STACK IDENTITY
Identity-first cloud security

The Shadow Access Impact Report

# How Identity and Access are Disrupting Cloud Security, Compliance and Governance

# Table of Contents

Stack Identity Research

# Shadow Access Impact Report:

## How Cloud Identity and Access Impacts your Risk, Compliance and Governance

### Executive Summary

Everything you deploy and run in the Cloud has an identity with access to data. Zettabytes of data pouring into the cloud has led to a proliferation of data stores containing sensitive information. As more cloud applications and services are created to leverage this data, more identities are generated, causing in turn more access to data. AWS alone has thousands of connection methods that can use thousands of permissions, creating millions of access combinations.

This cycle of growth of cloud data, applications and identities has radically changed our identity and access reality, making identity and access management more complex & increasing the risk of cloud breaches and data theft.

This new reality is further complicated by the plethora of IAM systems used by enterprises to manage IAM, with 25 different systems reportedly used in 41% of companies surveyed.

Cloud and identity growth in an environment of IAM sprawl has several impacts on businesses. The most significant impacts are on security, compliance and governance, resulting in costs (OPEX and CAPEX), skills shortages, and constant pressure to minimize cybersecurity risks while advancing digital transformation initiatives.

This report will uncover how these challenges are unfolding and share some key impacts discovered in live production environments.

| IAM sprawl cost and complexity | Cloud and data Risks | Governing cloud access |
|---|---|---|
| **41%** of companies have **25** different systems to manage access rights. [1] | **80%** of breaches are identity related. [2] | AWS alone has over **13,000** connection methods with over **14, 000** permissions creating millions of access paths. [3] |

1 https://www.itsecurityguru.org/2022/12/15/the-state-of-identity-security-widespread-attacks-wasted-invesment-and-identity-spawl/

2 Verizon DBIR 2022

3 https://aws.permissions.cloud/

# 1 The ‘Access Surface’ is Automated and it’s Expanding

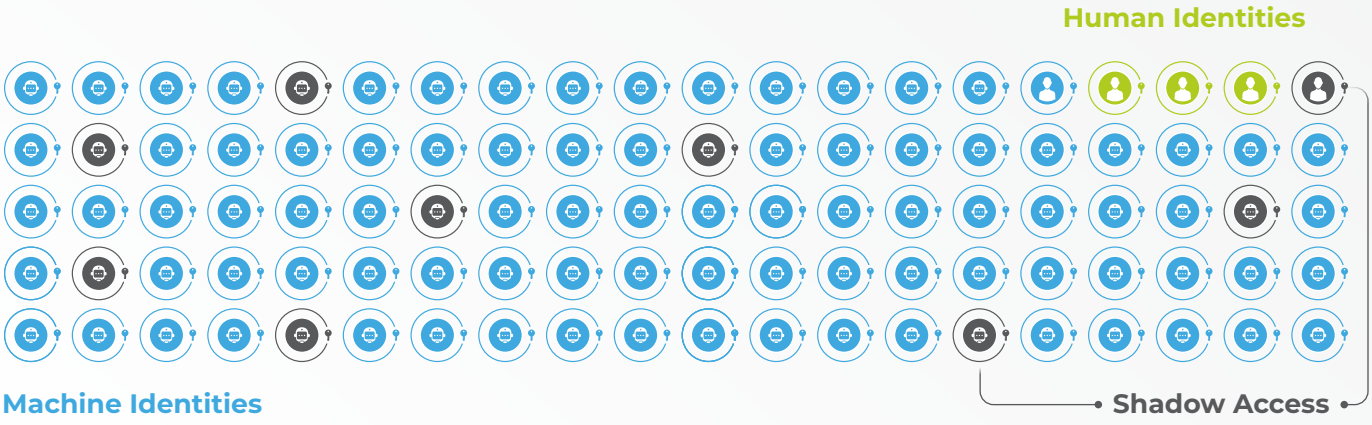
A key contrast between the old and new worlds is a look at identities. Whereas in the past virtually all identities were human, today automated, machine identities are overtaking human identities. This is driven by two key trends - digital transformation and automation. Digital transformation has accelerated the use of cloud services, which in turn consume other cloud services to create the desired value chain for businesses. To enable these services, developers use Cloud APIs as a common interlock between services that automatically create identities for the services that they connect.

