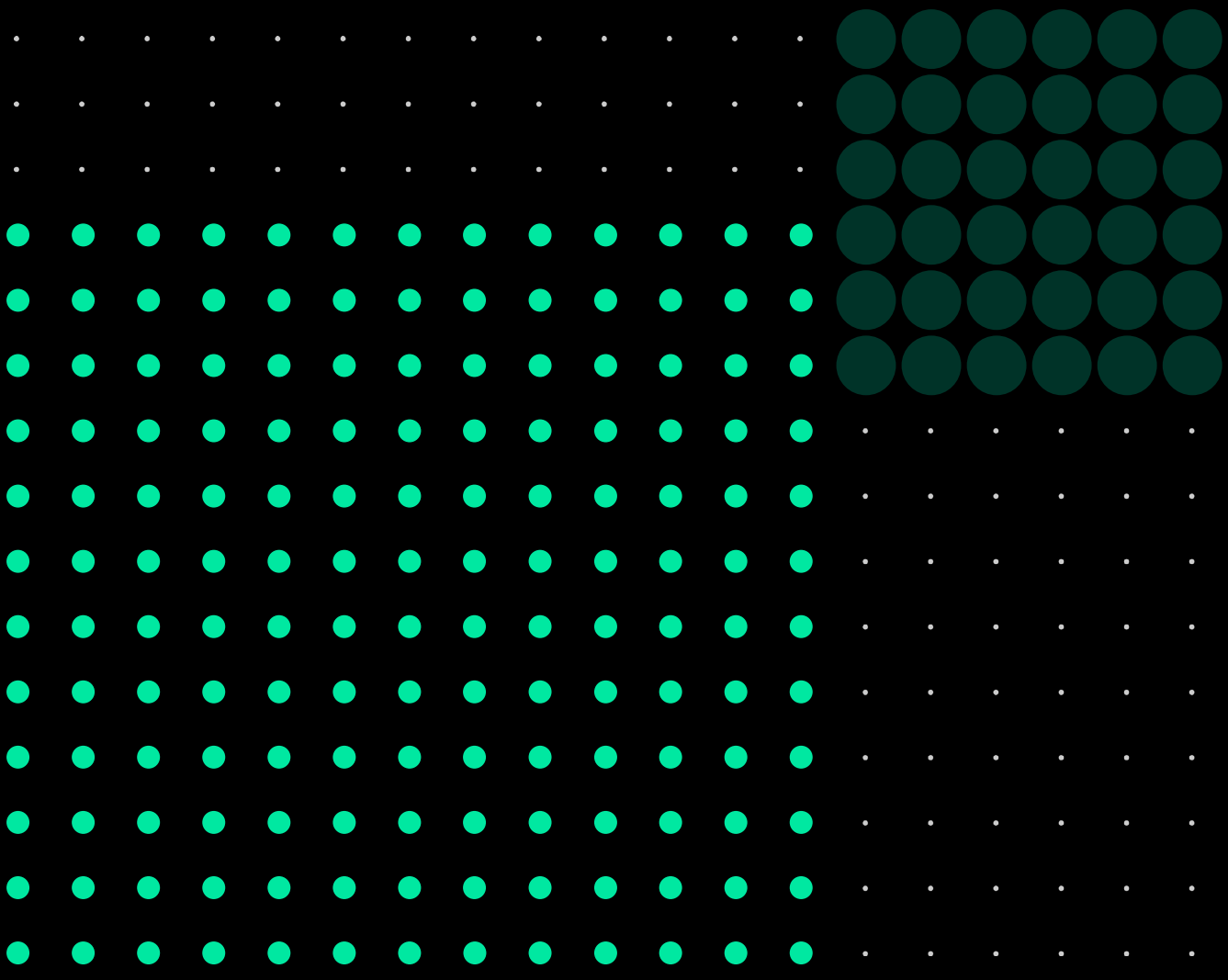
cyera

Cloud Cost Optimization Guide

How CISOs are Reducing Costs
While Improving Data Defense



info@cyera.io | cyera.io

EXECUTIVE SUMMARY

CISOs must balance the competing demands of improving security, while also consolidating resources. This task is made all the more challenging by business growth which can expand attack surfaces.

