



Prepare for attack – Luck is not a strategy

Jaap Brasser, Technical Marketing Engineer
Salvatore Buccoliero, Channel SE Rubrik

Salvatore Buccoliero



Tweets @ totobucco
Private Father. Dog, Cat & Horse owner
Works Channel SE @ Rubrik.com
Does IT Startups, Speaker, Enabler
Likes Automation & Simplicity

Jaap Brasser



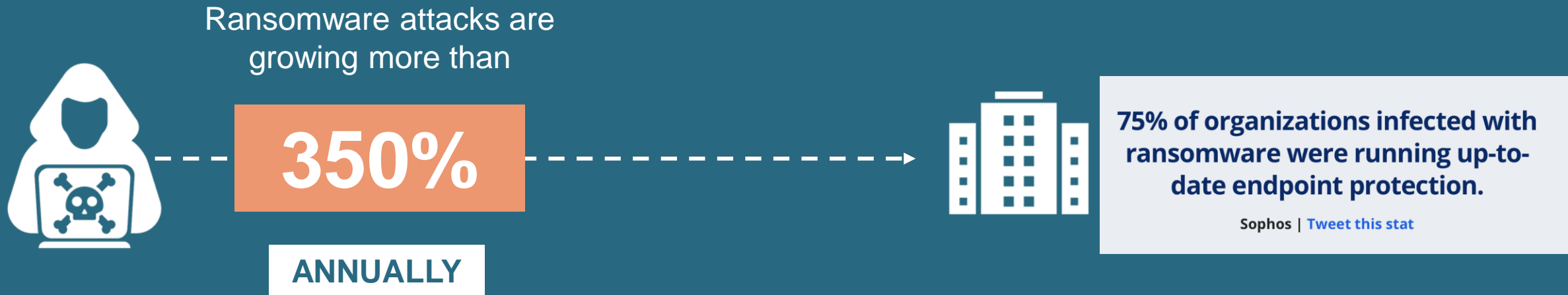
Tweets @ jaap_brasser
Blogs @ jaapbrasser.com
Works Tech Marketeer @ Rubrik.com
Does Blogger, Speaker, Tech Enthusiast
Likes Cloud Automation & Security





We've got BUGS Incoming!!!

Security Attacks Happen



Source: Cisco 2017 Annual Cybersecurity Report

Agenda

Ransomware Landscape

Foundation – Rubrik Cloud Data Management

Polaris – Platform, GPS & Radar

*Demos

ran · som · ware

/ˈransəm , we(ə)r/

noun

a type of malicious software designed to block access to a computer system until a sum of money is paid.

Base Definition

We'll make it fast.

- Malware that typically infects **endpoints** (laptops, etc.)
- Encrypts **local filesystems** and **attached network mounts**
- Spread via browser vulnerabilities (malicious pages), e-mail attachments
- In some cases Targeted Malware created by foreign agencies to attack specific targets. Others may fall victim
- Targeted attacks on individual storage vendors plausible – immutability will come into play over time.
- (Previous) Best known name = Cryptolocker

Impact

- In a report published by *Wired*, a White House assessment pegged the total damages brought about by **NotPetya** to more than **\$10 billion**. This was confirmed by former Homeland Security adviser Tom Bossert, who at the time of the attack was the most senior cybersecurity focused official in the US government.^[42]
- During the attack initiated on 27 June 2017, the **radiation monitoring system** at Ukraine's **Chernobyl Nuclear Power Plant** went offline.^[43] Several Ukrainian ministries, banks and metro systems were also affected.^[44] It is said to have been the most destructive cyberattack ever.^[45]
- Among those affected elsewhere included British advertising company **WPP**,^[44] **Maersk Line**,^[46] American pharmaceutical company **Merck & Co.**, Russian oil company **Rosneft** (its oil production was unaffected^[47]), multinational law firm **DLA Piper**,^[44] French construction company **Saint-Gobain** and its retail and subsidiary outlets in Estonia,^[48] British consumer goods company **Reckitt Benckiser**,^[49] German personal care company **Beiersdorf**, German logistics company **DHL**,^[50] United States food company **Mondelez International**, and American hospital operator Heritage Valley Health System.^{[8][51]} The **Cadbury's Chocolate Factory** in **Hobart**, Tasmania, is the first company in Australia to be affected by Petya.^[52] On 28 June 2017, **JNPT**, India's largest container port, had reportedly been affected, with all operations coming to a standstill.^[53] **Princeton Community Hospital** in rural West Virginia will scrap and replace its entire computer network on its path to recovery.^[54]
- The business interruption to **Maersk**, the world's largest container ship and supply vessel operator, was estimated between **\$200 and \$300m** in lost revenues.^[55]
- **Jens Stoltenberg**, **NATO** Secretary-General, pressed the alliance to **strengthen its cyber defenses**, saying that a cyberattack could trigger the **Article 5 principle** of collective defense.^{[56][57]}

The world has gotten scarier
And it's not slowing down...

Trends

- Backup media also getting attacked
- Delivering ransomware through files rather than email
- Delivering ransomware through infected websites
- Using multi-threaded attacks
- Slowing down the encryption process
- Targeting modern operating systems less
- We are seeing a drop of attacks, but increase in vectors

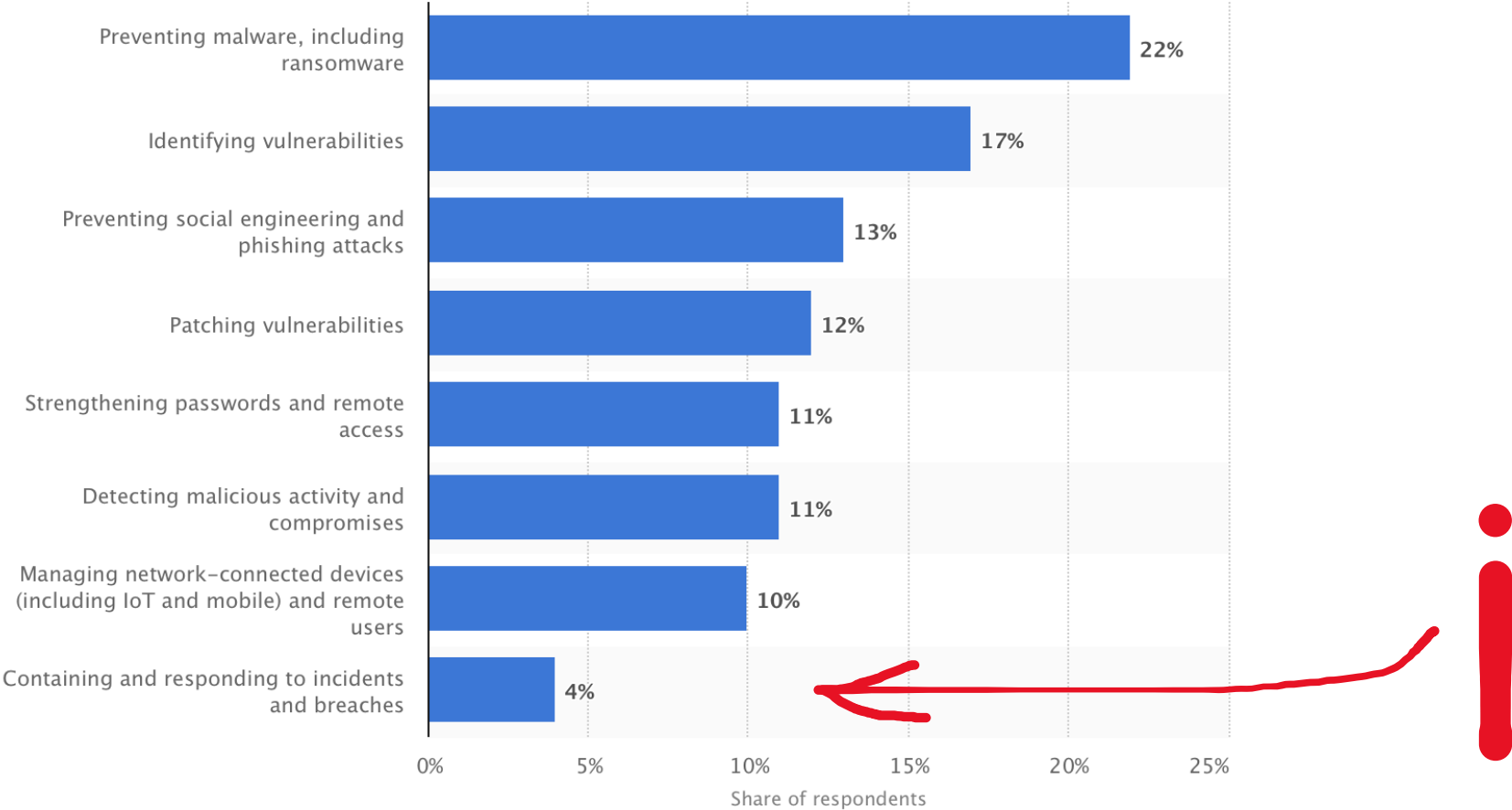
What's New

Maturing Market

- RaaS Kits – Ransomware as a Service Kits
 - Market Segmentation
 - Customer Service Improvements
- Reliable Payment Model – Bitcoin Impact

How the CIO's think today

Which IT security tasks are you facing the most pressure to address?



Classic Defense Recommendations

Operational Overhead?

1. Education
2. Antivirus, Patching, Filtering
3. Insurance
4. Data Protection – Backups

Key Solution Components

What we've seen that makes a difference...

