Rubrik Zero Labs

The State of Data Security:

THE HARD TRUTHS

Contents

Data sources

(RT) **RUBRIK TELEMETRY** (WR) **WAKEFIELD RESEARCH** (ER) **EVENT RESPONSE DATA**

ABOUT THE DATA

Rubrik Zero Labs strives to deliver actionable, vendor-agnostic insights to help reduce data security risks. We incorporated findings from different sources, all covering 01 January through 31 December 2022.

RUBRIK TELEMETRY:

We use Rubrik telemetry to stay close to the ground truth of everyday organizations while also providing context about our bias.

5000+
customers

3
regions

22
industries

57
countries

Total volume of data secured:

28
exabytes (EB)
of logical storage

659
backend
petabytes (BEPB)

Sensitive data located in:

8.7+ billion
files

1 of every 38
files contains
sensitive data

19+ billion
sensitive data
records within the files

A Sense of Scale:

Some estimates say every word ever spoken across all of history in every language equates to 5 EB... or just 18% of the data secured by Rubrik in 2022.[1,2,3,4]

28 EB vs 659 BEPB

AKA Hey Nerds!!!:
When most of the world hears "data," they imagine logical storage, also known as frontend storage. Those of us in the data business focus on backend storage.

Rubrik takes the entirety of an organization's data and performs different functions—including deduplication and compression—to reduce the amount of data placed in backend storage. That's why we'll focus on backend storage throughout the rest of this report.

Case Study:
We also took a closer look at an attack against one of the organizations included in the Rubrik telemetry. The organization's name has been changed to protect its privacy.

1 https://www.space.com/18383-how-far-away-is-jupiter.html
2 https://www.sizes.com/tools/filing_cabinets.htm
3 https://www.zmescience.com/science/how-big-data-can-get/
4 https://www.backblaze.com/blog/what-is-an-exabyte/

WAKEFIELD RESEARCH:

We commissioned a survey conducted by Wakefield Research to round out our Rubrik telemetry with a broader view of the data security landscape.

We chose to engage IT and security leaders to study the difference in their perspectives.

1600+
IT and security leaders

49%
CIOs
and CISOs

3 Regions
United States, EMEA and APAC

16%
VPs

38%
Senior Directors or Directors

10 Countries
United States, United Kingdom, France, Germany, Italy, Netherlands, Japan, Australia, Singapore, India

EVENT RESPONSE DATA:

We engaged respected cybersecurity organizations for a more holistic view of the data security landscape and appreciate the use of their findings.

Mandiant:
Global median dwell times and ransomware investigation ratios from M-Trends 2023

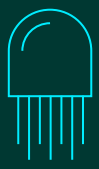
Palo Alto Networks Unit 42:
2022 Ransom demands from 2023 Unit 42 Ransomware and Extortion Report

Expel:
Ransomware precursor activity and growth of intrusions in public clouds from Great Expeltations 2022

Permiso:
Illicit credential use in cloud intrusions and credential privilege levels from Permiso 2022 - End of Year Observations

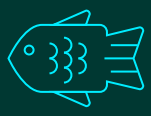
THE DATA SEASCAPE

Organizations are sitting on an ocean of data.
On the surface that ocean looks vast, yet stable.



But anyone dropped into its depths knows that it's teeming with life.

Vision is limited, but the more you look, the more data you'll find—in caves, under rocks, nearly everywhere. The currents are swift. It's never the same scene twice.



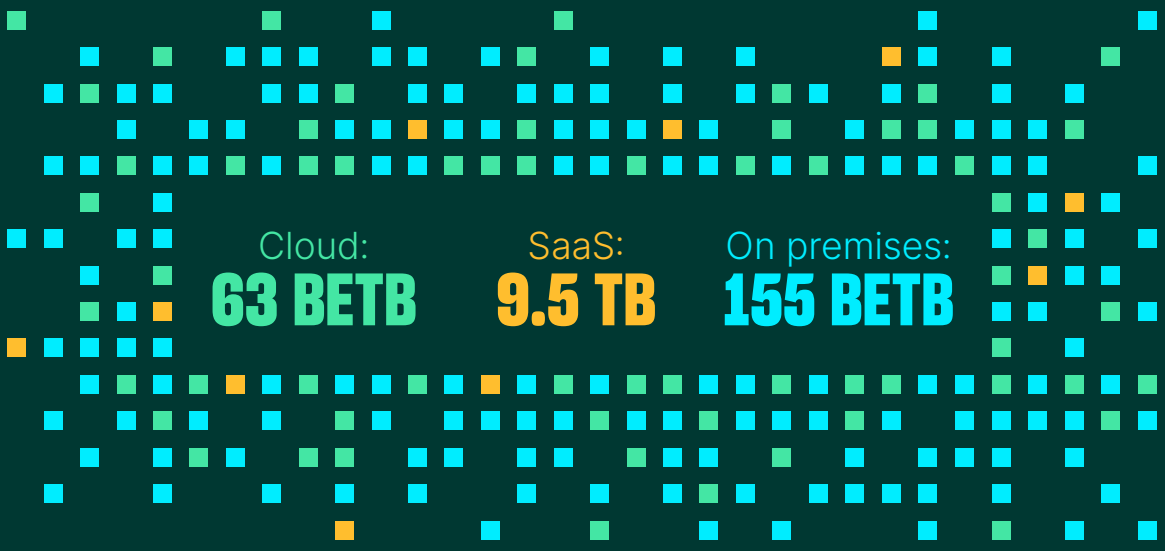
And all the while you're wondering,

ARE PREDATORS SITTING IN THE DARKNESS WAITING TO ATTACK?

Data is growing faster and in more places than we think ®

Data secured in a typical environment:

TOTAL: 227 BETB



Average growth of secured data during 2022:

Total:	Cloud:	SaaS:	On premises:
25%	**61%**	**236%**	**19%**

A typical organization's data volume will triple in the next five years and require

545 BETB

to secure if growth rates hold steady.

45%

of global organizations secure data in a mix of on-premises, cloud, and SaaS.

36%

of global organizations use multiple cloud vendors concurrently.

For each data security solution, there's a follow-on challenge ®

The last line of defense during a crisis is the data backup and recovery systems with it's associated processes. But organizations are finding simply having a backup solution isn't enough.

99%

of external organizations reported having a backup and recovery solution.

However, 93%

encountered significant issues with their solution. The most common issues are staff shortages, bandwidth limitations, infrastructure gaps, and lack of pre-coordinated plans or priorities.

