REFERENCE ARCHITECTURE

Rubrik Data Security Command Center

February 2023

Table of Contents

THE NEED FOR DATA RISK MANAGEMENT

Protecting business data and applications is at the forefront of many organizations' security initiatives. According to Checkpoint, 2021 saw a 50% increase in cyberattacks year over year, with the number only expected to increase further. In order to combat attacks, organizations go to great lengths to mitigate risk at the network edge. However, zero-day exploits and previously unknown vulnerabilities are popping up every day, circumventing network security and attacking a business's most valuable asset, its data. The increased number of attacks, coupled with organizations' increased use of digital services, has naturally led to increased risk for business data. Thereby to truly assess an organization's security posture, an additional form of risk management is required—data risk management. This paper will explore the following:

- The need for data risk management processes
- Why data risk management is important
- How to perform data risk management
- How Rubrik aids in the data risk management process

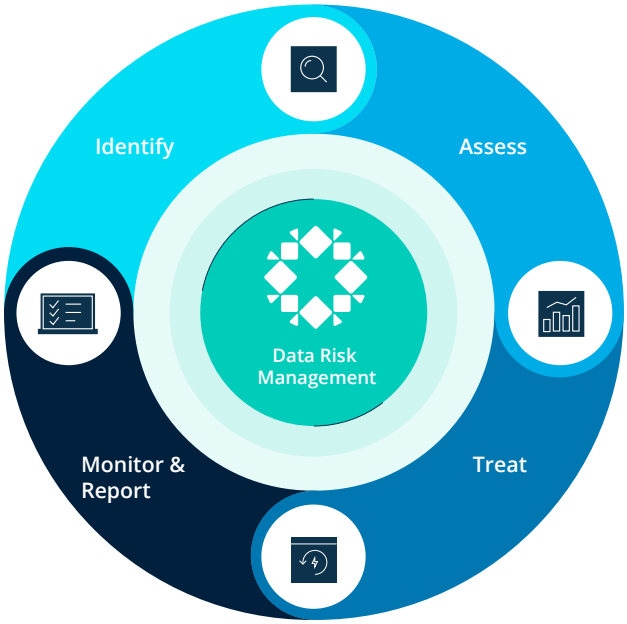
Traditionally risk management has focused solely on application implementation and network security—ensuring newly introduced applications or network modifications minimize the risk they introduce into environments. Rarely does traditional risk management inspect data or its usage as part of the overall process. Furthermore, backup systems are often left behind during these conversations, leaving a global catalog of an organization's data neglected and open to attack. Data risk management adds a layer that focuses solely on data, both in production and backup, identifying risks and answering important questions such as:

- Is my backup data immutable? Can ransomware encrypt my backup data? Am I able to successfully restore from my backup data?
- Is my backup data clean? Can I safely restore it without reinfecting my environment? Is all my data protected?
- Where is my sensitive data located? Who has access to this sensitive data?
- Are the user accounts with access to my data secure? Is multi-factor authentication globally enforced? Can a rogue administrator circumvent these protections?
- Data risk management provides continuous visibility into the safety of data, both identifying and mitigating data risk as well as validating data usage and recoverability of the backup systems protecting it.

THE DATA RISK MANAGEMENT PROCESS

The result of a proper data risk management process is to minimize the probability of data being exposed or breached, while also minimizing the business impact should a breach occur. There are four main steps to continuously assessing and mitigating data risk:

1. Identifying data risk
2. Assessing data risk impact
3. Treating data risk
4. Monitoring and reporting data risk



Following the data risk management process will not only minimize business impact and known risks but drive awareness of unknowns within data, ultimately increasing the overall security posture of an organization.

IDENTIFYING DATA RISK

The first step in data risk management is to identify and document all of the risks and events that can threaten the safety or security of an organization's data. Often, organizations informally follow this process without even knowing they are performing risk management. For instance, data resilience risk is mitigated by ensuring RAID or erasure coding is utilized to protect against hardware failure. Data integrity risks are mitigated through the use of filesystems that deploy frequent thumbprint checks or immutability. Data availability risk is mitigated by ensuring a backup system is in place. While these common risk mitigations are table stakes for most organizations, it's important to ensure that these risks are properly managed and documented.

