



# Automated Data Security Platform

How to continuously minimize risk and prevent  
insider threats.

14 May 2025

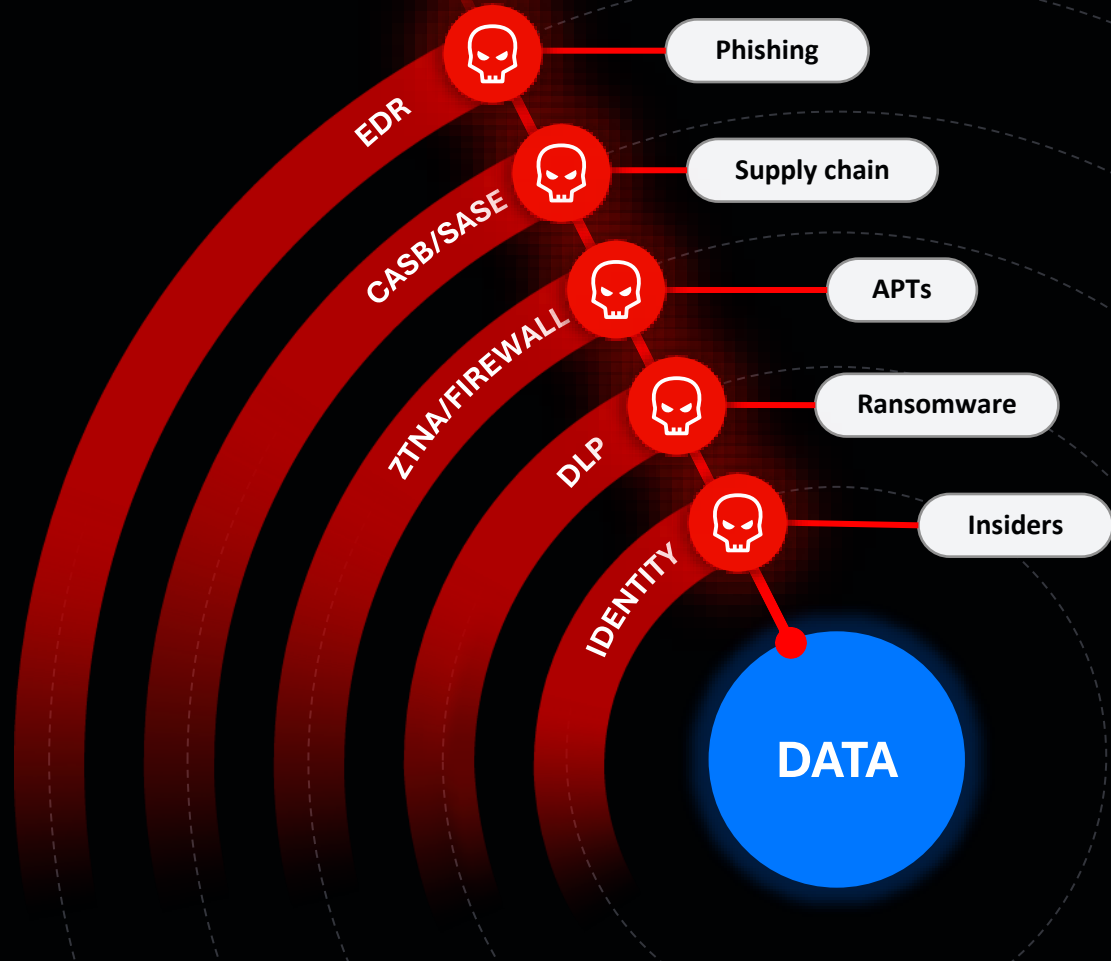
VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



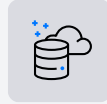
# It's all about the data.

For most companies, data is their most **valuable** and **vulnerable** asset.

Data is always the target.