1. Reliability of Data Recovery

- a. Simplicity of Setup + Day to Day Operation
- b. Immutability of Snapshots
- c. Accelerated Detection

2. Speed of Data Recovery

- a. Speed of restore via live mount
- b. Automation/API to enhance Restore Capabilities

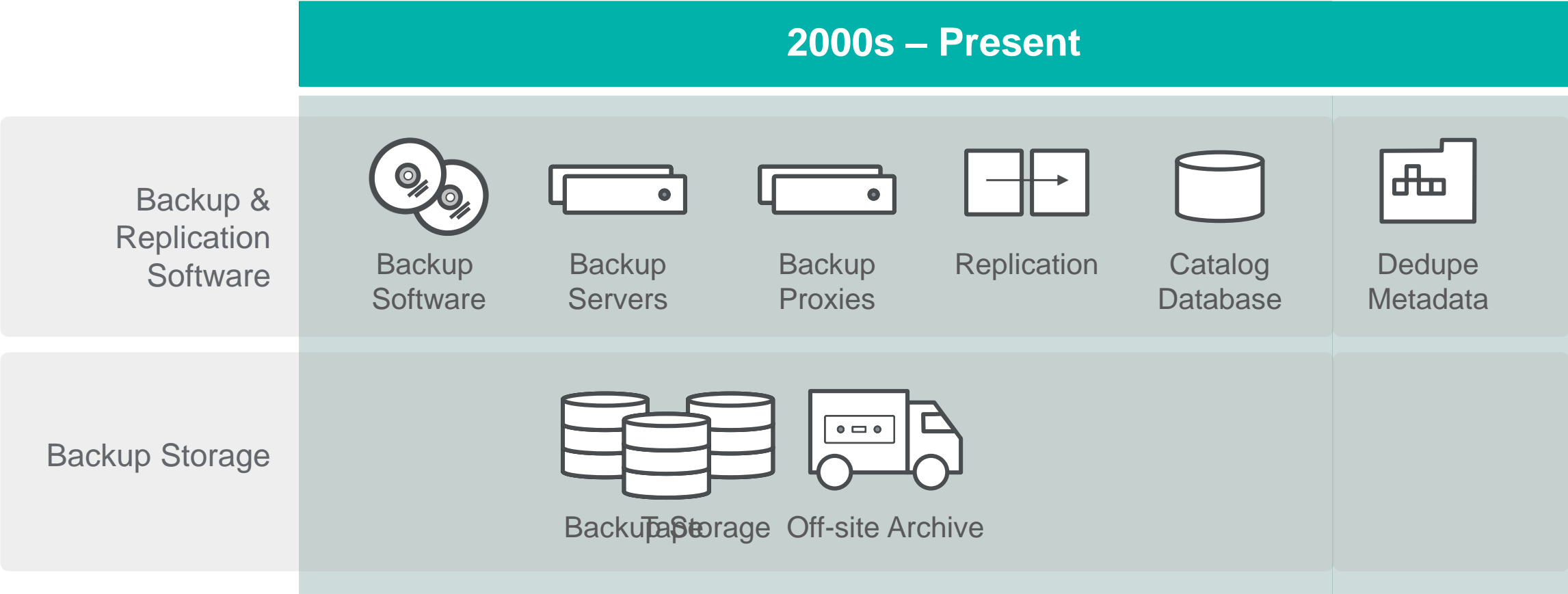
Foundation - Rubrik Cloud Data Management

Simplicity is the ultimate sophistication

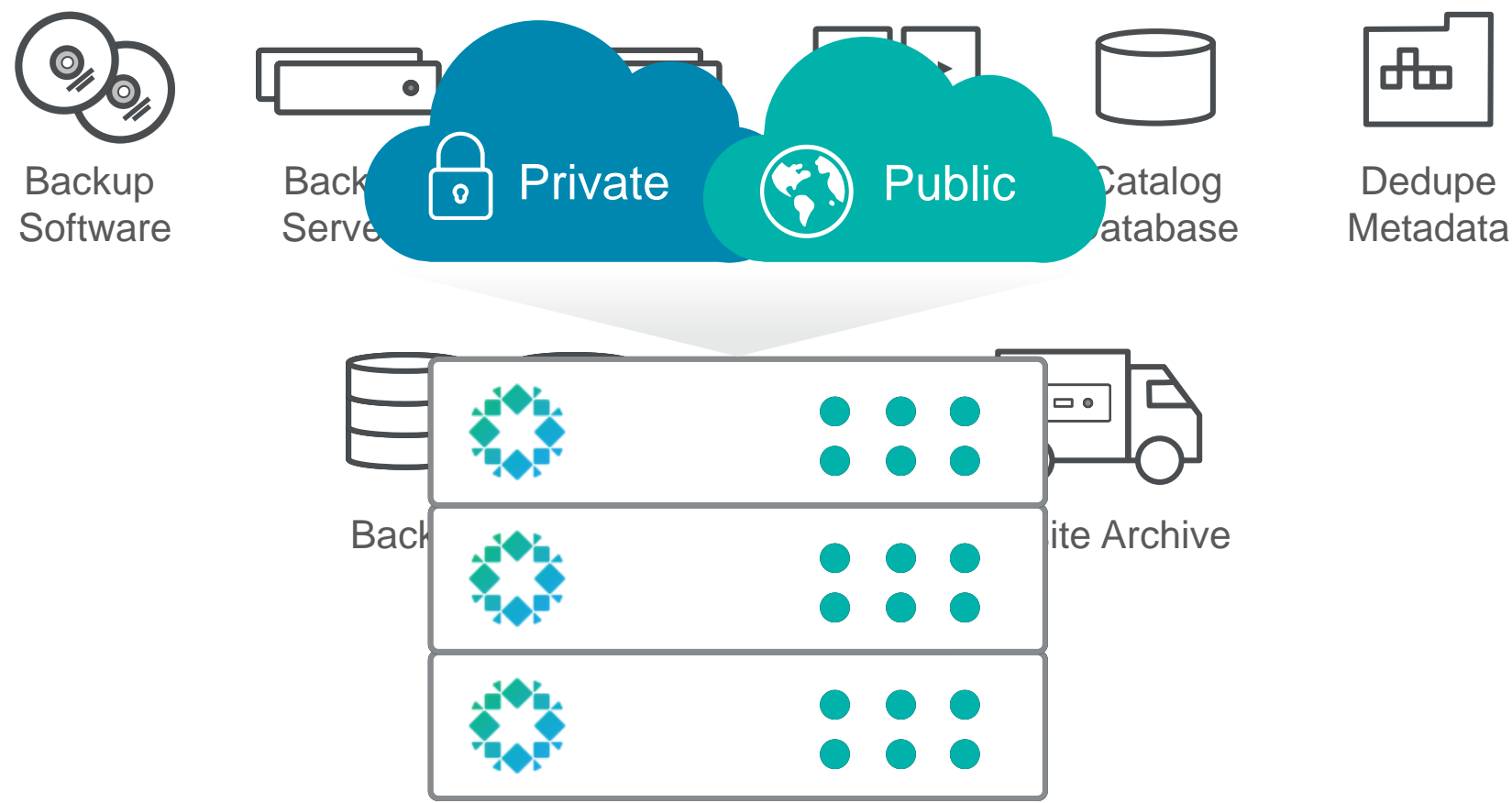
Leonardo da Vinci

Whatever you do. Whatever you buy.
Simplify your Architecture & Expect More.

Data Management: 2000s to Present

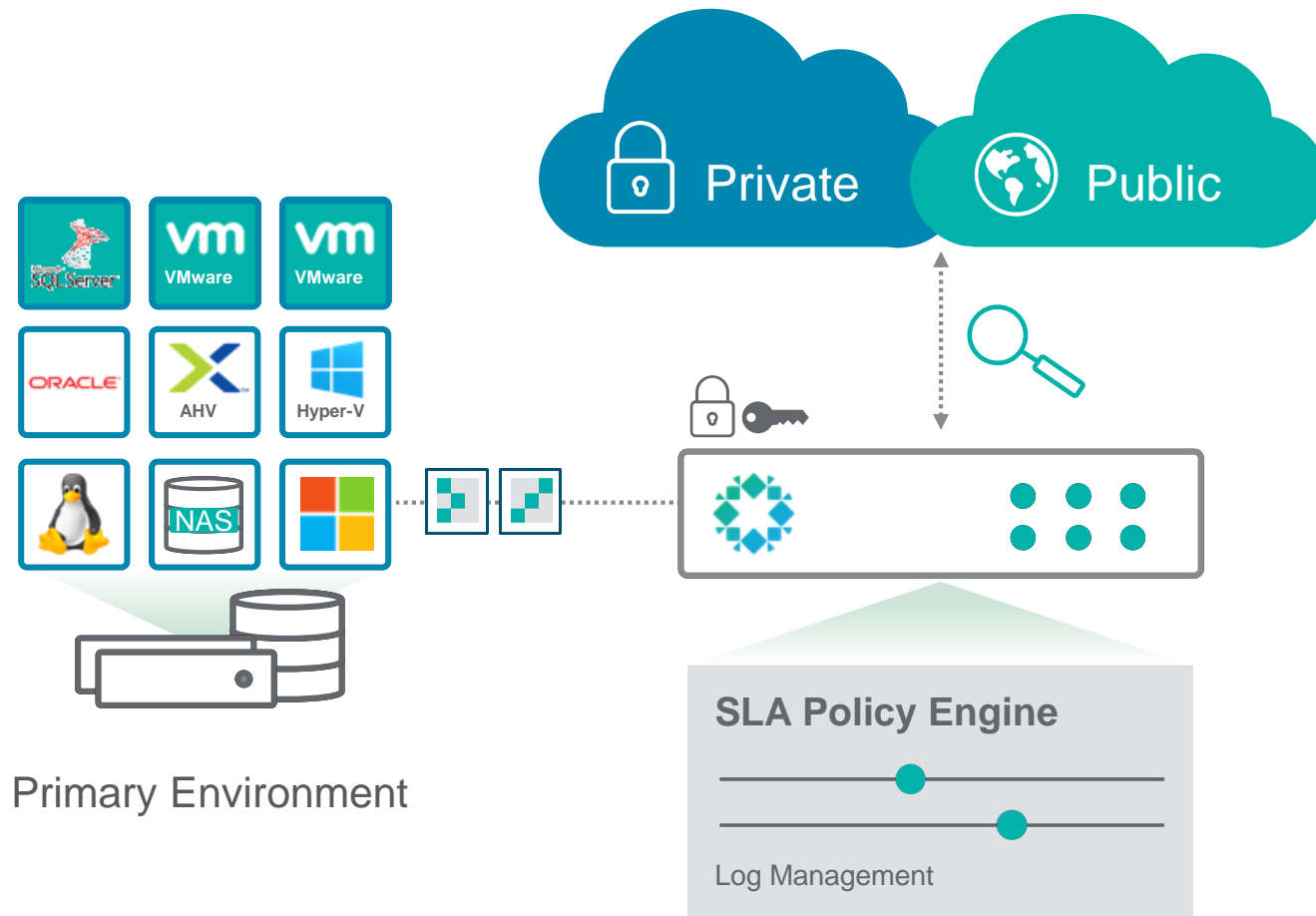


Meet Rubrik Cloud Data Management



Software fabric for orchestrating apps and data across clouds. No forklift upgrades.

How It Works



Quick Start: Set up in minutes. Auto-discovery.

Automate: Intelligent SLA policy engine for effortless management.

