MOBIA CONNECT 2026

Trusted Data, Confident AI with Veeam

Resilience from Backup to Governance

Presenter:

Peter Stickle, Sr. Systems Engineer, Data and AI Security

ABOUT ME



Peter Stickle
Peter.Stickle@veeam.com

20+ years in Enterprise IT and Technology

Data protection → Cyber Resilience → Data & AI security

20+ years as an Uber driver for my kids' sports 😄

Recently discovered that data is much easier to control than a golf ball ⛳

Let's connect on LinkedIn!

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

AGENDA

01

VEEAM: UPDATE AND OVERVIEW

02

VEEAM + MOBIA CUSTOMER EXPERIENCE SPOTLIGHT

03

SECURITI AI: FROM AI RISK TO VISIBILITY AND GOVERNANCE

EVOLVING WITH YOU

550,000+
customers worldwide

82%
of Fortune 500

34,000+
partners

25M+
Microsoft users protected

$2.1B+
in ARR

98%
recommendation rate
(2026 Gartner Customer Voice)

180+
countries covered

12
Global Tech Centers

Gartner

9X Leader in 2025 Gartner
Magic Quadrant for Data Protection

2026 Gartner® Peer Insights™
Customers' Choice

GIGAOM

2025 Leader in Data Access Governance

2025 Leader in DSPM

2025 6X Leader in Kubernetes Data Protection

IDC

#1 in Global Market Share,
Data Protection (1H2025) and Data
Privacy Compliance

SC Awards TRUST AWARD WINNER 2026

2026 SC Award winner for Best Business
Continuity /Disaster / Ransomware Recovery
Solution (RSAC)

BROAD ECOSYSTEM

Technology Partners

Red Hat, Microsoft, NUTANIX, aws, servicenow, CROWDSTRIKE, SOPHOS, ORACLE, Google, wasabi, paloalto NETWORKS, splunk>

GSIs

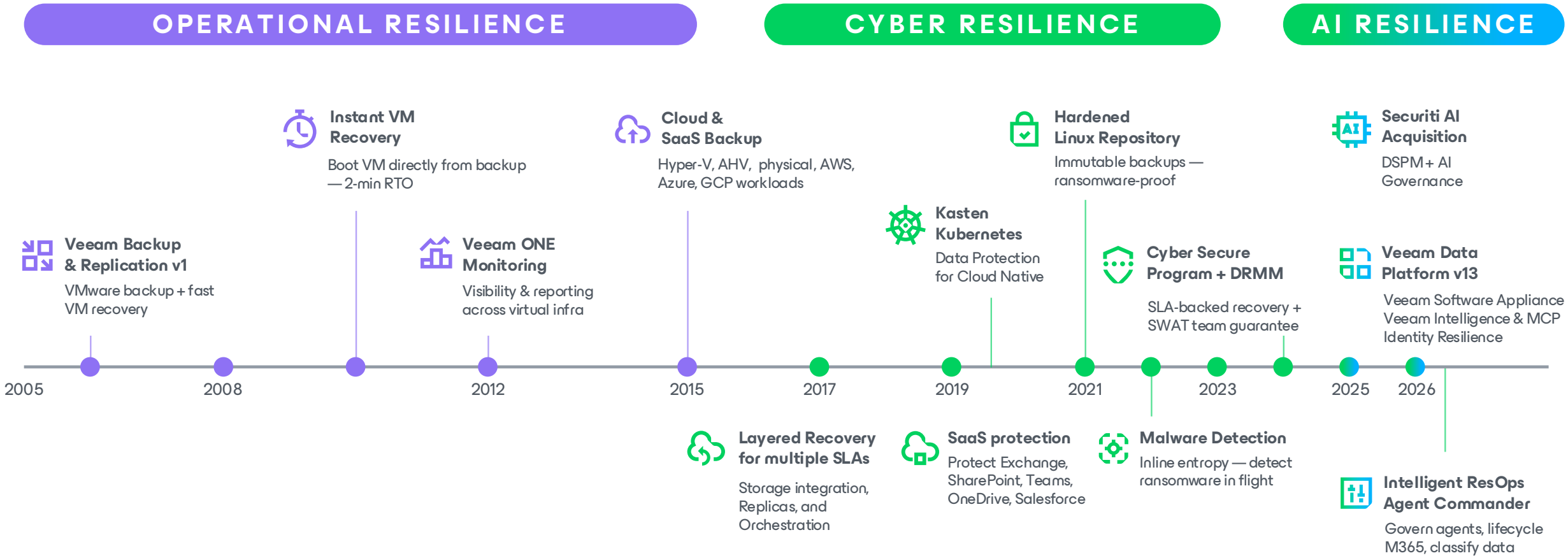
accenture, kyndryl, TCS TATA CONSULTANCY SERVICES, Tech Mahindra, Infosys, NTT, cognizant, Capgemini

