Solution Brief

Five Critical Endpoint Security Requirements During Cloud Migrations

CONTENTS

Introduction

Cloud migrations are among the more complex exercises faced by IT and infrastructure teams. Public clouds, private clouds, and hybrid clouds all have different configurations and tooling. There are differences in networking, security models, access controls, and many other areas. Moving from one cloud setup to another can take months of planning and preparation. The wholesale changes during migrations can negatively impact security postures. During the transition, the enterprise has a massively expanded attack surface of two cloud architectures with many moving parts that may or may not be properly locked down. Setting up cloud configurations for both security and stability remains challenging, in spite of excellent tools to verify cloud security offered by the various public cloud vendors.

Migrations also underscore the requirement for rock-solid endpoint security before, during, and after migration processes. The endpoints topology over the average enterprise has skyrocketed over the past decade. While the number of devices per employee has remained largely the same — between two and three — the number of connected systems across IoT, smart peripherals, video conferencing and video systems, and other IP-connected devices has climbed steadily, reaching into the tens of billions globally. Consider that the average worker may only have two primary devices (smartphone, laptop) but more and more also use Bluetooth headsets and keyboards, smartwatches, fitness trackers, networked printers, smart speakers and more — each potentially offering a secondary path into privileged environments. Workers are accessing sensitive enterprise systems from a wider array of network endpoints (WiFi, 5G, etc.), both public and private, and some of those access points may be open and lightly secured. The number of cloud-based endpoints with public IP exposure has also skyrocketed; this number is particularly challenging to tally and monitor due to the nature of containerized ephemeral infrastructure with cloud deployments in e.g. Kubernetes.

Beyond these systemic risks, environmental risks that are particularly prominent now heighten endpoint risk during cloud migrations.

- **Increased security risks due to an unstable political environment:** ongoing political conflicts frequently spill over into cyberspace. More criminal actors and government-sponsored advanced persistent threat groups (APTs) are active and seeking to breach enterprise systems for financial and political gains.
- **Rapidly expanding attack vectors (e.g. RaaS):** the diversity and number of published attacks continue to grow quickly. Published vulnerabilities are transformed into attack playbooks in a matter of days. Advanced cyberattack capabilities are now offered on an "as-a-Service" basis, just like regular software such as Customer Relationship Management (CRM) or design tools.
- **Expanding attack surface due to hybrid work models:** the now permanent shift to hybrid work extends the attack surface by forcing IT security to cover network connectivity and diversity over which they have little to no control.

Security Requirements for Cloud Migrations

For all the reasons cited above, endpoint security and cloud security have converged as enterprise endpoints and related IP-enabled devices are more tightly woven into cloud-based infrastructure and applications. IT and security teams planning a cloud migration need to build a plan for their migration path. There are five key requirements any effective and secure cloud migration plan should take into account for ensuring continuous endpoint security.

1

A Clear Understanding of Your Cloud Computing Model (Private, Public, Multi-Cloud, Hybrid)

Migrations can take many forms. Migration may be from one public cloud to another, from a public cloud to a private or hybrid cloud, or from one public cloud to two public clouds for different applications or geographies. The first step in any effective endpoint security policy and practice during a cloud migration is to have detailed insights into what the cloud computing model looks like right now, what it will look like after the migration and all the intermediate steps in between. This is essential because during the transition, mapping endpoint protection measures to cloud infrastructure is challenging and a potential point of massive security failure.

2

Complete Visibility Into Endpoints on Your Network

During the migration, it is absolutely essential that IT and security teams have comprehensive, accurate, and up-to-the-hour visibility into the status, location, ownership, and state of endpoints accessing enterprise networks. This means being able to work in multiple directions quickly with simple queries that anyone can execute to deliver the following parameters:

- Mapping an IP, NIC, or MAC address back to an asset and owner, location, business unit, and set of privileges
- Looking up an individual and seeing their devices and endpoints
- Identifying anomalous behavior and associating that behavior immediately with all the assets that can be affected by or exposed to the behavior
- Identifying all assets and endpoints that are out of compliance with required and recommended endpoint protection policies such as encryption, running anti-malware software, etc.

3

Well-Defined Access Controls

This is particularly important if the migration is in a public cloud, where multi-tenancy can allow other entities to scan and breach unsecured cloud instances and storage buckets. Role-based access controls are likely in use at most enterprises. Cloud migrations should trigger a reevaluation and reconfiguration of access controls to optimize security postures and enforce "least privilege" access to everything in the cloud as well as access to networks and even private hosted servers and storage arrays.

4

Well-Defined Responsibilities for Device Types

This is closely related to access controls but is more focused on IoT assets and endpoints, most of which are not general computing platforms. For this reason, least privilege may be more static and easier to determine and enforce. Ideally, device types will be accurately marked in the ITAM, MDM, UEM, and any other system used to monitor, track and secure endpoints. However, keeping device responsibilities updated and accurate in technology databases does require constant checking and tuning of responsibilities. For any cloud migration, the IT team should do a device accountability audit and redefine all responsibilities accurately prior to launching the migration. Once the migration is complete, they should conduct a second quick audit.