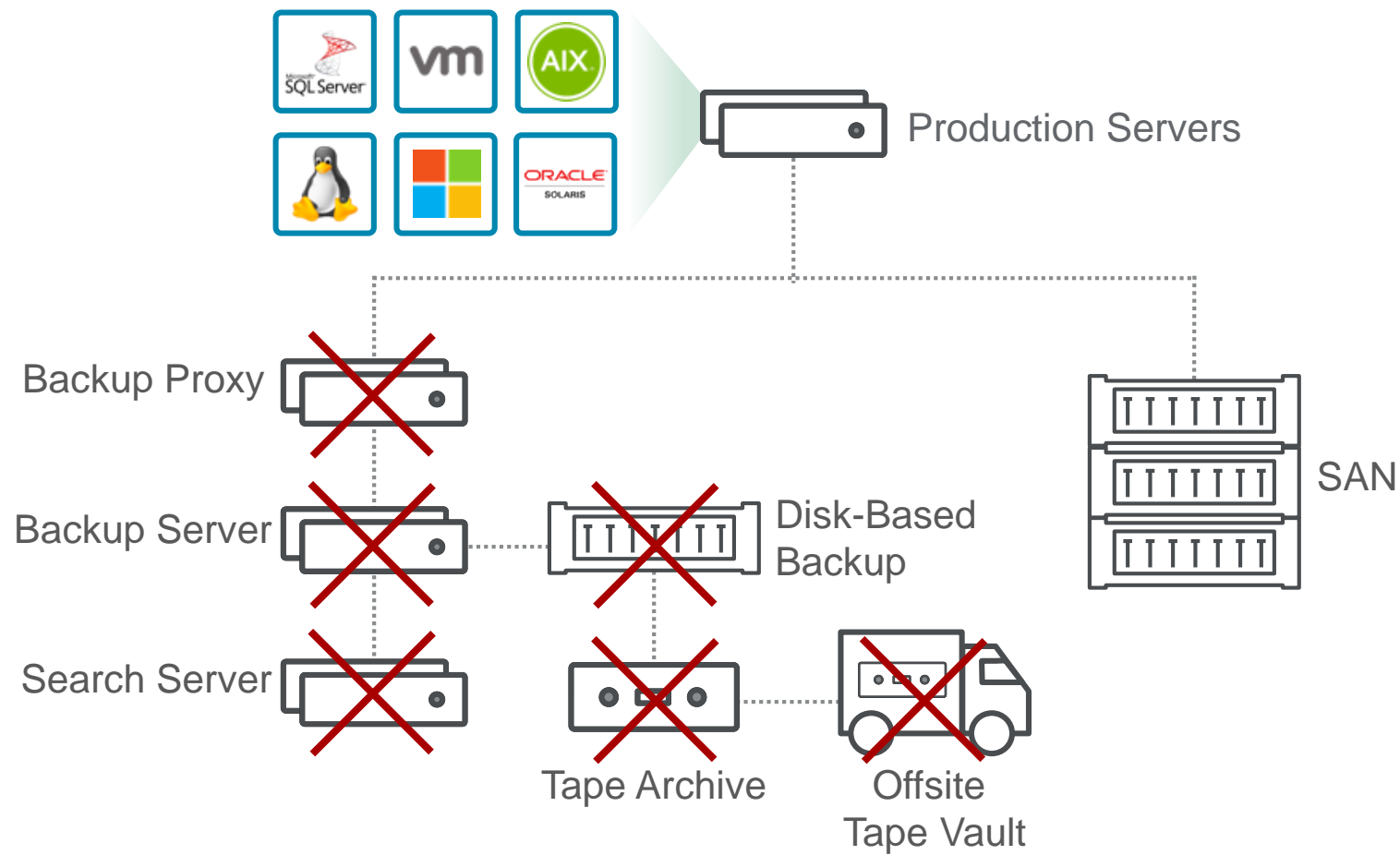
Rapid Ingest: Parallel ingest accelerates snapshots and eliminates stun. Content-aware dedupe. One global namespace.

Instant Recovery: Live Mount VMs & SQL Server. Instant search and file restore.

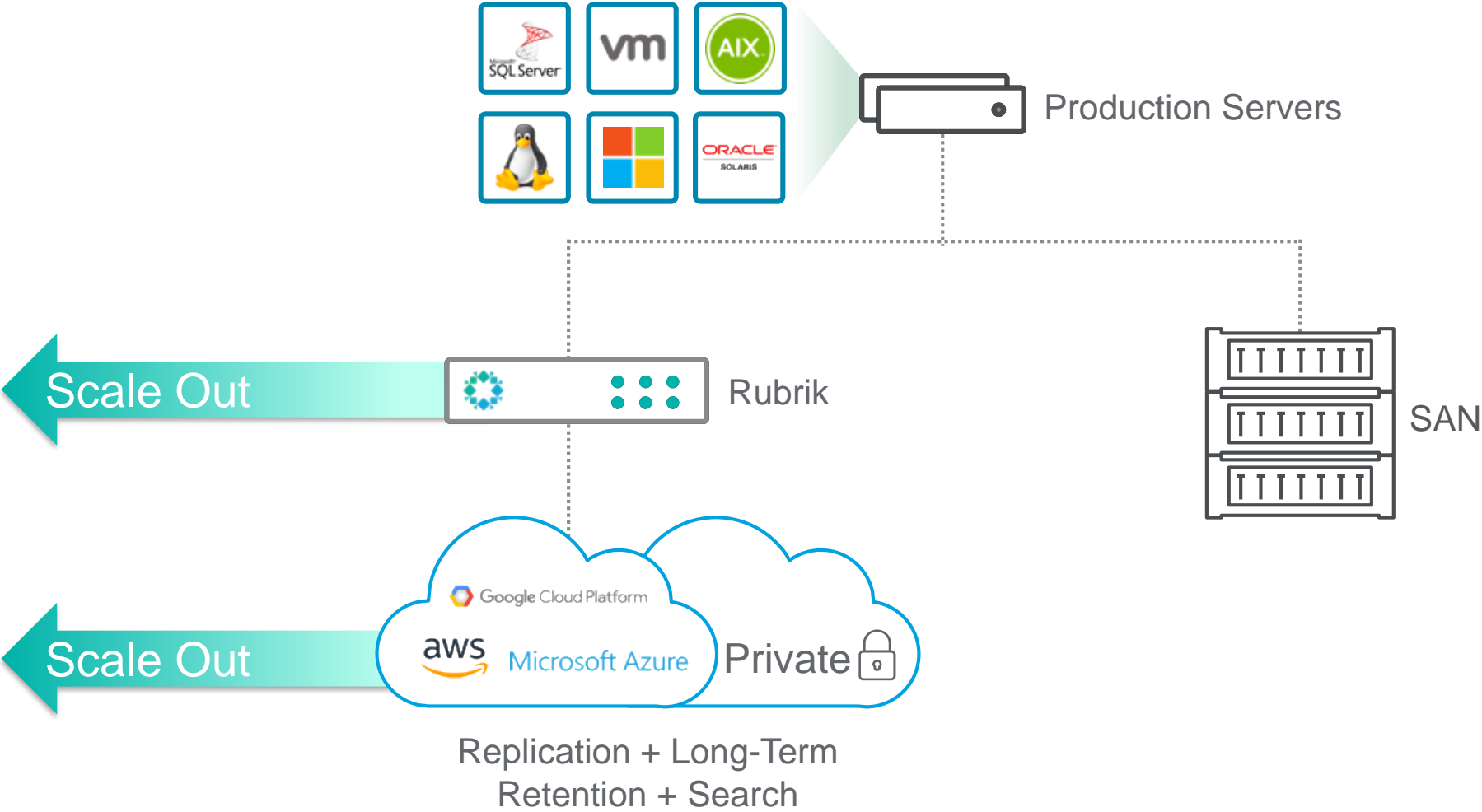
Secure: End-to-end encryption. Immutability to fight ransomware.

Cloud: Archive to the public or private cloud with CloudOut. Adopt the cloud for DR or test / dev with CloudOn. Protect apps in cloud with CloudCluster.

Your Data Center Today






Rubrik Simplifies Your Data Center



Mix and Match – True Webscale

- Unlimited scalability
- Scale cluster with different capacities
- Scale cluster across different series
- Grow or shrink without downtime

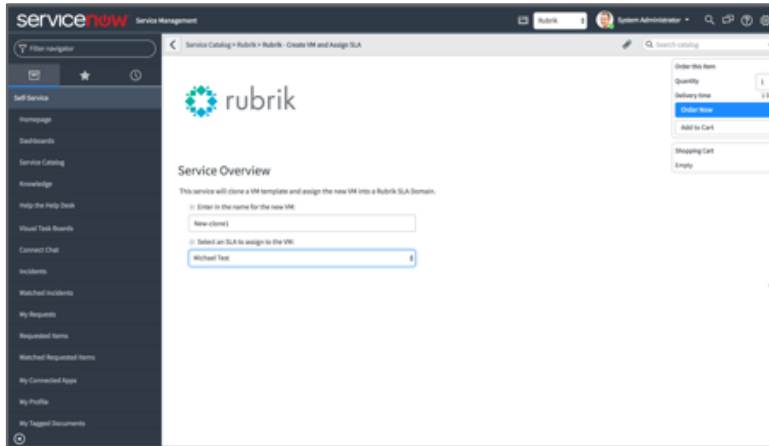
	r334 Hardware Specs*	r344 Hardware Specs*	r348 Hardware Specs*	r3410 Hardware Specs*	r528 Hardware Specs
CPU	3 x Intel 8-Core 2.4 GHz Haswell	4 x Intel 8-Core 2.4 GHz Haswell	4 x Intel 8-Core 2.4 GHz Haswell	4 x Intel 8-Core 2.4 GHz Haswell	4 x Intel 8-Core 2.4 GHz Haswell
Memory	192 GB DDR4	256 GB DDR4	256 GB DDR4	256 GB DDR4	256 GB DDR4
Storage	9 x 4 TB HDD 3 x 400 GB SSD	12 x 4 TB HDD 4 x 400 GB SSD	12 x 8 TB HDD 4 x 400 GB SSD	12 x 10 TB HDD 4 x 400 GB SSD	12 x 8 TB HDD 2 x 800 GB SSD
Network Connections * SFP+ or 10GbE-T	6 x 10GbE* 6 x 1GBase-T 3 x 1GBase-T (IPMI)	8 x 10GbE* 8 x 1GBase-T 4 x 1GBase-T (IPMI)	8 x 10GbE* 8 x 1GBase-T 4 x 1GBase-T (IPMI)	8 x 10GbE* 8 x 1GBase-T 4 x 1GBase-T (IPMI)	4 x 10GbE* 4 x 1GBase-T 2 x 1GBase-T (IPMI)
	 100-125	 200-300	 500-700	 600-800	 500-700



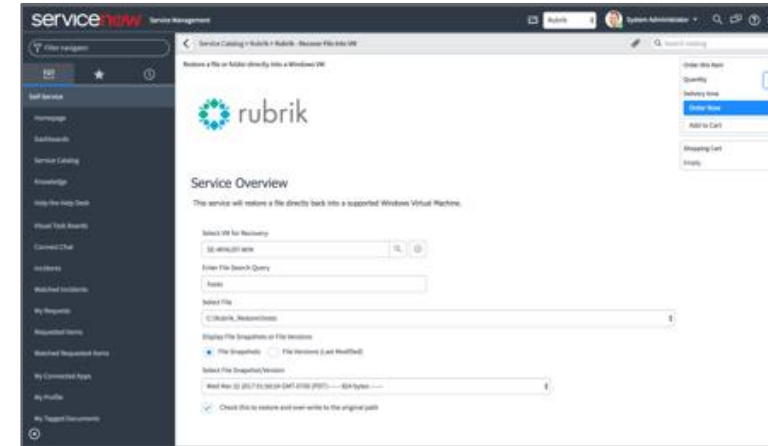
	r6304 Small Environments	r6404 Growing Environments	r6408 Enterprise Environments	r6410 Large-scale Environments
CPU	3 x Intel 10-Core 2.2 GHz	4 x Intel 10-Core 2.2 GHz	4 x Intel 10-Core 2.2 GHz	4 x Intel 10-Core 2.2 GHz
Memory	192GB DDR4	256GB DDR4	384GB DDR4	384GB DDR4
Storage	9 x 4TB HDD 3 x 400GB SSD	12 x 4TB HDD 4 x 400GB SSD	12 x 8TB HDD 4 x 400GB SSD	12 x 10TB HDD 4 x 400GB SSD
Network Connections	3 Dual-Port x 10GbE/25GbE (data) ¹ 3 Dual-Port x 10GBase-T (mgmt) 3 x 1GBase-T (IPMI)	4 Dual-Port x 10GbE/25GbE (data) ¹ 4 Dual-Port x 10GBase-T (mgmt) 4 x 1GBase-T (IPMI)	4 Dual-Port x 10GbE/25GbE (data) ¹ 4 Dual-Port x 10GBase-T (mgmt) 4 x 1GBase-T (IPMI)	4 Dual-Port x 10GbE/25GbE (data) ¹ 4 Dual-Port x 10GBase-T (mgmt) 4 x 1GBase-T (IPMI)



