Ransomware Resilience

Building a Robust Defense Against Cyber Extortion

MicroAge®

rubrik | Zero Trust Data Security™

Ransomware Resilience

Building a Robust Defense Against Cyber Extortion

Areas of Risk	Immutability – Real vs Marketing	Recovery is Prevention	Cyber Insurance Trends	Call to Action
• Where is your company is most vulnerable for an attack?	• What is “immutable data”	• Prevention and Recovery Strategies	• Cyber Insurance coverage for ransomware	• Key takeaways

Ransomware Resilience

Building a Robust Defense Against Cyber Extortion

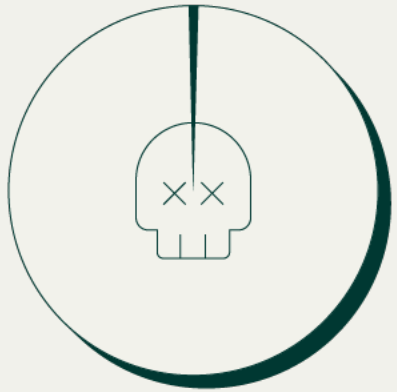
Areas of Risk

- Where is your company is most vulnerable for an attack?

THREATS ARE EXPANDING AND PREFER THE CLOUD

99%

of IT and security leaders were made aware of at least one attack in 2022. On average, **leaders dealt with attacks 52 times in 2022.**



59% experienced a data breach

54% BEC or fraudulent transfer

40% encountered ransomware

THREATS ARE EXPANDING AND PREFER THE CLOUD

Expel reported a 70% increase in malicious events in the three major public clouds

from 2021 to 2022

100%

Permiso reported 100% of their cloud investigations were the result of a compromised credential

Rubrik Zero Labs

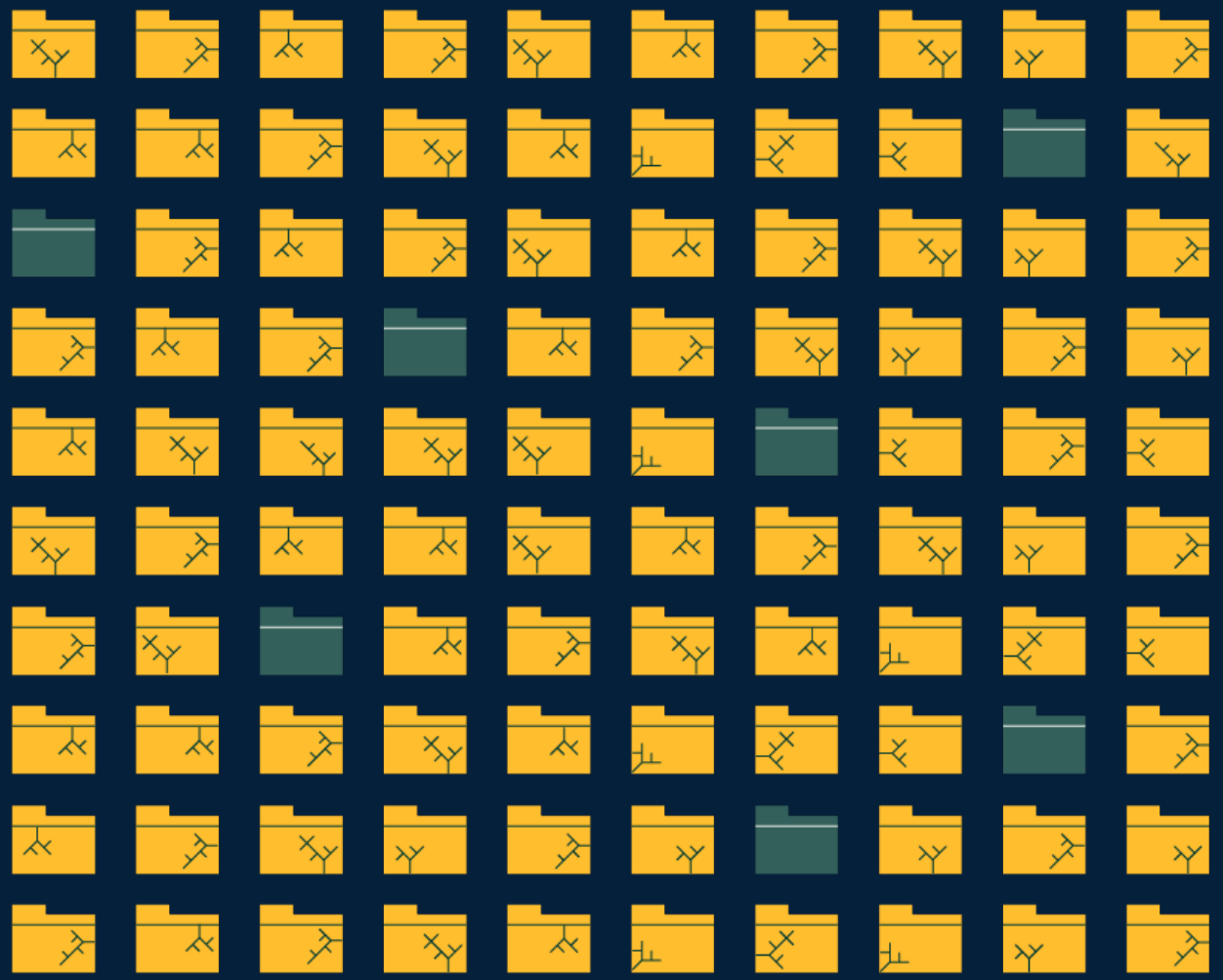
Don’t forget your backups...

