Red Hat and eXate facilitate cloud sovereignty compliance

Protecting critical national infrastructure

Overseeing critical national infrastructure has never been more complex or risky. Systems that manage national energy grids and telecommunications (telco) networks, as well as financial market infrastructure and public health services, are inextricably linked by an endless dynamic flow of data. While this interconnectivity inspires efficiency and innovation, it also exposes this infrastructure to unprecedented vulnerabilities. These services form the foundation of our national economy, and the integrity and sovereignty of these services are now paramount to national stability and prosperity.

Unfortunately, these challenges transcend existing, traditional data security. Safeguarding data is occurring increasingly in a world governed by strict sovereignty rules. The global environment is marked by geopolitical tensions and a proliferation of conflicting legal frameworks with data protection surpassing the technical task—becoming a matter of national security. Extraterritorial legal demands, foreign operational influence, and sophisticated cyber threats all pose existential risks to critical national infrastructure. A breach of sensitive data or an attack on the underlying systems would not only have catastrophic operational consequences, but can lead to the loss of public trust and severe financial penalties. Data sovereignty is undermined if the underlying technology is not protected. The challenge is verifying that the entire technology platform is clean from backdoors, vulnerabilities, or unwelcome influences.

Data is a dynamic asset that is created, processed, moved, and archived across multiple jurisdictions. A principal challenge is tracking and enforcing sovereignty rules on data streams as they move across borders—not just data at rest. Every component of data generates metadata, logs, and backups. Ensuring that this ancillary data also adheres to the same residency rules can be complicated because it may be processed or stored in a noncompliant location.

Traditional security controls are focused on the perimeter, such as firewalls, network, and access, but are insufficient for the dynamic movement of data around the world. The technological challenge is to shift to a data-centric security model where the protection (e.g., encryption, tokenization) travels with the data itself, regardless of its location or the application using it.

Facilitating data security and sovereignty with Red Hat and eXate

The strategic imperative for technology executives is clear, to continuously reconcile the promise of global agility with the nonnegotiable mandate of national sovereignty. The resilience of software supply chains and the integrity of sovereign controls are no longer separate technical considerations. They form the foundation of operational security and public trust, particularly for the infrastructure that powers national economies and societies. The collaboration between Red Hat and eXate allows organizations to build and deploy sovereign clouds that are not just compliant, but inherently autonomous and security-focused.

Red Hat cloud solutions have long been the gold standard for empowering customers with the freedom and choice of where to deploy critical services. By using Red Hat® Advanced Cluster Management for Kubernetes and Red Hat Advanced Cluster Security for Kubernetes, organizations gain unified visibility and proactive risk management across their cloud estate—fundamentally

f facebook.com/redhatinc
𝕏 @RedHat
in linkedin.com/company/red-hat

reducing the attack surface and fortifying their cloud defenses. These reliable and flexible solutions, with service interconnect capability, serve as the essential infrastructure for sovereign operations—giving control to place workloads and data where they must be to meet regulatory demands.

Building on this powerful foundation, eXate adds an important security layer that protects data as it moves. By integrating eXate's automated data classification, jurisdiction-aware policy enforcement, and real-time data protection into Red Hat solutions, we can eliminate the manual burden of cross-border compliance. This is a data-centric security model where protection travels with the data itself—ensuring that sensitive information is handled in accordance with local regulations, wherever it is located or however it moves. This functionality creates a verifiable chain of custody for every piece of sensitive data.

The joint initiative achieves a new level of uncompromising control over data, operations, and technology. By adding eXate's data-centric security, confidence is gained to accelerate innovation and mitigate risk in global expansion. Going beyond mandated adherence, eXate data security expands functionality by streamlining cloud operations and reducing costs. Together, Red Hat and eXate can help customers safeguard critical services, comply with national imperatives, and maintain absolute authority over every aspect of their cloud environment.

Comprehensive functionality, capability, and data security in a sovereign world

eXate's policy management, combined with its distributed data protection engine and suite of privacy enhancing techniques, delivers a unique approach toward comprehensive data shielding. In addition to encryption, eXate effectively addresses critical challenges related to meeting data residency, localization, and sovereignty requirements for data in motion, at rest, and in use.

eXate provides automated tools to detect and classify sensitive data across the entire technology estate. This helps organizations identify privacy and security risks and consistently apply appropriate data protection policies at a granular level.

Because data residency is a policy-driven requirement, eXate automatically enforces both the relevant policies and the appropriate privacy-enhancing techniques protecting sensitive data attributes subject to regulation. The decision-making process considers many factors, such as the location data may be stored and processed, access control, and usage.

Data localization, by contrast, is a regulatory concept that prohibits cross-border data transfers. eXate supports compliance with data localization requirements by ensuring that sensitive data is stored and processed exclusively within the specified jurisdiction.

