SPOTLIGHT

Sponsored by: Nutanix

Application and infrastructure modernization are critical investment priorities in 2026 and key to success in the current competitive environment. Unified management for data sovereignty with multicloud visibility, compliance, privacy, and control capabilities can accelerate enterprise modernization.

Digital Sovereignty Is an Enterprise Imperative, Requiring Unified Management and Visibility

March 2026

Written by: Dave Pearson, Group Vice President, Infrastructure Solutions

Introduction

Forward-looking organizations are leveraging IT modernization for both infrastructure and apps to increase their maturity in the modern era. The demand for greater control over data and infrastructure has never been more urgent, especially as AI initiatives bring a variety of data storage and management issues to the forefront — sovereignty, compliance, privacy, security, and data protection, among others. According to *Sovereign AI: What, Why, and How* (IDC #EUR153902925, December 2025), 86% of organizations expressed a desire for freedom to choose platforms beyond public cloud for AI inference at scale.

AT A GLANCE

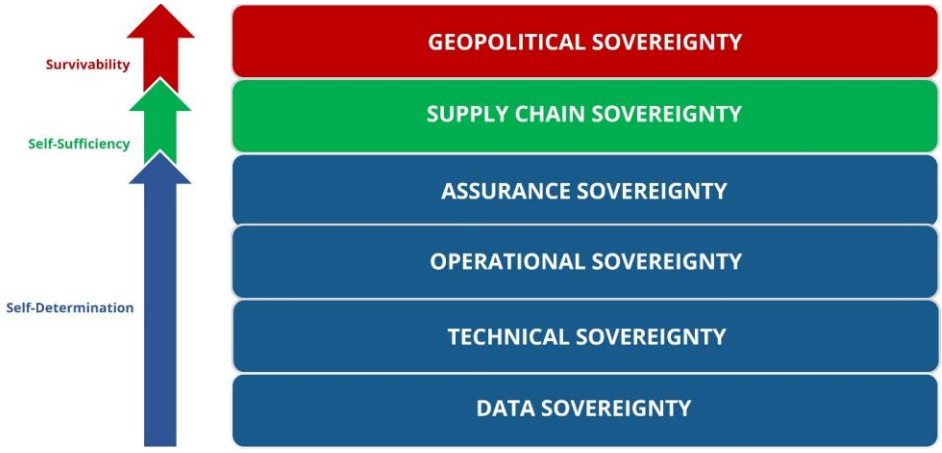
KEY STATS

- Fewer than one in five enterprises report full observability across their networks.
- Application and infrastructure modernization spending will increase for 28% and 30% of organizations, regardless of their budgetary plans.

The rapid evolution of regulatory frameworks and the proliferation of hybrid multicloud environments are reshaping how enterprises approach data residency, security, and operational efficiency. Organizations that fail to comply with regulations can face strict fines and penalties. Those who lose control of their data may face existential threats from exposure of customer or competitive data and IP. And those who fail to operate efficiently or provide value at scale will fall behind their competitors.

IDC formally defines digital sovereignty as "the capacity for digital self-determination by nations, organizations, and individuals." According to IDC's Digital Sovereignty Taxonomy (see Figure 1), a core component of digital sovereignty is data sovereignty, which requires that data owners have total control over how and where their data is managed, stored, and processed, whether that be on their own infrastructure or that of service providers.

FIGURE 1: ***IDC's digital sovereignty stack***



Notes:

Sovereignty taxonomy — digital is represented in blue, supply chain is represented in green, and geopolitical is represented in red.

The figure is from IDC's Worldwide Sovereign Cloud Taxonomy, 2024 (IDC #US50699324, September 2024).

