Mandiant

White paper

Cyber Resiliency Through Cloud Isolated Recovery Environments

A White Paper on Improving Time to Recovery from Cyber Events

Introduction: The Growing Need for Cyber Resiliency

In today's digital landscape, organizations face an ever-increasing threat of cyberattacks, including destructive events like ransomware. The impact of these incidents extends beyond technical disruptions, leading to significant business downtime and substantial financial losses due to interrupted operations. A traditional disaster recovery approach, focused primarily on technical restoration, often falls short in addressing the complexities of recovering from a cyber event, particularly the need to re-establish trust with third parties. This white paper explores the concept of proactively establishing a cloud isolated recovery environment (CIRE) as a strategy for enhancing cyber resiliency and minimizing the impact of cyber incidents.

The Limitations of Traditional Recovery and the Rise of Isolated Recovery Environments

The recovery of a large enterprise following a cyber event is not a simple on-off process. Experience has shown that there are three primary types of recovery: technical recovery, involving the restoration of applications, clients, and servers using traditional recovery or rebuild methodologies; business or operational recovery, which entails restarting business processes and understanding the interdependencies of restored systems and data flows; and recovery of trust with vendors, partners, and other third parties, which entails demonstrating that the recovered environment is reliable, secured and safe for use.

A significant challenge arises immediately after a cyber event as external partners often disconnect from the affected organization's environment to protect themselves. A lack of a "gold standard" for reconnection criteria makes this process lengthy and difficult. The victim organization may need to provide assurances of a secure and sound environment that may be difficult to deliver in a short timeframe.

To address these challenges, the proactive establishment of a cloud isolated recovery environment (CIRE) has emerged as a crucial strategy. This approach involves creating an isolated environment with pre-defined security controls, allowing for rapid recovery of critical business functions and a faster re-establishment of trust with external stakeholders, helping to mitigate the cost and impact of a cyber incident.

Key Benefits of a Cloud Isolated Recovery Environment

Establishing a CIRE offers several key benefits:

- **Reduced Downtime and Financial Impact**
  One of the most significant costs of a destructive cyberattack is business disruption and revenue loss. By enabling faster recovery of critical operations, a CIRE can significantly reduce this downtime and minimize financial impact in situations where data recovery or failover data centers are also impacted by a cyber event.
- **Accelerated Recovery of Trust**
  A preconfigured and secured CIRE, potentially validated by a trusted third party, can drastically reduce the time needed to convince third parties that it is safe to reconnect. The ability to demonstrate a secure recovery environment can often provide the necessary assurances.
- **Focus on the Minimal Viable Business**
  A CIRE strategy necessitates identifying the minimal viable business – the most critical parts of an organization's operations. This allows for a prioritized recovery of essential functions, enabling the business to resume critical activities even as a forensic investigation of the incident is ongoing.
- **Enhanced Security Controls**
  A CIRE provides a unique opportunity to implement stronger security controls that might be operationally burdensome in a normal production or disaster recovery environment but are acceptable during the immediate recovery phase. This includes enhanced protections, telemetry, and detection capabilities.
- **Practiced Recovery Processes**
  Regularly rehydrating, testing, and validating the CIRE allows organizations to practice their operational recovery processes, ensuring they are effective and successful during a real incident.
- **Improved Ability to Demonstrate a Compromise-Free Environment**
  A strong security baseline and the ability to monitor the CIRE for indicators of compromise (IoCs) enables organizations to demonstrate that the recovered workloads are secure. Using backup and recovery partners with the capability to scan backups for IoCs can further accelerate this process.
- **Agility and Efficiency of Cloud**
  Cloud platforms such as Google Cloud offer scalability, global infrastructure reach, flexible pay-as-you-go pricing, and comprehensive suite of technologies, enabling organizations to build robust and isolated recovery environments.