In addition to the well-known data risks, it's important that organizations think beyond how data is stored and take a broad and holistic approach to identify other types of data risk. A good way of identifying data risks is to run through various scenarios that apply to your organization, asking yourself "what if" and documenting the outcomes. For example:

- What if an account was breached? What would you have to think about? Does that account have access to sensitive data?
- What if one of your applications were breached? What issues does that present? What data does that app contain?
- What would happen if ransomware encrypted your entire environment today? Is your backup data also at risk? How quickly can you identify and mitigate a cyber threat such as this?

Identifying data risk is a crucial first step in the data risk management process because it bubbles up unknowns and drives awareness around commonly overlooked data risks.

ASSESSING DATA RISK

Once data risks have been identified and documented, the next step is to assess the overall qualitative and quantitative impacts each data risk presents. Data risk assessment involves understanding both the probability of the risk becoming a threat and the potential business impact. Once complete, a proper risk assessment will take the probability and impact of a risk and combine them to produce a quantitative result. This result, be it a risk score or matrix (low/medium/high severity), can be used to prioritize mitigation strategies. For example, take the following scenario:

- Our sensitive data is stored unencrypted and secured by Active Directory groups. Multi-factor authentication (MFA) isn't globally enforced.

A number of risks and associated quantitative risk scores can be generated from the above example. For instance:

- Without the requirement to enable MFA, the ability for external threats to easily compromise accounts is increased, which increases the risk of exposing sensitive data – HIGH SEVERITY
- Sensitive data is not encrypted, meaning if breached, it is easily readable – HIGH SEVERITY
- System administrators have the ability to add themselves to certain Active Directory groups, which means they can grant themselves access to sensitive information. This opens the door for internal threats – MEDIUM SEVERITY

Properly assessing each risk is very useful in determining the budgets and resources needed in order to successfully mitigate the risk itself.

TREATING DATA RISK

Once risks are identified and assessed, the next step is to treat the risk. Treating risk involves taking action on the risk assessment and most often results in either:

1. Reducing the probability of an issue occurring.
2. Reducing the impact of the risk should it occur.

Following along with the sensitive data risk example from above, risk treatments might include:

- Globally enforcing multi-factor authentication to reduce the probability of an outside threat gaining access to sensitive data.
- Encrypting sensitive data to reduce the impact an internal or external breach may have, should it occur.

Risk treatment should always result in the risk being either eliminated or contained and should positively contribute to an organization's overall data security posture.

MONITORING AND REPORTING DATA RISK

The idea of monitoring and reporting on data risk is to ensure that the process is not just a one-time function, but a continuous ongoing mechanism within an organization. Some organizations may deem a risk to be acceptable and skip the treatment step, however, it's of the utmost importance that this is reported. Furthermore, reporting on the risk may in itself help to discover new risks. For instance, in the ongoing example,

treating the sensitive data encryption risk by enabling encryption does help reduce impact. However, encryption in itself presents a number of other risks that need to go through the assessment process. For example:

- Who owns the decryption keys?
- Who has access to these keys?
- Where will they be stored?

Monitoring and reporting ensure that organizations are in control and aware of all identified, assessed, and treated risks and can shed light on any new risks introduced by treatments.

DATA RISK MANAGEMENT MUST BE CONTINUOUS AND AUTOMATED

Organizations are constantly creating, modifying, and deleting data. They migrate or relocate it, feed it into analysis solutions, and utilize it to drive business decisions. Without an automated data risk management solution, organizations run the risk of leaving their data unprotected, or worse losing track of it altogether.

