AHEAD

CYBER RESILIENCE:

A Guide to Building an Effective Cyber Vault to *Protect Critical Data*

How AHEAD helps enterprises build cyber vaults to ensure *operational cyber resilience*

Cyber threats are everywhere and rapidly growing as organizations increasingly rely on data and digital services to maintain business operations. The latest cyber attacks are more sophisticated and more costly than ever, highlighting the need for enterprises to modernize their cybersecurity and cyber recovery strategies.

An effective cyber resilience strategy needs to combine both data protection and cyber recovery components to overcome data breaches and cyber attacks if they do occur. This means today's data-driven organizations should consider enhancing the maturity of their cyber vaults to restore operations during attacks and protect recovery data if an incident occurs.

It's important to note that an immutable backup is not the point of an effective cyber vault – the point is the ability to recover business-critical functions as quickly as possible. All technical aspects of a cyber vault should be assessed by the ability to bring core applications online in a known good environment with isolated hardware, where you can validate the integrity of your data and ultimately reduce overall recovery times. The design of a cyber vault is determined by what data is being protected, and how. For AHEAD, cyber vault designs account for patching, management, monitoring, and access controls that are driven by an in-depth business impact analysis.

In this guide, we'll discuss the need for cyber vaults in today's data driven business landscape, and the key considerations for designing, implementing, and operating cyber vaults and cleanrooms.

Why Enterprises Need Cyber Vaults

Most enterprises have disaster recovery plans in place, which usually includes backups for restoring data that has been encrypted, corrupted, or deleted. However, this backup infrastructure is often targeted by malicious actors to prevent victims from restoring operations during an attack.

The greater prevalence of more sophisticated threats means existing disaster recovery backup infrastructure is not sufficient for recovering from ransomware and other cyber attacks. Modern enterprises need to create a dedicated cyber vault or isolated recovery environment (IRE) that stores a copy of critical data and is hardened against attacks.

Cyber vaults are isolated and immutable environments — sometimes even air gapped or physically segregated — that are protected against ransomware and other malware. Cleanrooms are additional components used to recover applications and conduct forensic analysis on malware to recover from a cyber attack. An effective cyber recovery solution often includes both cyber vaults and cleanrooms for the rapid recovery of critical data and applications. It is possible that multiple restores are required to identify a successful recovery point and having the clean room allows that process to be expedited.

Designing and Implementing a Cyber Vault

Here are some key steps for designing and implementing an effective cyber vault.

1 IDENTIFY CRITICAL DATA & APPLICATIONS

Before creating a cyber vault solution, it's crucial to understand which data and applications should be stored and protected in the vault. This requires in-depth analysis to determine the components most critical to rapidly restore business operations in the event of an attack.

Before any business applications can be considered, infrastructure applications which are core to standing up business services must be restored!

Evaluating the potential business impact of different files and workloads is the key to designing appropriately sized and cost-effective vaults and cleanrooms. The more data and workloads that are included in the cyber recovery plan, the more complicated and costly the solution will become.

2 EVALUATE CYBER VAULT SOLUTIONS

There are many cyber vault technologies on the market, so it's important to carefully evaluate potential solutions to ensure they meet specific requirements. Some of the leading cyber vault solutions include:

rubrik

Rubrik Secure Vault offers enterprises immutability on first backup, intelligent data locks, retention locks, access controls, an air gap, and encryption to ensure data integrity and availability. Rubrik also helps enterprises easily identify clean recovery points to quickly recover to an IRE, cleanroom, or back to the production environment.

DELL Technologies TITANIUM BLACK PARTNER

Dell PowerProtect Cyber Recovery allows organizations to create immutable backups and store them in an isolated location on-premises or in multiple cloud environments. CyberSense for PowerProtect is an additional layer of support that scans the data within the cyber recovery vault for anomalies and uses machine learning for threat detection.

Commvault

Commvault Cloud Backup & Recovery enables secure and rapid recovery of data and workloads with flexible backups. In addition, Air Gap Protect enhances cyber protection of backups with air gapped, immutable cloud storage and Cleanroom Recovery provides a secure environment for rapid and safe recoveries.

COHESITY

Cohesity FortKnox provides ransomware resilience with highly secure, SaaS-based cyber vaulting. Organizations can simplify the operations and lower the costs of implementing a secure cyber recovery solution with immutable copies of data in a Cohesity-managed cloud vault.

3 CHOOSE A SUITABLE ARCHITECTURE

Along with the vault technology itself, it's important to design appropriate supporting infrastructure. Although a logically isolated cyber vault in the cloud might be faster and easier to implement, a physically isolated and air gapped cyber vault deployed on-premises will be inherently more secure. Organizations will need to strike their own balance between ease of use, cost, security, and other factors.

The purpose of the vault, though, is not backup, it is recovery. All aspects of it must be examined with the lens of how fast recovery can occur and if it's appropriate for the Tier 0 and Tier One applications under consideration.

The supporting architecture also needs enhanced security protections and secure configurations for the cyber vault to be effective. For example, critical security measures for cyber vault environments include separated identity and access management (IAM), privileged access management (PAM), and remote access design to prevent malicious actors from impacting recovery operations.

