

Veeam Intelligent ResOps

Get insight in to your M365 data



Nemanja Pejic

Advisory System Engineer, Veeam Software

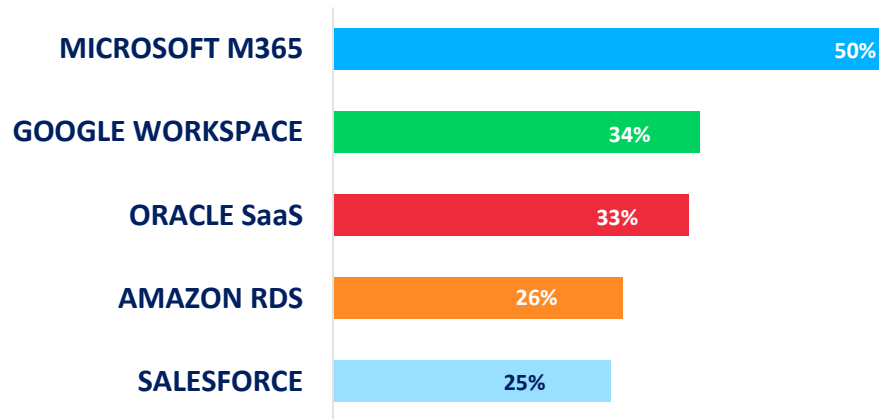
VDC for M365 overview

MICROSOFT 365 DATA LOSS FEARS ARE REAL

KEY TAKEAWAY:

Microsoft 365 is top of the list across SaaS and PaaS environments for data loss concerns.

Q. In which of the SaaS and PaaS environments currently in use in your organization are you most concerned about data loss, accidental deletion, lack of recovery, lock-in, or discovery and auditing challenges?