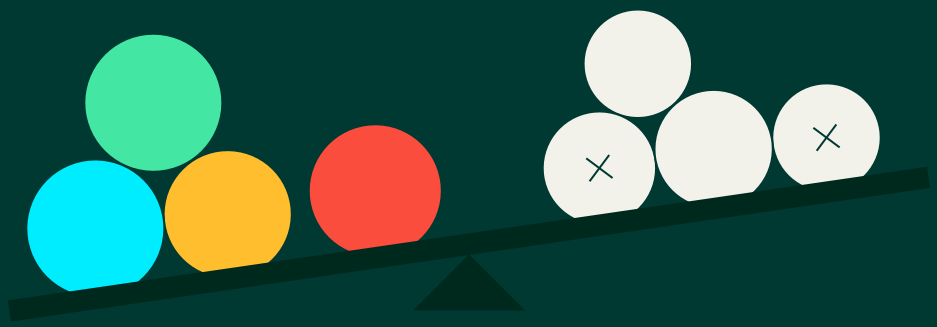
93%

of external organizations reported malicious actors attempting to impact data backups during a cyberattack

73%

said the attempts were at least partially successful.

Everyone is **"doing"** data security, but the reality in 2022 is uneven ®



56%

of organizations employed 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 recovery orchestration.

The Case Study

2024

In 2022, a US-based educational organization experienced the harsh realities of data security first hand. Through their story, we'll explore just how common their experience is.

The facts in this case study are true, but the actual name of the organization is anonymized to protect client privacy.

The Stone University Environment:

2.9 PB
logical storage

64 BETB
physically stored

Data in two
distinct environments

155%
data growth across 2022

WHAT YOU DON'T KNOW

WILL HURT YOU

Attackers compromised Stone University using a Log4j vulnerability that left the institution's help desk ticketing system server susceptible to exploitation.

Log4j

In late 2021, a vulnerability in one of the most deployed pieces of open-source software, Apache's Log4j software library, sent the technology industry into overdrive. Cybercriminals were exploiting this vulnerability, now labeled Log4Shell, within 12 hours and continue to exploit it to this day[5].

5 The Guardian: Recently uncovered software flaw 'most critical vulnerability of the last decade'

By accessing this server, the attackers successfully evaded the boundary infrastructure security measures.

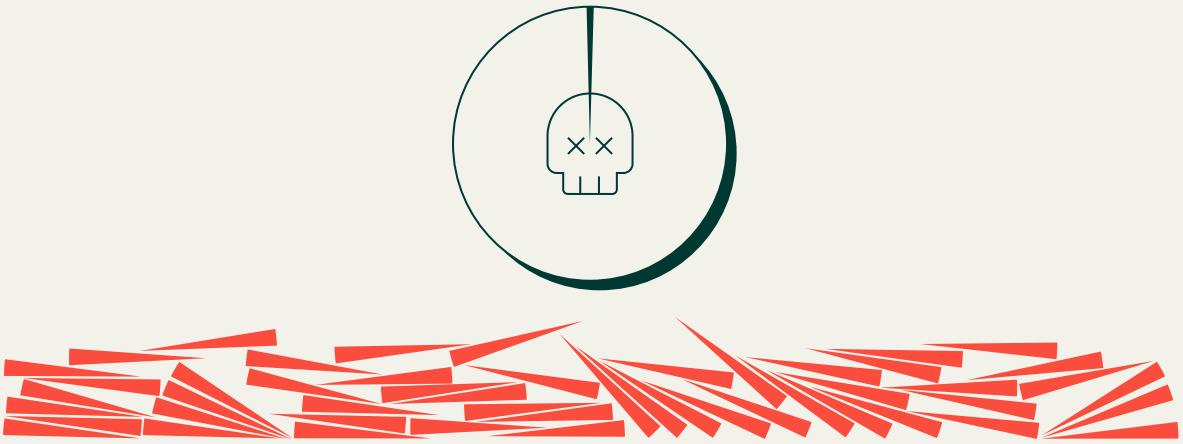
Attackers used a mix of legitimate tools to create illicit credentials, expand their access, create additional footholds across the environment, and compromise Active Directory.

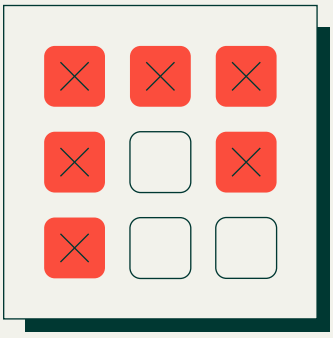
The cybercriminals moved laterally across Stone University gaining access to five distinct machines in their VMware environment and picking up key details along the way—all without Stone University knowing.

Stone University's experience, while alarming, is surprisingly common compared to what many organizations faced last year. [WR]

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.**





61%

of these attacks affected SaaS applications, the most targeted environment.

DATA DEEPDIVE:

All environment types were affected by malicious activity with ratios of:

61% SaaS

62% Cloud

50% On-Premises

According to Expel, malicious incidents in the three major public clouds increased by 70% from 2021 to 2022.

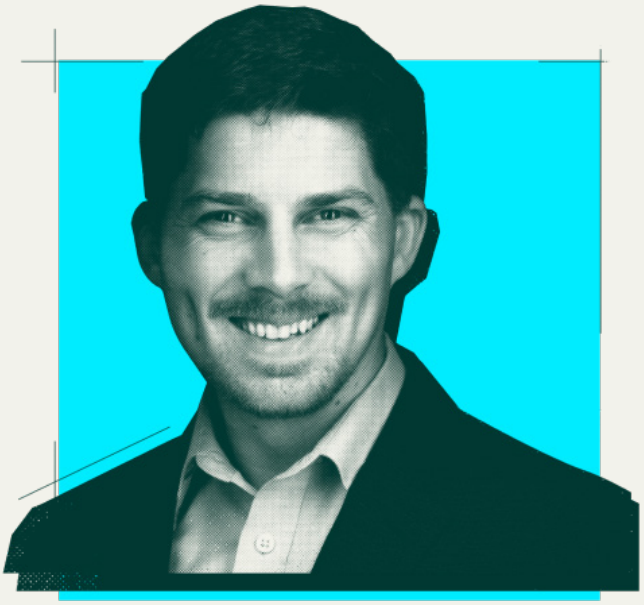
Note: The three public clouds referenced are Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure (Azure).[6]

Once the cybercriminals gained access to Stone University's environment via the vulnerability, they quickly pivoted to malicious credential use. Permiso reported that 100% of the cloud intrusions they detected and responded to were the result of a compromised credential.[7]

Additionally, these credentials were more than 90% overprivileged, or, put another way, the credentials only used 5-10% of the amount of assigned privileges.[8]

"Most companies have little to no visibility into how their identities are used... they aren't monitored or audited...and aren't easily identified when compromised. With the growth of API-driven ecosystems ... these are being leaked and sprayed at a staggering rate, drastically increasing the number of compromised keys, tokens, and certificates."

