ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

CLOUD SECURITY BUYER'S GUIDE

How to Select a Cloud Security Solution for Your Organization

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Organizations across all industries continue to leverage the dynamic efficiencies and scalability offered by the cloud.

Along with these significant advantages, however, the cloud also brings new security challenges.

92 percent of organizations admit they have a gap between their cloud use and their cloud security.[1]

70 percent of organizations hosting data or workloads in the public cloud experienced a security incident in 2019.[2]

Cloud assets were involved in 24 percent of breaches in 2019.[3]

While cloud providers continue to harden their infrastructure, your organization is responsible for the secure use of cloud-based services—and this is where we see a major gap in cloud security.

Gartner forecasts that 99 percent of failures in cloud security through 2025 will be the customer's fault.[4] That's up from 95 percent, which Gartner forecast through 2020.[5]

When you plan your cybersecurity strategy, understand what you're accountable for and where your gaps are.

Use this guide to get a deeper understanding of the different kinds of cloud security and the capabilities your cloud security solutions should provide.

What Are the Gaps in Cloud Security?

Operational challenges:

TOOLS

Companies average 47 different tools.

Ponemon

PEOPLE

Cybersecurity skills gap is 4.07 million worldwide.

(ISC)2

PROCESS

75 percent of organizations can't respond to security incidents within one day.

Ponemon

02

THREE TYPES OF CLOUD SECURITY

THREE TYPES OF CLOUD SECURITY

Cloud security solutions today include three categories defined by Gartner as:

01

Cloud Access Security Broker (CASB)

Cloud access security brokers are policy enforcement points (in the cloud or on-premises) that sit between cloud end users and service providers. CASBs help enforce security policies such as encryption, authentication, logging, single sign-on, and malware detection. Unlike CWPP and CSPM solutions, CASBs cover all cloud service models.

CASB has benefits for use cases such as shadow IT, malware protection, and data exfiltration. But the capabilities vary widely between vendors, and the vendor you use today may not support new applications that you adopt in the future.

02

Cloud Security Posture Management (CSPM)

Cloud security posture management primarily protects against misconfigurations of cloud resources and other vulnerabilities in your IaaS and other cloud infrastructure. These solutions provide prevention, detection, and response capabilities based on best practices, common frameworks, regulatory compliance, and your IT policies.

CSPM solutions don't offer consistent coverage of all platforms—while AWS support is typically included, some don't support the Google Cloud Platform or Microsoft Azure.

03

Cloud Workload Protection Platforms (CWPP)

Cloud workload protection platforms, as the name implies, protect workloads. These platforms are best for hybrid environments that span on-premises, multiple public infrastructure-as-a-service (IaaS) clouds, private cloud, and virtual machines. CWPP solutions are often—but not always—agent-based.

Platform capabilities may include firewalls, network visibility, identity-based segmentation, anti-malware scanning, application controls, and workload behavior monitoring. One of the drawbacks of CWPP is that only some vendors include tools for container-based architectures, and many legacy vendors are not agile enough to respond to your changing needs.

Each of these categories has its own advantages and disadvantages.

KEY CONCERNS

- Many solutions don't offer enough context to help you prioritize risks.
- Some solutions don't provide automation, which slows down your mitigation efforts.
- Even if you implement CASB, CSPM, and CWPP, you may not have comprehensive protection. Cloud security is rapidly evolving, and some important capabilities don't fall into these categories.

03

THE FIVE CORE FUNCTIONS OF CLOUD SECURITY

THE FIVE CORE FUNCTIONS OF CLOUD SECURITY

The NIST Cybersecurity Framework provides standards, guidelines, and best practices for hardening your IT infrastructure. Based on risk-management processes designed to prioritize mitigation, these practices apply to cloud security as well.

The NIST framework centers around five core functions: ***identify, protect, detect, respond,*** and ***recover.*** When you're evaluating cloud security solutions, consider how well they score on these five functions.

01

Identify

You can't protect what you can't see, and you can't have an effective strategy if you don't understand your risks. You need complete visibility into your cloud assets and other elements, along with the ability to prioritize your risks.

Choose a solution that include capabilities such as asset inventory and risk assessment.

02

Protect

A common challenge for security teams is the proliferation of tools that solve single, specific security problems. This makes it challenging to prioritize risks across the attack surface. It also leads to alert fatigue and results in ineffective security operations.

Choose a solution that provides a unified approach and consistency across your entire landscape.