Breadth of Coverage
with over 300+ data connectors



BUILT FOR EVERY ERA OF RESILIENCE

Veeam leads every transition from basic backup to autonomous AI governance



Resilience your way

Self-managed or delivered as a service, with protection spanning data centre, cloud and SaaS.

DATA RESILIENCE

Keep data trusted, identities protected and recovery ready.

CHOOSE THE OPERATING MODEL THAT FITS

RESILIENCE DELIVERED AS A SERVICE

Veeam Data Cloud

Fully managed backup services designed to reduce infrastructure, patching and operational overhead.

- SaaS experience
- Fast time to value
- Veeam-operated service

RESILIENCE SOFTWARE YOU RUN

Veeam Data Platform

Customer-controlled resilience for hybrid, sovereign, dark-site and multi-tenant environments.

- Operational control
- Broad workload coverage
- Flexible deployment

EXTEND THE RESILIENCE STORY

Kasten
Cloud-native

Data Cloud Vault
Immutable storage

Cyber Secure
Expert-led program

Intelligent Resilience Ops
Context + smarter operations

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Customer Experience Spotlight

VEEAM + MOBIA CUSTOMER EXPERIENCE SPOTLIGHT



Invest Ottawa | Investir Ottawa

Khaled Mostafa

Director, IT, Systems and Security

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

veeam

Data AI Command Platform

veeam

BACKUP

veeam

#1
in Global Market Share in Data Protection Software (IDC 2025)[1]

