Rubrik Zero Labs

The State of Data Security:

Cybersecurity threats don't care about your business continuity plans!

How To Boost Cyber Resilience Amid Increasing Threats

Mark Shaw
April 2024

NOTABLE REPORT ASPECTS

Rubrik Zero Labs

1st Rubrik Use of Rubrik telemetry in public report

1st use of trending data gained from external research

1st region-specific data availability

1st Rubrik intrusion case study - https://www.rubrik.com/zero-labs

Rare combination of internal data, external data, and other cybersecurity organization data

Provides objective views of data security in real environments, observed threat landscape, and actual impacts to organizations

METHODOLOGY

Rubrik Zero Labs

RUBRIK TELEMETRY

5000+
Customers

57
Countries

22
Industries

EXTERNAL RESEARCH

1600+
respondents

49%
CIO and CISOs

10
Countries in 3 Regions

Specific Data points from 4 other Cybersecurity Organizations

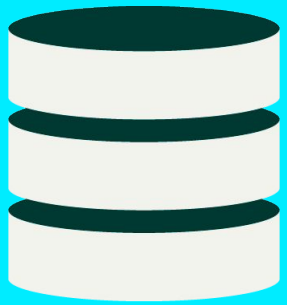
Data covers 01 January through 31 December 2022

RUBRIK TELEMETRY

Rubrik Zero Labs

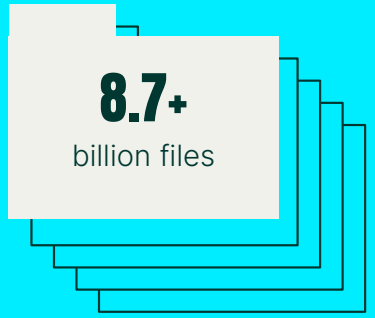
Total volume of data secured:

28
exabytes (EB) of logical storage



659
backend petabytes (BEPB)

Sensitive data:



8.7+
billion files

19+
billion sensitive data records within the files

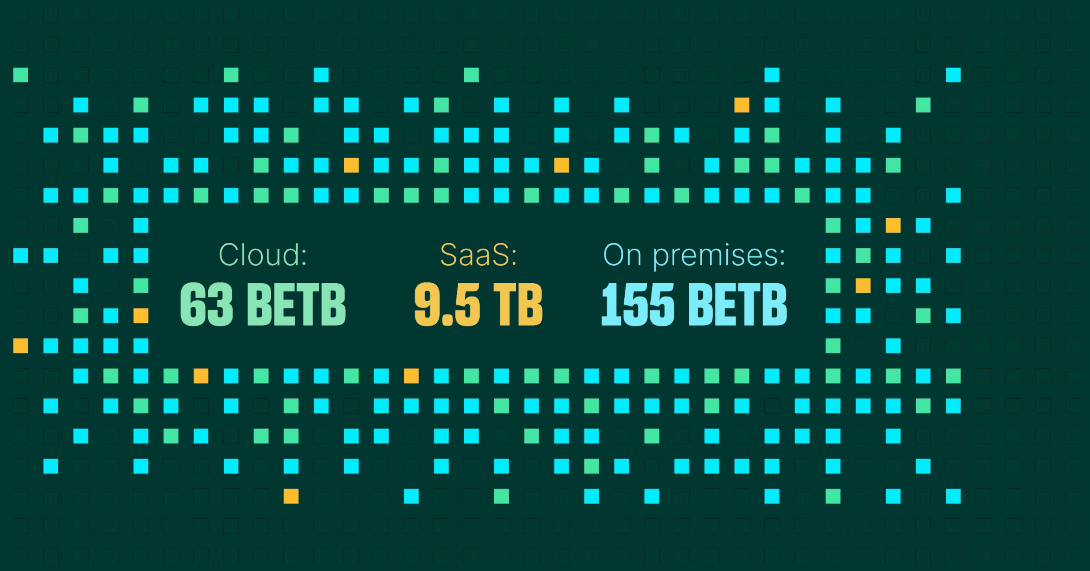
1 IN 38
files contains sensitive data

DATA SECURITY = HYBRID ENVIRONMENT(S)