Automation is also applied in many other areas such as employee onboarding into apps such as Workday, which then automatically grants access per the selected employee profile type.

**How many identities do you think are in your company, vs how many identities actually exist ?**

A recent Stack Identity analysis of cloud native, enterprise environments showed only **4%** of identities as human.

**<5%**
of Enterprise Identities are
**Human**



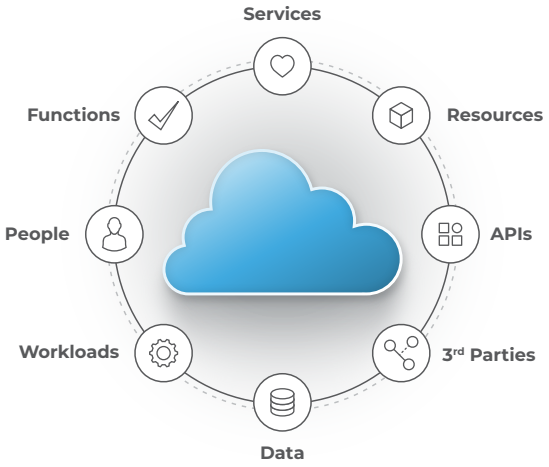
This also highlights the gap between actual identities vs what cloud and security teams think exist in their cloud environments.

There are many identities that exist in the cloud, both human and non-human.

Human identities are of course, developers, administrators, end users, 3rd party partners or contractors, and many other types.

Non-human identities are often automatically generated for applications that access other applications, APIs, cloud workloads, data stores, microservices, and other multi-cloud services.

## CLOUD IDENTITIES





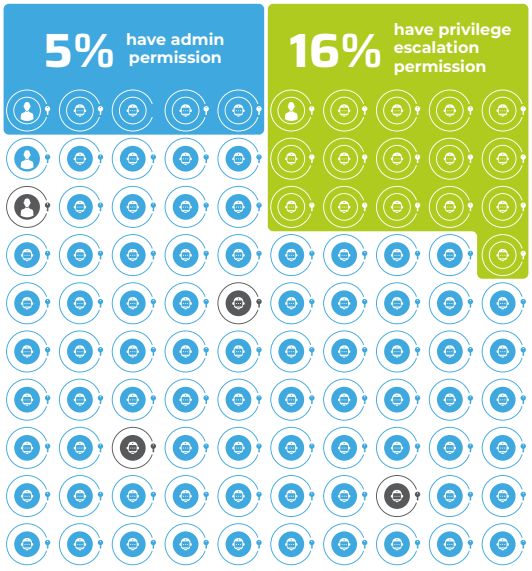
source: https://aws.permissions.cloud/

Every identity has sets of permissions to access cloud data and applications. In AWS alone there are over 14,000 permissions that give access to 13,000 cloud services.

The powerful permissions that are exploited to breach cloud services and data most often include **admin permissions** and **privilege escalation** permissions.

Stack Identity research of active cloud environments shows almost 5% of identities in the enterprise have admin permissions, a level that is slightly greater than the average percentage of human identities.

These same production cloud systems show 16% of identities with privilege escalation permissions, a level that is over 3x of admin permissions.



Over-permissioned access coupled with powerful permissions in cloud environments creates many gaps through which organizations can suffer cloud breaches, intellectual property and sensitive data loss.