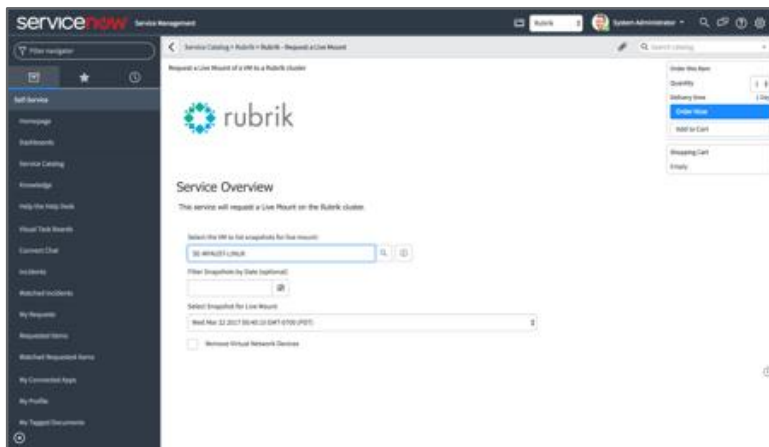
Rubrik + ServiceNow ITOM: How It Works



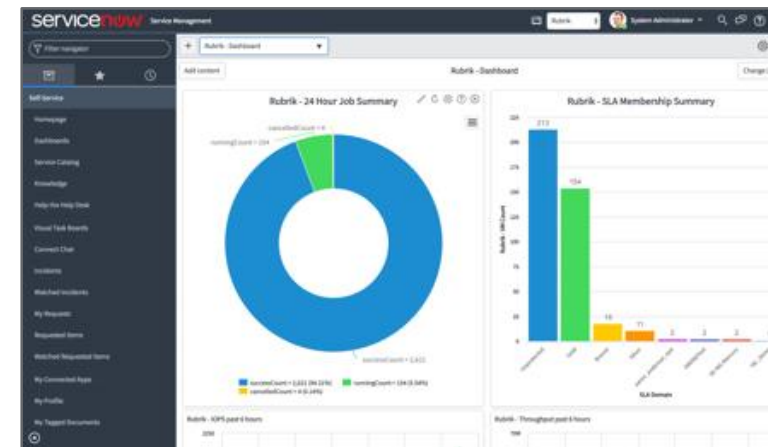
Automated Data Protection
Provision VMs automatically with one policy engine



Self-service File Recovery
Instantly recover files or entire VMs within ServiceNow

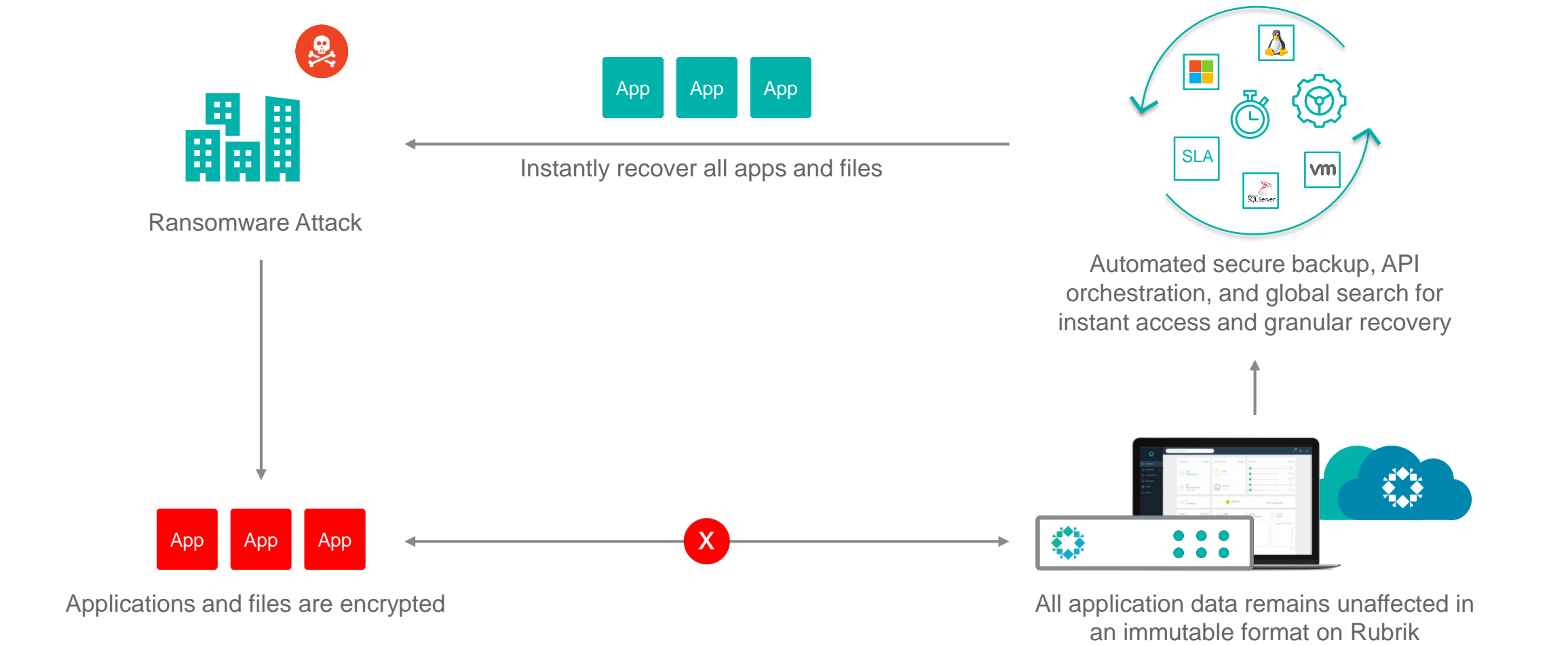


Test/Dev
Accelerate test/dev by instantly mounting VMs on Rubrik



Customized Analytics
Generate insights on operational efficiencies

Native Immutability to Fight Ransomware



Why is this important?

Backup Job

File Home Share View

⏮ ⏪ ⏩ ⏭

This PC > Veeam Backup (V:) > Backup Job

Search Backup Job

★ Favorites

This PC

Desktop

Documents

Downloads

Music

Pictures

Videos

Local Disk (C:)

DVD RW Drive (D:) S

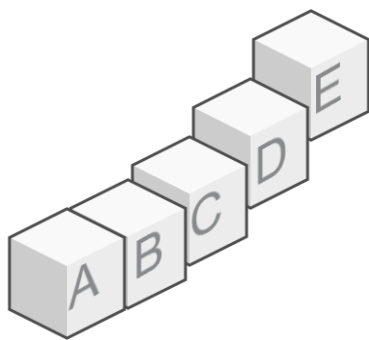
Veeam Backup (V:)

Network

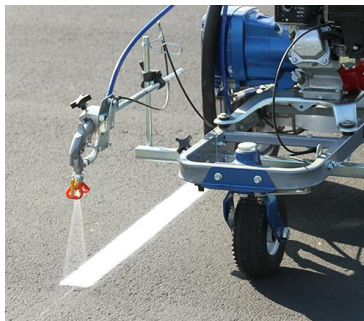
Name	Date modified	Type	Size
Backup Job.vbm.rapid	16.1.2018 22:32	RAPID File	293 KB
Backup JobD2017-12-08T220030.vrb.rapid	19.1.2018 1:51	RAPID File	22 167 353 ...
Backup JobD2017-12-09T220021.vrb.rapid	16.1.2018 22:32	RAPID File	3 582 666 KB
Backup JobD2017-12-10T220017.vrb.rapid	19.1.2018 1:51	RAPID File	14 213 337 ...
Backup JobD2017-12-11T225828.vrb.rapid	19.1.2018 1:51	RAPID File	12 175 955 ...
Backup JobD2017-12-12T220030.vrb.rapid	19.1.2018 1:51	RAPID File	16 132 094 ...
Backup JobD2017-12-13T220023.vrb.rapid	19.1.2018 1:51	RAPID File	15 646 919 ...
Backup JobD2017-12-14T220025.vrb.rapid	19.1.2018 1:51	RAPID File	18 602 280 ...
Backup JobD2017-12-15T220034.vrb.rapid	19.1.2018 1:51	RAPID File	4 861 085 KB
Backup JobD2017-12-16T220027.vrb.rapid	16.1.2018 22:31	RAPID File	2 579 172 KB
Backup JobD2017-12-17T220036.vrb.rapid	19.1.2018 1:51	RAPID File	13 704 103 ...
Backup JobD2017-12-18T220013.vrb.rapid	19.1.2018 1:51	RAPID File	11 650 873 ...
Backup JobD2017-12-19T220023.vrb.rapid	19.1.2018 1:51	RAPID File	13 598 616 ...
Backup JobD2017-12-20T220020.vrb.rapid	19.1.2018 1:51	RAPID File	13 820 155 ...
Backup JobD2017-12-21T220029.vbk.rapid	19.1.2018 1:51	RAPID File	2 325 267 4...
How Recovery Files	16.1.2018 22:57	Text Document	1 KB

16 items

Scalable immutable filesystem



Append-Only



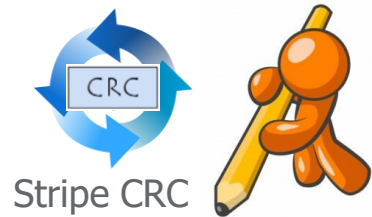
Full Stripe
Writes



Distributed
everything



How Rubrik leverages checksums



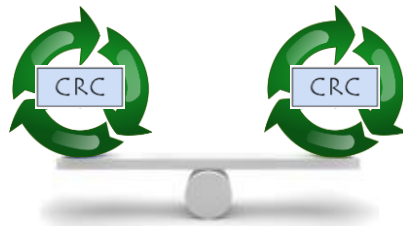
When data is written

it is validated against the checksum to ensure it was written without corruption.