Rubrik Zero Labs

Data secured in a typical environment:

TOTAL: 227 BETB



Data is moving across these environments:

45% of organizations secure data in a mix of on-prem, cloud, and SaaS

36% of organizations use multiple cloud vendors concurrently

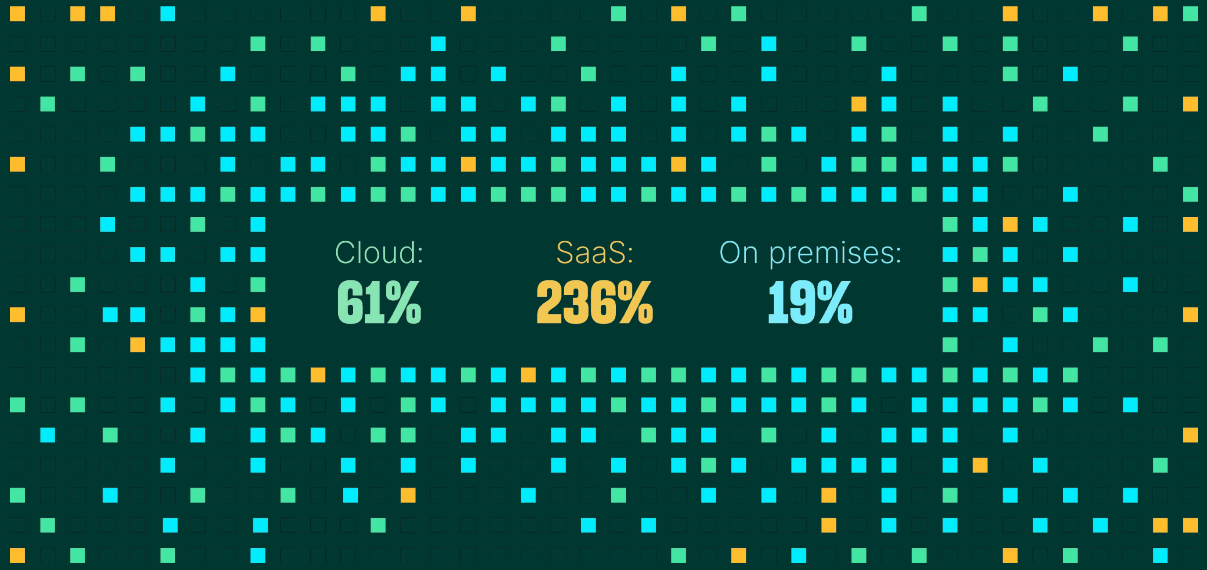
On-premises data is frequently stored in the cloud

DATA SECURITY = GROWING HYBRID ENVIRONMENT(S)

Rubrik Zero Labs

Data is growing at 25% YoY:

3X IN 5 YEARS = 545 BETB



Malicious Targeting in 2022:

61% of malicious attempts against external orgs involved SaaS

60% of malicious attempts against external orgs involved Cloud

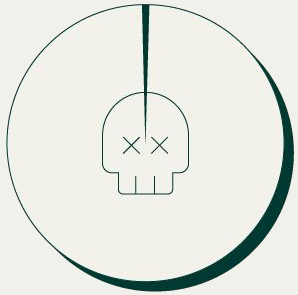
52% of malicious attempts against external orgs involved on-premises

THREATS ARE EXPANDING

Rubrik Zero Labs

99%

of IT and security leaders were made aware of at least one attack in 2022. On average, **leaders dealt with attacks 52 times in 2022.**