A recent example is the 2022 LastPass breach:

LastPass

| Initial Intrusion | Source Code Exfiltration | Mandiant Investigation Closed | LastPass corporate vault customer data backup exfiltration |
|---|---|---|---|
| **August 8th 2022** | **August 12th 2022** | **August 13th 2022** | **Oct 26th 2022** |
| 1st Identity & Access Breach: | | | 2nd Identity & Access Breach: |
| • Attacker leveraged overly scoped access permissions that were never used before<br>• Access to S3 bucket containing:<br>a) source code folder<br>b) encrypted backup folder of LastPass customer data | • Exfiltration of source code and encrypted backup data<br>• Suspicious access activity<br>• Investigation begins | • Access occurred from anonymous VPN gateway<br>• Anti evasion tools bypassed EDR<br>• Incident closed | • The encrypted data stolen in the first incident revealed the identitites of 4 DevOps engineers who had access to the master key<br>• Attacker targeted a DevOps engineer to exfiltrate keys and data |

**Threat actors left identity footprints that no one tracked...**

source: https://stackidentity.com/lastpass-breach-investigation-an-analysis-through-the-lens-of-cloud-iam-operations/

In addition to cloud security risks, the expanding access surface of cloud identities and access paths breaks IAM operations and complicates access audit, compliance and governance processes.

Compliance and governance teams rely on manual processes and static tools to collect information from distributed systems, such as AWS, Identity systems (IdP, IAM) (Okta), approval systems (JIRA), etc.

## 2 Toxic Combinations Exploit Cloud Services and Data

Let's examine the risk equation of identities and access.

Toxic combinations are created by the intersection of identity exploit vectors, such as over - permissioned or stale identities with access exploit vectors, such as chained or secondary access, to cloud applications or software supply chains and their associated data.

Looking beyond admin and privilege escalation permissions to some typical policy permissions, Stack Identity research found that 76% of policies used in enterprise cloud environments include write permissions and 28% of policies have some level of permission management permissions.

This makes enterprises vulnerable to toxic combinations of permissions, allowing attackers to exploit cloud infrastructure with malware, such as ransomware, or exfiltrate sensitive data assets.