Ian Ahl, VP and Head of P0 Labs, Permiso



6 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
7 https://permiso.io/blog/s/permiso-2022-end-of-year-observations
8 https://permiso.io/blog/s/permiso-2022-end-of-year-observations

DAY 4:
RANSOMWARE PREPARATION

KNOCK KNOCK

Organizations often don't know they're under attack until the attackers tell them.

Still undetected, Stone University's attackers **prepared to make their presence known.**

They ensured they had multiple access points to Stone U's systems, so...

They also established access on a legacy data backup server to **observe Stone U's response.**

In a twist of fate, Stone University had previously replaced the backup vendor and technology, but left this server in place despite no longer needing it.

Finally,
the cybercriminals exfiltrated eight gigabytes (GB) of data from across Stone University.

The cybercriminals

REMAINED UNDETECTED

throughout this process.

How common are ransomware events? ®

40%

40% of external organizations surveyed reported a successful ransomware event.

11%

Expel reported 11% of all malicious events encountered by their SOC were tied to ransomware activity.[9]

18%

Mandiant reported 18% of their engagements were ransomware events.[10]

DATA DEEPDIVE:

How common are cyberattacks?
Types of attacks external organizations faced in 2022:

- 59% data breach
- 54% business email compromise or fraudulent transfer
- 41% insider event
- 40% ransomware

Stone University's attackers' actions are consistent with Mandiant's attacker median global dwell times:

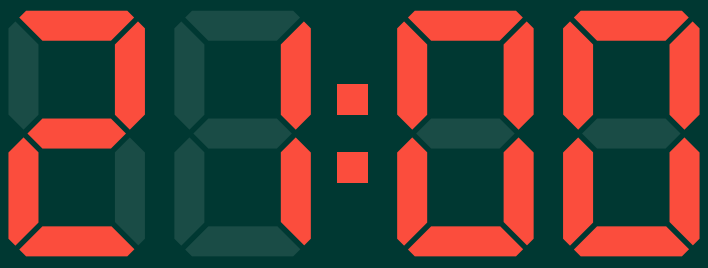
- Median global dwell time
- 16 days - All investigations (espionage, financial gain, unknown outcome, etc.)
- 9 days - Ransomware investigations only (18% of total Mandiant investigations)
- Ransomware investigation dwell times are typically shorter because the attacker "self-reports" by sending the ransom note or encrypting an environment.[11]

9 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
10 https://www.mandiant.com/m-trends
11 https://www.mandiant.com/m-trends

DAY 5:
RANSOMWARE DEPLOYMENT

OH SH*T

Stone University's attackers began the ransom phases of their intrusion at approximately 9 pm on Sunday evening.



They used AvosLocker to encrypt files within the VMware ESXi infrastructure across 150 VMs, including the initial five VMs from the intrusion.

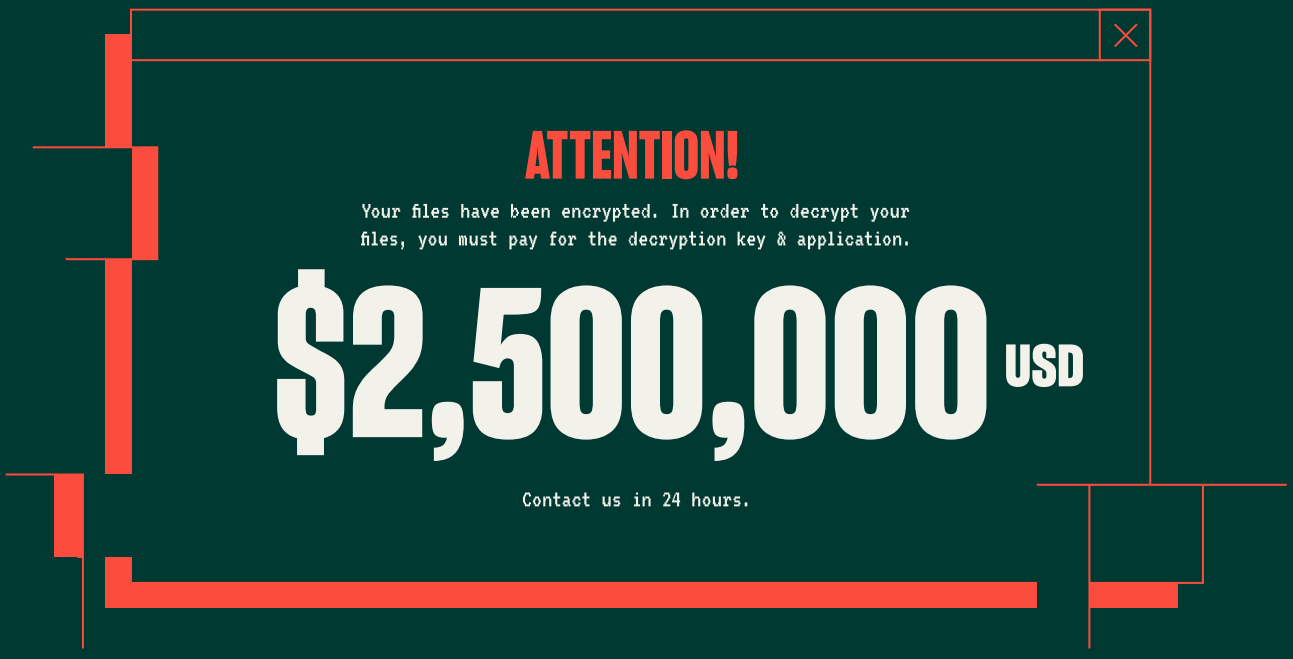
AvosLocker also shut down the virtual machine management tools shortly before encrypting files to prevent Stone University from responding in an effective manner.

