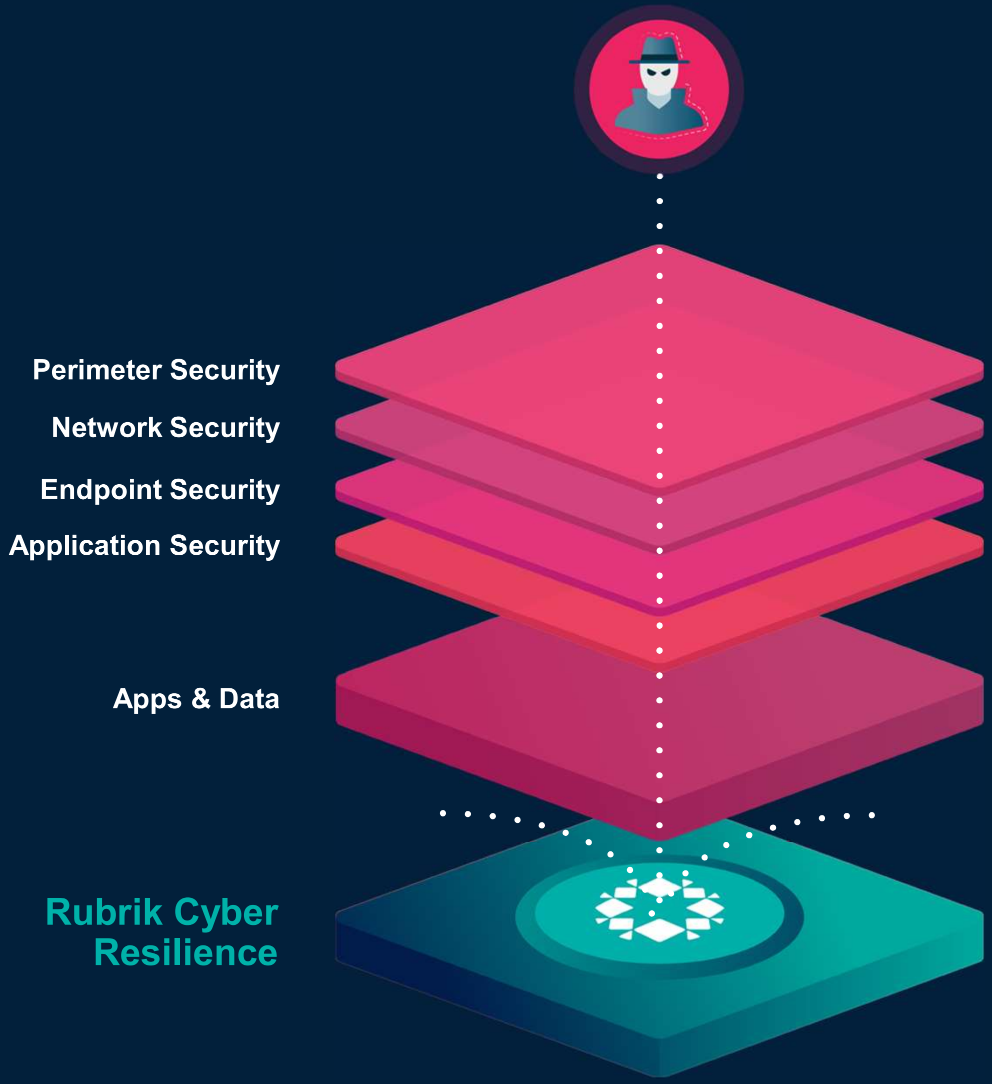
rubrik | Zero Trust Data Security™

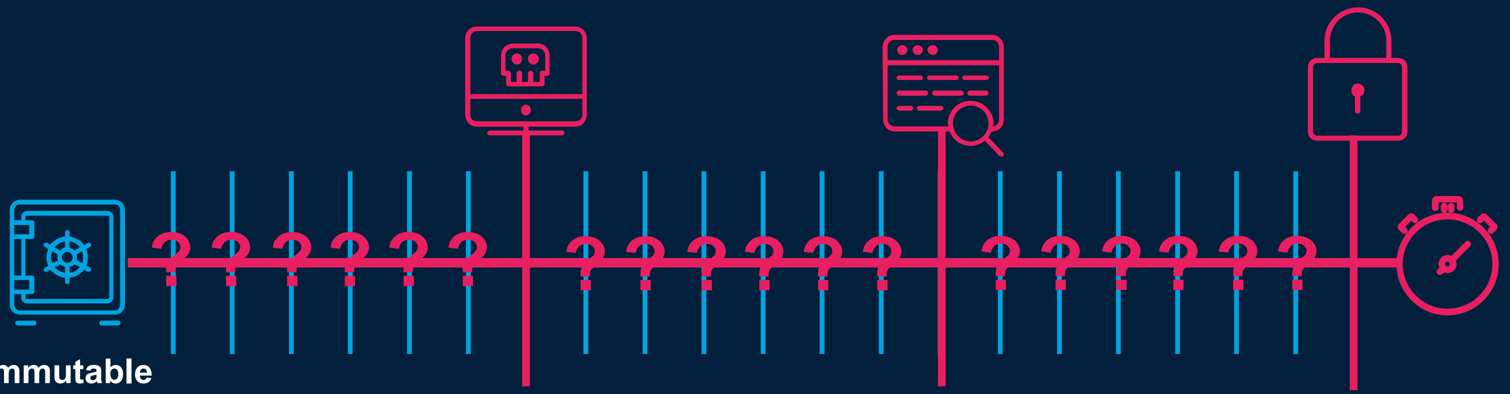
Verschlüsselt – und jetzt?

Martin Kucharcik
Christian Gladrow

Can You Recover From A Cyber Attack Within 24 Hours?



Why Backup ≠ Cyber Resilience



Immutable Backups

Attacker Gains Access ~5 Day Median Dwell Time

Data Exfiltrated Min Employee & Customer PII

Data Encrypted 60% VM-Level <5 Hour Attack

Business Impacted
Cost Increasing
What? When? How?

Can We Recover

1. Is your backup infrastructure & data 100% immutable?

What Do We Recover

2. How do you know what was encrypted if EDR is bypassed?

What Was Stolen

