IT Sovereignty Starts with Visibility

Understanding Dependencies, Infrastructure Configurations, and Security Posture in Hybrid IT Environments

A Whitepaper by NiCE IT Management Solutions



Overview

Cloud services, hybrid infrastructure and increasingly complex IT environments are creating new challenges for organizations striving to maintain control over their technology and data.

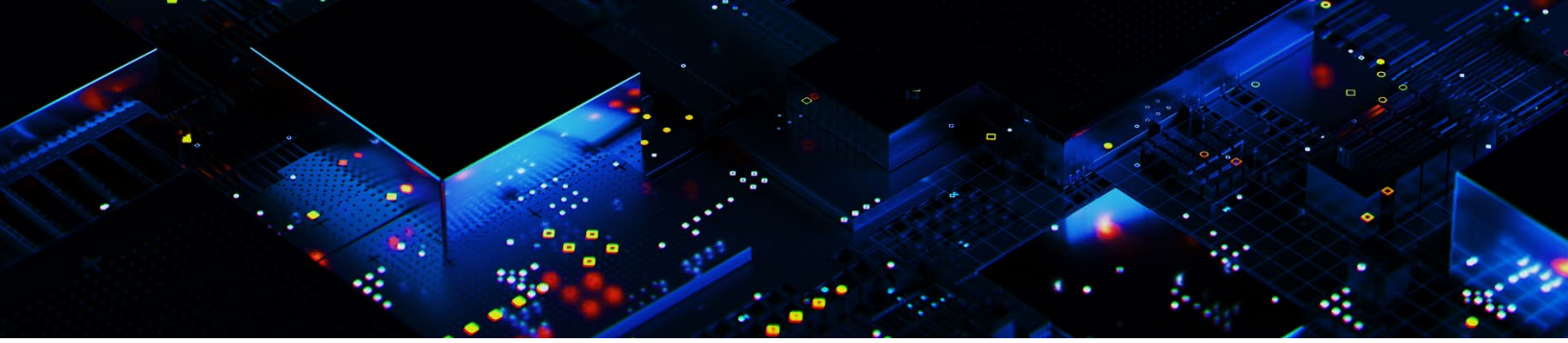
But do you really know what runs in your IT environment, where it resides, which services it depends on and whether it is adequately protected?

Digital sovereignty starts with visibility. Discover how infrastructure monitoring, Management Packs and CMDB integration can help you uncover dependencies, improve transparency and build more resilient IT operations – without sacrificing the flexibility of hybrid IT.

© NiCE IT Management Solutions GmbH
November 2026 | www.nice.de

Content

Executive Summary 3
The Cloud Dependency Question 4
Digital Sovereignty: More Than Data Residency 6
Hybrid IT: Choosing Where Control Resides 8
You Cannot Protect What You Cannot See 10
Turning Monitoring Data into IT Inventory Intelligence 12
From Infrastructure Visibility to Security Posture 15
From Information to Actionable Intelligence 17
Building a More Resilient Monitoring Strategy 19
Conclusion: Visibility Creates Control 20
Practical Self-Assessment: How Much Control Do You Have Over Your IT Environment? 21
About NiCE 23



Executive Summary

Cloud services have become an **integral part of modern IT** operations. Organizations rely on external platforms for infrastructure management, monitoring, data processing, collaboration and business-critical applications. While these services offer flexibility and scalability, they also introduce dependencies that are not always fully understood.

What happens if a cloud provider changes its service offering, restricts access to certain regions, changes its licensing model or becomes temporarily unavailable? Where does operational data reside? Which systems depend on external services? And how long could an organization continue operating if a critical dependency disappeared?

These questions are no longer limited to cloud strategy or data protection. They are increasingly relevant to the **resilience, sovereignty and operational control** of entire IT environments.

Digital sovereignty does not necessarily mean avoiding cloud services or moving everything back on-premises. It means understanding where technology and data reside, who controls them, which dependencies exist and whether an organization retains sufficient control to continue operating under changing conditions.