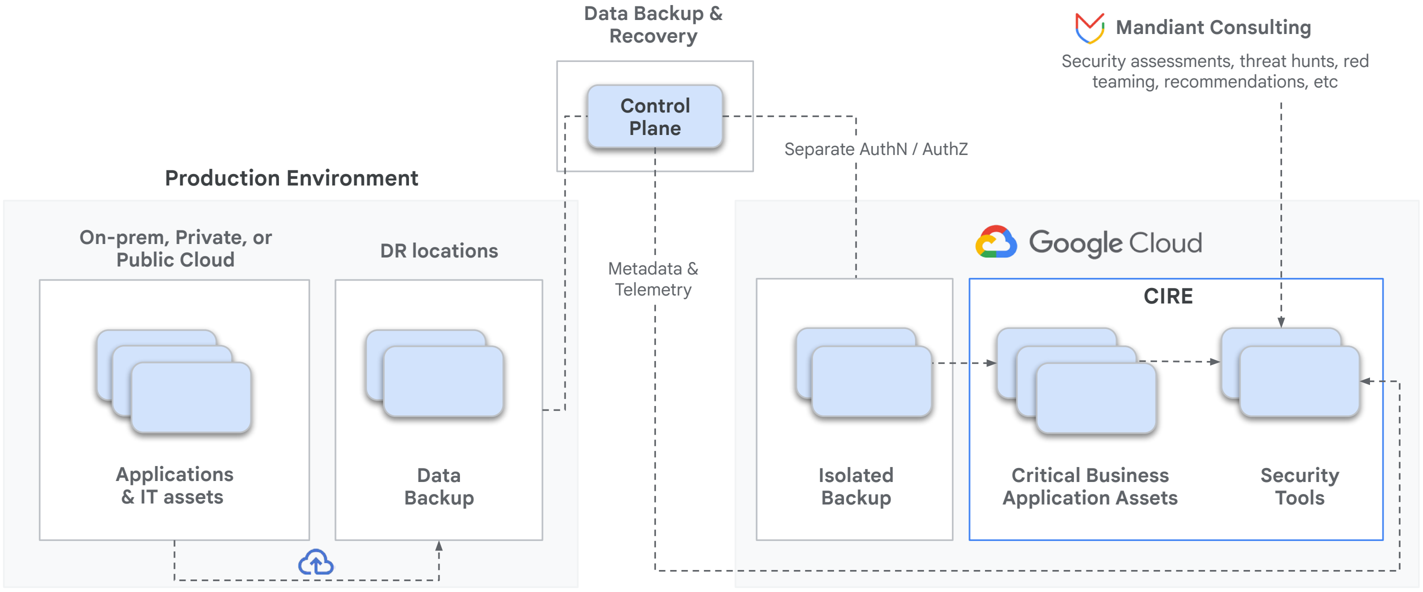

Figure 1: Conceptual design diagram of a Cloud Isolated Recovery Environment (CIRE).

Building and Maintaining a Cloud Isolated Recovery Environment: Key Considerations

Establishing and maintaining an effective CIRE requires careful consideration of several technical and operational aspects:

- **Platform Isolation and Identity Segregation**
  The CIRE should be completely isolated from the production environment and use a separate identity and control plane to prevent the propagation of security issues.
- **Independent Security Control Management**
  Security controls safeguarding the CIRE must be managed from within the isolated environment and have no dependencies on production systems to maintain proper isolation, in the event of a cyber event in the production environment.
- **Independent Administrative Capabilities**
  All administrative tasks required for management of the CIRE, restoration and recovery of systems should be possible with no dependencies on production systems.
- **Infrastructure Services**
  Organizations must identify and potentially stage critical infrastructure services (e.g., DNS, network routing, VPN, MFA) required for applications to function in the CIRE.

- **Essential Security Tools**
  Implementing core security tools is crucial for establishing trust in the CIRE. These typically include Endpoint Detection and Response (EDR), Cloud-Native Application Protection Platform (CNAPP), and Log Aggregation/SIEM/SOAR solutions. Network traffic visibility tools (e.g., DNS, NetFlow) are also beneficial for monitoring and inspecting outbound communications.
- **Backup and Recovery Solutions**
  Selecting a backup and recovery partner with capabilities such as looking into backups for IoCs can significantly expedite the recovery and validation process.

Key Stakeholders

The decision to proactively establish a cloud isolated recovery environment requires the involvement of several key stakeholders:

- **Technical Infrastructure Teams:**
  Responsible for the underlying infrastructure of the CIRE (e.g., cloud providers like Google Cloud).
- **Technical Application Teams**
  Responsible for understanding the dependencies of key applications that will be hosted in the CIRE.
- **Backup and Recovery Providers**
  Responsible for enabling the hydration and recovery of resources into the CIRE.
- **Security Teams**
  Responsible for defining and implementing the security architecture, controls, and protections within the CIRE, and ensuring a strong security baseline.
- **Business Leadership**
  Responsible for identifying what constitutes a minimal viable business and helping to establish cyber event specific RPO and RTO objectives.
- **Contractual Compliance**
  Responsible for identifying if your organization has any contractual obligations associated with disaster recovery.
- **External Partners (Indirectly)**
  While not directly involved in the decision-making process, the needs and requirements of key partners for re-establishing trust are a critical consideration.
- **Incident Response Teams**
  Whether conducted within the organization or conducted by an external forensic partner, it’s critical to ensure your investigative team is familiar with the CIRE and able to perform a successful investigation.

