# Practical Cyber Resilience

## Affordable, Meaningful Risk Reduction

Bringing together people and process for faster recoveries

# We've All Seen The Headlines

**Cancer treatments cancelled after Canadian hospitals hit by ransomware attack**

Graham CLULEY
November 08, 2023



**Canadian hospital handles ransomware attack**

Ottawa hospital restored its computers after wiping their hard drives

**Hospitals in Maine, New Hampshire lim after cyberattack on Catholic health org**

A cyber-attack that affected more than 60 trusts within the United Kingdom's National Health Service (NHS) has spread to more than 200 000 computer systems in 150 countries, including Canada. One hospital in Ontario — Lakeridge Health in Oshawa — reported that its computer system was threatened by the ransomware. The hospital's antivirus software contained the threat, however, and patient care and access to health records were not affected.

**Ransomware attack contributed to patient's death, says Britain's NHS**

Investigation into hospital cyberattack determines some patient data accessed

By Dean Shalhoup Union Leader Correspondent Jul 14, 2025 Updated Jul 15, 2025

Source: Recorded Future

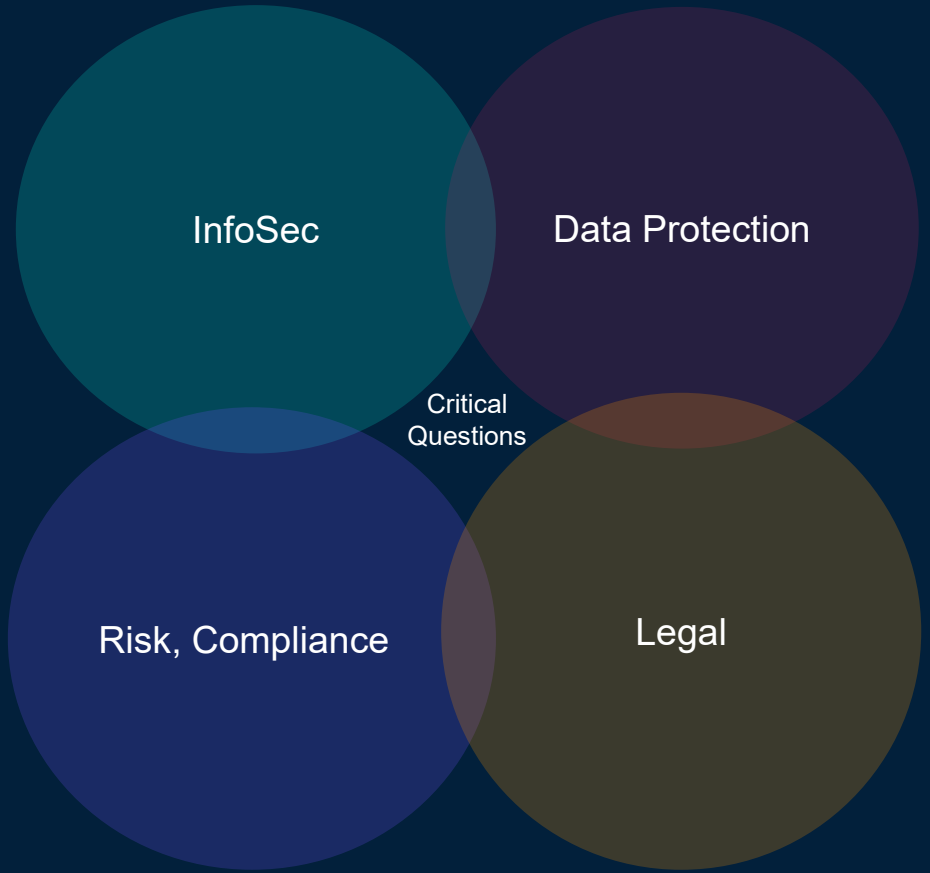
# The Status Quo

## Weeks to Months

Operations down, patient impacts, and financial losses

| Time to first notification of an attack in progress | Notify & gather response team | Provision recovery environment | Restore copies and script threat hunts | Manual malware quarantine | Manual restore of applications without automation | Manual, estimated sensitive data discovery | Reactive, manual sensitive data remediation |
|---|---|---|---|---|---|---|---|
| No threat monitoring | No contingency communications methods, plan | No existing IRE, lack of spare equipment | Manual scripting in restored data | Care to avoid reinfection slows work | Constant triage to determine where to focus recovery efforts | Lengthy, uncertain process | Begins setup for next breach, no continuing automated process |
| | Inability to Recover Collab | Inability to Recover Identity | | | | | |

