Recovering from a Ransomware Attack: How Today's Data Protection Can Keep You Operating After an Attack

cStor
We look beyond IT

rubrik

David Siles
Global Field CTO
Rubrik

Andrew Roberts
Chief Cybersecurity Strategist
cStor

cStor: AN AWARD-WINNING PROVIDER

- Helps clients solve tough IT challenges with best-of-breed technology and expert consulting
- Creates and implements end-to-end solutions to fit your business needs
- Helps create a cost-effective architecture
- Displays a competitive advantage over other providers
- Creates flexibility by offering vendor agnostic solutions
- Always puts clients first

We look beyond IT

cStor

SOLUTION OFFERINGS

Professional Recommendations to Ensure Your Infrastructure
Evolves Alongside Your Business

DIGITAL TRANSFORMATION

CYBERSECURITY

DATA CENTER SOLUTIONS

We look beyond IT

OUR APPROACH

Our mission is to put people on a path to success

Clients First

Vendor Agnostic

Highly Specialized

cStor SERVICES

CONSULTING AND OPTIMIZATION

CLOUD

STAFF AUGMENTATION

CYBERSECURITY

DATA MIGRATION

DELIVERY

MANAGED SERVICES

We look beyond IT

Recovering from a Ransomware Attack: How Today's Data Protection Can Keep You Operating After an Attack

David Siles
Global Field CTO
Rubrik

ZERO TRUST DATA MANAGEMENT

FIGHTING BACK AND RECOVERING FROM RANSOMWARE

STATE OF RANSOMWARE

EVOLVING THREAT LANDSCAPE

\$30+ MILLION

ransomware
payment demands
In 2020[1]

Ransomware as a Service

Double Extortion

Exponential Damages

rubrik

[1] Palo Alto Network Unit 42 Ransomware Threat Report 2021

THE PROBLEMS WITH RANSOMWARE RECOVERY

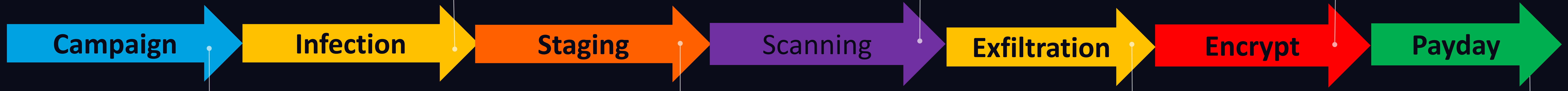
Your last line of defense?
No longer working.

You can't determine the
blast radius of attack.

Quick recoveries are a pipe dream.
Avg: 7+ days to recover.

rubrik

THE ANATOMY OF A RANSOMWARE ATTACK



Distribution Campaign attackers use techniques like social engineering and weaponized websites to trick or force users to download a dropper which kicks off the infection

Malicious Code Infection – the dropper downloads an executable which installs the ransomware itself

Malicious Payload Staging – the ransomware sets up, embeds itself in a system, and establishes persistency to exist beyond a reboot

Scanning - the ransomware searches for content to encrypt, both on the local computer and the network accessible resources

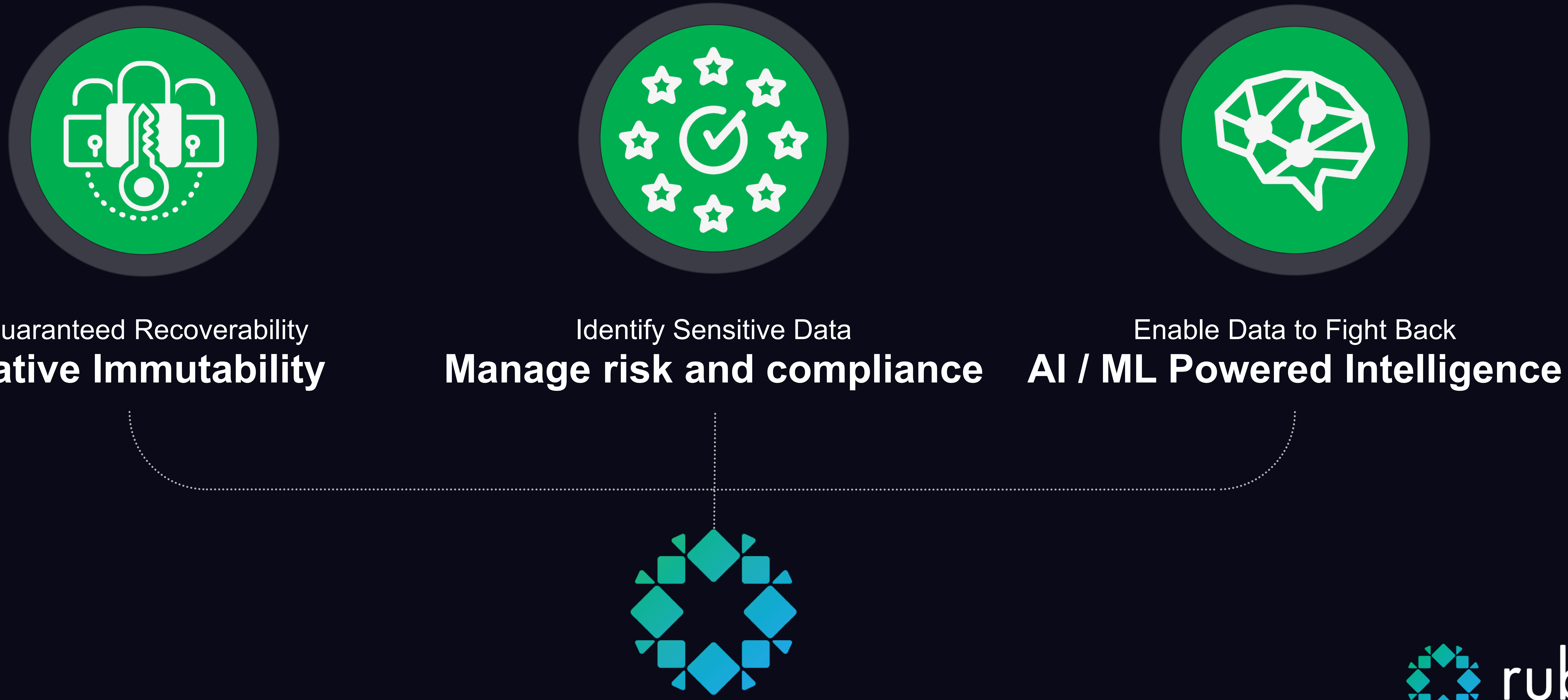
Exfiltration - the cyber criminals copy and steal the victim’s most sensitive and privileged information to use in extortion efforts