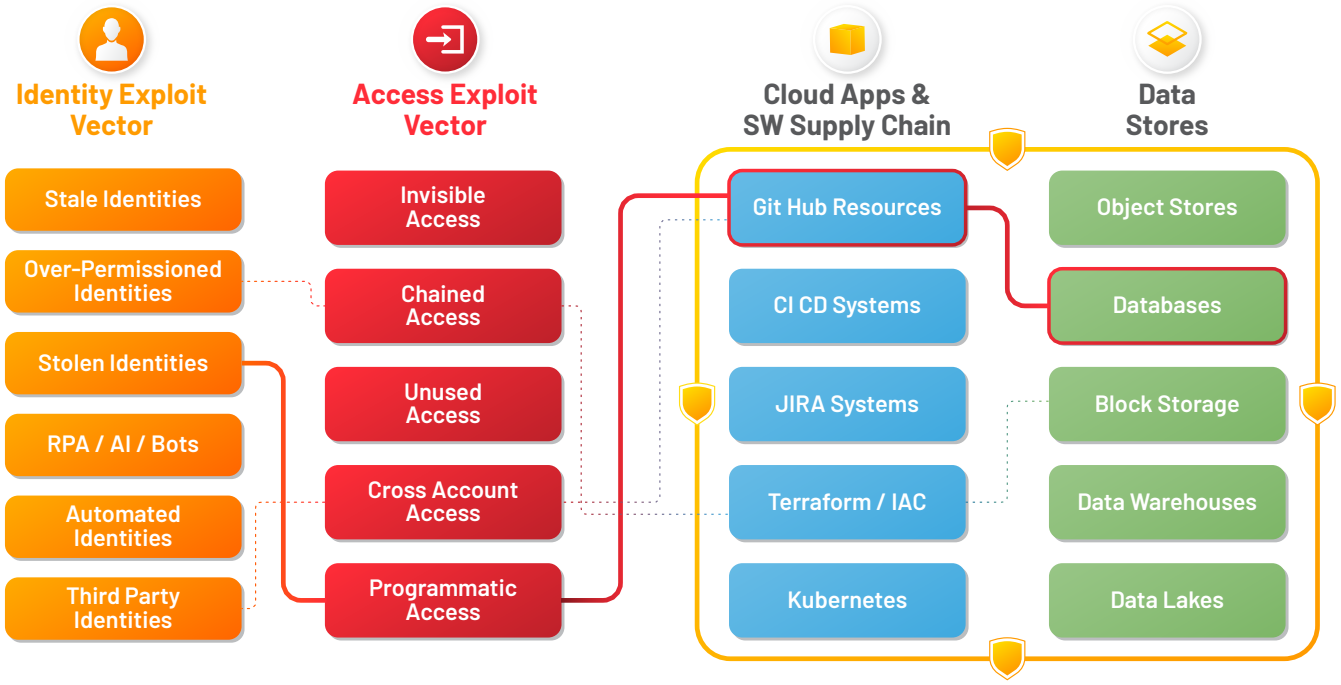

**76%** of identities have write permissions

**28%** of identities have permission management permissions

" The existence of hundreds or sometimes thousands) of identities - both **human and programmatic** - across the CI/CD ecosystem, paired with a lack of strong identity and access management practices and common usage of overly permissive accounts, leads to a state where compromising nearly any user account on any system, could grant powerful capabilities to the environment, and could serve as a segue into the production environment. "

*OWASP Top 10 CI CD SEC-2*

Toxic combinations of identities + IAM blind spots create weaponized pathways to your cloud data and infrastructure




Toxic combinations of identities and IAM blind spots create weaponized pathways to your cloud infrastructure, including applications and your software supply chain, and cloud data. These pathways are called Shadow Access, the unauthorized, unmonitored and ungoverned access that is easily exploited to breach cloud environments and exfiltrate data.

Identity practitioners, governance teams and data owners all contend with IAM in their own tools and process silos.

Given that the average enterprise uses more that 25 IAM tools, all of which are blind to Shadow Access, security and cloud teams lack a complete view of identities and access across their clouds.

These IAM blind spots are caused by 2 realities that exist in most organizations today.

First, visibility to who is accessing your data and who has access to data is scattered across Cloud IAM, Cloud IDP, Infrastructure as Code, data stores and HR systems.

Second, visibility to who is authorized to access your data is scattered across ticketing systems, emails, spreadsheets and screenshots.

This leaves most organizations without the full context they need to fully govern cloud IAM and secure their cloud assets.

**Key vectors that you should be able to see across your cloud environments are:**

1. All the pathways by which third parties can access your sensitive data stores.
2. Breached identities that have accessed your systems in the past 48 hours.
3. Cloud identities with no Jira tickets accessing your sensitive data.
4. Data pathways that violate customers' data sovereignty and data residency.
5. “Permission drift” to your production systems that violate your FedRamp baseline.

Below is one example from the Stack Identity team of how shadow access was exploited in a live customer environment.

## Customer Profile: Telecommunications, Public

Below are risk details of a critical S3 bucket – Prod-Swagger-UI

A risky path is discovered between the S3 bucket and a business intelligence agent (prd) [us-east-1] (Compute) Named Default Application5

**The S3 bucket (Prod-swagger-UI) ;**

- Is created by the **identity aws account-ids-prd**
- Is connected to an application **Business Intelligence - Agent Linux/Unix Compute Instance** *(Default App5)*
- Via the role **bi-agent-prd-use1-ec2.**

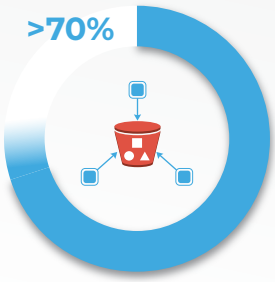
This role is provisioned with a critical **permissions management** permission. This can be used for **privilege escalation**, making it a high risk role.

Attached to this role, is the AWS managed policy (AdministratorAccess) which provides the role **full access *** to all resources and all services.

This is very high risk as an attacker who gains access, for example via a vulnerability, can execute an almost unlimited number of exploits.

### Potential exploits include

- Directly exploit the S3 bucket to exfiltrate sensitive data
- Create another IAM user to fire up new EC2 instances or buckets
- Extend the same AWS infrastructure, services, apis, tools to any data centre, co-lo space or on prem facility to execute cyber attacks




**>70%** **accounts have 1 or more EC2 instances accessing all S3 buckets**

**Implication:**
Attackers can leverage compromised EC2 instances to access sensitive data stores leading to data breaches

**Best practice:**
Configure S3 bucket policies to restrict broad access

Source: 2023 State of Cloud Permissions Risks Report

Toxic combinations of identities and access impact risk posture as well as finance and operations.

