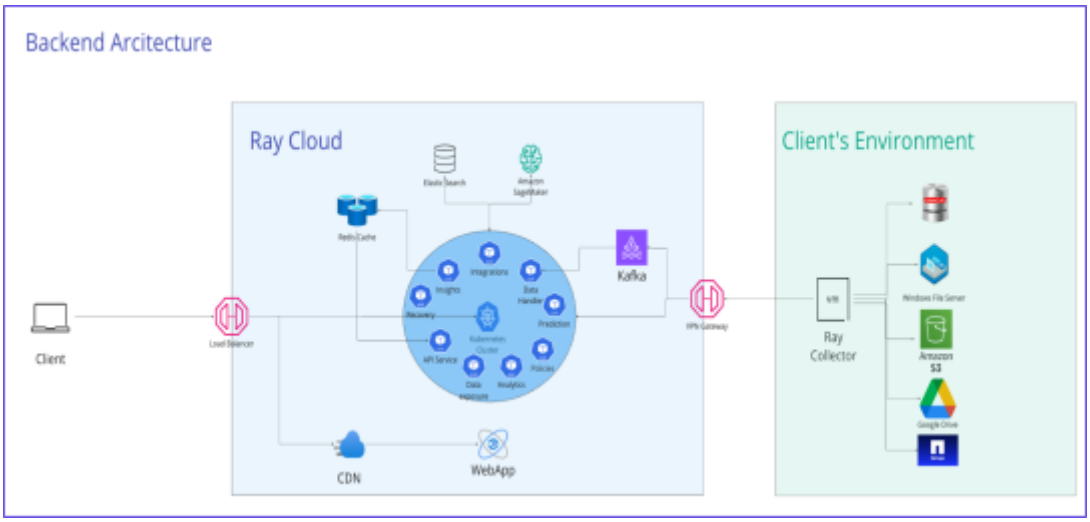
ARCHITECTURE

Components

Virtual Private Network

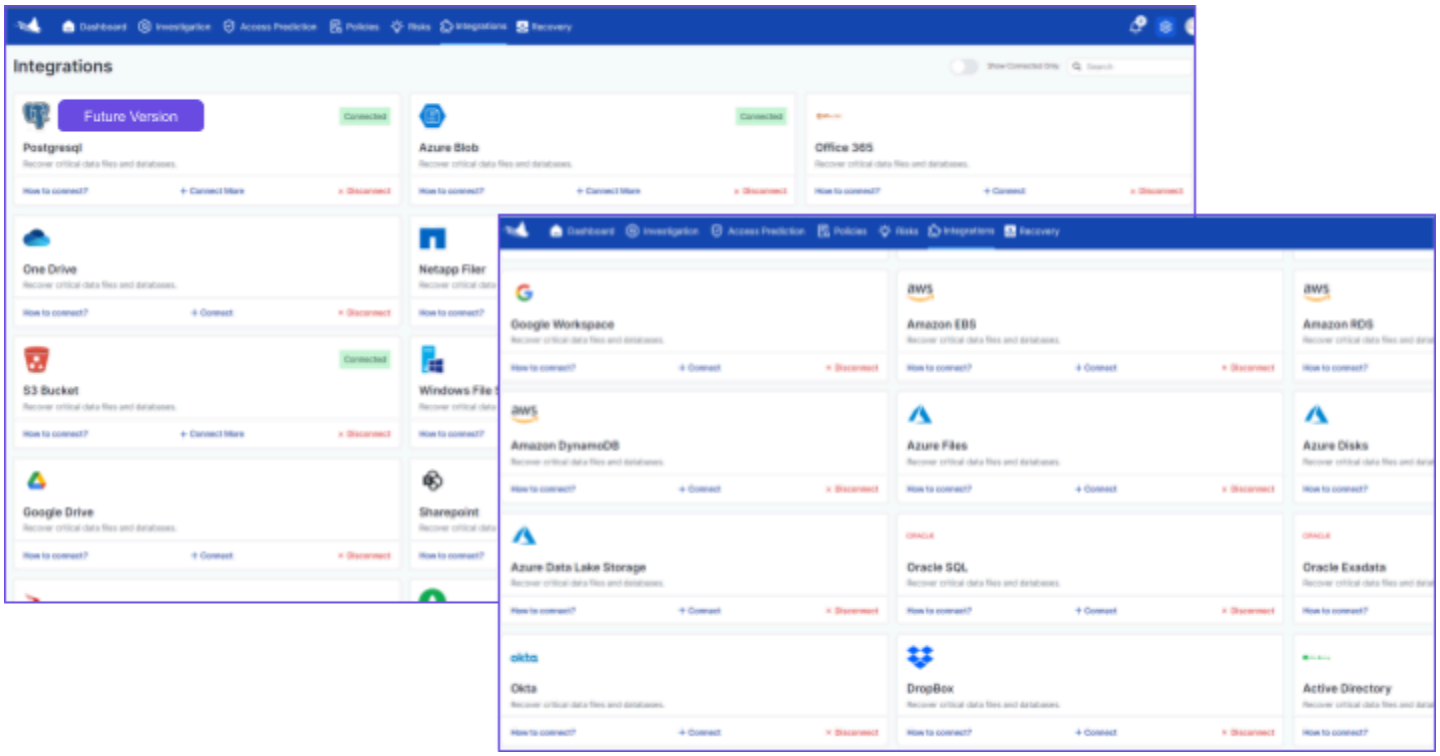
The diagram presented here assumes the customer uses a Private Network to provide a secure and isolated network environment within the Azure/AWS/GCP cloud or On Premise, allowing resources such as VMs, databases, and applications to communicate privately, securely, and efficiently.

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 part 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 for 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

Represents the Kubernetes (K8S) cluster used to orchestrate and manage containerized applications within the architecture. This cluster hosts multiple services like 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 proactively identify threats. 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.