MICROSOFT 365 + ENTRA ID

DATA RESILIENCE IS YOUR RESPONSIBILITY



600M

identity-based attacks
every day



2B

new Microsoft 365 files added
every day

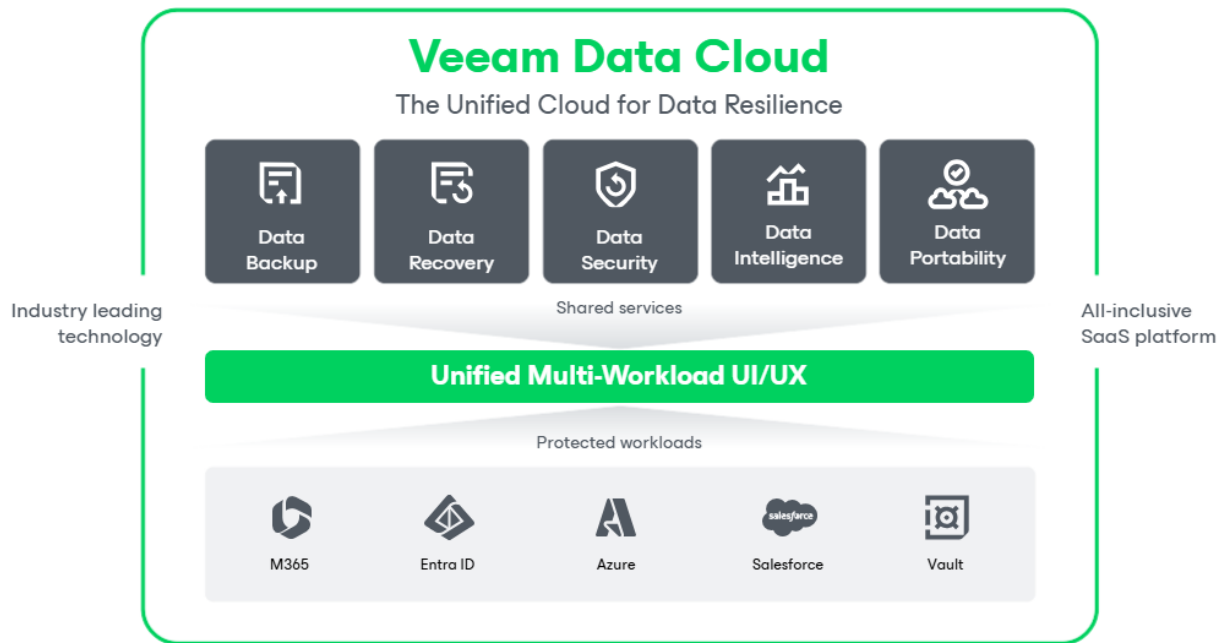


69%

Felt well-prepared before
experiencing an attack.
Only **10%** managed to recover
90% of their data

Veeam Data Cloud Platform

Veeam Data Cloud Platform allows you to protect other critical SaaS workloads like **Entra ID, Salesforce, Azure**, and more all through the same console, and more on the way.



VEEAM DATA CLOUD FOR MICROSOFT 365



Microsoft Graph [API](#)

Veeam Data Cloud *for Microsoft 365*

Microsoft Backup Storage [API](#)

Day-to-Day Operations

Veeam
Tenant



Data separation
and security



Flexible, granular
restore



Customizable
backups



Support for
Teams



Advanced
search



Exit
strategy



Data stored in location
of your choice

Disaster Recovery

M365
Tenant



Fast Backup of
Initial M365 Tenant



Bulk restore



Cyber attack
recovery



Data stored inside
Microsoft security boundary

Powered by Microsoft 365 Backup Storage

Each backup is a separate, independent backup method embedded inside of Veeam's M365 backup solution.

EVERYTHING IS INCLUDED

Software, backup infrastructure and unlimited storage bundled together with ongoing maintenance covered by the experts

Veeam Data Cloud for Microsoft 365

Veeam-managed service delivery

Core components



Veeam Server



Proxies



Unlimited storage

Operations



Networking



Infrastructure management



Maintenance

Automation



Updates



Patches



Network security

User-controlled

Backup



Create backup jobs

Restore



Recover quickly & easily

eDiscovery



Advanced search and find

Optional configuration:

Backup Operations

Customize your backup

Alter retention period

Storage region of your choice

Security

Role Based Access Control

Restrict access by IP range

Diversify storage repositories

Analytics

Generate reports

Manage licenses & monitor activity

Intelligent ResOps for m365

Better Intelligence = Better Resilience



DATA RISK EXPOSURE

Stale sensitive data that can be leveraged in a breach.

Redundant, obsolete, and trivial data accumulates unchecked inside M365. Every backup copies it again. Blast radius grows. Storage costs grow. Risk exposure grows if organization is breached.



PROTECTED SENSITIVE DATA

Ensuring Sensitive data is protected at scale.

PII, PHI, PCI land in SharePoint and OneDrive folders. HIPAA requires sensitive data be protected at least every 48 hours. No classification means no ability to prove this. Breach impact is unknown until it's too late.



AI AGENT BLIND SPOT

Copilot is already touching your data.

AI agents read, summarize, and act on M365 data today. Backup has no visibility into what they access or change. When an agent touches bad or sensitive data, there is no audit trail and no clean rollback point.

The Big Gap

Missing data context ...



"Where does sensitive and regulated data live?"



"What Agents are running and what data they can access?"



"Is user access to data configured correctly?"



"Are we compliant with data and AI regulations?"



"How much does ROT data cost us?"



"How to prioritize recovery of business-critical data?"

VEEAM INTELLIGENT RESOPS

Add-on for VDC M365

Backups tells you the data is safe.

ResOps tells you what the data is, who and what touches it, and whether AI can be trusted with it.

Across SharePoint, OneDrive, Teams, and Exchange.



MINIMIZE ROT DATA

Find redundant, obsolete, and trivial data. Tier it or delete it and cut Microsoft 365 spend.



PROTECT SENSITIVE DATA

Discovery, classification, and labeling with contextual accuracy. Know the SharePoint site holding PCI data is backed up.