5

Continuous Tracking and Management as Assets Move Through Their Lifecycle

This is a general rule for managing technology, cloud migration or not. Continuous tracking and management of all assets at every point in their lifecycle is harder said than done. However, comprehensive tracking and management is a foundational piece of all security efforts. Performing granular, enterprise-wide tracking and management can be challenging. Different asset and management systems tend to be siloed and different teams manage different types of assets. Coordination across functions — between operations, IT, security, networking, and HR, for example — tends to take place in email or chat, or is confined to rigid workflows hard-coded in during system setup and integration. For truly continuous tracking and management, IT and security teams must break down the silos and enable all roles that need the information to build workflows pushing data to and from their systems of record. The technology management system must reconcile data across endpoint management and related systems. Ideally, this tracking should happen in near-real-time, with increments of 30 minutes or less.

Enterprise Technology Management for Endpoint Security in Cloud Migrations

To address challenges to endpoint security during cloud migrations, a comprehensive, holistic Enterprise Technology Management (ETM) solution is the best option. Mobile Device Management and Unified Endpoint Management solutions are necessary but not sufficient; they remain siloed and hard to integrate with other critical systems required for security planning, management and response.

Modern, holistic ETMs are meta-systems that connect all point solutions used for different lifecycle tasks to create a single system of record, management, orchestration, and compliance. What makes ETM so powerful is a bi-directional aggregation, publishing, management, and orchestration layer that works across all departments in an enterprise. ETMs take data from mobile device management (MDM), configuration management database (CMDB), software asset management (SAM), IT asset management (ITAM), human resource information systems (HRIS), enterprise resource planning (ERP), and security sub-systems with relevant information about asset lifecycle, status, and usage and create a single data record source for IT information.

With rich APIs and extensible connectors, ETMs can power workflows that automate key IT-related processes. Unlike point solutions for endpoint management or even UEMs, ETM systems are designed to ingest and clean API data from numerous sub-systems and then present a unified, accurate, and trustworthy view of every IT endpoint and associated system. In addition, modern ETMs are agentless (collecting data via other installed agents) and require minimal integration work. This flexibility and extensibility are crucial for addressing the full spectrum of lifecycle challenges because new classes of technology infrastructure appear continuously.

For full lifecycle tracking and orchestration, ETMs can deliver the following capabilities:

Full-lifecycle tracking
Designed for extensibility and agility, ETMs easily integrate with OEM and distributor systems to start asset tracking from the moment the PO is signed. By connecting across all the sub-systems, ETMs can follow the status and path of any endpoint from provisioning to refresh to retirement.

Compliance and auditing automation
By crossing silos and enabling comprehensive near-real-time tracking, ETM can deliver repeatable playbooks for compliance and auditing of IT infrastructure.

Enhanced IT security
Because ETM discovery is ongoing and agent-less, security teams can continuously survey their IT landscape for potential risks and anomalies such as lack of encryption, lack of endpoint protection, or anomalous behaviors. Part of this discovery is enabling security teams to remain abreast of all security processes required to improve the security stance at each lifecycle point in an endpoint's journey.

For cloud migrations and endpoint security, ETM offers the following benefits:

Aggregation of all endpoint data across hardware and software, and all cloud instance types (SaaS, PaaS, IaaS)
Modern ETM captures all data and puts it into a single database and reporting structure. The ETM updates data roughly every 30 minutes (this is configurable) and continuously reconciles for accuracy. This enables security teams to quickly verify that cloud migration processes are not creating security holes or configuration errors.

Complete visibility
ETM makes it easy for IT and security teams to see what is happening with endpoints at any level, based on individual users, anomalies, business groups, assets types, SKU, software packages, container images, and more. As a database of record for endpoint data, ETMs can fire off automated reports or populate visual dashboards to help IT and security teams view all relevant information at a glance or quickly query for specific data.

Enforcement of access roles and device responsibilities
ETM can flag violations of access policies and anomalous device responsibilities, kicking off remediation steps and workflows to properly secure any endpoint under management.

Conclusion: ETM is A Critical Piece of Secure Cloud Migrations

Change brings risk. Cloud migrations are periods of rapid and extensive change. Moving clouds mean changes to many moving parts, from configurations and subnets and IP addresses to namespaces and load balancer instances, all of which might require subtle but important changes for cross-cloud porting. ETM provides a means to continuously verify what endpoints are exposed to enterprise networks and cloud infrastructure, the security and activity status of those endpoints, who or what system owns them, and the responsibilities and access privileges to which they are entitled. By relying on existing agents, ETMs can aggregate information from numerous sub-systems related to endpoint management and present a unified substrate. With this unification, IT teams can easily count and validate all endpoints accessing networks prior to migration and remediate anomalies and risks showing up in this count. As migrations proceed, ETMs can verify that devices are configured and secured properly, reducing risks from shifting clouds This gives IT teams, CISOs, CTOs, and CIOs an easy and highly-configurable solution for reporting on and monitoring cloud migrations to improve overall enterprise security.

About Oomnitza

Oomnitza offers the industry's most versatile Enterprise Technology Management platform that delivers key business process automation for IT. Our SaaS solution, featuring agentless integrations, best practices and low-code workflows, enables enterprises to quickly achieve operational, security and financial efficiency leveraging their existing endpoint, application, network infrastructure and cloud infrastructure systems. We help some of the most well-known and innovative companies to optimize resources, mitigate cyber risk, expedite audits and fortify digital experience.

Learn more at Oomnitza.com.

oomnitza