Encryption - the discovered files are encrypted

Payday - a ransom note is generated, shown to the victim, and the hacker waits to collect on the ransom

DATA PROTECTION HAS TO EVOLVE

INTRODUCING SECURITY AT THE POINT OF DATA

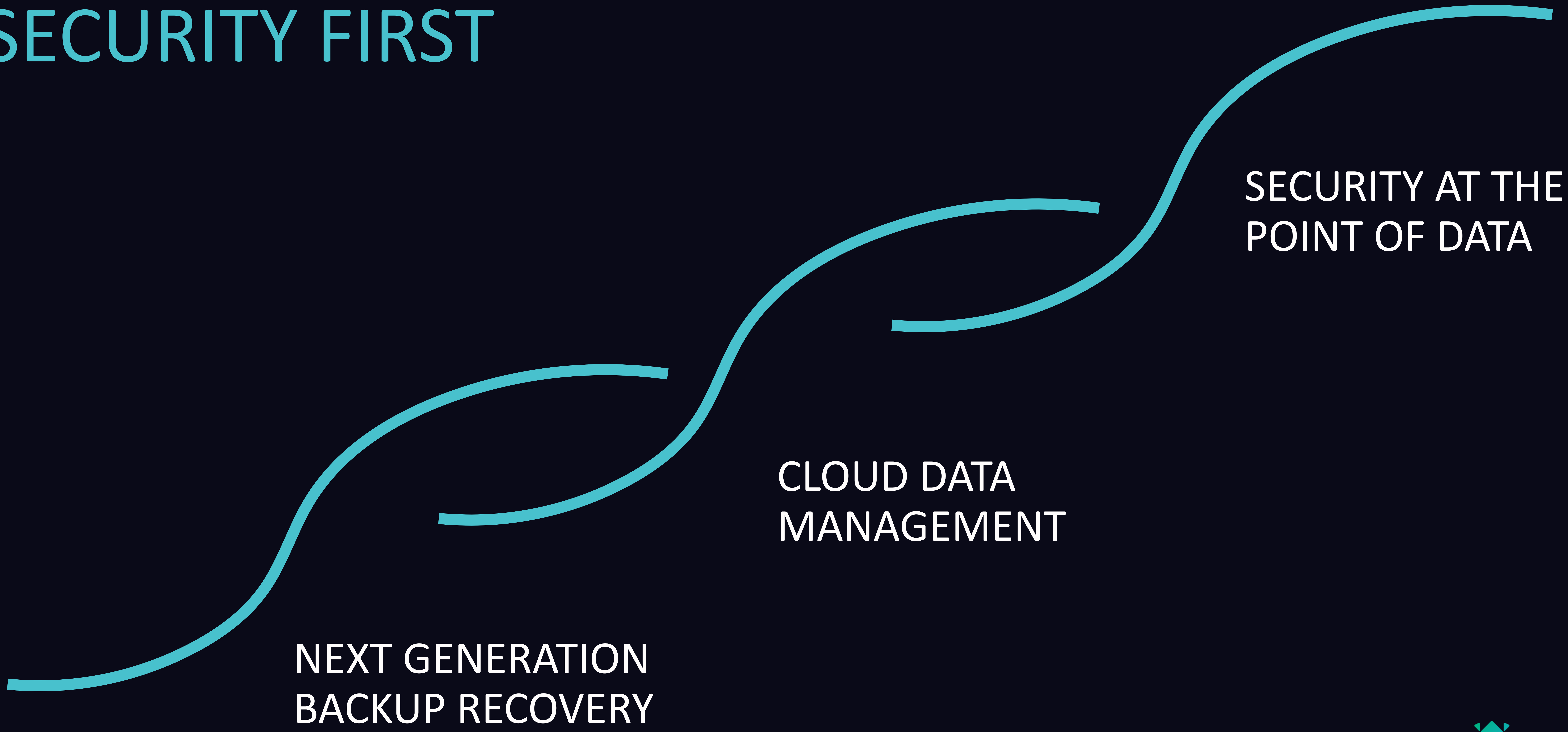


Guaranteed Recoverability
Native Immutability

Identify Sensitive Data
Manage risk and compliance

Enable Data to Fight Back
AI / ML Powered Intelligence

NEW DATA IMPERATIVE:
SECURITY FIRST



NEXT GENERATION
BACKUP RECOVERY

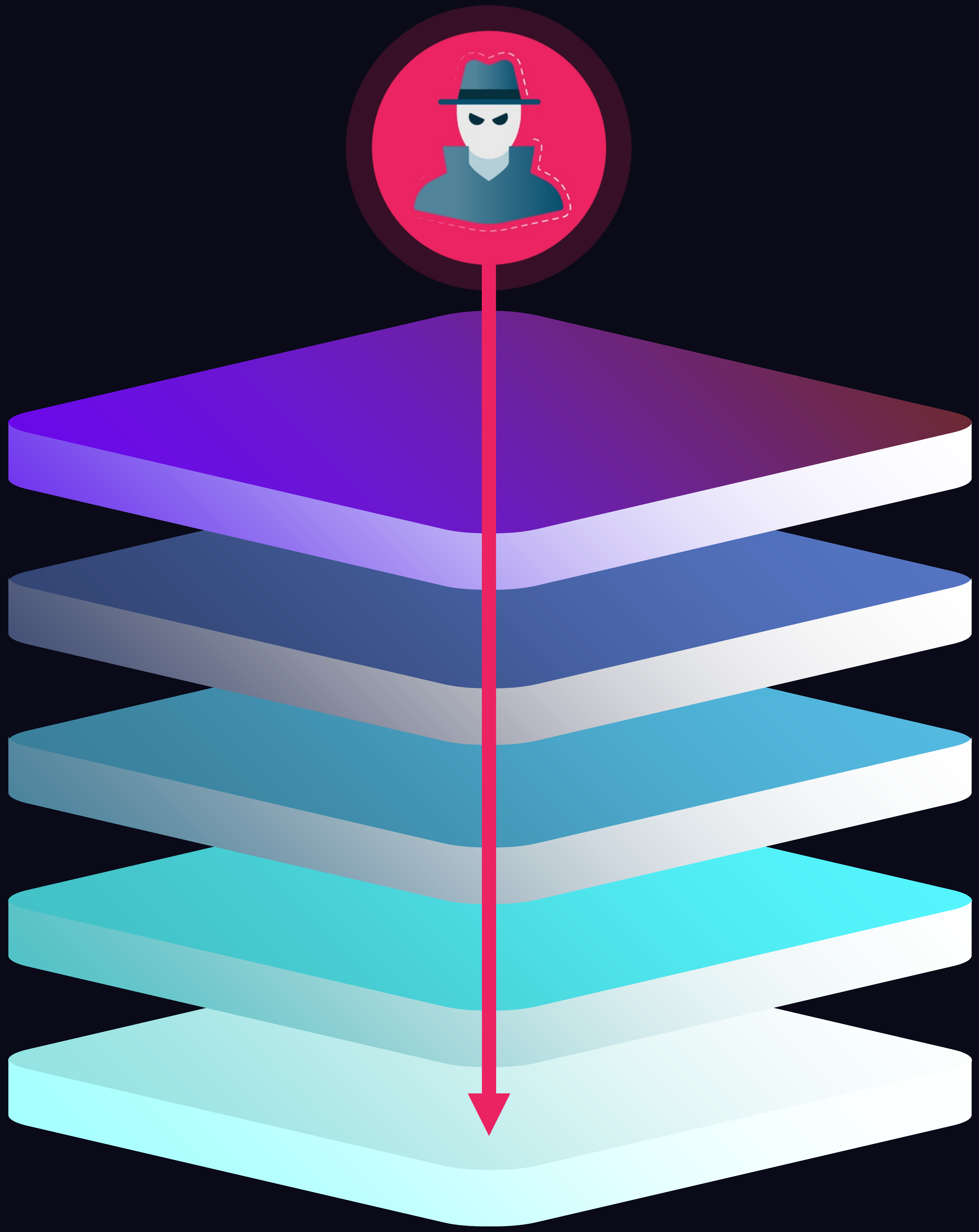