By most accounts, we're headed into (or are already in) a global recession. For chief information security officers (CISOs), that means prioritizing finding credible cost savings, while still protecting the organization against attacks and vulnerabilities. CISOs must balance the competing demands of improving security, while also consolidating resources. This task is made all the more challenging by business growth which can expand attack surfaces.

In this paper, we will look at how cloud optimization can reduce costs while improving security and compliance, including:

- **What's at Risk** - As cloud adoption grows, so too does the volume of data, introducing the risk of security vulnerability and an added cost around managing this sprawling data.
- **Balancing Business Opportunity, Cyber-Resilience, and Cost** - While the steady shift to cloud services is opening the door to significant new business opportunities, these services require continuous optimization to deliver benefits cost-effectively.
- **Data Minimization to Optimize Storage Costs** - Reducing data overconsumption and storage costs is an effective means of reducing security risk and containing cloud costs. Organizations can benefit by discovering, understanding, and eliminating unused data that includes stale data, ghost data, and copy data.
- **Minimize Overlap in Tool Capabilities** - Many organizations rely on multi-cloud infrastructures, which leaves them a wealth of tools with overlapping capabilities provided by different vendors. Security teams should look at tools based on what the business is trying to achieve and find the best capabilities to meet that need.
- **Improve Employee Efficiency to Optimize Productivity Costs** - One of the keys to achieving cost savings is enhancing employee efficiency. Managing data more effectively is essential for optimizing production costs and achieving the fundamental goal of lowering security risk.

How Cloud Optimization Can Reduce Costs While Improving Security and Compliance

CISOs will want to focus on enabling the business to be agile, while achieving least-privileged access to sensitive data and workloads.

Gartner's 2022 Top Trends in Cybersecurity points to attack surface expansion and vendor consolidation as two key industry trends. With enterprise attack surfaces multiplying, the report states, "organizations must look beyond traditional approaches to security monitoring, detection, and response to manage a wider set of security exposures."[1]

Gartner highlights the ongoing convergence of security technology, which is aimed at reducing complexity and lowering administrative overhead. The report predicts, "consolidation of security functions will lower total cost of ownership and improve operational efficiency in the long term, leading to better overall security."[2]

Clearly, these two trends will influence how organizations evaluate their upcoming security investments. At the same time, security leaders will need to ensure that any consolidation program they engage in does not conflict with risk-reduction objectives. CISOs will want to focus on enabling the business to be agile, while achieving least-privileged access to sensitive data and workloads.

What's at Risk?

Worldwide end-user spending on public cloud services is expected to reach nearly $600 billion by 2023.

Gartner

Businesses have moved boldly to adopt cloud services to better engage customers and improve the quality of service, as well as to create new revenue streams and opportunities for the business. According to Gartner, worldwide end-user spending on public cloud services is expected to reach nearly $600 billion by 2023.[3]

As cloud adoption grows, so too does the risk of that data producing both a security vulnerability and an added cost around managing sprawling data. This comes at a time when IT organizations are increasingly cost-conscious and under pressure to do more with less. These dynamics have created an impetus for CISOs and other C-suite stakeholders to work together to drive efficiency that will have a meaningful business impact in the years to come.

The ever-present concern for security professionals is balancing the need to expand cloud services while reducing risk to the organization. A PWC report found that fewer than 40 percent of executives surveyed indicated they have fully mitigated the risks their bold moves incurred.[4] The good news is that more than 70 percent of senior executives saw improvements in cybersecurity last year — thanks to increased investments and greater cooperation from the C-suite. That said, the key is to find ways to achieve such results while still containing costs.

[1] https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

[2] https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

[3] https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

[4] https://www.pwc.com/dti

Balancing Business Opportunity, Cyber-Resilience, and Cost

Today, every business must balance business opportunity, cyber-resilience, and cost optimization - there is no opportunity to compromise on any of these three imperatives. While the steady shift to cloud services is opening the door to significant new business opportunities, these services require continuous optimization to deliver benefits cost-effectively.