Source: IDC, 2024

The four key aspects of digital self-determination are defined as follows:

- **Data sovereignty:** This refers to the entirety of the data owned, processed, managed, or stored by an organization and requires controls for privacy, security, data transfers, regulatory compliance, and portability. Solutions that provide a holistic, cross-enterprise view of where and how data is created, collected, classified, processed, stored, managed, and monitored are critical to establishing a baseline for data sovereignty.
- **Technical sovereignty:** Technical sovereignty establishes control and protection of all digital infrastructure, including tools and processes to manage interoperability and security. It includes all datacenters (servers, storage, networking, and security/other IT hardware) wherever they physically reside or however they are managed. This infrastructure should remain separate from non-sovereign digital infrastructure and protected from all extraterritorial interference and control.
- **Operational sovereignty:** Operational sovereignty is the ability to control access and utilization of both data and data infrastructure based on granular, adaptable policies across the organization, as well as its customers and partners. Complete and autonomous control requires solutions that offer capabilities to enable transparency in controlling operations, from provisioning and performance management to monitoring physical and digital access to infrastructure.
- **Assurance sovereignty:** Assurance sovereignty focusses on data availability, integrity, and security and guarantees the sovereign control and availability of critical workloads and infrastructure resources, including data protection, security, business continuity, and disaster recovery. This is tied to mandates such as the European Digital Operational Resilience Act (DORA) that enforce harsh financial penalties for noncompliance with oversight requirements to a global organization that does business in Europe.

Achieving true digital sovereignty requires control to extend beyond the data itself, including all underlying digital infrastructure (hardware and software) used for the data, ensuring organizations are not limited in their deployment options, handcuffed by vendor lock-in, or subject to regulatory risks.

For IT decision-makers, the ability to adapt to evolving regulatory requirements, avoid vendor lock-in, and optimize costs is central to sustaining competitive advantage and business continuity. The strategic use of unified management platforms and hybrid multicloud architectures is increasingly seen as a pathway to achieving these objectives, as well as the following:

- **Sovereignty and control in complex environments:** A core challenge facing IT leaders is balancing the need for digital sovereignty and risk mitigation with the operational demands of managing complex, distributed environments. Whether this is about precise control, improved protection, regulatory compliance and privacy requirements of data sovereignty, or the data localization regulations required for geopolitical sovereignty, organizations are faced with the need to control their own choices; to operate their choice of infrastructure in their choice of operating model in their preferred location with strict controls over their and their customers' data.
- **Data sovereignty and control in next-gen applications:** As organizations enter and mature in the data-centric, AI-driven era, they learn that certain workloads require a massive amount of data, often from disparate sources that have varying requirements for privacy, compliance, and data protection. 29% of organizations surveyed in *Sovereign AI: What, Why, and How* (IDC #EUR153902925, December 2025) are concerned about data or IP loss due to improper AI implementation or use.
- **Avoiding vendor lock-in:** Risk mitigation strategies are evolving, with organizations increasingly focused on avoiding vendor lock-in and ensuring interoperability, especially as enterprises see the value of new entrants or the effects of acquisitions between their existing vendor partner ecosystem.
- **Increased visibility and observability:** According to IDC's 2025 *Enterprise Infrastructure Pulse Survey,* only 19% of enterprises reported full observability across their networks, without which proactive optimization and anomaly detection remain elusive.
- **Legacy system modernization:** According to IDC's December 2025 *Future Enterprise Resiliency and Spending Survey*, nearly one-third of enterprises struggle to align traditional IT architectures with modern workloads that expect dynamic scaling, low latency, and AI-ready performance. Respondents indicated that infrastructure modernization spending will increase for 28% and 30% of respondents, respectively, regardless of their budgetary plans.

For this document, we interviewed two Nutanix customers, both of whom made Nutanix Central a key component of their application and infrastructure modernization journey.

The benefits of unified management

Improved operational efficiency results from centralized management interfaces that reduce administrative overhead and streamline life-cycle management across distributed environments.

Risk mitigation and operational as well as competitive resilience are strengthened by reducing exposure to vendor lock-in and enabling organizations to maintain flexibility in technology choices and deployments.