### Risk Posture Impact

IAM impacts risk posture through toxic access combinations that increase in severity with depth of access and scope of access

### Financial & Operations Impact

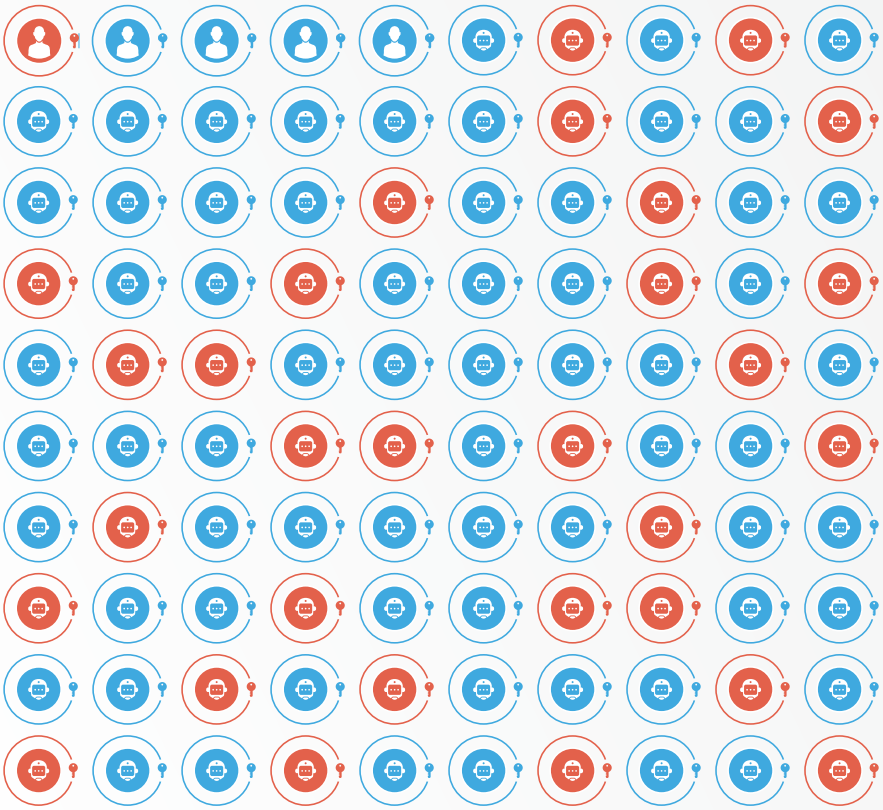
The time and resources involved in managing current cloud identity and access are high and therefore expensive. Cloud teams suffer from IAM sprawl across many IAM applications and data tools in use.

In fact Stack Identity analysis of live production clouds reveals that on average **31%** of enterprise identities have toxic combinations of identities and access.

**31%**

of Enterprise Identities have

**Toxic Combinations**



## 3 Shadow Access Types and Tactics

The mathematics of access combinations shows millions of possible permissions. However, there are important shadow access types that affect compliance and governance efforts and are commonly targeted by cyber-attackers:

| | |
|---|---|
|  **INVISIBLE ACCESS** | AWS console did not show effective permissions for an S3 bucket when scanning which led to an S3 bucket being left open |
|  **UNWANTED ACCESS** | Lambda function replaced by malicious code creating unauthorized external access being left open |
|  **EXCESSIVE ACCESS** | Policy with full access is given where only access to specific data stores, or cloud services are needed |
|  **DORMANT ACCESS** | Policy with full access has not been used in 60 days but was still available for assignment to a role |
|  **CROSS ACCOUNT ACCESS** | Not a customer for 2 years yet still has cross account sharing enabled |
|  **DATA RECOVERY ACCESS** | Assumed role access to programmatic access to an S3 bucket used for data backup for DR |
|  **RISKY ACCESS** | Customer critical situation allows developers access to resources but permissions are not revoked after the situation is resolved |
|  **TOXIC COMBINATION** | Programmatic access to S3 Bucket via application identity along with permissions management permissions |
|  **UNUSED DATA** | The flip side of Dormant Access, where data has not been used for 60 days, but access is still enabled |
|  **RIGHT SIZING** | Understanding which policies and permissions are not being used and change them to make sure access is correct |

## Cloud IAM Actions

As mentioned earlier, cloud authentication (who has access) and authorization (who has permission) are key variables in the equations for risk as well as for compliance and governance.

