ermetic

IDC Cloud Security Survey Highlights

Top Identity and Data Access Risks

IDC Survey Highlights the Importance and Challenges of Implementing Least Privilege in Cloud Production Environments

A recent IDC survey of CISOs in the US found that 80% of respondents are not able to identify excessive access to sensitive data in cloud production environments, a first step on the organization's journey to least privilege. The IDC survey found least privilege to be considered best practice by many CISOs, with 73% of them citing the implementation of least privilege as the top challenge.

Traditionally, security has been the main inhibitor for public cloud adoption. Over the years, this concern has gradually given way to the understanding that public clouds are at least as protected as any on-premise data center. But regardless of where the IT operations reside, cybersecurity postures are only as strong as their weakest link, which is almost always the human factor.

Many companies today believe that by relying on the public cloud provider, they can actually achieve better security. Indeed, public cloud providers offer a range of security tools as part of their core offerings as well as advanced automation capabilities that help reduce human error. However, they cannot provide visibility into each and every workload that customers deploy and run on their infrastructure. According to the shared responsibility model for public cloud security, it is up to enterprises to protect their own identities and data in the cloud, and define the access to and configuration of their cloud services.

This is where things may get complicated. The flexibility of public cloud environments enables customers to provision resources with the click of a button, spin up containers based on dynamic scaling requirements, and more. A typical public cloud deployment can quickly turn into a vast maze of interconnected machines, users, applications, services, containers and microservices. Keeping track, evaluating risks and defining access policies and permissions for a multitude of machine and human identities is therefore a huge undertaking, especially as more and more organizations adopt a multi-cloud strategy.

As access policies must be frequently adjusted, the potential for human error increases sharply. Some of the most high-profile cybersecurity incidents in recent years were the direct result of customers failing to properly configure their cloud environments, or granting excessive or inappropriate access permissions to cloud services, rather than a failure of the cloud provider in fulfilling its responsibilities. For example, the Capital One breach in 2019 where 106 million credit card applications were exposed was the result of excessive permissions assigned to a WAF that were used by the attacker to gain access to a sensitive AWS S3 bucket.

The Risks of Excessive Permissions

The proliferation of cloud data breaches was evident in a recent end-user survey of more than 300 CISOs and other decision makers at U.S. companies of all sizes in different industries. The survey was conducted by market research firm International Data Corporation (IDC), and more than 79% of the companies that participated in the survey reported that they had experienced a cloud data breach in the last 18 months. Forty three percent of respondents reported that they have experienced ten breaches or more.

Figure 1: Exposure to Cloud Data Breaches

Q. Has your company experienced a cloud data breach in the past 18 months?

Percentage of respondents who answered “Yes”

INDUSTRY	Yes (%)
Manufacturing	58%
Banking	94%
Health	81%
Goverment	70%
Retail	71%

BUSINESS SIZE	Yes (%)
1,500 - 2,499	81%
2,500 - 4,999	89%
5,000 - 9,999	79%
10,000 - 19,999	71%
20,000 +	72%

The Capital One incident has raised overall awareness of the risks of failing to properly protect sensitive data in the cloud. In accordance, nearly 73% of survey respondents cited the issue of data access governance and permission management to databases in IaaS/PaaS as either very important or extremely important.

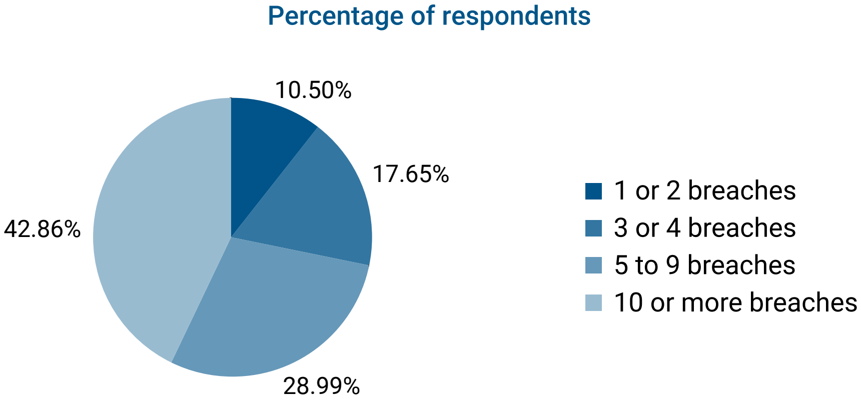
One of the main reasons that cloud data breaches like the Capital One incident are so frequent and damaging is the prevalence of excessive access permissions. Driven by the dynamic and on-demand nature of public cloud deployments, users and applications often accumulate access permissions beyond what is necessary. These excessive permissions are a primary target for attackers as they can be used for malicious activities such as stealing sensitive data, delivering malware or causing damage (e.g. deleting or exposing sensitive files or directories).