# Why Is Cyber Resilience Hard?



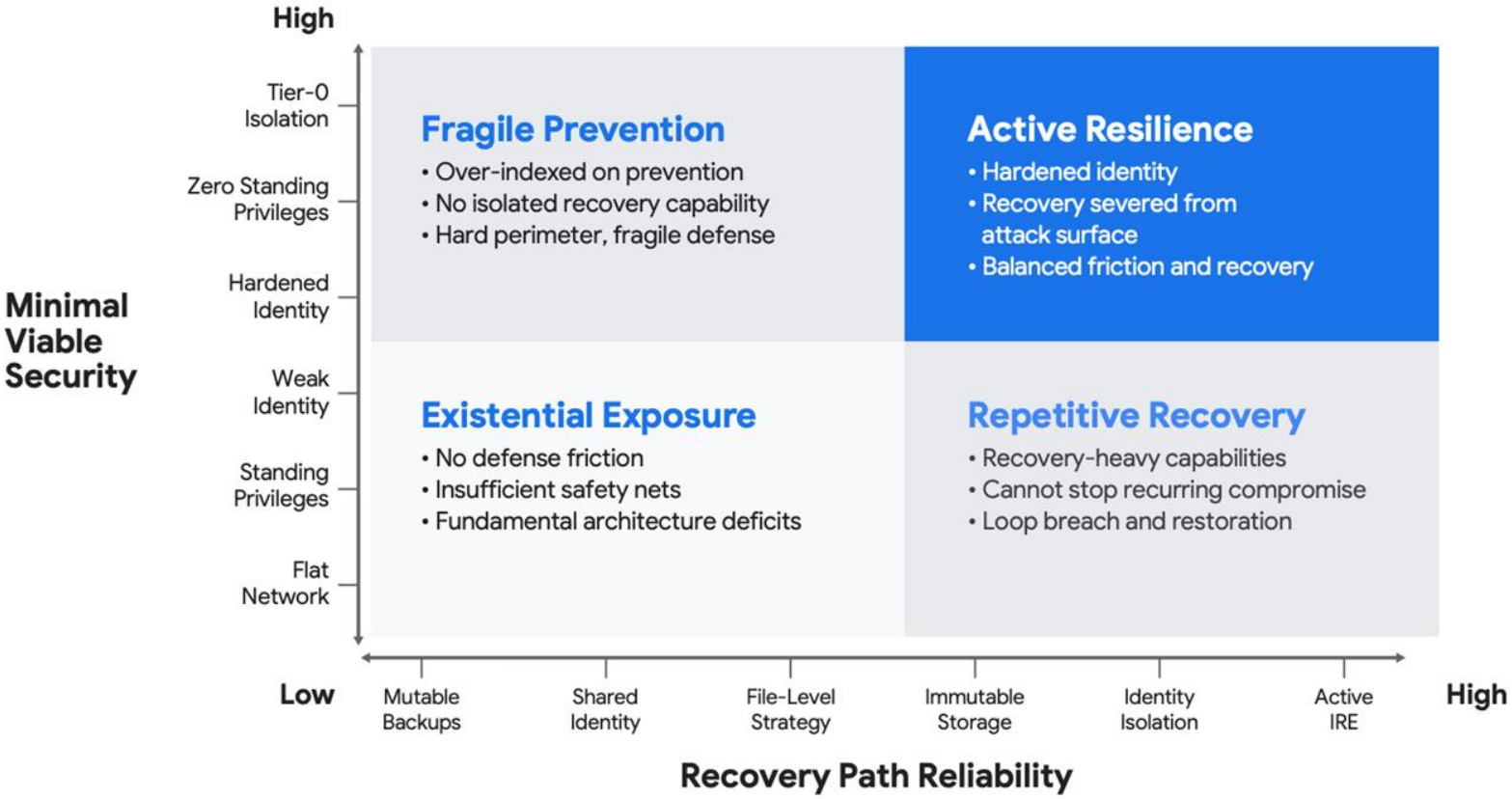
# Selling *Cyber Resilience*


## The Resilience Maturity Matrix

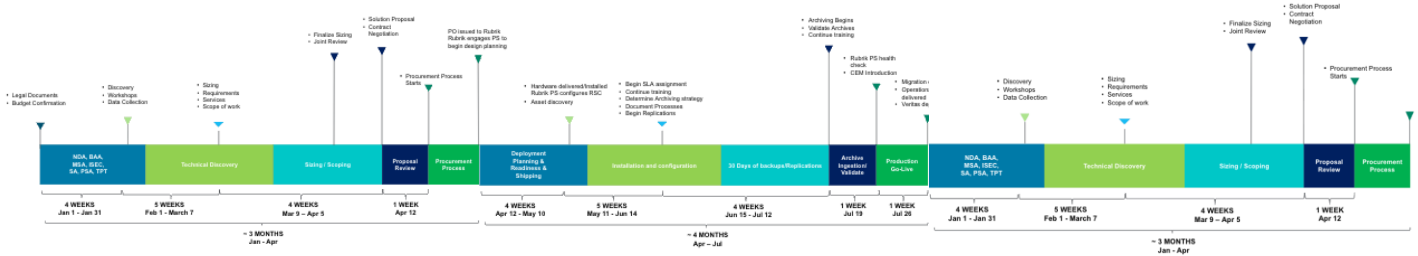
Resilience is not a single metric; it is the product of **prevention** and **recovery**. Prevention can be measured as the degree of friction a threat actor experiences

adversaries to move unimpeded within the environment, while the absence of offline safety nets ensures that the recovery environment is likely destroyed alongside production. The outcome is often severe; recovery is statistically unlikely without acceding to extortion demands, and even then, success is not guaranteed.

Active Resilience is the target state, characterized by balanced friction and trusted recovery. The adversary is slowed by hardened identity controls, and the recovery fabric is architecturally severed from the attack surface. In this state, attacks are degraded from existential crises into containable incidents. The organization retains the authority to refuse extortion demands, secure in the knowledge that their recovery path remains untainted.


High
Minimal Viable Security
Tier-0 Isolation
Zero Standing Privileges
Hardened Identity
Weak Identity
Standing Privileges
Flat Network
Fragile Prevention
• Over-indexed on prevention
• No isolated recovery capability
• Hard perimeter, fragile defense
Active Resilience
• Hardened identity
• Recovery severed from attack surface
• Balanced friction and recovery
Existential Exposure
• No defense friction
• Insufficient safety nets
• Fundamental architecture deficits
Repetitive Recovery
• Recovery-heavy capabilities
• Cannot stop recurring compromise
• Loop breach and restoration
Low
Mutable Backups
Shared Identity
File-Level Strategy
Immutable Storage
Identity Isolation
Active IRE
High
Recovery Path Reliability

# Risk Reduction Timeline



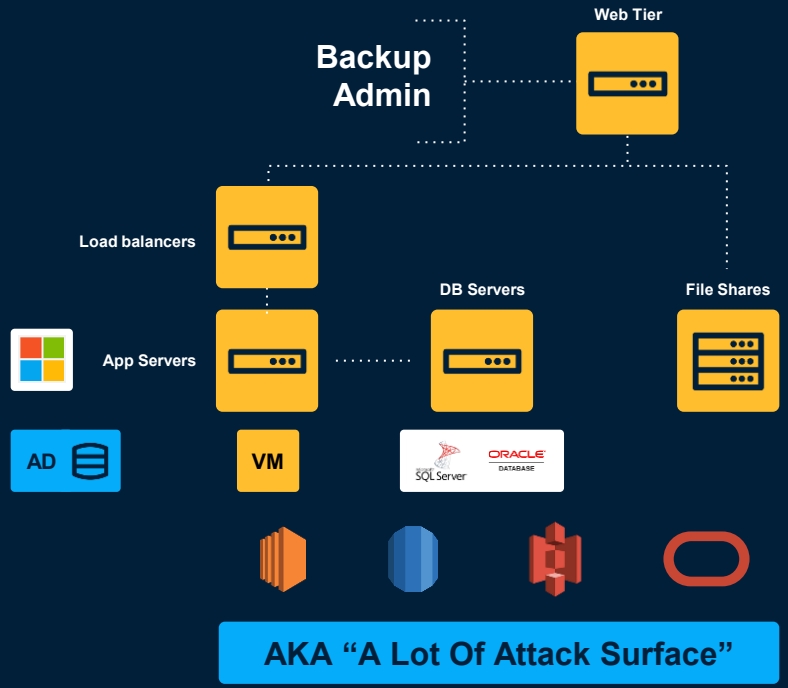

Procurement produces a PO

Deployment produces a running thing.

Operationalizing produces risk reduction.

# Q: Can We recover?

## Will your data protection stand up to targeted, prolonged attack by professionals?




**93%** of external organizations reported malicious actors attempting to impact data backups during a cyberattack.

**73%** said the attempts were at least partially successful.

### Not designed for an adversary behind the firewall

- Are there open network protocols?
- Is anything running windows?
- How much of it is virtualized?
- Is MFA and TOTP deployed and enforced?
- Does it depend on NTP?
- Can a single administrator change policies?

# “Immutability”

“*We* don’t change the data once it’s written.”