While traditional risk management is often applied once, during the implementation of an application or project, data risk management must be continuously running in the background to keep up with the pace of data creation and modification. As organizations mature, they start to use more apps and store their data in more places, including the cloud. This data sprawl, and the rate at which the data is changing, is more than any one team can keep up with even with a continuous manual data risk management process. Teams need automation to tell them how their data has changed over time, whether or not it's protected, and who has access to it.

Automated data risk management processes give organizations the nearly instantaneous feedback they need in order to make smart, intelligent, and often crucial security-related business decisions. Automated data risk management solutions also go beyond simply mitigating risk to show just how risk mitigation can impact the overall security posture of an organization with risk scores that can be tracked and trended over time.

RUBRIK DATA SECURITY COMMAND CENTER – AN AUTOMATED, CONTINUOUS DATA RISK MANAGEMENT SOLUTION

Rubrik Data Security Command Center (DSCC) helps organizations determine whether their data is safe and protected. Data Security Command Center is a SaaS service that provides visibility into an organization's data risks and security gaps, and offers recommendations to improve its overall security posture. It radically simplifies data risk management by using a single dashboard for global visibility and collaboration. As a result, organizations can reduce the complexity of data risk management, avoid unnecessary costs and make smarter, data-driven business decisions around data security.

VISUALIZE DATA RISK

Get data risk scores, identify cyber exposures, and gain insights into security weaknesses.

BOOST DATA SECURITY

Improve your overall data security posture with an advanced recommendation engine.

BENCHMARK AGAINST PEERS

Compare your data security against peers and get actionable next steps to meet standards.

KEY BENEFITS

Quantifies data risk using a data security score and gives you an at-a-glance view of your data security posture.

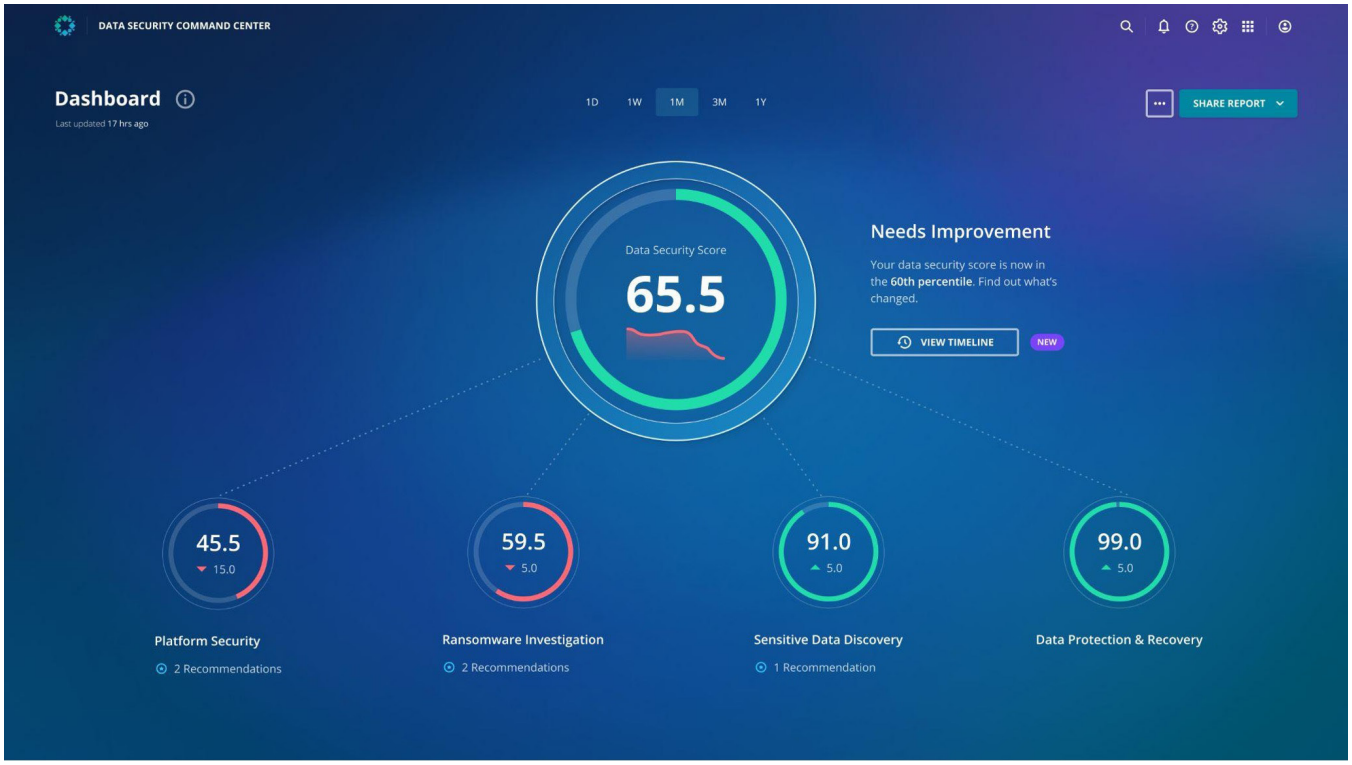
Identifies security gaps and gives actionable recommendations to reduce data risk across four categories:

