ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

SECURING CLOUD INFRASTRUCTURE

AWS & AZURE

How to Limit Risks When Moving to the Cloud

TABLE OF CONTENTS

A GUIDE TO SECURING YOUR CLOUD INFRASTRUCTURE: HOW TO LIMIT RISKS WHEN MOVING TO THE CLOUD

Most organizations now view the cloud as essential infrastructure, but they often adopt or expand their cloud footprint without a plan for new complexities and risks. As a result, misconfiguration and mismanagement are some of the biggest causes of successful attacks on cloud infrastructure.

To mitigate these risks and ward off attacks, IT leaders must implement a comprehensive and effective cloud security program. This guide takes a look at cloud risks, as well as the components of infrastructure-as-a-service (IaaS) security that are important to consider.

THE NEED FOR CLOUD SECURITY

Cost efficiencies, faster delivery of products and services, and improved business continuity are among the factors behind soaring cloud adoption. Today, an estimated 96 percent of organizations use at least one public cloud.[1]

95%

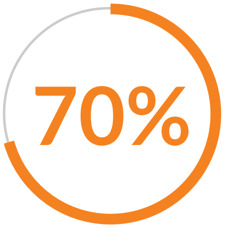
In 2021, Cloud traffic is expected to account for 95% of total data center traffic.[2]

From major organizations to small and medium enterprises (SMEs), the cloud plays a vital role in building a stronger, more versatile security posture. In today's environment, the cloud is no longer considered a frontier, but instead has become a baseline for IT operations.

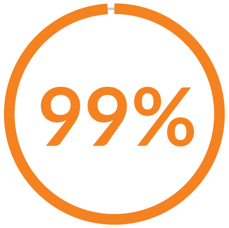
However, if the rising number of cloud breaches and incidents are any indication, security is badly lagging behind the expansion of cloud infrastructure.

BY THE NUMBERS: **CLOUD BREACHES**

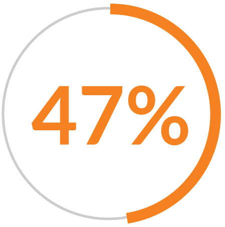
Looking at these numbers, it’s clear the cloud is where your organization needs to boost security. As the adoption of hybrid architectures and the multicloud grows, the risks will only increase.



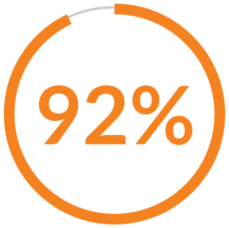
70% of organizations fall victim to public cloud security incidents each year.[4]



Up to 99% of cloud breaches are the fault of the customer (i.e., a result of human errors such as misconfigurations and mismanagement).[5]



47% of breaches include a cloud component.[6]



92% of organizations have a cloud security readiness gap.[7]

TOP CLOUD RISKS

Adoption of IaaS has grown from an estimated 62 percent in 2018 to 76 percent in 2020.[8] Here are the top risks organizations face today:

01 Data breaches

Regardless of your organization's size, this is the highest risk—and it comes with significant consequences, both in terms of the cost of mitigating the breach and the damage to your reputation. No organization can afford to lose customer trust.

Along with compromised credentials, misconfigured clouds are the leading cause of data breaches,[9] and misconfigurations increase the average cost of a breach by more than half a million dollars, to a total of $4.4 million.[10]

02 Resource misuse

Both outsiders and insiders (acting maliciously or inadvertently) can misuse cloud resources in a variety of ways, including:

- **Cryptojacking**—when insiders or outsiders mine for digital currency using your cloud resources, the resulting bill can be substantial. One way to carry out cloud cryptojacking is through unsecure (e.g., unencrypted or misconfigured) databases.
- **Unauthorized access**—both insiders and outsiders can access sensitive data and read, delete, and modify it. This is especially common when organizations lack a proper identity and access management program.
- **Insider misuse**—without firewalls and other security defenses to stop them, insiders not only have easy access to data but can also leak critical information. This may happen, for example, when employees store sensitive data in unsecure cloud storage.

03 Shadow IT

Shadow IT is not just a concern restricted to unauthorized user devices. When a development team or another department launches a project without the IT department's knowledge or authorization, sensitive data is potentially created, stored, and shared in unvetted IaaS environments.

Agility and speed are often the reasons for such shadow projects. While they might help you reach your organization's business objectives faster, such projects may compromise your IT infrastructure security.

