EBOOK

5 Things You Might Not Know About Cloud Security

Though cloud providers offer help, the cloud comes with security challenges too often overlooked

INTRODUCTION

The Cloud: False Assumptions Create Unnecessary Security Risks

Many organizations underestimate the security risks of the cloud, often assuming their cloud provider will take care of any issues. Unfortunately, they won't.

It's been 15 years since Amazon Web Services launched the first cloud infrastructure platform. At the flip of the switch, you could fire up a data center without having to buy any hardware or bury capital.

But initially many companies eyed the cloud with suspicion. Leery of losing control, they held tight to running their own data centers. They thought the cloud was risky.

Over time, the value of the cloud proved too compelling to ignore. Today, nearly every business uses the cloud to one degree or another. And many organizations rely on the cloud to host critical operations — unthinkable a decade ago.

While the cloud has provided far-reaching benefits, its risks and challenges remain. Enforcing comprehensive, Zero Trust security in the cloud is just as important as it is for any other part of your digital infrastructure.

The biggest problem? Organizations often do not fully understand the ways that their cloud infrastructure exposes them to cyberattacks and ransomware.

This ebook examines **five false assumptions** about cloud security that could put your organization at risk. By understanding the truth behind these assumptions, you'll take an important step toward improving your cloud security.

Enforcing comprehensive, Zero Trust security in the cloud is just as important as it is for any other part of your digital infrastructure.

Assumption #1

Your Cloud Provider Is Responsible for the Security of Your Applications

If not your cloud provider, then who is responsible for cloud security? The truth is that security is a shared responsibility.

Whether you're working with Amazon, Microsoft, Google or any other cloud vendor, if you look at the fine print, you'll see their security responsibility is limited to protecting just the network fabric — that is, everything that makes up their hosting environment.

Application security is still your responsibility. As soon as you deploy an application instance with an operating system on top of the cloud network, protecting it is your job, not theirs.

Further, cloud security support from vendors uses a "best effort" model, not service-level agreements (SLAs). This means cloud providers need only promise to do their best to protect you from network-born threats like distributed denial of service (DDoS) attacks. But if one gets through, well, they tried their best. As for protecting your workloads, that's always on you.

Also, while cloud providers will patch systems such as Linux servers that host applications, that doesn't address your potential application vulnerabilities. Without visibility at the application layer, you can't know whether an application has been deployed or configured properly.

Assumption #2

Cloud Security Is Easy to Manage

The cloud's benefits — speed, agility and elasticity — actually make cloud security more difficult. That's because the cloud lets virtually anyone in your organization spin up a new application or resource with just a few clicks of their mouse.

Making things even more difficult, few organizations centrally manage cloud services within their IT and security teams. Instead, various business units and groups can independently set up new cloud accounts.

In other words, any user or developer with access rights can create applications that have open ports to the Internet, where anything can communicate with anything. And this all can happen without IT or security even knowing these applications exist, let alone securing them.

Moreover, large companies often have hundreds of cloud accounts on AWS, Microsoft Azure, Google Cloud and other cloud platforms. Each of these accounts may have many virtual private clouds with their own security groups.

All this makes managing those groups and understanding their security exposure increasingly difficult. It would help to have tools for visualizing the application traffic to and from cloud environments, but typically, cloud providers don't offer them.

Assumption #3

Cloud Services Are Isolated From the Internet

To help customers make the most of their investments, cloud vendors provide their customers with infrastructure as a service (IaaS) and platform as a service (PaaS) infrastructure resources. These can include virtual machines, containers, serverless functions and managed cloud databases.

But these cloud services can be open to the Internet, often by default. That means they are points of entry for a potential breach. Limiting their access is the responsibility of the customer, not the cloud provider.

Remember, the cloud is not “least privilege” by default. Instead, it operates on “excess privilege.” This means you need to first determine which resources can communicate with each other, then block everything else.

Without visibility into which applications are in the cloud and what’s communicating with them, you could be hosting critical resources in the cloud without adequate controls. This is especially dangerous if you have workloads and process functions in the public cloud that are exposed to internal data center resources.

