Software-Defined Zero Trust Data Management

Modernizing Mission & Enterprise Resiliency

Jeffrey Phelan
Chief Technology Officer, Public Sector

Nov 2021

rubrik

Rubrik's Innovation, Security, and Cloud Pedigree

John Chambers

Former CEO | Cisco

Mark Leslie

Founding CEO | Veritas

Frank Slootman

CEO | Snowflake

John Thompson

Chairman| Microsoft

Enrique Salem

Former CEO | Symantec

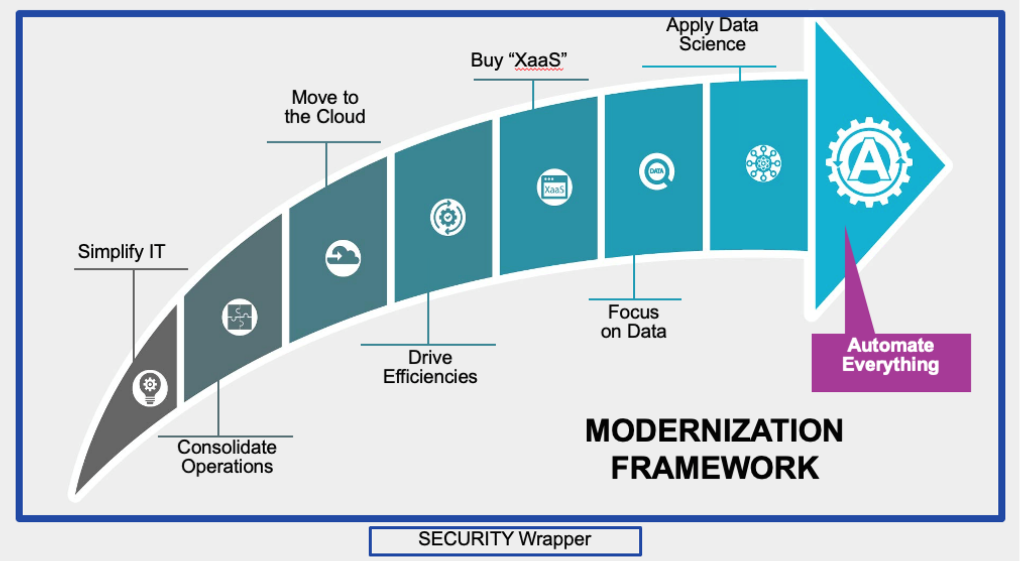
Lightspeed greylockpartners. khosla ventures IVP BainCapital VENTURES

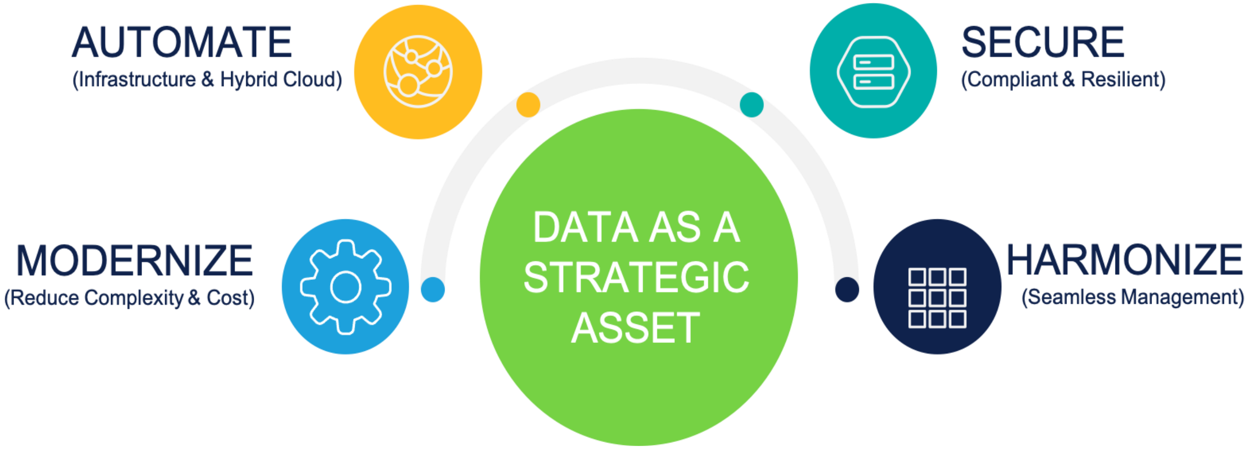
1. **Rubrik is the Fastest Growing Software Company in the history of Silicon Valley**
2. **Rubrik is the most comprehensively Federally Certified data management solution on the market and a Gartner industry leader; FedRamp High, IL-5, IL-6, JWICS**
3. **Growth fueled by Ransomware, IT Automation, Remote & Tactical Data Requirements, and Cloud/Hybrid Cloud Migration & Adoption**

MICROSOFT MADE AN EQUITY INVESTMENT IN RUBRIK IN AUGUST 2021

Common Digital Transformation Strategic Activities:

Every Organization is Operating Against A Documented Modernization Plan




AUTOMATE
(Infrastructure & Hybrid Cloud)
SECURE
(Compliant & Resilient)
MODERNIZE
(Reduce Complexity & Cost)
DATA AS A STRATEGIC ASSET
HARMONIZE
(Seamless Management)

MEASURED OUTCOMES:

1) Complexity Reduction
2) Cost Avoidance
3) Enterprise Recovery (Operations, Mission, Cyber)

Consistent Problem Set Across Public Sector & DoD:

Modernization Efforts Slowed by Expensive & Complex Environments

NAS PLATFORMS

NetApp
ISILON SYSTEMS
DELL EMC
HITACHI

DATABASES

Microsoft SQL Server
ORACLE DATABASE
MySQL
Epic
mongoDB
PostgreSQL
SAP HANA
cassandra

OPERATING SYSTEMS

AIX
ORACLE SOLARIS
UNIX®

VIRTUALIZATION

vmware
Microsoft Hyper-v
NUTANIX

CLOUD + SAAS

aws
ORACLE CLOUD
Azure
Office 365

AUTOMATION & MANAGEMENT

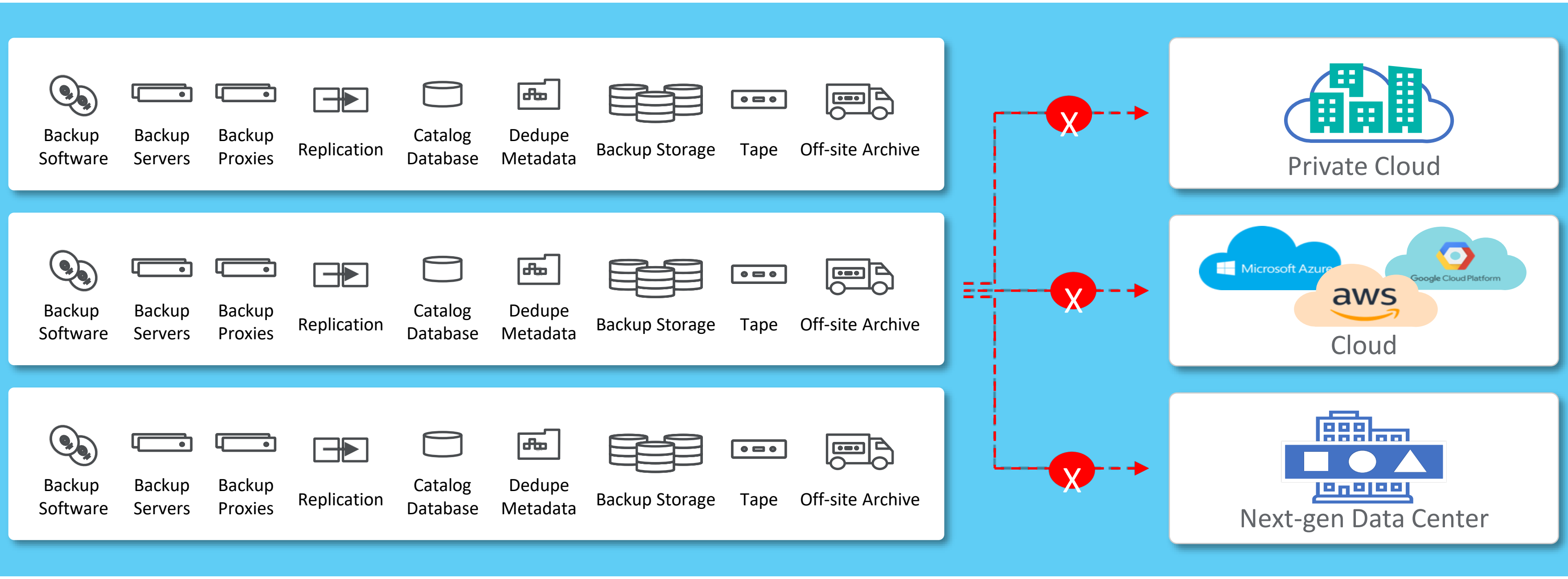
vm
vmware vCloud Director
HashiCorp Terraform
ANSIBLE
RED HAT CLOUDFORMS

3RD PARTY

servicenow
splunk>
DATADOG

Legacy Systems:

