Secure isolated recovery environments: Enabling smarter, faster recovery through isolation architecture

Executive summary

Organizations today face a rapidly escalating landscape of cyber threats, particularly ransomware and identity-based compromises, which impose significant financial and operational harm. The 2025 IBM Cost of a Data Breach Report highlights that credential-based intrusions remain the leading cause of breaches, with the global average breach cost rising to $4.44. Against this backdrop, traditional disaster recovery (DR) solutions—designed for availability rather than contamination prevention—are increasingly unable to ensure clean, trusted recovery in the wake of a major compromise.

A secure isolated recovery environment (SIRE) addresses this gap by creating a fully segregated, independently governed recovery environment designed to restore critical services without reintroducing compromised identities, systems or data. Unlike standard DR models, a SIRE is a last resort environment activated only after catastrophic cyber events.

This white paper explores why a SIRE has become a strategic necessity, the architectural and operational principles that define it and how cloud-based capabilities—including immutable backups, air gapped architectures and zero trust controls—enable rapid recovery. It also outlines a structured SIRE implementation framework, including governance, identity separation, recovery automation, testing cycles and operational guardrails.

Introduction

Cyberattacks targeting identity infrastructure, cloud workloads and business critical applications continue to increase in scale and sophistication. Ransomware and credential compromise remain the leading causes of high impact breaches, and organizations with distributed cloud footprints face an attack surface that expands faster than traditional defenses can keep pace.

While DR solutions are essential for availability, they are not designed to ensure trust—meaning that the systems being restored are free from compromise. SIRE, also referred to as a minimum viable environment (MVE), provides a secure, segregated environment that enables organizations to run periodic sanity testing and restore essential systems and data in the aftermath of a major cybersecurity event.

Implementing a SIRE is a proactive measure that safeguards resilience, minimizes downtime and reinforces confidence in your organization's ability to recover from severe disruptions.

Why a SIRE and why now?

Recent studies, such as the IBM Cost of a Data Breach Report, confirm that compromised credentials and email-based attacks remain the leading root cause of ransomware incidents, significantly elevating the risk of data loss and prolonged downtime. For instance, the average cost of a single data breach in 2025 is at $4.44 million.

As if the financial risks aren't enough, organizations need to be wary of the following challenges as well:

- Reinfection risk: DR restores often reintroduce compromised identities or dormant malware.
- Unknown compromise points: Detection often lags initial intrusion by days or weeks.
- Privilege escalation: Compromised identity stores require rebuilding authentication infrastructure.
- Cloud scale: Complex hybrid architectures make containment difficult.
- Insider threats: Privileged access can become an attack vector.

Suffice it to say, traditional recovery methods are increasingly unreliable. Therefore, organizations are advised to implement a SIRE, which offers strategic advantages by enabling:

- Rapid, secure restoration of critical systems and data
- Protection against reinfection during recovery
- Enhanced resilience in the face of evolving cyber threats

What a SIRE is and isn't

A SIRE is a purpose-built environment designed to enable recovery without the risk of contamination from the primary environment. At its core, it is a standalone virtual network, completely isolated and provisioned only when needed. However, successful implementation requires careful planning—not just in how it's built, but in how it's used.

It's important to note that a SIRE is not a traditional DR solution in an active/passive configuration, whether within the same region or across regions. Such scenarios demand reliability considerations based on workload criticality and acceptable downtime.

Instead, a SIRE serves as a last resort recovery option—a secure environment to restore operations following a catastrophic event in which the primary environment has been compromised. It is not designed for day-to-day operations. Although critical services can be replicated to an air gapped virtual network, organizations must still be able to identify the precise point of compromise—often taking days or even weeks after the initial incident.