Building and maintaining trust with customers, and complying with regulations focused on data protection and stewardship are critical to enable any business. And with the consistent threats posed by malicious actors who use an increasingly diverse and sophisticated set of tools, cyber-resilience is a top priority for every business. A recent report[6] highlighted that emerging tech creates privacy concerns for organizations centered around cloud adoption and data. Minimizing the threat surface, in part by focusing on data minimization, is a good step toward addressing those concerns because precursors to effective data minimization are effective discovery and classification to gain an understanding of what data a company is managing, and what it represents.

Cost benefits have been an important driver of cloud adoption programs. A 2020 Gartner Public Cloud Initiatives study reported a large consensus on the expectations that cloud adoption would reduce operating costs. The key to achieving cost efficiency is proper optimization. Organizations that fail to prioritize cost optimization planning end up overspending on cloud services by up to 70 percent without deriving the expected value from it.[7]

Conversely, data optimization solutions can deliver rapid return on investment. According to a Forrester report, hard savings from an effective data optimization solution can result in a 30 percent decrease in cloud spending upon initial implementation and ongoing savings of 15 percent.[8]

Emerging tech creates privacy concerns for organizations centered around cloud adoption and data. Minimizing the threat surface, in part by focusing on data minimization, is a good step toward addressing those concerns.

Savings from an effective data optimization solution can result in a 30 percent decrease in cloud spending upon initial implementation and ongoing savings of 15 percent.

FORRESTER®

[5] https://www.pwc.com/dti?WT.mc_id=CT3-PL300-DM1-TR1-LS2-ND30-PR5-CN_DTICyber-globaldti&gclid=CjwKCAjw7p6aBhBiEiwA83fGusUIPZ98UddW91pgJoshP7C1DUgPKMEXGViyuu2UkhdXLgx4HuGTcxoCDDMQAvD_BwE&gclsrc=aw.ds

[6] The State Of Privacy And Cybersecurity, 2022", Forrester, September 8, 2022

[7] https://www.govtech.com/sponsored/capitalize-on-the-cloud-without-overspending

[8] Forrester report, "Top 10 Facts Tech Leaders Should Know About Cloud Cost Optimization"

Focus on Data Minimization to Optimize Storage Costs

CISOs understand the importance of data minimization as a key security activity. EU General Data Protection Regulations (GDPR) point out that data minimization efforts should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. GDPR dictates that data should only be retained for as long as is necessary to fulfill that purpose. At the same time, data minimization is also vital to optimizing costs.

Because cloud resources are priced by consumption, this means that as data in the cloud delivers important business value, it also has built-in costs, particularly when it comes to storage. That is why reducing data overconsumption and storage costs is an effective means of containing cloud costs.

To combat overconsumption, and thus lower cloud expenditures, organizations can benefit by discovering, understanding, and eliminating data that is no longer being used. Gaining a deep level of insight into the data being stored is instrumental for empowering measures to mitigate storage and reduce risk.

The first step in evaluating stored data is recognizing it can take different forms. Unused data falls into three categories: Stale data (that which is no longer accessed), ghost data (where the original data no longer exists), and copy data (data that is duplicated, typically without business justification):

Identify Stale Data

It has been reported that more than 50 percent of an average company's data is stale, and that 85 percent of organizations have aggregated more than 100,000 folders filled with stale data.[9] This suggests the scope of the problem is real and significant.

To identify stale data, businesses need to maintain an up-to-date data inventory, as well as fully understand the lifecycle of their data. The key is to be able to articulate why stored data is no longer accessed. If there is no business processing purpose, then the data represents a compliance risk, especially if it contains PCI, PHI, or PII. In cases where it is PII, then it also represents a privacy risk.