59% experienced a data breach

54% BEC or fraudulent transfer

40% encountered ransomware

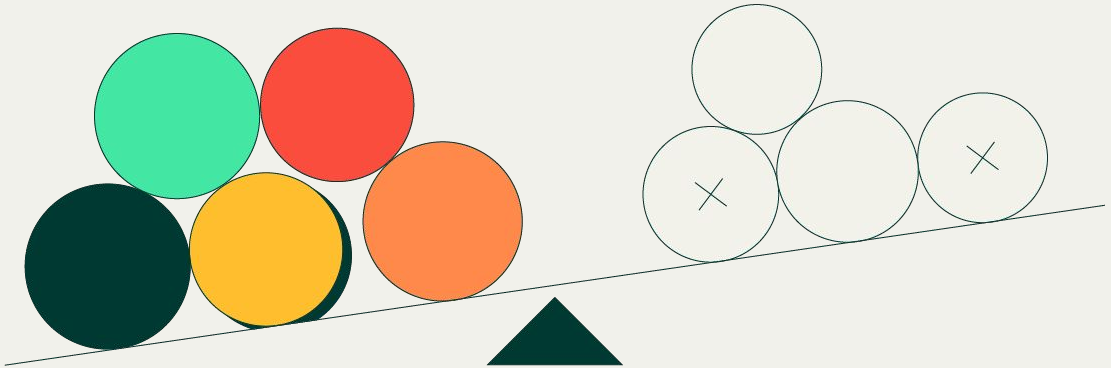
Expel reported a 70% increase in malicious events in the three major public clouds

from 2021 to 2022

100%

Permiso reported 100% of their cloud investigations were the result of a compromised credential

Everyone is **“doing”** data security, but reality is uneven



56% employ at least one zero trust initiative

56% developed or reviewed an incident response plan

54% tested backup and recovery options

52% created or refined data orchestration

50% conducted a senior leader tabletop exercise

PAYING A RANSOM ISN'T THE END EITHER

Rubrik Zero Labs

72%

of external organizations reported paying a ransom

ONLY 16%

of organizations recovered all of their encrypted data via attackers

39%

paid a ransom demand to prevent data leaks

40%

paid a ransom due to encryption events

46%

of organizations paying a ransom recovered half or less of their data via the attacker

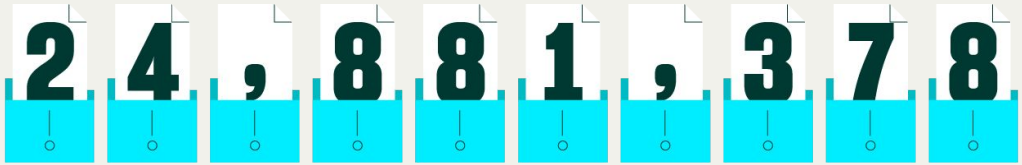
SHIFTING DATA PRESENTS REAL ORGANIZATIONAL RISK

Rubrik Zero Labs

A typical organization has:

files containing sensitive data

and



sensitive data records

1 of every 38 files contains sensitive data

Penalties for sensitive data exposure:

GDPR Up to 20 million Euros or 4% of global company revenue for severe violations, whichever is higher.

HIPAA $50 to $50,000 USD per violation, with a max penalty of $1.5 million USD.

CPRA Up to $2,500 USD per violation, or up to $7,500 for each intentional violation. No penalty cap.

INTRUSIONS AFFECT OUR BUSINESS

Rubrik Zero Labs

FCA
FINANCIAL CONDUCT AUTHORITY

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

DORA
Digital
Operational
Resilience
Act

UK organisations:
Strengthen your
cyber resilience

National Cyber
Security Centre
a part of GCHQ

Ransomware happens in the **MIDDLE** of the story not the beginning or end.