When data is read

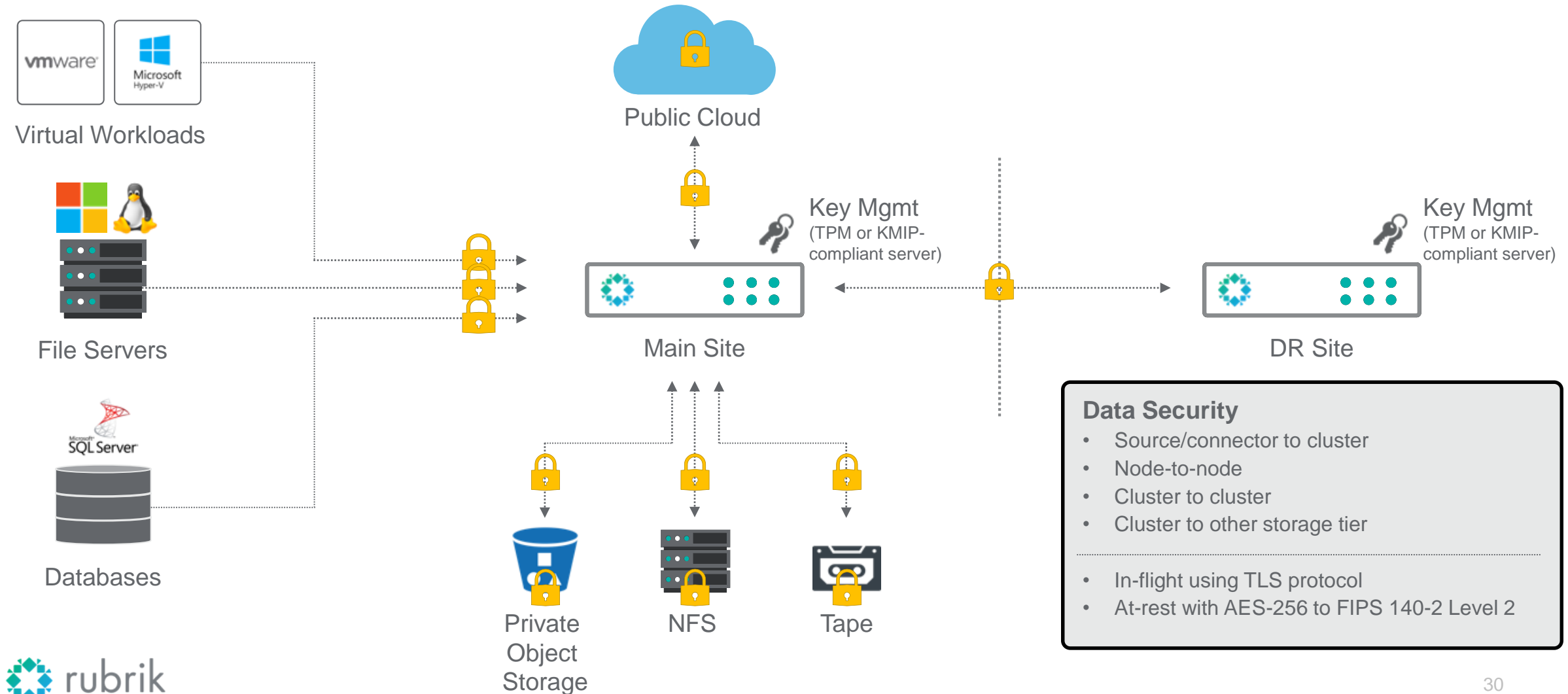
the checksum is validated as a check against corruption.



Background Scans

look for data corruption or inconsistency.

End-to-End Encryption



Review - Key Solution Components

What we've seen that makes a difference...

1. Reliability of Data Recovery

- a. Simplicity of Setup + Day to Day Operation
- b. Immutability of Snapshots
- c. Accelerated Detection

2. Speed of Data Recovery

- a. Speed of restore via Live Mount
- b. *Automation/API to enhance Restore Capabilities*

Rubrik Polaris

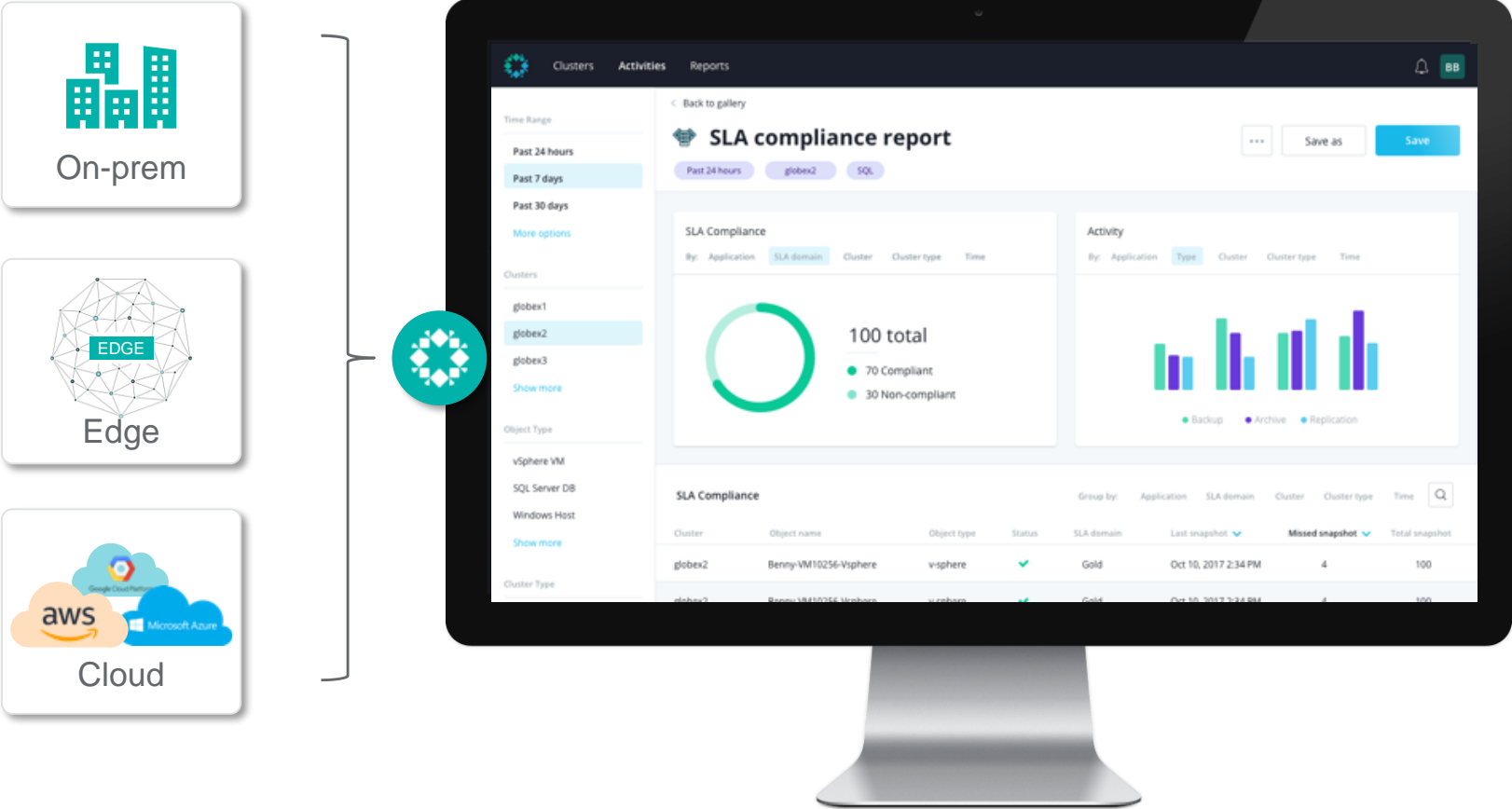
Platform & GPS

Introducing Polaris SaaS Platform



- The challenge: Cloud fragments everything
- A unified system of record brings all business apps and data together on a common platform
- Polaris offers a new class of data mgmt apps via open APIs
- Apps address data control, policy, information governance, security, data intelligence

GPS: Multi-Cloud Control and Policy Mgmt



AI Platform for Deep analysis

Structuring Unstructured Data



1

Detect Anomalous Events

Use query filters to detect Ransomware and trace origins and extent of attack

2

Meet Compliance

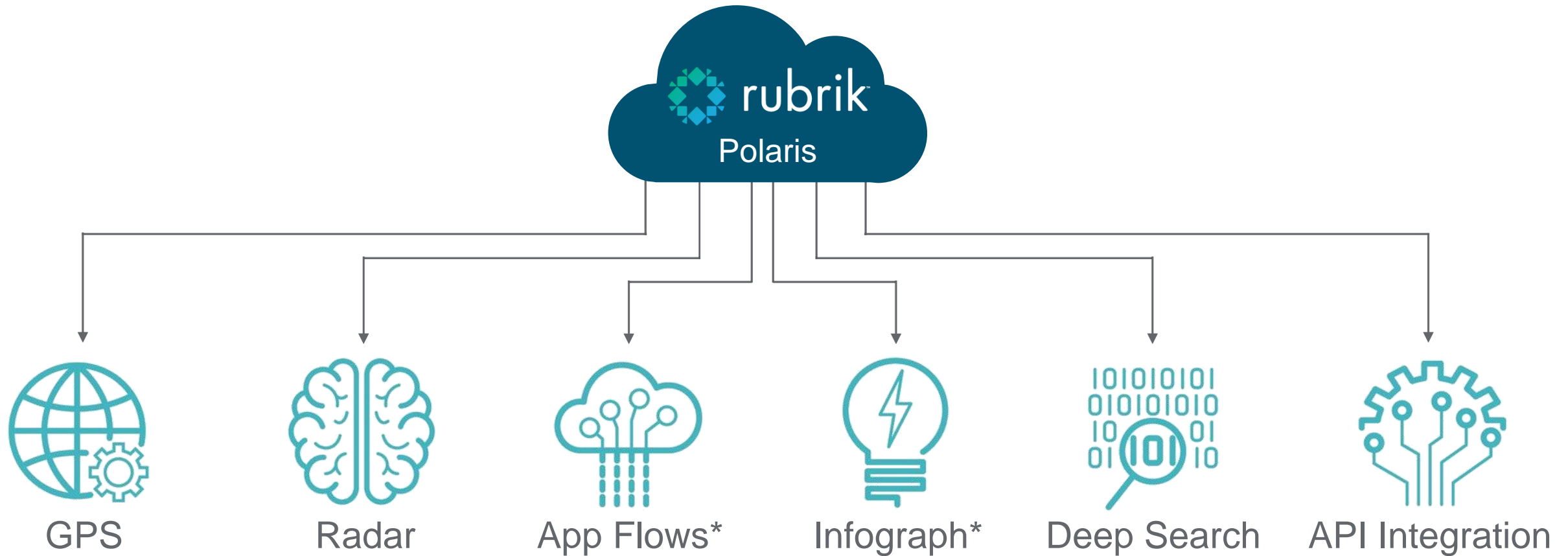
Find and remove personally identifiable information (PII) for GDPR, PCI, HIPPA