04 Other threats

From malware and phishing to credential theft and advanced persistent threat (APT) activity, anything that can happen on premises can also happen in the cloud. Yet, many organizations don't have the same level of monitoring and protection in their cloud environment as they do on-premises.

SHARED RESPONSIBILITY FOR CLOUD SECURITY

Based on Gartner's shared responsibility model, the Cloud Security Alliance's guidelines[11] state that the responsibilities of cloud security providers (CSPs) include:

- Physical security of infrastructure
- Security of computing, storage, and network hardware
- Cloud storage security, such as backup and recovery
- Secure access to cloud resources by tenant
- Security of basic networks

Customers are responsible for:

- Security of terminals (e.g., hardware, software, and applications) accessing the cloud service
- User identity and access controls of the systems
- Data security

This means that, although you can expect your CSP to provide robust security for the underlying infrastructure, security of your data along with the secure use of the IaaS services rests with you. For that reason, you need to build an effective IaaS security program to address your cloud risks.

Looking at these numbers, it's clear the cloud is where your organization needs to boost security. As the adoption of hybrid architectures and the multicloud grows, the risks will only increase.

BUILDING EFFECTIVE IAAS SECURITY

IaaS platforms generate a lot of security data streaming in through APIs, but they don't necessarily aggregate or correlate the data.

Additionally, IaaS platforms lack security alert customization and collaboration across platforms. Even if the IaaS platform generates the data you need, you're likely to miss cloud security incidents.

To address these security gaps, you need a centralized detection and response approach for IaaS that:

01 Enables you to track security-relevant event data and generates actionable insights so you can protect your cloud workloads

02 Provides real-time detection, response, and containment for threats such as misconfigurations and vulnerabilities

03 Boosts your security posture and improves regulatory compliance

CLOUD SECURITY POSTURE MANAGEMENT

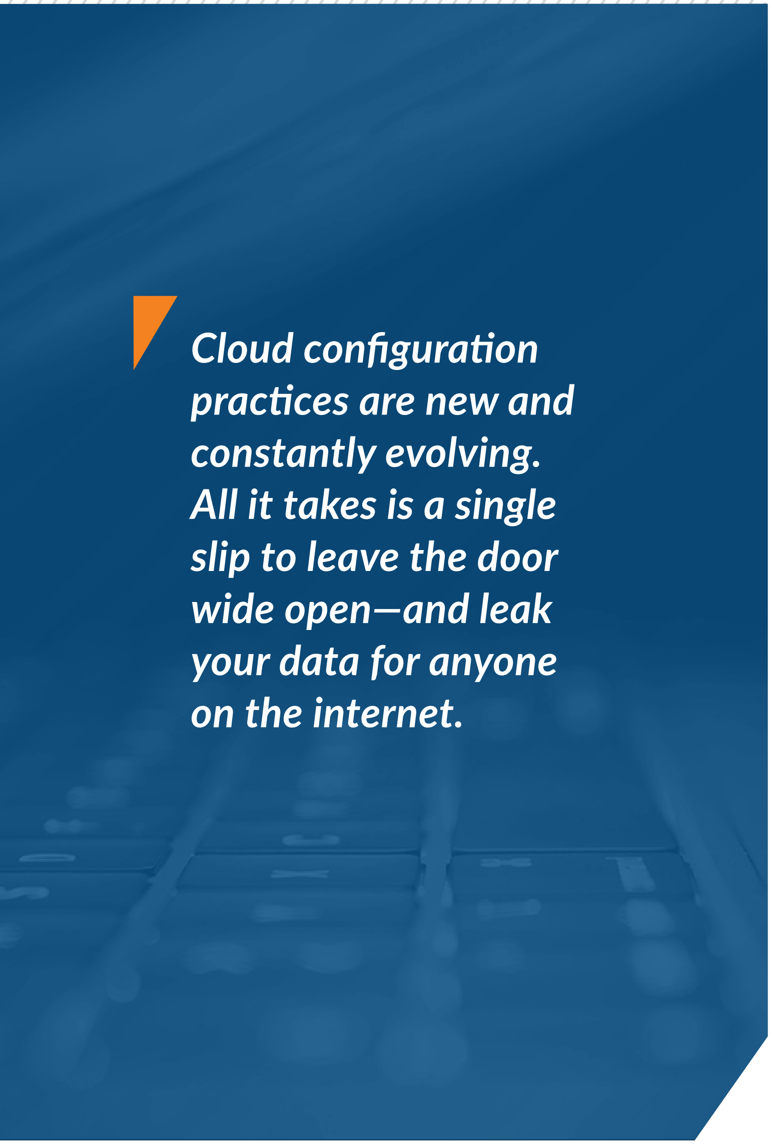
Cloud security posture management (CSPM) is a type of IaaS threat detection and response that provides you with the tools you need to protect against vulnerabilities.