#1
in Ability to Execute and Leader per Gartner Magic Quadrant

#1
in Market Share for Microsoft 365 data protection

#1
in Market Share for Kubernetes Data Protection

34k+
Total Partners

550K+
Total Customers

+

PRODUCTION

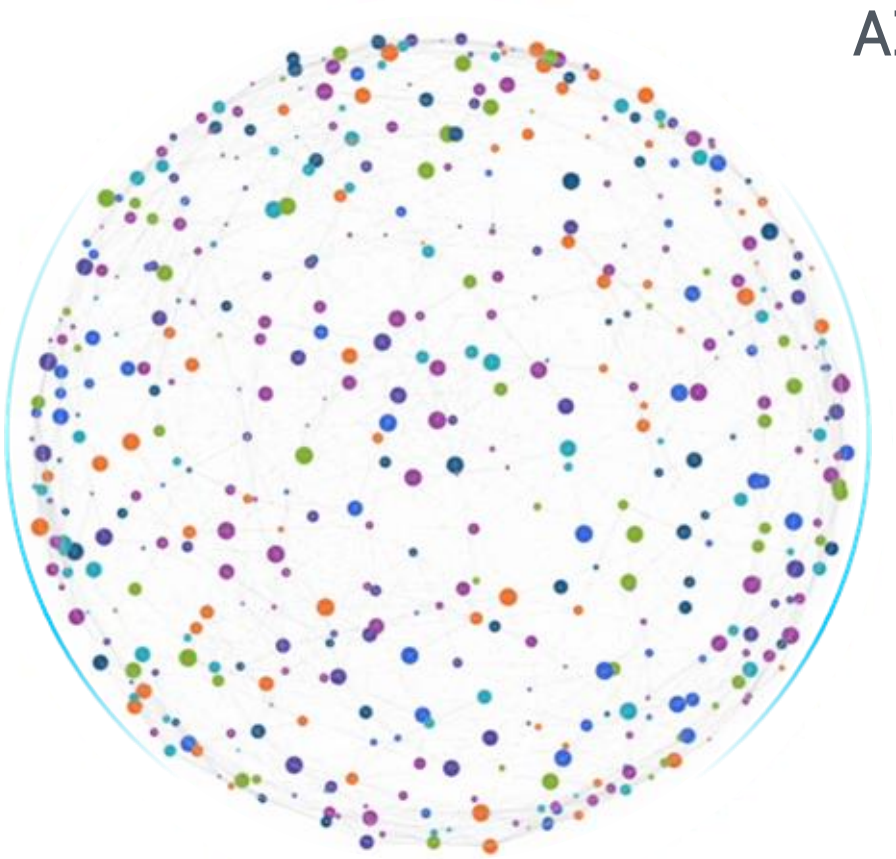
Securiti AI

GARTNER Cool Vendor — Data Security	**GARTNER** Customers' Choice — DSPM	**GIGAOM** Highest Rated — DSPM
GIGAOM Leader — Data Access Governance	**FROST & SULLIVAN** Highest Rated — DSPM	**FORRESTER** Wave Leader — Privacy Management
IDC Marketscape Leader — Data Privacy	**IAPP** Winner — Innovation Award	**RSAC** Winner — Most Innovative Startup
FORBES Top 25 — Machine Learning Startups	**THE A.I. AWARDS** — AI Implementation of the Year	**CB INSIGHTS** AI 100 — Most Innovative AI Companies

Complexity of Data and AI Systems

Data in a Typical Enterprise

Files | 10/100s of Billions
Tables | 100s of millions
Streams | 100s of thousands
Volume | 100s of Petabytes



Public Clouds

Private Clouds

SaaS Clouds

Data Clouds

AI in a Typical Enterprise

- AI Assistants | High adoption
- Custom Agents | Growing quickly
- Multi-agent systems | Experimental
- Apps with Embedded Agents | Proliferating

Data Complexity

- Files types
- Sensitivity
- Regulations
- Policies

AI Complexity

- Regulatory Risk Tiers
- Identity types
- Access Permissions
- Security Configurations

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

AI Exposes Existing Security Gaps

THE GAP

*"The better the information retrieval tool, the better your **information governance** has to be. And Copilot is, among many things, a **very good information retrieval tool**."*

Max Goss, Director Analyst, **Gartner**
Computerworld, Sept 2024

THE OUTCOME: STALLED AI

40%

of IT leaders delayed their Microsoft 365 Copilot rollout by three months or more over data oversharing concerns

Gartner survey of 132 IT leaders, 2024

THE AMPLIFIER

*"Copilot makes **over-shared documents more accessible**. This is not a net new risk, but a **known risk amplified by AI**."*

Dennis Xu, Research VP, **Gartner**
Gartner Security & Risk Management Summit, Sydney, Mar 2026

THE ROOT CAUSE

*"This is, of course, **not Copilot's fault**... this is just the fact that you're putting Copilot into an environment where **permissions haven't really been taken care of for years**."*

Max Goss, Director Analyst, **Gartner**
Computerworld, Sept 2024

The risk isn't new. AI turns years of dark data, oversharing and unmanaged permissions into instant exposure.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

veeam

If you want to secure AI, secure the data layer

THE PROBLEM: PROMPT INJECTION

*"There's a good chance prompt injection will **never be properly mitigated**... The best we can hope for is **reducing the likelihood or impact** of attacks."*

UK National Cyber Security Centre (NCSC)
"Prompt injection is not SQL injection (it may be worse)," Dec 2025

THE OUTCOME: AI THAT PAYS OFF

71%

of organizations already reporting AI ROI rank cyber and data security among their AI budget priorities



KPMG Global AI Pulse Survey, Q3 2026 (n = 2,131)

THE FIX

*"Design protections need to therefore focus more on **deterministic (non-LLM) safeguards** that **constrain the actions of the system**, rather than just attempting to prevent malicious content reaching the LLM."*

