DirSys

White Paper

Evaluation of DirSys Security Hub

A Unified Architecture for Security Intelligence, Distributed Scanning and Governance Automation

Version: 1.0
Date: December 2025
Prepared by: DirSys AB

---

1 Introduction

As digital infrastructures grow more fragmented and complex, organizations are increasingly challenged by a lack of unified visibility across their systems, data and identity structures. Information resides simultaneously in cloud services, local directories, web applications, legacy databases, networks, and public-facing platforms. In this distributed landscape, cybersecurity teams struggle to form an accurate understanding of risks, compliance teams face escalating regulatory expectations, and operational units lack the tools they need to maintain consistent control.

DirSys Security Hub was created to address these challenges with a fundamentally different approach. Rather than acting as ***yet another dashboard***, the Security Hub serves as the central intelligence layer in a distributed ecosystem of scanners, analytics engines and governance models.

It unifies findings from across the entire IT environment—including directories, data stores, networks, applications and web systems—and transforms these findings into meaningful governance insights. By combining object-centric modeling, advanced runtime algorithms and AI-supported interpretation, the platform enables continuous, holistic visibility across the organization's security posture.

Security Hub is built for a world where compliance frameworks such as NIS2, GDPR, ISO 27001 and CIS Controls now require not only technical safeguards but also demonstrable governance structures. It connects deeply technical scanning results with the language of regulatory evidence, risk management and organizational accountability.

2 Distributed Scanning and Local Runtime Intelligence

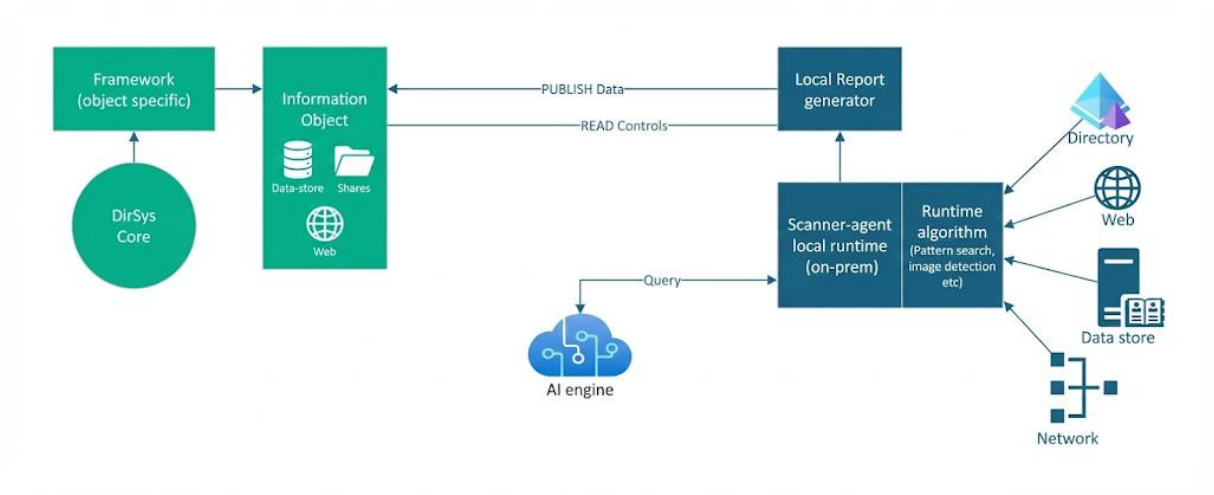
An essential element of the Security Hub is its use of localized, on-premise scanning agents. These agents execute deep analysis of the systems they assess without moving sensitive content beyond the customer environment. By employing a modular runtime engine, the agents can interact with a wide array of system types, including Active Directory domains, Microsoft Entra ID tenants, file systems, cloud storage, relational databases, web portals, and network devices.

The agents rely on specialized runtime algorithms that are tailored to their domain. **DirectoryScanner** reconstructs privilege structures, evaluates delegated access, maps authentication risks and identifies escalation paths across both AD and Entra ID. **FileScanner** performs pattern recognition, semantic content inspection and classification of sensitive information. **PrivacyScanner** examines web behaviors, script interactions and potential exposure of personal data. Other scanning components probe network-facing systems, application infrastructures and data repositories.

This localized processing ensures both security and efficiency. Organizations maintain full sovereignty over their data, while benefiting from advanced analytical methodologies designed to extract meaningful insight from complex, interconnected structures.

