TD SYNNEX

Cloud Security Handbook

02.14.2022

Intro

How to Take a Security-First Approach to Cloud Migration

Cloud adoption was on the rise well before 2020, and it's only accelerated as organizations seek greater agility and resiliency. Gartner now predicts that "enterprise IT spending on public cloud computing... will overtake spending on traditional IT in 2025."[1]

The cloud offers great promise...and new risks. Organizations find promise in having better protection over a greater portion of their security surface and dynamic intelligence that enhances threat detection and response.

But, as organizations plan their move to the cloud, they face a stark problem: the security practices built for their on-premises environments are no match for a software-based, tightly integrated cloud environment.

The challenge for organizations is to evolve their people, processes and technology stacks and take a security-first approach as they shift to cloud computing.

[1]Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025. Gartner. Feb. 9, 2022.
[2]Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences. Gartner. Nov. 11, 2021.

By 2025, over 95% of new digital workloads will be deployed on cloud-native platforms, up from 30% in 2021[2]

On-prem vs Cloud Security

3 Ways On-Premises Security Differs from Cloud Security

In an on-premises datacenter, you own security for the entire stack. However, this changes as you migrate to the cloud, making the differences between on-premises security and cloud security more profound:[3]

1 Shared responsibility model

All cloud service providers (CSPs) share responsibility for cloud security with their customers, but not all CSPs share the same model. Your agreement should clearly spell out who is responsible for what.

2 Software-based

Another major difference is that everything in the cloud is software-based, creating unique requirements for controls and processes, along with potentially new tools and services to meet security objectives.

3 Governance

Finally, governance workflows in the cloud will be much more dynamic and integrated and involve many more stakeholders, which will require considerable modification to on-premises workflows.

By shifting some responsibilities to a CSP, organizations can better protect their entire security surface, while reallocating in-house resources to higher value business priorities.

[3] Migration Security Considerations and Challenges. TechTarget.com. Nov. 24, 2021.

Shared Responsibility

Who Is Responsible for Security?

It's not an easy answer. Make sure to understand the shared responsibility model and CSP agreement. Regardless of cloud deployment type, you will almost always be responsible for securing your account, identities, devices/endpoints, and data. If you're not sure, ask your CSP to clarify. Here's a typical shared security arrangement (your CSP agreement may vary).

	On-Premises	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Examples	• Physical network • Infrastructure • Hypervisor • Virtual network • Operating systems • Firewalls • Service configuration • Identity and access management	• Microsoft Azure • Amazon Web Services (AWS) • Google Compute Engine (GCE) • IBM Cloud	• Amazon Web Services (AWS) Elastic Beanstalk • Oracle Cloud Platform (OCP) • Google App Engine • Microsoft Azure • Salesforce PaaS • Red Hat OpenShift PaaS • IBM Cloud Platform • SAP Cloud Platform	• Microsoft 365 • Google Workspace • Salesforce • Cisco WebEx • HubSpot • DocuSign • Zendesk • Slack • Dropbox
Account	Customer	Customer	Customer	Customer
Identities	Customer	Customer	Customer	Customer
Data	Customer	Customer	Customer	Customer
Endpoints	Customer	Customer	Customer	Customer
Data	Customer	Customer	Customer	Customer
Apps	Customer	Customer	Customer	Service Provider
O/S	Customer	Customer	Service Provider	Service Provider
Runtime	Customer	Customer	Service Provider	Service Provider
Middleware	Customer	Customer	Service Provider	Service Provider
Virtualization	Customer	Customer/ Service Provider	Service Provider	Service Provider
Servers	Customer	Service Provider	Service Provider	Service Provider
Storage	Customer	Service Provider	Service Provider	Service Provider
Networking	Customer	Service Provider	Service Provider	Service Provider

Migration Tips

5 Tips for a Secure Cloud Migration

1 Assemble the right team

Make sure that anyone impacted by a migration—decision makers, IT specialists, security managers, legal advisors, etc.—has a place at the table. If the IT team lacks the needed skills, consult external security experts for help.

2 Build a migration plan

Migrations are notoriously complex, making careful planning essential. A solid plan addresses the migration strategy, cloud type, which apps and data will be moved and how, who will be involved when, and how risks will be managed. It should also include provisions for:

- Adapting existing on-premises security policies to the cloud and adopting industry best practices.
- Evaluating which regulatory requirements apply to your data so you can avoid penalties later.
- Performing an application rationalization to determine which applications should be kept, replaced, re-platformed, retired or consolidated.
- Inventorying all licensing, maintenance and support contracts to determine migration timeline and priority.
- Discovering and mapping application dependencies to determine the best migration approach.

