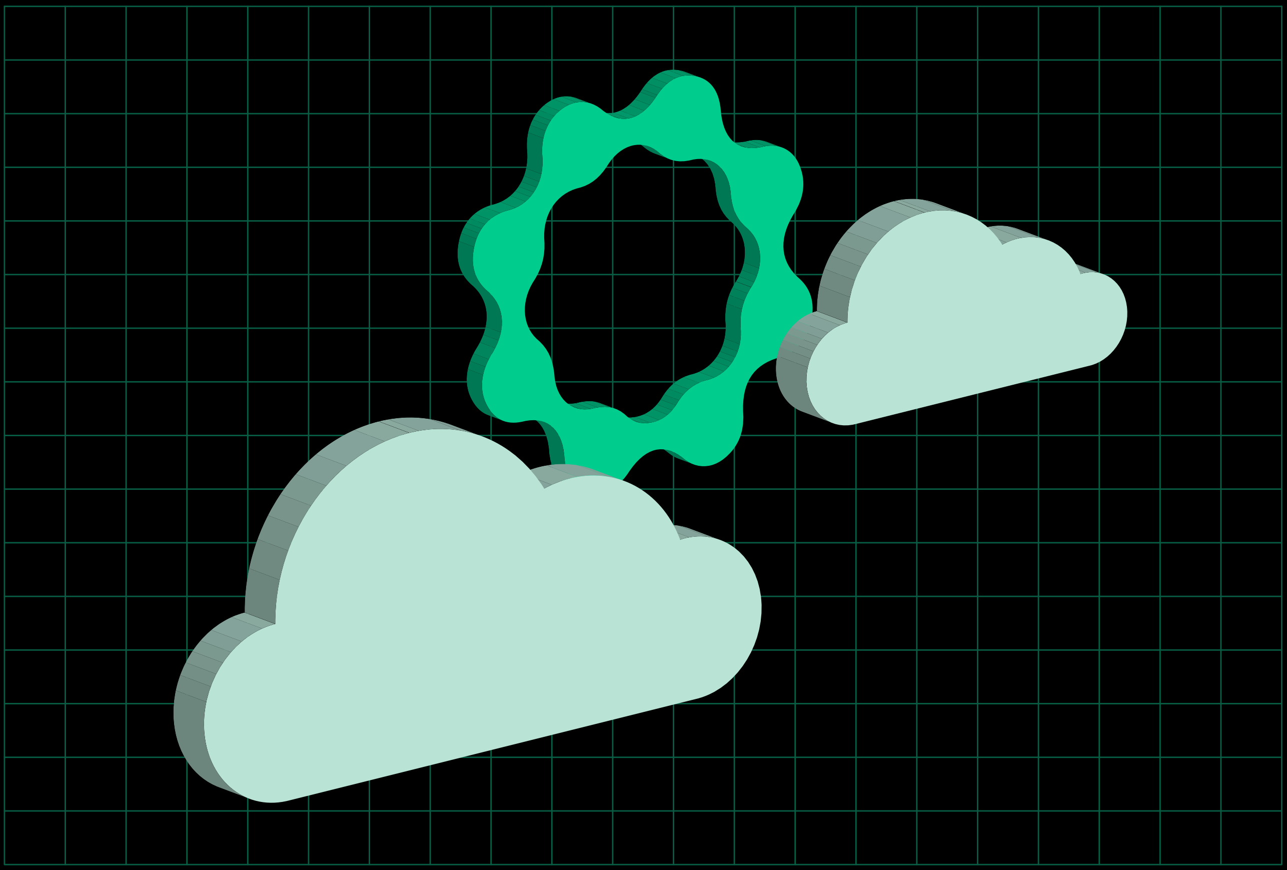
cyera

CLEARING UP THE CLOUDS

Turning Cloud Data Security Risk Into Business Opportunity

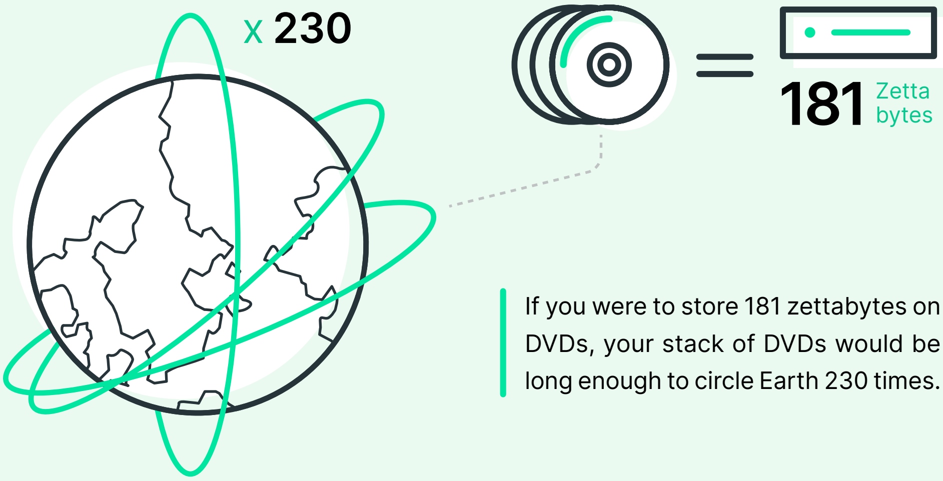


info@cyera.io | cyera.io

Improving customer engagement. Increasing insight. Accelerating innovation and time to value. Simplifying operations. These are just a few of the benefits that organizations hope to capitalize upon as they increasingly move data to the cloud.

And there's no question that organizations are doing just that – so much so that by 2025, 95 percent of new digital workloads will be deployed on cloud-native platforms, up from just 30 percent in 2021. Practically speaking, organizations need the cloud to store the massive amounts of data that are created each day. In 2022 alone, 97 zettabytes of data will be created, and that figure is expected to grow 87 percent to 181 zettabytes by 2025.

But the growing dependence upon the cloud isn't without its challenges. Organizations now are struggling to balance the benefits they're striving to attain from the cloud against the issues the cloud creates in terms of compliance and security. The clearest example of this is the astronomical increase in data breaches in recent years.



If you were to store 181 zettabytes on DVDs, your stack of DVDs would be long enough to circle Earth 230 times.

In 2021 alone, there were more than 4,100 publicly disclosed data breaches, and adversaries continue to strengthen and improve attack methods, which include utilizing cryptocurrency mining abuse, phishing campaigns, ransomware, supply chain attacks, and more. Likewise, attackers increasingly target personal data stored by companies, including names, birthdates, Social Security numbers, physical and email addresses, credit card, and other payment information, all of which has led to more stringent legislation and requirements to control how data is stored.

> *Organizations face challenges mitigating data security and privacy risks as data rapidly proliferates across multi-cloud and hybrid IT architectures. Identifying meaningful data risk is impossible to solve without combining metrics from data sensitivity, data lineage, infrastructure configurations that create data risks, and access risk into a common view. This is an urgent problem that is encouraging rapid growth in the availability and maturation of this technology.*
>
