rubrik

User Access: Understanding who has access to your Sensitive Data

Understanding what type of sensitive data your organization has, where it is located, and how much of it exists is critical for an organization's compliance purposes—knowing exactly who has access to that data takes Sensitive Data Monitoring to a new realm, enabling organizations to take critical, proactive measures to ensure their sensitive information is protected and secure.

CHALLENGE

As organizations grow, so does the amount of data they generate. Part of this growth results in the increase in sensitive data exposure from several factors, including cloud adoption, remote work, and utilizing 3rd party vendors or supply chain partners—all needed to meet crucial technological requirements. Still, they also increase the attack surface targeted by bad actors. The sophistication and volume of cyber-attacks organizations face are also growing at an alarming rate, with 99% of IT & security leaders reporting that they were aware of at least one attack in 2022. Of all the attacks faced by organizations in 2022, 59% were data breaches, and 41% were insider events. The risk of data exfiltration and double extortion is higher when user access to sensitive data is assigned broadly. Organizations need to become more proactive to avoid lengthy and costly downtime. Failure to do so can result in financial loss, reputational damage, erosion of customers' trust/loyalty, legal issues, and more.

SOLUTION

Rubrik User Access enables organizations to reduce the risk of sensitive data exposure by providing insights into data access permissions. With User Access, organizations can proactively identify and remediate data exposure risks before they result in breaches. By leveraging advanced analytics, organizations can also achieve faster incident response times without cumbersome agents. With Rubrik's proactive approach to data security, organizations can safeguard their sensitive data from unqualified access.

HOW IT WORKS

Before User Access can perform risk management related to data access, organizations need to specify the types of sensitive data that are critical within the environment. By assigning risk levels to the pre-built and custom analyzers within Sensitive Data Monitoring, organizations can align User Access risk assessment to the priorities and goals of the business. For instance, organizations may set an analyzer scanning for PCI and financial data as high-risk, while configuring an analyzer scanning for IP Addresses as low risk.

Once analyzers are assigned to policies, then policies to workloads, Rubrik will automatically begin scanning workloads for sensitive data after backups have been ingested into the platform. Metadata generated around the ACLs within the workload is then coupled with metadata retrieved from an Active Directory backup, allowing Rubrik to query and resolve SSIDs on the ACLs, and report on not just the types of sensitive data, where the data is located, but also who has access and what types of access those users have.

CUSTOMER BENEFITS

By classifying sensitive data, pointing out where it is located, and indicating who has access to it, Rubrik customers gain key insights into their sensitive data landscape to:

Proactively Prevent Unqualified Access:

Reduce data exposure risk by proactively ensuring only qualified users have access to sensitive data.

Accelerate Incident Response:

Empower your incident response teams with intelligence detailing who had access to sensitive data involved in a breach.

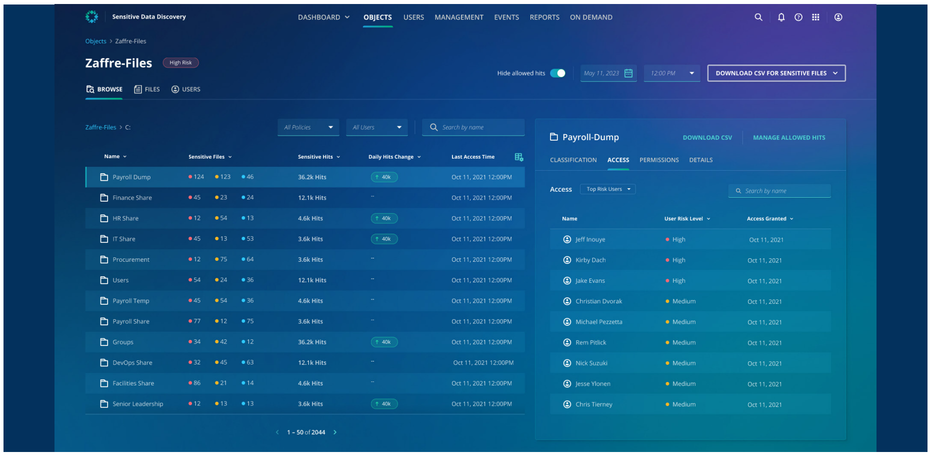
Operational Efficiency:

Reduce data exposure risk and accelerate incident response without the need to deploy and manage cumbersome agents that slow down business.

ASSIGN RISK TO SENSITIVE DATA ANALYZERS

No two pieces of sensitive data are the same—so why treat their risk levels the same?

User Access allows organizations to assign risk levels to the pre-built and custom analyzers within Sensitive Data Monitoring. For instance, analyzers scanning for PII data may be deemed high risk, while those looking for IP Addresses are set to low risk. Assigning individual risk levels to sensitive data analyzers allows User Access to better report on and reflect an organization's risk based on their business priorities and initiatives.