AvosLocker

AvosLocker is used to describe both a malware family and a threat group. It operates under a "Ransomware as a Service" model, where affiliates subscribe to a service to execute ransomware deployments and collect ransoms. In the case of AvosLocker, the subscription covers direct handling of ransom negotiations, publishing exfiltrated victim data, and the actual use of a specific ransomware tool.[12]

12 https://www.cisa.gov/news-events/alerts/2022/03/22/fbi-and-fincen-release-advisory-avoslocker-ransomware

Finally, the attackers posted ransom notes demanding...



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

Many people believe the encryption event is the end of the ransomware story, but that's almost never the case. For instance, cybercriminals possessed unfettered access in the university systems for days, undetected. And it will take several more days until this ransomware story is fully resolved.

DATA DEEPDIVE:

Ransomware is a type of data denial threat.

Data denial can involve ransomware, wipers, data deletion using valid access, and denial of service efforts. Additionally, cybercriminals routinely exfiltrate data for a range of goals before encryption events.

In 2022, Rubrik's Ransomware Response Team assisted dozens of organizations with recovery operations.

The most prevalent ransomware families in these responses were:

- LOCKBIT2.0
- BLACKCAT/ALPHV
- AVOSLOCKER
- META
- PLAY
- HIVE
- SPARTA
- BLACK BASTA
- SPIDER
- VICE Society

TAKE BACK CONTROL

Beating the attackers depends on your readiness to respond

Stone University quickly started working the event, but were limited by widespread encryption.

To overcome this, they restored data to forensic and test environments to investigate and prioritize their next actions.

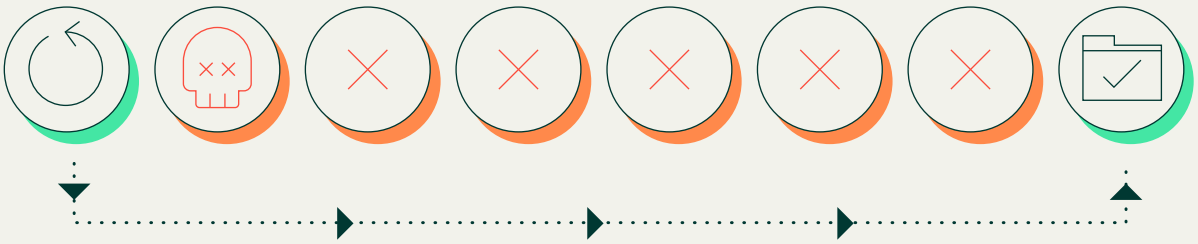
Stone University also analyzed their offline data backups, uncovered a suspected compromised server, and livemounted this server into the forensic environment for detailed analysis.

Then, they hit the JACKPOT

They found the attackers' notes including their compromise plan, compromised accounts, and timeframe. Additional forensics revealed seven more compromised servers and the initial compromise point.

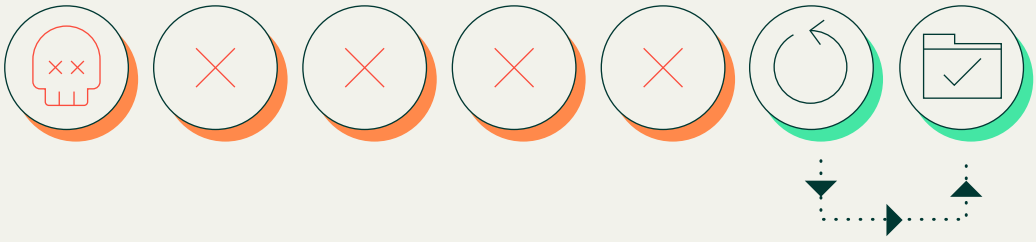
Hopeful, Stone University began rapidly rebuilding their environment in two waves:

First, the actual compromised servers from the initial intrusion



The Stone University team restored the eight compromised servers resident in five VMs from a point-in-time one day before attackers arrived, losing six total days of data.

Secondly, the servers that were encrypted with ransomware, but not part of the initial compromise.



This left the remaining 145 VMs–these required a less intensive response based on only suffering the encryption action. They were restored from backups taken just one day before the ransomware deployment, avoiding five additional days of lost data across these 145 VMs.

The overall recovery operation also required new ESXi hosts, a new vCenter, and an active directory rebuild.

Of all the possible outcomes, this was the best that Stone University could hope for. Optimistic about their progress, Stone University was determined not to pay the ransom.

It can be easy to look past the first major hurdle in an encryption event:

How do you diagnose and analyze something that's encrypted? Does paying the ransom work? Being prepared for this initial encryption moment with clean copies of data provides opportunities. Stone University was prepared, but what factors into being ready for this moment?

Does Paying a Ransom Work? [WR]

46%

External organizations that paid a ransom saw limited returns using attacker-provided decryption solutions with 46% recovering half or less of their data via the attackers.

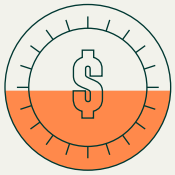
16%

Only 16% of all external organizations recovered all of their data via attacker decryption tools.

Rubrik telemetry revealed the prevalence of ransomware precursors and encryption rates. ®

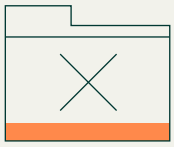
75%

of global organizations observed some level of anomalous activity.



48%

of global organizations observed some form of ransomware attempt against them.



15%

of global organizations encountered some form of successful encryption in their environments requiring data restoration.

Less than **.004%** of all data secured encountered an encryption event. ®

REFERENCE TERMS:

Anomalous behavior detection
Anomalous behavior detection is the first phase in a two-phase process for identifying ransomware. During this process, Rubrik analyzes file system metadata for anomalous behavior, such as an unusual number of files being added, deleted, or replicated. Most anomalous activity isn't ransomware, but needs follow-on investigation.

Suspicious file detection
The second phase of the two-phase ransomware identification process is suspicious file detection. This phase uses a combination of AI and machine learning to evaluate the files identified in the anomalous behavior detection phase for data entropy, file extensions, compression, known malicious ransomware actions, and a variety of other factors indicative of ransomware.

Snapshot analysis
A snapshot is a copy of the offline data backup and typically occurs on an automated, recurring pattern or in ad-hoc tasking. Analytics can then be performed against the completed snapshots.