A quick comparison: DR vs. SIRE

Dimension	Traditional DR (active/passive)	SIRE
Primary purpose	Business continuity and rapid failover	Last resort recovery after catastrophic compromise
Usage pattern	Warm/hot and ready for failover	Provisioned only when needed—not for day-to-day operations
Architecture	Continuous replica of production (same or cross region)	Standalone, air gapped virtual network that is completely isolated
Isolation level	Connected/peered by design	Strictly isolated to avoid contamination from primary
Data source	Ongoing replication/snapshots	Replicated backups to an air gapped store
Intended workloads	Critical workloads requiring continuity	Minimal critical services to restore core operations safely

Architectural principles of a SIRE

The foundational principle behind a SIRE is separation. The environment must not share any critical infrastructure, identity, network, hypervisors, storage or other services with the production environment. In most cases, this means:

- Dedicated platforms (on-premises or cloud-based) and tightly controlled virtualization platforms
- No access points from production to the SIRE network
- Physical air gaps or highly restricted one-way replication mechanisms
- Independent DNS, DHCP and identity services

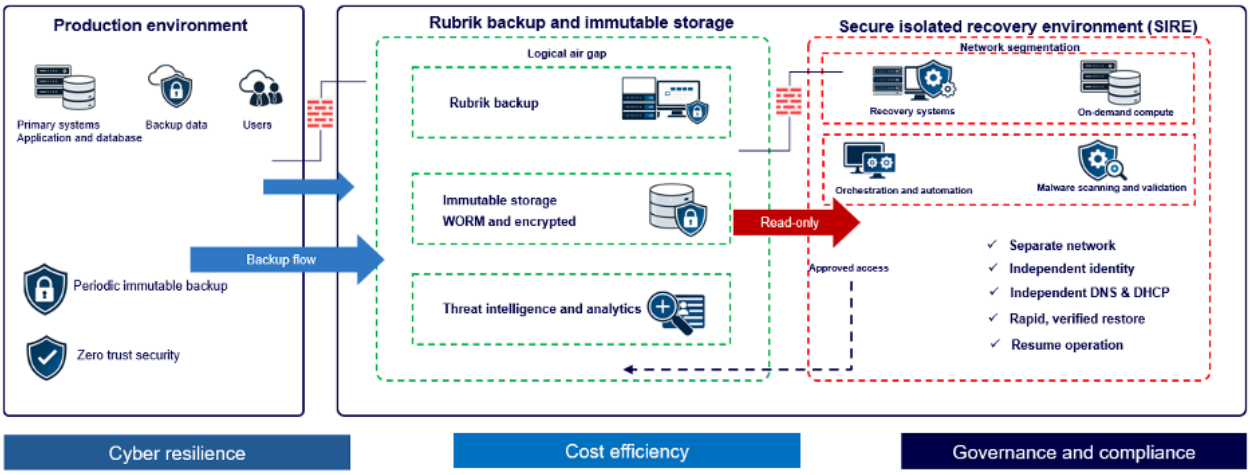


Figure illustrates the permitted flows into and within a SIRE

Design principles of a SIRE

The effectiveness of a SIRE is grounded in adherence to fundamental design principles that prioritize security, isolation and automated recovery.

Immutable recovery foundation

- Ensure recovery data is immutable, protected against alteration or deletion by malicious actors, forming an unassailable baseline for restoration.
- Implement write once, read many (WORM) policies along with robust versioning and retention strategies to maintain a verifiable history of recoverable data.
- Leverage infrastructure as code (IaC) for consistent, repeatable deployments of both recovery and production environments, preserving the exact state at the time of the incident and enabling rapid, error-free reconstruction.

Zero trust security model

- Adopt a "never trust, always verify" posture, enforcing continuous authentication and authorization for all access attempts, regardless of origin.
- Apply the principle of least privilege access through granular role-based access control (RBAC) with just-in-time (JIT) elevation for critical tasks.
- Maintain continuous monitoring and threat detection using integrated security information and event management (SIEM) and cloud security posture management (CSPM) tools.
- Access controls: Implement JIT access, privileged access management (PAM) and conditional access policies to reduce the overall attack surface
- Infrastructure isolation: Use dedicated subscriptions and resource groups to isolate workloads—simplifying management and strengthening security boundaries.
- Physical isolation: Deploy workloads across availability zones to strengthen resilience against physical failures and localized incidents, while enabling proactive quota and capacity planning for recovery operations.