CLOUD DATA
MANAGEMENT

SECURITY AT THE
POINT OF DATA

rubrik

DATA MANAGEMENT AND SECURITY

MUST CONVERGE



PERIMETER SECURITY

NETWORK SECURITY

ENDPOINT SECURITY

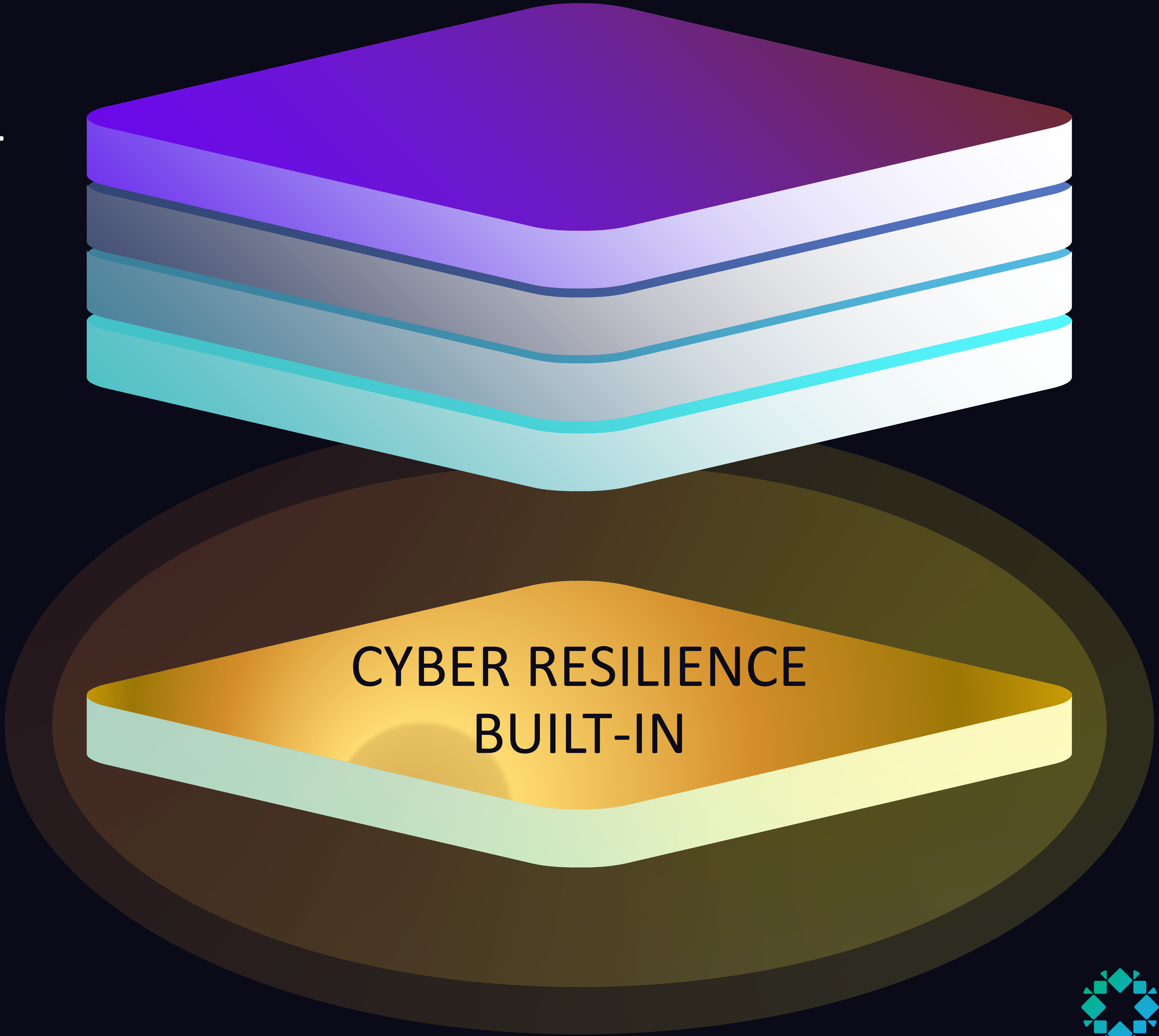
APPLICATION SECURITY

DATA

rubrik

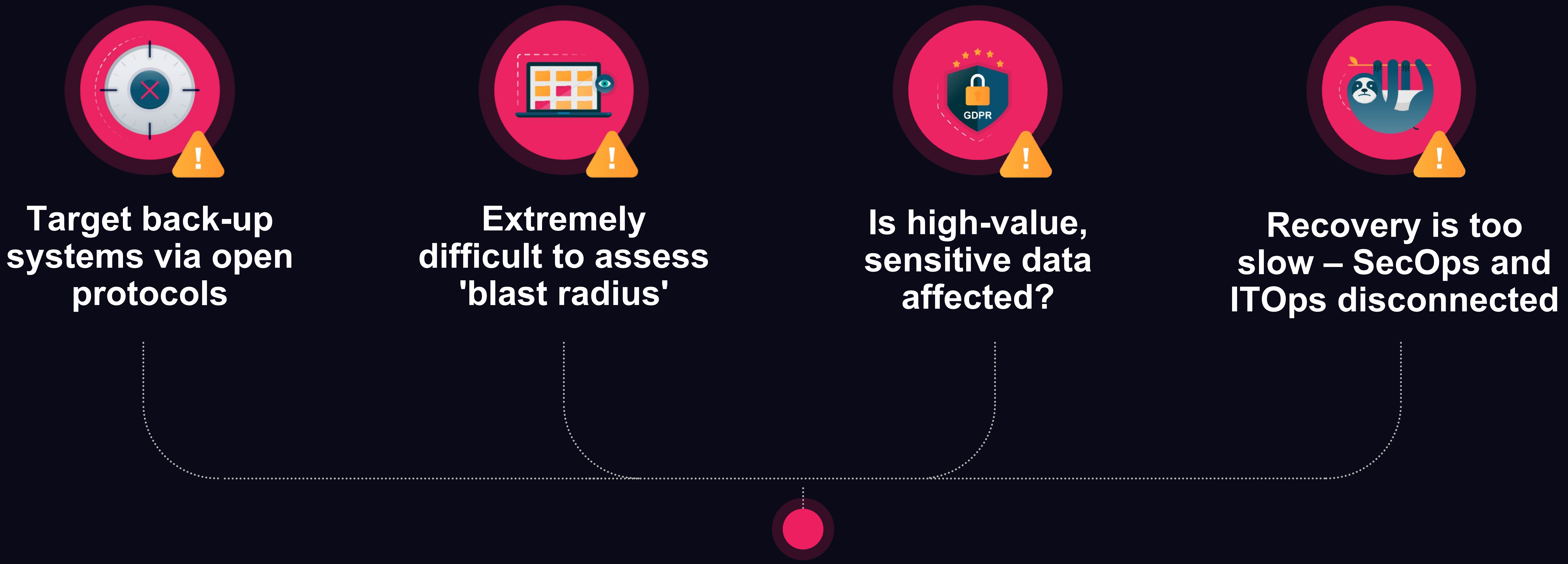
DATA MANAGEMENT AND SECURITY

MUST CONVERGE



rubrik

THE PROBLEM WITH RANSOMWARE RECOVERY TODAY



Target back-up systems via open protocols

Extremely difficult to assess 'blast radius'

Is high-value, sensitive data affected?

