**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. 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.

**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.
Rubrik is on a mission to secure the world’s data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit [www.rubrik.com](http://www.rubrik.com) and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

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.

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?