Lack Security & Resiliency Required to Operate in today's Hybrid Cloud & High Security Environments



Backup Software | Backup Servers | Backup Proxies | Replication | Catalog Database | Dedupe Metadata | Backup Storage | Tape | Off-site Archive

Backup Software | Backup Servers | Backup Proxies | Replication | Catalog Database | Dedupe Metadata | Backup Storage | Tape | Off-site Archive

Backup Software | Backup Servers | Backup Proxies | Replication | Catalog Database | Dedupe Metadata | Backup Storage | Tape | Off-site Archive

X
X
X

Private Cloud

Microsoft Azure
Google Cloud Platform
aws
Cloud

Next-gen Data Center

rubrik | public sector

Teams are married to Legacy Systems/Blockers

Organizations Throw People & Money at Data Management

20+ Year Old Technologies Can't Protect, Manage, and Move Data Away from Modern Cyber Adversaries

Infrastructure Team

- Backup Software
- Backup Servers
- Backup Proxies
- Replication
- Catalog Database
- Dedupe Metadata
- Continuous Data Protection
- Backup Storage
- Tape
- Off-site Archive

COMMVAULT DELLEMC SPANNING Quest
VERITAS IBM Spectrum Protect Plus UNITRENDS RecoverPoint
veeAM IRON MOUNTAIN FalconStor arcserve

Application Team

- Database Backup
- Manual Scripts
- Copy Data Mgmt
- Orchestration / Data Migration

ORACLE SAP HANA DELLEMC LITESPEED
Microsoft SQL Server redgate DELPHIX Data Platform Studio aws
cassandra mongoDB. actifio Acronis Azure

Cloud Team

- Manual Scripts
- Cloud Backup Service
- Replication
- AWS Tool
- Azure Tool
- GCP Tool

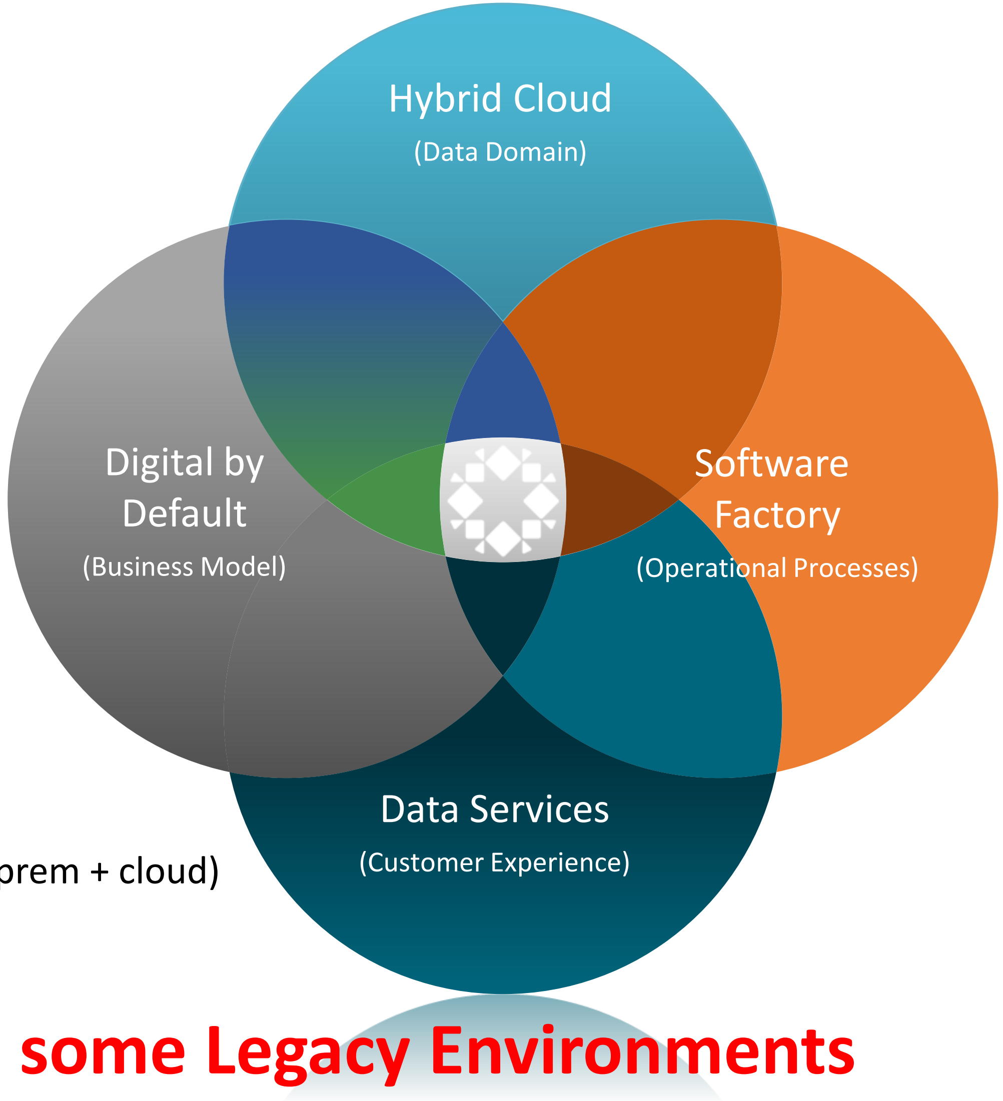
Azure aws VEEAM N2WS CloudRanger Now a Druva company
Barracuda SPANNING UNITRENDS
CLOUDALLY Axcient CLOUDDADDY

LICENSE & TOOL COST AVOIDANCE + FTE REDUCTIONS = $Ms IN SOFT DOLLAR SAVINGS

SW-Defined Data Management as a Transformational "Operating System"

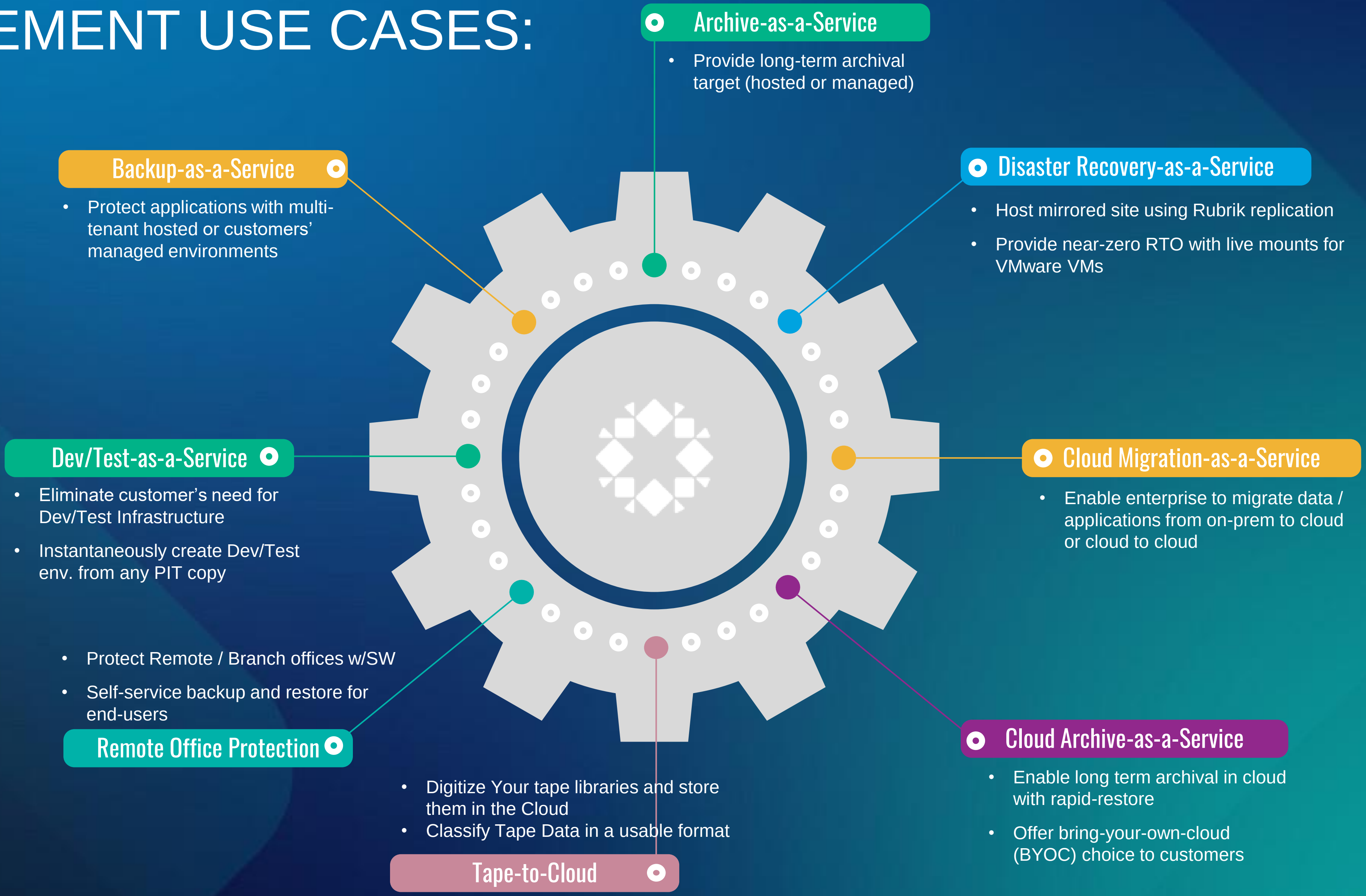
Digital Workstreams & Key Strategic Impact Areas