Enhanced control over data residency and compliance can be achieved by allowing organizations to determine and optimize where data is stored and processed, in response to constantly evolving regulatory requirements. IDC expects that by 2027, 75% of non-U.S. G2000 enterprises will prioritize the pursuit of data and technology sovereignty for their most critical data and applications, using a blend of nonpublic cloud deployments (on premises, hosted, and dedicated edge), open technologies, and regional partners.

> If it wasn't for this platform, I think we would be spending probably 30—40% more money on every aspect of our business. The overall reliability of the platform makes it cost-effective and efficient for us long term. — Lead systems engineer, Retail

Real-world use cases

IDC interviewed two Nutanix Central clients, one in the retail space and another in personal banking.

Retail case study

Client situation

This client operates nearly 300 retail stores across the United States with 60–70,000 employees, but no dedicated IT staff at those locations. Edge deployments at the retail locations are managed by two primary datacenters and three regionalized store operations locations. To the lead system engineer, technical sovereignty is paramount; they need the ability to operate the infrastructure required to support their business in whatever model and location they deem to be correct, with hybrid cloud being the preferred model (despite a preponderance of on-premises infrastructure), along with centralized datacenters and light edge deployments. Data sovereignty, to maintain control and ownership of internal data and to protect against external threats, was also considered critical.

Previous infrastructure pressures and complaints

This client suffered frequent outages at its retail locations due to its previous environment and hypervisor choices. Data protection and disaster recovery improvements were at the top of its list. Store outages were estimated to cause losses of $500,000–1 million per day. Licensing costs for its previous environment were also a pain point, and budget constraints were a primary challenge to its long-term growth and infrastructure plans.

Criteria for improvement/business success outcomes

Maintaining control of its data, reducing downtime and improving disaster recovery objectives, and cost control are the three areas that matter most to this client.

Improvements provided by Nutanix and Nutanix Central

According to the interviewed lead systems engineer, uptime improved markedly, from an estimated 80% to 99.995%. While the hardware vendor's firmware caused difficulties during the transition to Nutanix Central, Nutanix support was praised for its responsiveness and broad expertise across platforms.

Cost savings were found in a variety of ways:

- **Simplifying and consolidation of infrastructure.** The five clusters currently replacing the previous environment are expected to be reduced to three. Workload consolidation and data efficiencies derived from Nutanix infrastructure

and Nutanix Central will allow further reductions in footprint and costs. Some previous infrastructure must continue to be maintained for the time being.

- **Increased availability, reduced downtime costs, and faster resolution due to centralized management and visibility across the entire infrastructure portfolio**
- **Reduced licensing costs.** Moving from perpetual to subscription licenses for monitoring tools has saved an estimated $2 million per year.
- **Data reduction capabilities far exceeding the client's expectations.** This led to a reduced need for infrastructure (from systems to media), a smaller datacenter footprint, reduced power and cooling costs, and administrative overhead.
- **Managing data protection and disaster recovery through Prism Central and Nutanix Central.** This allowed the client to discontinue usage and licensing of third-party offerings that were no longer necessary.

By maintaining dedicated infrastructure for sensitive workloads rather than modernizing by moving to public cloud, the client was able to maintain complete control over its data — sovereignty was integral to its deployment choice rather than something it needed to depend on third parties to manage and certify.

Future outlook

Although the client has a preference for on-premises solutions at this time, it noted the growth and availability of capabilities and scalability with hybrid operating models being supported; this flexibility is important to the growing organization. The client is prepared to continue to make significant investments in what it considers to be "preventative IT infrastructure"; that is, taking a proactive approach to providing performance and capabilities to its IT teams and internal customers while preventing system failures and protecting data to avoid external threats to its data and technical sovereignty.

Personal banking case study

Client situation

This client operates traditional on-premises retail banking, along with a growing set of online digital services for customers, as well as a dedicated private banking business. In this highly regulated and competitive field, sovereignty has multiple meanings for the client. Geopolitical sovereignty comes in the form of data localization and control of personal and financial information. Assurance sovereignty (availability and resilience of data) is achieved through regulatory compliance and oversight, along with strict ISO and cybersecurity certifications. Finally, data sovereignty is critical to the bank; while the client utilizes public cloud infrastructure as a part of its digital operating strategies, it depends on local, hybrid cloud technologies to secure and protect its customers' data, with long-term retention policies dictated by the client's country's central bank.