99%

of organizations reported having a backup and recovery solution

HOWEVER 93%

encountered significant issues with their solution



Rubrik Zero Labs

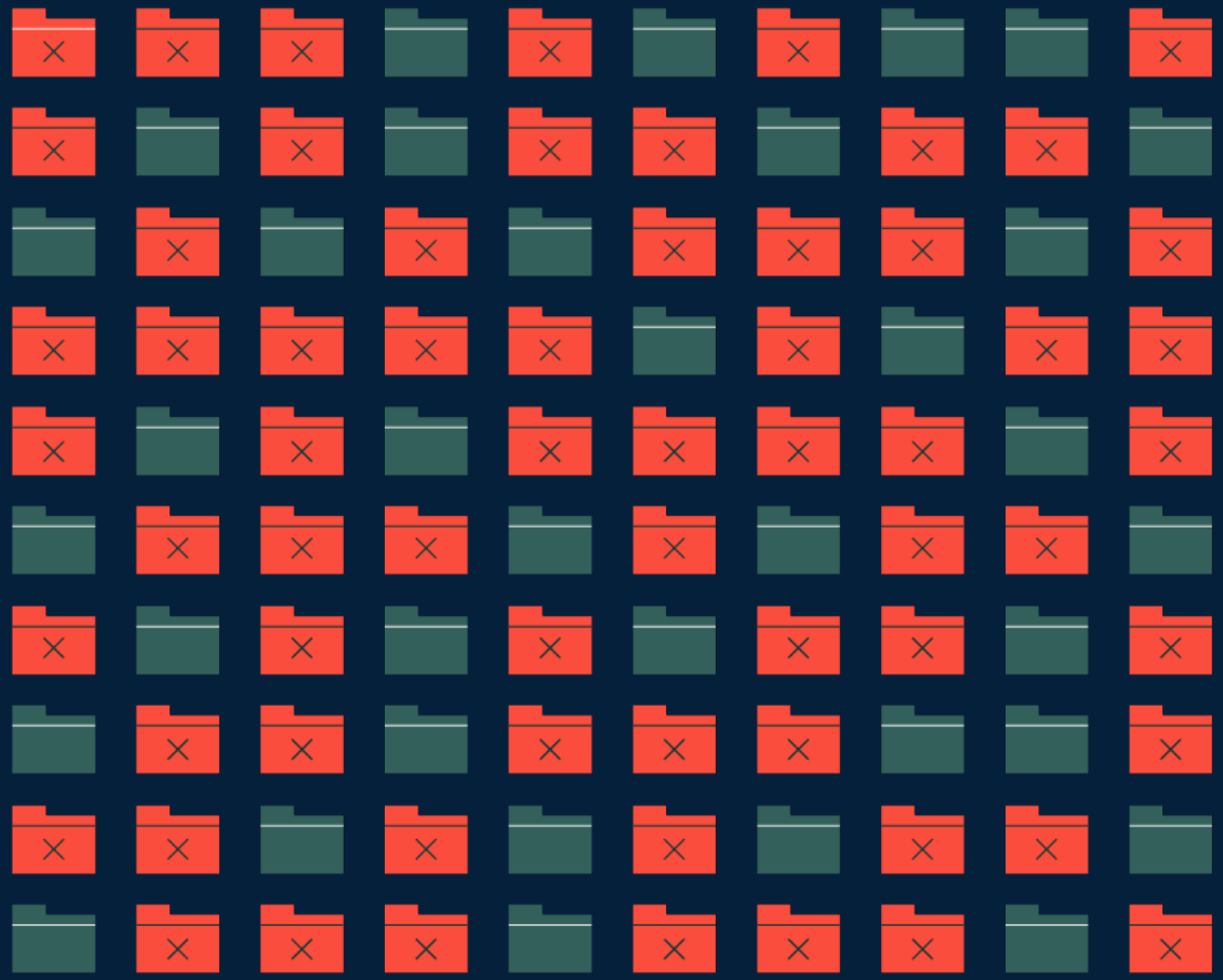
Don’t forget your backups, the bad guys remembered

93%

of organizations reported malicious actors attempting to impact data backups

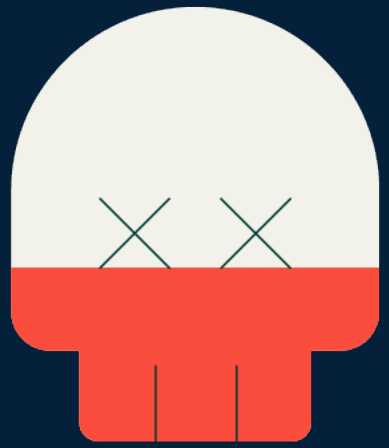
AND 73%

of these efforts were at least partially successful



Rubrik Zero Labs

HOW PREVALENT IS RANSOMWARE?



40%

of external organizations reported a successful ransomware intrusion

75%

Rubrik identified anomalous activity at 75% of organizations

18%

of all Mandiant incident response engagements were ransomware

11%

of all Expel SOC analysis was tied to ransomware

48%

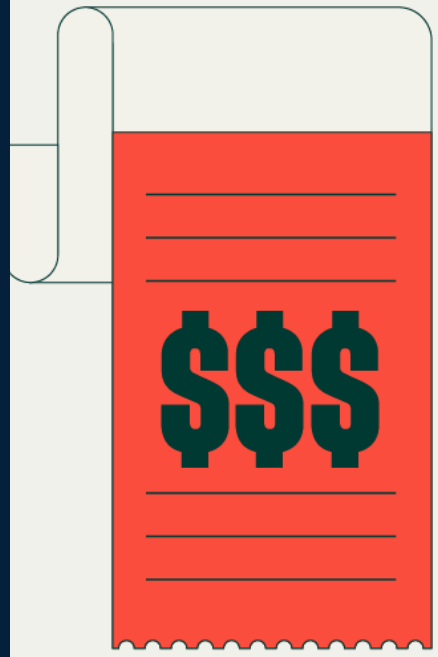
of these organizations observed some form of ransomware attempt