- Hybrid Cloud - Data Domain
  - ✓ Infrastructure Sizing, Workload Validation, Indexing, Inventory
  - ✓ Application & System Dependencies; Workload Prioritization
  - ✓ Mobility Tooling, Tiering Automations, Costing Analytics
- Software Factory – Operational Processes
  - ✓ Digital Twin Capabilities, Live DR & COOP Testing
  - ✓ DevOps, Automated Pen Testing, Malicious Code Countermeasures
- Data Services – Improved Customer Experience
  - ✓ Self-Service Automations – ServiceNow
  - ✓ Security Ops Integrations – EDR, Logging, Incident Response
- Digital by Default – Improved Cash Flows, Lower Costs
  - ✓ AWS & Azure Marketplace – Burn down consumption commitments (on prem + cloud)
  - ✓ Multiple Consumption, Subscription, and Points Models available



COST AVOIDANCE approaching 90% in some Legacy Environments

MODERNIZED DATA MANAGEMENT USE CASES:



Archive-as-a-Service

- Provide long-term archival target (hosted or managed)

Backup-as-a-Service

- Protect applications with multi-tenant hosted or customers' managed environments

Disaster Recovery-as-a-Service

- Host mirrored site using Rubrik replication
- Provide near-zero RTO with live mounts for VMware VMs

Dev/Test-as-a-Service

- Eliminate customer's need for Dev/Test Infrastructure
- Instantaneously create Dev/Test env. from any PIT copy

Cloud Migration-as-a-Service

- Enable enterprise to migrate data / applications from on-prem to cloud or cloud to cloud

Remote Office Protection

- Protect Remote / Branch offices w/SW
- Self-service backup and restore for end-users

Tape-to-Cloud

- Digitize Your tape libraries and store them in the Cloud
- Classify Tape Data in a usable format

Cloud Archive-as-a-Service

- Enable long term archival in cloud with rapid-restore
- Offer bring-your-own-cloud (BYOC) choice to customers

rubrik

Infrastructure Modernization Benefits: Advanced Resilience Capabilities

1 LIVE RECOVERY & TESTING

- DATA, APPLICATIONS, SYSTEMS
- DISASTER RECOVERY
- 2ND SITE + HYBRID CLOUD

2 DIGITAL TWIN DEVOPS

- AUTOMATED TEST, PATCH, STIG
- PENTESTING, CYBER HUNT
- APP PERFORMANCE

3 CROWN JEWELS MOVING DEFENSE

- TACTICAL EDGE, DATA CENTER, HYBRID CLOUD
- AUTOMATED PROTECTION SCHEMES

4 INFRASTRUCTURE COUNTERMEASURES

- AUTOMATIONS WITH EDR, LOGGING, IR PLAYBOOKS
- DETECT & HUNT MALICIOUS & SLEEPING CODE

Flexible, Agnostic, Automated, Hyperscale

Designed to be vendor-agnostic from Day 1.

Support industry-leading data sources, hypervisors, clouds.

Virtualized Applications

VMware AHV Hyper-V

Physical Applications

ORACLE SQL Server NAS AIX

ZERO TRUST Data Management

ZERO TRUST Architecture

CHEF servicenow splunk> p ANSIBLE SALTSTACK. vm

Public Cloud

Microsoft Azure Google Cloud Platform aws

Private Cloud

NFS Tape Object Storage

Azure Stack

rubrik | public sector

So What?
Measured Outcomes

1

LOWER FTE COSTS

- 4:1 Reduction in FTEs
- ~40%+ Reduction in Labor Rates

2

INCREASED EFFICIENCY

- 64x faster than manual workflows
- 96% reduction of manual processes

3

REDUCED COMPLEXITY

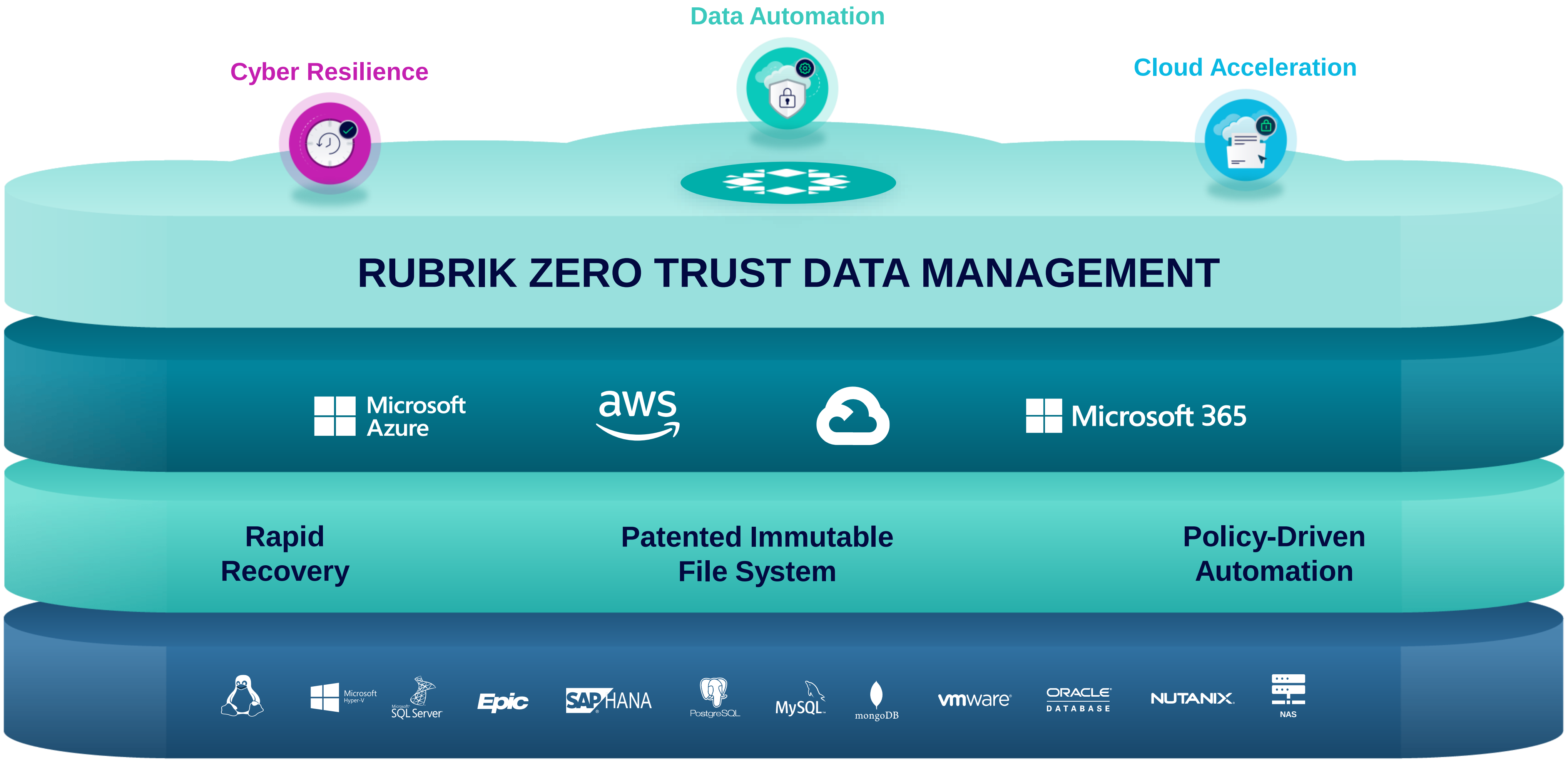
- 3:1+ Tool Overlap/Redundancy

4

COST AVOIDANCE

- 30-40%+ reduction in licensing
- 40%+ reduction in Labor costs
- 90% reduction in time