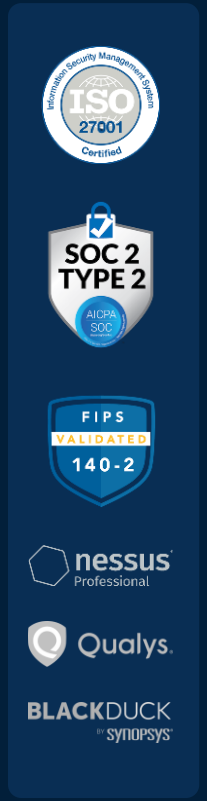
“You can configure our solution to be resilient.”

“It’s immutable. . . IF you put another copy elsewhere behind yet another, more magical firewall and keep it disconnected most of the time.”

rubrik

**Your data and backup solution from Rubrik WILL survive the attack and you’ll be able to recover everything, and do it much more quickly than with any other tooling.**

# Why Rubrik Survives an Attack




- Quorum Authorization, Retention Lock
- External MFA & Extremely Granular RBAC
- Always On Built-in MFA & TOTP
- NTP Protection, Monotonic Clock
- End-to-End & D@Rest Encryption
- Append Only File System
- Minimal, Hardened Linux, No Default Creds
- Isolated, Converged HW

**Resistant to Insider Attack or Compromised Credentials**
- Quorum authorization for sensitive actions, levels of approvals
- Locked policies to ensure frequency and retention compliance

**Always On, Built-in MFA**
- Globally enforced using TOTP, no insecure email reset option
- Scan QR code with smartphone, secure any local or AD account in seconds
- Local account for recovery in event of attack (AD compromised)
- Multi-factor on all AD integrated logins, alerts/syslog for failed logins

**True End-to-End Encryption**
- Client to Rubrik & node to node with no performance impact
- In-flight TLS 1.2 SHA-512 hash & at-rest FIPS 140-2 L2 RSA 2048-bit key
- Key mgmt using TPM or KMIP for key rotation

**True Immutable File System**
- Nothing accesses storage - no OS, Shell, or GUI access
- Append-only
- No access by any other applications/vendors/code

**Hardened, Minimal OS**
- Hardened, stripped down Linux - no Windows
- Vendor patched
- No default vendor credentials

**Fully Isolated Hardware**
- IPMI/OOB Mgmt disconnected
- No reliance on any other infrastructure
- No virtualization/hypervisor

# Rubrik: Now an AHA Preferred Cybersecurity Provider

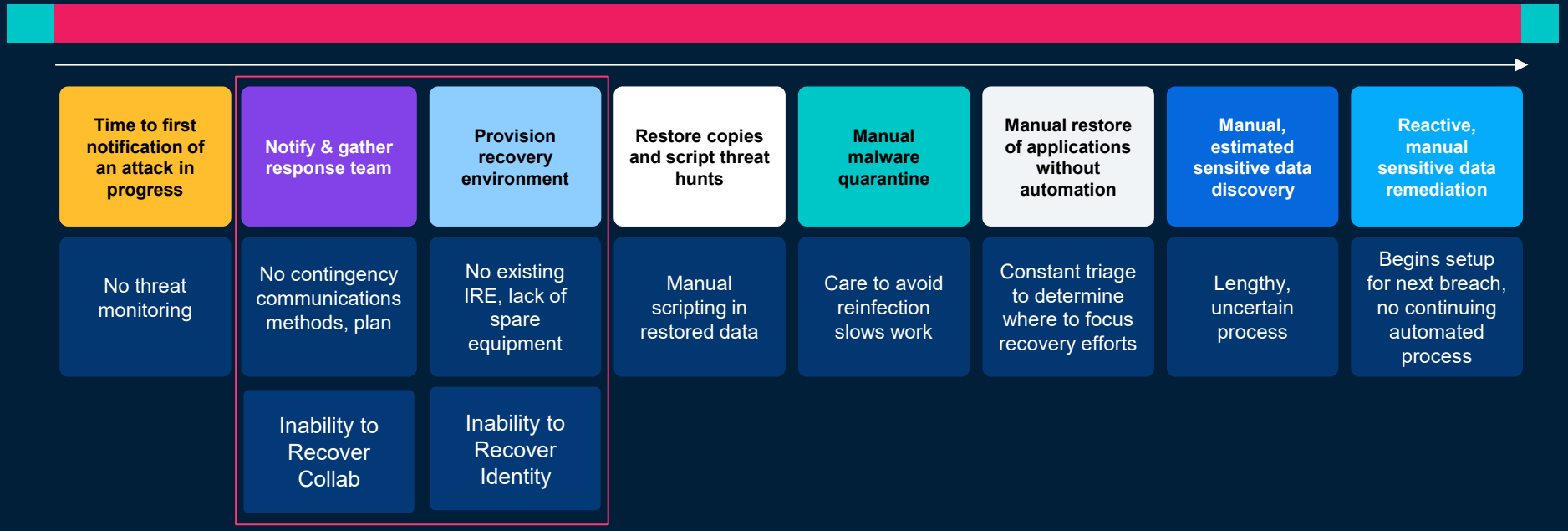

> *We can confidently recommend Rubrik as a reliable source of support for our nation's hospitals and health systems in their efforts to defend against sophisticated cyberthreats and ransomware attacks.*