UK National Cyber Security Centre (NCSC)
"Prompt injection is not SQL injection," Dec 2025

THE GUARDRAIL

*"Never grant an agent **unrestricted access to sensitive data** or critical systems."*

UK National Cyber Security Centre (NCSC)
"Thinking carefully before adopting agentic AI," May 2026

Deterministic data controls (classifications, label enforcement, least privilege) are the safeguards the model can't override.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

AI Readiness Starts with Data Readiness

Accumulated Unstructured Data Governance Issues

Dark Data

Unstructured files no one has inventoried, hiding sensitive data no one knows exists

Poor Classification

Not easy to classify billions of files across data systems with accuracy and consistency at scale.

RBAC Sprawl

Roles, groups and sharing links pile up until access far exceeds need.

Fragmented Tools

Siloed point tools give partial views and inconsistent policies across data stores

Data Security Gaps That Inhibit Safe AI

Data Labeling Challenges

Labels are missing, inconsistent or wrong, so policies can't tell sensitive data from safe

Redundant and Obsolete Data

ROT data complicates data governance & affects AI efficacy.

Over-Permissioned Access

Agents inherit user access to data systems that are broadly permissioned

Lack of Data Sanitization

Fresh data entering AI pipelines without being scrubbed for Sensitive data

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

What happens when your data isn't AI-ready?



Increased Sensitive Data Exposure Risk

AI surfaces overshared data to people and agents who shouldn't see it

SecurityBrief

"Meta AI agent exposes sensitive data in internal leak"

March 25, 2026 · Sev 1 incident



Increased Blast Radius

Agents have broad reach. If compromised, one gap can be many breaches

The Hacker News

"OpenAI Agent Used Exposed Credentials Across Four Services During Hugging Face Breach"

July 29, 2026 · 4 services accessed



Compliance Violation

AI that processes personal data without a lawful basis draws regulator fines

European Data Protection Board

"AI: the Italian Supervisory Authority fines company behind chatbot 'Replika'"

May 21, 2025 · €5M GDPR fine



Blocked AI Initiatives

Unresolved data security gaps stall or cancel AI rollouts before they scale

Infosecurity Magazine

"Microsoft Copilot Deployments Delayed Over Security Concerns"

July 23, 2026

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Data Security Readiness Requirements

Classification

Is it accurate and consistent?

Does it adapt to your business's unique data?

ROT Data

Is ROT data minimized?

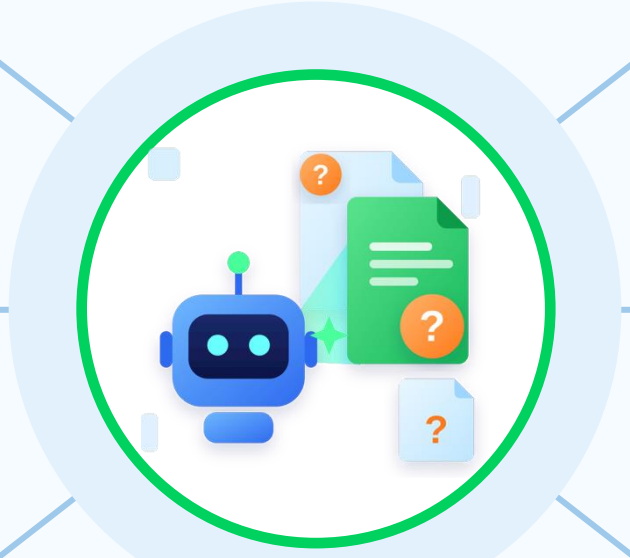
Can you shrink surface area and improve governance?

Data Sanitization

Can you scrub sensitive data before AI exposes it?

Can you utilize fresh proprietary data?

Can you answer...



..across DataAI systems?

Labeling

Are labels consistent?

Do they take into account data context to enforce policy?

Least Privilege

Can you enable least privilege data access?

Can you remediate gaps at the data source level?

Compliance

Can you test to ensure data is safe for use?