3. What sensitive data was on the network & at risk from exfiltration?

When To Recover To

4. How quickly can you find a clean recovery point & not re-infect?

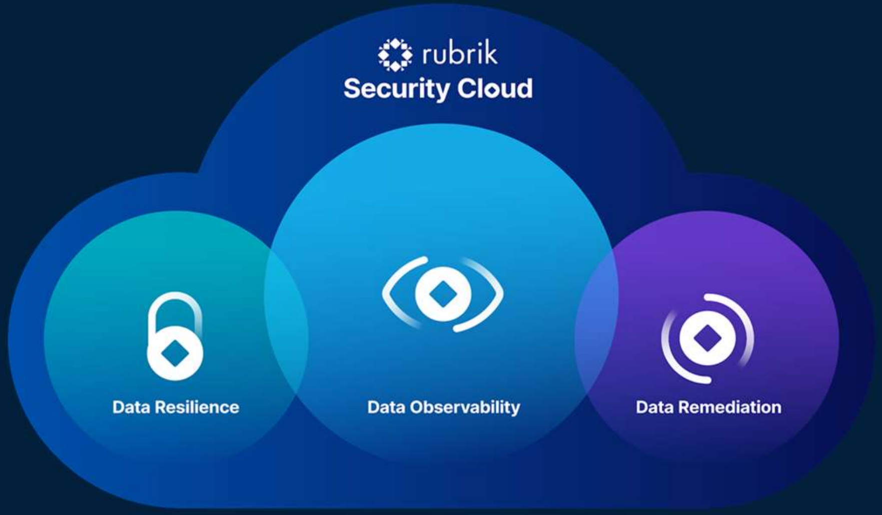
How Long Will It Take

5. How do you automate recovery, reduce downtime, test & prove?

Cyber Resilience

The Next Frontier in Cybersecurity is Data Security

Secure your data, wherever it lives, across enterprise, cloud, and SaaS – making your business unstoppable



rubrik

Security Cloud

Data Resilience

Data Observability

Data Remediation

Secure your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups

- **Enterprise Data Protection**
- **Cloud Data Protection**
- **Microsoft 365 Protection**