Rubrik Data Management Platform Overview



Data Automation

Cyber Resilience

Cloud Acceleration

RUBRIK ZERO TRUST DATA MANAGEMENT

Rapid Recovery

Patented Immutable File System

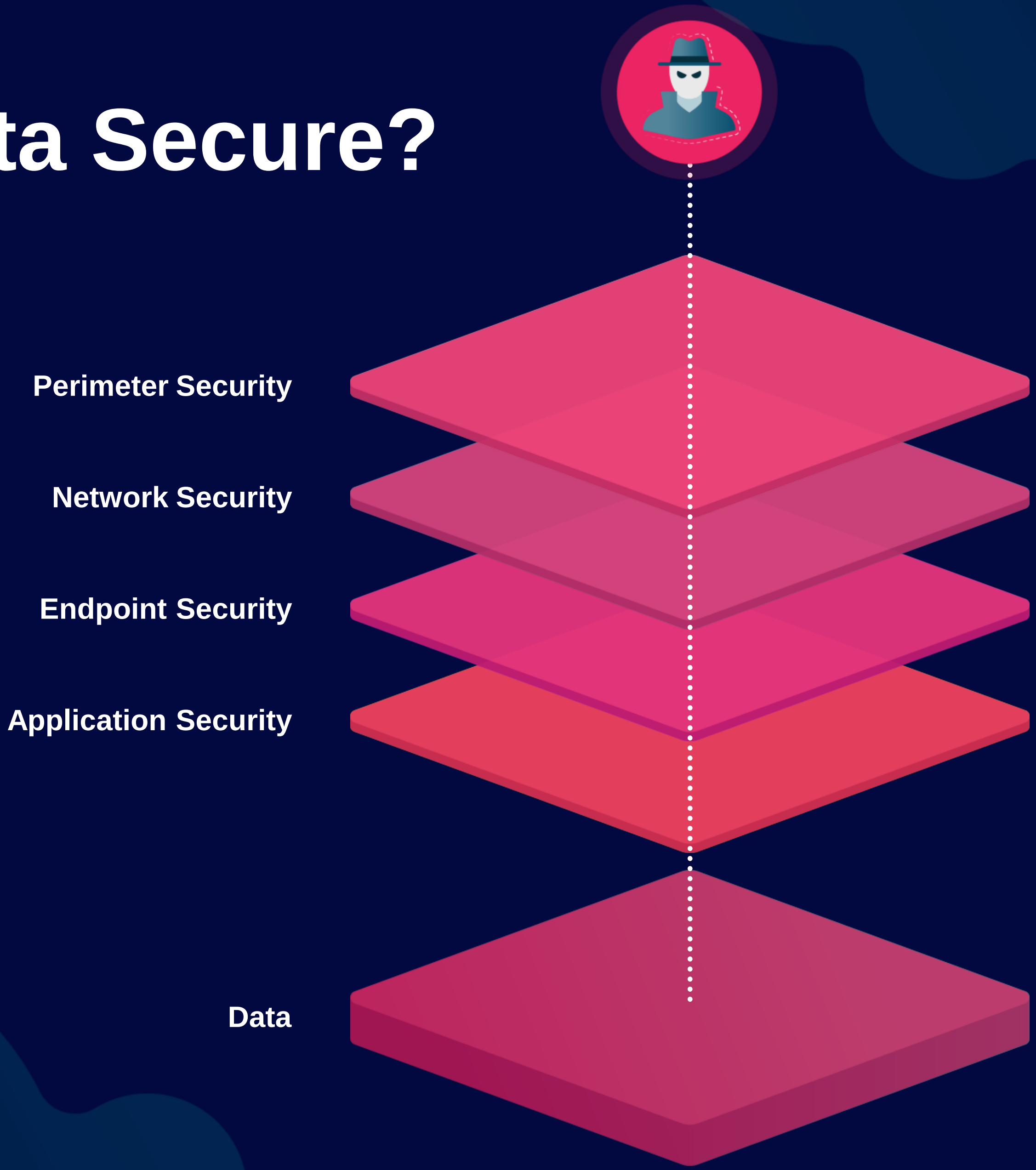
Policy-Driven Automation

Complete data availability, security, compliance, and governance on a single platform for on-premises and cloud

Zero Trust Data Security Best Practices

NOVEMBER 2021

Is My Data Secure?



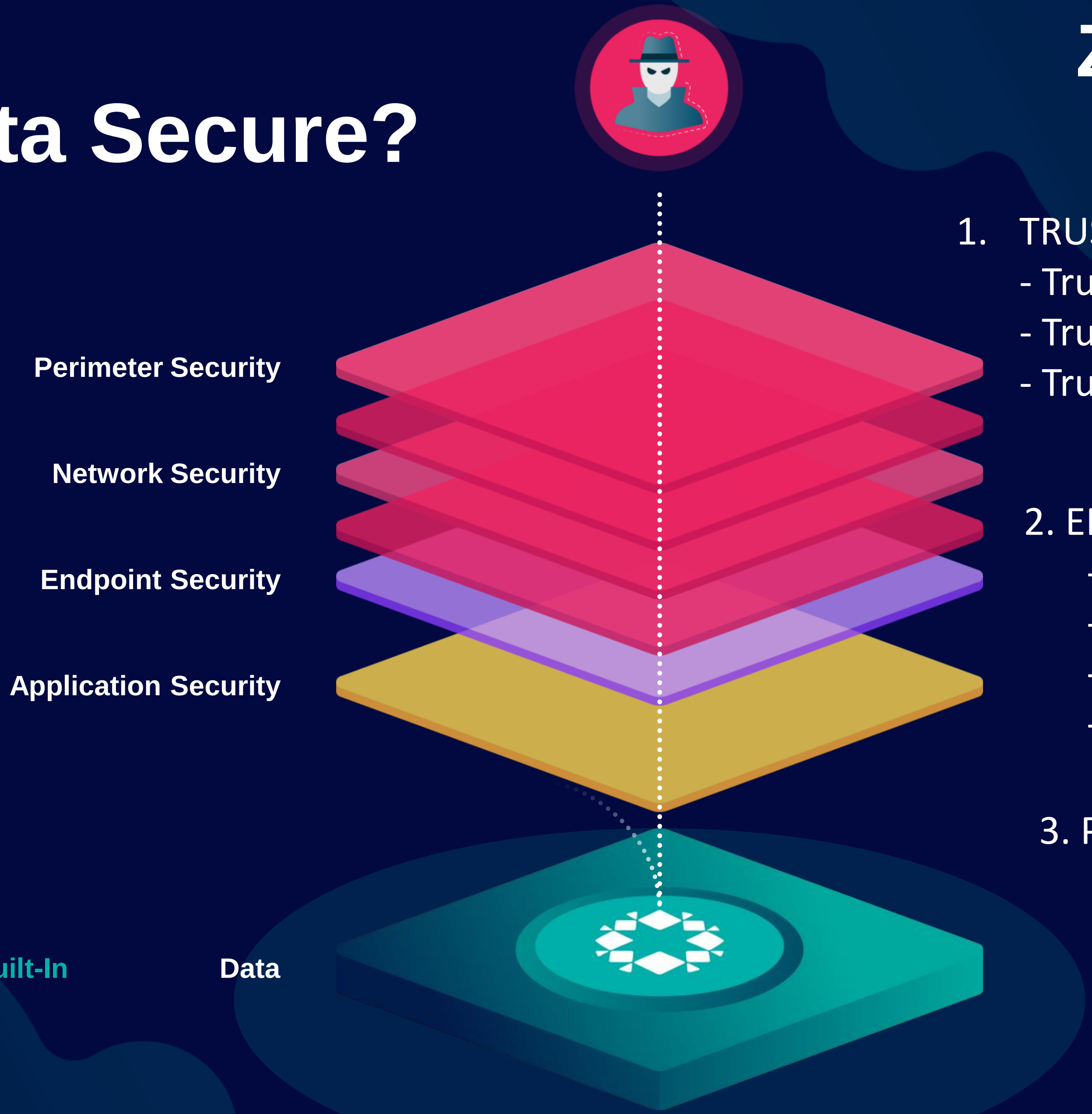
Is My Infrastructure Resilient?

1. Adversaries are using AI & ML to custom design exploits against targets

2. Traditional 3-Tier Data Protection Architectures are easily compromised
   - Media Servers
   - Proxy Servers
   - Disk Backup Targets
   - Third Party Apps/Services

3. Hacked Administrative Privileges are Keys to the Kingdom
   - Deletions
   - Edits
   - Timeouts
   - Exfiltration

Is My Data Secure?



Cyber Resilience Built-In

Zero Trust Data Management

1. TRUST NOTHING – SUSPECT EVERYTHING

- Trust NO User – Validate Everything
- Trust NO Service – Authenticate 100%
- Trust NO Port, Protocol, Connection

2. ENCRYPT DATA EVERYWHERE

- All Data at Rest
- All Data in Flight
- All Data Between Nodes & Clusters
- Add Data to & from the Cloud

3. PATENTED IMMUTABLE FILE SYSTEM

- ***UNEDITABLE*** File System
- Continuously Fingerprinted
- Append Only
- Non-native formats

Key Principles of Cyber Resiliency: Rubrik Zero Trust Data Management

Air Gap	Immutable File System	Retention Lock	Data Encryption
None (backups online)	**Can be edited** (mutable)	**Backups can be deleted/expired**	**Encrypt only data at rest**
Logical (backups offline)	**Cannot be edited** (immutable)	**Cannot be deleted** (expired)	**Encrypt all data – at rest and in-transit**
Physical (disconnected)			**Data left unprotected**

RUBRIK BEST PRACTICES

CREATING A THIRD COPY OF DATA OFF SITE DOES NOT ACHIEVE IMMUTABILITY – IT'S JUST ANOTHER COPY YOU PAY FOR

EXECUTIVE ORDER PRIORITIES – RUBRIK OVERLAY

ZERO TRUST ARCHITECTURE & CYBERSECURITY DIRECTIVES

CYBERSECURITY FOCUS AREAS (www.build.rubrik.com)