4 ESTABLISH OPERATIONAL PROCESSES

Implementing a technology stack is not enough to maximize the value of a cyber vault solution. There also needs to be operational processes in place to prepare for a cyber event, including integration with incident response processes to ensure the vault is utilized effectively during a cyber attack.

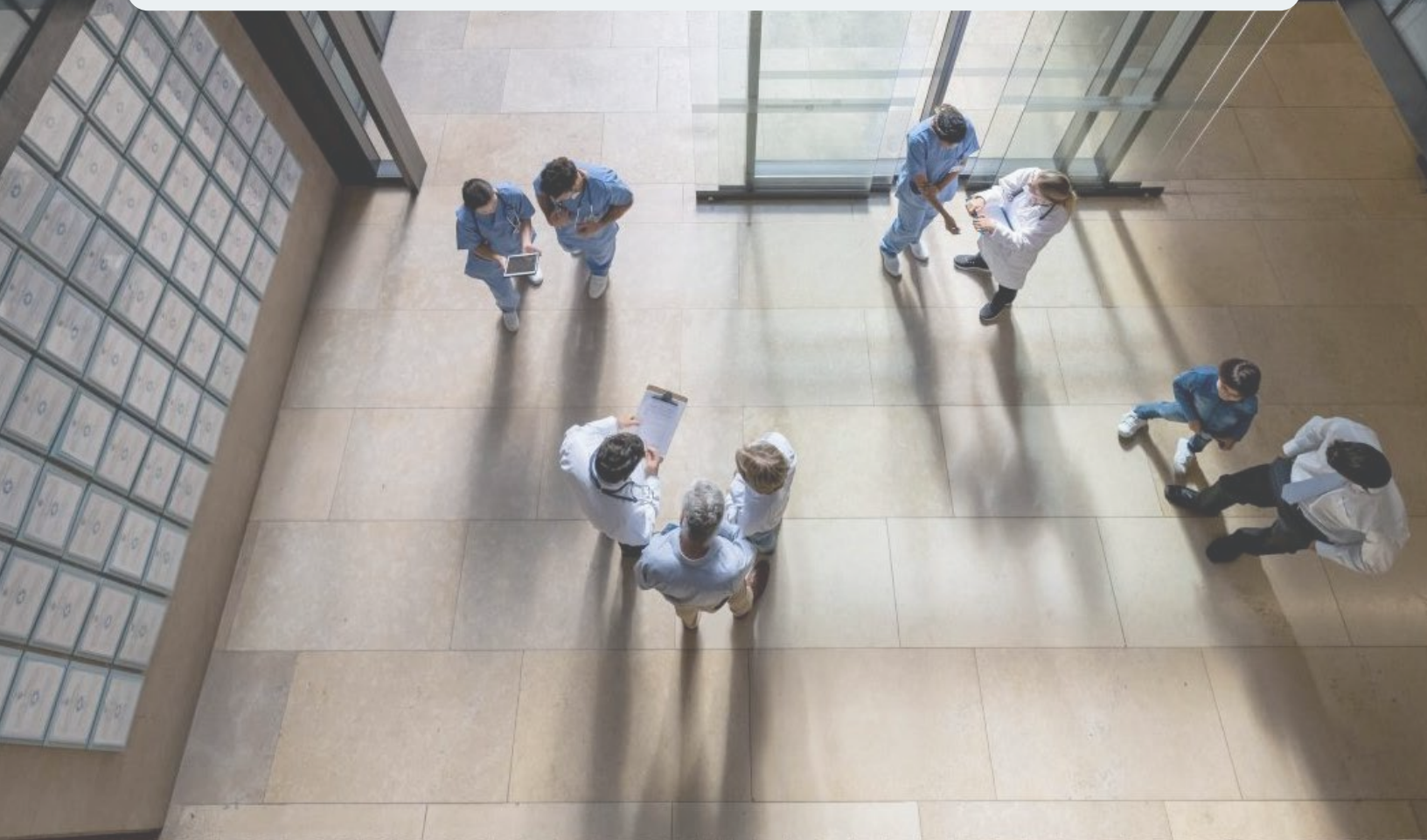
In addition, regular validation tis also crucial to ensure that recovery is successful. Penetration testing of the cyber vault to verify isolation is also recommended. The recovery validation should also confirm that key personnel are familiar with how the cyber vault fits into their cyber recovery processes and that they're able to execute on their responsibilities.

AHEAD Partners with Healthcare Company for Cyber Recovery Project

A large healthcare company recently partnered with AHEAD to design a comprehensive cyber recovery solution. This includes designing an isolated recovery environment (IRE) for platform services and building data flows for backup replication and recovery. AHEAD will also design additional cleanroom sidecars for ransomware recovery and standby production environments for critical systems.

The IRE reference architecture from AHEAD will likely include Dell Cyber Recovery on-premise components as well as Rubrik anomaly detection and threat monitoring. The engagement will also involve IRE and standby production environment workshops, analysis, and documentation to educate the client on key features and best practices for their new solution.