Cost-saving measures are directly related to the need for reducing security exposure. The incidence of stale data reveals that an organization is not securing data as effectively as it does actively used, production/business-critical data, which has the net effect of exposing the business to cyber-resilience risk. Stale data can be an

9 https://ghostvolt.com/blog/Stale-Data-Your-Invisibe-Cyber-Security-Threat.html

easy target for phishing, ransomware, or other external entities looking to compromise weak/non-existent defenses in an attempt to steal sensitive data.

This highlights the importance of having security teams examine backup and recovery strategies to see how sensitive data is being stored. Teams will have to balance the priorities of different technology stakeholders. In the case of developers, there is a need to copy production databases to build the next versions of an application, but it remains incumbent on security teams to minimize risk throughout cloud environments. This requires conducting data cleansing exercises that remove customer data either by eliminating it or by obfuscating or tokenizing it so developers don't have access to sensitive data. Such exercises reduce the risk of data loss, accidental misuse, or data leakage in a less secure production environment.

The key to identifying stale data is comprehensive visibility into data changes, data access, and data usage within the cloud. Effectively identifying stale data is an important first step in reducing compliance risk, as well as reducing costs.

Find Ghost Data to Stay Compliant

The second form of unused data is ghost data. Ghost data represents a similar cost challenge and security risk for most organizations. In a recent study, Cyera found that over 30 percent of customer cloud data stores were ghost data.[10] Of the ghost data uncovered, more than 56 percent was determined to contain sensitive or very sensitive data.[11]

Having sensitive or very sensitive data in a ghost data store can represent several cyber-resilience challenges including exposing that data to misuse, insider threats, and ransomware. By definition, ghost data is not actively managed by the business, which means it likely is not actively being safeguarded by security controls. When sensitive or very sensitive data is left outside the bounds of a security program, it is more vulnerable to threats, and worse, can be compromised without any monitoring or alerting in place to notify the business that there has been a breach.

Adding to the challenge faced by security professionals, large stockpiles of ghost data tend to be difficult to identify, protect, organize, and manage, making compliance more complicated. GDPR statutes require that enterprises practice data protection principles, such as data minimization. These regulations state that if an organization no longer has a business justification for managing data, such as ghost data, that

10, 11 https://www.prnewswire.com/il/news-releases/cyera-finds-ghost-data-expands-threat-surface-making-businesses-more-vulnerable-to-ransomware-attacks-compliance-violations-301602192.html

data should be eliminated. Failure to do so could subject the business to a fine.

This puts the onus on security teams to develop effective methods of keeping track of where ghost data resides to empower teams to minimize and eliminate it. Armed with the necessary insights, teams are better equipped to make proper decisions, allowing the organization to stay compliant and avoid costly penalties. And with data minimization comes highly desirable cost savings, as well.

Eliminate Copy Data Safely

The third form of unused data is copy data. Backups are vital for ensuring data resilience and business continuity, but they also end up generating copy data, which adds to data storage costs. Unneeded copies often persist due to a lack of visibility and clear governance policies. Security teams need to have a full understanding of copy data to eliminate it safely.

To mitigate copy data, businesses must first recognize the rate of change in their data. The more frequently data is changed, the more often backups will be generated. Also, organizations should take into consideration high availability and disaster recovery processes. Data must be maintained to ensure business continuity in the event of a bug, attack, or outage. Further complicating the job of minimizing copy data are legislative and regulatory requirements that stipulate how long data must be retained.

Maintaining an accurate data inventory is key to compliance with GDPR, as well as industry-specific regulations, such as HIPAA, PCI DSS, and the Sarbanes-Oxley Act. Armed with such an inventory, organizations can determine how often to take snapshots, how long to keep them, and when they should be kept in active storage versus archives (e.g. AWS Glacier).

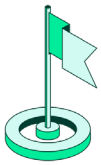
When stale data, ghost data, and copy data are properly identified, organizations are better equipped to right-size storage environments, achieving data minimization, thus reducing security risk and costs.

Minimize Overlap in Tool Capabilities to Optimize Technology Costs

Taking a closer look at tool capabilities is another area that can reveal opportunities to reduce data risk and lower costs.