Recovery is too slow – SecOps and ITOps disconnected

OUR APPROACH: RANSOMWARE PROTECTION AND RECOVERY

Native Immutability

Data is air-gapped and cannot be accessed or encrypted by ransomware

Scoped Anomaly Detection

Assess what data has been impacted and determine blast radius of attack

Sensitive Data Assessment

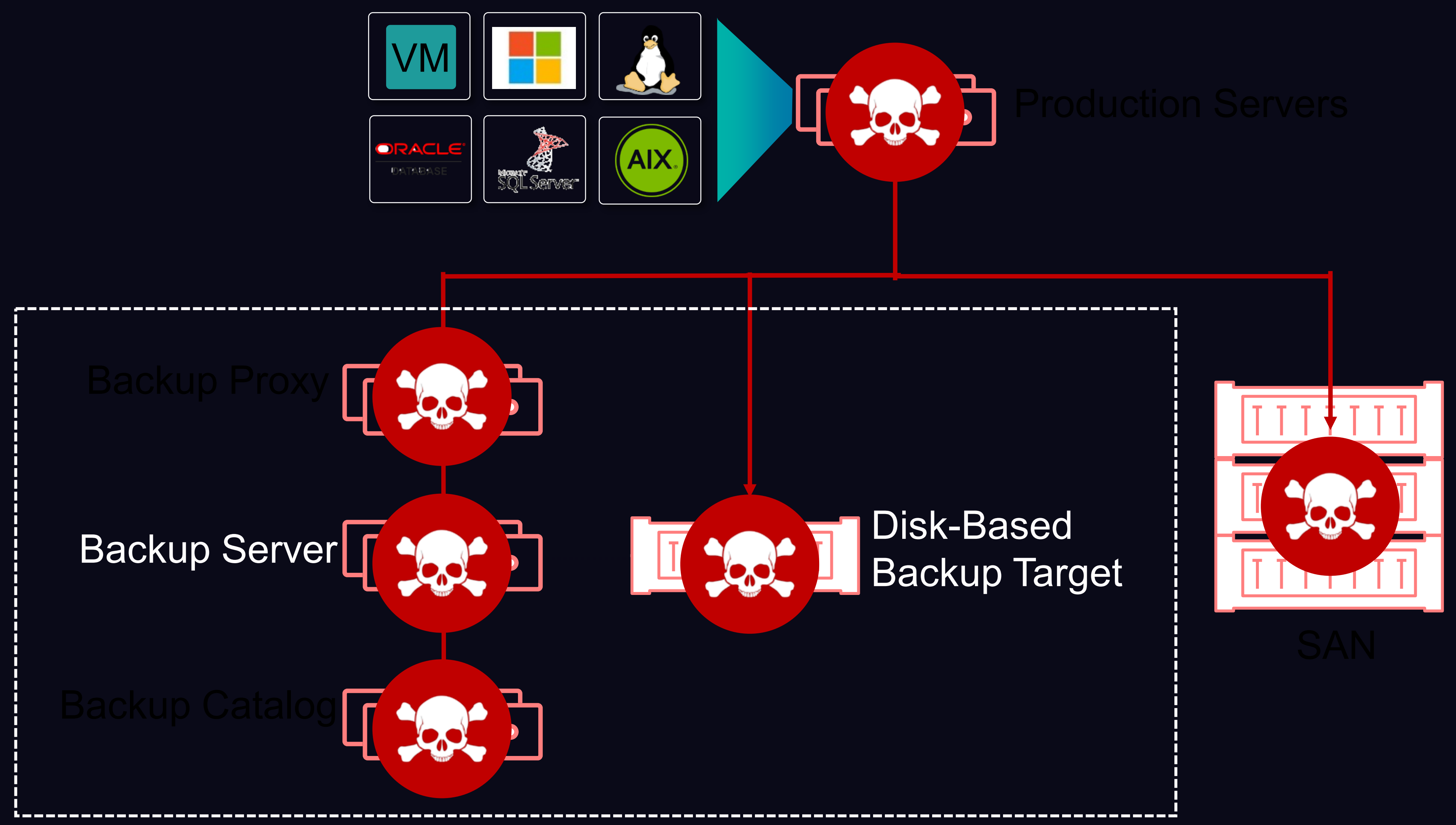
Discover if sensitive data is at risk

Expert Guided Recovery

Automated recovery playbook to get your application the nearest clean data, with sequencing order and recovery type