With CSPM, you can evaluate IaaS configurations against relevant benchmarks such as:

- Common frameworks
- Compliance requirements
- Best practices
- Your IT policies

CSPM benefits include:

- Improved visibility across cloud resources and flagging of vulnerabilities
- The ability to prioritize vulnerabilities to guide remediation actions
- Reduced alert fatigue



> *Cloud configuration practices are new and constantly evolving. All it takes is a single slip to leave the door wide open—and leak your data for anyone on the internet.*

SECURITY OPTIONS BUILT FOR IAAS

The cloud is now a critical part of your security operations, which means you need consistent visibility, threat detection, and response across your entire environment.

Integrating cloud security makes your security operations more efficient by ensuring you don't have gaps between your on-premises and cloud systems. It also ensures that you prioritize risks regardless of location.

For many organizations, however, adding cloud security operations presents a number of challenges, including:

ACUTE LACK OF EXPERTISE

Finding skilled security talent in general is a challenge across industries, with many organizations already struggling to fill security roles.

Even if you don't have a problem staffing your IT team with security talent, your generalists are likely not well equipped to handle the growing cloud complexity and threat sophistication. Unfortunately, finding talent with the right cloud security skills is exceedingly difficult.

GAPS IN PROCESS

There's no shortage of vendors offering cloud security tools. But a tool-first solution leaves IT teams behind the eight ball—they may have the data they need to protect their business but not the processes and the people required to actually achieve cloud security.

Tools alone don't protect your on-prem environment, and they're not enough for your cloud infrastructure either.

To solve these challenges, organizations are now turning to vendors who can provide actionable expertise and an ongoing relationship. Partnering with a vendor for IaaS security brings many advantages, but it's important to make sure your partner not only supports your needs today but also supports what you may require in the future as your challenges grow and new needs evolve.

FINDING AN IAAS SECURITY VENDOR

If you're considering outsourcing IaaS security to a managed security services provider, make certain the vendor can customize their services to your needs and your environment.

And be sure to ask the following questions:

01

Can you deliver IaaS threat detection and response?

Look for a vendor who can help you understand your cloud risk surface, identify IaaS risks, provide visibility across all your cloud platforms, and detect unauthorized cloud use (shadow IT).

02

Can you deliver cloud security posture management?

Make sure your partner can detect misconfigurations and other vulnerabilities in real time, as well as help you prioritize mitigation based on the highest risks.

03

Can you deliver security operations?

You don't want to add more work for your IT team when you hire an IaaS security provider. Consider a partner who will provide white-glove service for the deployment and management of your security solution.

WHAT'S NEXT?

Huge security gaps caused by a move to the cloud will only widen. The growing number of cloud data breaches in the last few years indicates that threat actors consider insufficient cloud security as low-hanging fruit for their attacks and are increasingly taking advantage.

Businesses should realize they not only need to step up their cloud security, but they also must choose a partner with a forward-looking cloud security strategy whose capabilities and vision will keep their cloud infrastructure protected well into the future.

Sources

1. Flexera 2020 State of the Cloud Report
2. Global Cloud Index, Cisco (2018)
3. Cloud Computing Market Size, Grandview Research (2020)
4. The State of Cloud Security, Sophos (2020)
5. "Is the Cloud Secure?" Gartner (2019)
6. Arctic Wolf data
7. Oracle and KPMG Cloud Threat Report (2020)
8. Oracle and KPMG Cloud Threat Report (2020)
9. Cost of a Data Breach Report, IBM (2020)
10. Cost of a Data Breach Report, IBM (2020)
11. CSP/Customer Shared Responsibilities, Cloud Security Alliance (2019)

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

CONTACT US

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com

END CYBER RISK

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

For more information about Arctic Wolf, visit **arcticwolf.com**.

REQUEST A DEMO