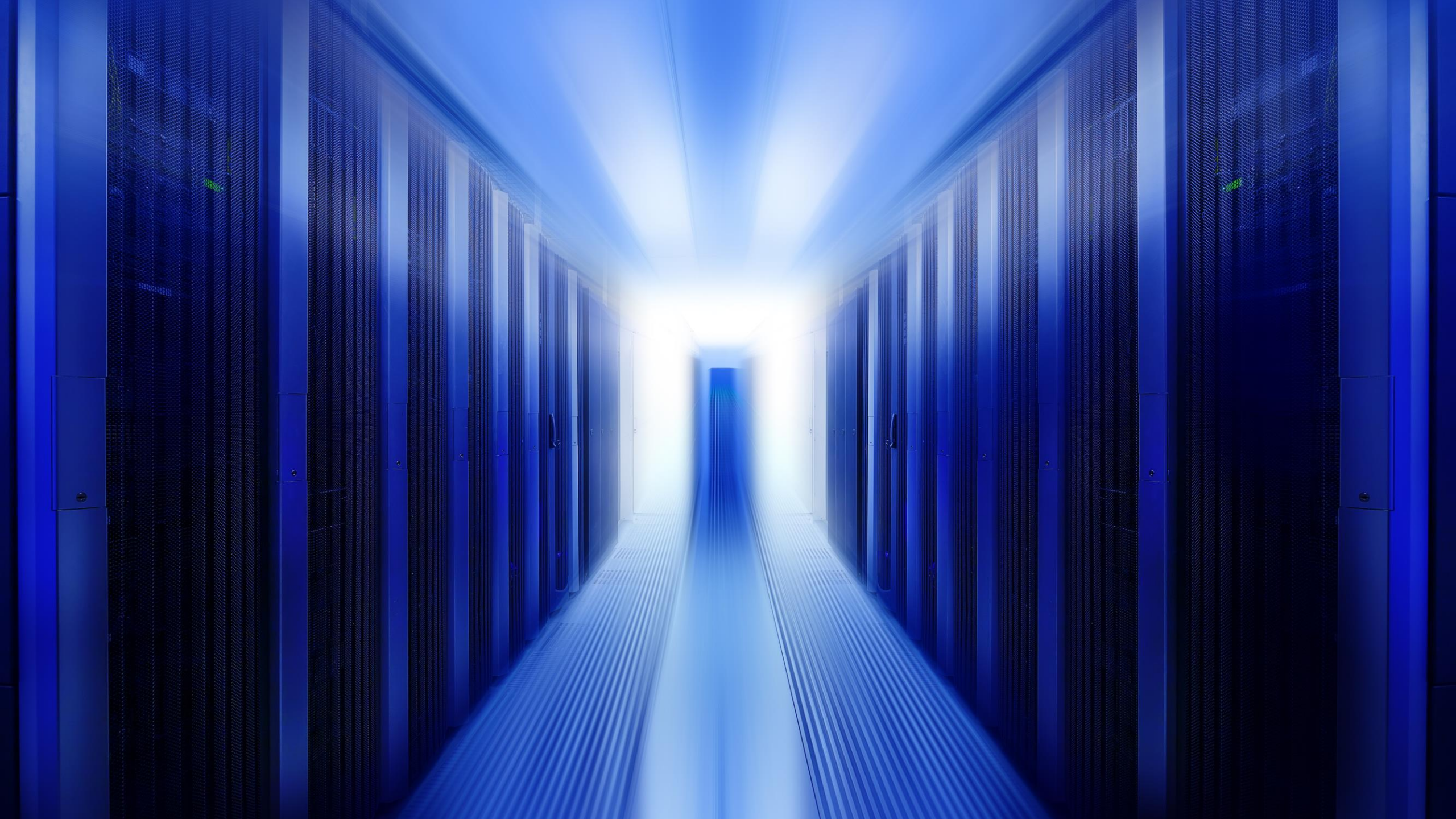
3

Perform Forensics

Use machine learning to categorize, secure, and enable eDiscovery of sensitive data

Act II: Rubrik Polaris





Back-to-back VMworld Best of Show Awards



Rubrik has been named Best of Show two years in a row.



Rubrik won Gold at VMworld three years in a row. In 2018, Polaris SaaS application, Radar, won Gold in Security.

YOUR COMPUTER AND FILES ARE ENCRYPTED

\$125 WITHIN 24 HOURS. \$199 AFTER 24 HOURS

OPERATING SYSTEM AND FILES DELETED AFTER 72 HOURS

-----WRITE THIS INFORMATION DOWN-----

The same information is on your desktop called

Payment_Instructions

Ransom Id:

BTC Address:

Email: towerweb@yandex.com

IF YOU LOOSE THIS INFO YOU WILL NOT BE ABLE TO CONTACT US

-----WRITE THIS INFORMATION DOWN-----

Your computer files have been crypted and moved to a hidden encrypted partition on your computer.

Without the decryption password you will not get them back.

No matter what you do the files will not re-appear and be decrypted until you pay.

Once payment is received you will get the decryption password and simple instructions to restore all your files and computer to normal instantly. Email us if you need assistance or have paid.

Email: towerweb@yandex.com

DO NOT LOOSE THE CONTACT INFO

Abfahrt Linie

Gleis

Nach

Olbernhau

Hbf

(S) Hbf

g-B. Süd

Hbf

Aue (Sachs)

Dresden Hbf

Zeit

Über

Flöha - Pockau-Lengefeld

Flöha - Freiberg

- Fährt heute

Hohenstein

Flöha - Zsch

Flöha - Zsch

Flöha - Zsch

Flöha - Zsch

Flöha - Zsch

Flöha - Zsch

Flöha - Zsch

Flöha - Zsch

Flöha - Zsch

22:10

RB81

22:30

RB30

22:31

RB30

22:36

RB80

22:36

RB45

22:44

RE6

22:45

RB89

23:30

RB30

8

11

10

8

9

5

14

11



23:32 12.05.2017

BMG | MIS

Under the Covers – How Radar works

Multi-level Defense

A Multi-Level Defense: How Radar Works



DETECT ANOMALIES

Leverage greater insights on suspicious activity to accelerate detection.



ANALYZE THREAT IMPACT

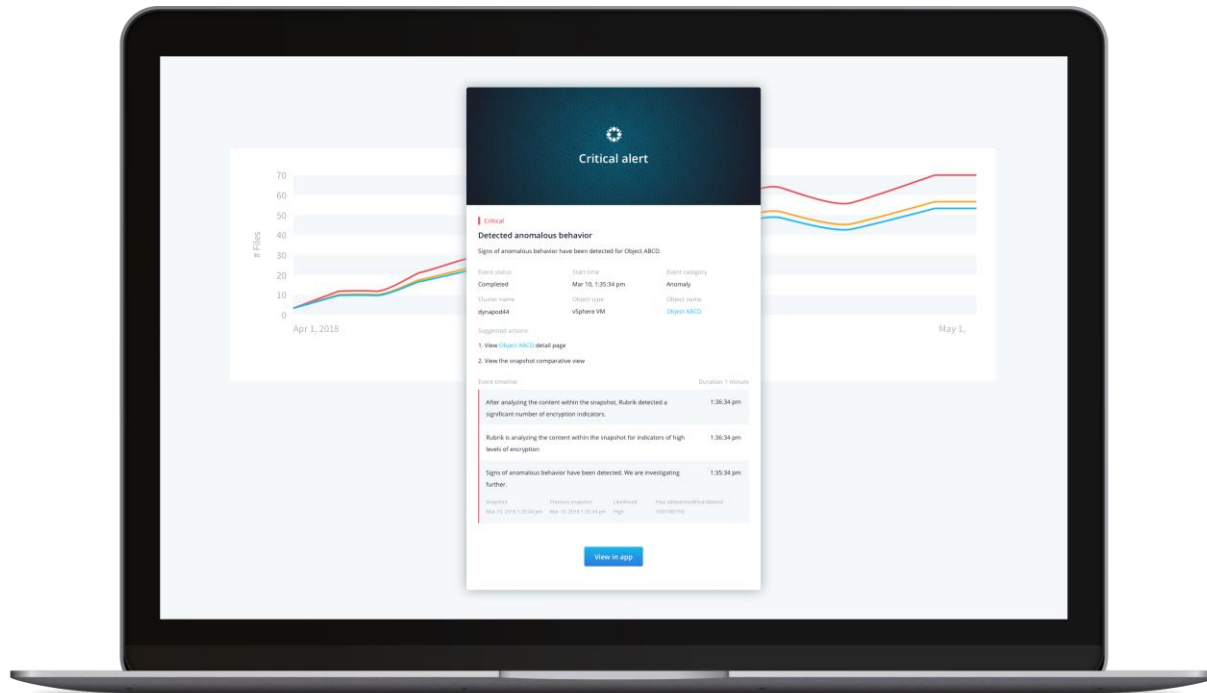
Prevent data loss with granular visibility into which applications and files were impacted.



ACCELERATE RECOVERY

Minimize downtime by replacing time-consuming processes with clicks.

Stay Ahead of Threats with Machine Learning

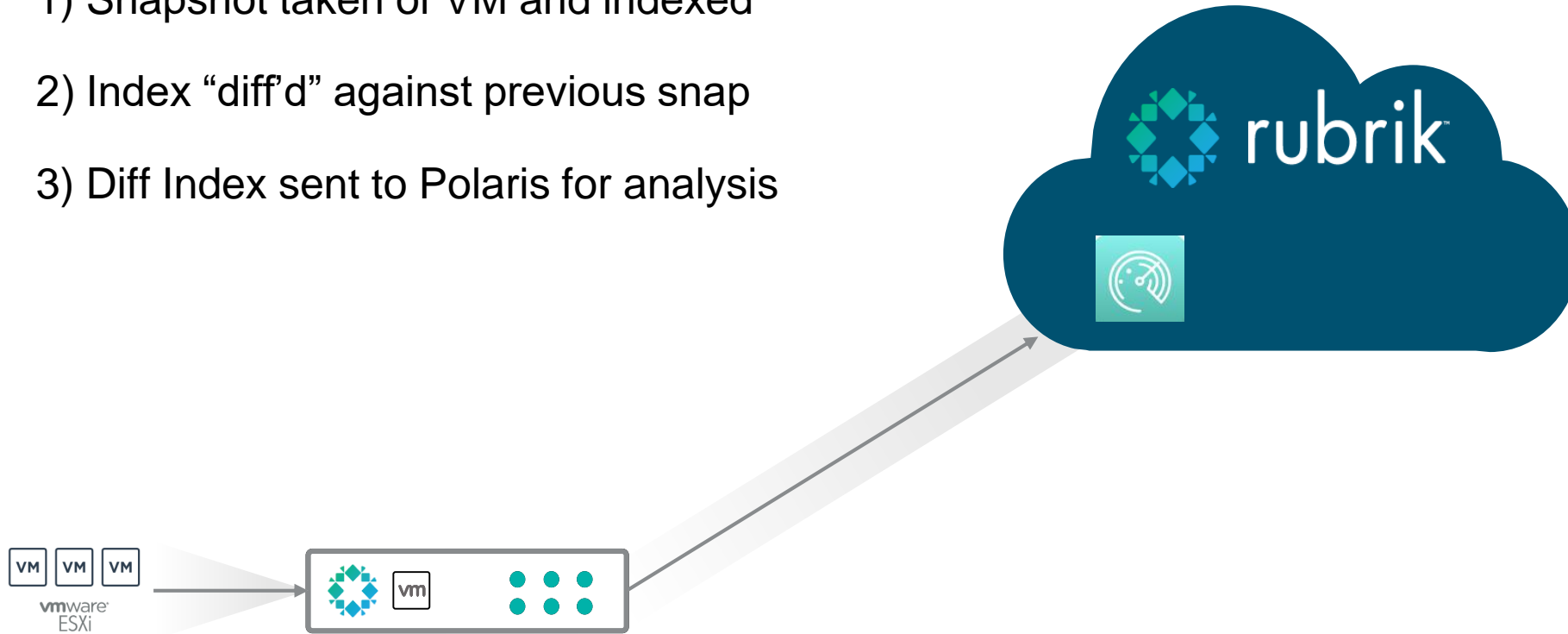


Detect Anomalies

We apply behavioral-based detection on application metadata to send alerts on unusual change activity. By using machine learning, we can detect new strains of ransomware.