AIR GAPPED NATIVE IMMUTABILITY

Without Air Gap / Immutability



Backups can be accessed, modified & deleted from the network

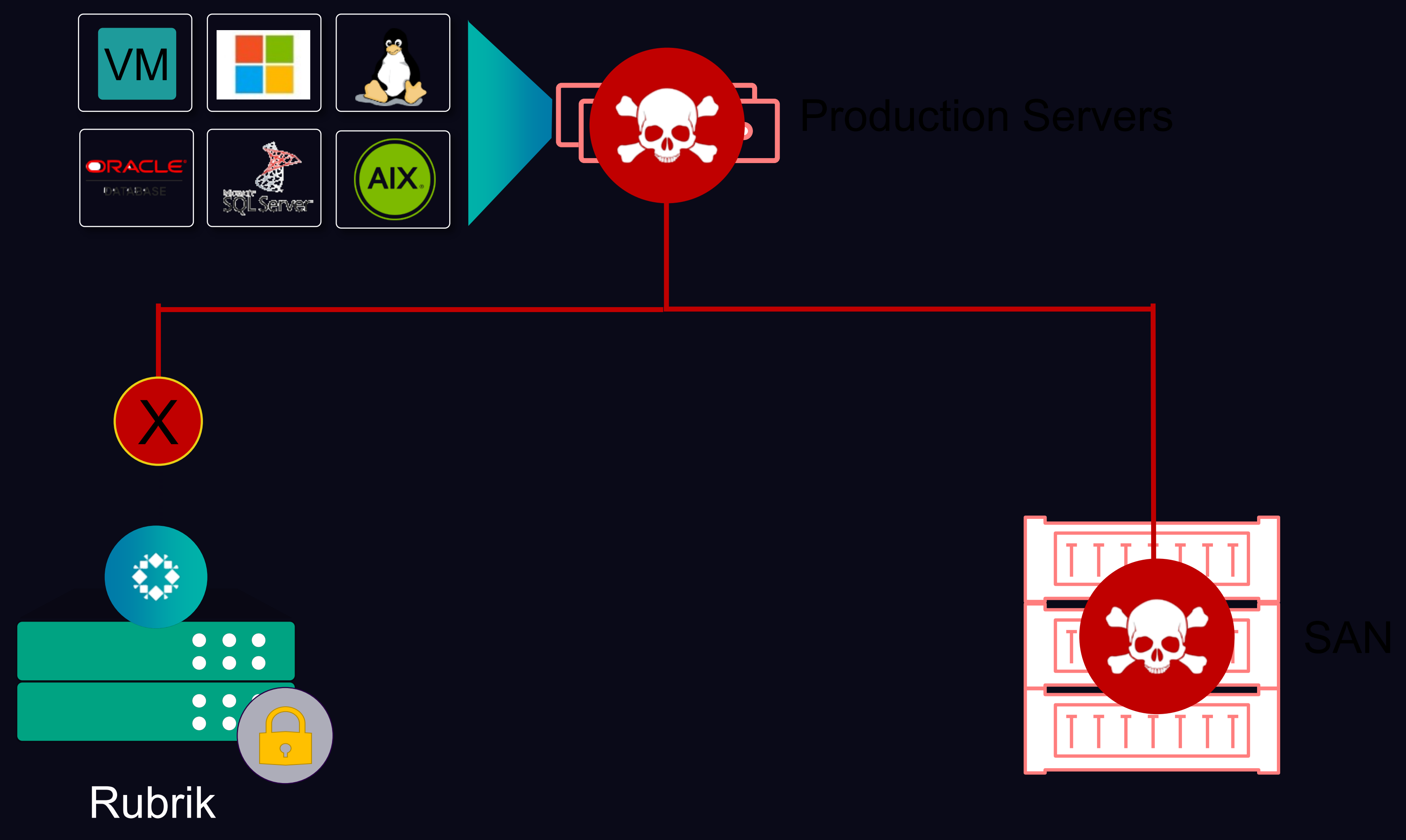
Anything using standard storage protocols is vulnerable