Isolation

- Network isolation: Deploy dedicated virtual networks with strictly controlled one-way connectivity. This often involves high-level architectural patterns such as utilizing an isolated region dedicated solely to recovery or implementing a hub-and-spoke model where the SIRE acts as a completely separate, disconnected spoke to prevent lateral movement and contamination from the primary environment.
- Data isolation: Use separate storage accounts with immutable policies and potentially separate encryption keys to safeguard backup integrity.
- Identity isolation: Enforce strict RBAC boundaries and establish cloud-only accounts where possible, ensuring clear separation across data, workload and management plans to minimize the blast radius from compromised credentials.

Automated recovery orchestration

- Use automated failover and recovery capabilities provided by modern backup and DR solutions (e.g., Rubrik, Commvault, Cohesity, Azure Backup, AWS Backup, Veeam) to restore virtual machines, applications and critical workloads quickly and securely.

- Centralize oversight through a unified management platform, providing end-to-end visibility and governance across backup, recovery and compliance operations.
- Implement recovery automation using APIs, scripts and orchestration workflows provided by these tools to ensure repeatability and accelerated restoration during incidents.

Air gapped backup options

Air gapped backups provide an essential safeguard by isolating critical data from online networks. This separation ensures that information remains inaccessible to cybercriminals and malware, which typically exploit internet-based channels. By implementing air gapped solutions, organizations add a robust layer of protection, significantly increasing their ability to withstand data breaches and other catastrophic events.

Air gapped backups operate by maintaining a storage system that is either physically or logically separated from the primary environment. The frequency of data transfers and updates depends on business requirements, such as the need for real-time recovery and the criticality of maintaining current data.

Organizations typically adopt one of the three following air gapping strategies:

1. **Physical air gaps**: The traditional approach involves storing backups in a physically isolated environment, disconnected from any network that could enable external access. This can include removable media such as tapes or external drives, as well as specialized hardware with built-in network isolation. Modern solutions often automate backup processes, reducing manual effort and operational risk.
2. **Logical air gaps:** Logical air gaps create virtual barriers through software and network segmentation, even when storage devices remain physically connected. This method prevents internet-based access, offering strong protection without the logistical complexity of physical isolation.
3. **Cloud air gaps:** Cloud-based air gaps extend this concept to infrastructure managed by cloud providers, enabling regional or zone-level segregation within provider-controlled environments. This approach delivers enhanced scalability and resilience while eliminating the need for on-premises resources.

Air gapped backup options: Advantages and disadvantages

Models	Advantages	Disadvantages
Physical air gap	• Strongest isolation • Naturally immune • Strict regulatory	• Slower recovery time objective(RTO) • Human/process risk • Longer recovery point objective (RPO)
Logical air gap	• Faster RTO • Operationally efficient • SIRE clean-room restore	• Misconfiguration risk • Control-plane compromise • Copy corruption
Cloud air gap	• Elastic and scalable • Rapid provisioning • Multiple isolation layers	• Cross-region egress costs/latency • Must ensure vault hardening • Compliance requirements

Getting started with a SIRE implementation

Implementing a SIRE requires a structured and phased approach, involving cross-functional collaboration between security, infrastructure, identity management and business continuity teams. The following steps outline a standardized implementation framework that organizations can use to build a reliable, cloud-ready SIRE capability, from foundational.

Step 1. Establish dedicated resources

This foundational step involves creating completely separate cloud subscriptions and resource groups specifically for the SIRE, ensuring rigorous isolation from all existing production environments. It also includes implementing regional or zonal isolation strategies to enhance overall resiliency and security against localized outages.

