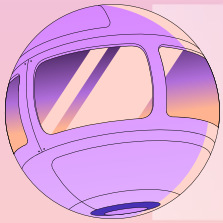
GUIDE

On-Prem Data Security Buyer's Guide

How to discover, classify,
and protect on-prem data at scale



cyera

On-prem data security focuses on discovering, classifying, and protecting sensitive data stored in on-premises systems such as file shares, databases, and legacy platforms. As enterprises operate in hybrid environments and adopt AI, modern DSPM platforms should provide continuous visibility and classification that goes beyond pattern matching to understand data in a full business context, analyze it across the data landscape, and operate autonomously in every environment once deployed. This approach delivers reliable findings and enables enforceable remediation to reduce risk without disrupting operations.

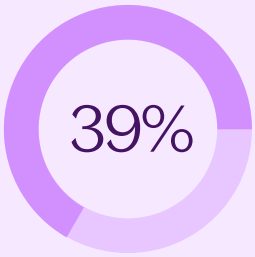
"Cyera's data discovery and AI-powered classification provides deep context and understanding of the data we are responsible for. With this simple extension of coverage to include on-premises databases and file shares, we now have for the first time a single solution for end-to-end visibility and control over all of our data, no matter where it resides."

- Mike Melo, CISO, Cyera Customer

Executive Summary

On-Prem isn't legacy. Secure it because it matters.

On-premises data remains a critical foundation for modern enterprises. Despite widespread cloud adoption, **39%** of organizations still store most of their data on-prem. It powers regulated workloads, legacy systems, high-performance applications, and core business operations. Yet for many security teams, it is the least visible and most difficult to secure.



Cyera provides end-to-end security over on-premises data through fast, actionable discovery, classification, governance, and protection using a modern DSPM platform. Cyera unifies data security across on-prem, SaaS, DBaaS, and IaaS environments, eliminating blind spots in hybrid estates.

Cyera deploys in minutes with a **lightweight connector or a fully connector-less architecture** that scans petabytes of data without disrupting operations and significantly lowers the total cost of ownership.

The platform discovers sensitive data across file shares, databases, and applications, and classifies it with over 95% precision through an adaptiveAI-native classification engine that understands data in a full business context. Each data asset is enriched with essential attributes, including sensitivity, purpose, human and non-human identities, access activity, exposure conditions, and more. This enables security teams to prioritize their efforts and act with confidence.

Cyera's lightweight deployment architecture is purpose-built for on-prem environments. Cyera supports both connector-based and connector-less deployment in SaaS or Outpost environments, giving organizations flexibility to meet security, operational, and architectural requirements.

Connector-less deployment enables rapid time to value by eliminating agents and ongoing maintenance, allowing teams to scan petabytes of on-prem data without disruption or operational overhead. For environments that require it, Cyera's lightweight connector is easy to deploy, requires minimal maintenance, and delivers significantly lower total cost of ownership than legacy connector- or agent-based solutions.

AI-powered insights across the data landscape quickly highlight high-risk data, excessive permissions, and compliance gaps, helping teams prioritize the exposures that matter most and take informed actions based on trusted data.

Who This Guide Is For

This guide is written for **cybersecurity and data leaders and practitioners responsible for securing on-prem data,** including:

C-suite executives such as CISO, CIO, CDO, Chief Privacy Officer

Security leaders such as Directors and VPs at large enterprises

Senior practitioners tasked with evaluating and recommending new solutions

Front-line security teams responsible for day-to-day data protection

The Reality of On-Prem Data in Hybrid Environments

Hybrid environments are now the norm.

Organizations have embraced the cloud for flexibility and scale, while keeping critical workloads on-prem for performance, regulatory, and operational reasons. The result is a **distributed data landscape** spanning on-prem data centers, field offices, manufacturing facilities, and multiple cloud providers and SaaS applications.

On-prem environments often include:

- Large volumes of unstructured files
- Legacy databases and applications
- Highly sensitive personal and regulated data
- Proprietary business IP

The risk profile of on-prem data is shifting dramatically as data volumes grow, evolve, and become accessible to AI systems and automation. AI amplifies the impact of weak data security foundations, allowing misclassified, over-exposed, or poorly governed data to be ingested, inferred, or misused at machine speed.

Legacy tools struggle to keep pace. Static inventories and manual scans create blind spots, allowing sensitive data to move or be used in ways teams cannot see, especially as AI systems interact with it.

Securing on-prem data now requires more than knowing where it resides. Teams must identify risk as it emerges, understand its business impact, and act quickly to reduce exposure without slowing operations or overwhelming security staff.

Unify Data Security Across All Environments

Modern data security cannot be siloed. Data moves freely across on-prem, SaaS, DBaaS, and IaaS environments, and risk often emerges at the boundaries between them.