From legacy to “modern” solutions - virtual or storage based

No air gap, no native immutability, vulnerable

Major attack is an unrecoverable event

Rubrik’s Native Air Gapped Immutable Solution



Hyperconverged backup software & backup storage

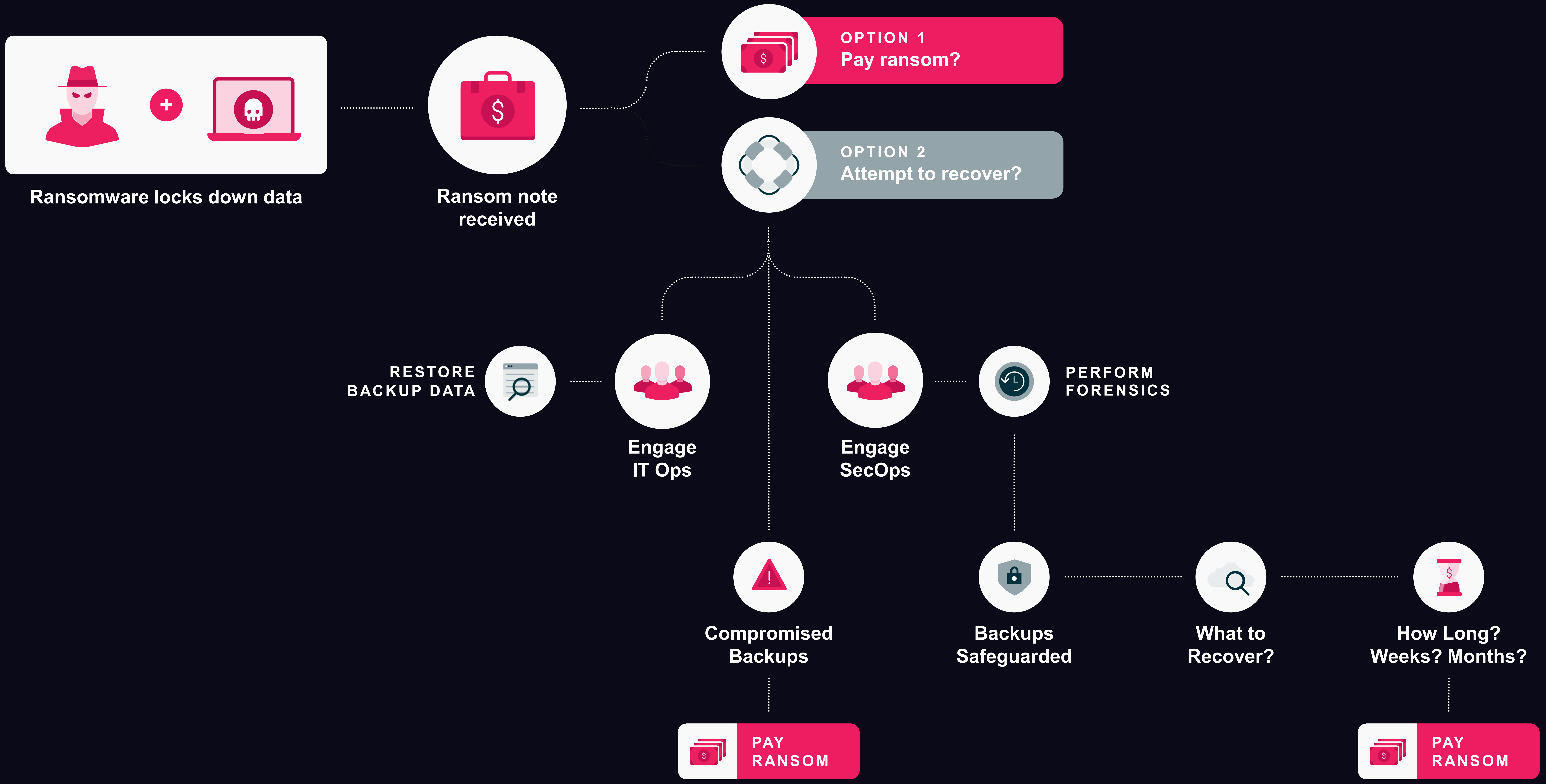
HTML5 , API-first, scale-out, cloud, live mount etc (table stakes)

No storage online or on the network (native logical air gap)

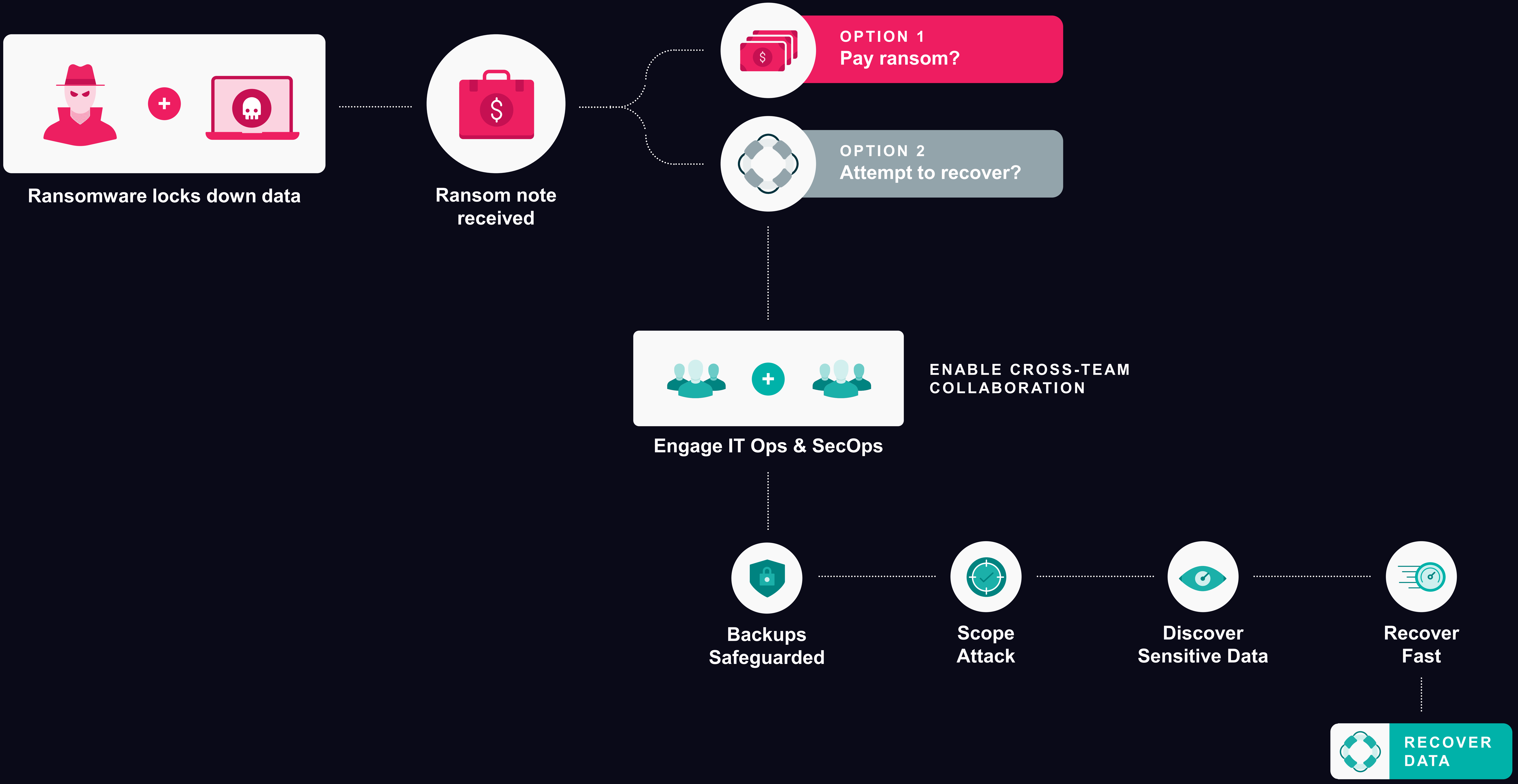
Backups CANNOT modified/encrypted (immutable file system)

Major attack is now a recoverable event from the 1st copy

TODAY’S THREAT



SECURITY AT THE POINT OF THE DATA



Ransomware locks down data

Ransom note received

OPTION 1
Pay ransom?

OPTION 2
Attempt to recover?

