Ray Security

Not All Data Is Created Equal

Jan 13, 2025

Ray Security

Ray Security Benefits

- → Reduce **data attack surface** by 90% within weeks
- → Classify 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

Comparative Analysis: Ray Security vs. Varonis

Executive Summary - Comparison Table

Feature	Ray Security	Varonis	Comments
Visibility	End to End	Mainly on-prem, select cloud apps	Unified control plane for data security
Active	Yes	No	Take active measures like data protection, alerts, permission management and more
Permission management	Automatic	Manual	Set policy once, and apply it everywhere
Preemptive security	AI-based	None	Based on the actual data usage
Classification	Automatic priority	No priority	Classifying all the data at no priority calls for an unmanageable project. Ray takes a phased approach with automatic prioritization
Deployment	SaaS or light on-prem	On-prem, friction	Minimal friction allows a much faster sales cycle
Integration with backup systems	Yes	No	Allows fast recovery of data to reduce ransomware impact
Data attack surface reduction	Automatic, Dynamic	Manual	Ray lets you set security policies around the data behavior and modernizes data hygiene

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 complete 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.

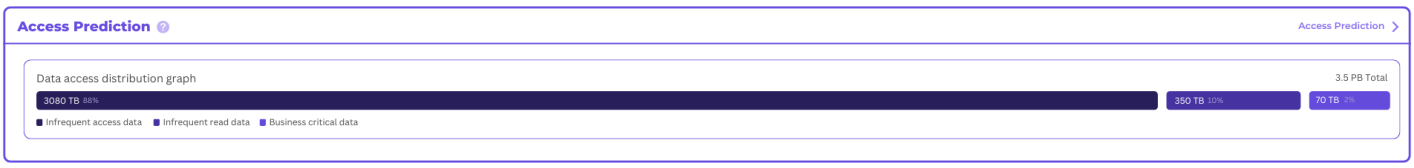
We get it.

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

Ray predicts which data will likely be accessed by leveraging proprietary time-series analysis. 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

Data Inventory and Visibility

Ray Security:

- Offers comprehensive visibility across hybrid, on-premise, and cloud environments.
- Provides a unified "Single Pane of Glass" interface for managing data across diverse systems such as databases, cloud storage, and enterprise applications.
- Leverages advanced machine learning to monitor data access patterns and prioritize critical data protection.

Varonis:

- Focuses on metadata collection and basic analysis of data relationships and access patterns.
- Primarily supports file systems, SharePoint, and limited cloud storage integrations.
- Relies on static risk assessments for identifying overexposed sensitive data.

Key Differentiator: Ray's predictive time-series analysis delivers preemptive protection, a significant advancement over Varonis' retrospective analysis.

Ransomware Resilience

Ray Security:

- Employs a proactive approach, predicting data access needs to minimize the attack surface.
- Integrates dynamic permission management and write-restriction policies to achieve over 90% data immutability.
- Enhances resilience through fast recovery mechanisms and targeted restoration of critical data.

Varonis:

- Detects ransomware through analysis of abnormal user behavior and file activity.
- Provides alerts and basic quarantine measures in response to potential ransomware attacks.
- Lacks the proactive measures necessary to prevent attacks before they occur.

Key Differentiator: Ray's proactive resilience features—such as immutability and preemptive protection—outperform Varonis' reactive anomaly detection.

Why Ray Security Ransomware Resilience Is Better

		Ray Security	Legacy Platforms (Varonis)	DSPMs	EDR	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 either read-only (simulating, to an extent, WORM) or protected from encryption with self-access governance, activity governance and automatic permission management. The protected data automatically changes daily.
[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 Security:

- Provides elastic permissions that adjust dynamically based on real-time usage patterns.
- Introduces advanced permission controls, including time-bound and record-limited access.
- Supports a unified dashboard for least-privilege enforcement and permission auditing.

Varonis:

- Offers static auditing tools to analyze data access and reduce over-permissive access.
- Focuses on compliance by identifying sensitive data and monitoring historical access trends.
- Does not provide automated or dynamic permission adjustments.

Key Differentiator: Ray's elastic permissions ensure real-time adaptability, whereas Varonis relies on static, manual processes.

Why Ray Security Breach Prevention And Data Access Governance Is Better

		Ray Security	Legacy Security Platforms (Varonis)	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:

- Utilizes machine learning and AI-based deep classification to identify sensitive data with high accuracy.
- Prioritizes classification efforts using predictive models to focus on critical data.
- Integrates classification with permission management to streamline security and compliance.

Varonis:

- Employs predefined rule-based methods (e.g., regex) for basic data classification.
- Provides automated workflows for classification but lacks prioritization capabilities.
- Limited to structured and semi-structured data, offering less flexibility.

Key Differentiator: Ray's predictive and integrated classification capabilities surpass Varonis' limited, rule-based approach.

Why Ray Security Classification Is Better

		Ray Security	Legacy Security Platforms (Varonis)	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	✅	✅Noisy

Deployment and Scalability

Ray Security:

- Offers flexible deployment options, including fully managed SaaS and on-premise solutions.
- Provides rapid deployment with minimal disruption, leveraging existing infrastructure.
- Scales seamlessly across large, diverse data environments.

Varonis:

- Typically requires on-premise deployment with additional cloud integration configurations.
- Involves longer deployment timelines due to manual setup processes.
- Faces challenges in scaling effectively across hybrid environments.

Key Differentiator: Ray's SaaS deployment ensures faster, simpler scalability compared to Varonis' traditional setup.

Cost Efficiency and Lifecycle Management

Ray Security:

- Optimizes costs by predicting future data usage and focusing resources on critical data.
- Reduces expenses through intelligent tiering and proactive data lifecycle management.
- Minimizes operational overhead with automated classification and permission adjustments.

Varonis:

- Reduces costs by mitigating risks associated with data breaches and compliance failures.
- Lacks predictive capabilities for resource allocation and lifecycle optimization.

Key Differentiator: Ray's predictive cost management outperforms Varonis' more reactive cost-saving measures.

Data Cost Reduction Comparison

		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)

Conclusion

Ray Security sets a new standard in data security with its innovative, proactive features like preemptive protection, elastic permissions, and predictive classification. Varonis, while reliable for traditional environments, lacks the modern capabilities required to address today's dynamic data security challenges. For organizations seeking cutting-edge, scalable, and efficient solutions, Ray Security is the clear leader.