An effective on-prem DSPM solution must operate across all of these environments through a single platform. A unified approach allows organizations to apply consistent policies, correlate risk across environments, and understand how sensitive data is accessed, shared, or exposed end-to-end. Without this visibility, teams are left with fragmented tools, disconnected insights, and blind spots that attackers and AI systems can exploit.

Discovery at Enterprise Scale

On-prem environments often contain hundreds of terabytes—or more—of data spread across file servers, databases, and applications. Discovery must be fast, continuous, and non-disruptive to be useful.

Cyera supports both connector-less and lightweight connector-based discovery architectures designed for enterprise scale. In connector-less deployments, smart sampling, clustering, and change-based monitoring enable rapid discovery across massive datasets without scanning file by file or introducing operational overhead.

For environments that require connectors, Cyera's lightweight connector is easy to deploy, optimized for fast and efficient discovery at scale, and delivers significantly lower total cost of ownership than legacy connector- or agent-based solutions. Both deployment models provide a continuously updated inventory of on-prem data without the performance impact, infrastructure burden, or operational complexity of traditional tools.

Exhaustive, Accurate Classification That Drives Action

Classification is only valuable if teams trust the results.

Cyera's AI-native classification engine goes beyond basic pattern matching to understand data in full business context. It supports structured, semi-structured, and unstructured data and applies the right level of intelligence—regex, machine learning, fine-tuned LLMs, or LLM validation—based on file and data types and complexity.

This adaptive approach delivers high precision and high recall without manual tuning. It uncovers sensitive, proprietary, and previously unknown data types that traditional DSPM tools miss, especially in unstructured content. The result is classification that teams can rely on to inform prioritization, policies, enforcement, and remediation.

From Visibility to Enforceable Protection

Cyera turns on-prem data visibility into insights you can confidently act on.

By combining autonomous discovery with enriched classification that reflects how the business understands its data, Cyera enables organizations to actively reduce risk—not just report on it. Data is enriched with multiple dimensions of insight, including:

- Data sensitivity and business purpose
- Human and non-human identities
- Access permissions and actual usage
- Exposure conditions and risk indicators

This depth of understanding dramatically reduces false positives and gives security teams confidence to act and support compliance with frameworks such as GDPR and HIPAA.

Answer the Questions That Matter

With Cyera, organizations can confidently answer foundational data security questions:

- Where is our sensitive data—and what environments does it span?
- What kind of data is it, and why does it matter to the business?
- Who or what can access it, and how is it actually being used?
- Is it exposed, over-retained, or misused?
- What risk does it create—and what action should be taken?

This shared understanding enables faster decisions, clearer ownership, and coordinated action across security, privacy, and data teams.

The On-Prem DSPM Checklist

When evaluating an on-prem DSPM solution, buyers should ensure it can:

- [ ] Deploy in minutes.
- [ ] Discover and classify structured and unstructured on-prem data in just a few days, not weeks or months.
- [ ] Operate seamlessly across hybrid environments
- [ ] Deliver 95%+ classification precision using fine-tuned LLMs, not just regex rules
- [ ] Keep data discovery and classification continuously up to date, without impacting operations
- [ ] Enrich data with deep business context, including data sensitivity, data purpose, human and non-human identities, access activity, exposure conditions, and risk indicators
- [ ] Identify true data exposure and prioritize the issues that matter most, dramatically reducing false positives and alert noise
- [ ] Enable remediation actions that teams feel confident taking - clearly scoped, auditable, routed to the right owners, and automated if desired
- [ ] Scale to hundreds of terabytes and billions of files

The Turning Point: Replacing Legacy Tools with Modern DSPM

Many organizations reach an inflection point where legacy on-prem data security tools can no longer keep up.

This moment often occurs when:

- Scan times stretch from days into months or years
- Infrastructure and licensing costs escalate dramatically
- Classification accuracy erodes at scale
- Teams lose confidence in alerts and remediation workflows

At this stage, organizations are no longer looking to optimize legacy platforms-they are actively replacing them.

In competitive on-prem evaluations, Cyera has demonstrated:

80%

reduction in breach likelihood by identifying and remediating high-risk exposures

$134K+

annual savings from replacing manual classification

Evaluating On-Prem DSPM at Enterprise Scale

On-prem environments demand immediate scalability.

Buyers should evaluate how solutions perform when faced with:

- Hundreds of terabytes of data
- Billions of files
- Predominantly unstructured data

Cyera has demonstrated real-world performance, including:

- Deployment in under 10 minutes
- 130 TB of Oracle databases classified in under 24 hours
- 82 million NetApp files scanned in 40 days
- 100 TB of file server data classified in under 3 days
- 1.4B files indexed with consistent precision

These outcomes are not achievable with tools that rely on heavy connectors, full data ingestion, or static scanning models.

Deployment Models Matter On-Prem

On-prem environments are not one-size-fits-all.

Cyera supports flexible deployment models designed to align with diverse security, operational, and architectural requirements, including:

Connector-Based Deployment: Cyera's lightweight connector is simple to set up, requires minimal maintenance, and provides a lower total cost of ownership compared to legacy solutions.