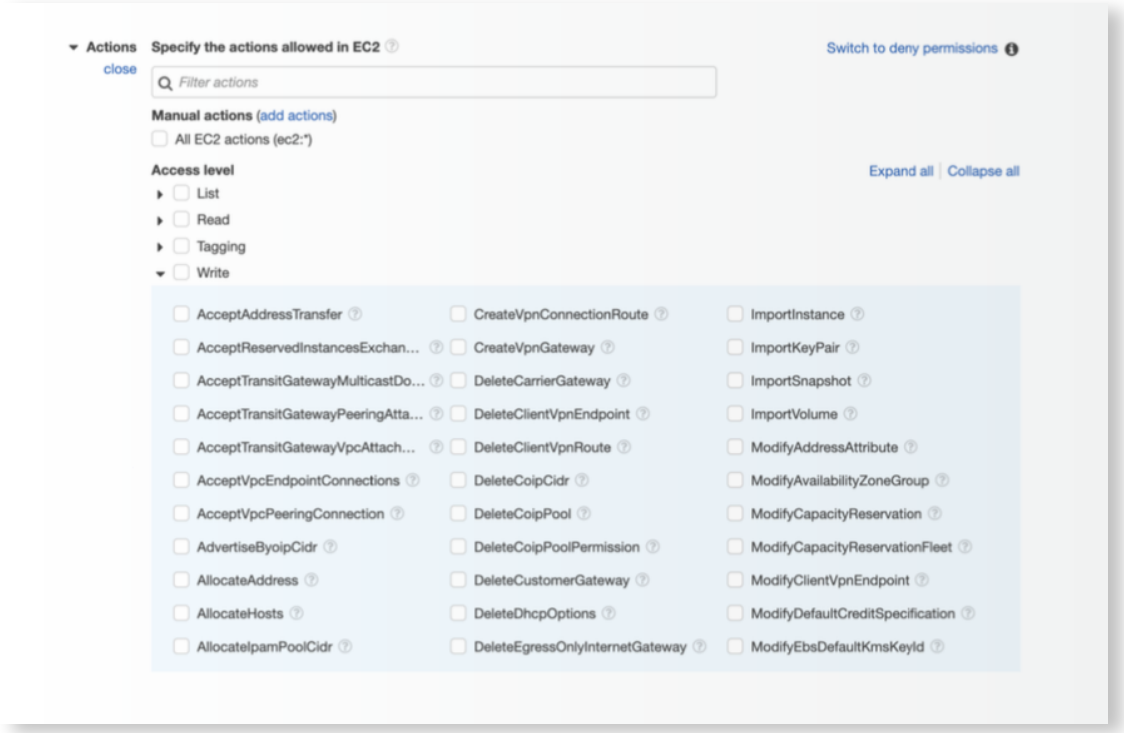
The basic flow of authentication and authorization works as follows, using AWS as an example:

1. The “Principal”, which can be a user, a role, or an application, authenticates to the AWS control plane either directly or via IdP, Cross Account, and SSO.
2. After authentication, the Principal’s permission is verified. This permission originates from the policies associated with it, which can be a session, resource, or identity-based, among others.
3. Once the permissions and their conditions are validated, the Principal will be able to perform the actions allowed on the resources assigned to him. Usually, this setting can be marked with an “*”, i.e., all.

    - Now that we understand how the control to access a resource in AWS works, we get to the real challenge: the use of policies in AWS based on the concept of minimum or least privilege. It’s very common in integrations with partners, such as SaaS services and analytics firms, to create an access policy between the environments based on an access key or roles.

      While doing this, are you aware of the actions under each permission type for a resource?

      For example, a simple write permission on EC2 service consists of 397 actions.