Previous infrastructure pressures and complaints

This client found that the blade servers running its virtual machine (VM) infrastructure were the cause of persistent freezing issues and looked for alternatives. Command-line interfaces (CLIs) were the primary point of management for its mixed vendor environments, with no centralized visibility or management tools. Complexity in maintaining and operating these environments led to an initial pilot with Nutanix for VDI and testing workloads, which led to a full product migration, eventually incorporating Nutanix Central.

Criteria for improvement/business success outcomes

Improving performance, reducing downtime, and improving management capabilities while simplifying operations were critical factors in selecting Nutanix and Nutanix Central, as was the ability to support data, assurance, and geopolitical sovereignty through on-premises and hybrid cloud operating models.

Improvements provided by Nutanix and Nutanix Central

Nutanix Central's ease of administration enables teams to focus on innovation and automation rather than focusing on "keeping the lights on." CLI usage has dropped considerably (certain legacy systems are still maintained where necessary), but consolidated environmental views and ease of management mean that this rapidly growing financial services company has been able to avoid equally rapid growth of IT teams through more efficient management. Performance and reliability were both noted to be improved after the conversion to Nutanix. Assurance sovereignty is supported by Nutanix Central's adherence to a variety of ISO requirements, including information security and security controls, protection for personally identifiable information (PII), privacy information management, supply chain security management, and business continuity management systems.

Future outlook

Container workload utilization has increased since 2019 and is expected to continue to grow as the client focuses on microservice architectures, which continue to be supported and improved by Nutanix. Nutanix Central's ability to manage both VMs and containers will allow the client to choose when and where to modernize its application portfolio. While the client has had concerns about relying so heavily on a single vendor, it is confident in Nutanix Central's ability to support future needs, as Nutanix's alignment with technology trends resonates with the client's expectations of future needs (an example given was the timely integration of S3 buckets via Nutanix Objects).

Nutanix Central supports infrastructure modernization and data sovereignty

- Nutanix, through its Nutanix Central solution, helps organizations seeking control, efficiency, and risk mitigation by addressing some of the challenges they face in digital sovereignty, unified management, and hybrid multicloud operations.
- Nutanix Central provides a unified management console for Nutanix environments, offering both SaaS and on-premises deployment options to support diverse sovereignty and compliance requirements. The solution enables centralized oversight of multiple Prism Central instances across regions, delivering a single pane of glass for managing distributed infrastructure and applications in a variety of deployment models and locations. Nutanix Central on premises allows organizations to keep workload data and management within their controlled datacenter, helping organizations achieve true data sovereignty.
- Nutanix Central is designed to support hybrid multicloud operating models, allowing organizations to seamlessly manage workloads across on-premises, private, and public cloud environments while maintaining control over data residency and governance. By managing IT resources across all of these deployment locations, Nutanix Central reduces customers' dependence on any single cloud provider's native management tools, both limiting lock-in and allowing for consistent management policies, security, and operational capability. The platform provides customers with opportunities to enhance operational efficiency by streamlining monitoring, alerting, and life-cycle management, with features that enable near-real-time issue detection and resolution. Nutanix is well-known for supporting and managing VMs through its own and third-party hypervisors, but it also supports

container workload management and integration with microservices architectures, enabling organizations to adopt modern application development and deployment practices.

- Nutanix Central enables improved licensing and cost management by providing unified visibility into subscription consumption and supports efficiency gains from data reduction technologies that contribute to cost optimization.
- Complementary technologies within the Nutanix portfolio, such as Nutanix AHV, Prism Central, and Nutanix Objects, are designed to further enhance the platform's capabilities in data protection, security, and operational resilience.