Step 2. Deploy an isolated network architecture

Designing and implementing a standalone virtual network for the SIRE is crucial, with strict directives against peering connections to existing production networks. This step also requires integrating a robust firewall or network virtual appliance (NVA) at all egress points to control outbound traffic, enforce security policies and ensure comprehensive logging for auditing and threat detection.

Step 3. Enforce governance and security controls

Establishing stringent policy-driven controls is paramount. This includes explicitly blocking virtual network peering to maintain isolation, mandating the use of private endpoints for all storage and key vault services to minimize public exposure and applying mandatory tagging for all SIRE resources to ensure compliance, proper cost allocation and enhanced visibility.

Step 4. Provision automation and management tools

To streamline SIRE infrastructure operations and ensure consistency, it is essential to deploy automation frameworks and tools. This involves leveraging IaC pipelines, scripting platforms and configuration management solutions to automate the provisioning, configuration and ongoing management of the SIRE environment, thereby reducing manual effort and accelerating recovery.

Step 5. Secure administrative access

Implementing hardened administrative access mechanisms is vital for protecting the SIRE. This typically involves deploying bastion security services for all privileged activities within the SIRE environment. Furthermore, ensuring session recording and continuous monitoring for all administrative sessions is critical for tracking actions, auditing and detecting suspicious behavior.

Step 6. Implement robust identity and access management (IAM)

This step focuses on creating SIRE-specific RBAC groups and custom roles, precisely scoped to the SIRE resource groups to enforce the principle of least privilege. Just as critical are configuring privileged identity management (PIM) with JIT access for elevated permissions and establishing secure "break glass" accounts for emergency scenarios.

Step 7. Configure immutable backup strategy

Developing and configuring a comprehensive immutable backup strategy is fundamental for data integrity. This involves enabling WORM policies for all critical recovery data, regularly validating restore points to ensure their viability and thoroughly documenting all restore sources and associated credentials to facilitate rapid and reliable recovery when needed.

Step 8. Define recovery prioritization and testing

A clear understanding of recovery priorities is essential. This step involves developing a criticality matrix to establish the precise restore order for applications and data tiers. Crucially, it mandates scheduling and executing quarterly SIRE restore tests and full-scale recovery drills to continuously validate readiness, identify any gaps and ensure the operational effectiveness of the recovery plan.

Step 9. Automate recovery operations

Leveraging IaC runbooks (e.g., Terraform, Ansible CLI) to automate critical recovery operations significantly accelerates restoration during an incident. This includes automating the provisioning of SIRE infrastructure, the execution of restores and the swift isolation of compromised links (e.g., disabling VPNs or peering) to prevent further damage.

Best practices to support SIRE sustainability

Sustaining SIRE integrity requires a balance of proactive operational discipline and repeated, scenario-based recovery validation. The following best practices outline the essential activities that keep a SIRE resilient and fully prepared to support clean recovery during major cyber events.

Operational and recovery assurance controls

Recovery readiness KPIs	The SIRE should be continuously validated using recovery readiness indicators such as RTO, RPO, identity and network success rates and immutability.
Operational guardrails	To preserve the integrity of the isolated recovery environment, operational guardrails such as policy-driven prevention, restricted administrative actions and enforced change control should be applied.
Quarantine rules	Restored workloads should initially run in a quarantined state within the isolated environment, with no outbound connectivity, malware scanning and manual or automated approval gates.

Recovery workflow

A SIRE only delivers value when it enables rapid restoration under pressure. This requires comprehensive planning and rigorous testing to ensure full recovery of core services. A standard SIRE implementation includes:

- Predefined templates for rebuilding domain controllers, authentication services and critical applications
- Automated provisioning of virtual machines or containers within the SIRE/MVE
- Immediate access to DR runbooks for incident responders
- Regularly scheduled exercises, including tabletop simulations and full-scale recovery drills (e.g., quarterly or biannually)

Strategic planning and governance

- Align organizational goals and KPIs to create SIRE blueprints with clear roles, architecture and governance controls
- Define the scope of the MVE
- Map application and infrastructure dependencies
- Identify critical business services and applications