- Now write may be a basic action at a high level under normal circumstances for any application to operate and write into a backend object storage service like S3. But in these 397 permissions almost 0.9% permissions are risky (according to CSPM and Opensource CSPM) BUT when configured to access a single resource like S3, then 2.7% becomes risky and can lead into privilege escalation if granted.
- Likewise, there are certain AWS managed policies wherein each policy has almost 1600 actions defined. And out of them, 13 permissions are risky when standalone , but when combined with a single data asset resource almost 41 actions becomes risky.
- It is a massively complex and time-consuming challenge to hunt for risky combinations. But DevOps teams don't have the time to test all the combinations because there are 12700 permissions residing inside these AWS services.

## Following Cloud IAM Footprints

Stack Identity has uncovered these types of access vectors in live enterprise cloud environments with associated risk impacts that were identified and mitigated.

The Cloud IAM footprints that are created in these exploit vectors are analyzed across the context of all identities, cloud data and resources.

**Impact:**

**Cloud Breach**

Invisible access by an attacker because the AWS policy console does not show effective permissions or inherited permissions to an identity or resource

**Impact:**

**Cloud Breach**

A compromised resource-based policy created a back door for an attacker

**Impact:**

**Cloud Data Exfiltration**

Abused IAM permissions attached to an application instance or application running on a compute instance to exfiltrate sensitive data

**Impact:**

**Cloud Breach**

Server-less (Lambda) function was replaced with malicious code that added an IAM user for an attacker's access from outside

**Impact:**

**Cloud Breach, Malware Hosting**

Programmatic access to an external vendor was compromised that caused S3 to be used for crypto mining and malware hosting

# 4 Cloud IAM Impact to Cloud Operations, Governance and Risk

The Cloud IAM reality affects more than risk of cloud breaches and data exfiltration. Both compliance and governance are unable to keep pace with the cloud, and consequently creates business impacts through costs, resources and time challenges.

Digital transformation requires businesses across all sectors to predictably and reliably demonstrate compliance to the relevant standards, such as HIPAA, PCI DSS, NIST, SOC2 etc. Access compliance is an important part of this - who has access to what, who is accessing what, what access has changed in the last 90 days and so on.

Security and compliance are both important but different aspects of cloud IAM. This is well summarized by the following table showing some key data breaches from 2022-23, and the compliance status of those companies.

## Compliance and Security: Related but different

| Company | soc 2 | soc 3 | FedRAMP | PCI DSS | ISO / IEC 27001 | BSI CS | Data breach |
|---|---|---|---|---|---|---|---|
| Atlassian | Yes | | Yes | Yes | Yes | | Yes |
| MailChimp | Yes | | | Yes | Yes | Yes | Yes |
| Slack | Yes | Yes | | Yes | Yes | Yes | Yes |
| LastPass | Yes | Yes | | Yes | Yes | Yes | Yes |
| Dropbox | Yes | Yes | | Yes | Yes | Yes | Yes |
| Uber | Yes | | | Yes | Yes | | Yes |

*https://ventureinsecurity.net/p/the-importance-of-adopting-a-security*

Today, access compliance in the cloud is time consuming, resource intensive and static, with compliance teams relying on disparate tools such as screenshots and spreadsheets, across the many cloud systems that manage some level of access. The result is that quarterly access audits become painful and expensive, and are often unpredictable.

Organizations across different sectors are uncovering business and security impacts from unmanaged cloud identity and access. Below are some common datapoints from cloud and security teams that illustrate the impact to cost, resources, data breaches and cloud threats.

## Business Impacts

- Existing CSPM & compliance tools were unable to deliver necessary insights, requiring 2 headcount and sixty days of manual effort on compliance.
    - CISO, Leading financial service provider in India.
- Over 60% of existing identities required access to be revoked or right-sized.
    - CISO, Service Management Software.
- Operating and capital expenses improved when engineers could control security and automate least privileged enforcement for SecOps and DevOps.
    - Security Service Leader, Digital infrastructure protection for thousands of brands.

