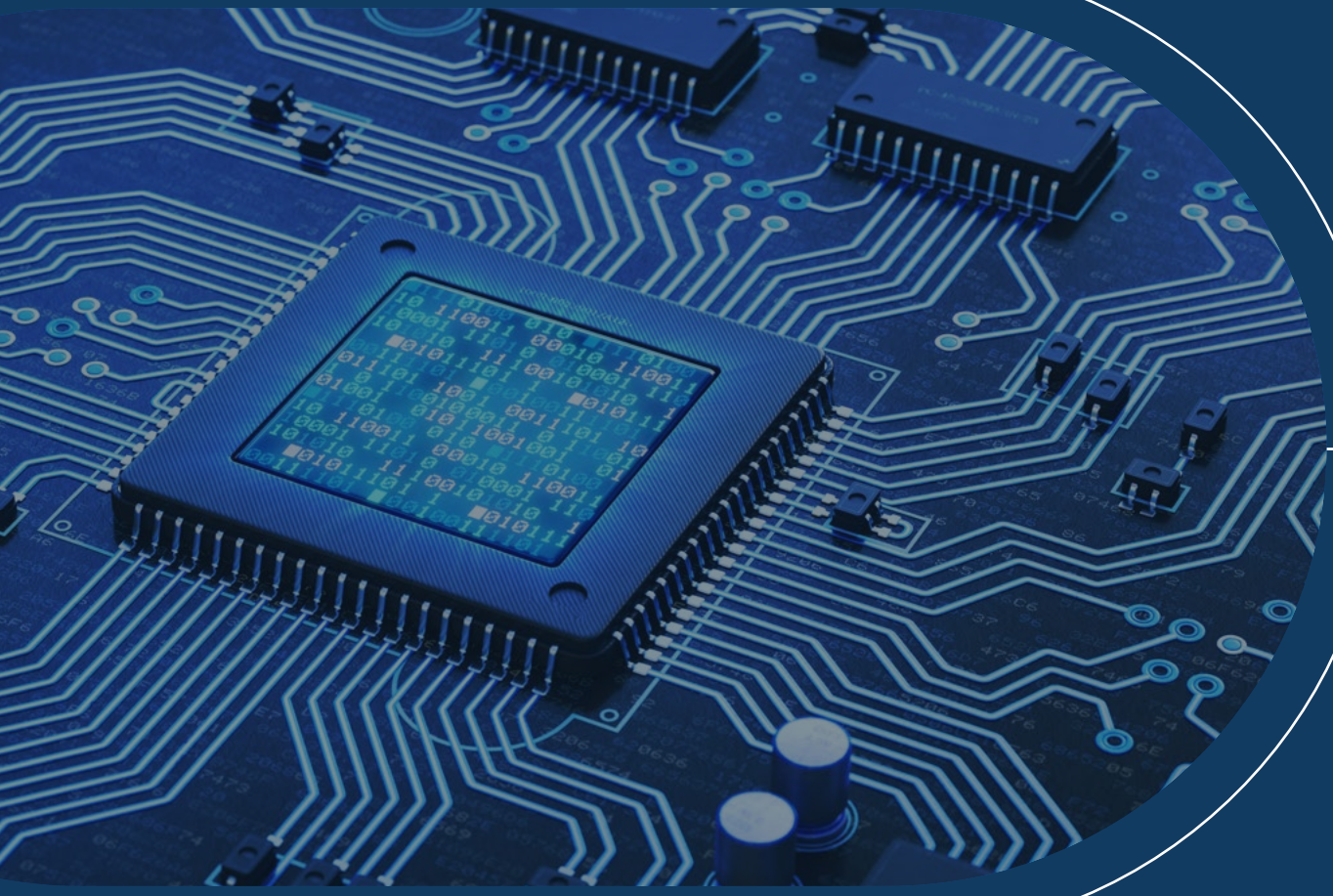
AHEAD

DELL Technologies
TITANIUM BLACK PARTNER

AHEAD + DELL TECHNOLOGIES:

Implementing Data Protection Against Sophisticated Cyber Attacks



How Dell Technologies & AHEAD are helping organizations protect their business-critical data against rapidly evolving cyber threats

Cyber threats are growing rapidly across all industries as organizations increasingly rely on data and digital services to maintain business operations. In fact, over 72% of organizations worldwide were hit by a ransomware attack as of 2023, and the average downtime was greater than 20 days. This highlights the need for organizations to enhance their current cybersecurity strategies.

Although organizations have invested heavily in real-time security, more sophisticated attack variants are circumventing these existing solutions. That's why today's data-driven organizations need a solid cyber resilience strategy to withstand day-to-day cyber threats, maintain operations during attacks, and recover if an incident occurs.

In this whitepaper, we'll discuss the importance of cyber vaults for cyber resilience, Dell's comprehensive data protection solutions, and AHEAD's services for implementing Dell's security solutions.