ACCELERATE SAFE AI

Reduce sensitive data exposure before Copilot rollout. Identify which data is safe for AI to use.



AI AGENT ACCOUNTABILITY

Inventory AI agents and the sensitive data they reach. Audit what they touch. Undo AI mistakes on your data.

Veeam Intelligent ResOps – How It Works

Agentic Reporting

Dashboards & Reports | Reporting Agent | Investigation Agent

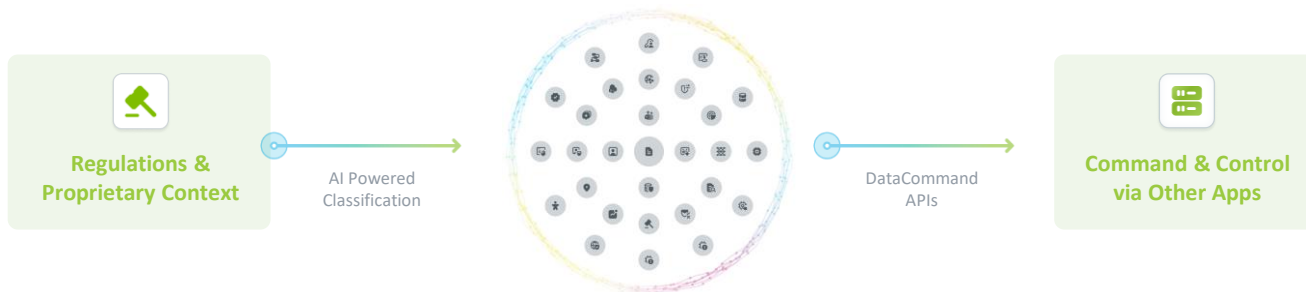
Automated Policies

Data Labelling | Data Quarantine | Undo AI | Insights Policies

Intelligent Insights

AI Agent & User | Data Access | Sensitive Data | ROT Data | Data Backup

Graph Correlation



DataAI Discovery



SharePoint



OneDrive



Teams



Exchange