✓ **DETECT:** Integrate with Leading Endpoint Detection & Response Platforms

✓ **IDENTIFY:** Integrate with Approved Logging Systems

✓ **PROTECT**: On-Premises, Hybrid Cloud, Tactical Edge

✓ **RECOVER:** At-Scale On-Premises, at Second Sites, and Across Hybrid Cloud

✓ **RESPOND:** Integrate with Leading Security Orchestration & Automation Platforms

COMPLIANCE & GOVERNANCE AREAS

✓ **MODERNIZATION** (MFA, End-to-End Encryption, Hybrid Cloud)

✓ **SUPPLY CHAIN SECURITY** (SecDevOps, CMMC Level 1)

✓ **INCIDENT RESPONSE** (SOAR Integrations)

✓ **THREAT DETECTION** (EDR + Logging Integrations)

✓ **INVESTIGATION & REMEDIATION** (Recovery at Scale)

Rubrik's Security Eco System & Integrations

REST API-driven using JSON, XML, or Syslog

SIEM/LOGGING INTEGRATIONS:

splunk> exabeam LogRhythm FORTINET

RAPID7 IBM McAfee elastic

EDR INTEGRATIONS:

Microsoft CROWDSTRIKE SOPHOS TREND MICRO

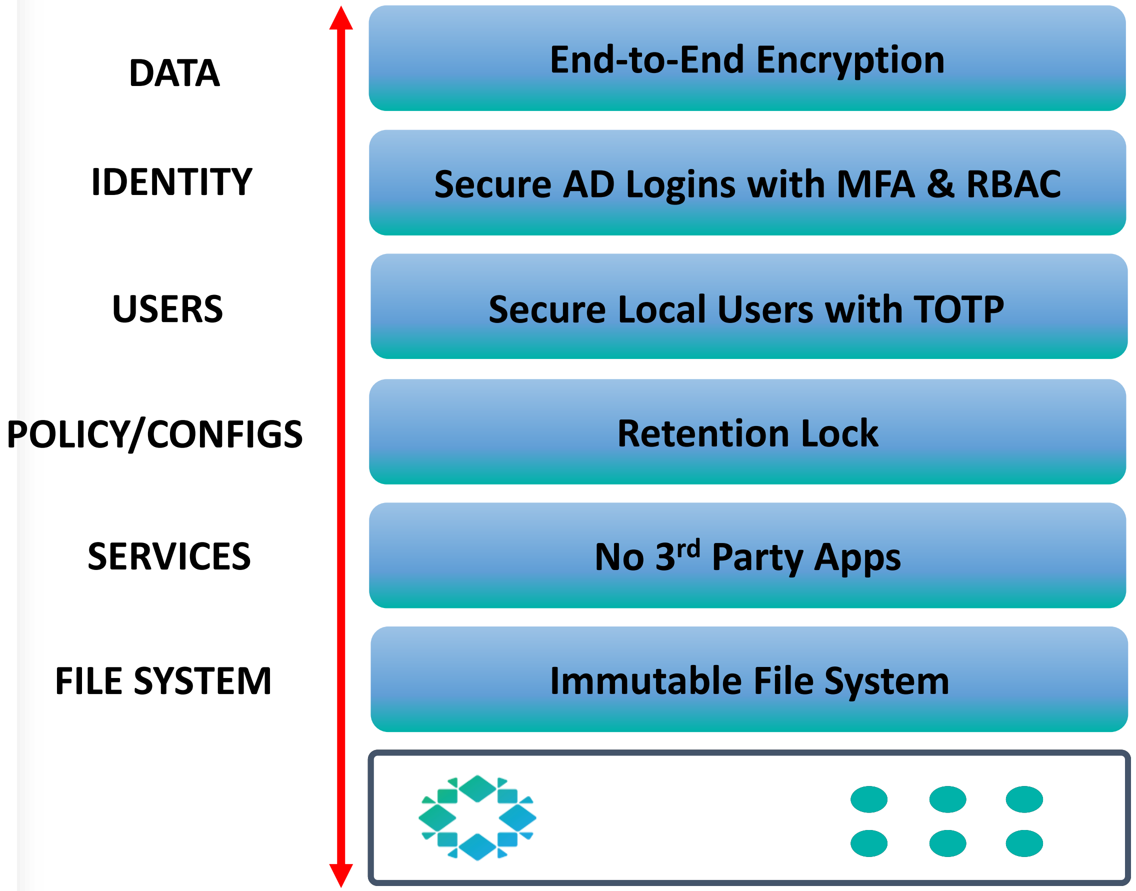
McAfee SentinelOne CARBON BLACK

SOAR INTEGRATIONS:

CORTEX XSOAR BY PALO ALTO NETWORKS splunk> SWIMLANE servicenow

Zero Trust Data Management Architecture

Native Counter Measures Against Adversary TTPs



DATA — End-to-End Encryption

IDENTITY — Secure AD Logins with MFA & RBAC

USERS — Secure Local Users with TOTP

POLICY/CONFIGS — Retention Lock

SERVICES — No 3rd Party Apps

FILE SYSTEM — Immutable File System

Hardened Secure Linux Build
Vendor Patched & No Shell Access

End-to-End Encryption

- All data encrypted in-flight using TLS 1.2 SHA-512 hash
- All data encrypted at rest to FIPS 140-2 Level 2 RSA 2048-bit key
- Key mgmt. using TPM or KMIP for key rotation
- No internal NFS/SMB, No ability to spoof, intercept, or read from network

Secure AD User/Group Logins & RBAC

- Integrate into RSASecurID, Duo, Any SAML2.0 Compliant
- Multi-factor on all AD integrated logins, alerts/syslog for failed logins
- RBAC, read-only admins, least privilege access & API tokens

Secure Local Admin Logins

- Built-in TOTP (Time-based One-Time Password)
- Secure local accounts in minutes using any Android/iOS device
- Removes backdoor of local account access, also applies to SSH
- Required account for recovery in event of attack (AD Compromised)

Retention Lock (Support driven process)

- Prohibits backup admin (adversary) from expiring backups prematurely
- No removal of replication, archiving, re-assign, shorten of retention
- Prohibits all node/cluster resets & NTP poisoning/drift (monotonic clock)
- Cohasset validated – SEC 17a-4(f) & FINRA 4511(c) compliant

FIPS VALIDATED 140-2

SOC 2 TYPE 2 AICPA SOC

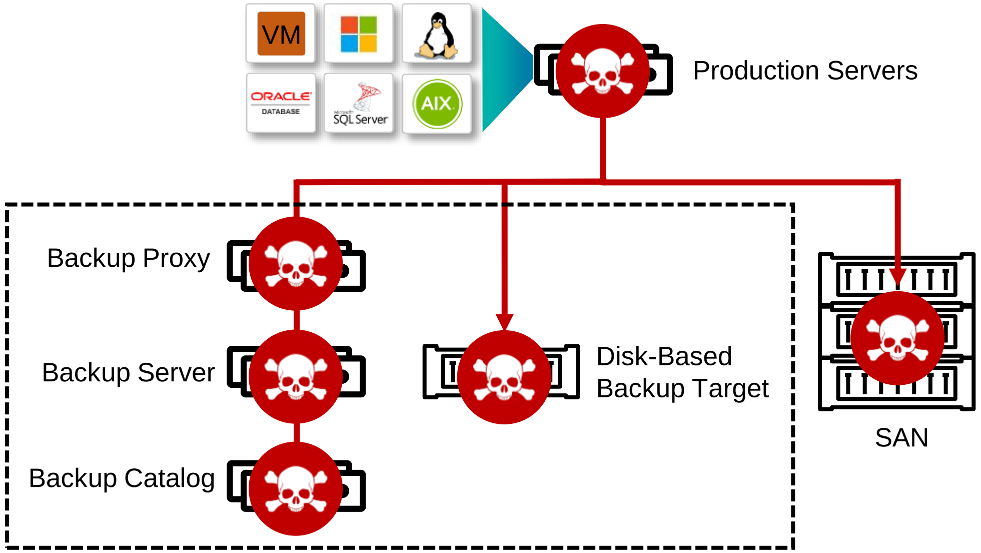
Information Security Management System ISO 27001 Certified

RUBRIK'S ZERO TRUST REFERENCE ARCHITECTURE:

Immutable Countermeasures Against Adversaries

INHERENT PROBLEM BEING EXPLOITED:

Backups Accessible from Network: No Air Gap +
Entire System Editable = NOT IMMUTABLE

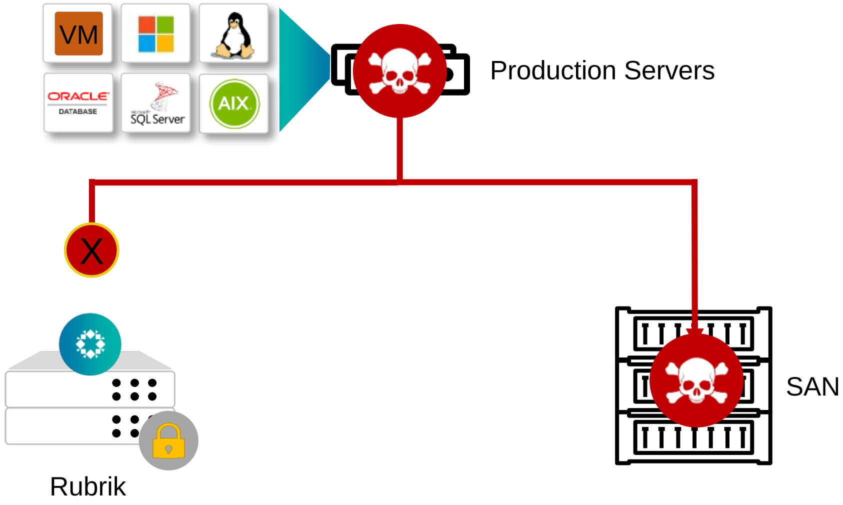


STOLEN CREDENTIALS UNLOCK THE KEYS TO THE KINGDOM

- **Backups can be accessed, modified and deleted from the network**
  - **Anything using standard storage protocols is vulnerable**
    - **Major Attack is an UNRECOVERABLE event**