15%

of these organizations encountered some form of successful encryption event

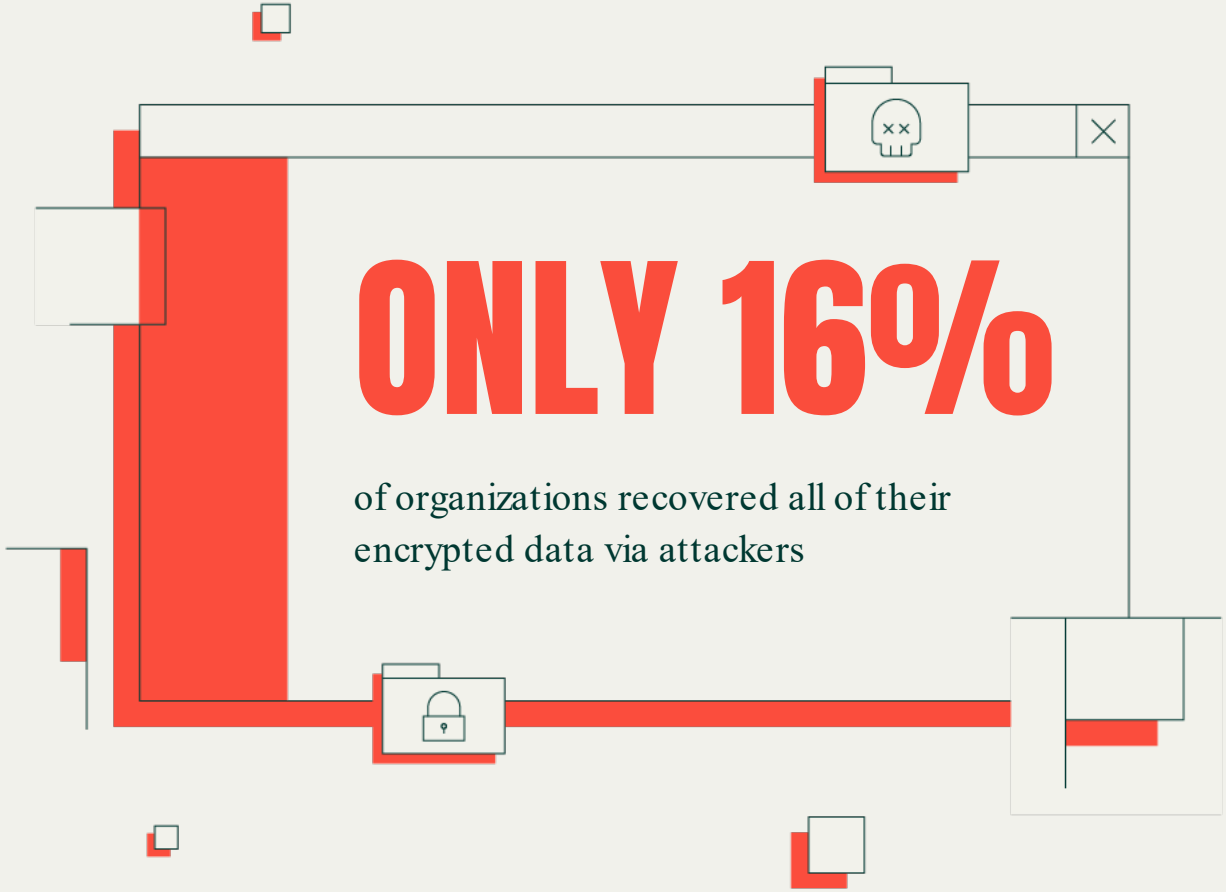
Rubrik Zero Labs

PAYING A RANSOM ISN'T THE END EITHER



72%

of external organizations reported paying a ransom



ONLY 16%

of organizations recovered all of their encrypted data via attackers

39%

paid a ransom demand to prevent data leaks

40%

paid a ransom due to encryption events

46%

of organizations paying a ransom recovered half or less of their data via the attacker

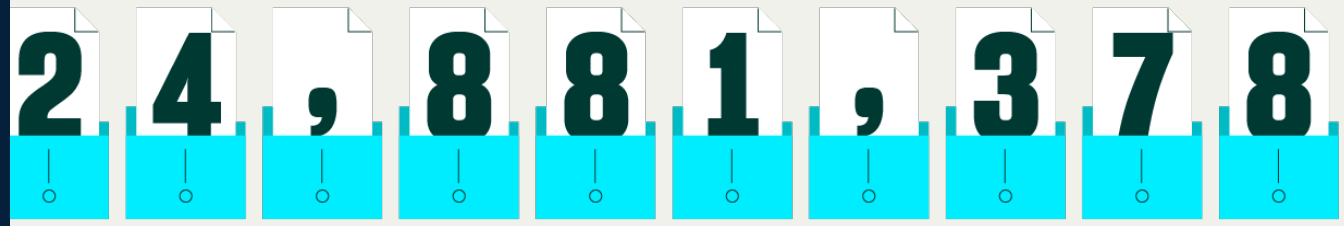
Rubrik Zero Labs

SHIFTING DATA PRESENTS REAL ORGANIZATIONAL RISK

A typical organization has:

files containing sensitive data

and



sensitive data records

1 of every 38 files contains sensitive data globally

Applied penalties to a typical environment:

GDPR Less than one Euro per record or less than four Euro per file = 20 million Euro maximum

---

HIPAA $1.5 million max at $ 50 minimum = 30,000 items

CPRA $2,500 per file = $1.4 billion

Rubrik Zero Labs

INTRUSIONS AFFECT OUR PEOPLE

98%

of IT and Security Leaders reported significant emotional and/or psychological impacts due to cyberattacks in 2022:

53% increased anxiety pertaining to daily tasks

46% worry over job security

43% are concerned about loss of trust amongst colleagues and team members

41% have loss of sleep or trouble sleeping

INTRUSIONS AFFECT OUR BUSINESS

93%

of external organizations encountering a cyberattack experienced a negative impact