**John Riggi**
*National Advisor for Cybersecurity and Risk*
American Hospital Association

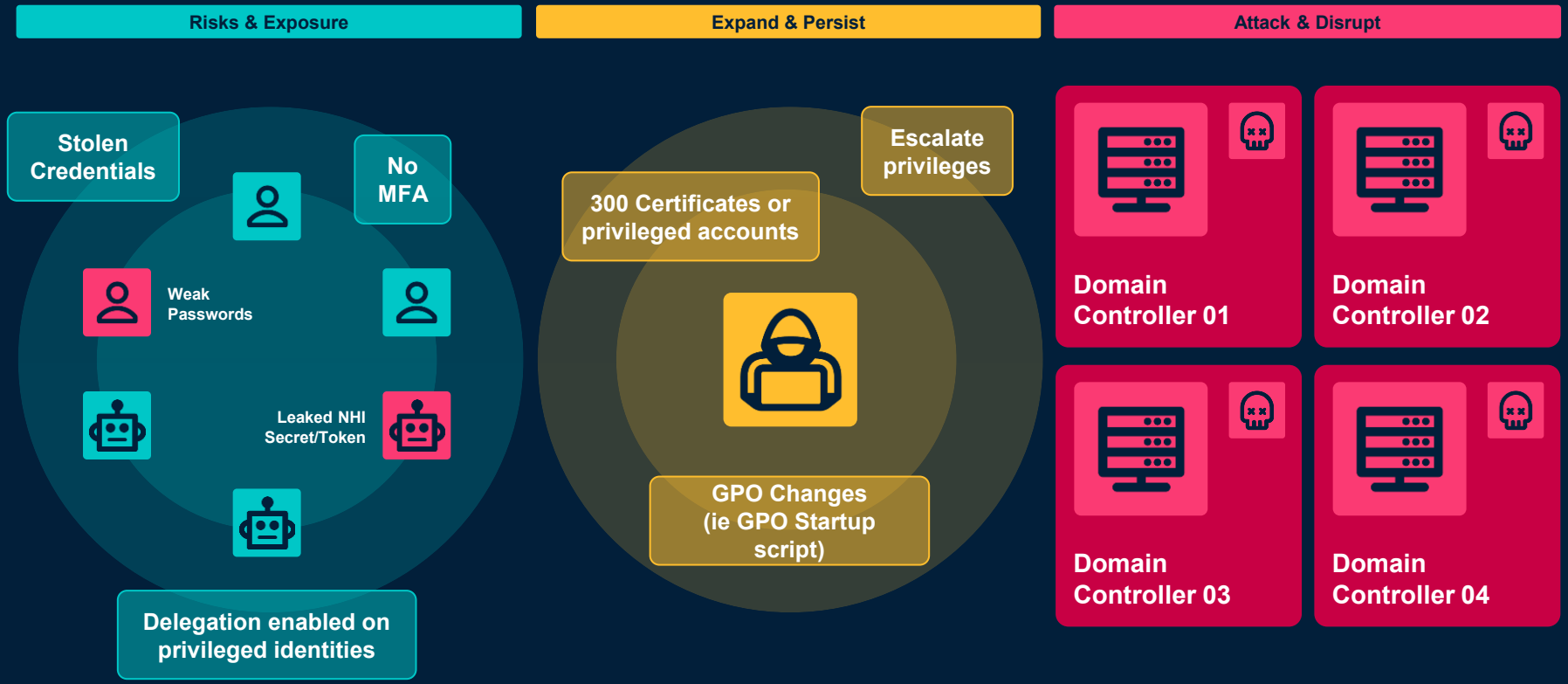
# Minimum Viable Hospital Foundations

## Weeks to Months

Operations down, patient impacts, and financial losses



# Anatomy of an Identity Attack



# IRE Options

## On-Premises IRE

**Pros:**
Maximum Control
Compliance
No Cloud Dependency

**Cons:**
High CapEx & OpEx
Lack of Scalability
More Complexity + You Manage

## Split DR IRE

**Pros:**
Very low cost
Rapid implementation
High flexibility

**Cons:**
Reduces DR protection
More Complexity + You Manage

## Cloud-Based IRE

**Pros:**
Elastic Scalability
Lower CapEx
Higher OpEx
Faster Deployment & Testing

**Cons:**
Mismatch of hypervisors
Requires Cloud Expertise

## Hybrid IRE

**Pros:**
Best of Both Worlds
Workload Flexibility

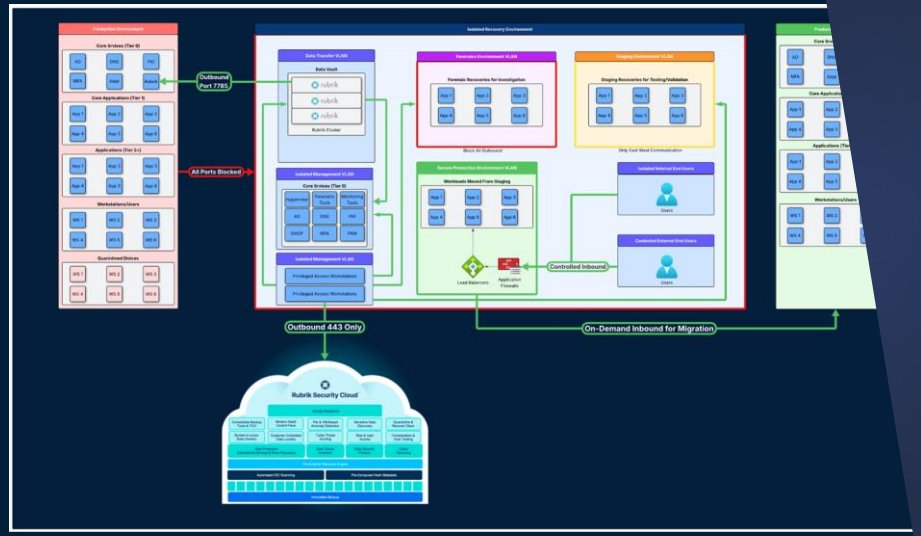
**Cons:**
Another vendor
Still expensive

## Application Specific IRE

**Pros:**
Optimized Recovery
Reduced Risk

**Cons:**
Limited Scope
Requires Deep App Knowledge

# Technical guides, Blueprints IRE Workshop




# MVH Foundations


## Identity

When the identity fabric is fundamentally compromised, such as via Windows NT directory service theft or AD Certificate Service forgery, the organization faces a systematic identity collapse. Defenders cannot simply reset passwords because the attacker possesses the cryptographic keys necessary to complete the reset. This can often force a "Greenfield" recovery during which a new, trusted AD forest is created while operations remain impacted in the production environment. This form of recovery imposes a staggering operational tax as restoration timelines stretch from days to weeks, and financial losses compound as IT teams are forced to rebuild the entire identity backbone manually rather than simply restoring data. Crucially, this often extends to organizational communication channels as well. If the compromised identity provider federates to corporate email or collaboration platforms, defenders lose their primary means of coordination during response activity. As a result, they are forced to rely on out-of-band communications or risk leaking sensitive information to an attacker who retains broad access to the collaboration and email platforms.

# Full Cyber Resilience Vision


## Ransomware is Now a Resilience Problem

The traditional framing of ransomware as simply a dual threat of encryption and data theft no longer captures the reality of modern extortion operations. Ransomware operators and affiliates have increasingly prioritized denying targeted organizations the ability to recover. Threat actors are targeting system and administrative planes also known as trusted service infrastructure . The terminology of "trusted service infrastructure" (TSI) is typically associated with management interfaces for platforms and technologies that provide core services for an organization such as backup technologies and virtualization platforms. This allows ransomware operators and affiliates to reduce an organization's ability to recover while maximizing the pressure to pay. They do this by attacking identity services, virtualization management planes, and backup infrastructure.

Ultimately, the transition to Active Resilience is achieved through architectural discipline rather than tool acquisition. It necessitates the strict decoupling of critical systems, the implementation of friction to impede lateral movement, and recovery abilities that operate independently of the primary identity fabric. Shifting towards Active Resilience enables leaders to do more than just secure their data; it helps ensure an organization can maintain their operations while under adversarial pressure.