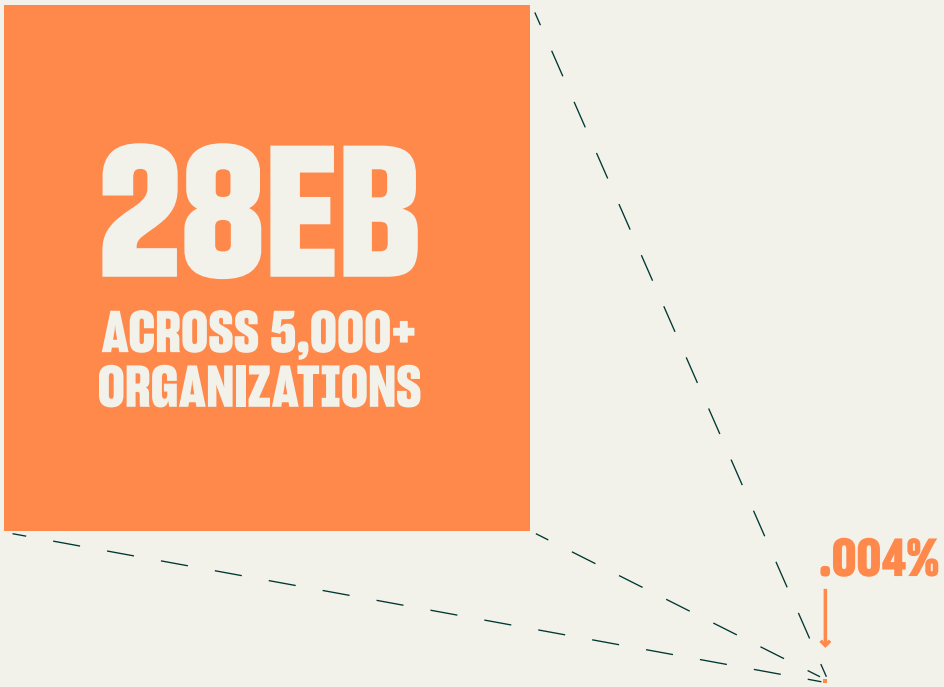
- 27,266,649 snapshots were evaluated for ransomware activity across all Rubrik customers.
- 20,692 snapshots, or .07% of the total number of snapshots, contained anomalous activity.
- 1,198 of the anomalous snapshots, or 6% of all anomalous activity, led to a follow-on encryption event preventing the snapshot completion.
- Of all the snapshots evaluated, only .004% had an encryption issue.
- All encryption events were previously identified as anomalous activity.
- 100% of the encryption events were tied to a lack of multi-factor authentication.

Across all Rubrik customers in 2022 ®

less than .004% of all data secured required further analysis or was indicative of ransomware activity.

This provides a snapshot (pun intended) of how an organization can gain control of its threat surface.

It's virtually impossible to remove your organization from the vast threat landscape, but it is more than possible to remove large swaths of your risk area from this attack surface.



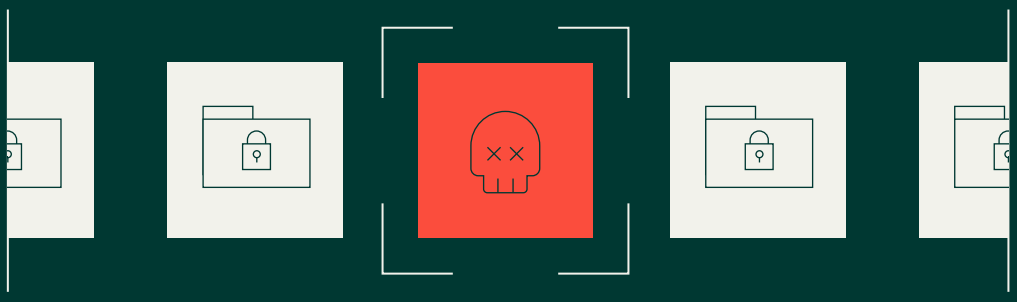
DAY 8:
SECOND RANSOM DEMAND

WAIT... WHAT? WHAT?

Encryption isn't the attacker's only (or preferred) weapon

3 DAYS AFTER

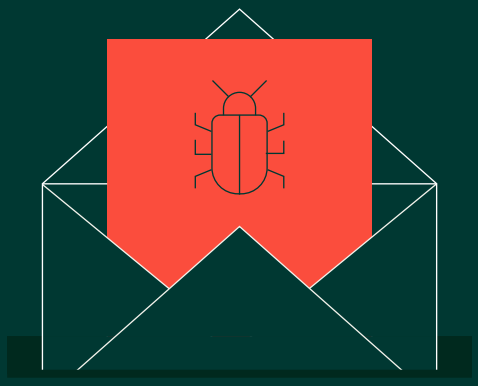
The original ransom demand, the attackers sent a second one. This ransom threatened to leak the 8GB of exfiltrated data to an AvosLocker controlled leak site if the ransom wasn't paid within four days.



The attackers also tried to compromise new portions of the Stone University environment in attempts to survive response actions.

After a hopeful start, this unexpected twist drove Stone University back to the beginning and left them with another tough decision:

Pay the ransom or see their data leaked online.



72%

of non-Rubrik organizations reported paying a ransomware demand.[WR]

DATA DEEPDIVE:

For non-Rubrik organizations who paid a ransom, the specific ransom ratios are: (WR)

40%

paid ransomware demand due to encryption events.

37%

paid ransomware demand due to extortion threats over data leaks.

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

+50M USD

Highest ransomware demand

+7M USD

Highest ransoms paid[13]

13 https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report

AND BREATHE

Data visibility creates decision making opportunity

Stone University shifted their response to three distinct efforts for tackling the data extortion ransom demand.

1

First, they conducted detection and response efforts to identify and counteract the follow-on intrusion efforts. This required replacing multiple servers and firewalls, as well as other hardening actions.

2

Second, they continued data restoration efforts by testing portions of recovered environments then moving these portions into the production environment.

NEW
3

Third, Stone University started assessing the impact if the attacker posted the stolen data online.

But...

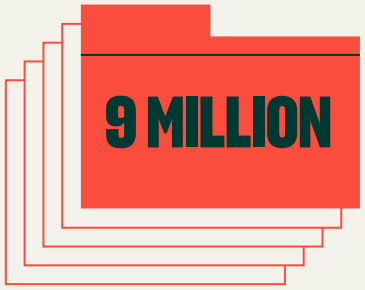
Stone University couldn't determine whether the attackers actually stole 8GB of data or what data was stolen because of the ongoing encryption issues.

So...

Instead, they shifted data impact discovery operations to their most recent data backup.