> Brian Lowans, Gartner Hype Cycle For Data Security 2022
>
> Gartner

Moreover, attacks are being launched more quickly and effectively every day. In 2021, Google Cloud found it took only 30 minutes for a compromise to occur when a vulnerable cloud instance was exposed to the internet. More recent research from Bishop Fox highlights that nearly 64% of hackers were able to collect and potentially exfiltrate data within a 5 hour window. All of these factors coalesce to drive up the cost of a data breach, which reached an average of $4.2 million in 2021.

Meanwhile, security professionals are faced with a growing list of responsibilities and challenges they must address to ensure governance and security requirements are met – things like ensuring resiliency and business continuity, cutting costs, finding skilled labor, and protecting vast amounts of stored data.

Challenges Security Teams Face Protecting Data

Despite the imperative that security professionals have to protect data, they face numerous challenges that make doing so more difficult, including:

Lack of Visibility:

Organizations create, collect, and store vast amounts of data that often becomes siloed within various business units. Likewise, applications and products are notorious for collecting data in silos. As a result, security and risk teams don't have the visibility they need to manage or understand data consistently. This makes it challenging to create effective policies for security leaders to implement at scale in the organization; reactive measures based on alerts, legislation, zero-day threats, critical vulnerabilities, and attacks keep security teams busy playing whack-a-mole with sprawling security challenges. This lack of visibility isn't just inconvenient – it's dangerous. You can't protect what you can't see. A class action lawsuit was filed against mobile payments company Cash App, and its parent Block, for "negligent" behavior that led to the personal information of 8.2 million users being compromised. The breach was the result of an ex-employee who still had access to reports that contained the full names and brokerage account numbers. This access was permissible during the employee's tenure with Cash App, however security measures should have detected that the user's permissions still existed after their termination, and that the user's credentials were being used to access sensitive information.