- **Platform Security:** Analyzes how well backup data is safeguarded against compromise, deletion, and threats of ransom. Also measures the effectiveness of user controls, admin authentication, and audit logs.
- **Data Protection and Recovery:** Checks availability of a clean copy of the latest backup and whether it meets the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).
- **Ransomware Monitoring and Investigation:** Determines which data is being actively monitored for ransomware threats and whether the data can be recovered post-attack.
- **Sensitive Data Monitoring and Remediation:** Measures how much sensitive data is being protected and prioritized for recovery.

Streamlines data risk management across the Rubrik data environment, and gives you comprehensive visibility and control over data risk.

Gets everyone invested in data security by generating easy-to-understand data security reports that can be shared with executives, internal security groups, GRC (governance, regulatory, and compliance) teams, and more.

Benchmarks you against industry peers and creates actionable plans to improve security posture and gain competitive advantage.

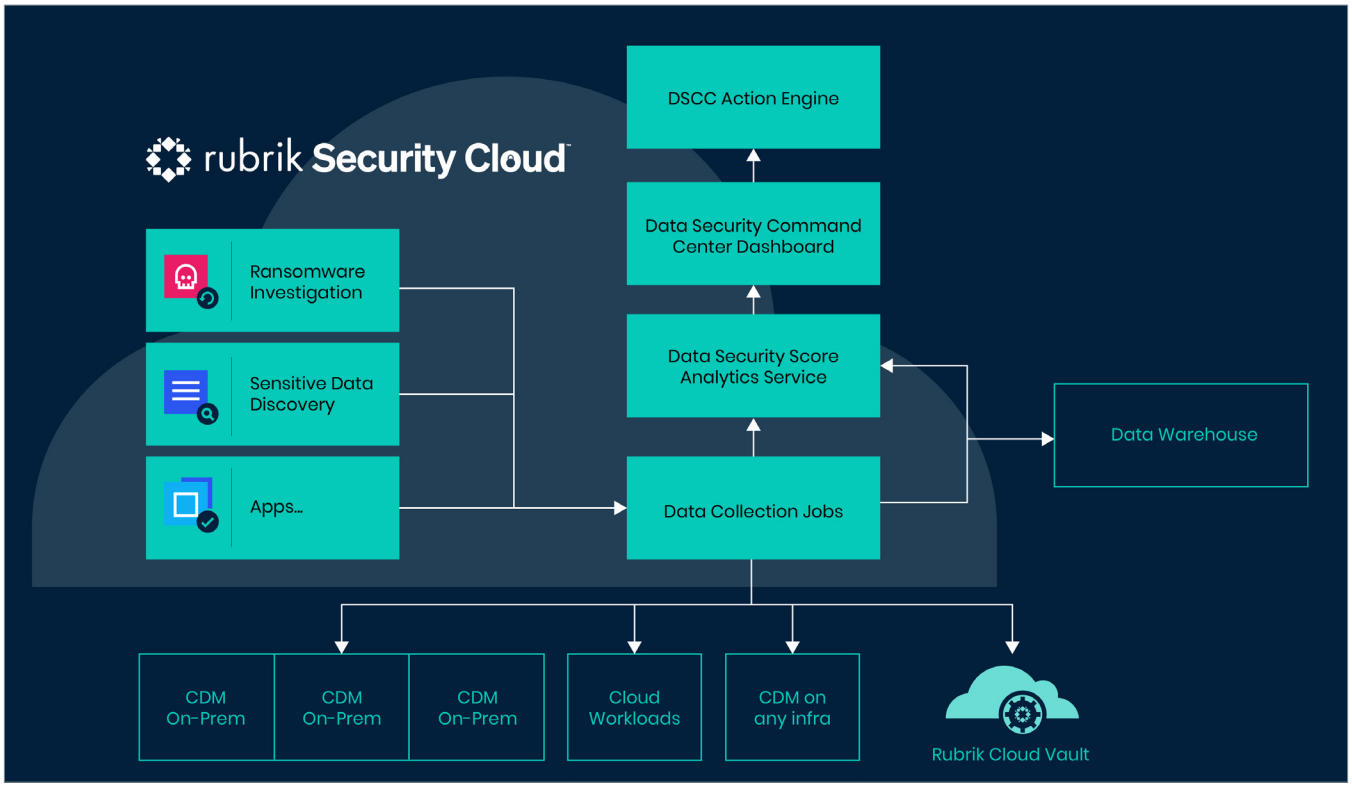


No installation is required. Data Security Command Center is part of the Rubrik Security Cloud, which unifies the management of your data security applications and data protection policies (backup, archival, replication, and DR).

Prerequisite: Organizations need a subscription to Rubrik Enterprise Edition to access all of Data Security Command Center's capabilities. Foundation and Business editions will include limited functionality.

HOW IT WORKS

Data Security Command Center analyzes data collected from Rubrik data security services, such as Ransomware Monitoring and Investigation and Sensitive Data Monitoring and Remediation services, as well as existing security configurations, access controls, audit logs, encryption scanners, security logs, and more. The collected data is cleaned and converted into meaningful risk metrics. These metrics are evaluated against Rubrik security best practices and used to determine the risk score for a given category. These scores are then aggregated and used to determine an overall data security score, which serves as a single security indicator for the entire Rubrik data environment.



