aws | COHESITY

EBOOK

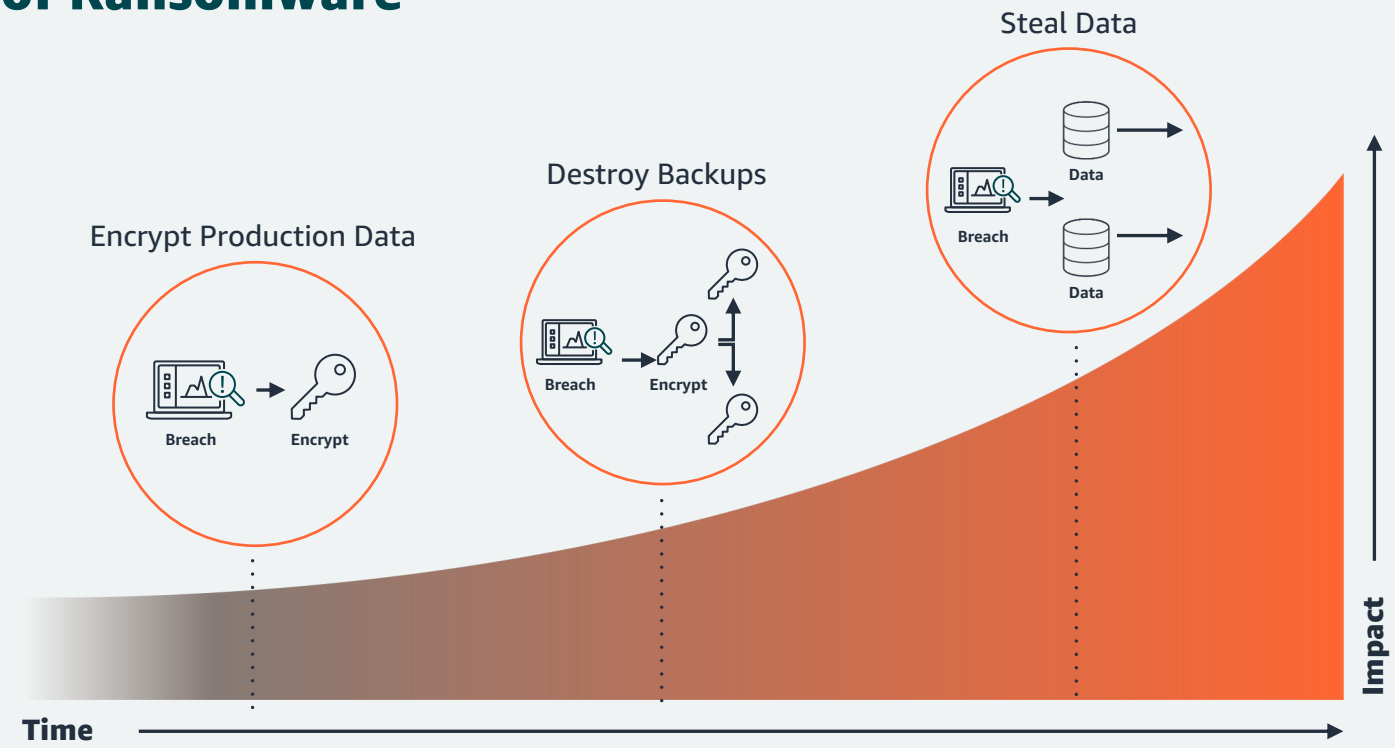
Defend Your Data and Refuse the Ransom

Protect your mission-critical data with Cohesity and AWS

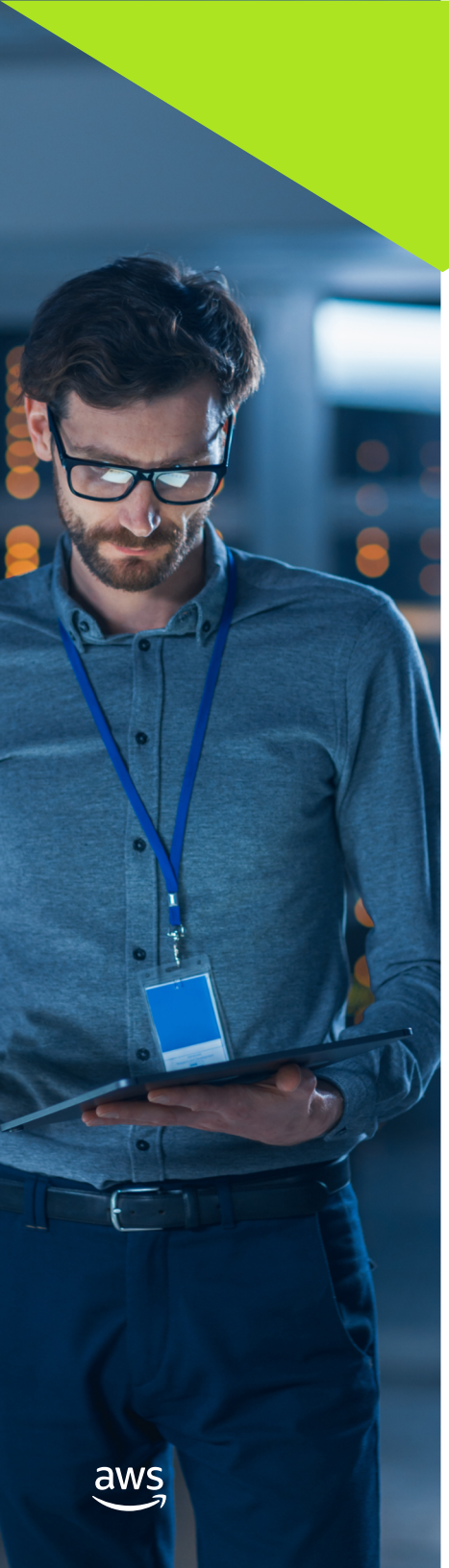
Cyberattacks are not a matter of "if" but of "when" and the costs to recover from an attack are only growing. In fact, businesses are spending on average more than $1.85 million to overcome a ransomware attack, without even paying the ransom.[1] One company that faced this challenge was Colonial Pipeline, who experienced a cyberthreat in 2021 that took hold of the firm's billing system and internal business network, leading to widespread shortages in multiple states. Colonial Pipeline eventually gave in to the demands and paid the group $4.4 million dollars in Bitcoin.[2]

As ransomware attacks have continued to rise, cybercriminals have begun developing new methods of cyber mayhem.

Evolution of Ransomware



1. Sophos: Ransomware Recovery Cost
2. AP News: Colonial Pipeline Hackers



Initially, cybercriminals targeted production data directly: encrypting it and then demanding a ransom to supply keys to unlock. But organizations could simply use backup and recovery solutions that allowed them to restore their production data to get around this demand. As a result, hackers began targeting backup data as a first point of attack. In this scenario, attackers gain access to target backup systems to encrypt or destroy the backup data before it can be restored to the production environment. With their backup "insurance policies" gone, organizations often are forced to pay the ransom and hope they can perform a complete recovery of their data.

The most recent evolution of ransomware incorporates data exfiltration techniques in which cybercriminals aim to steal data and threaten to sell or publish it on the dark web unless a ransom is paid. Law Enforcement Health Benefits Inc (LEHB) suffered a similar fate when a ransomware attack impacted over 85,000 people.[3] In September 2021, cybercriminals infiltrated LEHB's network and exfiltrated personal information including names, social security numbers, driver's license numbers, health insurance information, and more.

To further complicate things, data exfiltration is not always an external threat. Cybercriminals are not always unknown, outside forces—an employee can also cause huge disruptions from the inside.

Organizations must leverage new innovations in data management to remain one step ahead of these growing threats. To enhance data resiliency and recoverability, many are turning to a next-gen data management platform that combines four unique elements: simplicity at scale, Zero Trust security principles, AI-powered insights, and third-party extensibility to help counter the actions of criminals. It's the combination of these elements that address today's threats and challenges and enable organizations to protect their business from ransomware and other cybercrimes.

