Software Defined Operations: Security Guardrails for your Cloud
Introduction

Enterprises are increasingly embracing public cloud (IaaS & PaaS) as a production hosting environment on par with their on-premises capability. Those on the cutting edge are even adopting strategies to make their Virtual Private Cloud the first (or only) choice:

These companies are choosing public cloud to differentiate themselves in a competitive landscape that disproportionately rewards those who can harness large-scale data, machine learning, AI and IoT to drive their business. IT agility is quickly becoming the metric for companies that plan to survive the next wave of innovation, and public cloud strategies allow traditional enterprises to leap-frog current incremental IT improvement strategies and immediately start realizing next-generation benefits:

- **Transparency:** IT is no longer one giant cost center. Know how much each application, or even each transaction, costs your business.
- **Scalability:** Cloud scale dwarfs even the largest Fortune 100 companies’ computing and storage needs.
- **Reliability:** Architect and scale for your workload’s needs, from 4 to 11 “9s”.
- **Business Agility:** Get on-demand provisioning and termination of infrastructure with no capital investment. Public cloud reduces the cycle-time and cost penalty for today’s Try -> Learn -> Iterate business models.
- **Security:** In public cloud, security becomes a pre-requisite to enabling strategy. The security professional must adapt from being “back-stage” to being “on-stage,” or risk quickly becoming obsolete.
Security Enables Business Agility

Turbot believes that public cloud (IaaS and PaaS) presents a clear transformational shift for Enterprise IT. This change requires a new approach for security, operations, planning, migration, and service transition of cloud platforms. The teams executing the change also need new skills and tools. The result of this transformation will be an IT organization dedicated to the principles and practice of Software Defined Operations (SDOps) as the new way of working with their Software Defined Infrastructure.

Software defined infrastructure (compute, storage, networking and services) offers security professionals a vast and powerful tool chest to secure workloads. In the old, data center model, physical access to infrastructure created a need for human, process-based controls to protect assets. Innovative organizations are using Software Defined Operations to replace manual processes (e.g. approval, ticketing, deployment) with controlled automation. This is the key to unleashing the agility of IT.

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, programmatically 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.
Maximizing Value from Application 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. For large enterprises (especially in regulated industries) Turbot recommends deploying separate production and non-production accounts for each business service; 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 a multi-account strategy and allowing SecOps and DevOps teams to focus on higher-value activities.
Turbot: Guardrails for Agility and Control

Turbot guardrails are the cornerstone technology for Software Defined Operations, enabling consistent, repeatable operations management. 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:

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.

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
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

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

Cost Management:
- 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
Security 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 Console and APIs) in conjunction with Turbot’s enterprise controls, the system integrator can be granted access to a cloud development 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 combined 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).

Out-of-the-Box DevSecOps

Turbot’s engineering and product teams bring decades of combined experience enabling cloud strategy for the largest multinational companies (including highly regulated entities in Lifesciences, Financial and Technology industries). Our Software Defined Operations Platform delivers over 600 configurable guardrails specifically tailored to enterprise security and operational needs.

Turbot also provides mappings for guardrails options to common control frameworks and regulatory requirements (NIST, GxP, HIPAA, PCI). As part of a typical 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