Connector-Less Deployment: Uses your existing routing from cloud to on-premises environments. This connector-less discovery reduces internal friction and delivers higher scan speeds without manual rules.

Secure outbound-only connectivity to reduce network exposure and simplify security approvals.

Private connectivity options, including Direct Connect or ExpressRoute, when required by enterprise or regulatory constraints.

Cyera Outpost deployment, which allows organizations to keep data fully within their own network while still benefiting from Cyera's AI-powered discovery and classification.

This flexibility allows organizations to choose the least disruptive path to value based on their architecture and risk posture—not vendor constraints.

Cost Is a Security Signal

On-prem data security costs are often driven by infrastructure requirements, deployment complexity, and ongoing operational overhead, including agents, connectors, and manual configuration.

Cyera uses connector-less discovery and enriched classification to scan on-premises databases, file shares, and application data. This approach does not rely on heavy agents or manual rules and identifies sensitive data types, relationships, and risk indicators.

Cyera also supports lightweight connector-based deployments across SaaS and Outpost environments. The lightweight connector is designed to be easy to deploy and to provide lower total cost of ownership compared to legacy connector- or agent-based solutions.

With Cyera Outpost, data can remain fully within the customer's network while still enabling enriched, AI-powered classification and contextual risk assessment.

Cyera integrates with existing SIEM, SOAR, IAM, DLP, ticketing, and workflow systems, allowing on-prem findings to be operationalized within the customer's existing security stack.

Why Cyera for On-Prem Environments

"With Cyera, we were able to use not just cloud but also on-prem. We still had hardships that we had to work through, and Cyera had those capabilities. They were able to not only do that, but also extend their capabilities to meet our requirements." **- Jorge Perez - CISO at a Financial Institution**

With Cyera, organizations gain:

1. Fast deployment:

Connector-less deployment delivers complete data visibility and rapid time to value-without ongoing connector maintenance or operational drag.

2. Classification teams can trust:

Cyera's enriched classification uncovers sensitive data across structured and unstructured sources, including what is unique to your business. Built on an AI-native engine, Cyera continuously learns and adapts to your environment based on business context and classifies data automatically, without manual tuning or rule maintenance.

3. Data, Identity, and Access Convergence:

Map every data asset to human and non-human identities, understand who can and did access it, and enforce least-privilege controls.

4. Effective Prioritization:

AI-driven severity scoring correlates sensitivity, identity, and exposure to surface the highest-impact risks, dramatically reducing noise for analysts.

5. Actionable Insights:

Address risks with confidence by using insights that are based on trusted data or by routing issues with context directly to data owners.

Buyer Questions to Ask When Evaluating On-Prem Data Security

What should enterprises look for in an on-prem data security solution?

Enterprises should look for fast deployment, continuous discovery, and enriched classification that automatically aligns to their unique business and correlates signals across the data landscape to drive risk-based prioritization. The solution should scale across large on-prem environments and enable safe, confident remediation without operational disruption.

Why is DSPM critical for securing on-prem data?

DSPM provides continuous visibility into on-prem data and enriches it with context such as sensitivity, access, and exposure. This allows teams to identify real risk, reduce false positives, and take confident action as data changes.

How should buyers evaluate on-prem DSPM at enterprise scale?

Buyers should assess how solutions perform across hundreds of terabytes of data, unstructured content, and complex access models. Key indicators include deployment speed, classification precision, remediation confidence, and total cost of ownership.

How does on-prem data security fit into hybrid environments?

Modern on-prem data security must integrate seamlessly with cloud and SaaS environments. A unified platform enables consistent policies, correlated risk analysis, and end-to-end visibility across hybrid data estates.

Final Takeaway

"Using Cyera has significantly improved our visibility into sensitive data across cloud and on-prem environment"-**IT Associate (Retail), Gartner Peer Insights**

On-prem data is too important to secure with outdated approaches.

The modern standard for on-prem data security is defined by:

- Speed without disruption
- Precision without manual validation
- Scale without runaway cost
- Action without operational risk

Cyera delivers that standard-giving security teams confidence, control, and measurable risk reduction across on-prem and hybrid environments.

Make On-Prem Data a Business Strength - Not a Security Blind Spot

On-prem data isn't going away - and neither is the risk that comes with limited visibility, slow discovery, and outdated tooling.

The right DSPM solution should help you:

- Understand exactly what sensitive data you have on-prem
- Prioritize which exposures matter most - and why
- Act quickly, safely, and at scale

Cyera was built to give security teams direct, real-time visibility and control over on-prem data, without the cost, complexity, or delay of legacy approaches.

See how Cyera delivers fast discovery, enriched classification, and actionable risk reduction across on-prem and hybrid environments.

Book a demo →

About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data and their security exposure, and delivers automated remediation to reduce their attack surface.

Learn more at www.cyera.com, or follow Cyera on LinkedIn.

cyera