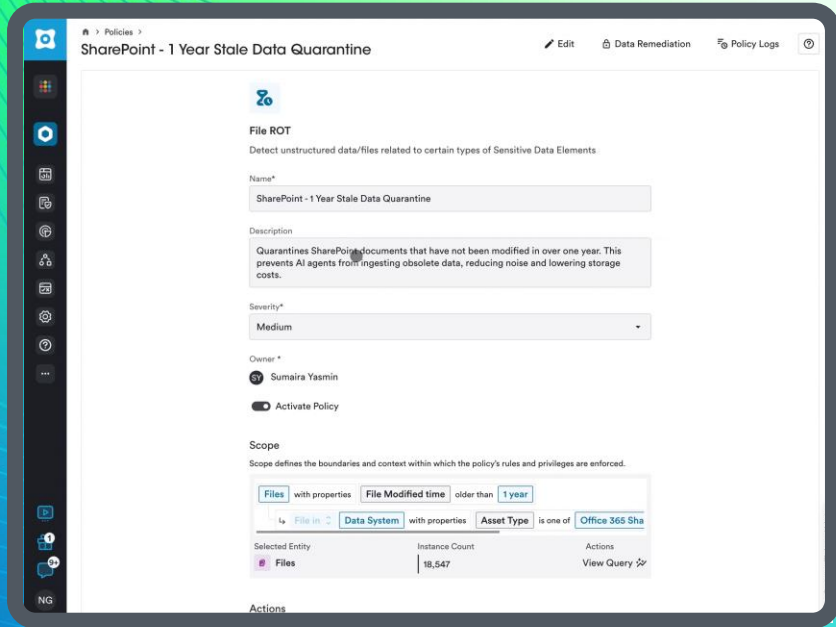


AI Agent



Copilot

Risk and Data Reduction



Data Lifecycle Intelligence

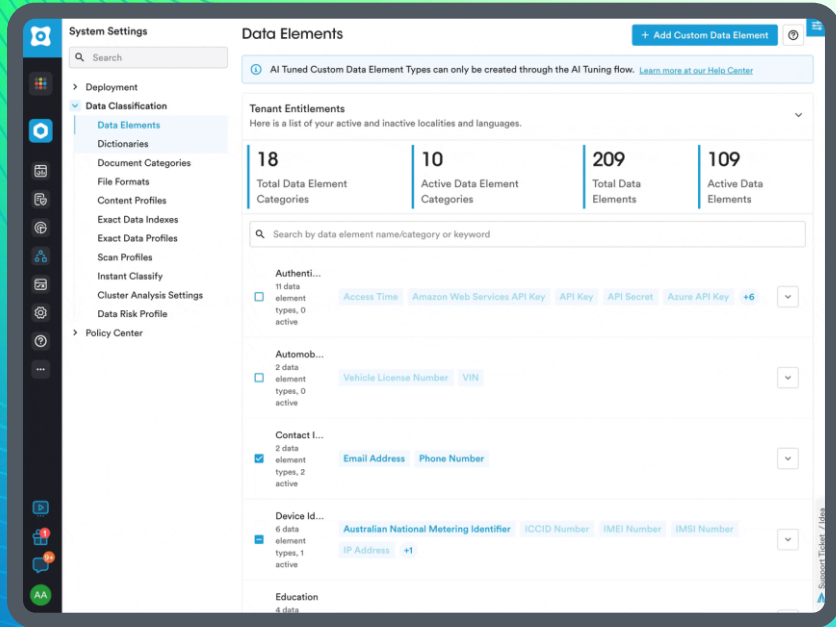
Find duplicate and near-duplicate files

Identify old files that are a retention risk

Automatically archive files to minimize data ROT

Example: Identify files older than 7 years that also contain SSN numbers.

Sensitive Data Discovery



Contextual DataAI Intelligence

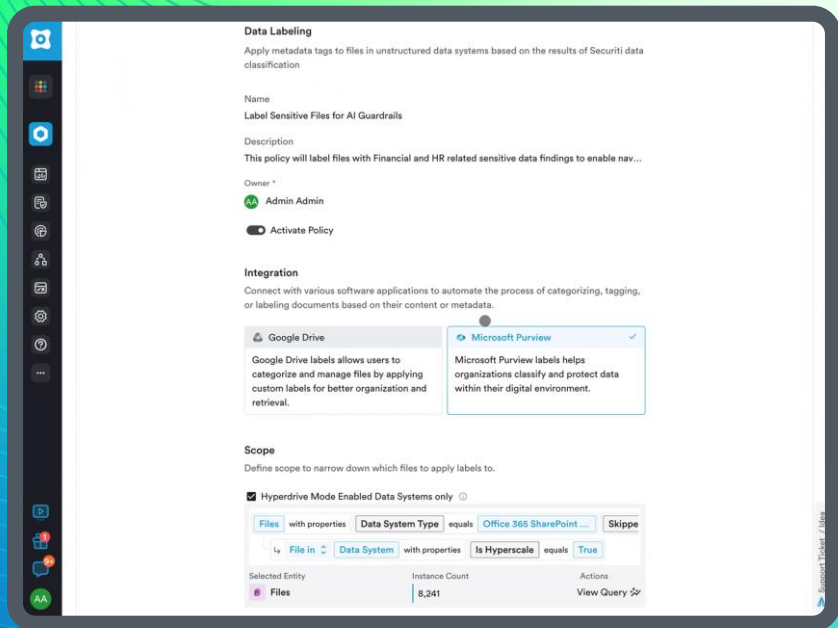
Automatically discover files and AI agents

Classify data accurately AI-tuning, regex, EDMs, contextual inference, etc

Spot toxic combination risks with graph context

Example: SharePoint files containing PHI data.