# The blast radius is growing relentlessly.



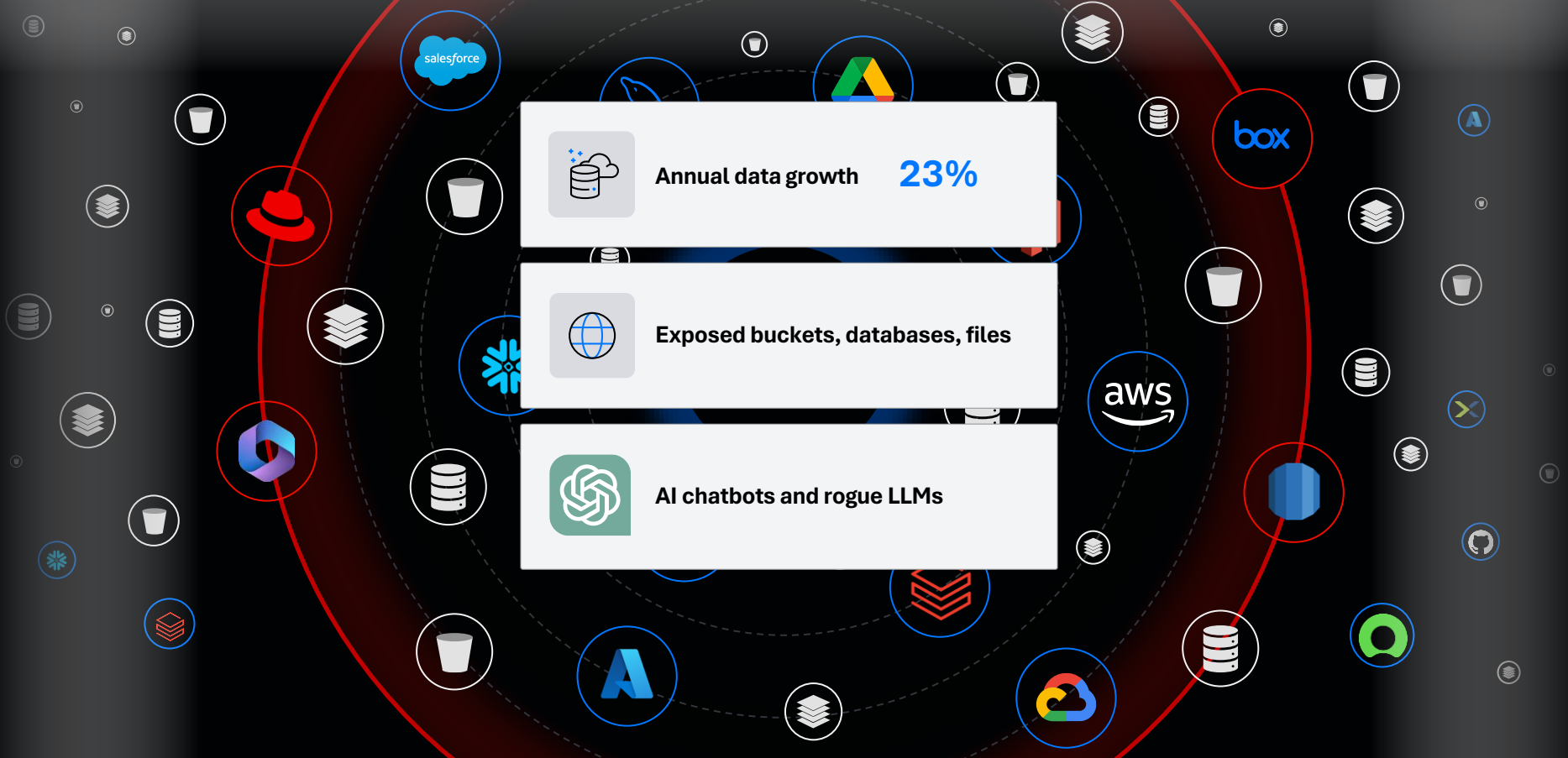
Annual data growth **23%**



Exposed buckets, databases, files



AI chatbots and rogue LLMs



# Common attempts to secure data



## Native controls

Purview

Built-in auditing

Built-in access controls

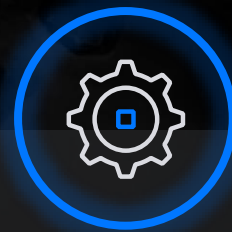


## Point solutions

Classification tools

Privacy tools

Auditing tools



## Legacy DLP

Manual labeling

Inline blocking

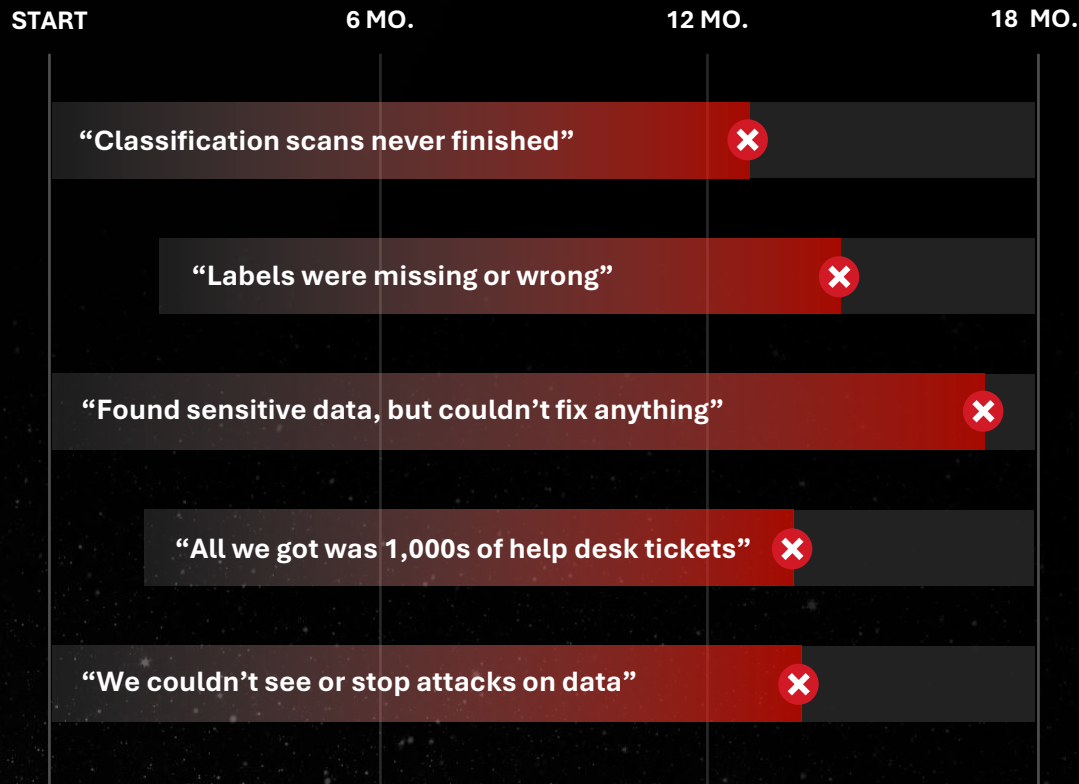
File-by-file remediation

# Most solutions result in busywork followed by a breach.

“

We spent 18 months struggling just to classify data with **no measurable outcome.**”

CISO, Global Financial Firm



“

Varonis easily saves us a few hundred thousand – maybe even half-a-million – dollars per year in terms of personnel cost and hardware cost recovery. If it also saves us from a security incident – that's priceless.

Michael Taylor  
CIO – USNS MERCY



## Fully automated data security



### Real-time visibility

Understand where your sensitive data is, who has access to it, and where it is at risk.



### Automated prevention

Continuously reduce the blast radius and enforce least privilege.