# Full Cyber Resilience Vision

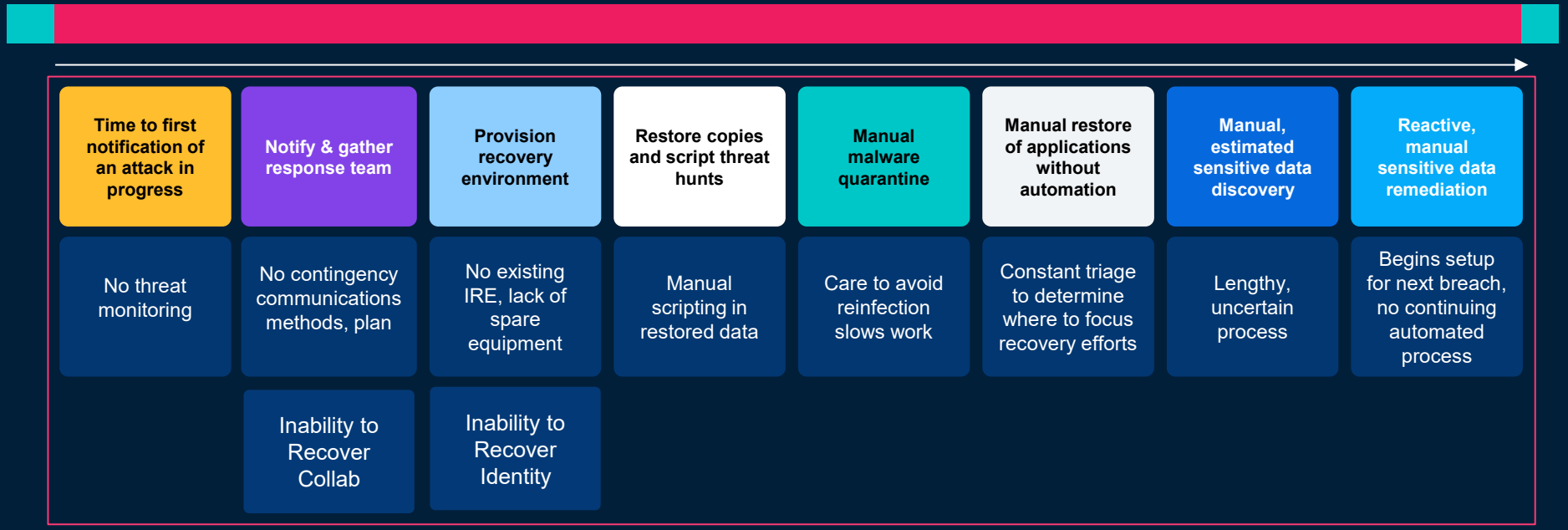

By working to overcome the limitations of standard logging and EDR through a proactive review of total available telemetry, identifying and closing gaps, and maintaining appropriate detail in documentation, defenders can more efficiently and effectively respond to incidents. Doing this prework enables defenders to move beyond atomic IOC searches, which are less effective against threat actors that proactively avoid techniques susceptible to static detections. It allows them to focus on more advanced analysis techniques like stack ranking data to look for outliers and comparison of data against known good systems. These techniques are much more effective in identifying sophisticated threat actor activity.

Organizations should also implement a routine of proactive threat hunting. Relying solely on reactive alerts generated by conventional security tools is insufficient for detecting sophisticated, evasive threat actors. Proactive hunting serves to bridge this critical visibility gap and can significantly curtail the dwell time of an adversary within the network. Since threat actors frequently use legitimate, native administrative utilities to hide their actions in plain sight, detection hinges on the analyst's ability to distinguish benign administrative activity from an attacker's malicious actions. Furthermore, integrating the latest threat intelligence into the hunting process allows organizations to focus on specific techniques currently employed by adversaries. Ultimately, the systematic practice of proactive threat hunting not only identifies existing breaches but also highlights and enables the refinement or remediation of operational deficiencies in the defense posture.

# The Status Quo

## Weeks to Months

**Operations down, patient impacts, and financial losses**



# Full Cyber Resilience

# Q: How Quickly Can We Recover?

## Type I Incidents

Detected Early
Limited Lateral Movement
Limited Blast Radius
Identity Stores Intact
Voluntary, proactive response

Restore to Production or DR
Shorter downtime

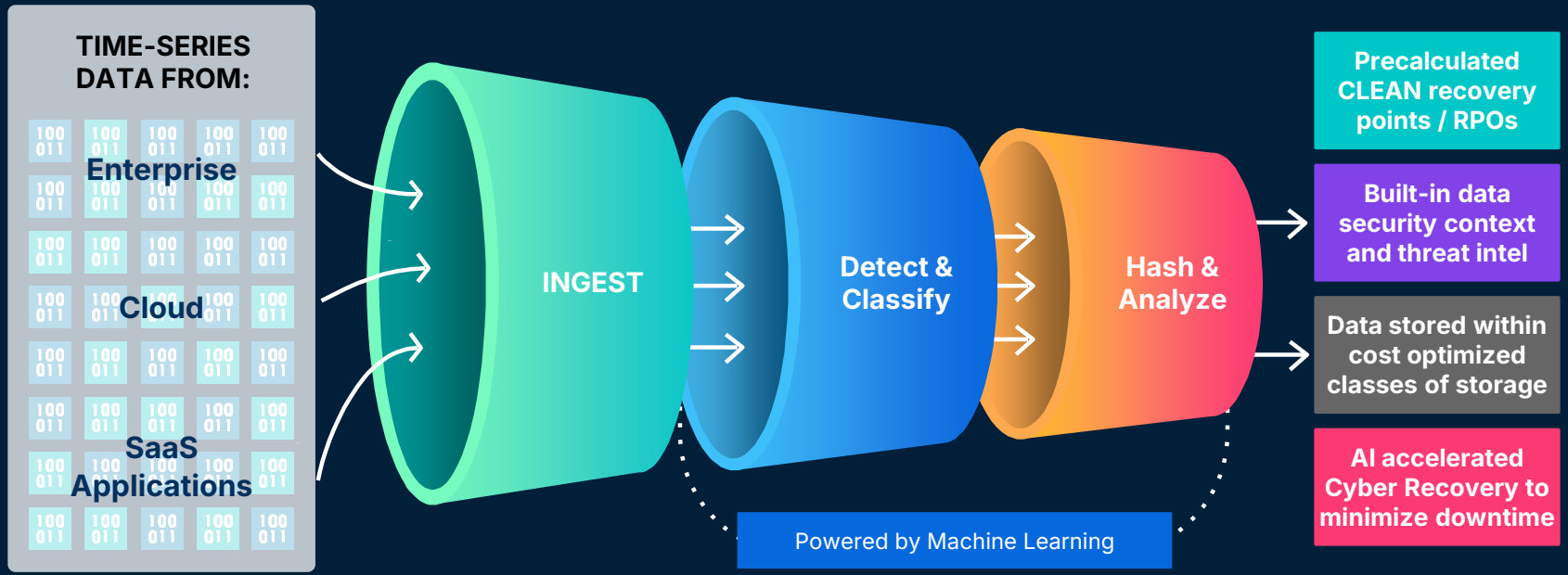
## Type II Incidents

Undetected
Extensive Lateral Movement
Wide Blast Radius
Destroyed Identity Stores
Involuntary, reactive response
Pervasive loss of trust