3 Architectural overview, DirSys AI-agent model

DirSys is designed with full architectural flexibility, enabling the entire platform to operate in cloud-native, hybrid, or fully on-premise environments. Organizations can deploy DirSys Core, the scanning agents, and all supporting services in the model that best aligns with their regulatory, operational, or security requirements. Whether running in a secure national cloud, a private data center, or a mixed topology with local runtime components and cloud-based correlation, the platform maintains identical functionality and governance capabilities. This deployment flexibility ensures that DirSys can support everything from highly regulated public-sector entities to large enterprises with complex hybrid infrastructures.



The diagram above illustrates the end-to-end operational architecture of the DirSys scanning ecosystem—showing how DirectoryScanner, FileScanner, PrivacyScanner, and other DirSys agents integrate with the DirSys Core, the Information Object model, on-premise scanning processes, runtime algorithms, and the AI-driven analytical engine. Together, these components form a unified and fully automated security-analysis workflow that covers directories, data stores, networks, web systems, and structured/unstructured information assets.

1. Framework and DirSys Core

On the far left, the diagram shows the DirSys Core, which serves as the foundational control layer for the entire platform. The Core defines the applicable Framework for each object type—such as NIS2, ISO 27001, CIS Controls, GDPR, or sector-specific governance models. These frameworks specify which controls apply to different classes of Information Objects.
The framework is dynamically bound to each Information Object, enabling object-specific compliance mapping and risk interpretation.

2. Information Object Layer

An Information Object represents any security-relevant asset in the organization—file shares, cloud storage, databases, web systems, or any structured/unstructured data domain.
The scanner agents interact with this layer by:

- Reading defined controls and expectations (e.g., identity governance rules, data-protection rules, access policies).
- Publishing detected data back into the Information Object for further correlation in the DirSys Security Hub.

This model ensures that every object is analyzed consistently, regardless of whether it resides in a directory, database, web environment, or network segment.

3. Scanner-Agent Local Runtime On-Premise (optional)

The scanning itself is performed by a local runtime agent, deployed on-prem or at the customer's chosen location. This design has several security and operational implications:

- No sensitive data leaves the customer's environment unless explicitly configured.
- Scanning is executed with least-privilege read access.

Complex environments—such as large AD forests or multi-site file structures—can be scanned efficiently without moving raw data to the cloud.

The local runtime invokes one or multiple runtime algorithms, depending on the agent type (DirectoryScanner, FileScanner, PrivacyScanner):

4. Runtime Algorithms

The diagram highlights runtime algorithms such as:

- Pattern search algorithms for detecting credentials, misconfigurations, or policy violations.
- Privilege-graph construction algorithms for (mapping identities, ACEs, delegation paths, nested groups, and RBAC structures).
- Image detection and metadata extraction for content scanning.
- Behavioral inspection algorithms for web and application environments.

These algorithms translate system configurations and raw artifacts into structured insights that can be interpreted at scale.

5. Integration with External Systems

At the right side of the diagram, the runtime systems interface directly with:

- Directories (Active Directory, Entra ID, LDAP)
- Web systems (public portals, intranets, APIs)
- Data stores (file systems, cloud storage, DBs)
- Networks (infrastructure components, endpoints, topology)

The local runtime collects data from these environments to build a complete operational picture of risks, identities, permissions, exposed assets, and compliance posture.

6. AI Engine for Advanced Interpretation

The central lower section shows the AI engine, which receives structured queries from the scanner runtime.
The AI component is used for:

- Contextual interpretation of DirectoryScanner findings

- Automated risk summaries for each identity or asset
- Transformation of technical findings into governance-ready language
- Pattern recognition across large identity and data sets
- Framework-specific compliance explanations

The use of AI accelerates reporting workflows and ensures that even highly technical results can be understood by governance and management layers.

7. Local Report Generator

Before data is exported to the DirSys Security Hub or other systems, results pass through the Local Report Generator, which compiles:

- Object-level reports (per identity, per group, per file share, per system)
- Framework-aligned compliance summaries
- Risk scores and remediation recommendations
- Technical deep-dive outputs for administrators and auditors

This step ensures that reporting can be done entirely on-prem, supporting environments with strict security or data-sovereignty requirements.

4 Conclusion

DirSys Security Hub represents a new architectural foundation for cybersecurity and information governance. By merging distributed scanning technologies with a central intelligence layer capable of contextualizing and correlating findings, the platform enables organizations to achieve a deeper, more accurate and more actionable understanding of their security posture.

It turns raw technical insight into governance-ready intelligence, bridges the gap between operational IT and regulatory compliance, and supports organizations in managing complexity across identity structures, data stores, networks and applications. As digital ecosystems continue to expand and regulatory environments become more demanding, this integrated, object-centric and intelligence-driven approach is no longer optional—it is essential.