3. Health IT Security: Law Enforcement Ransomware Attacks

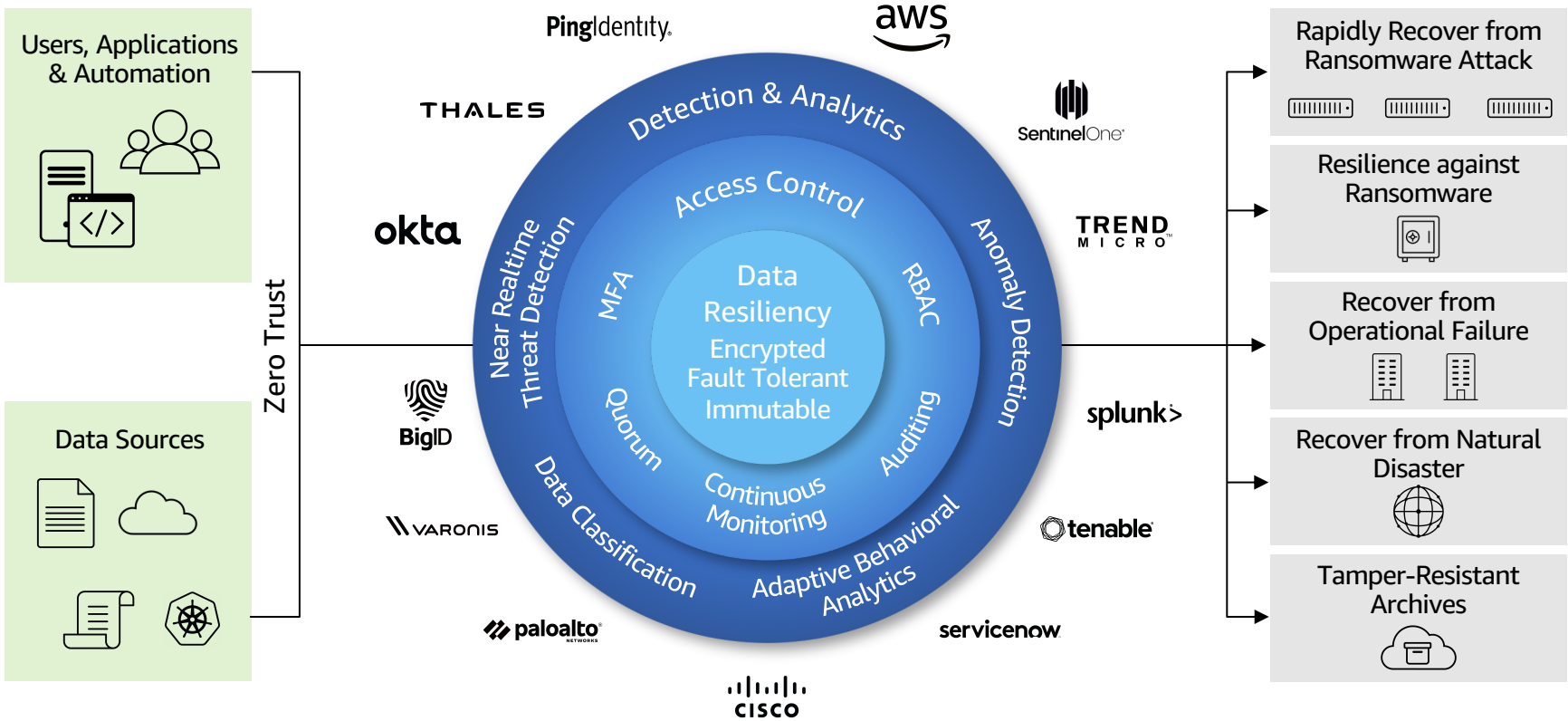
Dedicated threat defense architecture at the platform level

When it comes to ransomware, Cohesity provides reliable solutions that enable organizations to protect and secure their mission-critical data at the platform level.

Cohesity's threat defense architecture helps data resiliency by providing key capabilities such as encryption and immutability that make it difficult for potential cyber criminals to modify or delete data. It also provides various access-control mechanisms to help keep criminals from accessing your data in the first place.

Before something occurs, businesses can take advantage of AI-powered detection and analytics across their IT environment to see who has access to their most sensitive data. With this intelligence, organizations can monitor their critical data and easily detect anomalous data access and user activities.