Must Restore to IRE
Extensive downtime

# Backup ≠ Cyber Recovery

## Preemptive Recovery Engine delivers Precalculated CLEAN recovery points



Data Security Posture

DASHBOARD | USER INTELLIGENCE | SENSITIVE DATA | POLICIES | EVENTS | REPORTS | ON DEMAND

Global Organization

60% Object coverage

Past 24 hours

152 +0
High-risk objects

1.5k +0
High-risk users

338.6k +0
Stale sensitive files

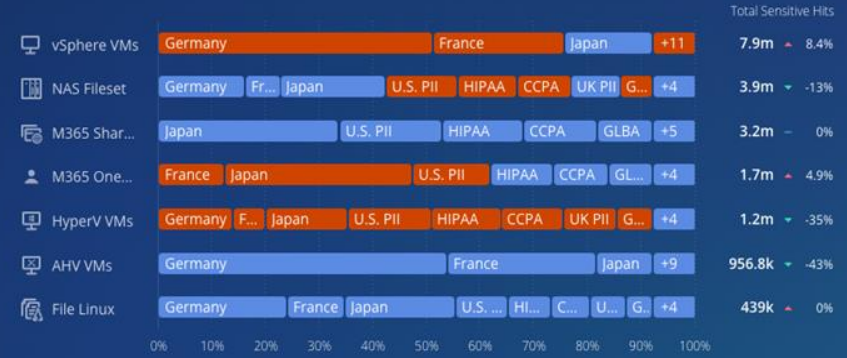
290.5k +0
Open access sensitive files

## Sensitive Data Distribution


## Data Distribution by Object Type

Past 7 days | All policies

VIEW ALL




## Unused Sensitive Files

3k sensitive files haven't been used and can be archived or restricted.

## Highest-Risk Objects

All Objects | All Policies | 10/23/2024

VIEW ALL

800k

## Insights

Objects Have New Policy Data
1 object has new Singapore policy data with 1 sensitive hit.
13 hours ago

Objects Have New Policy Data
5 objects have new GLBA policy data with 57K sensitive hits.
13 hours ago

Objects Have New Policy Data
5 objects have new PCI DSS policy data with 15K sensitive hits.
13 hours ago

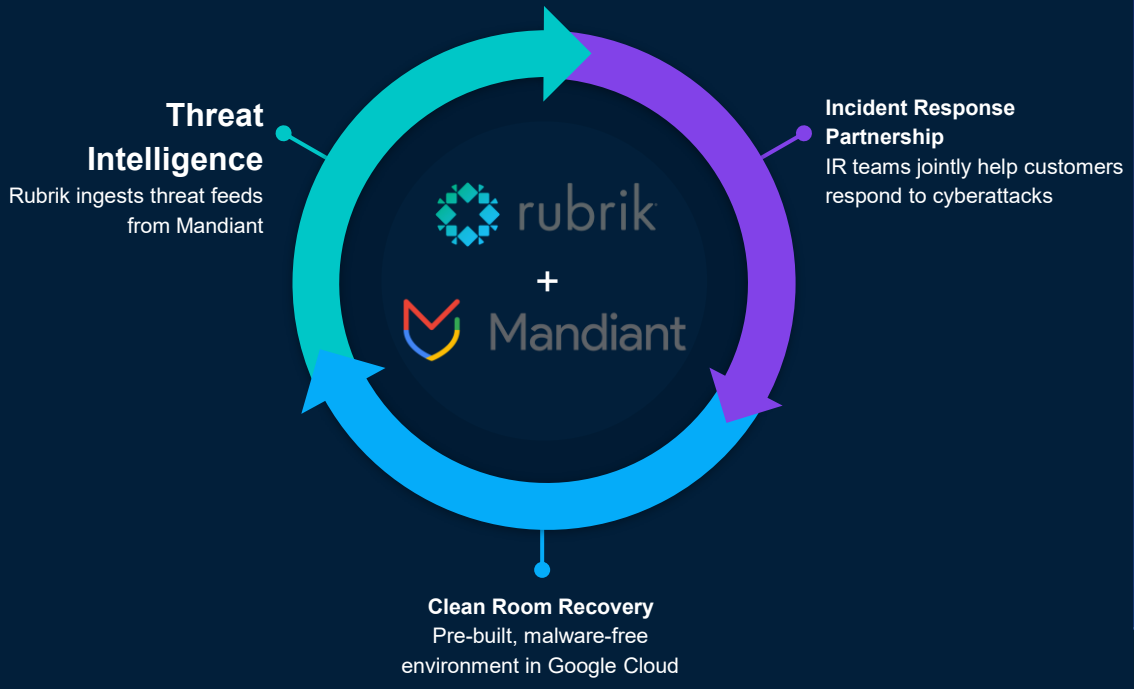
Objects Have New Policy Data
5 objects have new U.S. Financials policy data with 16K sensitive hits.
13 hours ago

Objects Have New Policy Data
7 objects have new U.S. PII policy data with 160K sensitive hits.
13 hours ago

Objects Have New Policy Data

# Threat Monitoring - A Mandiant Strategic Partnership

## Improve cyber resilience with a tightly integrated, end-to-end solution spanning cyber threat detection, incident response, and data recovery




# Recovering without re-introducing the attacker backdoor is like looking for a needle in a haystack...

## 240 Million

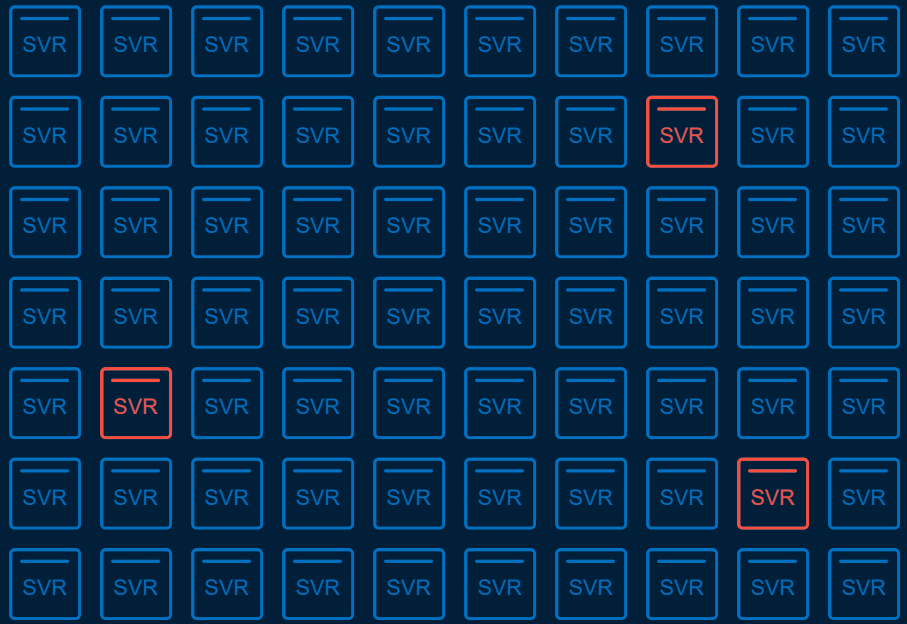
files on average in 1,000 Windows/Linux servers

## 1 File

could be the remote access tool file (RAT) allows the attacker to regain access on recovery

## 1-3 Servers

will be used to maintain redundant access, can be physical or virtual, an existing server or created by the attacker, likely non-prod to reduce chance of detection, it could be encrypted, could be still running, you have no idea..