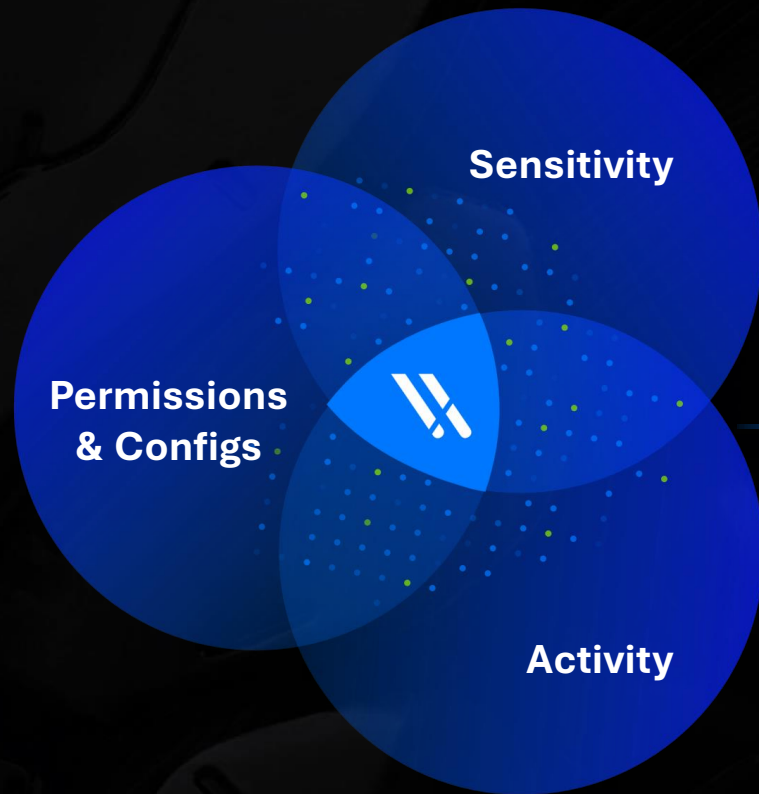


### Proactive detection

Data-centric UEBA to identify insider threats and other threats before they escalate to a data leak.



# Real-time automated data risk visibility



## Complete

Full scans across cloud and on-prem resources. No blind spots.



## Contextual

Is sensitive data exposed, labeled, or under attack?



## Current

We know what's changed and created, so visibility is always up-to-date.

# Automated prevention

The screenshot displays the Varonis Automated Prevention interface. At the top, there is a 'Resource' dropdown set to 'prod1.sharepoint.com' and a 'Preview results' button. Below this is a grid of filter options: 'Permission', 'Removal link' (set to 'Yes'), 'Link type' (with 'anyone on the internet' and 'org-wide' buttons), and 'Sensitive (incl. subfolders)' (with 'OneDrive' and 'SharePoint Online' buttons). An 'Add filter' button is at the bottom left of the filter grid. Below the filters, the 'Actions' section features a blue bar with a 'Remove permission' button. At the bottom, the 'Execute actions' dropdown is set to 'Continuously'. An inset window titled 'Org-wide sharing links' shows a line graph of sharing activity over time.

Resource: prod1.sharepoint.com

Preview results

Permission Removal link Yes

Permission Link type anyone on the internet org-wide

Resource Sensitive (incl. subfolders) OneDrive SharePoint Online

+ Add filter

Actions

Remove permission

Execute actions Continuously

Org-wide sharing links

75K

0

4/1 5/1 6/1 7/1 8/1 9/1

## Auto-enforce policies:

- ✓ Revoke excessive access
- ✓ Remediate spills
- ✓ Fix mis-applied labels
- ✓ Fix misconfigurations
- ✓ Data lifecycle
- ✓ Data residency
- ✓ ACCM



# Proactive detection



# AI is all about data.

“

Varonis allowed us to deploy AI.  
Without it, I don't think I would've been  
able to safely greenlight Copilot or any  
other AI tools that crawl our data.

Jim Bowie, CISO,  
Tampa General Hospital

[Watch video →](#)