MVC (B)

Sec OPS <> IT OPS <> Legal <> Compliance <> Regulations <> Investor relations

Rubrik Zero Labs

The top 5 issues contributing to misalignment between IT and security were:

52%

Separate toolsets

Prevention focussed

51%

Visibility differences

50%

Conflicting priorities

Ownership

47%

Lack of formal planning or process

45%

DR ≠ Cyber Resilience

Don’t forget your backups, the bad guys remembered

93%

of organizations reported malicious actors attempting to impact data backups

AND 73%

of these efforts were at least partially successful

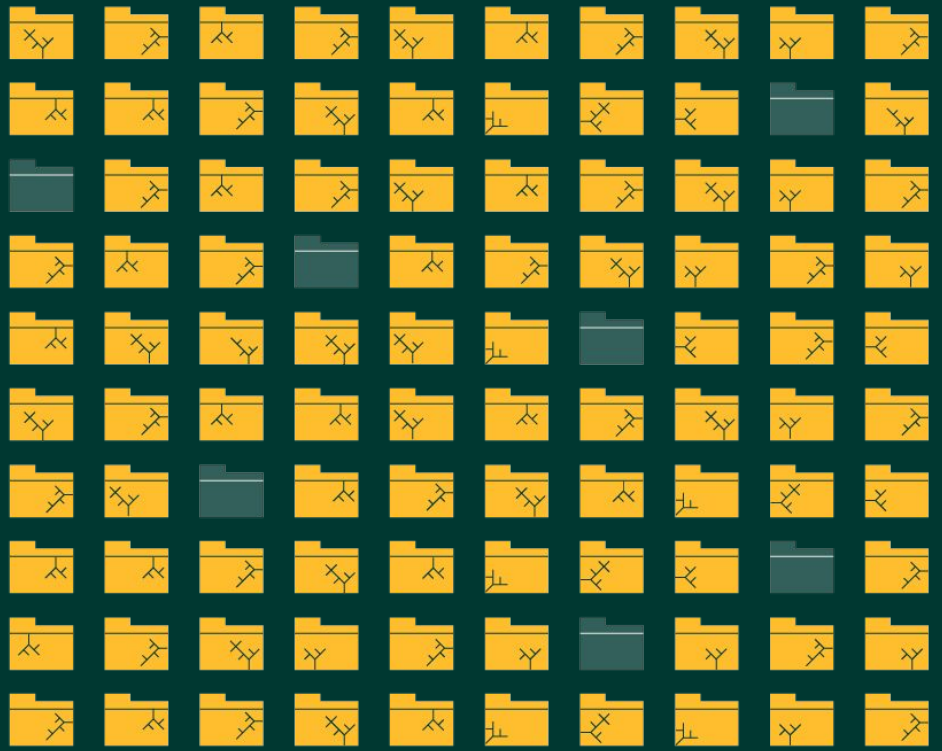
Don’t forget your backups...

99%

of organizations reported having a backup and recovery solution

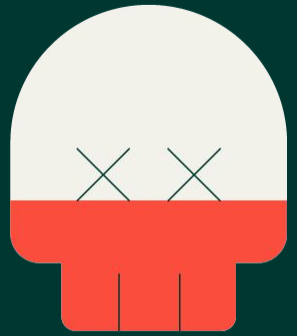
HOWEVER 93%

encountered significant issues with their solution



HOW PREVALENT IS RANSOMWARE?

Rubrik Zero Labs



40%

of external organizations reported a successful ransomware intrusion

75%

Rubrik identified anomalous activity at 75% of organizations

18%

of all Mandiant incident response engagements were ransomware

11%

of all Expel SOC analysis was tied to ransomware

48%

of these organizations observed some form of ransomware attempt

15%

of these organizations encountered some form of successful encryption event

RANSOMWARE HAPPENS IN THE MIDDLE ... NOT THE END

Rubrik Zero Labs

27,266,649

Analyzed Snapshots

20,692

contained anomalous activity – .07% of total

1,198

encountered an encryption event – .004% of total

100%

of encryption events previously identified as anomalous

100%

of encryption events tied to a lack of MFA

Largest single encryption event was 10+ million affected files

The median affected files for an organization with an encryption event was 48,521 files

