Pitfall5: Failure to prioritize and leverage data activity monitoring

Bookmark this page

Monitoring data access and use is an essential part of any data security strategy. An organization leader needs to know who, how and when people are accessing data. This monitoring should encompass whether these people should have access, if that access level is correct and if it represents an elevated risk for the enterprise.

Privileged user identifications are common culprits in insider threats.5 A data protection plan should include real-time monitoring to detect privileged user accounts being used for suspicious or unauthorized activities. To prevent possible malicious activity, a solution must perform the following tasks:

- Block and quarantine suspicious activity based on policy violations.
- Suspend or shut down sessions based on anomalous behaviour.
- Use predefined regulation-specific workflows across data environments.
- Send actionable alerts to IT security and operations systems.

Accounting for data security and compliance related information and knowing when and how to respond to potential threats can be difficult. With authorized users accessing multiple data sources, including databases, file systems, mainframe environments and cloud environments, monitoring and saving data from all these interactions can seem overwhelming. The challenge lies in effectively monitoring, capturing, filtering, processing and responding to a huge volume of data activity. Without a proper plan in place, your organization can have more activity information than it can reasonably process and, in turn, diminish the value of data activity monitoring.

Solution: Develop a comprehensive data detection and protection strategy

To that end, when starting on a data security journey, you need to size and scope your monitoring efforts to properly address the requirements and risks. This activity often involves adopting a phased approach that enables development and scaling best practices across your enterprise. Moreover, it’s critical to have conversations with key business and IT stakeholders early in the process to understand short-term and long-term business objectives.

These conversations should also capture the technology that will be required to support their key initiatives. For instance, if the business is planning to set up offices in a new geography using a mix of on-premises and cloud-hosted data repositories, your data security strategy should assess how that plan will impact the organization’s data security and compliance posture. If, for example, the companyowned data will now be subject to new data security and compliance requirements, such as the GDPR, California Consumer Privacy Act (CCPA), Brazil's Lei Geral de Proteção de Dados (LGPD) and so on.

You should also prioritize and focus on one or two sources that likely have the most sensitive data. Make sure your data security policies are clear and detailed for these sources before extending these practices to the rest of your infrastructure.

You should look for an automated data or file activity monitoring solution with rich analytics that can focus on key risks and unusual behaviors by privileged users. Although it’s essential to receive automated alerts when a data or file activity monitoring solution detects abnormal behavior, you must also be able to take fast action when anomalies or deviations from your data access policies are discovered. Protection actions should include dynamic data masking or blocking.

As you develop your data activity monitoring and protection plans, it’s often helpful to consider the following questions:

- What are my top two most sensitive data sources?
- Which five to ten data sources should I prioritize next, based on their volume of sensitive data?
- Are certain endpoints or cloud assets associated with higher-risk data?
- Is sensitive data freely moving to and from on-premises, hybrid and cloud environments?
- Which users should be granted access to the data source and under what conditions?
- What high-risk users or privileged accounts need to be turned off or require closer scrutiny?
- Does my data security solution support real-time activity monitoring and automated data protection capabilities?
- Is real-time monitoring in place to track data in files residing in data stores, such as Structured Query Language (SQL) databases, Hadoop distributions, Not only SQL (NoSQL) platforms and so on.
- Does my monitoring solution account for data stores spanning hybrid multicloud environments and allow me to generate customized reports that go to the right people at the right time?
- Do I have the risk analytics and filtered monitoring capabilities needed to effectively prioritize risk, vulnerabilities and remediation efforts?

The more specific you can be about monitoring priorities and protection requirements, the more effective the solution will

‹ Previous

Next ›