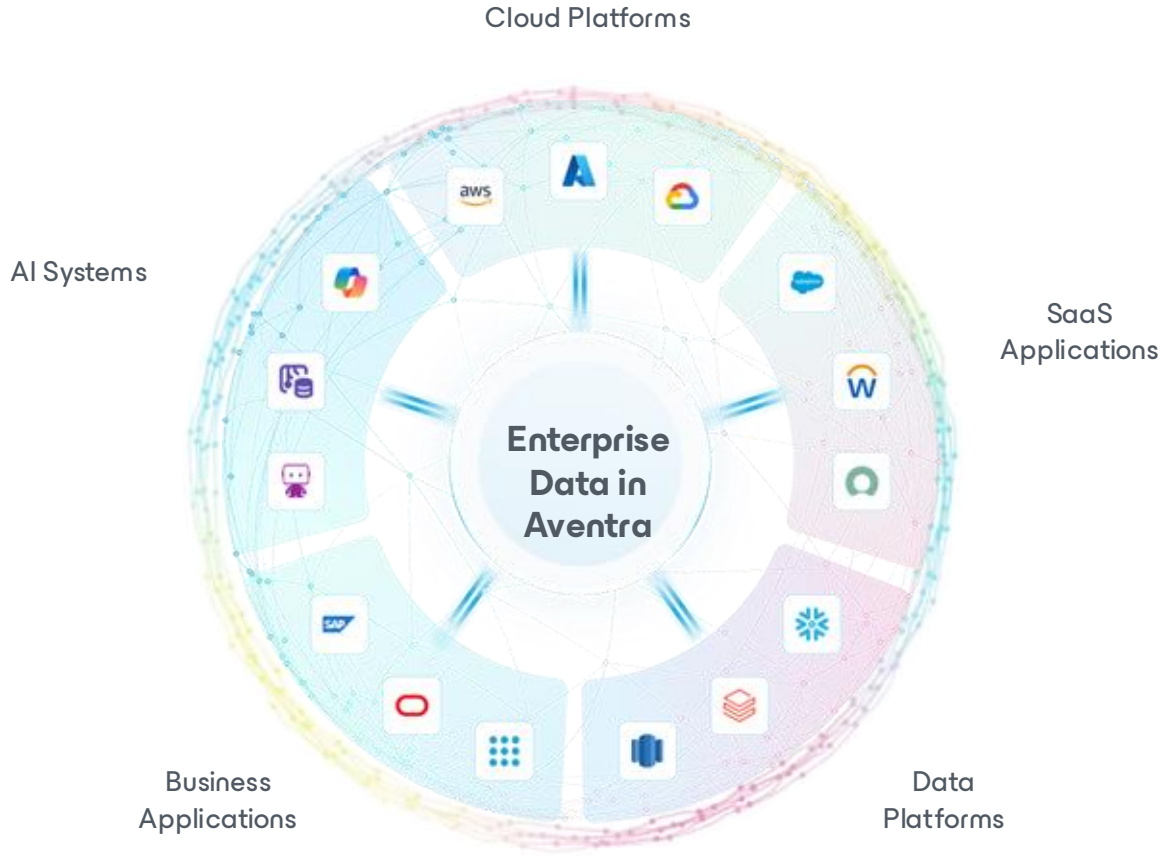
Can you prove it to regulators or stakeholders?

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

AI Readiness in Practice

Introducing Aventra

- Aventra is a Healthcare Organization paired with a financial arm: claims, member benefits and more
- Holds member PHI, payment data and financial records in one estate
- The analytics business unit is experiencing tremendous growth.
  - AI initiatives have tremendous potential but carry significant risk as well.
- Organic growth, new business units, autonomy in technology decisions and growth via acquisition has created a **complex and sprawling data environment**



No single team has the full map of where any of this data lives, or how it is used by AI.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

What Happened: Copilot Switched Off on Day One



The mandate

The board: "accelerate safe AI." The business took "accelerate" seriously.



The launch

Microsoft 365 Copilot rolled out to ~4,000 people who appeal denied claims.



The prompt

"Summarize examples of successful appeals for cardiology denials."