49% Loss of customers

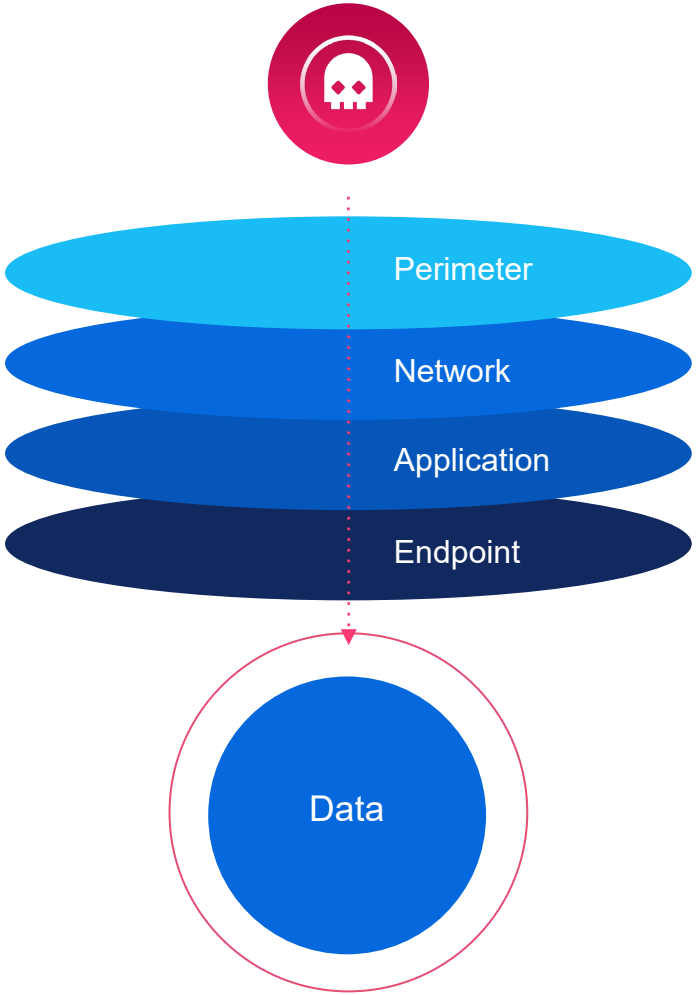
45% Revenue loss

44% Negative press and/or reputational damage

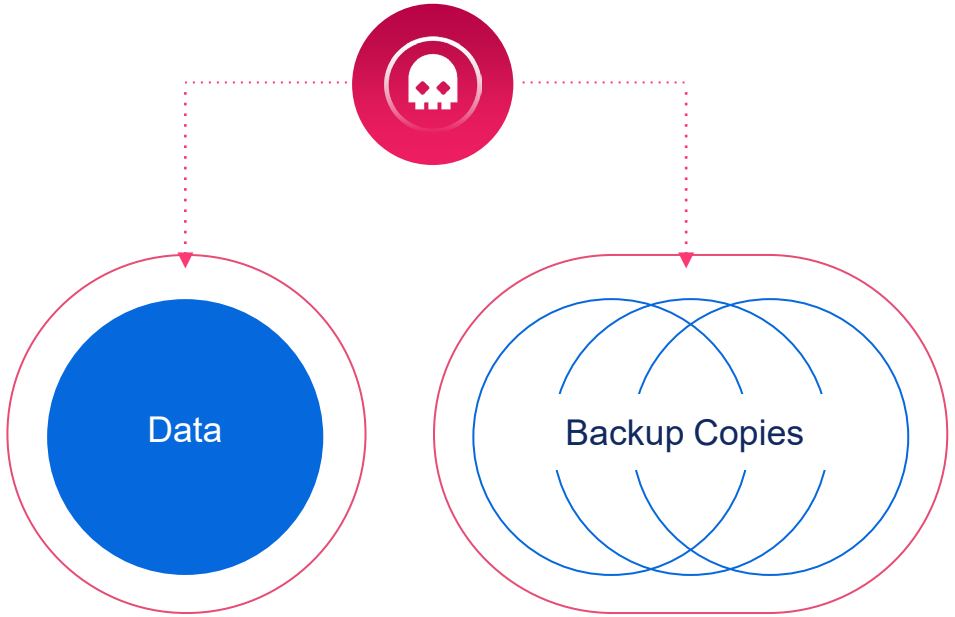
5% Stock negatively impacted

Businesses Are Under Attack

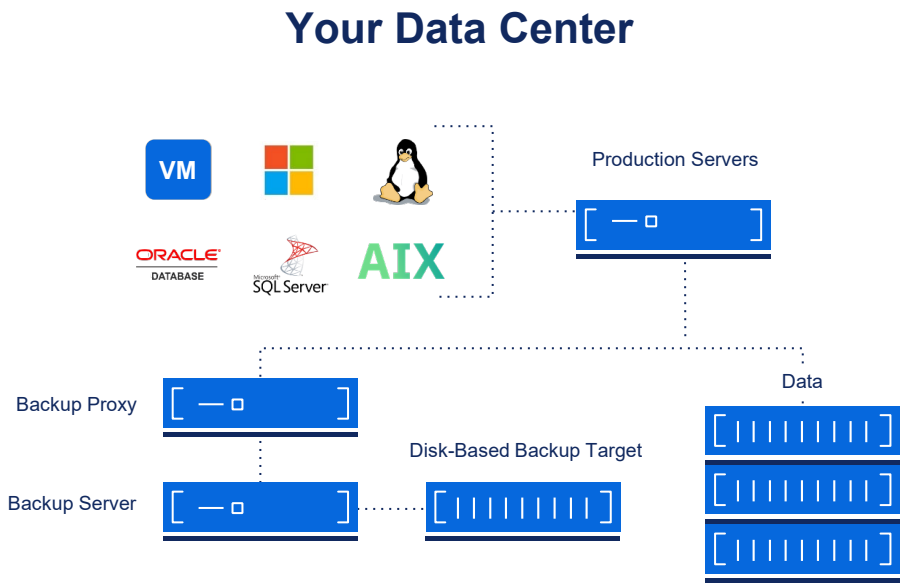
"Assume Breach"



Data and Backups are the targets, most often through credential exposure and admin escalation



Is Your Data an Easy Target?



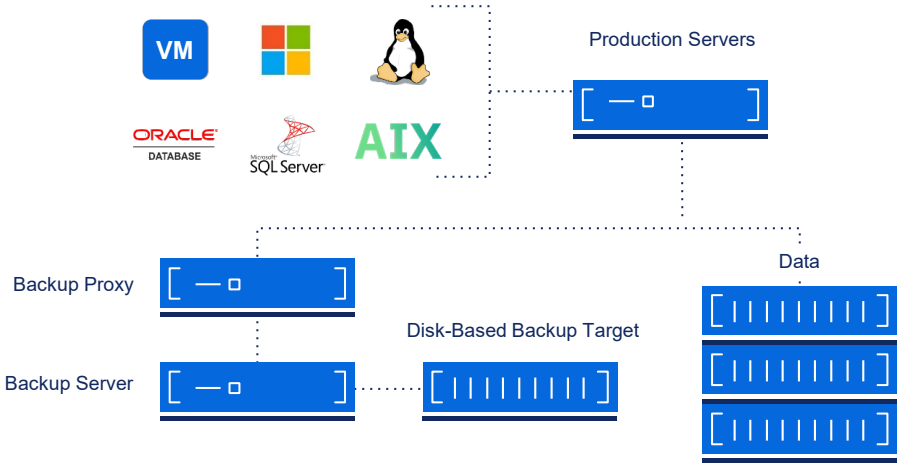
Not designed for adversary behind the firewall

- Are 100% of your backups immutable?
- Is your backup infrastructure physically isolated from the environment it's protecting?
- Does the backup infrastructure run in VMs?
- Is any part running Windows?
- Is MFA & retention lock enforced?