Protecting your data is not a job that Cohesity can do by itself. Cohesity's threat defense architecture also provides support for cloud providers like Amazon Web Services (AWS) to further enhance the security and recoverability of your enterprise data.



Start protecting your data with Cohesity Data Management Delivered as a Service

Enterprises are accelerating their journey to the cloud and need data management solutions that streamline business operations while combating ransomware and cybercrime. To stay competitive and thwart off cybercriminals, organizations are seeking to modernize their data management strategy by moving to a next-gen data management solution that is delivered through an as-a-service model. By removing infrastructure complexity, breaking down data silos, and protecting data from ransomware, enterprises are protecting what matters most—their mission-critical data.

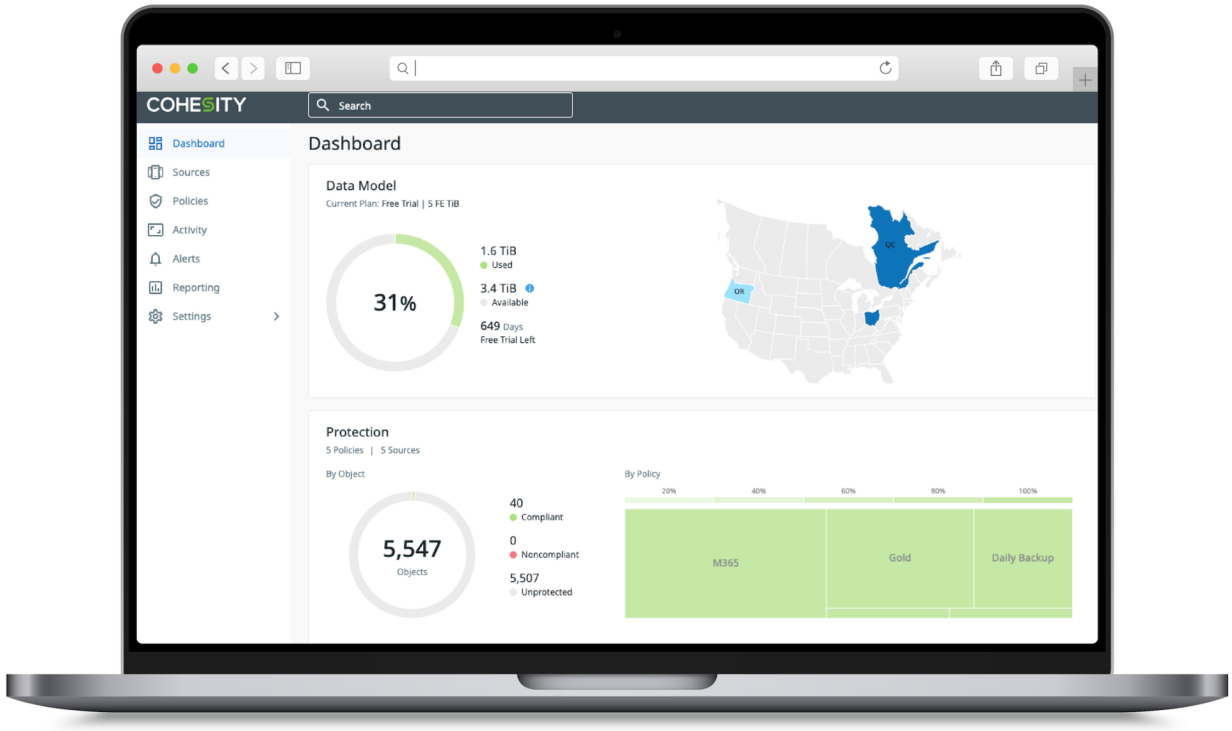
Cohesity Data Management as a Service (DMaaS) is a portfolio of as-a-service offerings for backup and recovery, disaster recovery, compliance and governance, and data isolation. Managed by Cohesity and hosted on AWS, DMaaS enables businesses to enhance cyber resiliency by easily recovering encrypted production data, isolating data to keep it safe from cybercriminals, identifying sensitive data, and detecting risky behaviors for potential threats.

Let's look at some of the key solutions within the DMaaS portfolio and how they help organizations combat growing ransomware threats.