Label Files Across M365



Scale Data Labeling

Automatically label files in Sharepoint and OneDrive

Improve labeling accuracy using AI classification and graph conditions

Integrate with Microsoft Information Protection (MIP) to apply existing labels (*E3+ license*)

Example: Label files containing PHI data as highly confidential.

What Better Labeling Means

AI SAFETY & GOVERNANCE

“Do not ingest”

AI agents skip it. Excluded from training and retrieval automatically.

COMPLIANCE & REGULATORY

“EU residents only”

Data stays in region. Residency rules enforce themselves, nobody routes it by hand.

SECURITY & DLP

“Confidential”

Sharing is blocked at the data level, not at the perimeter or a downstream firewall.

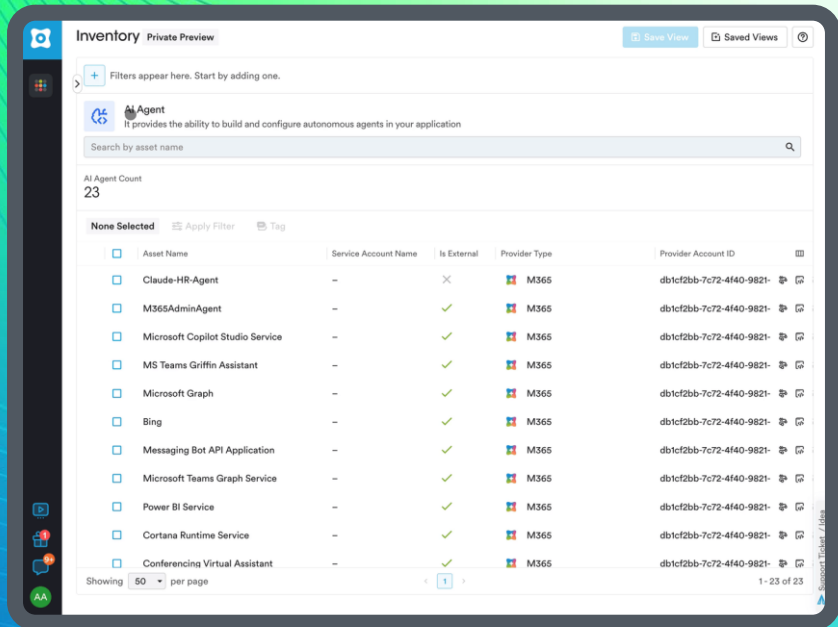
OPERATIONAL EFFICIENCY

“PII, restricted”

Audits, access reviews, and workflows trigger instantly, without configuration.

Labels tell every system what to do with data. If the labels are right, the estate runs itself.

Discover AI Agents and Rollback Mistakes



AI Trust & Resilience

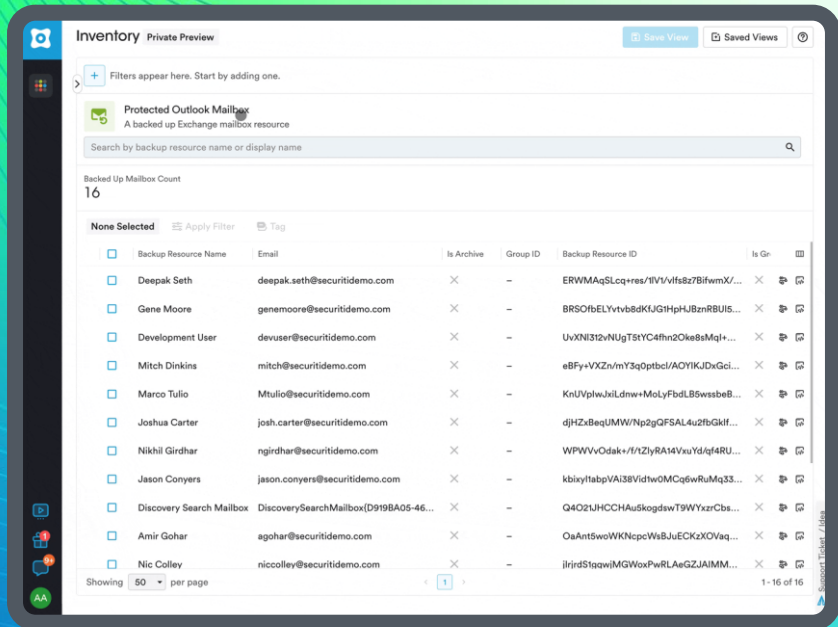
Inventory AI agents and sensitive data they can access