Engage IT Ops & SecOps

ENABLE CROSS-TEAM COLLABORATION

Backups Safeguarded

Scope Attack

Discover Sensitive Data

Recover Fast

RECOVER DATA

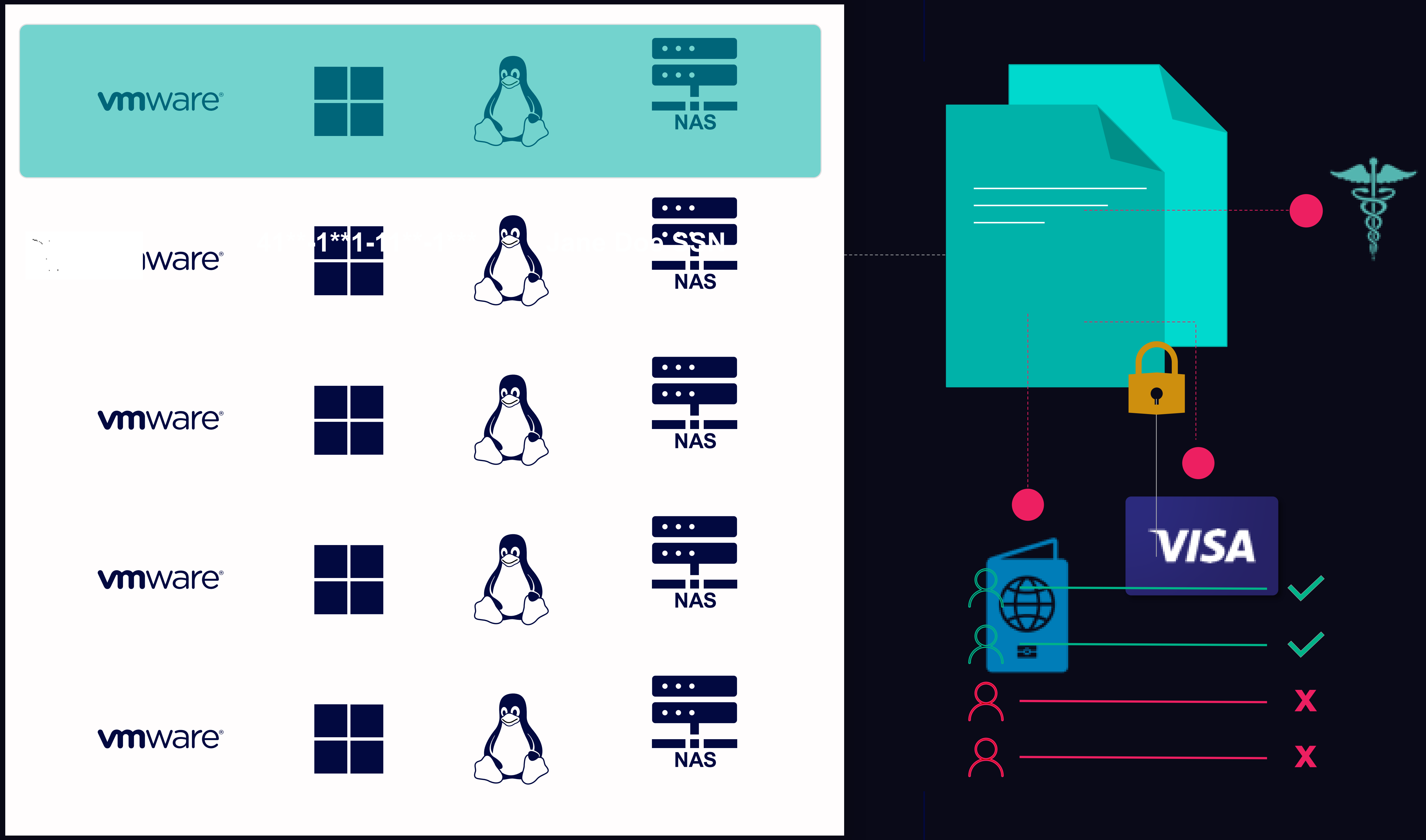
THREE KEY QUESTIONS

What is happening to your data?

Who is doing what to your data?

How sensitive is the content of your data?

Risk Insights For Stronger Security Posture



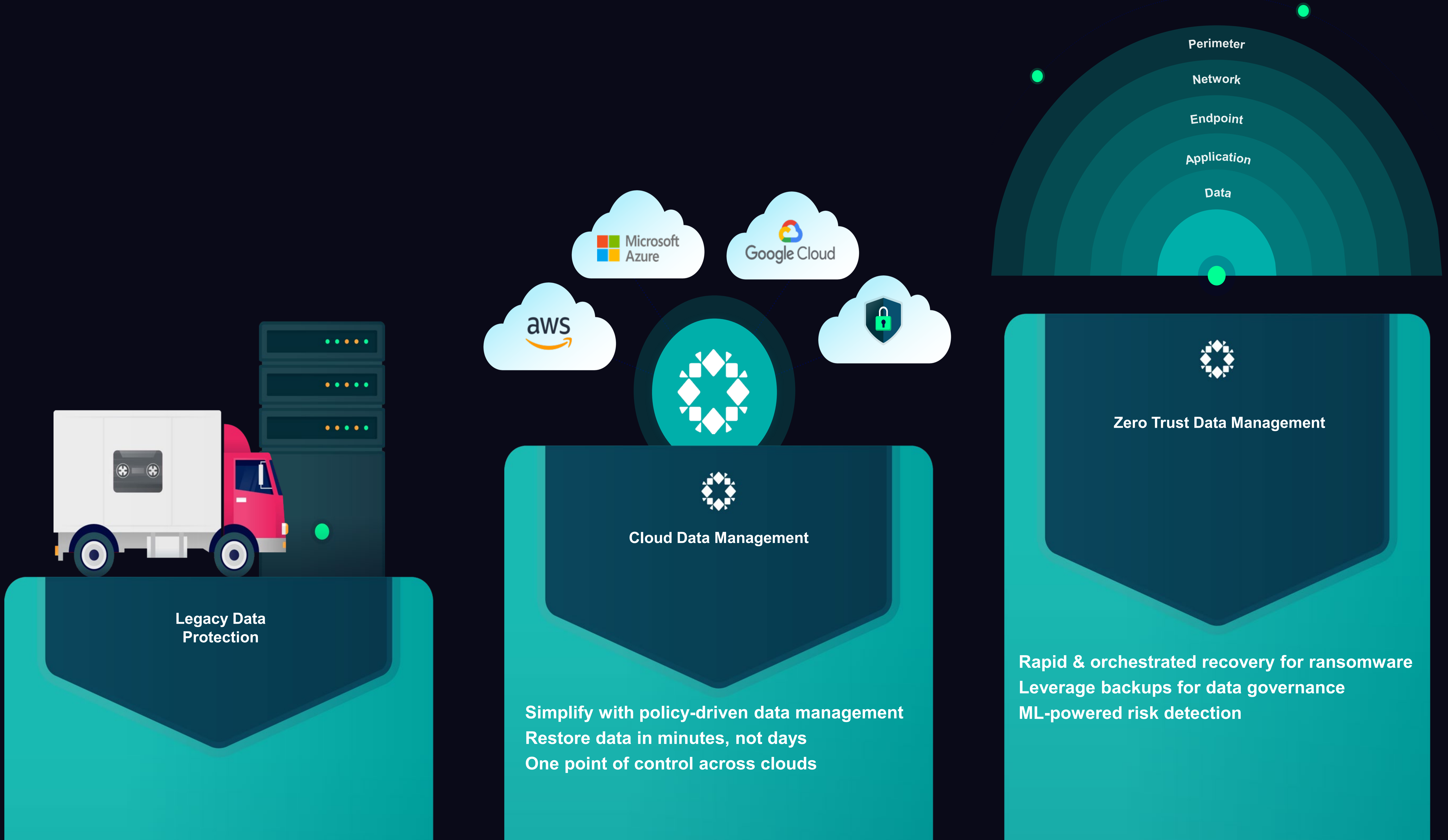
✓ Backup data is scanned for sensitivity to answer ‘was sensitive data in scope’?