More than 71% of respondents cited detection of excessive permissions in the cloud as either very important or extremely important attributes when selecting a solution for cloud access protection.

The rising concern over excessive permissions in the cloud is reflected in the IDC survey as more than 71% of respondents cited detection of excessive permission in the cloud as either very important or extremely important attributes when selecting a solution for cloud access protection. In addition, only 20% of respondents reported that they were able to identify situations in which employees in their organization have had excessive access to sensitive data. These numbers clearly reflect the gap between the importance decision makers attribute to the issue, and their limited capabilities.

Figure 2: Frequency of Cloud Data Breaches

Q. How many times has your company experienced a cloud data breach?



Excessive permissions may go unnoticed as they are often granted by default when a new resource or service is added to the cloud environment. This is where the human factor comes into play: an overworked security or IT admin may fail to identify and remove such permissions and create a significant vulnerability that may only be detected after the fact. Furthermore, early detection doesn't necessarily guarantee prevention; more than 13% of respondents that detected excessive permissions reported that they were unable to mitigate the risks before data was exposed.

Unsurprisingly, many of the organizations that reported the largest number of cloud data breaches were among those who identified excessive access to sensitive data among their employees. According to the survey, the healthcare industry appears to be particularly exposed to this risk as 31.25% of healthcare organizations reported that they have identified a situation where employees had excessive access permissions.

In accordance, a CISO of a large healthcare organization reported that "accessing and using confidential patient data from different departments provides more access for hackers to break into the network." He went on and explained that after identifying the problem, the next step was to "focus on providing limited data access to our staff."

Least Privilege to the Rescue

The need to limit access privileges was mentioned by other respondents as an effective means to mitigate excessive access permissions. For example, a CISO in a very large bank acknowledged that "we have restricted our IT admin and access rights to a very small number of users, which is invaluable in minimizing the risk of data breaches." Another bank cited "managing and restricting excessive access to the sensitive data" as its top IT security priority, while a CISO of a mid-size insurance company said that its company has taken action to "limit access to the company's networks and confidential data to the person who is assigned to it."

The steps taken by CISOs to mitigate risks stemming from excessive permissions reflect the growing interest in the least privilege model which is based on limiting every user or application to the exact permissions required to complete legitimate work activities in order to protect cloud environments. Least privilege relies on continuous and accurate understanding of the relationships between entities – whether human or machine identities – and the systems they need to access to perform their job. Then, we should be able to create access policies to define and enforce permissions based on the estimated level of risk involved in these interactions, track their actual use and remove any permission that is not being used.

Why is it so Difficult to Achieve Least Privilege?

Defining and enforcing dynamic, least privilege access policies involves significant challenges. Most notably, in a typical cloud environment consisting of multiple applications, services and dependencies, implementing least privilege permissions for even a single user could be a daunting task – let alone when dealing with multi-cloud environments.

In this regard, the proliferation of machine identities exacerbates the difficulty of achieving least privilege. Unlike human identities that employ usernames and passwords to authenticate and access resources, machine authentication is based on certificates and encryption keys. However, due to lack of adequate solutions, many organizations rely on cumbersome manual processes and homegrown tools to manage and track their certificates and keys. This approach is infeasible when dealing with dynamic cloud environments where machine accounts are frequently created for multiple entities, many of which have a lifespan of only a few days or hours, resulting in limited visibility and control.

These difficulties were evident in the IDC survey where “ensuring that users, applications, and services can access only the cloud data and cloud resources that are necessary for their legitimate purposes” was selected as the top cloud data protection challenge among organizations of all sizes. Least privilege was mentioned as the main challenge to protecting sensitive data in banking and healthcare, two of the most regulated industries in relation to data protection and privacy.

Figure 3: Top 5 Challenges of Protecting Sensitive Data

Q. Using a 5-point scale on which 1 = not a challenge at all and 5 = a critical challenge, please rate the following operational challenges of protecting your organization’s sensitive data in the cloud.