To ensure good cloud security, you must understand the communication paths among your cloud and on-premises workloads. Just as you do with the data center, you need to know exactly what’s connected to the Internet. Then you should ensure that these connections don’t become paths for hackers or malware to enter your network.

Without visibility into which applications are in the cloud and what’s communicating with them, you could be hosting critical resources in the cloud without adequate controls.

Assumption #4

There Are No Limits to Scaling Cloud Services

From a security standpoint, public clouds like AWS and Microsoft Azure limit the number of segments that can be created to manage security. This prevents you from achieving fine-grained control of your cloud applications and data.

The cloud providers' answer to segmenting is the virtual network segment — in the case of Amazon, the Virtual Private Cloud (VPC), and in the case of Microsoft, the Azure Virtual Network (VNet). For these environments, security groups create the perimeter both in and out of the segment.

But the number of security groups that can exist in a virtual network segment is limited. If you need more than the limit, you must use multiple hosts in a segment. But to scale efficiently, every segment should have only one host. Multiple hosts on one segment generate greater management complexity.

Also, multiple hosts on a segment create greater security risk. If one host is breached, you don't want it talking to (and possibly infecting) another host.

To scale, you'll need additional help beyond what your cloud providers offer for segmenting access. Otherwise, you'll face the same problems organizations have encountered with traditional data center segmentation: poor visibility, complex policy management, and the need to manually "rewire" network configurations and firewalls.

Assumption #5

Once You Secure a Workload, Your Work Is Done

When people think about workload security, many mistakenly assume their workloads stay in one place.

But in the cloud, your workloads can move across multiple public clouds, with each having its own policy model. When that occurs, it's unlikely the security segments will share the same security controls. And even if they do, your security team must constantly monitor this movement to ensure the workloads are protected by appropriate policy.

Remember, all compute resources, serverless resources and objects in the cloud are dynamic. And as these resources and cloud objects move, their IPs change, too. These resources may change where they reside inside a public cloud. They can also move across multiple cloud providers. They may even "die," only to come back to life with a new IP address.

As a result, you can no longer write policy using a traditional approach. Instead, examine your cloud workloads to understand how the application components talk to one another. Once you have clear insight into your application behavior, you can then write appropriate enforcement policies.

The key takeaway is that all cloud applications, regardless of where they live or what associated resources they use, must be protected just as diligently as any application running on a server in a traditional data center.

The key takeaway is that all cloud applications, regardless of where they live or what associated resources they use, must be protected just as diligently as any application running on a server in a traditional data center.

illumio

The Cloud Is Here to Stay — and So Are Its Security Risks

As organizations both large and small consider moving workloads to the cloud, they too often leave security out of the discussion. Why? Because some teams may view security as an inhibitor that slows the business down, not as an enabler that can accelerate the business.

This creates a tough dilemma for CIOs, security executives and other technology leaders. If you can't support initiatives and applications that drive the business, you're not helping the business grow. But if you aren't managing the potential security risks the cloud presents, then you're exposing the business to serious threats.

Here's the key: Leading organizations make security planning a fundamental part of their cloud migration plan, not an afterthought.

Critically, your cloud provider only has partial responsibility for protecting your cloud-related applications and data. True cloud security rests with you.

> Leading organizations make security planning a fundamental part of their cloud migration plan, not an afterthought.

Illumio: Lighting a Path to Zero Trust

Illumio pioneered Zero Trust segmentation and leads the industry in providing fine-grained control of your digital infrastructure, down to the application and workload level.

Illumio's intelligent visibility and automated security enforcement stops lateral movement, preventing ransomware and cybercriminals from infiltrating your network, data centers and devices.

Now, with the introduction of Illumio CloudSecure, the power of Illumio is simple and easy to extend to the cloud through agentless visibility and cloud-native controls.

CloudSecure continuously monitors and protects cloud-native apps, virtual machines and containers, as well as serverless, PaaS and IaaS infrastructure.

You can now embrace the cloud with confidence.

Learn more about how Illumio can help you build stronger digital security for your multi-cloud and hybrid cloud environments.
www.illumio.com/cloudsecure

Or talk to one of our experts about how Illumio can help you build your digital defenses against ransomware and cyberattacks:
www.illumio.com/contact-sales

Copyright © 2021 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.

illumio