Factory setup and automation

- Establish pods, SLAs and onboarding playbooks while integrating CI/CD pipelines and automation tools for efficiency
- Define cyber recovery RTO and RPO for the MVE

Environment provisioning and integration

- Provision cloud or on-premises infrastructure with secure networking to support development and deployment activities
- Decide on operating model—persistent vs. on-demand infrastructure

Testing, deployment and continuous improvement

- Conduct comprehensive testing, manage releases with risk mitigation and drive ongoing improvements using site reliability engineering (SRE) and AIOps

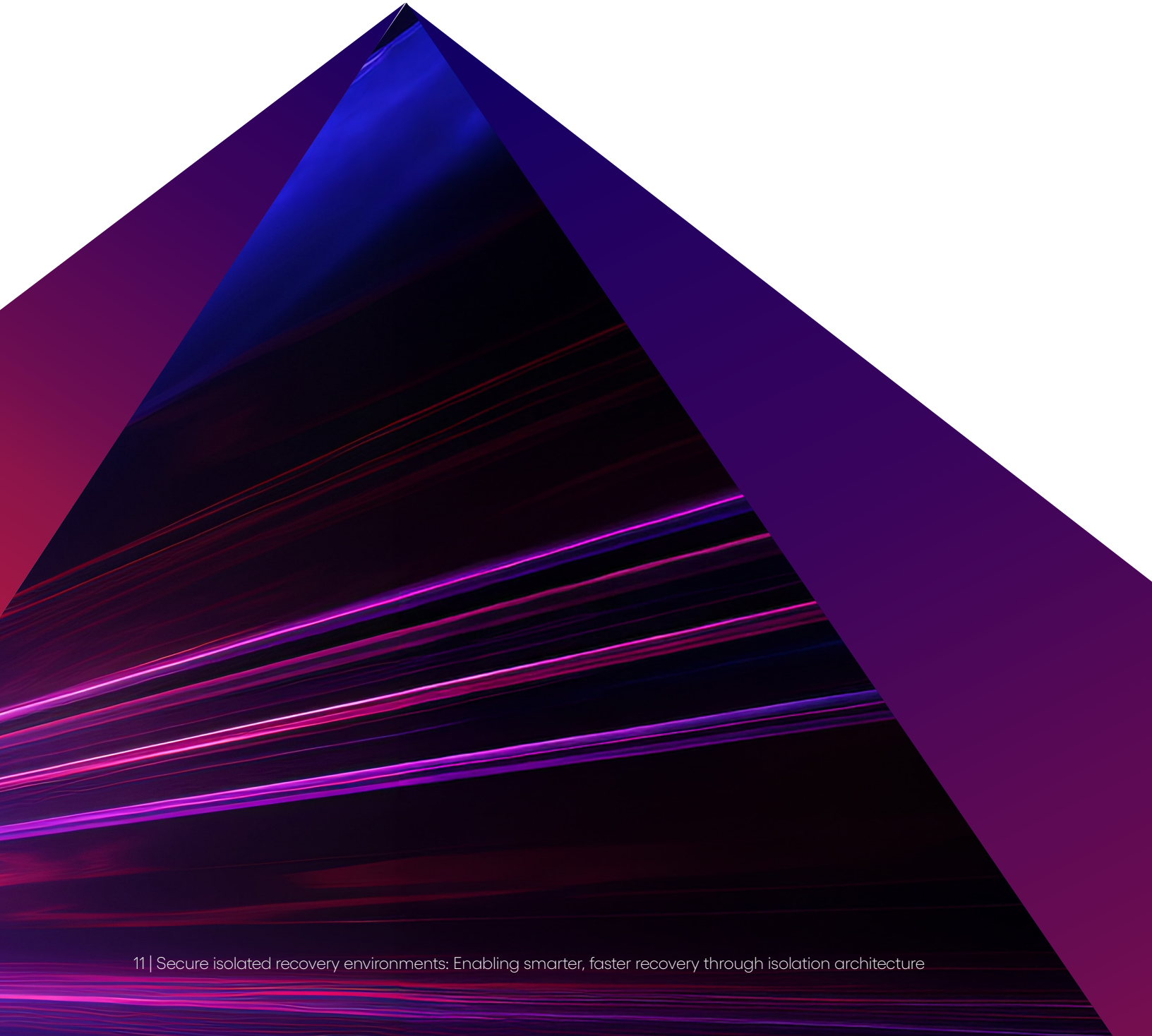
Choosing the right SIRE deployment model