See files agents access and identify protection gaps

Automatically roll back AI-driven changes to data

Example: Restore files deleted by “Copilot HR Agent”

Data Resilience Intelligence



Backup Intelligence

Pinpoint whether a system is backed up or not

Prioritize back up of systems containing sensitive data

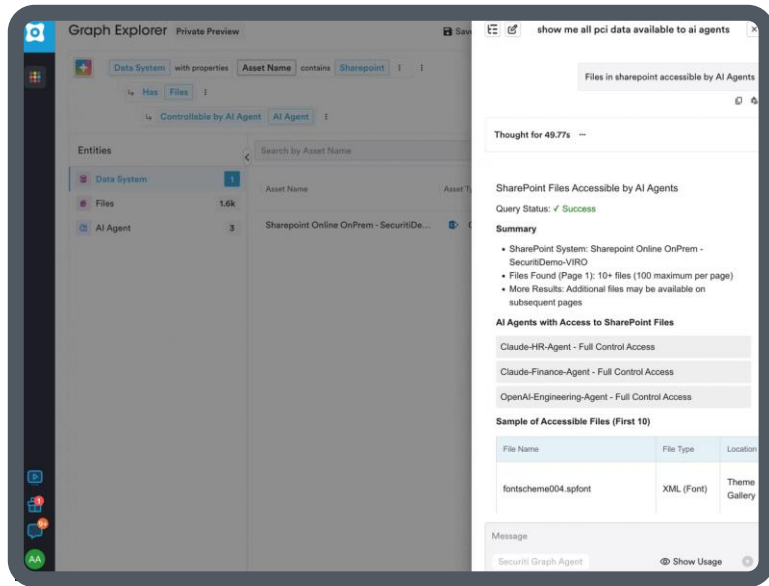
Precisely recover files you need, avoid bulk restores

Example: Ensure SharePoint site with PCI data is protected.

Realize Business Value Faster By Automating Investigations

Powered by Agentic AI & Contextual Graph Intelligence

Example: “Which files with sensitive data are accessible by AI agents?”



**Answer any question about your data and AI
using natural language queries and context embedded in the graph**

Add-On for VDC M365 Users

Entire M365 tenant must be licensed

FOUNDATION

Core Intelligence

\$2.49 PER USER / MONTH

- ✓ Data & AI Access Intelligence
- ✓ Backup & Recovery Context
- ✓ Data ROT & Retention Context
- ✓ AI Agent Discovery and Audit log
- ✓ Undo AI actions on files

ADVANCED

Full Resilience

\$4.99 PER USER / MONTH

- ✓ Everything in Foundation
- ✓ Data Classification
- ✓ Data Labeling

Veeam Intelligent ResOps Complements Microsoft Purview

Getting The Most Out of Your Microsoft Investment



Reduce Your M365 Spend
by Reducing Data ROT



Enhance Accuracy of
Microsoft Purview Labels



Access Intelligence by
Human & Non-Humans



Backup intelligence into
Sensitive and Business
Critical Data



Audit Data Access by AI
Agents and Undo AI
Mistakes

Veeam Intelligent ResOps Complements Agent 365

Agent 365 governs and manages the lifecycle of agents. **ResOps ensures** the data agents are accessing is accurate and protected.