Achieving this level of control requires more than documentation and policy. Organizations need reliable, continuously updated information about their infrastructure, applications, configurations and dependencies.

IT monitoring can play a much broader role in this context. Beyond detecting performance problems and service interruptions, monitoring platforms collect valuable information about infrastructure components, installed products, configurations, relationships and operational status.

By combining this information with external data sources and Configuration Management Databases (CMDBs), organizations can build a more complete picture of their IT environments.

This paper explores how organizations can use monitoring, infrastructure discovery and configuration intelligence to strengthen digital sovereignty, reduce dependency risks and improve operational resilience.

The Cloud Dependency Question

Cloud adoption has transformed how organizations deploy, operate and manage IT services. Infrastructure can be provisioned on demand, applications can be delivered globally, and management platforms can provide centralized visibility across geographically distributed environments.

However, every external service introduces a dependency.

Organizations often focus on the benefits of cloud adoption while paying less attention to the operational implications of losing access to a particular provider, platform or service.

Consider a hypothetical scenario

An organization relies on a cloud-hosted monitoring service operated by an international provider. The service collects infrastructure metrics, processes alerts and provides operational dashboards.

Following **regulatory, contractual or commercial changes**, the provider announces that the service will no longer be available to customers in a particular region.

The organization suddenly faces several questions:

- Can administrators still access historical monitoring data?
- Are alerts and notifications still being generated?
- Can infrastructure continue to be monitored locally?
- Are configuration information and dependencies documented elsewhere?
- How much time is available to migrate to another solution?
- Which business services could be affected?

Even without a complete service withdrawal, changes to regional availability, licensing, data residency or connectivity can create significant operational challenges.

The problem is not necessarily the use of cloud services itself. It is the lack of visibility into the dependencies they introduce.

Understanding what runs where

Organizations need a reliable overview of their IT landscape, including:

- Which applications and infrastructure components are deployed?
- Where are they hosted: on-premises, in private clouds or public clouds?
- Which external platforms and services do they depend on?
- Where is operational and business data processed and stored?
- Which products and software versions are installed?
- When do support agreements, licenses and product lifecycles expire?
- What happens if a particular service or provider becomes unavailable?

Operational resilience starts with understanding what you depend on. Without this information, organizations may discover critical dependencies only when they become a problem.

Digital Sovereignty: More Than Data Residency

Digital sovereignty is often discussed in the context of data residency and regulatory compliance. While these aspects are important, they represent only part of the picture.

For IT operations, sovereignty encompasses several interconnected dimensions.

Data sovereignty

Where is information stored and processed? Which legal jurisdictions apply? Who can access the data, and under which conditions?

Monitoring data deserves particular attention. Infrastructure metrics, application dependencies, system configurations and operational incidents can reveal detailed information about an organization's technology landscape.

Operational sovereignty

Who has control over the systems and services required to operate the IT environment?

Organizations should understand whether critical administrative functions, monitoring capabilities and management interfaces remain available independently of external providers.

Technological sovereignty

How dependent is the organization on individual vendors, proprietary platforms, specific licensing models or technologies that are difficult to replace?

A technically functioning environment may still be highly dependent on external components that cannot easily be substituted.

Service continuity

Can critical IT operations continue if connectivity to external services is interrupted?

This includes monitoring, identity management, administration, security operations, backup and recovery processes.

Security and compliance

Can the organization demonstrate which systems are deployed, how they are configured and whether relevant security requirements are being met?

This requires more than periodic audits. It requires current and trustworthy information.

The European Commission's 2026 work on technological sovereignty and its Cloud Sovereignty Framework reflect this broader perspective, addressing legal, operational, technological, security and supply-chain considerations.

The practical implication is clear: organizations need to understand not only where their data resides, but also how their entire IT operating model depends on external technologies and services.

Hybrid IT: Choosing Where Control Resides

Discussion about digital sovereignty should not become a simplistic argument for or against cloud adoption.

Public cloud, private cloud, on-premises infrastructure and hybrid architecture all have their place. The appropriate model depends on business requirements, regulatory obligations, technical constraints and operational priorities.