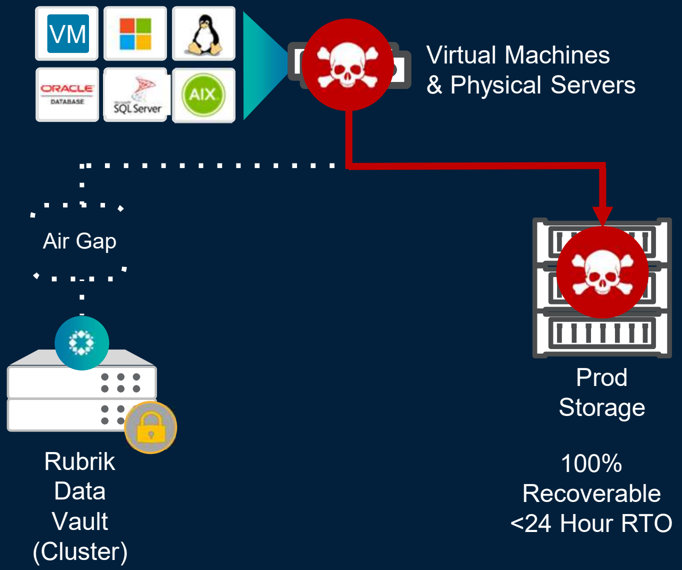
Continuously monitor your data for ransomware, manage sensitive data exposure, and hunt for indicators of compromise

- **Ransomware Monitoring & Investigation**
- **Sensitive Data Monitoring & Management**
- **Threat Monitoring & Hunting**
- **Data Security Command Center**

Surgically recover your apps, files or users while avoiding malware reinfection

- **Threat Containment**
- **Mass Recovery**
- **Orchestrated App Recovery**

Rubrik Data Vault Architecture


VM
ORACLE DATABASE
SQL Server
AIX
Virtual Machines & Physical Servers
Air Gap
Rubrik Data Vault (Cluster)
Prod Storage
100% Recoverable <24 Hour RTO

Physical Appliances - Converged backup, dedupe storage & vault

Physically Isolated - Survivable from attack, nothing running in hypervisor

Hardened Linux - No Windows, no downtime upgrade, minimal attack surface

Scale-out - Multi-TB to Multi-PB cluster, masterless, fault tolerant, massive parallelism

Encrypted - End-to-End by default, validated FIPS 140-2, BYOK via KMS

Air Gapped - OS, shell & storage not accessible on the network (no NFS/SMB)

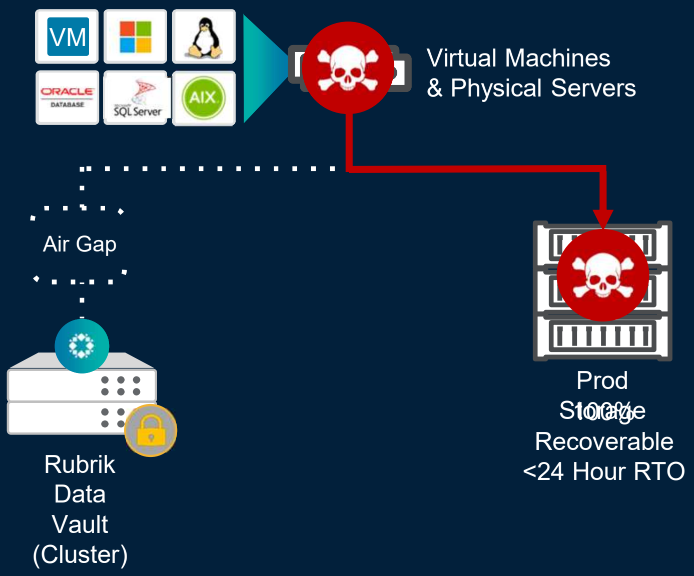
Immutable - 100% of backups CANNOT modified/encrypted, append only filesystem

Secured - Mandatory MFA, local users w/TOTP, retention lock & NTP protection

Built-in Scanners - 1st copy, scale-out performance, reduce RPO & RTO

Major attack is now a recoverable event in hours, not days..

