COHESITY

TIPSHEET

3 Reasons why Data Governance is Key In Your Battle Against Cyber Criminals

Overview

What is important to an organizations' bottom line? Customers, reputation, innovation, the list goes on. But what about data? Data is the lifeblood of businesses worldwide, as more data needs to be managed and secured every day. As more data breaches and cyber attacks impact businesses world-wide while at the same time more data privacy mandates are enacted, the ability to govern and manage sensitive data becomes both more challenging and more important. Now is the time to reduce the risk of hefty compliance fines while simultaneously guarding against data breaches and cyber attacks. Organizations need a governance solution that provides visibility into sensitive data and user access patterns, reduces the risks of non-compliance, and mitigates the threat of ransomware and unauthorized data usage.

In this tip sheet, we will discuss the three ways data governance is key to an organizations' data management strategy. Let's take a look.

Realize Value with Cohesity

- It is estimated that a ransomware attack will occur every 11 seconds
- Roughly 81% of attacks involve data theft and exfiltration

1. Ransomware Is Getting More Sophisticated

Ransomware and cyber attacks are no longer matter of if, but of when. In fact, it is estimated that a ransomware attack will occur every 11 seconds[1]. These attacks have been making headlines in recent years, with organizations worldwide having to pay millions of dollars, often directly to hackers to restore data and application access. And they haven't stopped there. These days roughly 81% of attacks involve data theft and exfiltration[2]. Where in this case, the ransom demand is made to stop criminals from exposing your data online or selling it on the dark web.

Many organizations also face the challenge of detecting abnormal activities initiated from the inside, such as unauthorized data downloads and either malicious or unintentional sharing, leaving them once again in a vulnerable situation. And, the time lapses between detection and remediation can have a devastating impact.

[1] Robb, Brenda. "The State of Ransomware in 2020." BlackFog, 26 Aug. 20211.

[2] Sobers, Rob. "81 Ransomware Statistics, Data, Trends and Facts for 2021 | Varonis." Inside Out Security, 7 July 2021, www.varonis.com/blog/ransomware-statistics-2021.

To avoid these risks, businesses need to implement a governance solution that monitors access privileges to data and ensures sensitive data does not get into the wrong hands. The right solution will use machine learning to first more accurately find and classify sensitive data and subsequently be able to match it against abnormal and risky user behaviors that can be indications of an insider threat or data exfiltration from ransomware.

2. Out of Sight, Out of Mind

Organizations are producing more data than even before. And as more data is produced, more dark data is being siloed throughout the IT infrastructure - across data center, cloud and edge environments. Much of this can end up as so-called "dark data" - where once created, it often sits idle and rarely gets re-used for additional value, but worse it can be a target for cyber criminals. This is especially true as some of this data often includes customer data or other sensitive information that has to be properly recorded and stored for regulatory purposes.

In the event of a compliance or regulatory investigation, businesses are often unable to find or report on all the data they need to to meet these requirements. In order to effectively protect and efficiently manage data, organizations need to ensure data governance and data security are more intertwined as part of their broader data management strategy. The right solution should be able to identify sensitive or at-risk data through a policy-based approach, appropriately classify it through the use of machine learning (ML), alert IT staff when an anomaly is detected, while leveraging artificial intelligence (AI) to detect risks of overexposure based on the content, location, user and access pattern behaviors.

3.Always More Rules to Follow

From GDPR, to HIPAA and PCI compliance, there are more and more regulatory mandates that need to be met. Just last year, it has been reported that there were 257 average daily alerts for regulatory events across 190 countries[3]. If a business is found to be out of compliance, they may face substantial fines and even lose loyal customers. And, it is not just misplaced or lost data that is the problem. Sensitive data needs to be safeguarded from loss, theft, corruption and misuse—such as from ransomware.

To combat these risks, businesses need a solution that can provide effective compliance policy monitoring. A governance solution will enable businesses to detect risky events and activities through custom policies and identify user access patterns on sensitive information. The goal is to enable organizations to promptly detect activities, such as sharing or downloading sensitive data, allowing them to take the necessary steps for remediation to ensure compliance.

Conclusion

Now is the time to protect what matters most to your business - your data. With Cohesity DataGovern, organizations can take advantage of AI-powered governance and anomaly detection for your enterprise's most sensitive data. It enables you to accurately discover sensitive data, meet compliance requirements, and respond quickly to ransomware and other cyber threats, all delivered as a simple to consume Software as a Service (SaaS) offer to reduce operational cost and complexity.

[3] Thomson Reuters Legal. "The Cost of Compliance 2021: Shaping the Future." Thomson Reuters Legal, 2021.

Register for our webinar to learn more today

COHESITY