Capabilities

- **Centralized data management:** Enables unified oversight and control of data across hybrid, multicloud, and edge environments, allowing organizations to manage data location and movement according to regulatory requirements
- **Data sovereignty controls:** Provides visibility into where data resides and supports policy-driven placement, helping organizations comply with jurisdictional mandates and local data residency laws
- **Compliance automation:** Facilitates consistent enforcement of compliance policies (e.g., GDPR, HIPAA) across all Nutanix clusters, with automated monitoring and reporting to support audit readiness
- **Governance framework:** Implements federated IAM and robust role-based access control (RBAC), policy management, and centralized configuration so that only authorized users can access or modify sensitive data and infrastructure settings
- **Global policy enforcement:** Allows organizations to define and propagate governance policies (security, access, data handling) globally, helping control risk and supporting compliance efforts
- **Audit and reporting:** Integrated tools for tracking changes, user activity, and policy adherence, supporting both internal governance and external regulatory audits

Customer benefits

- **Data sovereignty capabilities:** Organizations can confidently manage and restrict data to specific geographies, supporting legal and regulatory obligations.
- **Simplified compliance:** Automated policy enforcement and reporting reduce the burden of manual compliance management and lower the risk of violations.
- **Consistent governance:** Centralized controls enable uniform application of governance standards, even as environments scale across clouds and regions.
- **Reduced risk:** Enhanced visibility and control over data and user actions can minimize exposure to compliance breaches and unauthorized access.
- **Audit readiness:** Built-in reporting and activity tracking streamline preparation for regulatory audits and internal reviews.

Landscape challenges

Life-cycle management for large-scale, distributed environments remains a primary area for improvement for organizations looking to improve their IT systems, particularly in scenarios involving hundreds of clusters and complex infrastructure topologies. The need for simplicity and modularity in management tools is a recurring theme, as users continue to express a preference for interfaces that allow incremental feature adoption without unnecessary complexity.

Furthermore, for organizations evaluating unified management and hybrid multicloud solutions, budget constraints and the need to balance short-term operational costs with long-term value remain significant considerations. As licensing costs present ongoing challenges for budgeting and long-term planning, it highlights the importance of vendors like Nutanix to remain transparent and flexible with its pricing models.

Conclusion

Organizations seeking competitive advantage and operational efficiencies in the AI era must modernize their applications and infrastructure to support business goals. Performance improvements are, of course, a part of every new generation of technology, but "speeds and feeds" are not the whole story.

Getting value from data requires effective management tools, enterprisewide visibility, and data sovereignty — control over your most precious resource. Reducing complexity, increasing administrator and developer efficiency, better data security and protection, faster time to value, and lower total cost of ownership are added benefits, as well as positive business outcomes that support the bottom line.

Getting value from data requires effective management tools, enterprisewide visibility, and data sovereignty — control over your most precious resource.

Nutanix Central simplifies hybrid cloud data infrastructure across multiple environments — on premises, in dedicated and public clouds, and at the edge. This enables organizations to choose the best fit for their applications and associated data, which is critical to establishing data sovereignty, managing assets, and extracting value from data.

About the Analyst

Dave Pearson, *Group Vice President, Infrastructure Solutions*

Dave Pearson is group vice president within IDC's Worldwide Infrastructure Research organization and global research lead for the Storage and Converged Systems, Compute, Infrastructure Software, and Performance-Intensive Computing practices. He manages a team of analysts that cover these research domains, as well as Canadian and APAC research. For the storage and converged systems practice, Dave and his team provide global insights on storage, integrated, hyperconverged and composable infrastructure technology trends, vendor strategies, and market adoption. It includes storage for performance-intensive computing use cases like high-performance computing, artificial intelligence, and analytics. It also includes cloud-enabled infrastructure and infrastructure used for cloud deployments.

MESSAGE FROM THE SPONSOR

More information about how Nutanix can help organizations accelerate their digital sovereignty initiatives can be found at https://www.nutanix.com/solutions/digital-sovereignty. To experience the simplicity and enhanced observability of Nutanix Central, take a FREE Test Drive.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com