Failure to Adopt a Data-Centric Security Architecture:

Security teams often prioritize security measures from the infrastructure to the application to the user, which creates data security challenges as they attempt to secure each layer of data individually. As such, the context of the data controls are lost in translation. Data is the lifeblood of any business - it informs strategic business decisions, customer

Continue →

support initiatives, development priorities, and investment scenarios. In some cases, data is the primary interface between the value-creating elements of the business (customers, partners, business units) and must be strongly protected. In others, it must be easily accessible (for instance, product or service information that is available for download on a corporate website as a demand generation vehicle). Cyberattackers weaponize infrastructure misconfigurations, application vulnerabilities, and overly permissive access to compromise defenses. And they have been remarkably successful, which has led to the bulk of regulatory and compliance rules that aim to protect data. By adopting a data-centric security architecture, security leaders can basically flip the pyramid right-side up, making data the top security priority, and in so doing better align to business partners.

Shadow IT:

Although it's not a new concept, shadow IT is coming under increased scrutiny as organizations prioritize improving their overall security posture. While there once was a sort of "wink-wink-nudge-nudge, say no more" mentality about people using technology, software, applications, and devices outside of the formal control or governance of the security department, most businesses are rightfully abandoning that policy. The permissive nature of the cloud - across IaaS, PaaS, and SaaS - has led to incredible sprawl. Not doing so places an organization at greater risk of attack and increases fines associated with governance, risk, and compliance (GRC), as well as massive losses related to cyberattacks.

Data Leakage:

Not only do security professionals lack clarity about what data actually exists, they lack visibility into where data is being created and context on how and why it's being accessed and shared. The tools that most security teams leverage are data blind - they lack focus and context on the data. That in turn blinds security teams to the point that they don't know what a given data store contains, the purpose of the data, whether it is sensitive, who should have access or is accessing it, or where the data is or should be going. This lack of clarity can leave security

Continue →

professionals feeling overwhelmed. Their tools create hundreds of alerts that lack any context or visibility into the data. They recognize that any action could create a cascade of other issues, while also understanding that their role is to act in a manner that protects the business. It's like they're in a constant state of plugging one or two holes in the dam, even as three or four others spring a leak.

Unclear and/or Complicated IT and Security Team Structure:

Security and IT teams are being pulled in three primary directions: enabling the business, driving efficiency, and reducing the threat surface. From an academic perspective, that list is prioritized in order of importance. However, in reality, the list is often addressed in reverse order due to the way in which vendors market their solutions, as well as by the fact that many security professionals are forced to procure solutions based on business objectives and the projects prioritized by executive leadership for the CISO. So while it's easy to understand the prioritization of these goals, it's generally not as easy to ascertain which teams are responsible for ensuring they are met. In many cases, it's difficult to even identify the person ultimately responsible for the protection of an organization's data. The result is that security teams are left to react to external threats, compliance requirements, and privacy audits, while they fail to make progress toward efficiency and business enablement goals.

Tool Sprawl:

Today's security teams use on average between 55 and 75 security products or applications – and more are added each day. That means dozens of management consoles, onboarding and training programs, and employee up-skilling requirements. Moreover, each tool is further complicated by its deployment requirements – for instance, whether it's deployed on-prem or in the cloud and what permissions are used for each deployment scenario. Capabilities tend to overlap, but integrations are sparse, leaving gaps in the security team's ability to approach that "single pane of glass" espoused by analysts. This battle of the "unknown unknowns" is a growing problem for all security and IT teams.

Weaknesses in Existing Cloud Data Security Tools:

For the past several years, organizations have increasingly adopted data loss prevention (DLP) and data detection and response (DDR) tools in an effort to better understand where their data is, what it contains, and its security posture. But instead of simplifying the data security process, DLP and DDR solutions often add additional layers of complication and don’t provide full visibility into data stores. For instance, such solutions often claim to perform automatic discovery and classification of data; however, they lack the intelligence to distinguish between similar data sets – say between a personal ID number and a Social Security number. The result is that security and IT teams often are forced to revert to manual processes for corrections. Additionally, unrealistic claims of real-time detection or any actual preventative measures have left security teams skeptical and cynical that any tool exists for improving their security postures.

Critical Questions Organizations Should Address to Improve Cloud Data Security

To overcome these challenges, organizations should utilize data security posture management (DSPM), which provides visibility into where sensitive data is located, who can access that data, how the data has been used, and what the security posture is for the data store or application.

