Rubrik’s Innovation, Security, and Cloud Pedigree

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

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

Teams are married to Legacy Systems/Blockers

Legacy Systems: Lack Security & Resiliency Required to Operate in today’s Hybrid Cloud & High Security Environments
Organizations Throw People & Money at Data Management

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

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:

**Backup-as-a-Service**
- Protect applications with multi-tenant hosted or customers' managed environments

**Archive-as-a-Service**
- Provide long-term archival target (hosted or managed)

**Disaster Recovery-as-a-Service**
- Host mirrored site using Rubrik replication
- Provide near-zero RTO with live mounts for VMware VMs

**Cloud Migration-as-a-Service**
- Enable enterprise to migrate data / applications from on-prem to cloud or cloud to cloud

**Cloud Archive-as-a-Service**
- Enable long term archival in cloud with rapid-restore
- Offer bring-your-own-cloud (BYOC) choice to customers

**Dev/Test-as-a-Service**
- Eliminate customer’s need for Dev/Test Infrastructure
- Instantaneously create Dev/Test env. from any PIT copy
- Protect Remote / Branch offices w/SW
- Self-service backup and restore for end-users

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

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

© 2020 Rubrik. All rights reserved.
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
   - PENETESTING, 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

© 2020 Rubrik. All rights reserved.
Flexible, Agnostic, Automated, Hyperscale

Designed to be vendor-agnostic from Day 1.
Support industry-leading data sources, hypervisors, clouds.
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
Complete data availability, security, compliance, and governance on a single platform for on-premises and cloud
Is My Data Secure?

- Perimeter Security
- Network Security
- Endpoint Security
- Application Security
- Data

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?

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

Data

Cyber Resilience Built-In

Perimeter Security
Network Security
Endpoint Security
Application Security
### Key Principles of Cyber Resiliency: Rubrik Zero Trust Data Management

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

**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
- splunk®
- SWIMLANE
- ServiceNow
Zero Trust Data Management Architecture
Native Counter Measures Against Adversary TTPs

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

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
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

- **Production Data Center**
  - Denver, CO
  - Allentown, PA
  - Salt Lake City, UT

- **Data Protection Architecture**
  - Backup Server
  - Disk-based Backup
  - Management UI

- **Future Architecture**
  - Tier 1
  - Tier 2
  - Object Storage

- **Backup Server**
- **Management UI**
- **Tier 1**
- **Tier 2**
- **Object Storage**

- **Backup Server**
- **Disk-based Backup**
- **Management UI**

- **Object Storage**
- **Cloud**
- **Tier 1**
- **Tier 2**
Use Case: Modernized Architecture & Hybrid Cloud

Production Data Center
- Denver, CO
- Allentown, PA
- Salt Lake City, UT

Data Protection Architecture
- SLA Policy Engine
  - servicenow

Future Architecture
- Secondary data center
  - Microsoft Azure
  - AWS
  - Private

40% + COST AVOIDANCE + SAVINGS
Use Case: Cost Avoidance for Remote Locations

Data Protection Architecture

Backup Server → Disk-based Backup → Management UI

Remote Protection
Backup Server → Disk-based Backup → Management UI

Remote Sites

© 2020 Rubrik. All rights reserved.
Use Case: Cost Avoidance for Remote Locations

60% + COST AVOIDANCE + SAVINGS
Ransomware Use Case in SLED, Healthcare, Education

Ransomware locks down data → Ransom note received → Pay ransom? (OPTION 1)

Pay ransom?

Attempt to recover? (OPTION 2)

Compromised Backups → Pay Ransom

Backups Safeguarded → Pay Ransom


Engage IT Ops → Perform Forensics

Engage SecOps → Restore Backup Data
Data Exfiltration & Sensitive Data Breaches in Public Sector

Adversary Typically Hits Endpoint

Payload Delivered
Lateral Movement
Reconnaissance
Credential Theft
Data Exfiltration

Engage IT Ops & SecOps

Backups Safeguarded
Recover Fast

Below "High Value Threshold
Recover

Meets High Value Threshold
Disclose, Recover, Report

Enable Cross-Team Collaboration

Recover Data
Some of Rubrik’s Partners

CDW  e+  shi  Microsoft

PRESIDIO®  NetApp®

aws  G  carahsoft  World Wide Technology
Jeffrey Phelan
jeffrey.phelan@rubrik.com
571-533-7726

Keith Evans
Keith.evans@rubrik.com
917-446-5036
Thank You.