Sensitive information is safeguarded locally using a token vault, while only nonsensitive data is permitted to flow to systems and users outside the jurisdiction. This approach allows global applications to operate smoothly across multiple regions without violating local data protection laws.

eXate also combines tokenization with distributed key management and jurisdiction-aware policies to handle situations where encrypted data is still classified as personal information (under certain regulations). By fragmenting ciphertext and tagging it with location and data-type metadata, eXate generates secure tokens stored centrally, maintaining both compliance and data utility.

Key sovereignty is an integral part of a tokenization approach, giving organizations exclusive control of their decryption keys rather than relying on cloud provider-managed hardware security modules (HSMs), which may place key control outside their jurisdiction. This approach ensures full authority over data access, storage, and processing, even in the face of external pressures.

Uncompromising operational control

Maintaining operational sovereignty begins with a single, auditable source of truth across your cloud environments. Red Hat Advanced Cluster Management provides an integrated dashboard that unifies the view across the whole Kubernetes fleet wherever they reside. This centralized visibility is a critical asset. It allows teams to monitor the health, resource inventory, and security posture from one location, proactively identifying configuration drift and potential vulnerabilities. Additionally, the central dashboard provides the essential foundation for operational control. It empowers organizations to enforce, verify, and scale cloud operations with confidence. Using this command-and-control capability is the first line of defense against both human error and malicious tampering, providing a transparent and auditable trail is required by national mandates.

Manual governance is a liability in a sovereign cloud environment. Red Hat Advanced Cluster Management elevates compliance from a reactive, labor-intensive task to a proactive, automated discipline. Its powerful policy engine allows teams to define security, compliance, and operational policies once and automatically enforces them across the full fleet of clusters. The ability to define these policies ensures a consistent security baseline and prevents misconfigurations that could expose data to a non-sovereign jurisdiction. For sovereign clouds, this is invaluable. Policies can be enforced to mandate the use of specific, trusted image registries. Policies can also enforce storage volume encryption with a customer-owned key management service and continuously scan for violations against national benchmarks using automated remediation capabilities.

True operational control requires the ability to make and enforce decisions about where and how applications run. Red Hat Advanced Cluster Management provides the granular control necessary to manage distributed infrastructure with precision. Its placement rules allow enforcement of data residency, ensuring that an application and its sensitive data are deployed only on clusters physically located within a designated sovereign environment. Furthermore, Red Hat Cluster Management provides full lifecycle cluster management from initial provisioning and scaling to non-disruptive upgrades. This capability establishes the ability to retain continuous control over the evolution of the software supply chain.

Achieving operational sovereignty requires organizations to have deep visibility and control over their cloud environments, making certain that critical workloads and data remain accessible, safeguarded, and compliant at all times. This includes the ability to audit and monitor operations, enforce policies, and respond swiftly to incidents or regulatory changes. Operational sovereignty is not just about meeting compliance requirements. It is necessary for reducing risk, enhancing agility, and maintaining trust in an era of rapidly evolving threats and regulations.

eXate plays a pivotal role in operational sovereignty by providing reliable policy enforcement that delivers fine-grained, attribute-level audit logs, capturing who accessed what data, when, how, and why. This level of transparency allows organizations to monitor and verify every data interaction, supporting both internal governance and external regulatory requirements. Real-time monitoring of data flows and policy violations provide proactive detection and rapid response to emerging issues, preventing operational failures before they escalate. By consistently applying data sovereignty policies across all environments and generating auditable logs, eXate empowers organizations to validate compliance and maintain operational trust with regulators and stakeholders.

Together, eXate and Red Hat provide a comprehensive foundation for operational sovereignty. By combining eXate's granular policy enforcement and audit capabilities with Red Hat's cloud-security posture management, organizations gain the visibility, control, and resilience needed to govern cloud operations with confidence. Governing with this level of confidence ensures that every aspect of their technology estate remains protected, compliant, and firmly under control.

Fortifying the sovereign cloud

Cloud sovereignty is essential to have full authority over your data, operations, and technology within a given jurisdiction. By unifying these components at the intersection of cross-border data protection, governance, and protection of critical national infrastructure, organizations can follow a straight path to security-focused, resilient, and transparent operations.

Codeveloped by Red Hat and eXate, the joint initiative addresses the growing challenges of protecting data across jurisdictions. The unified approach streamlines compliance across any environment by combining Red Hat cloud-security posture management and workload protections with eXate's data-protection capabilities. This partnership empowers organizations to maintain control of their cloud environments, meet regulatory requirements, and safeguard information through jurisdiction-aware data protection.

For more information

Visit the eXate solution page on the Red Hat Ecosystem Catalog to learn more about the partnership and how it can help you protect your organization.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

f facebook.com/redhatinc
𝕏 @RedHat
in linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com