The leak

Real patients' PHI from the answer went into an appeal emailed to a different payer.



Within four hours, Copilot was disabled
for the entire line of business. The flagship AI project of the year was switched off on its first day.

Copilot did exactly what it was designed to do. So what went wrong?

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

What Caused It: The Problem Was What Was Accessible



Appeals specialist
Asks a routine question



Microsoft 365 Copilot
Uses what she is permitted to see



SharePoint site: denials & appeals
Set up years earlier for an initiative later abandoned

Over permissioned Access



Clinical justifications: patient names, diagnoses, treatment histories

PHI · No label



Denials and appeals documentation

ROT Data

Sensitive Data Unsanitized

1 Abandoned, never locked down

Set up for an initiative that was later abandoned, and never locked back down.

2 Access widened automatically

Permissions widened when members were added to a related Microsoft Team. Nobody noticed.

3 PHI never labeled

No downstream control had any way to know it was sensitive.

Copilot didn't create the risk. It indexed it, and made it searchable in plain English.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Resolution: Remediate Data Security Gaps with DataAI Command Platform

Microsoft 365

- SharePoint sites
- OneDrive & Teams files
- Claims notes & appeals



DataAI Command Platform
DSPM for Microsoft 365

Classify and Label sensitive data
PHI tagged Restricted and Not for AI use

Minimize ROT data
Archive or delete records past retention

Enforce least privilege
Overshared sites moved from all employees to restricted

Validate continuously
Prove data is safe before Copilot uses it

Remediate at the source. Fix the data once, and every Copilot answer inherits the fix.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Outcome: Copilot Back On, Safely



Daniel Cross CISO

"I can finally show the board what data our AI reaches."



Priya Nair Director of Data Security

"PHI is labeled, ROT is gone and access is right-sized."



Sofia Alvarez Head of AI Governance

"Copilot is approved for appeals, with guardrails that work."

Microsoft 365 Copilot
Revenue cycle appeals

✓ APPROVED

Data validated and safe
Labels, least privilege and ROT checks pass

PHI excluded by guardrails
Restricted / Not for AI use content never ingested

Answers from current data
Stale and duplicate records archived or removed

Access right-sized
Appeals site limited to the appeals team

Accelerate. Safe. Both words of the board's mandate, delivered.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Scan QR Code or Go to:

https://securiti.ai/assessments/ai-readiness-assessment/

Is Your Organization Ready to Govern & Protect AI Agents?

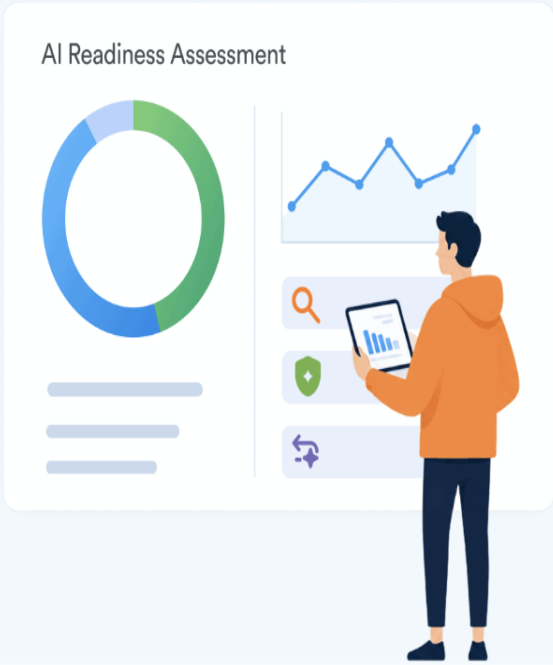
Check Your AI Data Security Readiness Level in 5 Minutes

AI agents are being deployed faster than security and governance teams can track them. From shadow AI to ungoverned data access and compliance gaps, the blast radius is expanding.

Do you know where your Data & AI security stands?

Take the quick Enterprise AI Readiness Assessment and see how prepared your organization really is across Detect, Protect, and Undo.

Start Assessment



© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.



THANK YOU