> “Data security posture management provides visibility as to where sensitive data is, who has access to that data, how it has been used and what the security posture of the data store or application is. In simple terms, DSPM vendors and products provide “data discovery+” — that is, in-depth data discovery plus varying combinations of data observability features. Such features may include real-time visibility into data flows, risk and compliance with data security controls. The objective is to identify security gaps and undue exposure. DSPM accelerates assessments of how data security posture can be enforced through complementary data security controls.
>
> Recently, the market for data discovery and classification tools underwent two important changes:
>
> 1. There is now a specific and growing market for privacy management and data tracking that includes classification capabilities that specifically discover, for example, personally identifiable information (PII) as a category.
>
> 2. Vendors are now looking to move away from algorithmically pattern matching and are adding AI- and ML-based capabilities with semantic capabilities that can be used to find out what something means. For example, the number 72 could be a house number, a temperature — almost anything. You can hardly find out what something is when a product is limited to pattern matching for discovery and classification.”

Brian Lowans, Gartner Hype Cycle For Data Security 2022

Gartner

DSPM Solutions Should Answer Three Fundamental Questions:

1. Where is your sensitive data?
2. Do you know if your sensitive data is at risk?
3. How can you take action to remediate that risk?

In answering these questions, security teams can engage business stakeholders to understand:

❑ **How does each business unit use the cloud (across IaaS, PaaS, and SaaS platforms) today, and their plans to expand that use in the future?**

❑ **How is the business managing cloud data today?**

↳ Do you have a process for maintaining an inventory of all of your cloud data?

↳ Does your cloud data fall within the scope of any compliance or regulatory controls today?

↳ If yes, which compliance and regulatory controls apply?

❑ **Where do you currently manage sensitive data? Do you have a detailed understanding of where you manage customer, partner, employee, or intellectual property data?**

↳ How is that data governed today?

↳ Does your team manage the access, localization, or data lifecycle of all data?

❑ **Do any of your current security tools maintain context on your data, and protect the data directly?**

↳ How are you using those solution(s) to address cloud data?

↳ If you use cloud-native solutions like security posture management (CSPM), or application protection platforms (CNAPP) how do you manage infrastructure configurations for sensitive data specifically?

↳ Have you noticed discrepancies or gaps between what the solution(s) shows you regarding structured and unstructured data, sensitive information, policy violations, or compliance concerns?

What to Look for in a DSPM Solution:

Not all DSPM solutions are created equally. An emerging technology in the data security space, DSPM enables many organizations to solve data security and privacy concerns, but they aren't fully aware of what to look for when selecting a solution. A top-tier DSPM solution will perform a number of functions, including:

Continuous discovery and classification:

DSPM solutions should continuously discover and classify all cloud data stores, sensitive data, and user roles. Agentless technology should automatically provide a comprehensive view of data and data stores in any cloud, container, or serverless environment.

Understand and classify data:

Such solutions also should determine the types of data that exist and provide security teams with graph-based data analysis using highly accurate, context-aware risk assessment of cloud data. Data should be classified based on sensitivity, volume, and regulatory or compliance exposure. Personally identifiable information (PII) should automatically create a dynamic sensitive-data inventory. Importantly, DSPM should automatically incorporate machine learning (ML) models to adjust and fine-tune classifications according to an organization's unique environment. Once an inventory is established, each data class should then be assigned a risk-based classification based on the context of privacy or regulatory risk it represents. Likewise, it should support a constantly expanding inventory of PII data classes as it scans the organization's environment.

Support multiple identifiers:

DSPM should identify data based on a number of factors, including:

- Is data public or internal?
- Is data sensitive, public, internal, personal sensitive, or non-personal but sensitive?
- Is data financial, technical, operational, or marketing?

Replace manually created inventories:
Instead of relying on inventories that are created by hand, DSPM solutions should provide automatic creation of personal data inventories across all cloud data stores, regardless of how the data store is deployed, discovered, classified, or categorized.

Protect and/or guided remediation:

DSPM solutions also should provide options for remediation, enabling security teams to quickly ascertain how they can protect vulnerable data, how policies can be applied against it, and what identities need to be managed.

About Cyera

Cyera is the cloud data security and privacy company that gives businesses context and control over their cloud data. The company's mission is to empower its customers to enable innovation, securely. As the industry's most advanced cloud data protection platform, Cyera instantly provides companies a strong baseline for all security, risk management, privacy, and compliance efforts and ensures the entire organization operates with the same policies and guardrails. Backed by leading investors including Sequoia, Accel, and Cyberstarts, Cyera is defining the way companies do cloud data security. To learn more, visit www.cyera.io.