At the heart of Data Security Command Center lies a data pipeline. The data pipeline gathers metadata and logging information from Rubrik software running both on-premises (Rubrik CDM) and within the Rubrik Security Cloud. This metadata is gathered regularly, processed, and placed in a data warehouse. From there, the data is analyzed and risk scores are calculated before being published through the main Data Security Command Center dashboard or generated pdf reports. Scores are updated on a daily interval.

COLLECTED METRICS

Each metric belongs to one of four main categories: Platform Security, Data Protection and Recovery, Ransomware Monitoring and Investigation, and Sensitive Data Monitoring and Remediation.

Platform Security Metrics

The platform security risk score is generated by evaluating metrics focusing on the security of Rubrik's core platform. Collected metrics within this category are

- **Encryption –** To determine an encryption score, DSCC evaluates information from Rubrik clusters in regard to both hardware- and software-based node encryption. A percentage is calculated by determining the number of nodes encrypted vs. the total number of nodes deployed and monitored. ***Encryption is a key layer in a defense-in-depth approach and should almost always be leveraged.***

*****NOTE*** Encryption metric is informational only and is not included in any scoring.**

- **Authentication and Authorization –** The metrics around authentication and authorization are driven by calculating the percentage of both local and Active Directory users that have time-based one-time passwords (TOTP) or multi-factor Authentication (MFA) enabled. Any externally provisioned SSO through third-party providers such as OKTA are not included within this calculation as they are not discoverable by the Rubrik platform. ***Ensuring MFA is enabled not only helps protect your data but ensures that even if accounts do get compromised attackers will need physical access to an additional user-defined device before being considered fully authenticated.***