The challenge is ensuring that organizations retain visibility and control across all of them.

Public cloud

Public cloud platforms provide scalable infrastructure and managed services. However, they also introduce dependencies on provider availability, connectivity, regional service offerings and contractual conditions.

Organizations should understand which workloads and management functions rely on these services and what alternatives exist.

Private cloud and on-premises infrastructure

Local infrastructure can provide greater direct control over data processing, system administration and operational dependencies.

However, on-premises does not automatically mean sovereign or resilient. Hardware, software, licensing, support agreements and external connectivity can still introduce dependencies.

Air-gapped environments

Some organizations operate environments that are deliberately isolated from public networks.

This can be necessary for highly regulated, security-sensitive or operationally critical environments.

Such environments require particular attention to:

- Offline installation and update processes
- Local monitoring and alerting
- Internal data storage and reporting
- Software and Management Pack lifecycle management
- Controlled transfer of information between environments

Monitoring solutions must be able to operate within these restrictions rather than assuming permanent internet connectivity.

Azure Local and disconnected operations

Azure Local illustrates how cloud-connected technologies can also support locally controlled operating models.

Microsoft documents a disconnected operations deployment model in which Azure Local can operate with a locally hosted control plane and local Azure portal capabilities.

Microsoft explicitly describes integration with external monitoring solutions, including System Center Operations Manager (SCOM), for monitoring the infrastructure, disconnected operations appliance, virtual machines and supported AKS environments.

This is particularly relevant for organizations that want to use modern infrastructure technologies while retaining local operational visibility.

It is important to distinguish a specifically deployed disconnected operations environment from an ordinary Azure Local installation that temporarily loses internet connectivity. The architecture and prerequisites differ.

The key consideration is not whether an environment uses cloud technology, but whether its critical operations remain manageable under the conditions the organization needs to support.

You Cannot Protect What You Cannot See

Understanding cloud dependencies is only one part of digital sovereignty.

Organizations also need to understand the actual contents and configurations of their IT environments.

In many enterprises, infrastructure information is distributed across multiple systems:

- Monitoring platforms
- Asset management solutions
- Configuration Management Databases
- Software deployment tools
- Cloud management platforms
- Security solutions
- Vendor-specific administration consoles
- Spreadsheets and manually maintained documentation

Each system provides a different perspective. Unfortunately, these perspectives are often incomplete or outdated.

A CMDB may contain an asset record but lack current operational information. A monitoring platform may know that a server exists and is healthy but has no information about its business owner or lifecycle status.

Security tools may report configuration weaknesses without providing a broader infrastructure context.

The result is fragmented information and limited situational awareness.

Moving beyond availability monitoring

Traditional monitoring answers questions such as:

- Is the server running?
- Is the application responding?
- Is storage capacity sufficient?
- Are performance thresholds being exceeded?
- Has a monitored component generated an alert?

These questions remain essential, but they are not sufficient for comprehensive infrastructure management.

Organizations increasingly need to answer questions such as:

- Which product and version are installed?
- Is the software still supported?
- Which components depend on this system?
- Is the relevant security functionality enabled?
- Which assets are affected by a configuration change?
- Which services would be impacted if a provider became unavailable?

This is where infrastructure discovery and configuration intelligence become important.

Monitoring platforms can contribute much more than health states. Depending on the technology and Management Pack, they can discover infrastructure objects, collect product-specific properties, identify relationships and expose configuration information.

When this information is combined with business and asset data, it becomes a valuable foundation for more informed IT decisions.

Turning Monitoring Data into IT Inventory Intelligence

A comprehensive view of the IT environment requires information from multiple sources.

Three particularly valuable building blocks are infrastructure monitoring, external data collection and CMDB integration.

Infrastructure discovery and monitoring

Monitoring platforms continuously interact with managed systems to collect information about their availability, configuration and performance.

Microsoft System Center Operations Manager (SCOM), for example, uses Management Packs to discover and monitor specific technologies.