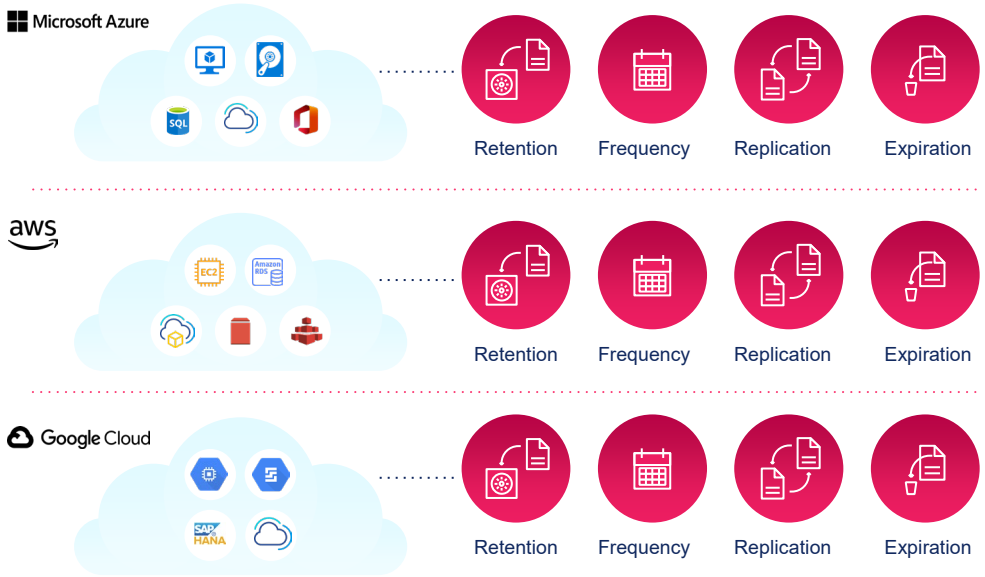
If not, you most likely will have nothing to recover.

Is Your Data an Easy Target?

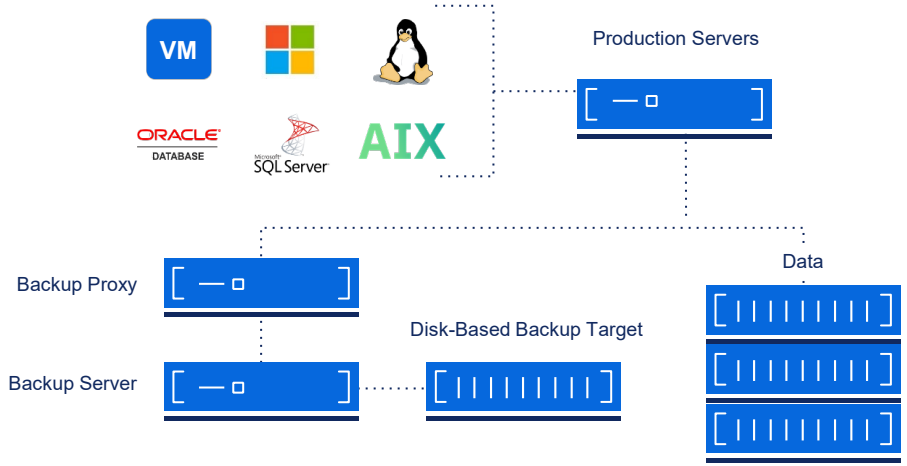
Your Data Center

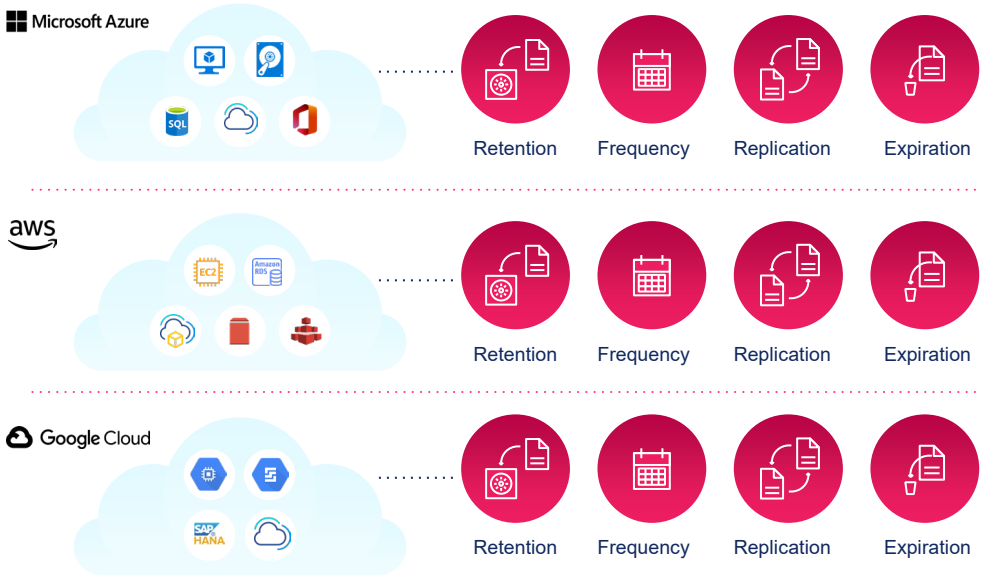


Your Cloud(s)



Backup ≠ Cyber Recovery





New Questions

- What exactly do I recover?
- Was sensitive data in scope?
- How do I ensure I don't restore the malware?