- **Outdated CDM Software Version –** This metric monitors the currently running version of all CDM clusters attached to Rubrik Security Cloud. Depending on the versions installed, clusters are labeled either stable (meaning they are currently up to date), Upgrade Recommended (meaning an upgrade is available), or Unsupported (meaning the currently running version is out of Rubrik support). ***Keeping your Rubrik software up to date ensures you always have the latest security patches applied.***

*****NOTE*** The outdated CDM version metric is informational only and is not included in the overall scoring.**

Together, the applicable metrics are averaged and bubble up to deliver the overall platform security risk score.

Data Protection and Recovery Metrics

The Data Protection and Recovery risk score is calculated by analyzing a number of metrics focused on the protection and recovery of the objects discovered and protected by the Rubrik platform. Collected metrics within this category are:

- **SLA Compliance –** The SLA compliance risk score is calculated by analyzing all of the objects within the Rubrik platform that have been protected by an SLA Domain, ensuring that backups exist within the defined RPO and retention values. ***Making sure that objects are compliant with their SLAs gives peace of mind that the proper number of restore points exist, allowing organizations to always be held accountable to designated RPO values.***

- **Protected Objects –** The protected objects metric is calculated by determining the percentage of objects protected versus the total number of objects that have been discovered and inventoried by Rubrik. Objects that have been explicitly set to "Do Not Protect" are excluded from these calculations. ***Understanding what objects are protected is important, but perhaps more valuable to organizations is understanding what objects have not been protected at all.***

- **SLA Retention Lock –** The SLA Retention Lock risk score is calculated by determining the percentage of SLAs leveraging retention lock versus the total number of created SLA Domains. ***SLA Retention Lock is often used as a last line of defense, ensuring that backups are not able to expire, be it by malicious or accidental deletion or NTP-focused attacks.***

- **Low Runway Remaining –** This metric records the number of CDM clusters that have low available runway remaining. Clusters are deemed to have low runway when the estimated runway drops below 30 days. The score is calculated by determining the number of clusters connected to Rubrik Security Cloud that have low runway remaining. ***Ensuring that available capacity exists on CDM clusters to support runway allows Recovery Point Objectives defined within the SLA Domain to be fulfilled without interruption.***

Together, the above metrics are averaged and bubble up to deliver the overall Data Protection and Recovery risk score.

Ransomware Monitoring and Investigation Metrics

The Ransomware Monitoring and Investigation risk score is used to rank an organization's preparedness and resilience in the face of a ransomware attack. Collected metrics within this category are:

- **Ransomware Monitoring and Investigation Enabled Clusters –** This metric is determined by calculating the percentage of the number of Rubrik clusters that have recently performed a Ransomware Monitoring and Investigation anomaly scan versus the total number of Rubrik clusters existing within the environment. ***Ensuring that Ransomware Monitoring and Investigation service is enabled and scanning is a key step in being able to quickly detect a ransomware attack and determine the blast radius.***

Sensitive Data Monitoring and Remediation Metrics

The Sensitive Data Monitoring and Remediation risk score is used to rank an organization's ability to detect and discover where its sensitive data is located. Collected metrics within this category include:

- **Sensitive Data Monitoring and Remediation Enabled Clusters –** This metric is determined by calculating the percentage of the number of Rubrik clusters that have Sensitive Data Monitoring and Remediation service enabled versus the total number of Rubrik clusters within the Rubrik Security Cloud instance. ***Ensuring that Sensitive Data Monitoring and Remediation is enabled and scans are being performed allows organizations to better understand the location of their sensitive data along with who has access to this data, providing a means to take action if necessary.***

- **Open Access Files with Sensitive Data –** This metric will capture the total number of sensitive files having open access, excluding those which have been marked as "allowed". The calculation is based on the latest available result for each object. ***Ensuring that files containing sensitive information are locked down through permissions and ACLs is crucial in minimizing the overall impact of attacks should they occur.***

COLLECTED INSIGHTS

While the metrics outlined above are utilized to determine an overall risk score, Data Security Command Center also collects a number of other insights which are only displayed, but not included as part of the overall category or security score. While Insights don't affect the overall score, they are still used to generate recommendations for an account and can be leveraged to improve an organization's overall security posture.

