White Paper

Why is Cloud Access Governance Critical?

orkus

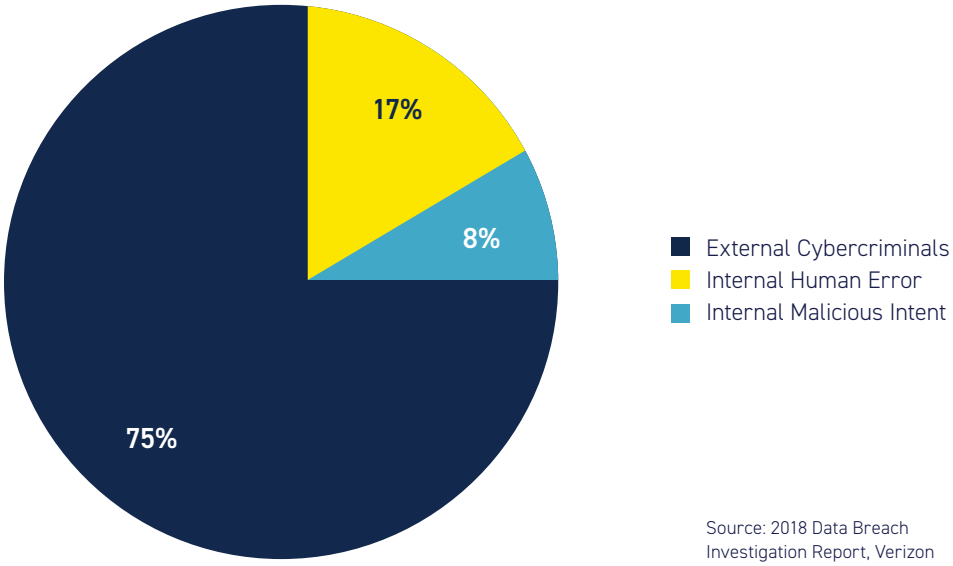
Today, corporations worldwide have business-critical corporate data and infrastructure in the cloud and unauthorized access is a major security challenge. Even a small cloud workload can have tens of thousands of access relationships, and a single mistake can open access to hackers and careless, disgruntled, or malicious insiders.

The Situation

Unauthorized Access is a Business Risk

New regulations, such as GDPR, mean unauthorized access to your data and critical infrastructure in the cloud can expose your business to significant financial risk. Failure to meet PCI, HIPAA, or SOX governance requirements also put your business in jeopardy. In addition, a breach can cause significant brand damage and have a lasting impact on long-term revenue. Securing access to critical cloud infrastructure is a top concern for C-level executives

Breach Sources



Source: 2018 Data Breach Investigation Report, Verizon

Traditional Access Management Doesn't Work in the Cloud

The complexity, scale, and rapid change of cloud workloads makes secure access and authorization a huge challenge for security and compliance teams. Data is exponentially and, often unknowingly, is exposed to inside or external threats. Infrastructure is continuously scaling and becomes vulnerable to operator error and mistakes due to overly permissive access. The large number of privileged actions and roles in the cloud causes privileged identities to get bloated with excess and stale privileges—which significantly increases the attack surface.

Serious and Growing Business Threat

Businesses everywhere agree that cybercrime is exploding and protecting cloud assets is a huge challenge—the facts are daunting. From 2017 to date, cybercrime damages have cost businesses $1 trillion and this figure is forecast to escalate to $6 trillion by 2021 (Cyber Security Venture's Cybercrime Report). The threat sources are both internal and external with 25% of breaches caused by employees, of which the majority are due to carelessness or human error.

Gartner Group's Emerging Risk Report, cites that four of the top ten security and risk audit findings organizations must avoid are related to access and the Deloitte Global Security Survey found that 45% of respondents had experienced audit findings involving excessive employee access rights, with 35% involving segregation of duty (SOD) violations. Real-time, proactive access governance is required in order to avoid unexpected loss and prevent potentially catastrophic disruption to business operations, reputation, and brand.

The Challenges

Large Scale

A small cloud workload can have tens of thousands of objects including data, instances and services. Due to the very nature of the cloud—every object can have its unique access and authorization controls. It only takes a simple access grant to expose a sensitive cloud object, which is one among thousands or millions, to unauthorized access. Manually spot checking or verifying access and authorization in cloud doesn't scale.

Organizations require new approach to securing cloud access and authorization that is continuous, intelligent, and automated.

Continuous Change

Due to the ephemeral nature of cloud workloads, continuous changes are happening. An Enterprise cloud workload can have hundreds of changes every day involving creation, deletion or modification of objects along with access and authorization policies and controls. Mistakes and operator error are one of most common reasons for data exposure and security incidents. A seemingly harmless change can expose your sensitive infrastructure to unauthorized access. Automating change analysis and preventing harmful changes, whether malicious or accidental, is key to securing your access.

Complex Access & Authorization

Access & authorization controls are very complex in the cloud. A simple AWS IAM policy can have thousands of lines of JSON and when multiple policies at IAM, roles, object and Active Directory are combined—it can be very challenging to understand. Security and compliance teams struggle to have even basic visibility on "who" has access to "what", let alone proactively secure access and authorization policies and controls.