RUBRIK IMMUTABLE COUNTERMEASURES:

Zero Trust Architecture + Logical Air Gap + Encryption + Retention Lock



✓ **Modern Hyper Converged Data Protection Platform**

✓ **No Backups accessible on or from the Network**

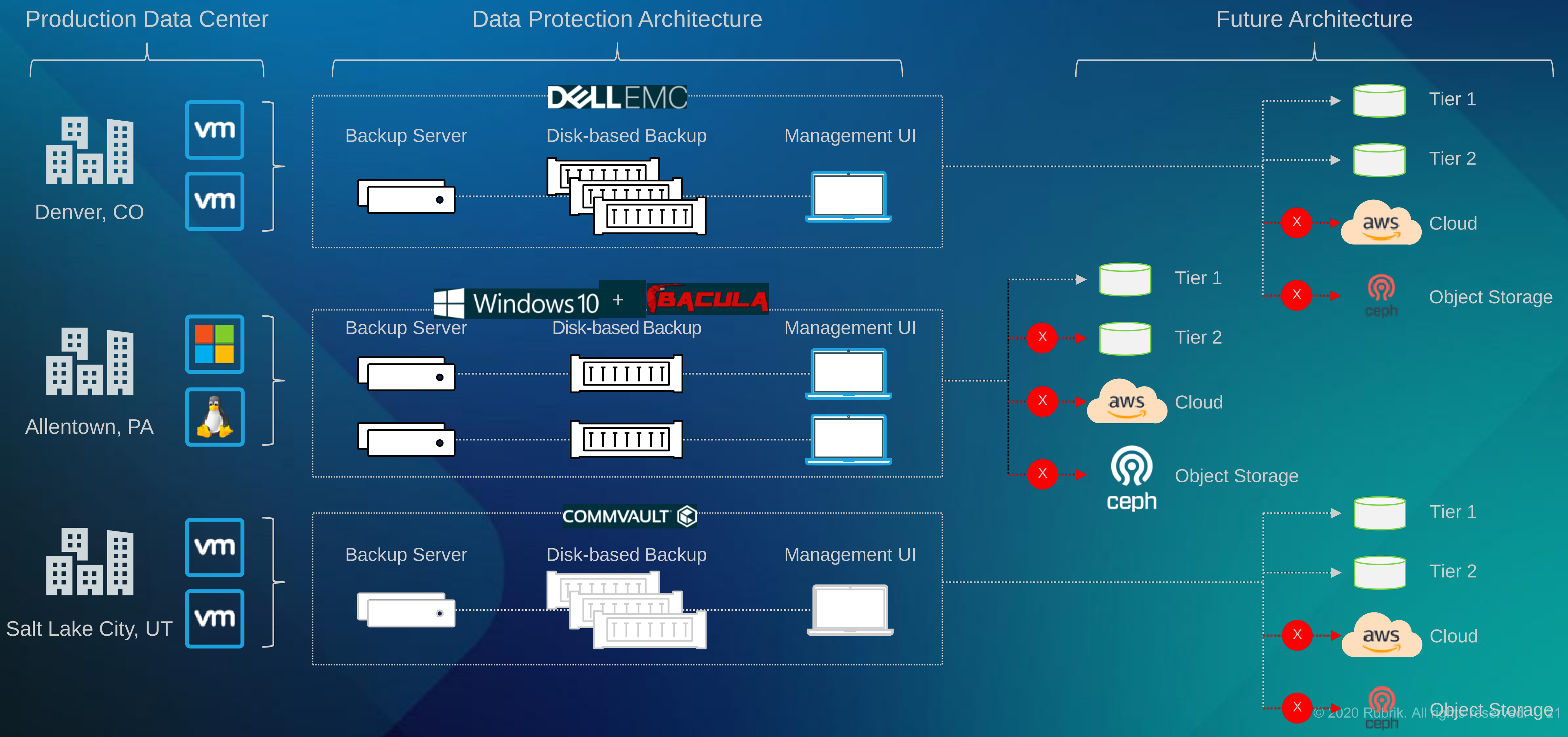
✓ **Backups can NOT be modified (IMMUTABLE)**

✓ **Major Attack is NOW RECOVERABLE from the 1st Copy**

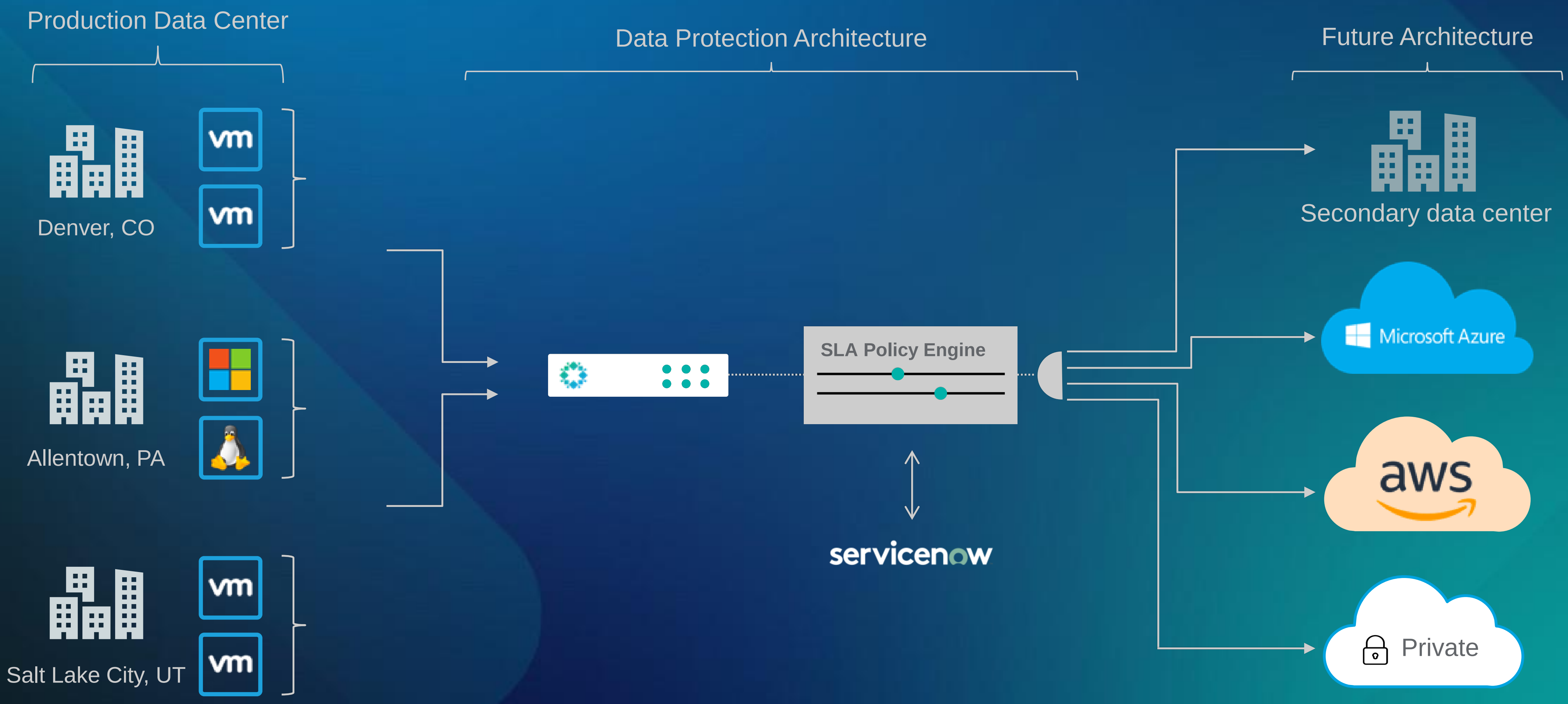
A 3RD COPY OF DATA OFF SITE IS EXPENSIVE, VULNERABLE TO BACKUP WINDOW ATTACKS, AND LENGTHENS RECOVERY TIMES

