**Security Enables Business Agility**

Software defined infrastructure (compute, storage, networking and platform services) provides world-class on-demand capabilities that can enable agility for Enterprise use cases. Because this infrastructure is created dynamically and virtually, security professionals need new methods and tooling to secure cloud workloads.

In the old data center model, physical access to infrastructure created a need for human, process-based controls to protect assets. With the move to public providers, organizations must rethink all aspects of governance and security to enable the new pace of delivery demanded by their business. Chief among these concerns are ownership, management and audit of Identity and Access Management (IAM).

**Identity and Access Management Control Objectives**

Because public cloud is designed to allow authenticated access from anywhere, special care must be taken to architect identity, authentication and access. In collaboration with some of the leading private and public sector cloud governance customers we have developed an IAM strategy that works across cloud providers, PaaS/SaaS services and even down to the instance/VM/OS level.

An effective Cloud IAM architecture will tightly balance seemingly competing priorities:

- Allow application teams to manage service accounts and IAM constructs used in securing their workloads while preventing them from modifying their own permissions and the rules by which those permissions are governed.
- Allow fast access across multiple cloud service accounts through a single control plane, while preventing the same users from authenticating directly to the cloud service provider with native credentials.
- Provision and maintain individual named user access across hundreds of cloud service accounts, and thousands of operating systems while ensuring you can proactively remove access once expired or revoked.
Best Practices for Cloud IAM

Isolate Workloads
By using the cloud service provider boundaries to set a hard blast radius for your applications; an organization will provide logical separation based on context (application environment type, data classification, compliance applicability, etc.) to apply specific policies and identity models where needed.

During a mass migration to cloud it can seem logical to bring all on premise workloads into the same small number of accounts; however, this model actually slows migration, as each application that moves successfully creates additional barriers (in terms of access and change control) that makes it harder to move in the next workload.

As teams further mature and start developing cloud native capabilities, this change control is further compounded by the use of platform level services. E.g. who administers serverless capabilities when you have ten teams in the same account all deploying applications to the same serverless environment?

Isolation of workloads solves both issues. This one design pattern yields massive benefits for effective security and control while simultaneously enabling application teams’ higher levels of self-service and autonomy. Key benefits:

- **Cost Savings / Transparency**: Ability to associate 100% of specific cloud costs to an application workload, environment, cost center, or business unit. Can use account service limits to impose restrictions on a business unit, development team, or project.

- **Administrative isolation between workloads**: Administrative isolation by account provides the most straightforward approach for granting independent administrative groups different levels of administrative control over cloud resources based on the workload, development lifecycle, business unit (BU), or data sensitivity.

- **Limit visibility and discoverability of workloads**: Accounts provide a natural boundary for visibility and discoverability. Workloads cannot be accessed or viewed unless an administrator of the account specifically enables access.

- **Isolation to minimize blast radius**: Separate accounts help define boundaries and provide natural blast-radius isolation; this provides a mechanism for limiting the impact of a critical event such as security breach or account suspension.

- **Strong isolation of recovery and/or auditing data**: Businesses that are required to control access and visibility to auditing data due to regulatory requirements can isolate their recovery data and/or auditing data in an account separate from their workloads (e.g., writing CloudTrail logs to a different account).
Multi-Cloud
Automate management of enterprise identity across multiple cloud providers and across organization/account/subscription structures within cloud providers.

Role-Based Access
Establish a role-based access model that organizes permitted information system access and privileges. This model needs to evolve over time as the cloud service providers add new capabilities and revise current ones.

For ease of use and simplified permission grants, the model should have consistent naming to be easily understood without constant need to interrogate the underlying IAM policy statements.

Dynamic Provisioning
The agility of cloud comes from the on-demand access and availability of services. In this model all factors of the environment are constantly moving. Users are added, changed or removed; new services are launched; new infrastructure is dynamically provisioned; new projects are started. To be successful your IAM capabilities must have the ability to constantly interrogate the current state of access and compare that against an expected state, dynamically provisioning access as needed:

- Enforce dynamic provisioning of approved access into defined roles.
- Enforce dynamic and time-based de-provisioning of expired/revoked access.
- Provide API for external access control systems to provision and de-provision access.