Cloud environments prize interoperability, thus allowing businesses to leverage technologies that will improve time-to-market, operating efficiency, and value. Because many organizations rely on multi-cloud infrastructures, vendors tend to sell tools based on categories of technology or functionality, such as data loss prevention, data governance, and data privacy. This leaves security leaders with a wealth of tools with overlapping capabilities which attack similar problems, but from slightly different vantage points – thereby creating a less-than-efficient scenario.

Instead of this more costly approach, security teams should look at tools based on what the business is trying to achieve and find the best capabilities to meet that need. The following factors should be considered:



Data Discovery and Classification

Most data discovery tools require users to know where their data resides before they can classify and protect it. This is because most solutions require either self-attestation or manual connections to be established and maintained to "discover" the data. Having a solution that can truly uncover unknown data stores will paint a more holistic picture of data throughout the entire ecosystem. This enables businesses to gain a comprehensive view of their data. In addition, businesses can consider consolidating the tools that perform data discovery and classification functions into a single, automated platform. By making data discovery easy to use and relevant to the needs of security teams (identifying high-risk data), privacy teams (identifying PII), and data governance teams (identifying organization-wide data), businesses can better align on a single solution as opposed to a stack of disparate tools.

Data Loss Prevention

Understanding and labeling sensitive data is key to effective data security and privacy compliance. Legacy and cloud-native DLP solutions struggle to provide protections because they do not dynamically discover data, force security teams to take on months-long projects to manually tag, classify and tune regular expressions to match sensitive data, and ultimately result in such high false positive and negative rates

that teams struggle to action them successfully. Since more than 90 percent of businesses distribute their structured and unstructured data across multiple providers[12] they tend to use multiples of such tools with overlapping capabilities, creating inefficiencies. A better approach is to take advantage of a modern solution that automates the process, requires only light tuning and adjustment, and provides a single-pane-of-glass to facilitate data loss prevention across IaaS, PaaS, and SaaS environments with actionable remediation to secure all cloud data.

Data Access Governance

With sprawling cloud environments, security teams have a challenging task managing who can access sensitive data. Two principles apply to governance policies. The first is that there must be a business purpose to access the data, especially when it is protected/regulated. The second is the concept of least privilege, where in ideal circumstances, service accounts access data via established applications or procedures versus direct access by individuals or ad-hoc access directly to the data.

Access to data should be managed through applications, processes, or routines. Adopting zero-trust principles in accessing data, ensuring that only users who have a business purpose to use an app, and that the app only has the specific access to sensitive data it needs to perform its function, is a best practice approach to minimizing direct threats and reducing the operational overhead of direct user access. If the business purpose is clear, and the application/identity/access is managed properly, then the level of effort to govern access permissions and policies is significantly reduced.

This highlights the importance of having an effective tool to search for sensitive data, thus allowing for modification of access permissions.

12 https://mitsloan.mit.edu/ideas-made-to-matter/tapping-power-unstructured-data

Improve Employee Efficiency to Optimize Productivity Costs

One of the keys to achieving cost savings is enhancing employee efficiency. Nearly 80 percent of IT professionals say that moving to the cloud improved their productivity.[13] However, when external forces place demands on an organization's security team, response time is critical, which often means all hands on deck. Improving employee efficiency around managing data is essential for optimizing production costs and achieving the essential goal of lowering security risk. Achieving improved efficiency requires:

1 **Maintaining an Accurate Private Data Inventory**

Many business processes rely on knowing what sensitive data the organization manages, where it's located, and who has access. Legacy approaches force teams to conduct surveys, collect information and manually process the data and determine what is sensitive. An effective, modern solution will streamline and dramatically reduce the number of full-time employees needed for generating data inventory.

2 **Complying with Audits from Privacy and Regulatory Bodies**

There are more than 130 different privacy laws, with the average company in scope for about 50 of them. To stay in compliance requires discovery and policy evaluations, creating the need to proactively address compliance issues that could result in fines, subsequent audits, or a loss of trust with customers.