NiCE Management Packs extend these capabilities to additional enterprise technologies, including databases, storage systems, operating systems, collaboration platforms and virtualization environments.

Depending on the individual Management Pack, the information discovered can include:

- Infrastructure components and their relationships
- Product-specific objects and properties
- Installed versions and configuration details
- Operational and performance information
- Relevant events and configuration changes

This information can serve as a source of inventory-related data in addition to its traditional monitoring purpose. The exact properties available depend on the technology, Management Pack version and discovery implementation.

External data collection and integration

Not all relevant information is available through monitoring. Business ownership, contractual information, organizational responsibilities, licensing details and other asset attributes may reside in separate enterprise systems.

Integration and automation solutions can help connect these sources. Kelverion provides integration and automation capabilities for Microsoft System Center Orchestrator and other automation environments. Its CMDB Population Solution documents how asset information discovered by SCOM and Configuration Manager can be transformed and transferred into third-party CMDB systems.

This creates an opportunity to combine monitoring-derived information with additional enterprise data.

CMDB enrichment

A Configuration Management Database provides a structured view of configuration items (CIs) and their relationships.

When monitoring and discovery information is integrated into a CMDB, organizations can improve the quality and timeliness of their configuration records.

For example, an asset record could combine:

Information	Potential source
System name and infrastructure identity	SCOM discovery
Installed product and version	Management Pack discovery
Operational health	SCOM monitoring
Performance and capacity	Monitoring platform
Business owner	CMDB
Business criticality	CMDB
Contract and licensing information	Enterprise asset management
Security-related configuration	Relevant monitoring or security interface
Infrastructure dependencies	SCOM discovery and CMDB relationships

The result is more than a list of monitored systems. It is a richer representation of the organization's IT environment, combining technical, operational and business information.

An example: BMC Atrium integration

Kelverion's documented CMDB Population Solution has included BMC Atrium as a supported target for transferring asset information from SCOM and Configuration Manager.

The documented integration approach includes creating and updating configuration items and maintaining relationships between discovered assets.

This illustrates how information already collected through existing Microsoft System Center investments can contribute to broader configuration management processes.

The specific integration product version, current availability and supported target configurations should always be verified before implementation.

The objective is to avoid maintaining multiple disconnected versions of the truth.

From Infrastructure Visibility to Security Posture

Knowing which systems exist and whether they are operational is important. Knowing how they are configured and whether relevant protection mechanisms are enabled is equally important.

Consider enterprise storage infrastructure.

A storage system can report healthy operational status while still having configuration weaknesses that expose the organization to unnecessary risk.

For example:

- Are relevant protection features enabled?
- Are replication relationships operating as expected?
- Are snapshots available?
- Are security-related configuration changes detected?
- Are certificates valid?
- Are access configurations consistent with organizational requirements?

This demonstrates why **operational health, and security should not be treated as interchangeable concepts.**

Example: NetApp and ransomware protection

NetApp ONTAP includes Autonomous Ransomware Protection (ARP), designed to detect abnormal activity that may indicate ransomware attacks. With newer ONTAP releases, ARP/AI uses a pre-trained machine learning model to identify suspicious activity in supported environments.

Protection is configurable at volume level, and its availability and behavior depend on ONTAP version, volume type, licensing and other technical prerequisites.

This creates a valuable monitoring scenario.

Imagine an operations dashboard showing:

Monitoring aspect	Example status
Storage cluster health	Healthy
Volume availability	Healthy
Capacity utilization	Normal
Replication	Healthy
Ransomware protection configuration	Requires attention

A storage environment can be operationally healthy while a relevant protection configuration still requires review.

Monitoring can help make such conditions visible, provided the required properties are exposed through supported interfaces and integrated into the monitoring solution.

The distinction matters: discovering that a protection feature is enabled does not prove that the entire storage environment is secure or that recovery will succeed.

Nevertheless, bringing operational and security-related configuration information together creates a much stronger basis for informed decisions.