Combined percentage of respondents who chose 4 and 5

73%

Least privilege access to cloud data

66%

Lack of integration for data protection solutions

66%

Visibility into structured data usage in the cloud

63%

Setting and enforcing data access policies across multiple clouds

63%

Tracking and monitoring privileged access and configuration changes in cloud environments

Figure 4: Top 5 Challenges to Protecting Sensitive Data by Industry

Manufacturing
Setting and enforcing consistent data access policies across hybrid environments

Banking
Least privilege access to cloud data

Health
Least privilege access to cloud data

Goverment
Gaining visibility into unestructured data

Retail
Tracking and monitoring privileged user access and configuratioin changes in the cloud

Figure 5: Top 5 Challenges to Protecting Sensitive Data by Company Size

1,500 - 2,499
Least privilege access to cloud data

2,500 - 4,999
Gaining visibility into unestructured data usage in the cloud

5,000 - 9,999
Least privilege access to cloud data

10,000 - 19,999
Setting and enforcing consistent data access policies across hybrid environments

20,000 +
Least privilege access to cloud data

When asked about their challenges regarding the management of and access to cloud data, respondents highlighted insufficient personnel/expertise (ranked as "significant" or "very significant" by 66% of respondents) as their top concern. This finding was consistent among all company sizes and vertical industries. The second biggest challenge was difficulty in integrating disparate security solutions (52%).

Figure 6: Top Operational Challenges to Managing Access to Cloud Data

Q. Using a 5-point scale on which 1 = not a challenge at all and 5 = a critical challenge, how significant are each of the following challenges regarding the management of and access to cloud data?

Combined percentage of respondents who chose 4 and 5

66%

Insufficient personnel/ expertise

52%

Difficulty in integrating disparate security solutions

39%

Currently available solutions not meeting our needs

On the same note, 88% of the participants in the IDC survey selected "integration and interoperability with other IAM solutions" as the most important attribute when selecting a solution for cloud authorization and permission management in the cloud. The ability to centrally manage access and permissions to unstructured data in the cloud was ranked second with 75%, followed by automation of permission adjustments with 64%.

Figure 7: Key Capabilities for Authorization and Permission Management in the Cloud

Q. Using a 5-point scale on which 1 = not important at all and 5 = very important, how important are each of the following attributes when selecting a solution for authorization and permission management in the cloud?

Combined percentage of respondents who chose 4 and 5

88%

Integration and interoperability with other IAM solutions

75%

Ability to centrally manage access and permissions to specific files within SaaS, IaaS/PaaS environments

64%

Automation of permission adjustments

60%

Ability to centrally manage access and permissions to databases within SaaS, IaaS/PaaS

60%

Ability to centrally manage permissions to specific actions within SaaS applications

These findings may point to the operational challenges faced by security teams today. The past several years have seen the emergence of identity and access management solutions to protect cloud resources. However, these solutions were not designed to provide the centralized, comprehensive visibility and control required for implementing least privilege access across multi-cloud IaaS and PaaS environments. In accordance, **more than 63% of the survey respondents cited "lack of adequate visibility of access to/in cloud production environments" as either a very significant or extremely significant security threat to their cloud environments.** The Capital One incident is likely the reason why AWS users expressed greater concern over this threat (70%) compared with users of other cloud platforms.

The lack of means to protect and control cloud access may also explain why insufficient personnel and expertise was highlighted as a key challenge by survey respondents. Due to the shortage of product capabilities, security teams struggle to manage access permissions across cloud environments that continue to grow in size, complexity and diversity. This, in turn, increases the potential for human errors and – consequently – cloud data breaches.

Automate, Analyze, Adjust

The IDC survey emphasizes the importance of the least privilege as a best practice in securing access to public cloud IaaS and PaaS environments. At the same time, it indicates the difficulty of effectively implementing least privilege access permissions using existing security solutions and approaches.

The survey findings indicate the need for a different approach when implementing least privilege access to cloud production environments and minimizing the exposure to excessive access permissions. Given the scale and flexibility of IaaS and PaaS environments, organizations are in need of integrated, centralized management and automation to reduce the reliance on humans and compensate for what appears to be a growing lack of adequate personnel and expertise.

As more workloads are running in IaaS and PaaS, and more sensitive data is located outside the corporate datacenter, these capabilities will become critical. Moreover, to achieve least privilege at scale, the next generation of cloud access security solutions should be able to analyze access policies spanning an ever-increasing number of human and machine identities and continuously compare them against actual access patterns to identify anomalies, excessive permissions and risk, and adjust them accordingly.

www.ermetic.com