Assessing the value of legacy apps and equipment is crucial to this process. Some apps may not be easily migrated to the cloud and may run better on upgraded on-premises infrastructure. Some on-prem infrastructure may be more “friendly” to the cloud. Often, leaving legacy systems behind and starting fresh can help standardize and simplify your infrastructure and accelerate the migration—providing greater business agility. Assessing the value of upgrading (or not) is critical to migration planning.

Migration Tips Cont.

3 Understand the shared responsibility model

Make sure to go over the agreement thoroughly with your CSP to understand your shared responsibilities.

4 Encrypt all data

Encrypt data both at rest and in transit using secure protocols, such as HTTPS, to ensure security on-premises and in the cloud. Using a zero trust framework from the start, for example, ensures that security is built in, not tacked on later. With zero trust, data is encrypted at rest and in transit and access to that data is also protected through authentication and authorization.

5 Keep communication flowing

Clearly discuss goals, requirements, and issues throughout the process with migration team members to minimize downstream risks and maximize success.

Workload Prioritization

3 Steps to Prioritize Migration Workloads

GOAL

Identify, prioritize, and move workloads over to the cloud in order by least disruptive to greatest disruption to the business

STEP 1

Intermittent Workloads

Start with applications that run periodically and pose the least operational risk to your organization, such as seasonal applications, sales demos, training labs, etc.

STEP 2

Low-Risk 24/7 Workloads

Next, migrate the low-risk applications that run 24/7 but that typically wouldn't disrupt normal business operations.

STEP 3

Business-Critical 24/7 Workloads

Finally, migrate mission-critical applications that run 24/7 last. These applications require the utmost technical expertise to minimize business disruption.

> From a security perspective, we could be in for a wild ride in 2022 as enterprises continue to move systems and workloads haphazardly to the cloud without taking proper security measures...one word of advice: incorporate security into your cloud migration. It is easier to plan than it is to backtrack." [4]

[4] *Cloud Migration Has Ended Enterprise Datacenter.* SecurityBoulevard.com. Feb. 10, 2022.

Workloads to Move Now

Workloads to Move to the Cloud Right Now

To take advantage of agility, flexibility, and scalability, Gartner suggests prioritizing these workloads for migration to the public cloud—if they're not already there.[5]

1 **Mobility**
Having mobile devices and associated applications—laptops, tablets, smartphones and other endpoint devices—in the public cloud are key to a work-anywhere model.

2 **Collaboration and content management**
Microsoft 365, Cisco WebEx, iWork, and other enterprise applications help engage remote workers and enable them to collaborate. These should be moved into the cloud for optimal flexibility.

3 **Videoconferencing**
From informal meetings with colleagues to sealing global deals, videoconference technologies consume considerable bandwidth and should be moved to the cloud.

4 **Virtual desktop infrastructure (VDI)/desktop virtualization** – Cloud-based VDI solutions enable employees to access their applications and documents from any location, easing the management burden on IT teams.

5 **Scale-out applications**
Hyperscale cloud environments make cloud the preferred environment for hosting applications with variable usage or scale-out requirements.

6 **Backup and disaster recovery**
By providing failover in case of disruption and keeping critical data secure and easily recoverable, the cloud provides far more business resiliency than does tape or legacy backup solutions.

7 **Business continuity solutions**
Cloud environments are much more resilient and offer better availability guarantees than what most private data centers can provide.

[5]7 Workloads that Should be Moved to Cloud Right Now. Gartner. Nov. 25, 2020.

Outsourced Experts

One Last Thing: Consider Outside Expertise

Managing the transition from on-premises to cloud requires seasoned cloud and security expertise already in short supply. If you already face challenges finding the right resources to manage and run your on-premises environments, you'll likely face challenges finding the right skills for a successful cloud migration.

Consider extending your IT team with outsourced cloud migration and security experts who can safely accelerate your transition to the cloud. After all, cloud migration shouldn't be an "after-school project."

[6] 4 Must-Have Technologies That Made the Gartner Hype Cycle for Cloud Security, 2021. Gartner. Sept. 8, 2021.

Cloud-first strategies are now common, even among risk-averse organizations. However, execution remains impeded by a lack of necessary skills and tools to ensure secure cloud computing deployments.

We're Here to Help...

If your IT team is challenged trying to manage a complex IT environment, let us help you add value with managed security services offerings.

We're backed by a team of dedicated security consultants with the expertise and resources to ensure your migration goes smoothly and your cloud environment is secure.

Contact us at MSPsecurity@techdata.com to find out more.