## Security Impacts

- Ransomware was identified through visibility of identity and access risks.
- Unknown machine identities that could disrupt security and audit processes were identified.
- Data risk was reduced using a definitive baseline of identities and what they can access in an enterprise cloud environment
- Customer data was secured with a consolidated and prioritized view of risks to cloud services hosting customer data.
- An environment with data sharing across accounts and source code delivery through a SW supply chain gained continuous visibility into cloud data exposure risks.

The rapid pace of cloud computing, data and identity creation leaves a gap between actual and perceived identity and access in the enterprise. This unmonitored, invisible and ungoverned cloud identity and access is called Shadow Access, and increases the risk of cloud breaches, malware, ransomware and data theft. Existing IAM tools are blind to shadow access primarily because they are highly distributed across many systems and lack full visibility across identities, cloud data and infrastructure. This leaves cloud and security teams without the complete context needed to continuously monitor and manage cloud IAM.

This report shows how shadow access and the current, fragmented IAM systems increase cloud risk and also impact cloud operations and governance areas. These impacts make it costly, time consuming and complex to right-size access, enforce least privilege access in real time and detect and remediate access risks in the cloud.

Even In the current economic climate, digital technology initiatives remain a top strategy priority. The best ROI for these tech initiatives is to consolidate cloud identity and access with a unified approach that is complete, continuous and actionable. This is an innovative and more effective approach to improve security posture that reduces risk, lowers costs and streamlines operational processes.

# 5 Best Practices and Recommendations

1. **Map a baseline of all identities, human and non-human, and all access permissions.**

   Develop a "single source of truth" and create an accurate baseline of identities that are operating across cloud environments. This baseline will help you answer three questions:
   **a)** Who is accessing what?
   **b)** Who has access to what?
   **c)** Who should be authorized to access what?

2. **Eliminate all "standing unused privileges" to reduce the cloud attack surface.**

   Use a retrospective 30/60/90 day analysis of your cloud access to identify all unused access - permissions, entitlements, policies, and roles, to build your evidence for removing all unused standing privileges without pushback. Track all privileged access against this new baseline.

   [Over time, implement automated drift detection over a 30/60/90/ day time window against your cloud baseline to operate continuously in least privileged mode.]

3. **Address high risk access permissions, especially third party access permissions, that do NOT have JIRA tickets, or other documented access approvals.**

   Get visibility into your governance gaps. This is determined by matching your cloud identities and permissions to your documented approval process. Get visibility into:
   **a)** cloud identities provisioned into your environments that don't have a matching ticket
   **b)** risky third-party access that has never been through an access review process
   **c)** over-privileged SaaS applications that you may not be using anymore
   **d)** any type of high-risk privileged entitlement that has been assigned to non-administrators

4. **Ensure you have access reviews for just-in-time 3rd party access reviews as well as quarterly audits.**

   Implement a process for just-in-time user access review by immediately flagging approval process deviations - proactively and immediately. An automated system for detection and remediation of unauthorized identity and entitlements can help reduce the effort required.

5. **Rightsize permissions and policies to reduce cloud misconfiguration and data exposures.**

   Automate the detection of risky cloud policies and entitlements for high-risk cloud accounts, such as production accounts, FedRamp ATO boundaries, etc that hold sensitive operational, customer and compliance data and whose exposures have negative impact on continued business operations.

## About Stack Identity:

Stack Identity transforms cloud IAM operations by automating access policies to secure cloud data with identity governance. Stack Identity's Cloud IAM data security platform continuously detects and removes unauthorized and invisible shadow access. Through its patent-pending Breach Prediction Index (BPI), Stack Identity reveals the 2% of toxic access combinations that impact 90% of data assets and enables cloud security teams to quickly prioritize remediation. Based in Silicon Valley, Stack Identity was founded by security industry veterans with decades of experience across IBM, Blue Coat, Netskope, Symantec, and McAfee and more.

**Visit us**

STACK IDENTITY
Identity-first cloud security

**Follow us**

LinkedIn

**Join us**

CSA cloud security alliance®

**Find the unauthorized, unmonitored and invisible access in your cloud in 60 minutes by registering for the Shadow Access Risk Assessment here:**


**SHADOW ACCESS RISK ASSESSMENT**