The Architecture

- 1) Snapshot taken of VM and indexed
- 2) Index “diff’d” against previous snap
- 3) Diff Index sent to Polaris for analysis

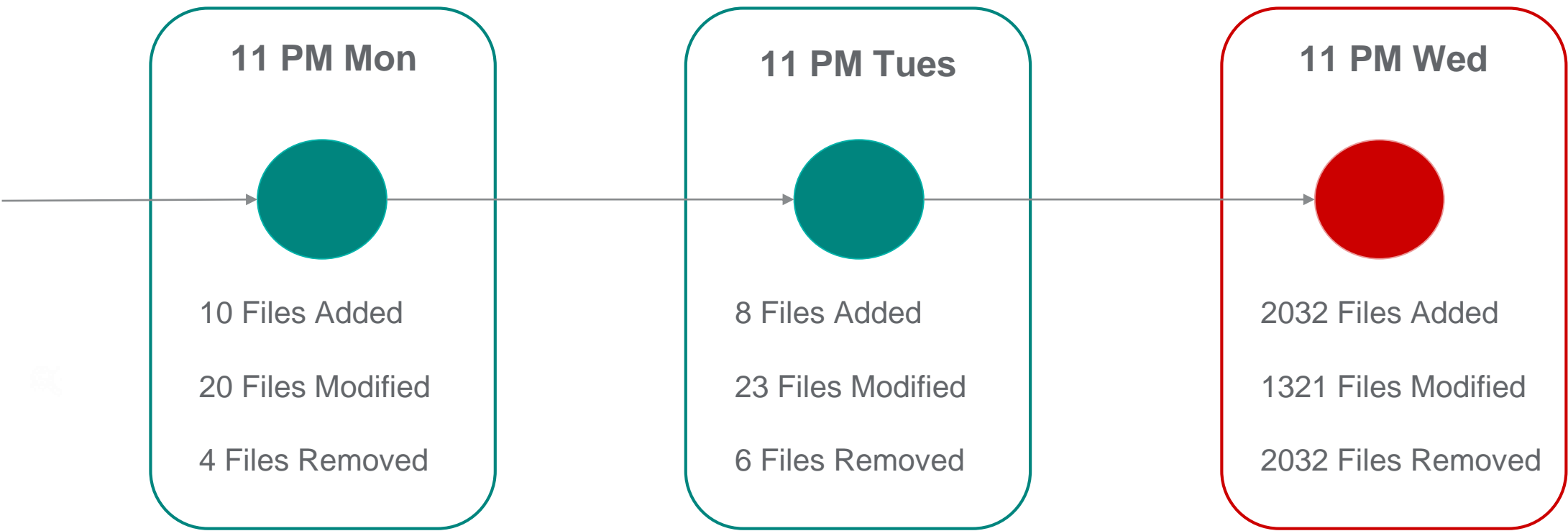


NOTE: Data never leaves the Brik, just metadata

Our Anomaly Detection Model

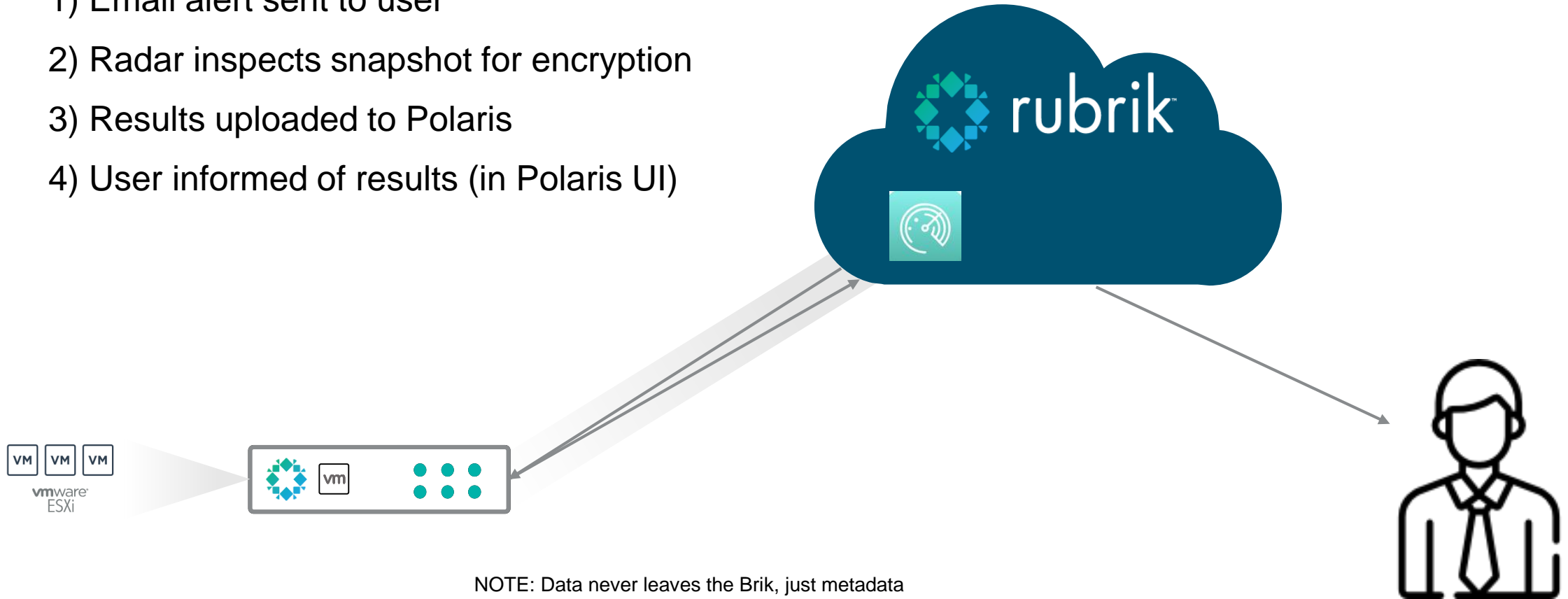
ML Model learns baseline behavior

Detect anomalies and alert as they come in

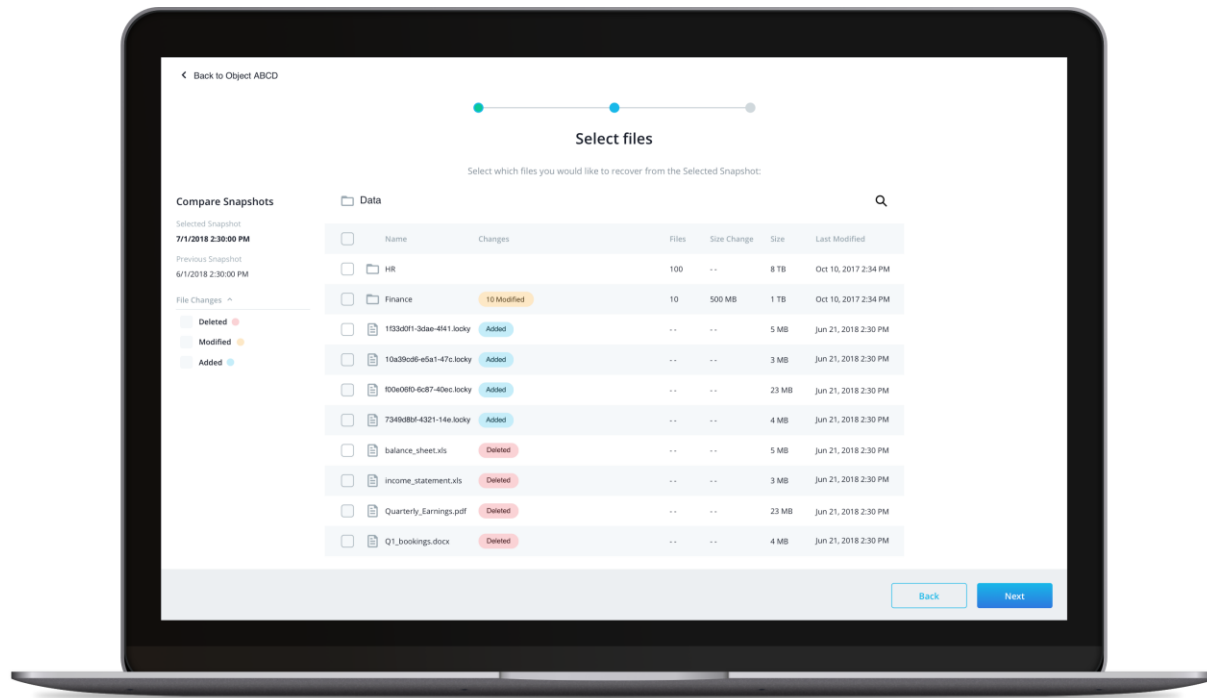


What happens post anomaly detection?