Protecting Data with a Cyber Vault

As more organizations become victims to ransomware and other cyber attacks, it's no longer enough to focus solely on prevention. 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.

When it comes to cyber recovery, backups are the starting point for restoring data that has been encrypted, corrupted, or deleted in a cyber attack. However, backup infrastructure is also often the target of more sophisticated attacks because malicious actors want to prevent their victims from quickly restoring operations. That's why it's crucial to create a cyber vault or isolated recovery environment (IRE) that stores a copy of critical data and is hardened against attacks.

While some industries have to adhere to regulations regarding cyber vaulting, many organizations across all industries are choosing to build cyber vaults to reduce their risk. Cyber vaults are isolated and immutable environments — sometimes even air gapped or physically segregated — that are protected against ransomware and other malware.

A key aspect of cyber vaulting is identifying the data and applications that should be protected in the vault. Companies often start from scratch, not knowing what data they have, where it is located, and which infrastructure is most essential. This lack of visibility makes it difficult for organizations to design an appropriately sized and cost-effective IRE.

An effective strategy also requires in-depth analysis to determine the components most critical to rapidly restore business operations in the event of an attack, such as Active Directory, DNS, LDAP, production databases, and backup images. These should be included in a cyber recovery clean room, which is a component of an IRE used to recover applications and conduct forensic analysis on malware.

Safeguarding Critical AI Data & Workloads

As AI becomes integrated into more applications and workflows, cyber vaulting this data will be crucial for business continuity and restoring operations after an attack. AI workloads are uniquely vulnerable because they often rely on large volumes of sensitive and constantly changing data to operate. This means isolated and immutable cyber vault environments are essential for minimizing downtime and maintaining AI-powered services.

Cyber attacks can also poison training datasets, impacting AI model performance and integrity over time. AI models are often trained on large datasets that could contain sensitive information, so regulations are increasingly requiring this data to be stored securely to maintain model reliability. For these reasons, AI data will likely need to be included in cyber vaults and will become a significant concern in the near future.

How Dell Enables Greater Cyber Resilience

Dell Technologies offers comprehensive data protection solutions to defend against ransomware and other cyber threats. Dell Cyber Recovery and CyberSense can reduce system downtime and time spent on data recovery, which minimizes the impact of a cyber attack. That's why Forrester has estimated a 53% ROI for adoption of these Dell cybersecurity solutions.

PowerProtect Cyber Recovery allows organizations to create immutable backups and store them in an isolated location on-premise or in multiple public cloud environments. The solution manages the cyber vault and data replication to ensure the data becomes locked and secure once it is in the vault.

The on-premise cyber vault deployment option offers maximum control over data and infrastructure with multiple layers of both physical and logical security. The public cloud option makes it quick and easy to deploy a secure and logically isolated cyber vault. Cyber Recovery can also be deployed to hybrid or multi-cloud infrastructure, including AWS, Microsoft Azure, and Google Cloud.

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. This is the last line of defense that checks the integrity of the data and detects suspicious behavior, including encryption, mass deletion, and corruption.

More specifically, CyberSense uses machine learning to continuously observe the data over time and evaluate whether it looks normal or suspicious. The solution also provides post-attack forensic reports to diagnose the damage and determine the last known good files to streamline recovery.

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 AHEAD proposed includes Dell Cyber Recovery on-premise components as well as Rubrik anomaly detection and threat monitoring. The engagement also involves 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 + DELL TECHNOLOGIES:

Comprehensive Data Protection for Enterprises

As malicious actors continue to target data-driven businesses, having a strong cyber resilience strategy has become a necessity. However, creating and implementing a cyber vault and data protection program from scratch can be challenging for many organizations without an experienced partner.

AHEAD is an enterprise solutions provider with deep experience in cybersecurity, data, and infrastructure. We have a diverse team of security professionals that can provide the multi-domain expertise and additional capacity you need to enhance your security capabilities. Our consultative approach, technical expertise, and innovative solutions combine to accelerate the impact of technology in every client we serve.

More specifically, AHEAD has the proven security expertise and Dell certifications necessary to ensure clients' success when implementing a new cyber resilience strategy. In fact, AHEAD is a Dell Technologies Titanium Black Partner focused on consultative solutions and one of the top 3% of Dell partners globally. We've obtained 400+ certifications and 24 competencies in storage, server, data protection, client, and CI/HCI services.

AHEAD's professional services include implementation, automation, and integration of Dell's cyber recovery solutions. Our team of experts can help clients understand and utilize their infrastructure safely and effectively. This includes building a cyber vault with Dell PowerProtect and protecting data stored within Dell PowerStore and on Dell PowerFlex infrastructure.

> Ready to protect your data and infrastructure against increasingly sophisticated cyber threats? **Contact AHEAD** to learn more about implementing Dell's cyber recovery solutions.

Contributing Authors:

Jonathan Kowall, Director, Specialist Solutions Engineering

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 Fifth Avenue
Suite 1500
New York, NY 10110

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

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