## AI Copilots



ChatGPT



Google Gemini



Claude

## AI Agents



Agentforce



Copilot Studio



Operator

## AI Infrastructure



Amazon Bedrock



vertex.ai

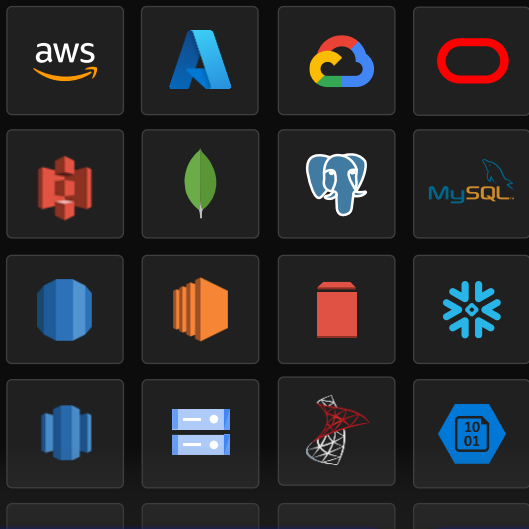


Azure OpenAI

# One platform for multi-cloud, SaaS, and on-premises.

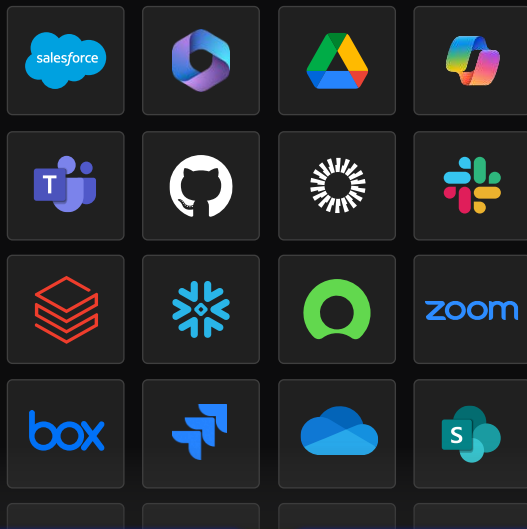
## Cloud

*Object storage, databases, VMs*



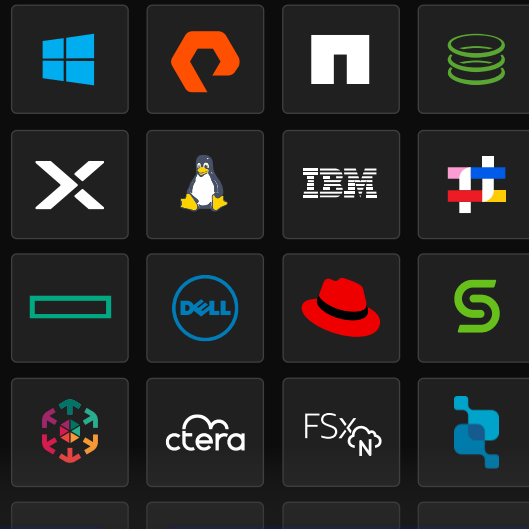
## SaaS

*Collaboration, email, source code*



## Data center

*File shares, NAS, databases*



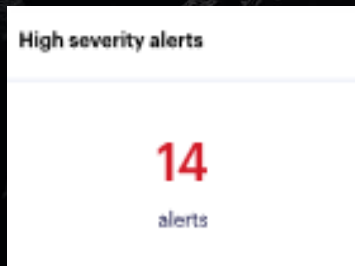
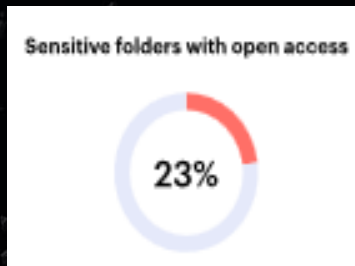
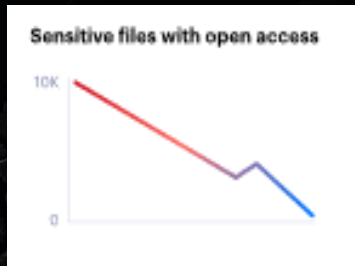
Identity

Network

Third-party apps

APIs

[View all coverage →](#)



# How we start: Free data risk assessment

## Map key data stores

- + Enable full platform access
- + Analyze permissions, identities, configurations
- + Discover & classify data

## Prioritize risks

- + Exposed sensitive data, shared links, rogue admins
- + Active Directory
- + Compliance gaps

## Monitor data usage

- + Enable activity
- + Enable meaningful, high-fidelity alerts
- + Accelerate investigations



 VARONIS