Bunker-in-a-box



Physical Appliances - Converged backup, dedupe storage & vault

Physically Isolated - Survivable from attack, nothing running in hypervisor

Hardened Linux - No Windows, no downtime upgrade, minimal attack surface

Scale-out - Multi-TB to Multi-PB cluster, masterless, fault tolerant, massive parallelism

Encrypted - End-to-End by default, validated FIPS 140-2, BYOK via KMS

Logical Air Gap - OS, shell & storage not accessible on the network (no NFS/SMB)

Immutable - 100% of backups CANNOT modified/encrypted, append only filesystem

Secured - Mandatory MFA, local users w/TOTP, retention lock & NTP protection

Built-in Scanners - 1st copy, scale-out performance, reduce RPO & RTO

Major attack is now a recoverable event in hours, not days..

Data Resilience - Zero Trust Data Management

Retention Lock

Secure Local Users with TOTP

Secure AD Logins with MFA & RBAC

End-to-End Encryption

No 3rd Party Apps

Immutable File System

Bunker-in-a-box
Hardened Secure Linux Build
Vendor Patched & No Shell Access
IPMI/OOB Mgmt Disconnected

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, anything SAML2.0 compliant
- Multi-factor on all AD integrated logins, alerts/syslog for failed logins
- RBAC, read-only admins, least privilege access & API tokens

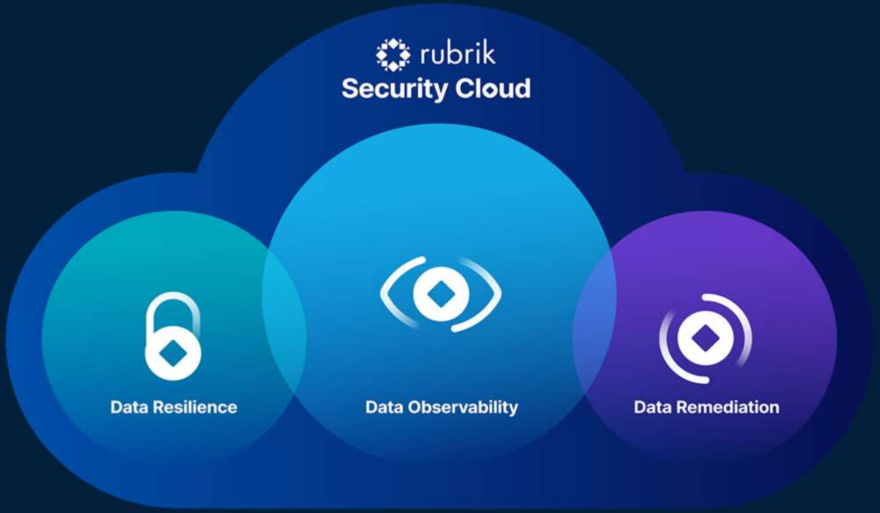
Secure Local Admin Logins
- Built-in TOTP (Time-based One-Time Password)
- Secure local accounts in minutes any Android/IOS device
- Removes backdoor of local account access, also applies to SSH
- Required account for recovery in event of attack (AD compromised)

Retention Lock (support driven process)
- Prohibits backup admin 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

Air Gap + Immutable + Encryption + Secured Logins + Retention Lock + NTP Protection
= Impenetrable From Ransomware Attacker

The Next Frontier in Cybersecurity is Data Security

Secure your data, wherever it lives, across enterprise, cloud, and SaaS – making your business unstoppable



Secure your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups

Continuously monitor your data for ransomware, manage sensitive data exposure, and hunt for indicators of compromise