3 **Responding to Security Incidents**

Once a security operations center (SOC) team is alerted to an incident, time is of the essence to understand the blast radius and its potential impact on the business. An alert raises the question – who has access to this sensitive data and what stakeholders and business units are involved? IT and security teams must work together to figure out the extent of the exposure. Having information at the ready is essential to keeping teams focused on remediation, instead of bogged down with research.

An effective solution will identify data store owners, the sensitivity of the data, and the alignment to risk or compliance frameworks in order to streamline what is typically a manual, survey-based or "get everyone into a Slack channel" approach. Such a solution can be invaluable for reducing mean-time-to-resolution (MTTR). Greater efficiency also comes with a reduction in cost.

13 https://uk.insight.com/content/dam/insight/EMEA/blog/2017/05/Trend%20Report%20-%20Why%20Businesses%20are%20Moving%20to%20the%20Cloud.pdf

How a DSPM Platform Can Deliver Cost Savings

Cyera's data security posture management (DSPM) platform empowers security teams with the ability to discover, understand, and protect cloud data without the complexity, cost, or operational overhead of legacy data protection solutions.

Agentless technology dynamically discovers all cloud data across structured and unstructured data throughout IaaS, PaaS, and SaaS environments, then classifies the type of data that exists in each environment, as well as any regulatory or cybersecurity risks that require remediation.

Security teams receive actionable, extensible scripts to remediate issues quickly, while also mitigating the risk to reputation, customer loyalty, and regulatory compliance stemming from data theft, loss, and compromise.

Cyera addresses a number of key use cases, as illustrated below:

CHALLENGE	SOLUTION
Optimize Storage Costs through Data Minimization	Cyera supports data minimization by: • Helping businesses highlight the overall volume and number of sensitive records in data stores so data owners can minimize stale data to optimize costs. • Identifying the compliance and security risks ghost data represents and helping security teams to remove it. • Identifying copy data and helping to eliminate it safely.
Optimize Technology Costs through Tool Consolidation	Cyera enables tool consolidation and lowers costs by: • Allowing businesses to eliminate license, storage, processing, and delivery costs from redundant tools and technologies. • Continuously discovering and automatically classifying all cloud data, eliminating the need for multiple tools. • Providing consistent data loss prevention across IaaS, PaaS, and SaaS environments, with actionable remediation to secure all cloud data. • Pinpointing overly permissive access and toxic data combinations across your cloud estate, providing a unified platform to govern data access.

CHALLENGE	SOLUTION
Optimize Productivity Costs through Employee Efficiency	Cyera productivity and efficiency by: • Helping streamline maintenance of an accurate sensitive data inventory, reducing the number of full-time employees and time to create that inventory by more than 80 percent. • Consolidating discovery and policy evaluation efforts into a single platform, enabling teams to proactively address compliance issues that would result in fines, subsequent audits, or a loss of trust with customers. • Ensuring that information is at the ready, allowing security teams to respond quickly and efficiently.

CONCLUSION

As data proliferates exponentially across multi-cloud environments, data protection, minimization, and compliance initiatives are taking center stage with security teams. Unused data in the form of stale data, copy data, and ghost data present significant risks and excessive costs for businesses. In today's cost-conscious business world, managing data stored in the cloud and mitigating risk must align with business imperatives. This necessitates continuous cloud optimization, which can reduce costs while improving security and compliance.

Cyera allows security teams to stay ahead of data regulations and risks. Our best-in-class data security posture management platform automatically discovers and classifies all data, across all clouds and datastores. It then analyzes an organization's security posture, prioritizes urgent issues, and provides context-rich remediation steps. This frees up the rest of the organization to harness data, and stay ahead of the competition.

Trusted by

ARMIS.

Cboe

Takeda

ACV AUCTIONS

LifeLabs

UTA

GRANICUS

About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data, their security exposure, and delivers automated remediation to reduce their attack surface. Learn more at www.cyera.io or follow Cyera on LinkedIN.

Learn more about how Cyera can help you manage your rapidly expanding cloud data at cyera.io

Learn more