From Information to Actionable Intelligence

Collecting infrastructure data is only the beginning. The real value emerges when organizations can use that information to identify risks, understand dependencies and take appropriate action.

Combining monitoring information with CMDB and external data can help answer questions that traditional availability monitoring alone cannot address.

Lifecycle and support management

Which systems are running outdated or unsupported software?

By combining discovered product versions with reliable lifecycle information, organizations can identify assets that require upgrades, replacement or additional support arrangements.

This is particularly relevant when planning migrations away from specific providers or technologies.

Dependency analysis

Which business services rely on a particular infrastructure component or external service?

Combining technical relationships with business context can help organizations understand the potential impact of service disruptions.

Security configuration visibility

Which systems have relevant security features disabled or incorrectly configured?

Where monitoring interfaces expose these properties, configuration information can be used to identify conditions requiring further investigation.

Cloud dependency assessment

Which systems rely on external platforms, services or connectivity?

An enriched inventory can support dependency reviews and help identify critical services that need alternative operating arrangements.

Change impact analysis

What happens when a system, application or provider changes?

Accurate configuration records and infrastructure relationships help identify potentially affected services and teams.

More informed strategic decisions

The combination of technical and business information also supports broader decisions about:

- Cloud migration
- Infrastructure modernization
- Vendor consolidation
- Technology replacement
- Capacity planning
- Security improvement
- Operational resilience

In this way, monitoring data becomes an input to strategic IT management rather than remaining confined to operational dashboards.

Building a More Resilient Monitoring Strategy

Organizations do not need to redesign their entire IT architecture to improve sovereignty and resilience. A structured approach can help identify weaknesses and make better use of existing monitoring investments. The following steps provide a practical starting point.

Assessment Area	What to Consider
Identify critical dependencies	Document the external services, platforms, providers and technologies required to operate critical business services. Consider both technical dependencies and contractual or licensing dependencies.
Understand where data and services reside	Establish where infrastructure is hosted, where monitoring data is processed and stored, and which jurisdictions and providers are involved. Include monitoring and management systems in the assessment.
Define operational continuity requirements	Determine which systems and capabilities must remain available during a cloud outage or loss of external connectivity. Consider monitoring, alerting, administration, identity and reporting.
Establish appropriate local monitoring capabilities	For critical on-premises and disconnected environments, ensure that monitoring and alerting can continue without relying on unavailable external services. SCOM can provide a foundation for centralized monitoring across supported hybrid and local infrastructure environments.
Enrich inventory and CMDB information	Use discovered infrastructure data to improve the completeness and accuracy of configuration records. Where appropriate, combine monitoring information with business ownership, product lifecycle, licensing and other enterprise data.
Track relevant configuration and protection information	Go beyond availability monitoring where technically feasible. Identify important configuration properties, security-related settings and protection mechanisms that should be visible to operations teams.
Review the architecture regularly	Dependencies change. Products reach end of life. Services are replaced. Infrastructure moves between locations and platforms. A sovereignty and resilience assessment should therefore be an ongoing process rather than a one-time exercise.

Conclusion: Visibility Creates Control

Digital sovereignty does not mean abandoning cloud services or avoiding external technology providers. It means understanding the dependencies they introduce and retaining the information and capabilities necessary to manage your IT environment under changing conditions.

Organizations need to know what they are running, where it runs, how it is configured, which services it depends on and whether relevant protection mechanisms are in place.

This requires more than traditional monitoring.

By combining infrastructure discovery, operational monitoring, Management Pack data, external information sources and CMDB integration, organizations can develop a more complete and continuously updated view of their IT environments.

Microsoft SCOM provides an established foundation for monitoring enterprise infrastructure across on-premises and hybrid environments. NiCE Management Packs extend that visibility to a broad range of technologies, while integration and automation solutions can help connect operational information with wider enterprise processes.

The result is not simply better monitoring. It is a stronger foundation for understanding dependencies, identifying risks, supporting compliance and maintaining operational control.

You cannot eliminate every dependency. But you can make those dependencies visible, understand their impact and prepare for what comes next.