Data Protection and Recovery Insights

The following Data Protection and Recovery Insights are generated in order to provide actionable recommendations:

- **Objects marked as Do Not Protect –** This insight displays the number of objects existing within Rubrik Security Cloud that are currently marked as "Do Not Protect". ***Objects explicitly marked as "Do Not Protect" will not inherit and SLA Domains and therefore will not be included within any backup tasks. It's important to know how many and which objects that have been explicitly assigned "Do Not Protect" to ensure optimal data protection and avoid any potential threats.***

Ransomware Investigation and Monitoring Insights

The following Ransomware Investigation and Monitoring Insights are generated in order to provide actionable recommendations:

- **Anomalies Detected –** This insight displays the number of anomalous snapshots detected by the Ransomware Investigation and Monitoring service that exist within the time range currently selected within the category view page. ***A high number of anomalous snapshots within a given timeframe can be a key indicator that a workload has been compromised.***

RISK SCORING

Scoring with Rubrik Data Security Command Center is simple and easy to understand. Each top-level risk score is generated by computing the average based on the individual metrics collected within that given category.

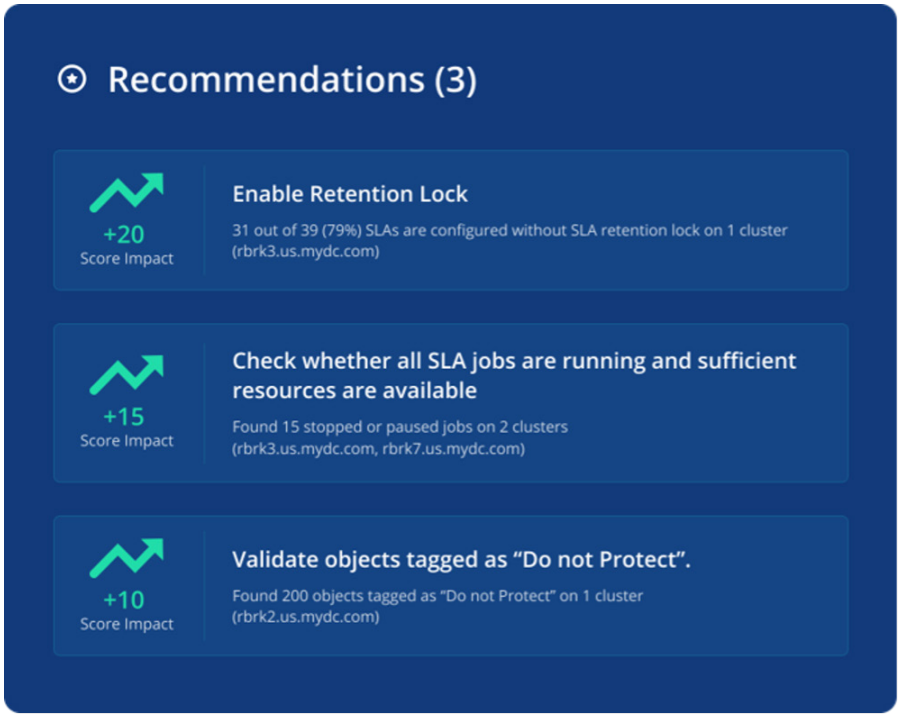
From there, the top-level risk scores are again averaged out and used to determine the overall Data Security Risk score.