The right model depends on your environment, compliance obligations and team maturity.

Model	Advantages	Challenges	Cost considerations	Compliance factors
On-premises	• Full control • Better for air gapped environments • Strict regulatory adherence	• Higher CapEx • Longer provisioning time • Less flexibility • Requires significant in-house expertise	• High initial capital expenditure (hardware, infrastructure, facility costs) • Ongoing operational costs for power, cooling and maintenance	Can simplify adherence to stringent on-premises data residency and sovereignty requirements; direct control over physical security and data governance.
Cloud	• Faster provisioning • Built-in automation • Easier to test • Elastic scalability • Reduced physical infrastructure burden	• Requires strong cloud security maturity and IAM separation • Potential for vendor lock-in • Data egress costs	• Operational expenditure (OpEx) model • Costs scale with usage • Potential for significant data transfer (egress) fees • Subscription-based pricing	Cloud provider certifications and the shared responsibility model need careful evaluation for regulations like GDPR, HIPAA, SOX, PCI DSS; ensuring data residency can be complex.
Hybrid	• Combines local speed with cloud resilience • Ideal for large organizations with diverse and critical workloads • Leverages existing investments	• More complex design and integration • Requires secure identity split and robust replication paths • Consistent management across environments	• Blended CapEx and OpEx • Allows optimization of costs by leveraging existing on-premises assets while utilizing cloud for scalable resilience • Can reduce overall egress costs	Requires careful mapping of data flows and storage locations to comply with diverse regulatory mandates across different environments; increased complexity in audit trails.

Protect your business

A SIRE is a critical pillar of an enterprise's overall resilience strategy. It is crucial to understand that the SIRE's purpose is singular and profound—to serve as a last resort recovery option following a catastrophic cyber event. Strategic takeaways include recognizing that using the SIRE beyond cyber recovery for routine DR testing, high availability or daily operations fundamentally compromises its isolation and trust model, thereby eroding its core value. Furthermore, assuming that hosting data in the cloud inherently provides isolation is a potentially harmful misconception. True isolation demands intentional, meticulous configuration and dedicated architectural design. Finally, effective SIRE implementation must extend beyond external threats to proactively mitigate potential insider threats and sabotage, ensuring comprehensive protection.



Cognizant's approach

Organizations must proactively assess their current recovery capabilities and invest in a well-designed, rigorously tested SIRE. Engaging with cybersecurity and cloud architecture experts is paramount to tailor a SIRE solution that aligns with your unique risk posture, compliance obligations and business continuity objectives Cognizant approaches SIRE as a service through a factory-based, repeatable delivery model. We have prebuilt blueprints and IaC templates to accelerate the deployments of SIRE using standardized patterns that can be tailored to your business, risk posture and cloud maturity.

SIRE readiness checklist

Before beginning your SIRE implementation, ensure your organization is prepared by using our SIRE readiness checklist.

- Have we clearly defined the scope and critical assets to be protected by the SIRE?
- Is our SIRE architected with full network, data and identity isolation from production environments?
- Are our backup data sets immutable and regularly validated for restorability?
- Have we established a robust identity and access management (IAM) framework, including JIT access and "break-glass" procedures for the SIRE?
- Are recovery workflows automated and regularly tested through full-scale drills?
- Have we addressed potential insider threats in the SIRE's design and access controls?

For more information about how we can help, connect with our security experts at BusinessResilience@cognizant.com.

WF 4420056