CYBER RESILIENCE USE CASES

Use Case: Legacy Architecture & Limitations

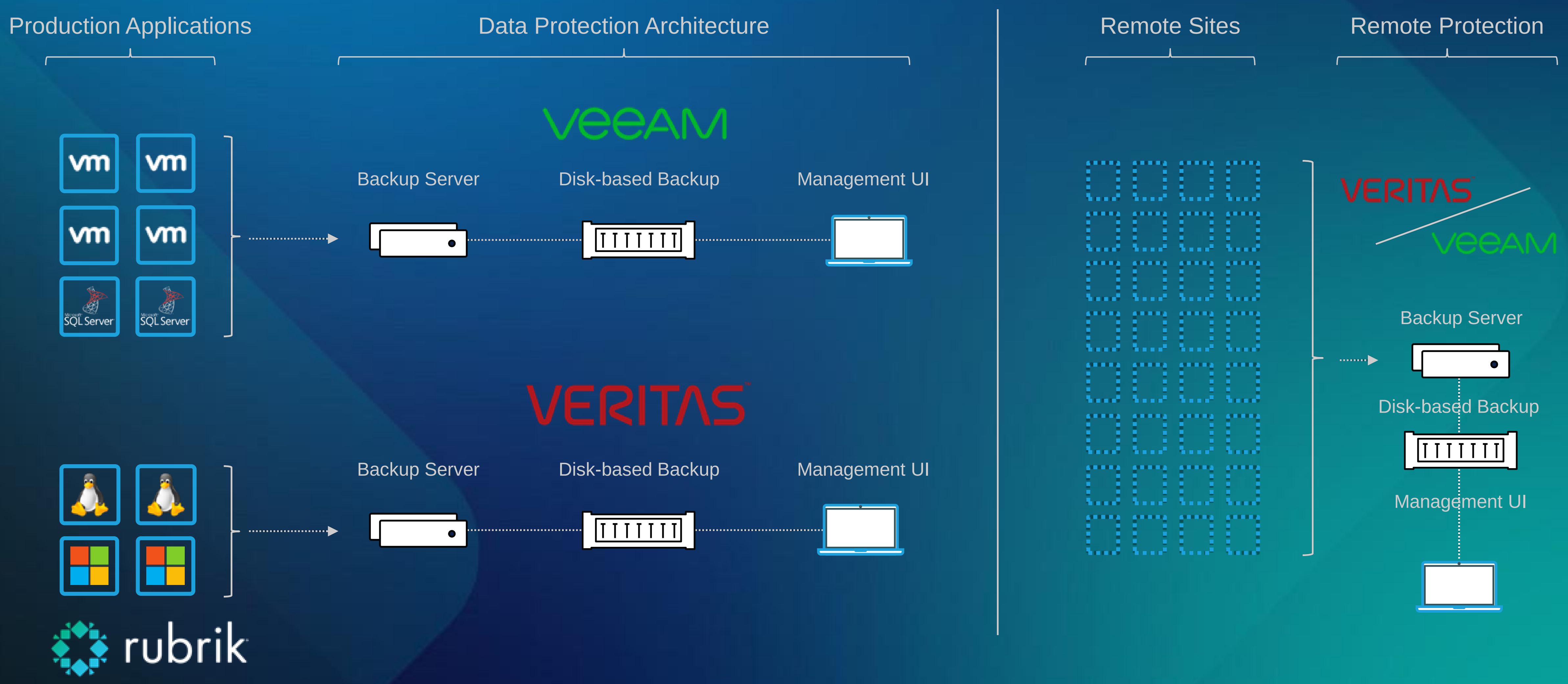


Use Case: Modernized Architecture & Hybrid Cloud



40% + COST AVOIDANCE + SAVINGS

Use Case: Cost Avoidance for Remote Locations



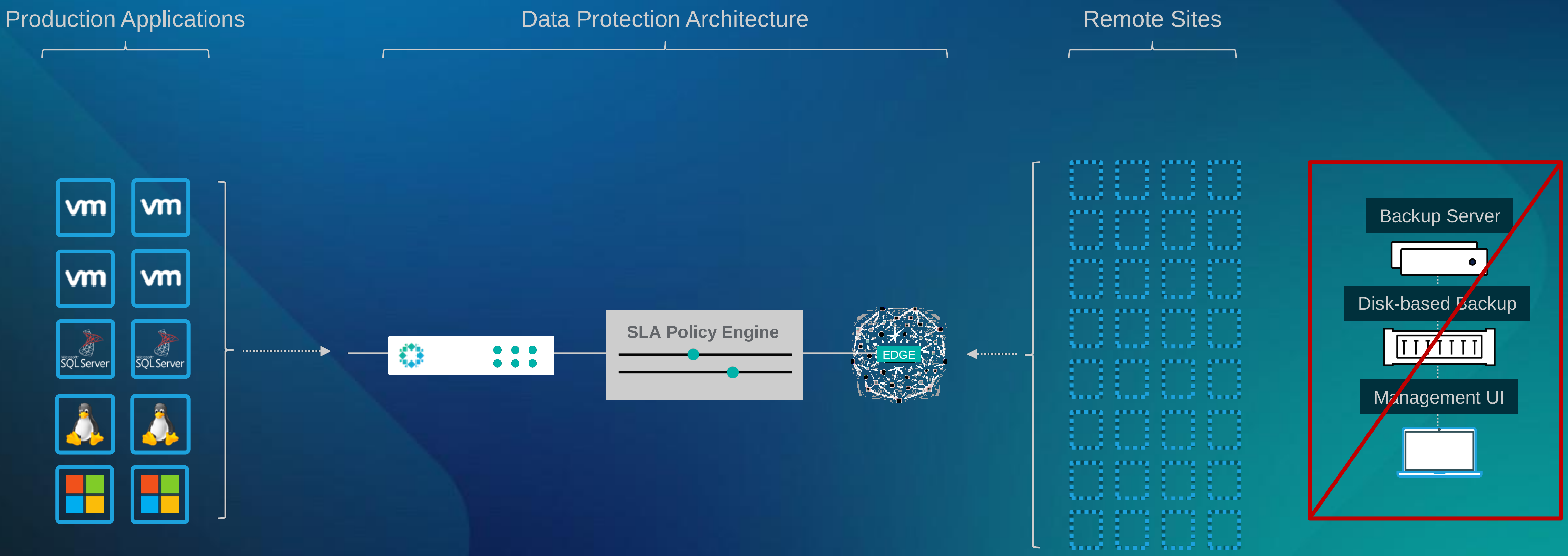
Production Applications

Data Protection Architecture

Remote Sites

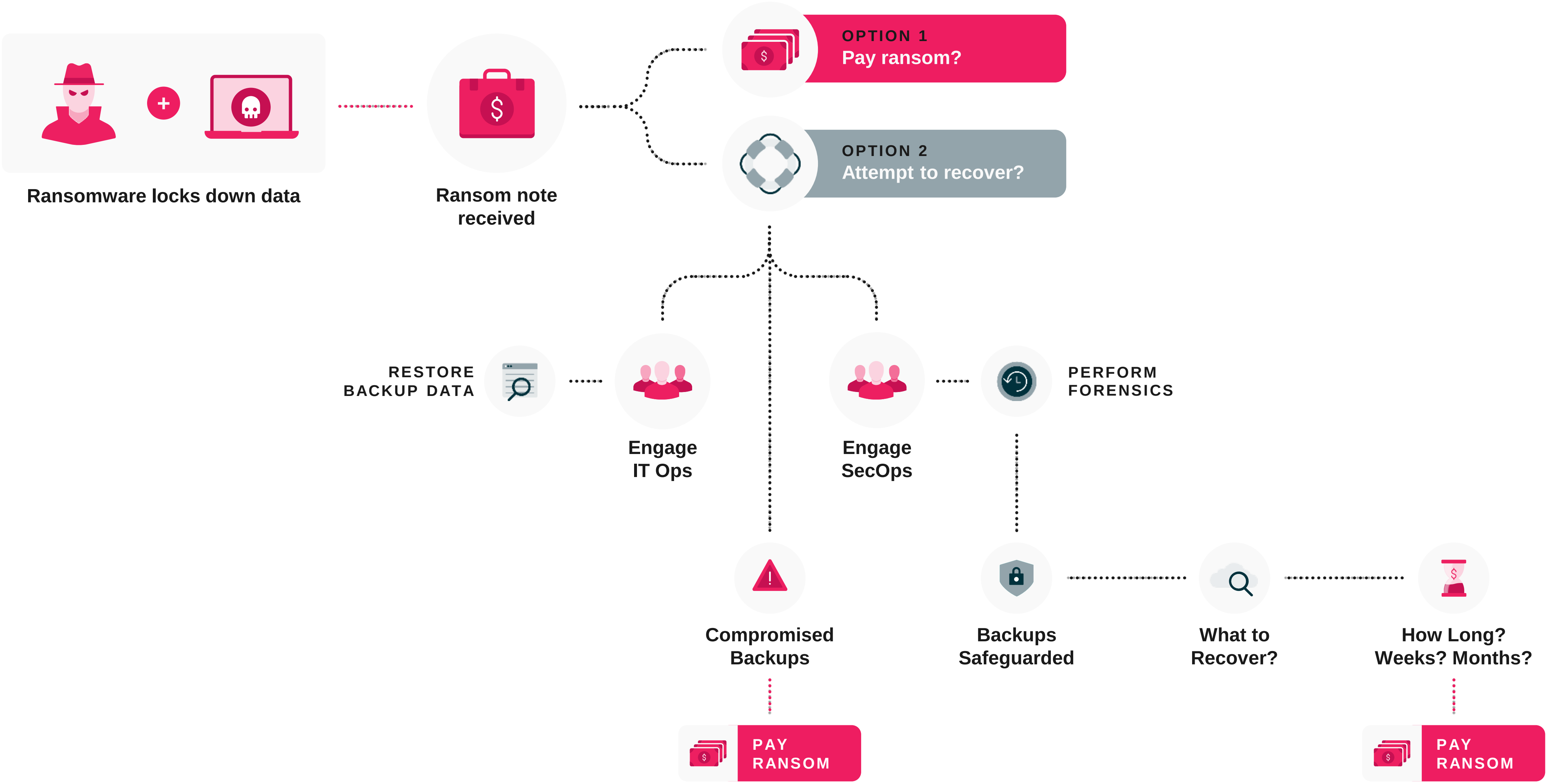
Remote Protection

Use Case: Cost Avoidance for Remote Locations

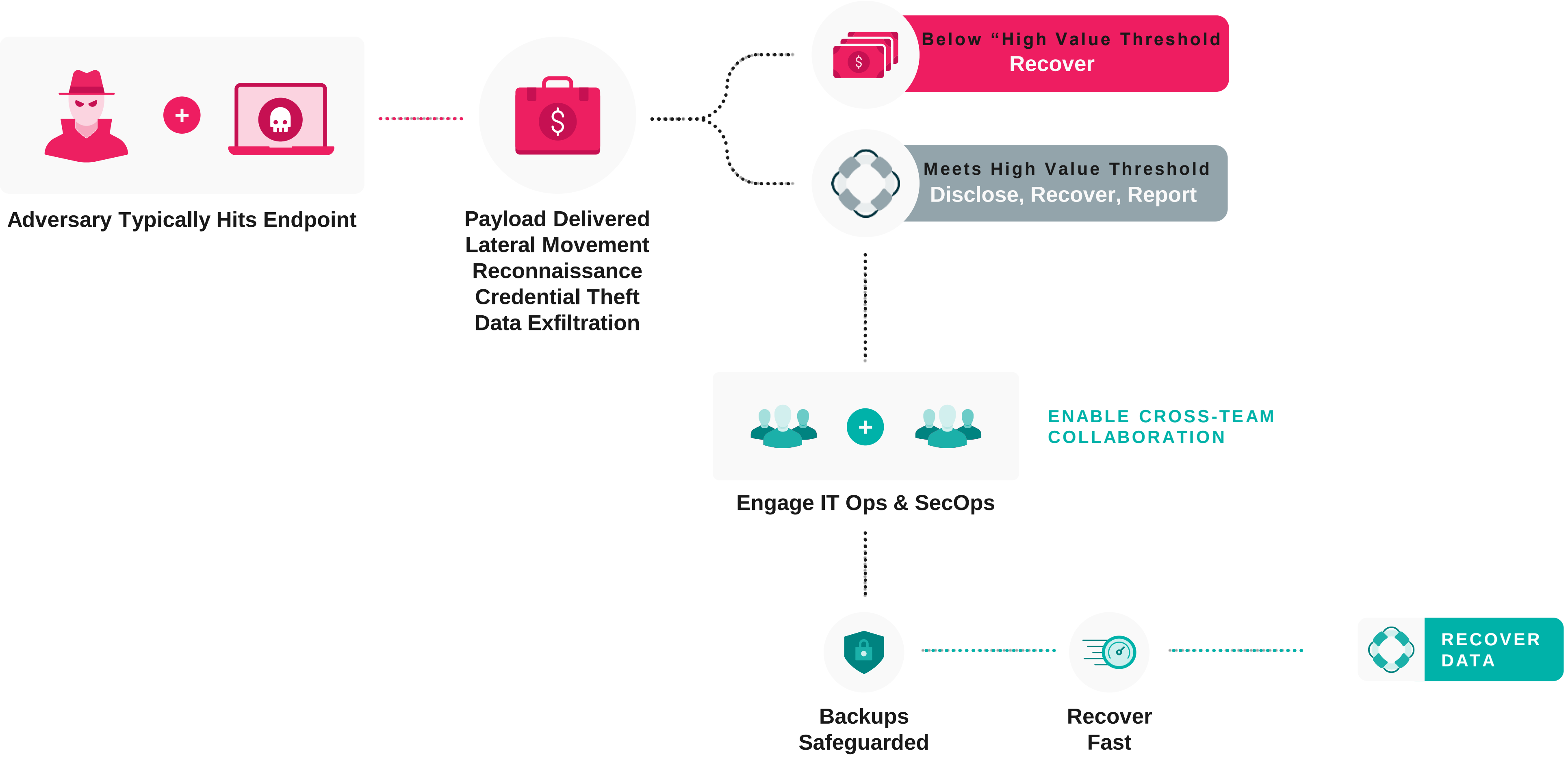


60% + COST AVOIDANCE + SAVINGS

Ransomware Use Case in SLED, Healthcare, Education