Now Board/C-Suite Priority

- Are we good?
- Can you prove it?
- How long will it take?

Why Are Organizations Stuck Paying Ransoms?

Ransomware locks down data

Option 1: Pay ransom

Option 2: Attempt to recover

Engage IT Ops

Engage SecOps

Is My Data Recoverable?

Has Sensitive Data Been Compromised?

What's the Scope of the Attack?

Can We Prevent Reinfection?

Can We Recover Quickly?

PAY RANSOM / HOPE FOR BUSINESS RECOVERY

Requirements to Mitigate Risk

Infrastructure Security

Data Security

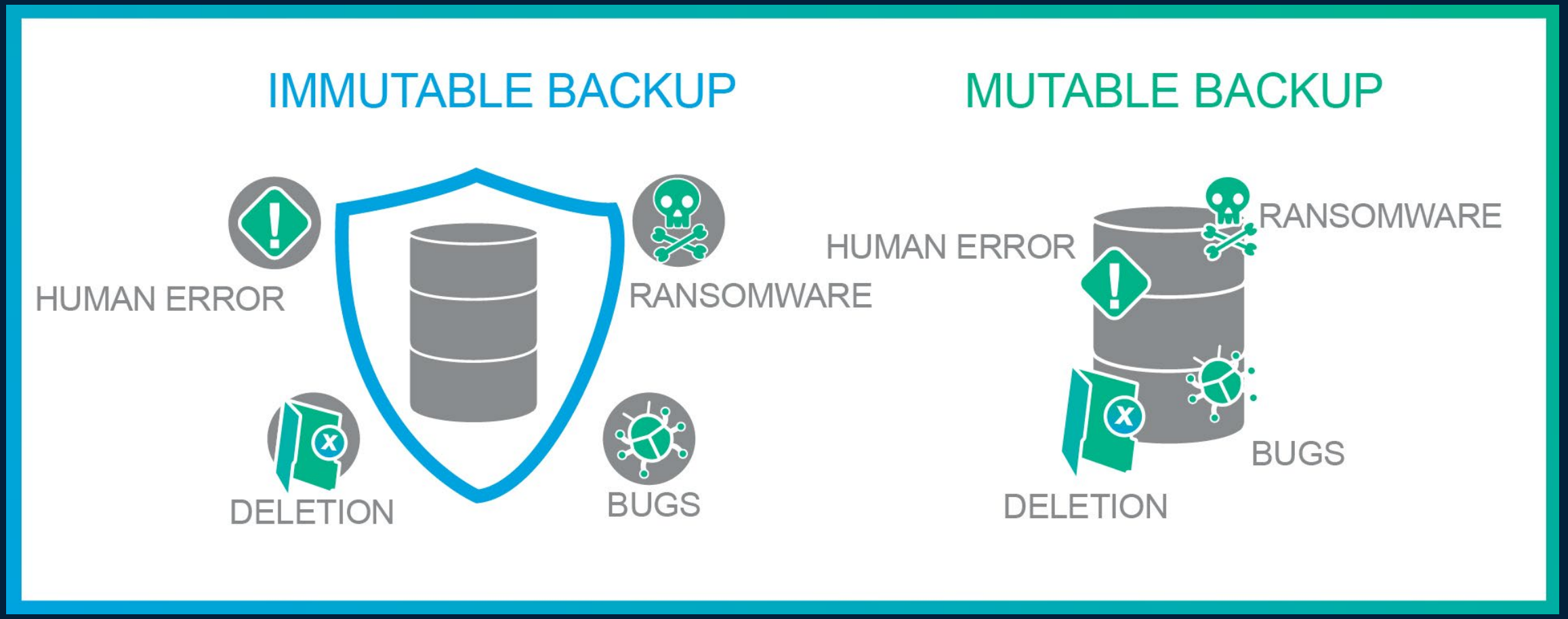
Ransomware Resilience

Building a Robust Defense Against Cyber Extortion

Immutability – Real vs Marketing

- What is “immutable data”

What is an immutable backup?