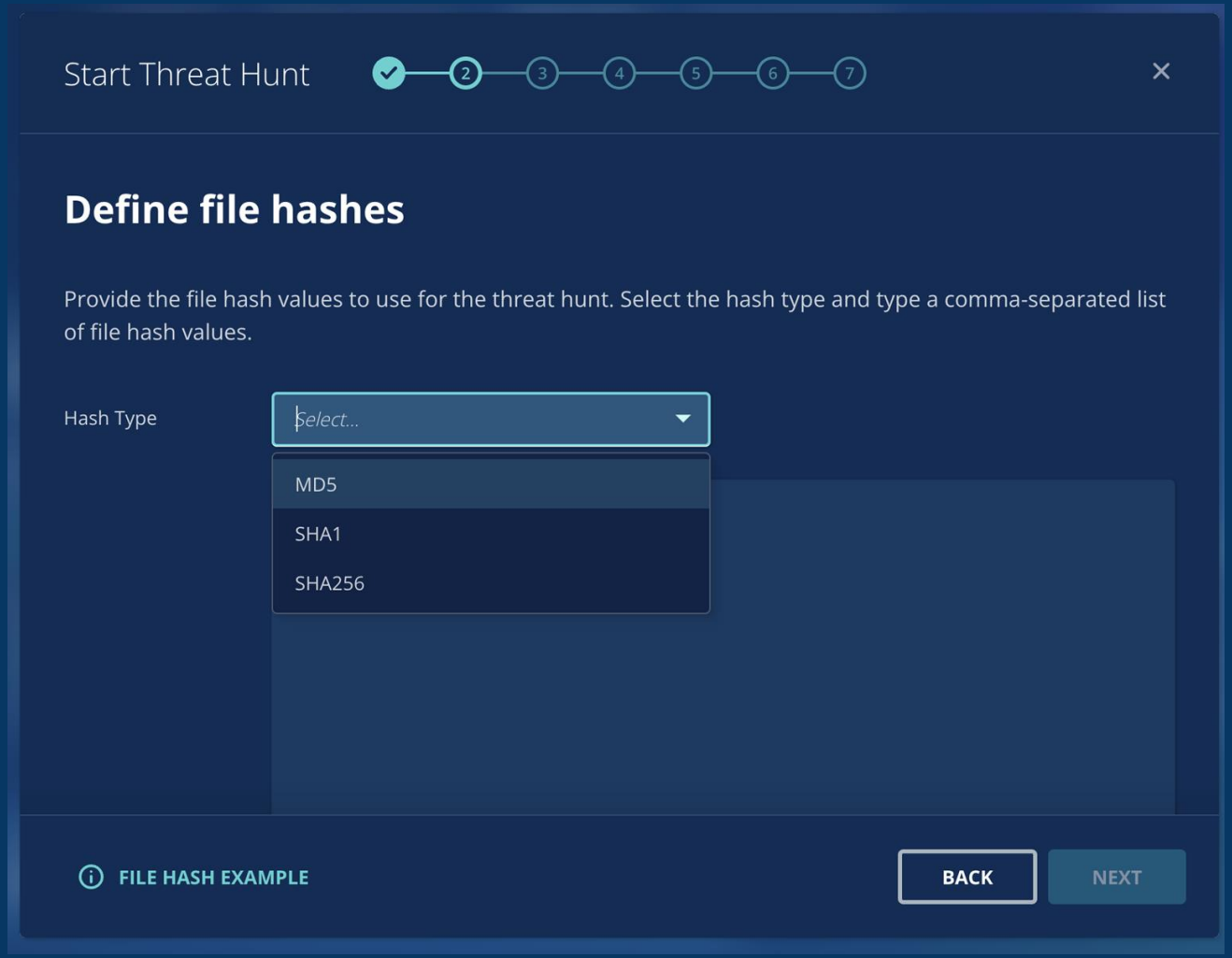


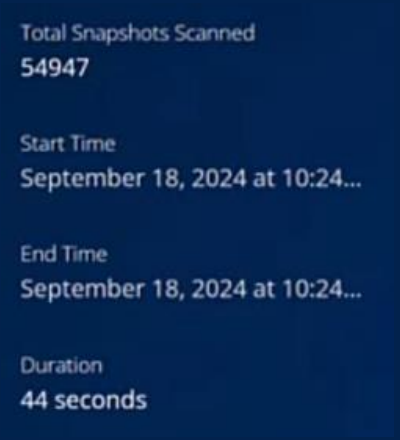
# Let’s recover from backups, but which one?

Total Servers x Daily Retention  = Total Backups To Scan

2,000 Servers/VMs  x 7 Daily Backups = 14,000 Backups!

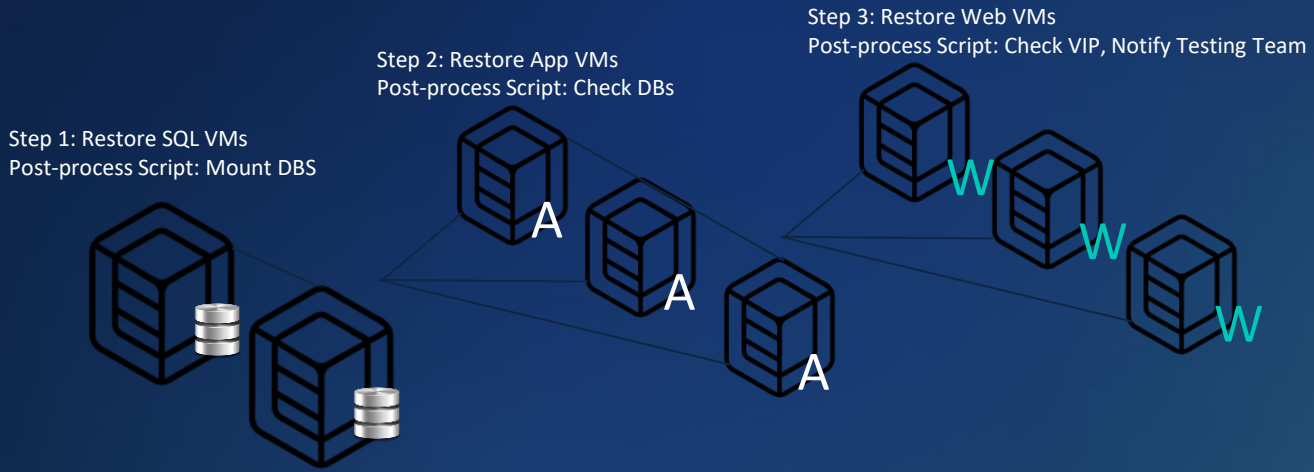
Even at 1 per minute, that would be 9.7 days!!