Surgically recover your apps, files or users while avoiding malware reinfection

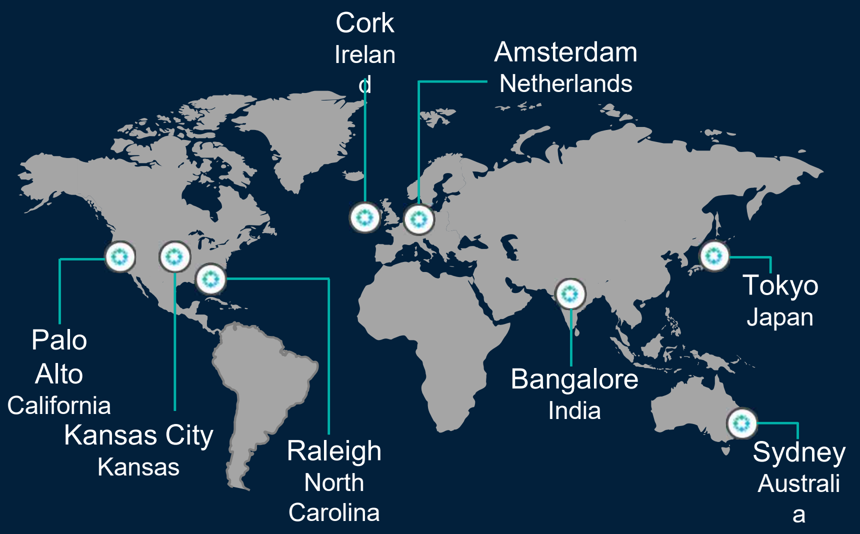
- Enterprise Data Protection
- Cloud Data Protection
- Microsoft 365 Protection

- Ransomware Monitoring & Investigation
- Sensitive Data Monitoring & Management
- Threat Monitoring & Hunting
- Data Security Command Center

- Threat Containment
- Mass Recovery
- Orchestrated App Recovery

Rubrik Ransomware Response Team (RRT)

- Call Rubrik support & report attack (1-650-300-5962)
- Global 24x7x365 team for all Rubrik customers
- Majority of attacks on weekends & national holidays
- Over 150 ransomware recoveries performed
- Bridge between Data Protection, Security & Incident Response
- Consistent, confidential, custom & speedy recovery
- We stay until you no longer need us



rubrik

Ransomware Recovery Warranty

Rubrik Enterprise Edition ™

Enterprise Edition

+

Industry Data Security Best Practices

Customer Experience Manager & Monthly health checks

=

Up to $10 M Ransomware Recovery Warranty*

250 TB – 500 TB $250K payout
500 TB – 750 TB $500K payout
750TB – 5 PB $1mil payout
5 PB – 10 PB $5 mil payout
10 PB and above $10 mil payout

**Warranty provides payout of up to $10m, based on data protected by Rubrik. For recovery related expenses. Subject to terms and conditions.*

5000+ customers. 100% Protected.

RANSOMWARE
rubrik
WARRANTY
RECOVERY

FinServ	Manufacturing	Healthcare	Government	Security	Education	Media	Technology	Retail
Allstate	Bioverativ	UCDAVIS HEALTH	IRS	SONICWALL	HARVARD UNIVERSITY	GANNETT	CARFAX	THE HOME DEPOT
BARINGS	Driscoll's	NAVAL MEDICAL CENTER SAN DIEGO	FDA	Trellix	Duke UNIVERSITY	SESAME WORKSHOP	CapTech	ESTĒE LAUDER
CITY NATIONAL BANK The way up.	LUCID	Atrium Health	UNITED STATES NAVY	Pulse Secure	UC San Diego	AMERICA'S TEST KITCHEN	NVIDIA	petco
elements FINANCIAL	gsk GlaxoSmithKline	Seattle Children's	Scottish Government Riaghaltas na h-Alba gov.scot	f5	NYU	Roku	Adobe	SEPHORA
MUFG	HONDA	DSH	U.S. DEPARTMENT OF HOMELAND SECURITY	proofpoint	Penn University of Pennsylvania	LAMAR	DocuSign	Domino's
CBRE	mazda	UCI Health	Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE	imperva	UCSB	HEARST	Expedia	Krispy Kreme DOUGHNUTS
KeyCorp	dermalogica	LEE HEALTH	CalEPA California Environmental Protection Agency	Carbon Black.	UNIVERSITY OF THE PACIFIC	meredith	T2 TAKE TWO INTERACTIVE	T··Mobile·

Don’t Backup. ***Go Forward.***