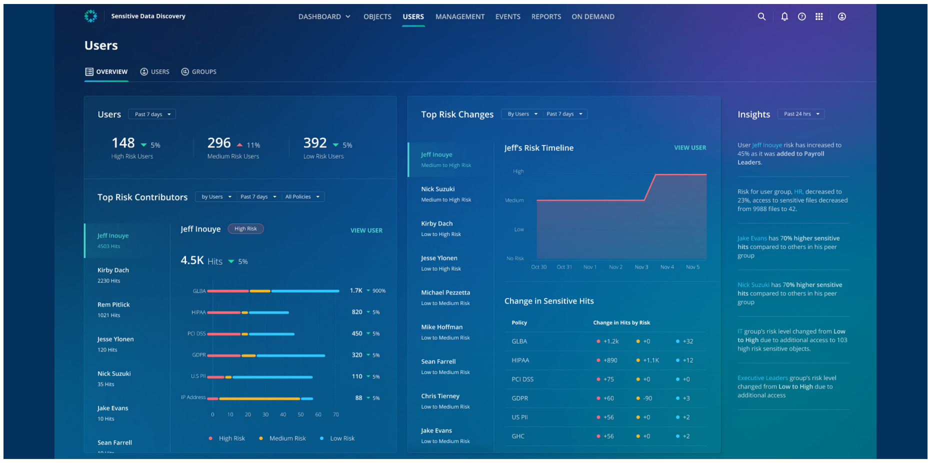
Zaffre-Files

Name	Sensitive Files			Sensitive Hits	Daily Hits Change	Last Access Time
Payroll Dump	● 124	● 123	● 46	36.2k Hits	↑ 40k	Oct 11, 2021 12:00PM
Finance Share	● 45	● 23	● 24	12.1k Hits	--	Oct 11, 2021 12:00PM
HR Share	● 12	● 54	● 13	4.6k Hits	↑ 40k	Oct 11, 2021 12:00PM
IT Share	● 45	● 13	● 53	3.6k Hits	↑ 40k	Oct 11, 2021 12:00PM
Procurement	● 12	● 75	● 64	3.6k Hits	--	Oct 11, 2021 12:00PM
Users	● 54	● 24	● 36	12.1k Hits	--	Oct 11, 2021 12:00PM
Payroll Temp	● 45	● 54	● 36	4.6k Hits	--	Oct 11, 2021 12:00PM
Payroll Share	● 77	● 12	● 75	3.6k Hits	--	Oct 11, 2021 12:00PM
Groups	● 34	● 42	● 12	36.2k Hits	↑ 40k	Oct 11, 2021 12:00PM
DevOps Share	● 32	● 45	● 63	12.1k Hits	--	Oct 11, 2021 12:00PM
Facilities Share	● 86	● 21	● 14	4.6k Hits	--	Oct 11, 2021 12:00PM
Senior Leadership	● 12	● 13	● 13	3.6k Hits	↑ 40k	Oct 11, 2021 12:00PM

Payroll-Dump

Name	User Risk Level	Access Granted
Jeff Inouye	● High	Oct 11, 2021
Kirby Dach	● High	Oct 11, 2021
Jake Evans	● High	Oct 11, 2021
Christian Dvorak	● Medium	Oct 11, 2021
Michael Pezzetta	● Medium	Oct 11, 2021
Rem Pitlick	● Medium	Oct 11, 2021
Nick Suzuki	● Medium	Oct 11, 2021
Jesse Ylonen	● Medium	Oct 11, 2021
Chris Tierney	● Medium	Oct 11, 2021

From there, Rubrik performs risk analysis functions by calculating risk on the sensitive files, the workloads containing those files, along with the users with access to the files. Information is bubbled up into the Rubrik Security Cloud dashboard that organizations can leverage to easily determine where within their environment high risk files are located, along with who their high-risk users are.



Change in Sensitive Hits

Policy	Change in Hits by Risk		
GLBA	● +1.2k	● +0	● +32
HIPAA	● +890	● +1.1K	● +12
PCI DSS	● +75	● +0	● +0
GDPR	● +60	● -90	● +3
US PII	● +56	● +0	● +2
GHC	● +56	● +0	● +2

User Jeff Inouye risk has increased to 45% as it was **added to Payroll Leaders**.

Risk for user group, HR, decreased to 23%, access to sensitive files decreased from 9988 files to 42.

Jake Evans has **70% higher sensitive hits** compared to others in his peer group

Nick Suzuki has **70% higher sensitive hits** compared to others in his peer group

IT group's risk level changed from **Low to High** due to additional access to 103 high risk sensitive objects.

Executive Leaders group's risk level changed from **Low to High** due to additional access

RISK ANALYSIS THROUGH VARIOUS LENSES

Rubrik's User Access provides valuable risk insights through the lens of files, objects, and users.

File Risk

Easily identify high, medium, and low risk files based on analyzer hits of containing high, medium, and low risk classifications.

Object Risk

Workloads containing high, medium and low risk files are subsequently deemed high, medium, or low risk objects. Easily discover all the high risk workloads within your environment.

User Risk

Depending on the risk classification of files and workloads that users have access to, the users themselves are marked as high, medium, or low risk accounts. Easily discover all the high risk users within your environment, and take proactive measures to ensure desired access is accurately reflected.

Aside from just pointing out who has access to the data, User Access also provides valuable insights into when and why a user's risk level has changed. In the end, organizations are armed with the information they need to proactively grant and remove access to various files and folders within their production environments. By ensuring proper and limited access is provided, organizations can proactively minimize the impact of an attack—should it occur through compromised credentials.

SUMMARY

User Access enables proactive data risk management by providing visibility into sensitive data access, calculating risk, and tracking changes to the data and associated risk over time. Using analytics, User Access will identify and rank the users and groups who have access to sensitive data, to enable administrators to take appropriate measures to protect their sensitive data. The entire process of scanning for sensitive data and determining user access will happen on your backup data, essentially, the catalog of your entire environment—requiring no heavy-duty agents, no impact on production. Remember, you wouldn't leave your valuables sitting out on your front porch accessible to the world, so why would you leave your data unattended?

rubrik

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

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