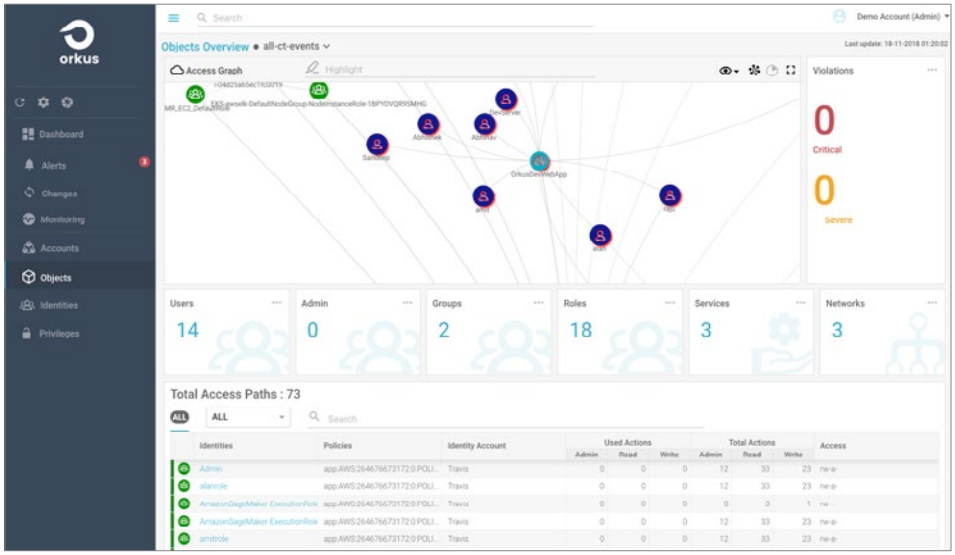
The certainty of cloud access and authorization administration is that the identities, infrastructure, and complexity are in a constant state of change; and, ineffective control unlocks and exposes valuable business assets to the escalating security risk landscape.

The Solution

The Orkus Cloud Access Governance Platform protects cloud infrastructure, data, and privileged identities from unauthorized access. By using Graph AI, Orkus learns the access relationships and patterns in your cloud workloads and uses that to continuously detect and prevent unauthorized access. Automated and intelligent access governance is critical for keeping up with the scale and rapid change in cloud workloads.

Real-Time Visibility with Access Graph

Orkus creates a real-time graph of access and authorization for your cloud workloads by capturing all of the access relationships among the data, infrastructure, and identities in your cloud. This graph can scale to thousands of objects and millions of relationships that can be changing continuously.



Continuous Access Visibility

Instantly know “who” has access to “what” from “where” and “how”. Map access from your Active Directory users to your cloud objects and back. Orkus simplifies understanding your access and authorization as well as enables continuous visibility.

Search on your Fingertips

Instantly search across your graph to understand access for an object or an identity. Query existing tags, data classification and user attributes to zero in on access. Orkus enables you to search using natural language auto complete queries without requiring you to learn a new query language.

Comprehensive Access Map

Access and authorization controls are distributed across many different layers in the cloud. These controls often stack on top of each other to result in effective access privileges. Orkus unifies the access and authorization layers across AD, cloud applications, infrastructure, and data—providing you a unified view.

Intelligent Access Governance with Graph AI

Orkus uses Graph AI to learn "who" has access to "what" and "how" the access is being used. By applying machine learning on the access graph, Orkus understands access intent and usage across infrastructure, data and identities in your cloud infrastructure.

Find Excess Privileges

Excess and unused privileges, one of the biggest security risks, are rampant in all organizations. Instantly identify user and service accounts with excess or stale privileges that pose a risk to your cloud infrastructure.

Identify High Risk Access

By performing clustering and peer group analysis, Orkus automatically identifies access relationships that are high risk in real time. This enables proactive lock down of high risk access before it is actually used by malicious insiders or attackers.

Detect Abuse Access

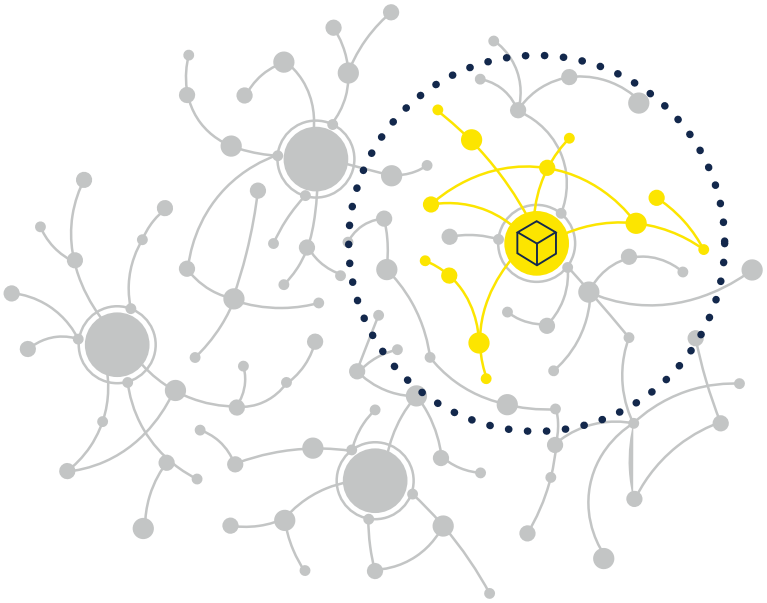
Orkus continuously analyzes the patterns of access including type, volume, location, time and many other attributes to identify anomalous or suspicious access activity. By learning access usage patterns both individually and across clusters, Orkus builds access usage profiles for every entity in the cloud.