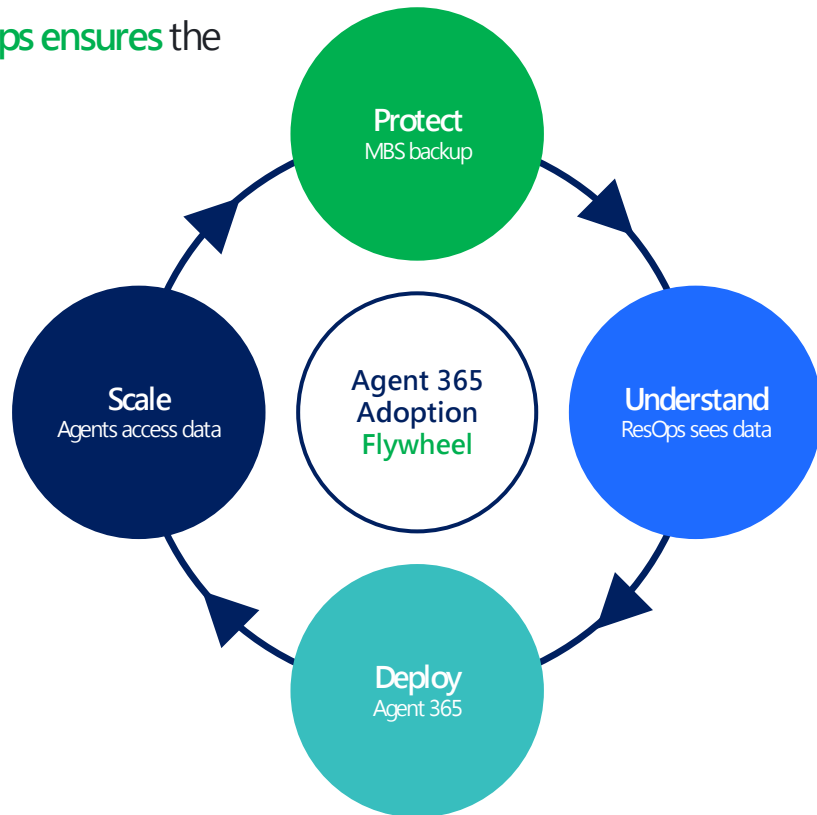
A Data Safety Net: AI Undo surgically rolls back agent actions at the file level to minimize data loss and downtime

Highlight unprotected sensitive data: Discover critical data and put into MBS policies

Accurate clean data: Data and risk minimization cuts oversharing what agents should be accessing

Time to value: readiness in weeks, not quarters by ensuring organizations trust the data agents are accessing

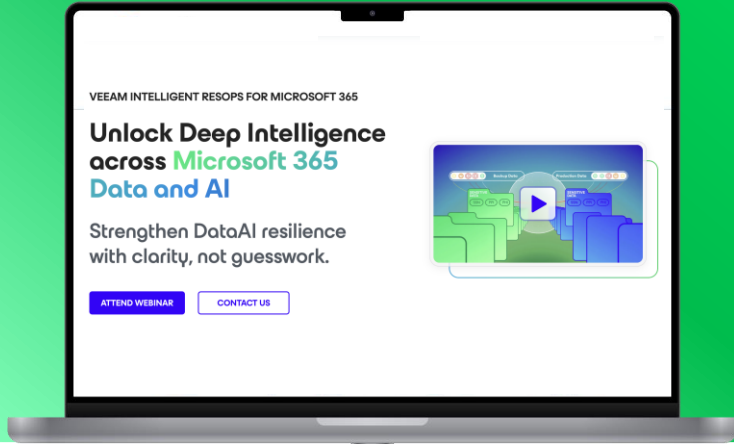
Compliance: Agent audit log + access intelligence show what data each agent can touch, making Agent 365's policies meaningful.



Resilience starts with knowing what you're protecting.

Learn More

Visit **Veeam Intelligent ResOps** Webpage



Request a
Personalized **Demo**



Veeam Intelligent ResOps For M365

Strengthen resilience
with **DataAI** intelligence,
not guesswork.

[Watch on-demand demo →](#)



. Thank you