Start Threat Hunt
2
3
4
5
6
7
Define file hashes
Provide the file hash values to use for the threat hunt. Select the hash type and type a comma-separated list of file hash values.
Hash Type
Select...
MD5
SHA1
SHA256
FILE HASH EXAMPLE
BACK
NEXT


Total Snapshots Scanned
54947
Start Time
September 18, 2024 at 10:24...
End Time
September 18, 2024 at 10:24...
Duration
44 seconds

# Application Details

Application Name: PACs Connector
Application Priority: Tier 1, Priority 17
Application Testing: PACs_Team@provider.org
Application Structure: Playbook_IRE_PACs_Connector
Application Assets: 2 DB VMs, 3 App VMs, 3 Web VMs



# Recovery Exercise at a Glance

**754**

vSphere VMs Recovered

**23:59**

Total Exercise Window (hrs:min)

**464 TB**

Total Data Transferred

**100%**

Success Rate

**1,685 hrs**

Cumulative Processing Time (parallelization)

**59.64 MB/s**

Average Throughput Across All Tasks

**0.46 TB/hr**

Avg Transfer Rate for Large (>1TB) Workloads

KEY CONCLUSIONS

# Three Takeaways from This Recovery Exercise

## Scalability Validated

754 VMs recovered concurrently with a 100% success rate. The 1,685 cumulative hours of processing in a 24-hour window confirms the platform's parallelization capability at enterprise scale.

## Predictability for Standard Workloads

673 VMs under 1TB completed within the first 13 hours, demonstrating highly predictable SLA performance. Standard workload recovery times are consistent and plannable.

## Scale-Optimized Infrastructure

As VM size increases, recovery time per TB decreases — large workloads are 40% more efficient per unit of data. The bottleneck for multi-TB VMs is per-task initialization overhead, not raw throughput capacity.

# The Minimum Viable Hospital -Tier 0 & 1

## Tier 0 - 15 Core Applications

### PATIENT MONITORING (4)

- Central Station Patient Monitoring
- ICU / Telemetry Systems
- Fetal & Perinatal Monitoring (e.g., OBIX)
- Neonatal Monitoring Systems

### INFRASTRUCTURE & SECURITY (4)

- Active Directory / Entra ID
- DHCP / DNS / NTP Services
- SSO / Identity Providers (SAML, Okta)
- MFA (Duo, Microsoft Authenticator)

### ADMINISTRATION (4)

- Microsoft 365 (Exchange, Teams)
- Enterprise Intranet / SharePoint
- Timecard systems
- Payroll

## Tier 1 - 32 Business Critical Applications

### CLINICAL SYSTEMS (8)

- Core Electronic Health Record (EHR)
- Clinical Integration Engine (HL7/FHIR)
- Enterprise Content Mgmt (OnBase)
- IV Pump Management (e.g., Alaris)
- Medical Device Integration (e.g., Capsule)
- Clinical Decision Support
- Patient Portal Backend
- Revenue Cycle Management

### RADIOLOGY / IMAGING (5)

- Enterprise PACS
- Vendor Neutral Archive (VNA)
- Enterprise Image Sharing Gateway
- Radiology Information System (RIS)
- Voice Recognition & Dictation (PowerScribe)

### LABORATORY (4)

- Laboratory Information System (LIS)
- Blood Bank Management (e.g., SafeTrace)
- Specimen Tracking System

### CLINICAL MONITORING (1)

- Predictive / Sepsis Monitoring (e.g., Sickbay)

### CARDIOLOGY (3)

- Cardiology PACS
- ECG Management System (e.g., MUSE)
- Hemodynamic Monitoring

### PHARMACY (3)

- Automated Dispensing Cabinets (Omnicell/Pyxis)
- Pharmacy Information System
- Robotic Dispensing Systems

### ONCOLOGY (2)

- Radiation Treatment Planning (e.g., Eclipse)
- Oncology Information System (e.g., ARIA)

### Facilities (3)

- Climate/HVAC
- OR and Pharmacy Air Pressure
- Keycard Systems


Immersive Ransomware Experience


eBook for Non-technical Stakeholders

Impact Quantification Workshop


Technical guides, Blueprints IRE Workshop


Hands-on technical training


Multidisciplinary Playbook Template


End-to-end Ransomware Simulation

# Rubrik Gets You There


- Breaks free of “analysis paralysis”
- Complementary Workshops
- Consultant Expertise
- Cross-disciplinary coordination
- Cross-vendor coordination
- Opinionated Reference Architectures
- Deliverable Templates
- Meaningful risk reduction on a finite timeline

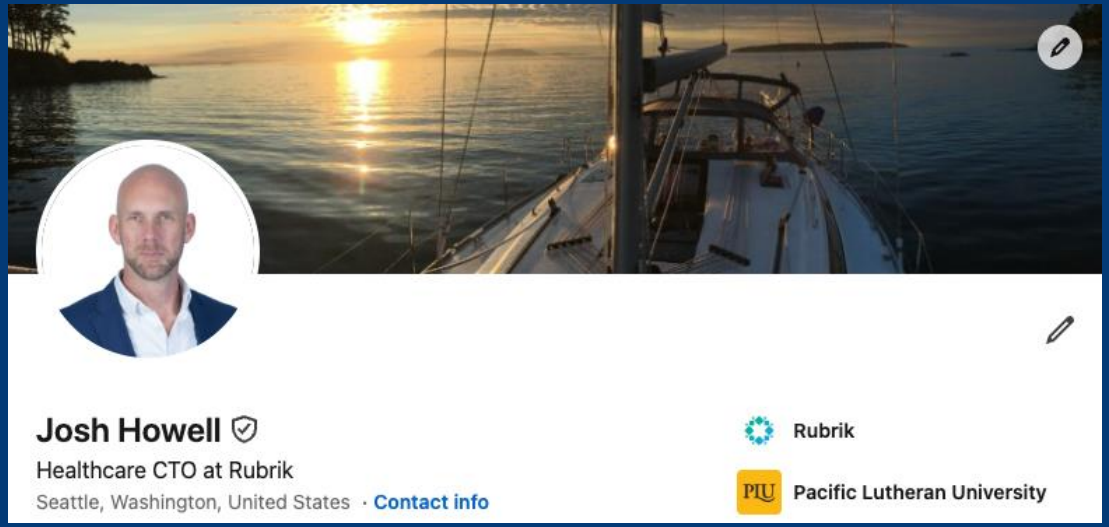
# What We Need From You

The goal is an end-to-end reduction in recovery timelines.
Localized optimization and isolated efforts will not succeed.

Rubrik will invest, but we need sponsorship to an audience with your combined leadership.

CTO, CISO, CIO, FP&A

# Get in touch




Linkedin

Josh.Howell@rubrik.com