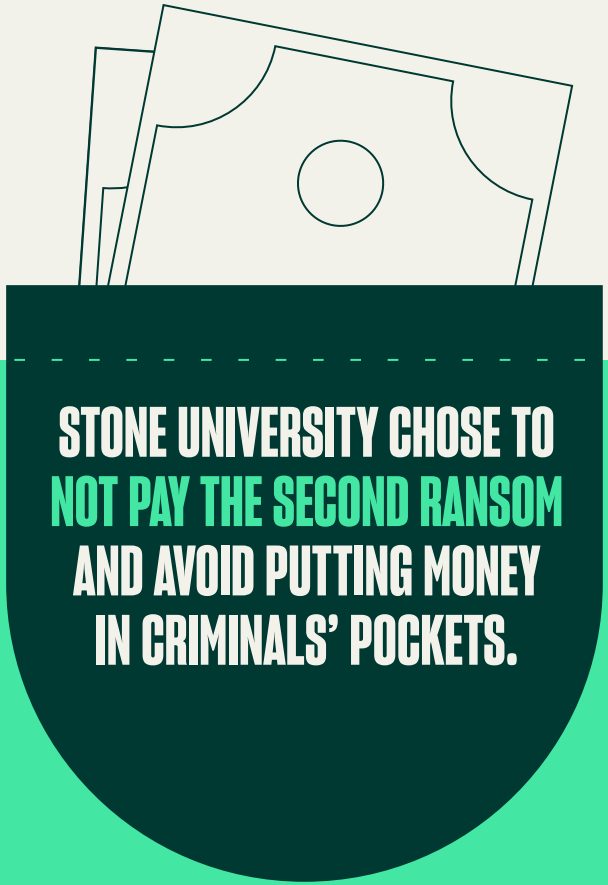
The good news

Stone University found answers within 24 hours and now had three days to make informed decisions.



The bad news

The attackers successfully stole 8 GB of data containing over 9 million sensitive data records ranging from 2013 to the present.



Having their sensitive data leaked would be a huge blow for Stone University, but they understood a hard-earned truth: There is no guarantee sensitive data wouldn't get posted **even if they paid the ransom.**

Instead,
Stone University used the three days to proactively notify impacted individuals and organizations.

By the time the data leaked, Stone University had done the hard, but necessary work to conclude all major response actions...

- ✓ Notify regulatory and compliance organizations
- ✓ Contact affected individuals
- ✓ Shifted to long-term improvements and other required data leak actions

The ripple effect

Most of Stone University returned to normal when the intrusion ended. However the two-week period when the ransomware event occurred had ripple effects that would require weeks to months of effort and decisions to resolve.

Rapidly shifting and scattered data presents real risk for organizations.[RT]

A typical organization has

files containing sensitive data

and

sensitive data records total

Files vs. sensitive data records: Files contain data records. Some of those records can be sensitive. For example, one spreadsheet file can contain hundreds of sensitive data records, while other files might not contain any sensitive data.

A typical organization contains enough sensitive data to max out any/all financial penalty

DATA DEEPDIVE:

Not only is every global organization sitting on a massive amount of data, some of that data would cause tremendous harm if suddenly unavailable or compromised.

One example is sensitive data: This is data derived from various industry standards or regulations—such as PII, HIPAA, GDPR, and CPAA.[14,15,16,17]

There are numerous challenges evaluating data impacts to consumers and organizations alike, but financial penalties for sensitive data offer one option.[18,19,20]

HERE ARE A FEW EXAMPLES:

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

In a typical environment, it would take a fine of less than two Euros per record to reach 20 million Euros.

HIPAA
Penalty for sensitive data exposure: $50 to $50,000 USD per violation, with a max penalty of $1.5 million USD.

Using only the typical file average count, the $1.5 million USD maximum penalty is easily surpassed with a total of $28 million USD at the lowest $50 USD penalty.

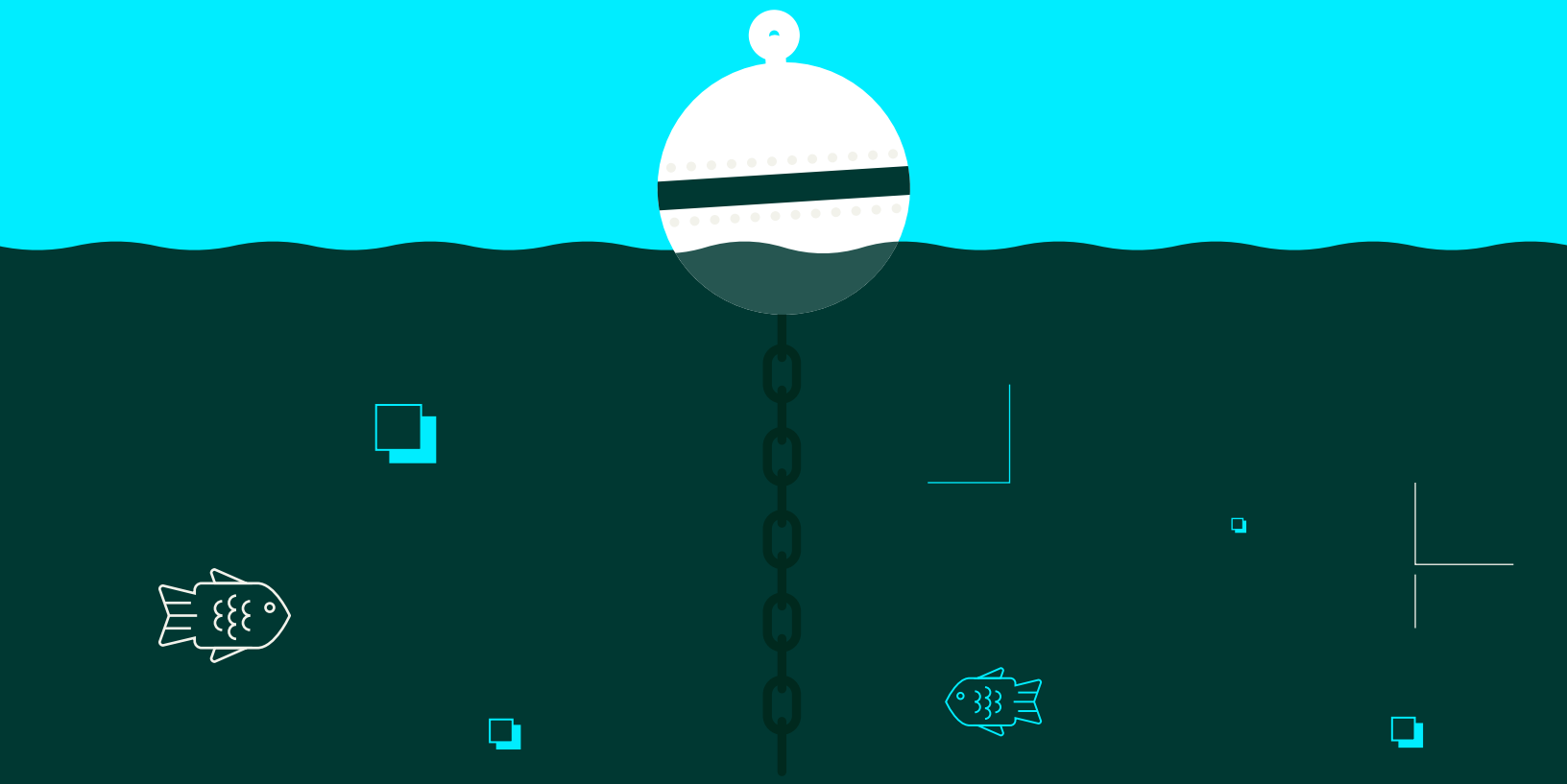
CPRA
Penalty for sensitive data exposure: Up to $2,500 USD per violation, or up to $7,500 for each intentional violation. No penalty cap.