73% of all observed encryption events affected virtualization infrastructure

PAYING A RANSOM ISN'T THE END EITHER

Rubrik Zero Labs

2022 ransoms observed by Palo Alto Networks' Unit 42 Incident Responses:

+$50M USD

as the highest ransomware demand

$7M USD

as the highest actual paid ransom

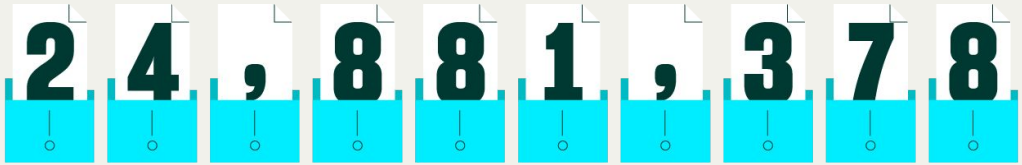
SHIFTING DATA PRESENTS REAL ORGANIZATIONAL RISK

Rubrik Zero Labs

A typical organization has:

files containing sensitive data

and



sensitive data records

1 of every 38 files contains sensitive data globally

Applied penalties to a typical environment:

GDPR Less than one Euro per record or less than four Euro per file = 20 million Euro maximum

HIPAA $1.5 million max at $ 50 minimum = 30,000 items

CPRA $2,500 per file = $1.4 billion

INTRUSIONS AFFECT OUR BUSINESS

Rubrik Zero Labs

93%

of external organizations encountering a cyberattack experienced a negative impact

49% Loss of customers

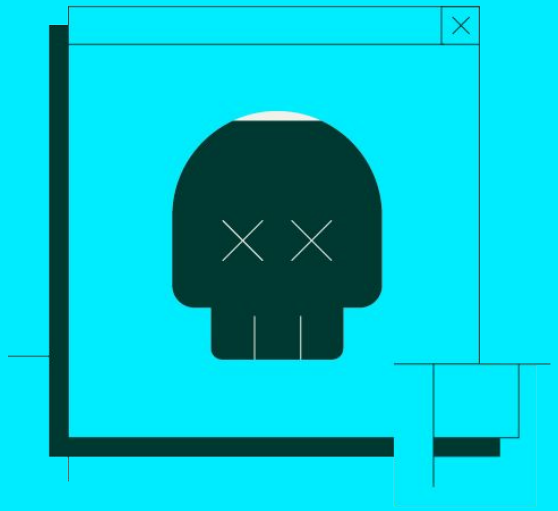
45% Revenue loss

44% Negative press and/or reputational damage

5% Stock negatively impacted

INTRUSIONS CAN DRIVE IMPROVEMENT OPPORTUNITIES

Rubrik Zero Labs



99%

of organizations increased their capability following a cyberattack

48% of organizations changed vendors or third party relationships

54% increased spending on new tech or services

43% hired additional staff

Intrusions will drive changes to the status quo–it is up to individual organizations if these changes are positive or negative

DATA SECURITY IMPROVING ACROSS THE BOARD

Rubrik Zero Labs

51.2
Jan 2022 average

59.5
Dec 2022 average

16%
16% Increase globally

100%
Improvements in all regions and industries

48%
of Rubrik customers enduring some form of ransomware activity

.004%
Encountered an encryption event

97%
Expel reported 97% of ransomware attempts stopped before ransomware deployment

Operational Recovery Timeline – As is - Key apps!

Ransomware Detonation
Ransomware attack initiated, encrypting systems and data

Locate and available Clean Recovery Point
Restore workloads into isolated environment and scan with 3rd party tools to determine if recovery point is safe to use

Recovery or Rebuild
If no clean recovery can be obtained (13 months retention) rebuild process necessary

Detect – 24 hours

Remediate – 2 Weeks or Never

Recover – 1 to 2 weeks

Rebuild – 2 - 3 weeks

Operational

Repeat for each workload and recovery point

Damage Assessment
Assess the blast radius of an attack across entire Infrastructure. Coordinate response efforts with organizational leadership

Objective: establish what workloads and data require restoring. Communicate estimated timelines to operational leadership.

rubrik

© 2022 Rubrik. All rights reserved.