✓ ML based anomaly detection integrated into SIEM / SOAR security platforms

✓ User access and abnormal user behavior coming this summer

rubrik

ZERO TRUST DATA MANAGEMENT



Legacy Data Protection

Cloud Data Management

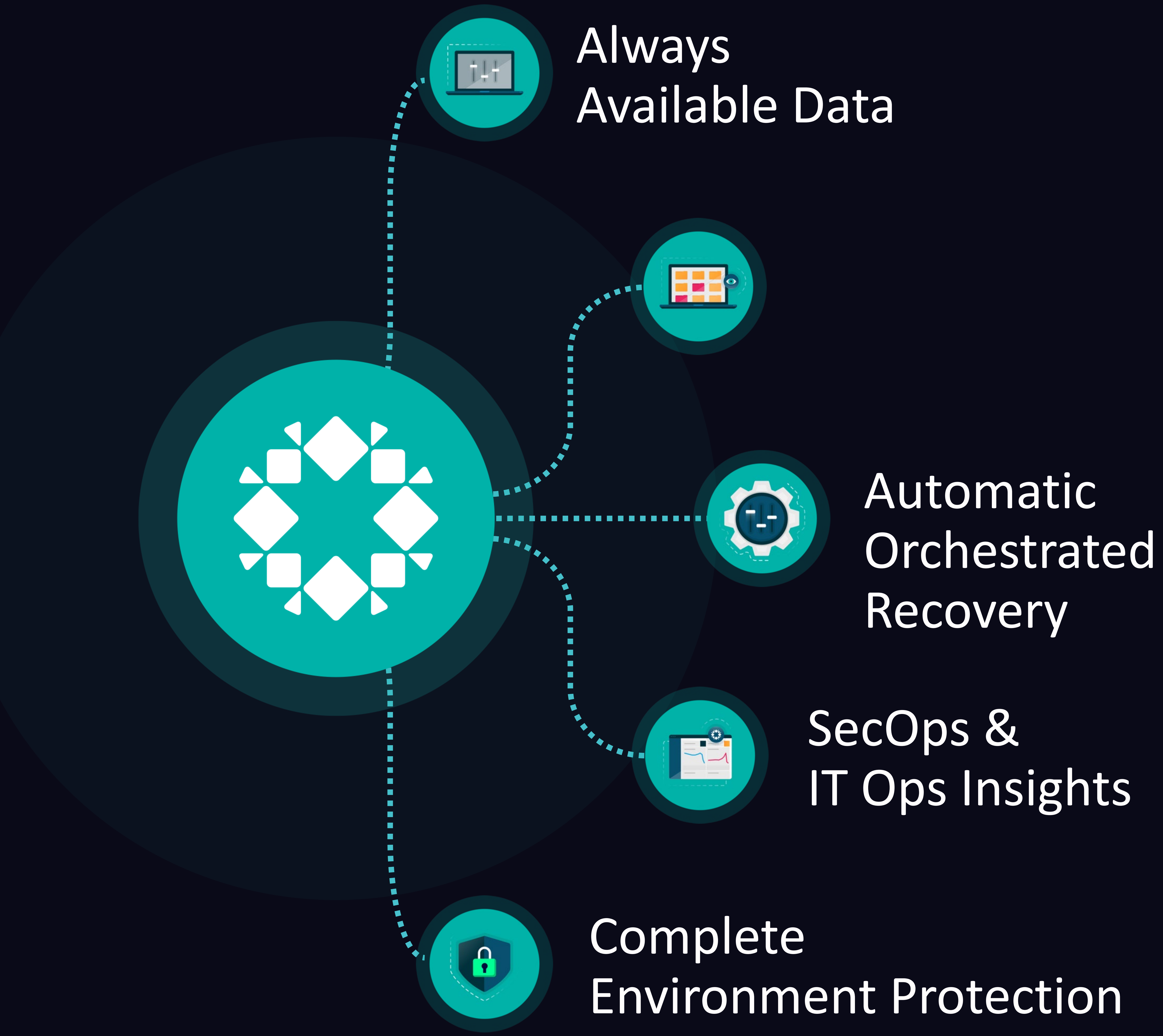
Simplify with policy-driven data management
Restore data in minutes, not days
One point of control across clouds

Zero Trust Data Management

Rapid & orchestrated recovery for ransomware
Leverage backups for data governance
ML-powered risk detection

rubrik

RUBRIK REIMAGINES
DATA MANAGEMENT & DATA SECURITY



Always Available Data

Automatic Orchestrated Recovery

SecOps & IT Ops Insights

Complete Environment Protection

rubrik

Customers Winning the Fight

“Ransomware cannot comprise our backups.”

– CITY OF DURHAM

“Rubrik helped us quickly recover 100% of the systems it was protecting.”

– KERN MEDICAL CENTER

“Rubrik significantly reduces the time to resolution for potential security incidents.”

– DUNN LUMBER

“Rubrik helps us identify if data was exposed in a data exfiltration attack.”

– CANTERBURY CHRIST CHURCH UNIVERSITY

“Rubrik drove over 90% operational savings by eliminating manual [processes].”

- CITY OF SIOUX FALLS

rubrik cStor

Questions?

rubrik

cStor

We look beyond IT

Thank You!