A typical organization's file count alone could result in 1.1 billion USD in fines.

14 https://gdpr-info.eu/art-4-gdpr/
15 https://www.cdc.gov/phlp/publications/topic/hipaa.html
16 https://www.dol.gov/general/ppii
17 https://oag.ca.gov/privacy/ccpa#:~:text=The%20right%20to%20limit%20the,personal%20information%20collected%20about%20them.
18 https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(5)%20GDPR%2C%20the,fiscal%20year%2C%20whichever%20is%20higher.
19 https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/united-states/topics/penalties-for-non-compliance
20 https://cppa.ca.gov/

IMPACT

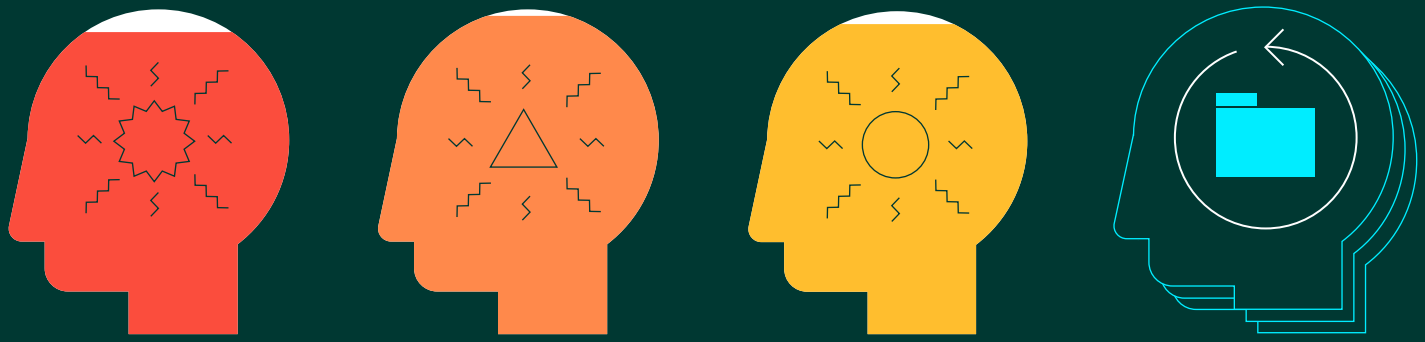
Every intrusion has a natural conclusion, however we shouldn't let our focus end with the event. Instead, let's imagine we've returned to the surface of our ocean of data.



What should we learn from
this deep dive (pun intended)?
What will we do differently?

Intrusions affect business and people ®

The impacts from these intrusions affect our businesses and people well past the end of forensic and IT actions. These impacts linger and make us doubt our ability to operate.



93%

of external organizations encountering a cyberattack in 2022 experienced a negative impact.

98%

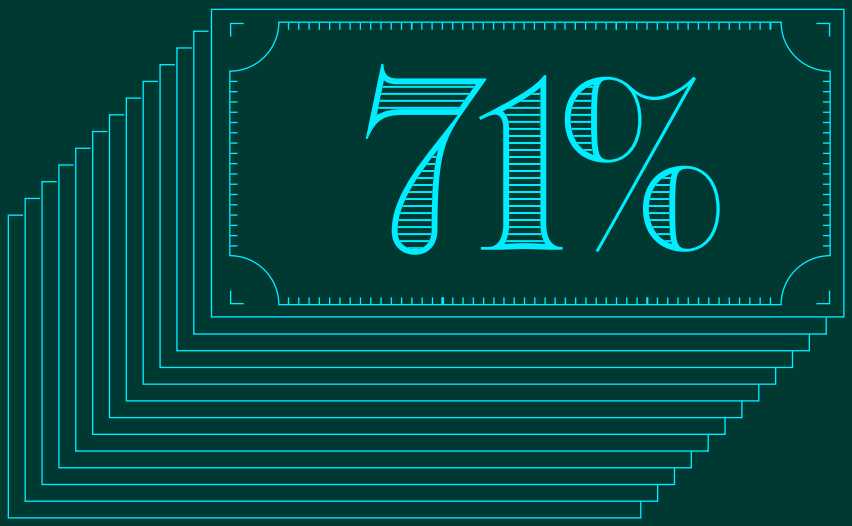
of IT and Security leaders reported significant emotional and/or psychological impacts from these cyberattacks.

96%

of IT and security leaders are concerned their organizations will be unable to maintain business continuity if it experiences a cyberattack.

39%

More than a third of these same leaders believe their board of directors or C-level leaders have little to no confidence in their organization's ability to recover critical data and business applications in the event of a cyberattack



of external organizations are likely to pay a ransomware demand.

93% of companies who experienced a cyberattack in 2022 dealt with negative impacts: (WR)

49% Loss of customers

45% Revenue loss

44% Negative press or reputational damage

42% Leadership forced to change

5% Stock negatively impacted

These attacks are putting strain on leaders with 98% reporting significant emotional and/or psychological impact due to cyberattacks last year:

53% Increased anxiety pertaining to your duties

46% Worry over job security

43% Loss of trust amongst colleagues and team members

41% Loss of sleep or trouble sleeping

Post-Intrusion problems join pre-intrusion problems (WR)

Intrusions aren't isolated events. Challenges existed before the intrusion and these pre-existing obstacles are now paired with predictable post-intrusion impacts:

47%

Almost half (47%) of IT and security leaders believe their 2023 cybersecurity budget is not enough of an investment.