- 1) Email alert sent to user
- 2) Radar inspects snapshot for encryption
- 3) Results uploaded to Polaris
- 4) User informed of results (in Polaris UI)



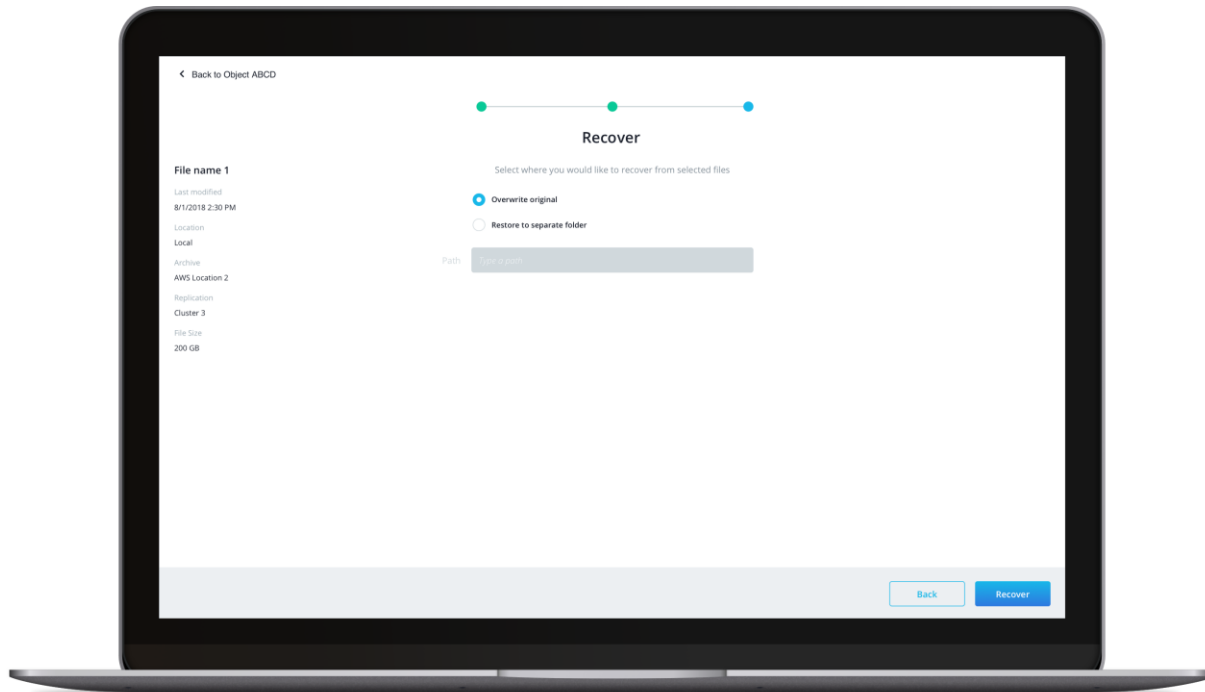
Prevent Data Loss with Intelligent Data Analysis



Analyze Threat Impact

Visualize how an attack impacted your entire system with a detailed view of file content changes at the time of the event. Drill-down to investigate what changed at the file-level.

Minimize Downtime with Fast Restores



Accelerate Recovery

Simply select all impacted resources, specify the desired location, and restore the most recent clean versions with just a few clicks. Rubrik automates the rest of the restore process.

Benefits

Features	Before Radar	After Radar
Immutable backups	✓	✓
Fast recovery	✓	✓
Machine learning-driven detection		✓
Data analysis on threat behavior and impact		✓
Granular recovery with just a few clicks		✓

Use Radar to Recover Quickly From Any Security Incident



Ransomware

Recover faster from cyber attacks with deeper insights on how malware impacted your entire environment.



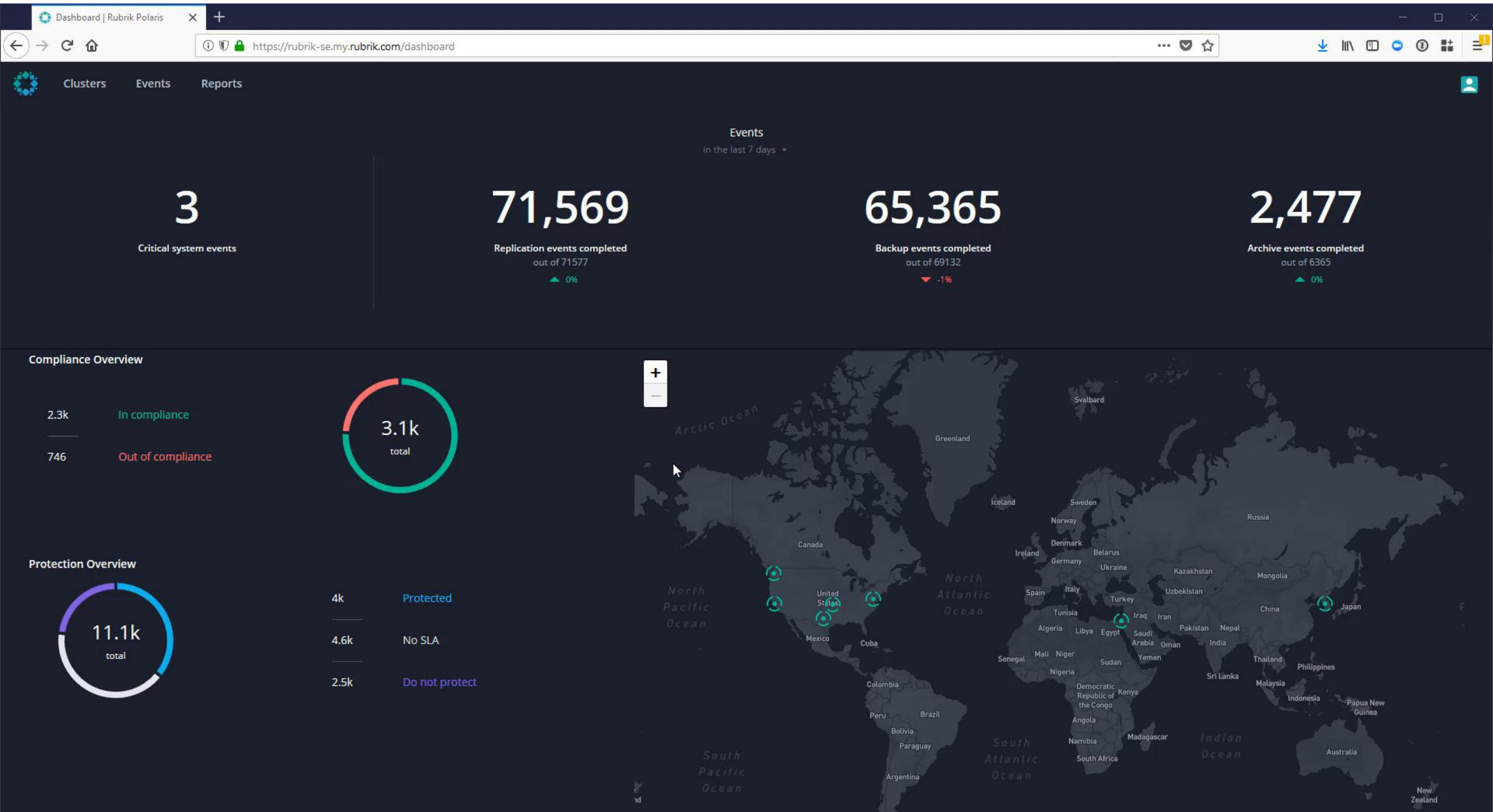
Insider Threat

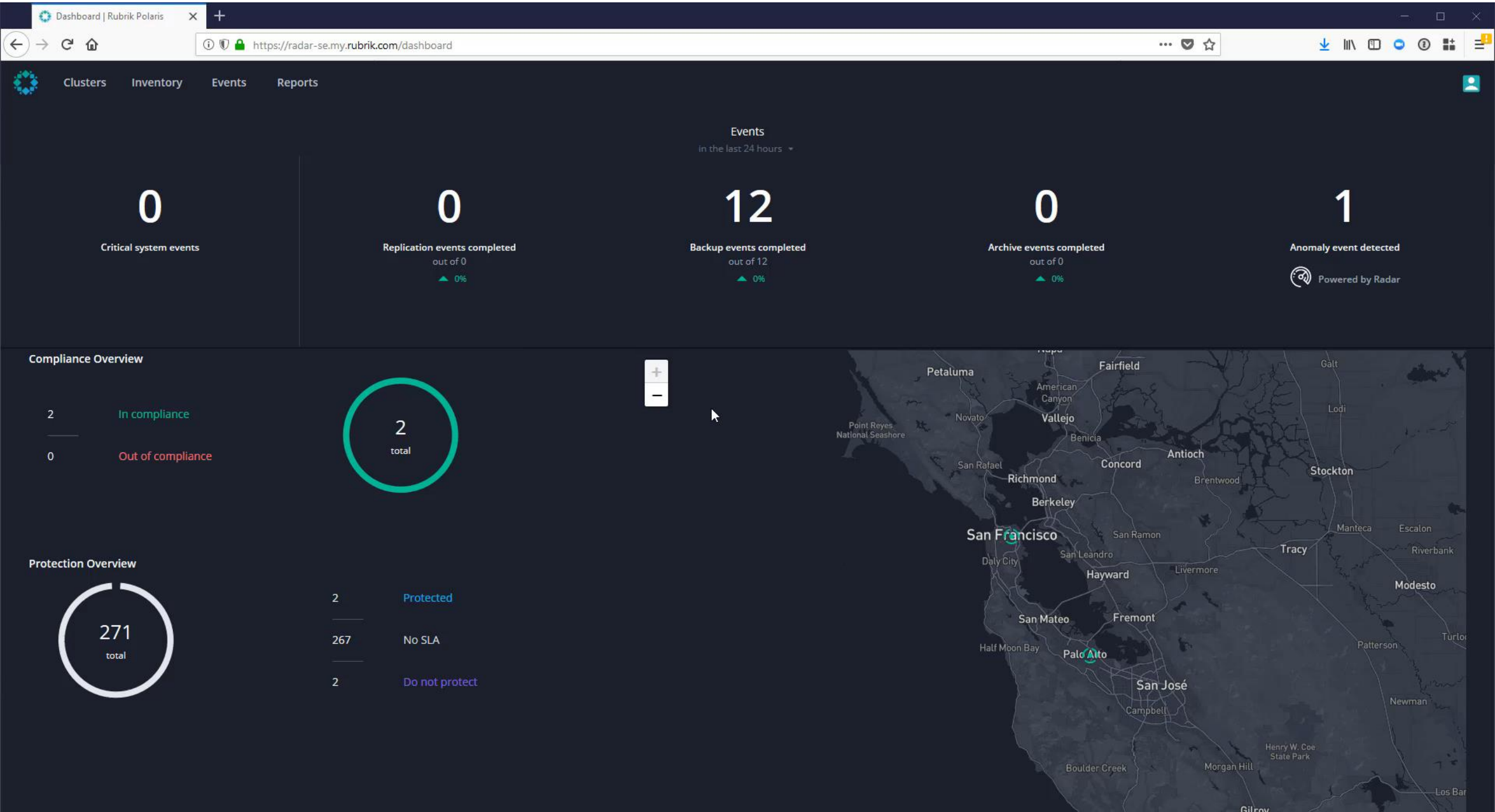
Identify and restore in the event employees, contractors, or business associates modify or delete sensitive information.



Event Monitoring

Monitor 24/7 for unexpected change rates. Get alerted to accidental user deletion or excessive file growth.





Questions?
Answers!



Don't Backup. Go Forward.