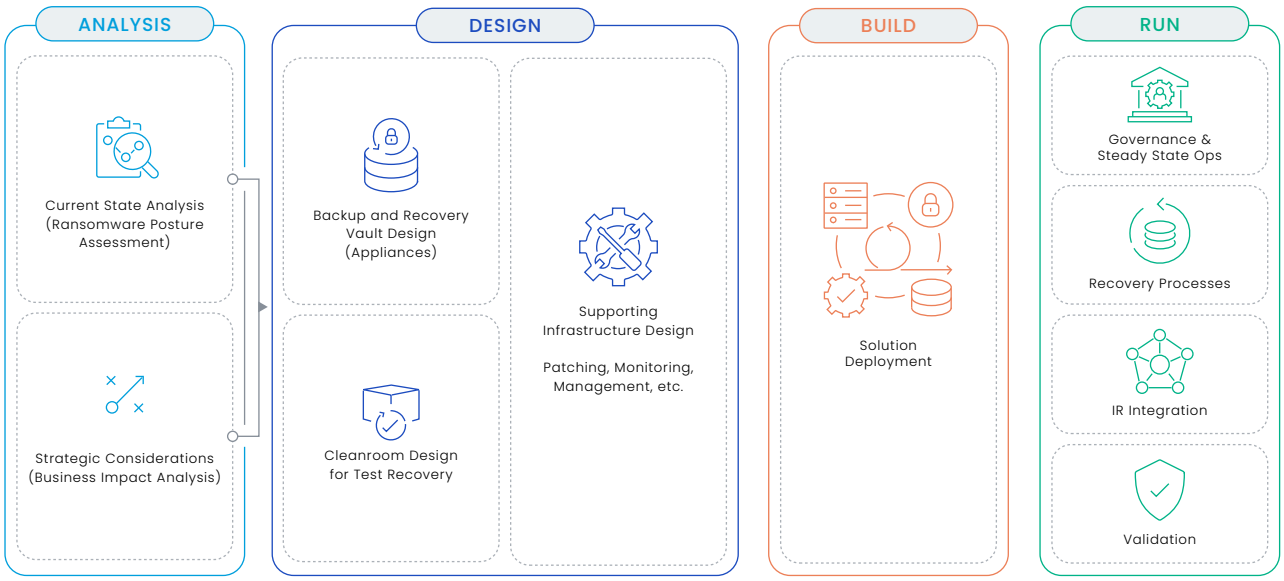
As a result of this engagement, the healthcare company will have a hardened isolated recovery environment to overcome ransomware and other cyber attacks. This solution will even enable the client to recover critical operations in an independent environment while malicious actors still have control of their production environment. AHEAD's proven cybersecurity expertise and deep experience in the healthcare industry will drive the success of this partnership.



AHEAD's Comprehensive Cyber Recovery Program

As data-driven organizations continue to face more sophisticated cyber attacks, building an effective cyber vault has become a necessity. However, creating and implementing a cyber vault along with its supporting infrastructure and processes from scratch can be challenging for many organizations without help from an experienced partner.

AHEAD is an enterprise solutions provider with deep experience in cybersecurity, data, and infrastructure. As part of our cybersecurity practice, we offer comprehensive cyber recovery services from security posture analysis to the design, implementation, and operation of cyber vaults.



ANALYSIS

AHEAD can conduct a current state analysis or ransomware posture assessment to identify gaps in your organization's existing cyber recovery plan to inform the vault design. We can also perform a business impact analysis to rightsize the recovery solution based on your specific recovery time objective (RTO) and recovery point object (RPO), which are parameters for the maximum downtime and data loss acceptable.

DESIGN

AHEAD's team of security experts can work with your organization to design backup and recovery vaults, cleanrooms, and supporting infrastructure to harden against ransomware and other threats. This will include evaluating design considerations and tradeoffs to ensure the solution minimizes cost and complexity while meeting your specific cyber recovery objectives.

BUILD

AHEAD works with innovative cybersecurity companies to provide clients with the best technologies on the market, including strategic partnerships with Rubrik, Palo Alto, Cisco Security, Commvault, and Dell Technologies. Our diverse team of engineers can help you integrate these leading technologies into a reliable and secure cyber recovery solution.

RUN

AHEAD can work with your organization to define processes for the day-to-day operations of the vault environment and to establish an approach for the recovery of data and applications from the vault. In addition, AHEAD can help you integrate these vault recovery processes into your existing incident response processes. We can also validate the secure configuration and implementation of the cyber vault solution and work with you to validate your related cyber recovery processes.

AHEAD

Combining cloud-native capabilities in software and data engineering with an unparalleled track record of modernizing infrastructure, we're uniquely positioned to help accelerate the promise of digital transformation.

Visit us at ahead.com.

National Hubs

CHICAGO
444 W. Lake Street
Suite 3000
Chicago, IL 60606

NEW YORK
500 5th Avenue
Floor 17
New York NY 10010

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

SAN FRANCISCO
2000 Crow Canyon Place
Suite 250
San Ramon, CA 94583