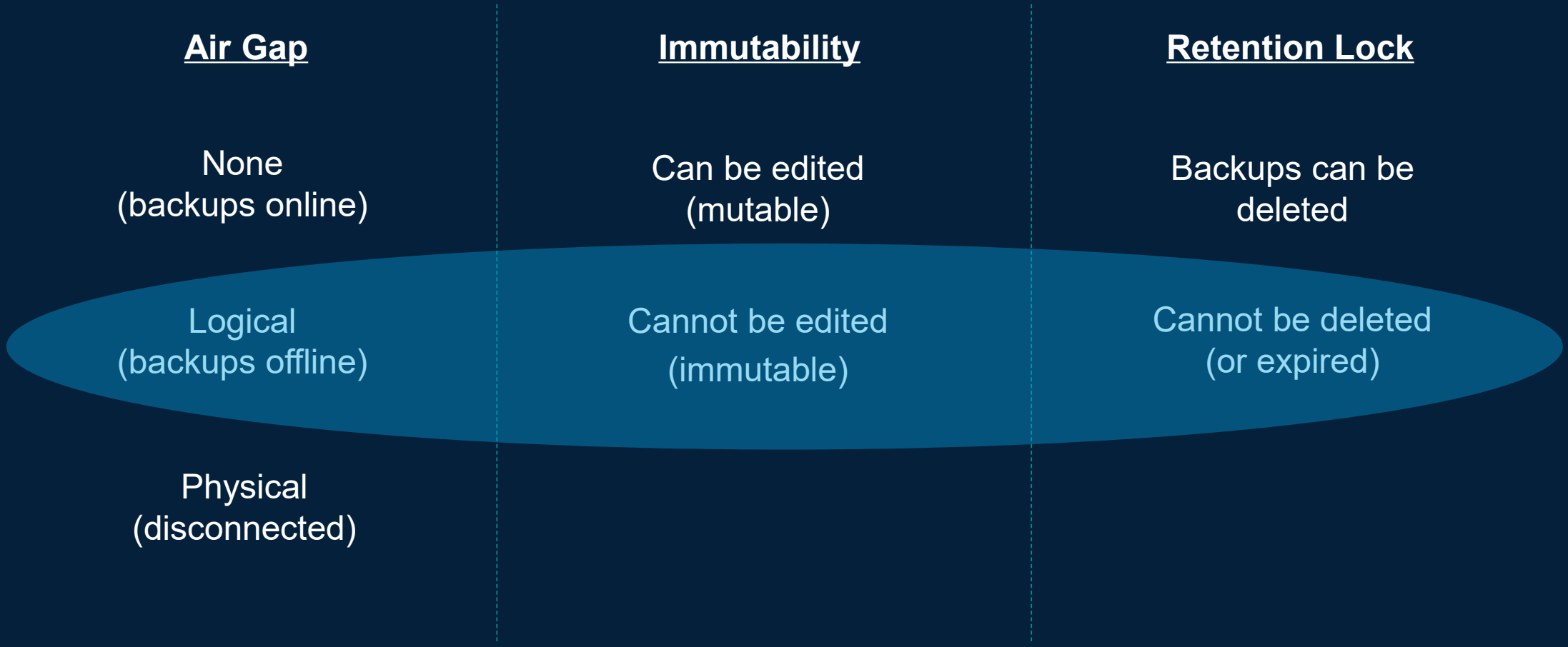
Immutable By Design

- On by default or on by configuration – No matter the vendor, turn on today!
- Risk Mitigation of Data Loss – immutability is only as secure as the platform it sits on
  - Storage Protocols – limit access, connection, update versions (NFS, SMB)
  - NTP Poisoning (advancement of deletion)
  - User Access (MFA, 2 Person Rule, limit access for admin – Active Directory risks)
  - Metadata Design (stored with file data?)
  - Communication Protocols (NFS, SMB, S3) – Encryption, access, management, Logical Air Gap
- Measure, Audit, Report
  - On-premises, Cloud, SaaS (M365, etc)

Everything can be secured, but what is the overhead of doing so? How heavy is the administrative and audit lift?

Who owns the responsibility for immutability?