Visual prompts, such as circular progress bars and numbers, are used to show the current score. These prompts are color-coded using the following guidelines:

- Green - 75%-100%
- Yellow - 50%-75%
- Red - <50%

RECOMMENDATIONS, ACTIONS, AND ALERTS

At the core of Data Security Command Center lies the recommendation and action engine. The engine provides organizations with recommendations and actions they can take to treat the identified risks, while providing insight into how those recommendations will impact the overall risk score.



As shown above, DSCC illustrates that enabling retention lock on the remaining SLA Domains will increase the respective score by 20 points, thus increasing the overall data security score.

DSCC recommendations are generated based on industry and Rubrik security best practices, allowing organizations to minimize the amount of risk present within their environments.

The recommendation and action engine covers the Risk Assessment and Risk Treatment steps of the data risk management process outlined above. However, DSCC automates the Risk Assessment step and provides suggestions for the Risk Treatment step, reducing the amount of effort it takes to practice data risk management.

INDUSTRY COMPARISONS

By combining an organization's risk score with other business metrics from trusted sources, Data Security Command Center provides customers with insight into how they rank against other customers within similar sectors or sizes. Customers can measure themselves against:

- The entire Rubrik customer population
- A specific sector or vertical
- Companies with similar annual revenues
- Companies of similar size (number of employees)

Note: Rubrik never shares scores or metrics with any external parties nor between customers. Metrics used for comparison are completely randomized and rolled up and used only to grant a reference point on how well organizations are doing in comparison to others.

Benchmarking against industry averages allows organizations to gain insight into and see how their security posture stacks up against that of their peers. These insights can be invaluable when looking to boost your overall security posture. Benchmarking metrics can also be shared with executives and the C-suite to make informed business decisions around areas in need of security-related budgets.

CUSTOMER USE CASES

DSCC extracts a variety of metrics from an organization's environment, which can then be used in a number of use cases. The top four business applications of DSCC include Data Risk Awareness and Assessment, Compliance and Data Risk Mitigation, Executive Reporting, and Industry Benchmarking.

DATA RISK AWARENESS AND ASSESSMENT

Utilizing DSCC, organizations are able to gain a solid understanding of exactly where they stand as it pertains to security-related configurations within their environment. With easy-to-use dashboards, security gaps can be quickly identified and organizations can take action to ensure that risks are mitigated and data is protected.

COMPLIANCE AND DATA RISK MITIGATION

Recovery from cyber attacks is nearly impossible if data isn't protected in the first place. DSCC provides organizations with a high-level overview of how well they are protecting workloads within their environment—pointing out where gaps exist—as well as whether or not protected workloads are compliant with the SLA Domain constructs applied to them. Ensuring all data is compliant with SLA Domains not only allows organizations to use Rubrik as a defense mechanism, but mitigates the risk of data loss when attacks occur.

EXECUTIVE REPORTING

Being able to provide executive and C-level professionals with an updated, easy-to-read risk report of where their organization stands within the realm of security helps to drive better-informed security-related decisions, prioritizations, and purchases. Ensuring investments, both financially and operationally, are targeted toward minimizing risk improves the overall security posture of an organization.

INDUSTRY BENCHMARKING

Comparing individual risk scores against those of their peers, based on location or size, is invaluable when an organization is looking to gauge where they stand. DSCC allows organizations to benchmark themselves against other similar industry peers, providing visibility into whether they are falling behind, staying in line with the status quo, or leading the way in terms of security best practices.

CONCLUSION

Data Security Command Center combines data observability that identifies and quantifies risks, intelligent data risk management for automated mitigation, and data resilience benchmarking to compare an organization's security posture to that of its peers. Through these three capabilities, DSCC helps organizations quickly assess whether data is safe and capable of recovering from a cyber-attack. It gives organizations the ability to identify security gaps, categorize risks, and get actionable guidance to improve their overall security posture. And it helps IT and Security teams compare their progress to industry peers and executives make smarter and more confident business decisions around data security.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

tr-rubrik-data-security-command-center / 20230201