Practical Self-Assessment: How Much Control Do You Have Over Your IT Environment?

Use the following questions to assess how well your organization understands its infrastructure, dependencies and operational resilience.

Infrastructure and dependencies

- We know where our critical IT services are hosted.
- We have documented dependencies on external cloud providers.
- We know which applications and systems rely on external connectivity.
- We understand the operational consequences of losing access to critical providers.

Inventory and configuration

- We maintain an up-to-date overview of deployed systems and applications.
- We know which product versions are installed.
- We track product lifecycles and support expirations.
- Our CMDB is enriched with current infrastructure discovery information.
- We can identify important relationships between infrastructure components and business services.

Monitoring and continuity

- Critical infrastructure can be monitored independently of public cloud services where required.
- We have defined operational continuity requirements for disconnected environments.
- Monitoring data remains accessible under our required operating conditions.
- We regularly review the availability and reliability of monitoring dependencies.

Security and protection

- We have visibility into relevant security configurations.
- We can identify important protection features that are disabled or incorrectly configured.
- We monitor relevant storage protection and replication configurations.
- We can correlate operational health with security-related configuration information.

The more questions you can answer confidently, the better equipped your organization is to manage dependencies and maintain control over its IT operations.

Further Reading and Technical References

- European Commission – Communication on European Tech Sovereignty (June 2026)
- European Commission – Cloud Sovereignty Framework
- Microsoft Learn – Monitor disconnected operations for Azure Local
- Kelverion – CMDB Population Solution
- NetApp – Autonomous Ransomware Protection
- NiCE – Management Packs for Microsoft SCOM
- NiCE – NetApp ONTAP Management Pack

Technical note: Specific discovery, integration and monitoring capabilities depend on product versions, supported interfaces, deployment architectures and configuration. Integration possibilities and individual Management Pack capabilities should be validated for the target environment before implementation.

About NiCE

NiCE Services for Microsoft System Center encompass consulting services tailored to System Center Operations Manager, Configuration Manager, and Service Manager. Our offerings include SCOM Health Assessments, training, advice and provisioning for third-party SCOM tools, as well as SCOM-centric monitoring solutions for business elements such as applications, databases, operating systems, services, and custom applications.

NiCE Management Packs for Microsoft SCOM are available for AIX, Azure AD Connect, Entra ID, Citrix VAD & ADC, Custom Applications, HCL Domino, IBM Db2, IBM HMC & VIOS, IBM Power HA, Linux on Power Systems, Log Files, MariaDB, Microsoft 365, Microsoft Teams, Microsoft SharePoint, Microsoft Exchange, Microsoft OneDrive, MongoDB, NetApp ONTAP, Oracle, URLs, Veritas Clusters, VMware vSphere, and zLinux.

Our commitment

1. Ongoing development, incl. latest version support
2. Top required metrics come out-of-the-box
3. Integrated source knowledge to solve issues faster
4. Custom development & coaching
5. Highly responsive support team
6. Easy onboarding & renewals
7. Largest set of Microsoft SCOM Management Packs

About Microsoft System Center Operations Manager (SCOM)

Microsoft SCOM is a powerful IT management solution designed to help organizations monitor, troubleshoot, and ensure the health of their IT infrastructure. SCOM provides comprehensive infrastructure monitoring, offering insights into the performance, availability, and security of applications and workloads across on-premises, cloud, and hybrid environments. With its robust set of features, SCOM enables IT professionals to proactively identify and address potential issues before they impact the business, improving overall operational efficiency and reducing downtime. By leveraging SCOM, businesses can achieve greater control over their IT environment, ensuring a seamless user experience and enhancing the reliability of their services.

Take advantage of all the benefits of advanced monitoring using NiCE Management Packs for Microsoft System Center Operations Manager. Contact us at solutions@nice.de for a quick demo, and a free 60 days trial.

NiCE IT Management Solutions GmbH
Liebigstrasse 9
71229 Leonberg
Germany
www.nice.de
solutions@nice.de