

# Defend Your Data and Refuse the Ransom

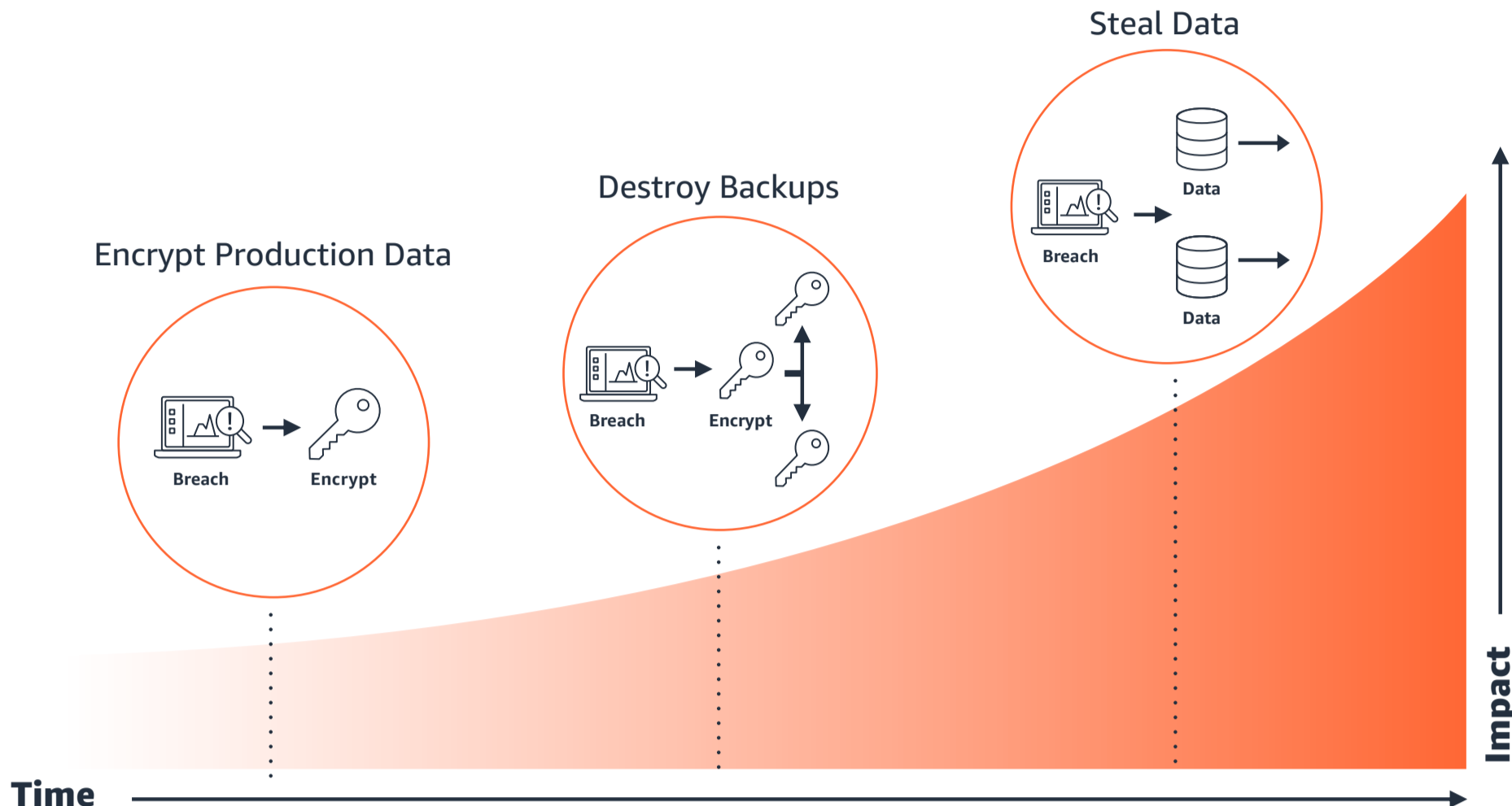
**Ransomware threats** have grown more prevalent, impacting organizations across a wide range of industries, sizes, and geographies.

**8%**  
The percentage of organizations that **recovered all data** after paying the ransom.<sup>1</sup>

**37%**  
The percentage of organizations worldwide that **experienced a ransomware threat** at some point in 2021.<sup>2</sup>

## The evolution of ransomware

Cybercriminals have evolved ransomware tactics from encrypting production data to targeting backup data to stealing data.



To enhance data resiliency, many organizations are adopting a next-gen data management platform that combines **simplicity at scale, Zero Trust security principles, AI-powered insights,** and **third-party extensibility** to bolster protection from cyberthreats and enhance the recoverability of enterprise data.

**\$265B**  
Increase in ransomware costs in less than 10 years.<sup>3</sup>

**130**  
The number of **different ransomware strains** detected since 2020.<sup>4</sup>

**82%**  
The percentage average ransomware payments climbed in 2020.<sup>5</sup>

## Reliable ransomware recovery

Cohesity provides next-gen data management solutions that enable organizations to protect their data at the platform level.

### Cohesity's Threat Defense capabilities deliver:

**Encryption and immutability** to deter cybercriminals from modifying or deleting data

**Access-control mechanisms** to help keep criminals from accessing data

**Detection and analytics** to monitor and detect anomalies in data access and user activities

**Third-party integration** with vendors such as Amazon Web Services (AWS)

## Data Management as a Service

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 the resiliency of their data by:**

- ✓ Isolating data to keep it safe from cybercriminals
- ✓ Preventing unauthorized changes to access settings
- ✓ Thwarting insider attacks
- ✓ Easily recovering production data that was maliciously encrypted



### Data backup and recovery

With Backup as a Service (BaaS), organizations can establish a separate environment for backup data. Cohesity's DataProtect delivered as a Service is an enterprise-grade BaaS solution that consolidates backup data across various locations and data sources.



### Data isolation

Data vaults provide isolated, virtual air-gapped environments that are separate from production and backup environments, delivering a highly secure, tertiary copy of data. Cohesity FortKnox is a SaaS data isolation and recovery solution that improves cyber resilience with an immutable copy of data in a Cohesity-managed vault on AWS.



### Data governance

Cohesity DataGovern\* is an upcoming threat detection and compliance solution that will leverage machine learning to discover sensitive data, analyze access and usage patterns, and simplify data classification.

## Enhance protection against ransomware with Cohesity and AWS

Cohesity's platform works with AWS to further enhance the security and recoverability of enterprise data. Now businesses can secure and protect mission-critical data with Cohesity DMaaS, managed by Cohesity and powered by AWS.

**Learn more about enhancing data protection with Cohesity and AWS**



- Public Sector
- AWS Outposts Ready
- Storage Software Competency

<sup>1</sup> Sophos: Ransomware Recovery Cost

<sup>2</sup> IDC: 2021 Ransomware Study

<sup>3</sup> Cyber Crime Magazine: Global Ransomware Damage Costs

<sup>4</sup> Virus Total: Ransomware Activity Report

<sup>5</sup> Palo Alto Networks: Ransomware Crisis Intensifies

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