Key Principles of Data Protection



rubrik

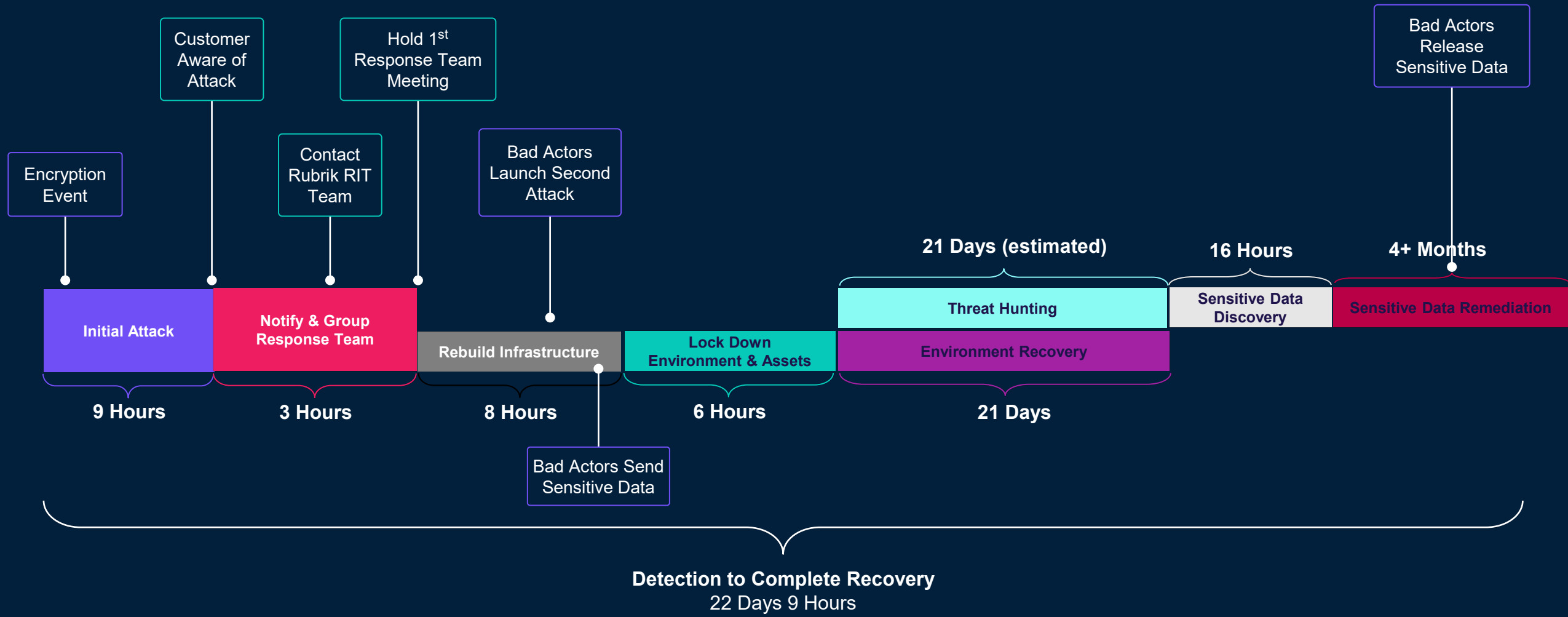
Ransomware Resilience

Building a Robust Defense Against Cyber Extortion

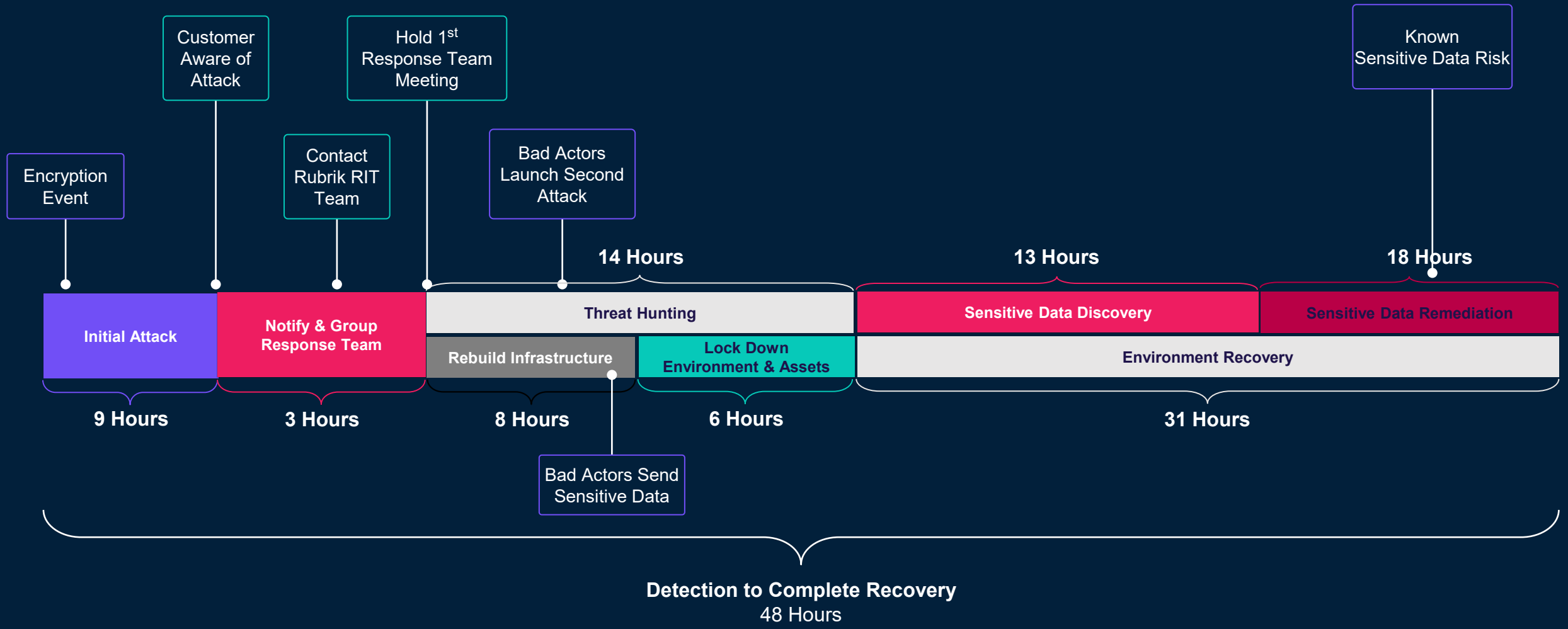
Recovery is Prevention

- Prevention and Recovery Strategies

Recovery Without Preparation as Prevention



Recovery With Preparation as Prevention



Prevention in an “Assume Breach” World

- Preserve against data loss (native immutability preferred)
- Secure access and control
  - Converged, secure solution design
    - Hyper-converged, isolated, API-only, encryption everywhere
  - Environmental controls
    - MFA/SSO, 2PR, local admin preference (least privilege),
    - NTP protection, logical airgap, API-based protocols
  - Regular security audit of data protection solution
  - Simplicity of management
    - Single code-base, limited third-party integrations (API, webhook preferred) - Log4j!
    - Streamlined, global administration – policy and API-driven

If peace time is complex, what will war time look like?

Prevention – Adding Observability

- Understanding critical business risks without impacting production!
  - Sensitive data discovery shared with DLP solutions for exfiltration prevention
  - Automate activity detection – file and user
  - Automate anomalous activity detection (defense in depth)
  - Threat scanning for Indicators of Compromise
  - Integrations with SIEM and SOAR solutions

Active vs passive value: Risk reduction IS active business value.

Recovery – Moving Prevention into Action

- Understanding the Blast Radius of an attack
  - Prevent the recovery/investigate/fail/repeat loop
  - Quarantine compromised data before recovery
  - Know what data and from when to recover to minimize business impact
  - Understand sensitive data exfiltration risk
- Practice Capabilities
  - Testable, repeatable prepared and on-the-fly recovery
  - Capability of recovering to new infrastructure quickly
- Vendor Partnerships
  - Ransomware Response Teams – white-glove support in challenging moments
- MicroAge Partnership
  - Strategic review of playbooks, solutions, process

Assume breach always. Move to the “left of boom”.

Ransomware Resilience

Building a Robust Defense Against Cyber Extortion

Cyber Insurance Trends

- Cyber Insurance coverage for ransomware

Cybersecurity Insurance Trends

- Claims are up 430% since 2012
- Requirements for Underwriting Standards are growing (MFA, EDR, Patching Cadence, EoL SW/HW, Backups, least privilege)
  - Backups
    - Immutability
    - MFA
    - Separate credentials
    - Rapid RPOs and short RTOs
    - Encryption, airgap (logical/physical), offline archive
    - Testing of restoration/recovery E6M or E12M
    - Ability to test integrity
- Proving immutability and other standards is a growing compliance/audit requirement
- Meeting strict standards can lead to slower growth in cost and/or reductions
- CFOs are bringing in CIO and CISO organizations into cybersecurity insurance negotiations with insurers and brokers
- Cybersecurity brokers are looking to understand best of breed vendor solutions for recommendations

Ransomware Resilience

Building a Robust Defense Against Cyber Extortion

Call to Action

- Key takeaways

Summary

Building a Robust Defense Against Cyber Extortion

Prevent data loss as a baseline

- Simple to manage, immutable, and security-first architecture
- Minimize exposure risks of underlying, legacy architecture
- Minimize command and control risks (IAUTH, least privilege)

Maximize observability before and after attack

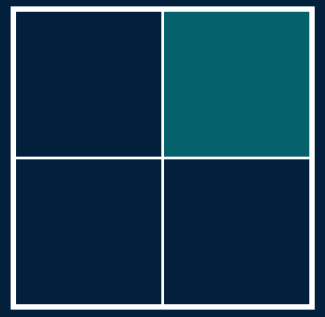
- Compliance and monetary risk with data exfiltration – know what is where, when it changes, and how user access changes
- Enhance pre and post attack intelligence, SIEM/SOAR integration

Minimize recovery time

- Utilize tools to simplify blast radius detection and quarantine
- Practice recovery in a repeatable, adjustable, and audit-capable manner
- Engage vendor/s in partnership for cyber recovery best practices

Rubrik recognized as leading innovator

Gartner®



Magic Quadrant Leader

Furthest to the Right in Vision

FORRESTER®

WAVE LEADER

Strongest in Overall Strategy

Forbes

THE Cloud100

Six Years Running