Software Defined Operations: Security Guardrails for your Cloud
Introduction

Turbot believes that public cloud (IaaS and PaaS) presents a clear transformational shift for Enterprise IT. That transition enables greater agility, faster delivery of services, and cost benefits by allowing developers and DevOps staff to directly provision services without relying on a central IT team. This change requires a new approach for security, operations, planning, migration, and service transition of cloud platforms because the traditional gates have been eliminated through this on-demand delivery model.

The teams executing the change also need new skills and tools to ensure that the company’s security and compliance governance is maintained. In order to balance speed and agility with compliance and governance, guardrails are needed to ensure that teams can achieve maximum speed while “staying on the road”. The result of this transformation will be an IT organization dedicated to the practice of Software Defined Operations (SDOps) – the automation of networking, operations, security, and compliance - as the new way of working with their Software Defined Infrastructure.

Security Enables Business Agility

Software defined infrastructure (compute, storage, networking and services) offers a vast and powerful chest of tools, and security professionals need new methods and tooling to secure workloads in the cloud. In the old data center model, physical access to infrastructure created a need for human, process-based controls to protect assets. These barriers have been eliminated in the cloud model; Innovative organizations are using Software Defined Operations to replace manual processes (e.g. approval, ticketing, deployment) with controlled automation to foster the new pace of delivery. This is the key to unleashing the agility of IT. And with this model, maintaining governance and consistency is key to an organizations overall success.
Security Roles in the New Model

**Security Architects** define the guardrails (automated detective, preventative and corrective controls) and document common patterns to accelerate application teams.

**SecOps** and IT Ops define in advance how they will respond to incidents and events, programatically taking action within seconds of detection. These automated responses don’t just send notifications, they should also take predefined actions to fix or remove the risk.

**Turbot: Fully Automated Guardrails for Agility and Control**

Turbot’s automated guardrails are the cornerstone technology for Software Defined Operations, enabling consistent, repeatable operations management. Turbot ensures that governance to policy is consistently applied, enabling continuous compliance. Traditionally, organizations apply the “Report, Analyze, React” model, Turbot eliminates the need for slow and costly manual processes. Turbot applies real-time guardrails to allow teams to achieve agility in the cloud, while ensuring your cloud is secure, compliant, scalable, and cost-optimized – Always.

Guardrails utilize a robust hierarchical policy engine that gives the enterprise control at higher levels of the hierarchy, and the flexibility to create exceptions for workloads on an account by account basis (or even at the resource level). This resolves much of the friction that is caused by “one-size fits all” models that are typical of cookie-cutter approaches to cloud security.
Some key examples of how Turbot guardrails can specifically be used to accelerate your cloud strategy and secure your environment:

**Services Whitelist:**
- Specify whitelisted cloud services based on workload types (e.g. GxP, HIPAA, PCI)
- Enforce least privilege and discovery of application needs by requiring that teams explicitly turn on the services they need as part of the deployment and testing processes.
- Specify allowable Regions for services (e.g. Only permit EC2 or Azure Compute in the USA and UK)

**Network & Firewall Management:**
- Application isolation; automate consistent and secure network constructs and security groups for predefined patterns (e.g. DMZ, intranet only, sandbox)
- Enforce lockdown of network and security groups to foster best practices, isolate workloads, and foster discovery of network usage
- DNS record management through customer defined schemes
- Automate and enforce “north-south” and “east-west” firewalls

**Operating System, Database & Data Protection:**
- Enforce use of specific AMIs and AMI publishers
- Enforce use of specific DB engines
- Enforce enterprise security hardening (e.g. CIS) on VM images
- Enforce custom application specific configurations
- Manage OS users, groups, and SSH keys
- Manage DB users, groups and passwords
- Automate snapshot and data retention policies
- Automate and enforce implementation of encryption policies

**Security & Encryption:**
- S3 Default Encryption & Encryption at Rest, Storage Account Encryption
- Define the minimum level of encryption required for EC2 or Compute volumes
- Prevent anonymous access to S3 buckets and public access to Storage Containers

**Cost Management & Organization:**
- Budget-setting for migration test accounts
- Cost allocation & show-back for application migration testing
- Auto-stop instances on a schedule
- Clean-up unallocated volumes, log & snapshot rotation
- Enforce tagging, and specify tag templates
- Automated CMDB updates
Identity and Access Management:
- Consistent identity management across AWS, Azure, GCP, OS, DB, Turbot & SaaS
- Full stack audit trail of user activity
- Active Directory & SAML integration
- Federation of application teams access across multiple organizations
- Time-limited privilege grants to maintain segregation of duties
- Secure audit trail of all activities, permissions grants and guardrail changes
- Simple point & click user interface to grant and track access

Automated Guardrails Maximize Value from App Isolation

One of the key “new ways of working” in public cloud is the principle of application isolation, which is best achieved through a well-architected and controlled multi-account strategy. It is recommended to deploy separate production and non-production accounts for each business service. For large enterprises (especially in regulated industries), this isolation can be difficult to manage at scale without Turbot’s automation and guardrails. By doing so, the organization gains extraordinary benefits.
Cost Savings / Transparency: Ability to associate 100% of specific cloud costs to a specific 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).

Turbot helps your cloud team be more efficient, giving it the tooling and automation necessary to manage the complexity of implementing the best practice of a multi-account strategy and allowing SecOps and DevOps teams to focus on higher-value activities. This shift to being a trusted advisor allows technologists to become more embedded in the business, being advocates for business solutions expediting time to value for new services and products.
Security Guardrails for Multi-Organization Development

Developing applications collaboratively creates unique challenges for security teams. Business partners faced with weeks or months of project delays often resort to starting application development offsite with their vendor to “accelerate” the project. Late in the project they discover that key enterprise controls were not considered part of the requirements, causing delays, rework and political battles.

Turbot allows you to turn this paradigm upside down: Utilizing native cloud services (e.g. the AWS, Azure, and GCP Console and APIs) in conjunction with Turbot’s enterprise controls, the system integrator or third parties can be granted access to a cloud account before the ink is dry on their statement of work. This account will be fully managed by automated guardrails configured to meet enterprise policies. Turbot’s guardrails ensure that the project team develops the application under full enterprise policy management, with federated authentication and access to core corporate resources (e.g. AD, DNS, NTP, Version Control, Databases & APIs) so that Development truly matches Production.

Out-of-the-Box DevSecOps

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 1500 configurable guardrail policies specifically tailored to enterprise security and operational needs, all aligned to best practices.

Turbot also provides mappings for guardrails options to common control frameworks and regulatory requirements (NIST, GxP, HIPAA, PCI, GDPR). During our Kick Start Program, we will work with you to configure the guardrails to meet your enterprise security and compliance framework.
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.

Contact Us

Email: info@turbot.com
Twitter: @turbothq
LinkedIn: https://www.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