Safeguard your backups in a separate environment

Data backup and recovery is essential to protect your business in the event of a ransomware threat. With Backup as a Service (BaaS), enterprises can leverage a completely separate environment for their backup data, which in turn adds an additional layer of protection against criminals for your data.

Cohesity's DataProtect delivered as a Service is an enterprise-grade BaaS solution that protects on-premises, SaaS, and cloud-native data by eliminating silos and consolidating backup data across a variety of locations and data sources. It enables businesses to have a clean copy of data if ransomware hits, so they can easily recover production data that has been encrypted. And, with immutability and access controls at the platform level, Cohesity DataProtect delivered as a Service keeps cybercriminals from reaching backup data to begin with.



Leveraging data vaults for data isolation

When it comes to further safeguarding sensitive and proprietary data, organizations are turning to data vaults. Data vaults provide isolated, virtual air-gapped environments that are separated from an organization's production and backup environment, providing defense against ransomware threats with a highly secure copy of production data.

Cohesity FortKnox is a data isolation and recovery SaaS solution that improves cyber resiliency with an immutable copy of data in a Cohesity-managed AWS cloud vault via a virtual air gap. The vaulted copy of data on the AWS Cloud can be used to rapidly recover data that has been lost or compromised and deliver the data back to the original source or an alternate location. In the event of a ransomware threat, an untainted copy of data can be easily identified, accessed, and retrieved, streamlining the recovery process.

With Cohesity FortKnox, customers can:

Simply connect, vault, and recover without shipping tape offsite or deploying a self-managed data vault.

Secure their data with physical, network, and operational isolation (aka a virtual air gap).

Meet stringent SLAs by quickly and easily recovering data when and where they need to.

Stop cyber criminals from reaching your data

Data governance has become a critical part of data management for most organizations, particularly those in heavily regulated industries such as financial services and healthcare. However, remaining compliant with privacy and data protection laws has become even more challenging, with more regulations regularly emerging.

DataGovern*, Cohesity's upcoming threat detection and compliance service, will leverage machine learning (ML) to automatically discover sensitive data while analyzing access and usage patterns for potential cyberthreats. The solution will identify overexposed sensitive data with real-time scanning of production and backup environments and will encourage proper access controls to deter threats from happening in the first place.

DataGovern will also simplify data classification with predefined and custom policies and reporting for GDPR, CCPA, HIPAA, and more.

*We expect to release DataGovern early access in the near future.

Bolster security with the AWS Cloud

By working with AWS, Cohesity helps organizations have access to the agility and security of AWS, which provides more security certifications than any other cloud provider in the market. With access to these AWS capabilities, organizations have access to cutting edge capabilities, including:

Amazon S3 Object Lock:

Amazon S3 Object Lock allows the creation of immutable copies of data, preventing it from being deleted or overwritten using Write Once Read Many (WORM) capabilities. S3 Object Lock can prevent ransomware from overwriting backup data and also can prevent inadvertent change or deletion from users.

AWS PrivateLink:

AWS PrivateLink provides private connectivity between virtual private clouds (VPCs), AWS services, and on-premises networks, without exposing network traffic to the public internet. Using AWS PrivateLink, on-premises backup software from AWS Partners such as Cohesity can communicate privately with Amazon S3 for storing and retrieving backup data.

Multi-Account Strategy and Network Segmentation:

Multi-Account Setup and Network Segmentation help protect data and applications in AWS with use of a multi-account-based strategy along with locked down network segmentation. Network segmentation allows networking isolation through capabilities that lock down access to applications and data via mechanisms including private and public subnets, security groups, and network access control lists, among others.

Ransomware attacks can have significant implications to businesses worldwide including the costs of overcoming and paying the ransom and the potentially negative impacts to reputation, public perception, and customer trust.

Now is the time to defend and protect your most sensitive data with Cohesity DMaaS, managed by Cohesity and powered by AWS. Have peace of mind knowing that your organization is prepared for a potential disaster, has reliable solutions in place to help prevent and deter cyberthreats, and that the data that drives your business forward is resilient and recoverable.

Learn more about strengthening your data protection with Cohesity and AWS

Cohesity is available in **AWS Marketplace**