Data Exfiltration & Sensitive Data Breaches in Public Sector



Adversary Typically Hits Endpoint

Payload Delivered
Lateral Movement
Reconnaissance
Credential Theft
Data Exfiltration

Below “High Value Threshold
Recover

Meets High Value Threshold
Disclose, Recover, Report

Engage IT Ops & SecOps

ENABLE CROSS-TEAM COLLABORATION

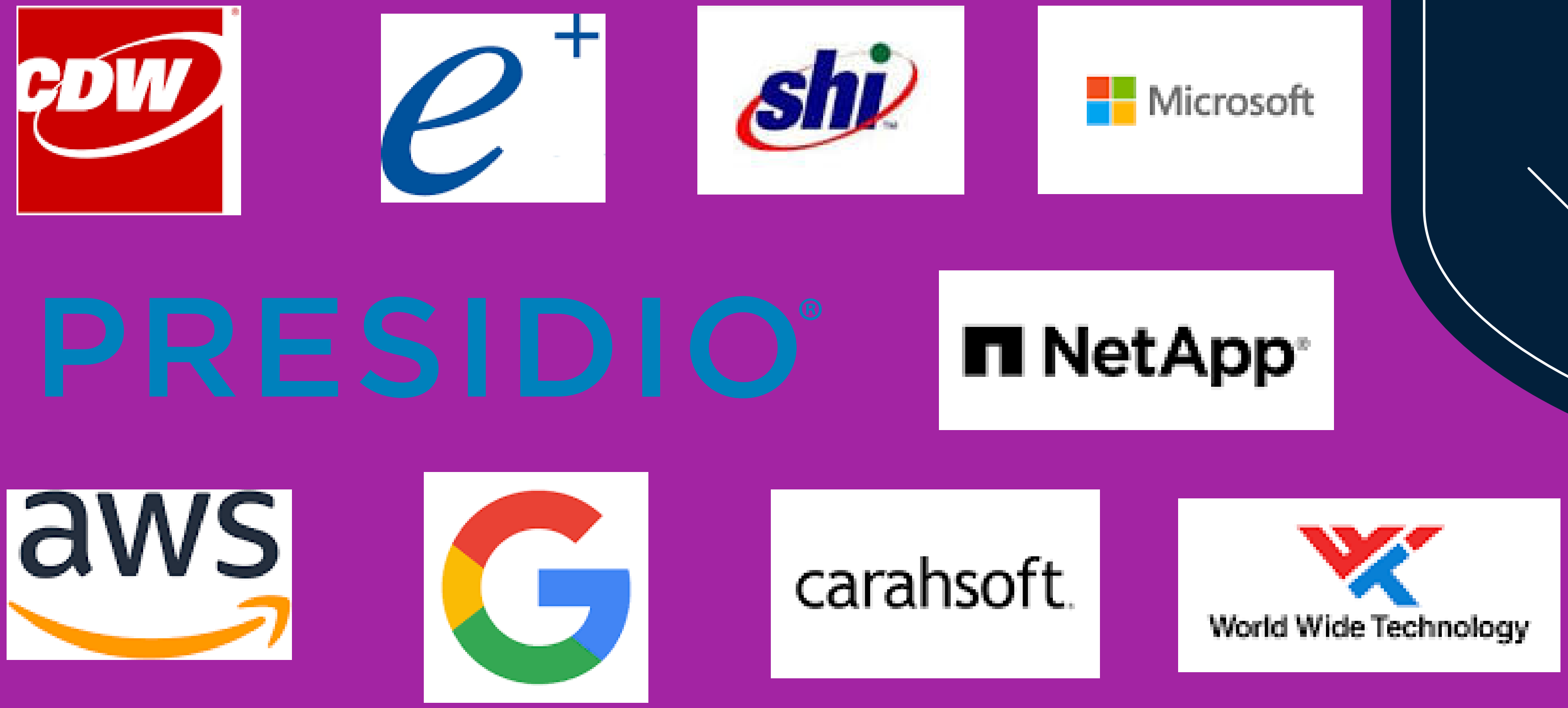
Backups Safeguarded

Recover Fast

RECOVER DATA

rubrik | **Zero Trust** Data Management™

Some of Rubrik’s Partners



rubrik | Zero Trust Data Management™

Jeffrey Phelan

jeffrey.phelan@rubrik.com

571-533-7726

Keith Evans

Keith.evans@rubrik.com

917-446-5036

Thank You.