Change Analysis

Orkus continuously analyzes all changes in access for every object and identity in the cloud and identifies high risk changes caused by malicious intent or operator errors. Since the volume of change can be very high in a dynamic cloud workload, automation is essential to keep up and prevent harmful changes.

Automated Guardrails to Prevent Unauthorized Access

The Orkus platform Access Guardrails provide a simple and powerful method of automating cloud access governance. Using guardrails, security and compliance teams can specify access control intent without the worry or time consuming task of managing hundreds of low-level access and authorization policies. Orkus enforces the guardrails across your cloud infrastructure in real time.



Secure Data Access

Orkus proactively restricts access to sensitive data with inbuilt guard rails that prevent unauthorized data exposure. Guardrails monitor every data object for exposure to high risk users, services and networks as well as for access abuse.

Automate Compliance

Orkus provides built-in guardrails for GDPR, PCI, SOX, and HIPAA access control requirements to assure Enterprise regulatory compliance and prevent stiff penalties. With GDPR, the financial risk of unauthorized access has increased significantly and it is no longer sufficient to very your access and authorization controls twice a year—leaving the business exposed.

Protect Your Infrastructure

Orkus built-in guardrails lock down access to hundreds of sensitive actions across your cloud infrastructure, preventing both user error and malicious activities. Unauthorized access to Infrastructure can not only result in security breaches but also downtime and outages—effecting your business's topline.

Custom Guardrails

Organizations can easily create custom guardrails to enforce access governance based on data classification, infrastructure tags and active directory user and group attributes. These guardrails provide security and compliance teams with the ability to continuously enforce access governance across their dynamic cloud environments.

Access Analytics for Audit & Investigations

In the world of DevOps and Infrastructure-as-code, access can change in real time and it is complex to analyze. The Orkus Access Graph automatically unifies silos of access control from your Active Directory, Cloud IAM, data, network, and encryption, and provides simple, searchable and actionable intelligence.

Automate Least Privilege

Orkus automates least privilege by detecting unused and stale privileged access across the access graph and quarantining it. Excess privileges are a significant security risk and an attack surface that is readily exploited by hackers and malicious insiders.

Investigate Incidents

Investigate present and historical access with one simple query. Analyze access pattern changes and identify threats over a user-selectable period i.e. the last week, month, or year. Security and audit teams spend countless days and weeks manually analyzing logs to understand and investigate issues—Orkus eliminates that labor with automation.

Automate Audit Reports

Easily create automated audit reports for privileged access and data access to validate your security controls for auditors. Orkus provides the ability to create single-click reports and dashboards that show the effectiveness of access and authorization controls across your cloud assets.

Prioritize Certifications

Prioritize access certifications to focus on high-risk access, eliminate rubber stamping, and stop ineffective, time consuming manual processes. As a part of a SOX audit, Enterprises are required to periodically certify access. This certification process can consume a lot of valuable resources and time. Orkus saves you time and improves the efficacy of access certifications.

Conclusion

The Orkus platform is like having a full-time, access and authorization management team at my fingertips!

If identity is the new perimeter, access and authorization is the firewall that keeps sensitive data and infrastructure safe in the cloud. GDPR, other regulatory demands, and the escalating risk of cybersecurity incidents, combined with the adoption of dynamic cloud platforms for digital transformation initiatives, has created the perfect storm for Enterprise security and compliance teams.

To overcome cloud access and authorization security risks, and assure regulatory compliance in a controllable and cost-effective manner, organizations require a new solution for access governance.

The Orkus Access Governance Platform, powered by Graph AI, is the next generation of cloud access governance. Orkus delivers the automated, intelligent, real-time access governance required to secure sensitive cloud data, critical infrastructure assets, and privileged identities in the cloud.

For more information visit www.orkus.com or reach us at sales@orkus.com

About Orkus

Founded in 2017 by cloud and cybersecurity experts, Orkus has solved the most critical, hard-to-manage risk vector that Enterprises face today in hybrid cloud computing—securing access to data, applications, and infrastructure. The Orkus Access Governance Platform builds a real-time graph that connects identities, data, applications, and infrastructure; and continuously learns, monitors and secures access and authorization for your hybrid cloud. The Orkus Access Governance platform enables companies to prevent malicious and accidental data exposure, tighten privileged identity access, and stop insider and external cyber threats. Orkus is privately held company based in San Jose, CA.

orkus

Orkus 1731 Technology Dr, Suite 690, San Jose, CA 95110 sales@orkus.com ph: 408.601.0417