Rubrik Operations - Recovery Timeline

Ransomware Detonation

Ransomware attack initiated, encrypting systems and data

Locate an available and Clean Recovery Point

Available copy utilising ***Data Resilience*** and Identify and Isolate IOCs with ***Threat Hunting*** and prevent from reinfection using **Threat Containment.** Ensure environment is clean prior to recovery with **Threat Hunting.**

Understand what sensitive data is compromised using ***Sensitive Data Discovery***

Objective: Establish latest clean recovery points and clean environment to recover

Pre/During/Post Event Investigation

Identify IOCs with **Threat Hunting.**
Understand, locate and classify data across the estate with **Sensitive Data Discovery** prevent reinfection with **Threat Containment**

Objective: Identify root cause and understand scope of data exposure. Proactively limit exposure.

Detect – mins/hours | Remediate – mins/hours | Recover – mins/hours | Operational | Investigate / RCA

Damage Assessment

Assess the blast radius of an attack using ***Ransomware Investigation***, and coordinate response efforts with University leadership

Objective: establish what workloads and data require restoring. Communicate estimated timelines to operational leadership.

Recover

Selectively recover - files affected, key data and LATEST required files only (Reduce TB to be recovered and reduced rebuild/Redo time) with ***Ransomware Investigation*** and ***Sensitive Data Discovery*** and ***Threat Hunting***

Time to ensure restored services are operational, accelerated by **Orchestrated Application Recovery and Fast Recovery**

Objective: stage recovery using blueprints in order of dependencies and restore/boot order, per University application

Tier 0 Apps Online

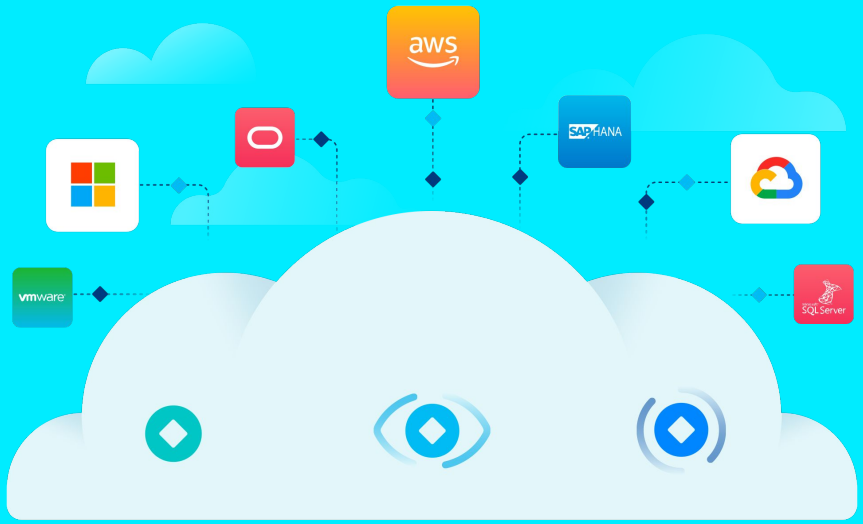
Resumption of services in minutes and hours, opposed to days and weeks

rubrik

© 2022 Rubrik. All rights reserved.

Introducing **RUBRIK**

We are on a mission to secure your data wherever it lives: across enterprise, cloud, and SaaS – making your business unstoppable.



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

Data Observability
Continuously monitor and remediate data risks, including ransomware, sensitive data exposure, and indicators of compromise.

Data Recovery
Surgically and rapidly recover your apps, files, or users while avoiding malware reinfection.

QUESTIONS?