27%

27% of these same leaders expect their IT and cybersecurity budgets to decrease in 2023.

4%

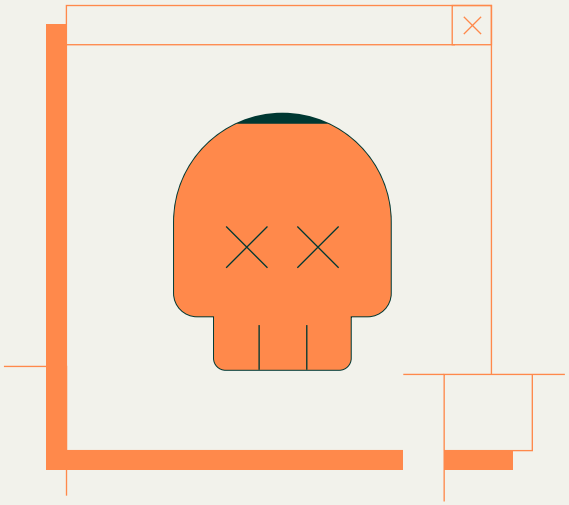
IT and security Leaders will need to work at bringing their teams together with only 4% said there are no factors limiting IT and security alignment.

The top five issues contributing to misalignment between IT and Security teams defending their organizations from cyberattacks are: (WR)

1. **52%** Separate toolsets
2. **51%** Visibility differences
3. **50%** Conflicting priorities
4. **47%** Lack of formal planning or process
5. **45%** Unaligned leadership structures

Intrusions present positive opportunities (WR)

There is light in the dark: Your organization can survive and excel through the inevitable threats. The same intrusions present opportunities for improvement and change.



99%

of organizations that experienced a cyberattack in 2022 implemented new actions:

48%

switched vendors or third party relationships to create better outcomes

54%

increased spending on new technologies or services

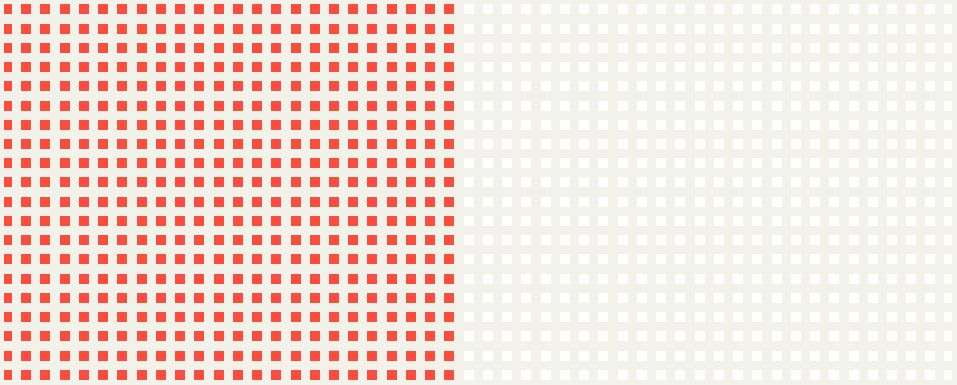
43%

hired additional staff

Despite all these challenges, organizations are improving across the board ®

But not all change has to be driven solely by cyberattacks. Several positive outcomes can be realized if we're ready to capitalize on the opportunities presented by crises as well as systemic resiliency efforts.

Despite **48%** of Rubrik customers enduring some form of ransomware activity...



Less than **.004%** of secured data encountered an encryption event.

Rubrik Zero Labs observed organizations making positive improvements across 2022 and expect this trend to continue throughout 2023. This improvement is seen across every industry and region.

16%

These changes resulted in a typical organization increasing their security posture by 16% in 2022.

97%

Expel notes 97% of ransomware attempts were stopped before ransomware deployment.[21]

21 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

DATA SECURITY VIEW FROM EXPEL: (ER)

11% of all incidents Expel observed in 2022 could have resulted in ransomware deployment

97% of these events were stopped before ransomware deployment. If defenders can detect and respond within the ransomware actors' intrusion cycle, there is a significant opportunity to thwart their malicious goals.[22]

Rubrik provides measurements of a cumulative data security score to its customers and sees an ongoing, positive trend in organizational improvement. The Data Security Score is calculated every 24 hours based on the following categories:

1. Platform Security: Measures the effectiveness of infrastructure security where data is stored and includes topics like user controls, administrative authentication, audit logs, etc.
2. Data Protection and Recovery: Analyzes how well the backup data is secured, if a clean copy of the latest backup is available, and other related factors.
3. Ransomware Investigation: Determines quality and frequency of ransomware threat monitoring and if this data can be recovered after an encryption event.
4. Sensitive Data Discovery: Measures how much sensitive data is being protected, access controls for this data, and if sensitive data is prioritized for recovery.
5. Scores are assessed as following:
   - 0-50: Unsatisfactory
   - 51-75: Needs Improvement
   - 76-90: Satisfactory
   - 91+: Excellent

A typical global organization saw their score increase from **51.2** to **59.47** in 2022, a **16% increase**.

Overall Score Averages: 59.47

Rate of improvement in 2022: 16.2%

"We must remember security doesnt exist in a vacuum. As businesses look to do more with less, theres an urgency to lean on scalable, efficient technology, such as cloud options. But fast adoption, particularly for companies not born in the cloud, comes with risk. As new tech is adopted to keep up with changing markets, security teams can likely anticipate upticks in security incidents--usually due to easy-to-miss, easy-to-exploit misconfigurations or exposed access keys."

Jonathan Hencinski, VP, Security Operations, Expel

22 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

The more our communities are affected by cybercrime, the more we owe each other.

We can build better products/services and advocate best practices, but we also must share what we learn. Every new lesson is a step forward.

To that end, Rubrik Zero Labs would like to end where we started: thanking the four organizations allowing us to leverage their data, extend our appreciation to Wakefield Research for their work, recognizing Shaped By for their efforts to craft this story, and highlight the contributions from the following Rubrik members for their direct work on this effort: Amanda O'Callaghan, Ajay Kumar Gaddam, Sham Reddy, Kumar Subramanian, Linda Nguyen, Lynda Hall, Kelsey Shively, Kelley Cooper, and the Rubrik Creative and "Dev" Teams.

Rubrik Zero Labs