Validating the Effectiveness of the Isolated Recovery Environment

To ensure the CIRE's effectiveness, regular validation by a trusted third party security team is essential:

- **Control Validation**
  Verify that the controls implemented in the CIRE align with the intended reference architecture and are suitably designed.
- **Effectiveness Testing**
  Conduct regular penetration testing and/or red teaming exercises to assess the effectiveness of the implemented security controls.
- **Security Validation and Threat Hunting**
  Regularly test and validate the security telemetry, tools, and visibility within the CIRE to ensure they can be leveraged for incident response and threat hunting activities and that the CIRE remains secure.
- **Threat Intelligence Integration**
  Stay informed about the latest threat actor tactics and ensure the CIRE's defenses are aligned to address relevant threats. Many backup and recovery providers can also use threat intelligence feeds to search your backup data for known-bad IOCs.

Target Businesses

While enhancing cyber resiliency is important for all organizations, certain types of businesses stand to benefit most significantly from implementing a CIRE:

- Businesses that are heavily reliant on third parties, including payment processors, remote workers, third-party labor sources, and mission critical SaaS platforms.
- Industries that cannot tolerate extended downtime, such as globally significant banks, healthcare organizations, life/safety systems, and manufacturing companies.

Conclusion

Proactively establishing a cloud isolated recovery environment represents a paradigm shift in how organizations approach cyber resiliency. By focusing on rapid recovery of critical business functions, enhanced security controls, and the ability to quickly recover trust, a CIRE significantly strengthens an organization's ability to weather destructive cyber events. Embracing this strategy is crucial for minimizing financial losses, maintaining business continuity, and ensuring long-term operational stability in an increasingly complex threat landscape.

How Mandiant and Partners Can Help

Mandiant, in partnership with data backup and recovery providers, empowers organizations to build, test, and validate CIREs for critical applications on Google Cloud. Coupled with periodic security posture assessments and expert incident response services, this approach ensures businesses can swiftly and confidently restore operations, safeguarding customer trust and minimizing the impact of cyber incidents. By embracing CIRE, organizations fortify their defenses, ensuring they are prepared to navigate the complexities of the modern threat landscape.

Mandiant Consulting

Mandiant assists customers with security architecture, assessment, and validation of the recovery environment before, during, and after an incident. With Mandiant as a trusted security advisor, customers have an advantage in rebuilding trust after a cyber incident.

Services include the following:

- **Validate Cloud Isolated Recovery Environment (CIRE) Design**
  Guidance and validation of design decisions for the customer's CIRE:
  - Provides a reference architecture to deploy an isolated and secure cloud environment that can be used to create a replica of business critical applications in Google Cloud, leveraging partners' backup solutions
  - Provides high level guidance on reference architecture implementation
  - Validates the design choices and security architecture for the customer CIRE.
- **Security Assessments and Threat Hunting**
  Periodic security assessment of CIRE in Google Cloud. Every quarter, Mandiant will engage with the customer to deliver the following:
  - **Validate Controls**
    Configuration and architecture reviews to ensure controls align with the reference architecture.
  - **Validate Telemetry / Detection Capabilities**
    Targeted threat hunts to identify evidence of attacker activity and validate the effectiveness of CIRE.

  - **Penetration Testing / Red Teaming**
    Test security posture of the CIRE through targeted penetration testing and/or red team activities.
  - **Threat Intel Briefings**
    Provide tailored insights into relevant threats.
- **Incident Response and Recovery**
  At time of activation of CIRE, Mandiant does the following:
  - Provide customer and restoration team with guidance on execution of recovery playbooks considering the incident realities and attacker tactics, techniques, and procedures.
  - Perform security posture assessments and targeted threat hunting in the CIRE.
  - Conduct Incident Response activities as needed.
  - Provide security assessment reports if required.

About our Partners

Cohesity

Cohesity is a leader in AI-powered data security and management. We make it easy to secure, protect, manage, and get value from data — across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring malicious behavior, and rapid recovery at scale. Cohesity is a Google Cloud partner. The two companies are partnering to develop solutions AI-powered data security and insights for our joint customers. Learn more about our joint solutions here.

Rubrik

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

About Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated, and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

Make Google part of your security team. Contact Google Cloud Security.

Google Cloud

For more information visit cloud.google.com