Pitfall 2: Failure to recognize the need for centralized data security

Bookmark this page

Without broader compliance mandates that cover data privacy and security, organization leaders can lose sight of the need for consistent, enterprise-wide data security.

For enterprises with hybrid multicloud environments, which constantly change and grow, new types of data sources can appear weekly or daily and greatly disperse sensitive data.

Leaders of companies that are growing and expanding their IT infrastructures can fail to recognize the risk that their changing attack surface poses. They can lack adequate visibility and control as their sensitive data moves around an increasingly complex and disparate IT environment. Failure to adopt end-to-end data privacy, security and protection controls—especially within complex environments—can prove to be a very costly oversight.

Operating security solutions in silos can cause additional problems. For example, organizations with a security operations centre (SOC) and security information and event management (SIEM) solution can neglect to feed those systems with insights gleaned from their data security solution. Likewise, a lack of interoperability between security people, processes and tools can hinder the success of any security program

Solution: Know where your sensitive data resides, including on-premises and cloudhosted repositories

Securing sensitive data should occur in conjunction with your broader security efforts. In addition to understanding where your sensitive data is stored, you need to know when and how it's being accessed, as well—even as this information rapidly changes. Additionally, you should work to integrate data security and protection insights and policies with your overall security program to enable tightly aligned communication between technologies. A data security solution that operates across disparate environments and platforms can help in this process.

So, when is the right time to integrate data security with other security controls as part of a more holistic security practice? Here are a few signs that suggest your organization may be ready to take this next step:

- Risk of losing valuable data: The value of your organization's personal, sensitive and proprietary data is so significant that its loss would cause significant damage to the viability of your business.
- Regulatory implications: Your organization collects and stores data with legal requirements, such as credit card numbers, other payment information or personal data
- Lack of security oversight: Your organization has grown to a point where it's difficult to track and secure all the network endpoints, including cloud instances. For example, do you have a clear idea of where, when and how data is being stored, shared and accessed across your on-premises and cloud data stores?
- Inadequate assessment: Your organization has adopted a fragmented approach where no clear understanding exists of exactly what's being spent across all your security activities. For example, do you have processes in place to measure accurately your return on investment (ROI) in terms of the resources being allocated to reduce data security risk?

If any of these situations apply to your organization, you should consider acquiring the security skills and solutions needed to integrate data security into your broader existing security practice.

© All Rights Reserved