Audit Logging/Monitoring
Monitor and maintain records of all activity linked to provisioning / de-provisioning and for changing rules that govern access. Provide a visual representation of current access status to humans while maintaining full audit log of who granted what access and what actions were taken for use by threat detection services and auditors.
**Federate Responsibility**
Forcing all permission grants and revokes through a central team (especially if that team is manually configuring access) greatly reduces the agility and security of your environment. Ideally you want to federate responsibility for allocating access to the business owner of the data/application, within well-defined scopes of control.

**Least Privilege**
Systematize least privilege and fine-grained permission grants: Cloud service accounts should fail to a closed system. With no authoritative action taken the environment should allow minimal or no access.

Whitelist cloud services: Cloud service providers are constantly improving and adding new IaaS, PaaS, and SaaS capabilities to the environment. These features are often developer focused and require evaluation of both applicability to the enterprise, and controls for appropriate use. This process takes compliance, security and operations time to assess and develop.

Ensure the organization has control of what services are enabled within a cloud provider and in what regions/countries/locations applications can store data.

**Virtual Network Isolation**
Ensure access to public cloud resources only occurs from trusted network locations. By default, cloud services provide access via web-based consoles, APIs and often CLIs as well. The authentication model must support controls that would prevent access (even to known individuals) from outside approved network boundaries.

**Time-Based Access**
- Ensure all access to cloud providers is session-based and time limited.
- Use time-limited access grants to reduce burden of periodic access review.
- Ensure API Keys, Encryption Keys, PKI Keys used for authentication for both humans and automated system identity are rotated frequently and are automatically revoked when a user changes role or leaves the organization.

**Multi-Factor Authentication**
**Plan for multiple authorized identity providers:** whether through change in vendors, merger & acquisition, partnership/joint ventures your cloud environment will need to support multiple authoritative identity providers over time. Planning for that initially saves massive rework later and can facilitate failover in the presence of an extended downtime from a single identity provider.

**MFA:** Ensure that human access to cloud portals, APIs, CLIs and Operating Systems is linked to a known enterprise identity and that the user associated with that identity has asserted it with at least two different identity factors.
**Separation of Duties**
Enable separation of duty between those authorized to manage cloud-based resources and those authorized to grant or change access levels and permissions.

By separating and creating a firm boundary between these administrative roles, you ensure auditability of your environment at any time and when an access breach is created this prevents the attacker from elevating their access and laddering up to attack other resource within the environment.

**Ensure Effectiveness of Controls**
Implement automated preventative, detective and corrective controls to ensure all company IAM policies are in place and effective.

Most traditional models only employ change at the moment access is added, removed or changed, and assumes that no change is coming from outside the access control system. Constantly monitoring current configuration of access controls against what is expected and having the capability to implement automated actions to correct, will identify and prevent unauthorized out of band changes.

**Ensure transparency**
At any point in time, your organization needs to visualize who can take what actions, to which resources, when, and for how long? This view must be consistent across public cloud, OS, DB and SaaS and it should allow for federation of responsibility for granting and removing access to the organization or individuals that hold the accountability.

Understand behavior of resources and users -- who is doing what, how are my resources changing over time? Full audit trail for security & compliance with detailed logs for visibility and easy troubleshooting.

- Complete version control of configuration drift -- see what's changing by who and when.
- Ability to filter all discoverable resources up and down your hierarchy.
- Ability to search quickly any configuration item and metadata to find resources or visualize inventory.
- Time Series of events per resource to follow the change history.
- Event logs coupled with context and debugging information provides valuable logs that describe the event, what was going on, details on the environment and actor, and transparency to logic of guardrail actions.
About Turbot

Our mission at Turbot is to unlock the value of public cloud for enterprises through innovation, insight and speed. Turbot has built a strong brand and reputation by hiring the right people, continually innovating and enhancing the product, and providing unparalleled customer service.

Turbot’s engineering and product teams bring decades of combined experience enabling cloud strategy for the largest global companies (including highly regulated entities in Lifesciences, Healthcare, Financial, and Technology industries). Our Software Defined Operations Platform delivers over 1600 configurable guardrail policies specifically tailored to enterprise security and operational needs, all aligned to best practices.

Contact Us

Email: info@turbot.com
Twitter: @turbothq
LinkedIn: linkedin.com/company/turbot
Phone: +1 973 922 0297
Address: https://turbot.com

Turbot HQ, Inc
1732 1st Ave #20232
New York, NY 10128 USA