03

Detect

Vendors typically offer 24x7 monitoring, but not all provide around-the-clock detection and response by a team of experts. While automated tools and advanced technology like machine learning are important for defending against today's threats, machines can't provide the critical thinking and analysis that humans bring to the table.

Choose a solution that incorporates the value you can only get from a team of experienced, threat-hunting experts.

04

Respond

Rapid response is critical after you detect a threat in your environment, so make sure you understand how your cloud security solution aligns with your mitigation workflows.

Choose a solution that supports your ability to quickly contain an incident as part of an initial response.

05

Recover

Part of recovery involves building resilience so you can minimize the likelihood, as well as the impact, of incidents that may occur in the future.

Choose a solution that delivers a continually improved security posture over time.

04 TOP CLOUD SECURITY FEATURES AND CAPABILITIES

TOP CLOUD SECURITY FEATURES AND CAPABILITIES

Managed cloud security can fill the gaps in your talent shortage and your security operations by removing the burden of protecting your cloud assets in-house. Since capabilities and features vary from vendor to vendor, make sure the solution you choose works to achieve the outcomes you expect.

Consider the following criteria to help you evaluate whether the solution will give you comprehensive coverage:

01

Identification

- Identify assets across cloud platforms for visibility, reporting, and auditing purposes.
- Detect unauthorized cloud applications and services (shadow IT).
- Provide a single, integrated view of risks and threats across the cloud environment.

02

Monitoring

- Monitor, assess, and prioritize threats such as vulnerabilities and configuration changes.
- Monitor compromised SaaS credentials and suspicious user and admin behavior and activity.
- Enable automated remediation and customized rules based on your environment.

03

Operations

- Bridge the gap between cloud-native security APIs and your team.
- Simplify your in-house operations with a solution that's easy to manage and maintain.
- Augment your team with outside experts who can provide strategic guidance.

Talent Is a Major Cloud Security Operations Challenge

The cybersecurity industry has long struggled with a shortage of talent. The ratio of existing U.S. workers to job openings (known as the supply-to-demand ratio) in cybersecurity is 1.8.[6] For comparison, the national average supply-to-demand ratio for all jobs is double that: 3.7.

Even more daunting, the number of unfilled cybersecurity jobs globally is expected to surpass 1.5 million by 2020.[7] Cloud security ranks second among roles that are the hardest to fill. As cloud adoption continues to grow at a brisk pace, the skills gap in cloud security will only grow wider.

05

12 KEY QUESTIONS TO ASK CLOUD SECURITY VENDORS

05

12 KEY QUESTIONS TO ASK CLOUD SECURITY VENDORS

CAPABILITIES

- Can you identify cloud assets and vulnerabilities?
- Can you benchmark misconfigurations against known good states or baselines?
- Can you provide guidance on addressing identified issues?
- Can you detect security incidents and attacks in progress?

COVERAGE

- Do you cover my IaaS platforms?
- Do you cover my SaaS tools?
- Do you integrate with on-premise security?
- Do you provide 24x7 coverage and SLAs that would allow my organization to respond to attacks in a timely fashion?
- Can you affordably scale to cover my growing and transforming cloud footprint?

OPERATIONS

- Does your solution include human expertise?
- Are these experts mapped to my organization?
- Do you have access to cloud knowledge and a track record with cloud platforms?

06 FINAL THOUGHTS

FINAL THOUGHTS

Most organizations today rely on at least one public cloud, and those looking for better flexibility and agility are embracing the hybrid multi-cloud. As cloud adoption continues to grow, so will the gaps in cloud security.

Many high-profile breaches in the last couple of years served as reminders that the business consequences of weak cloud security are enormous. Yet many of these same incidents were preventable, and even simple measures can have a big impact on cloud security.

There's no shortage in the marketplace of vendors offering tools, but being a savvy cloud security buyer means looking beyond the shiny gadgets. Technology alone won't solve your security problems.

Find a partner who has the mix of tools and expertise capable of addressing the risks in your environment. One who can cover your major areas of exposure today, while securing your cloud as you journey to bigger things well into the future.

Sources

1. Oracle and KPMG Cloud Threat Report 2020
2. The State of Cloud Security 2020, Sophos
3. 2020 Data Breach Investigations Report, Verizon
4. "Is the Cloud Secure?" Gartner blog, 2019
5. "Why Cloud Security Is Everyone's Business," Gartner blog 2016
6. Cybersecurity Supply/Demand Heat Map, CyberSeek data, 2020
7. Cybersecurity Talent Shortage, CyberTalk, 2020

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

CONTACT US

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com

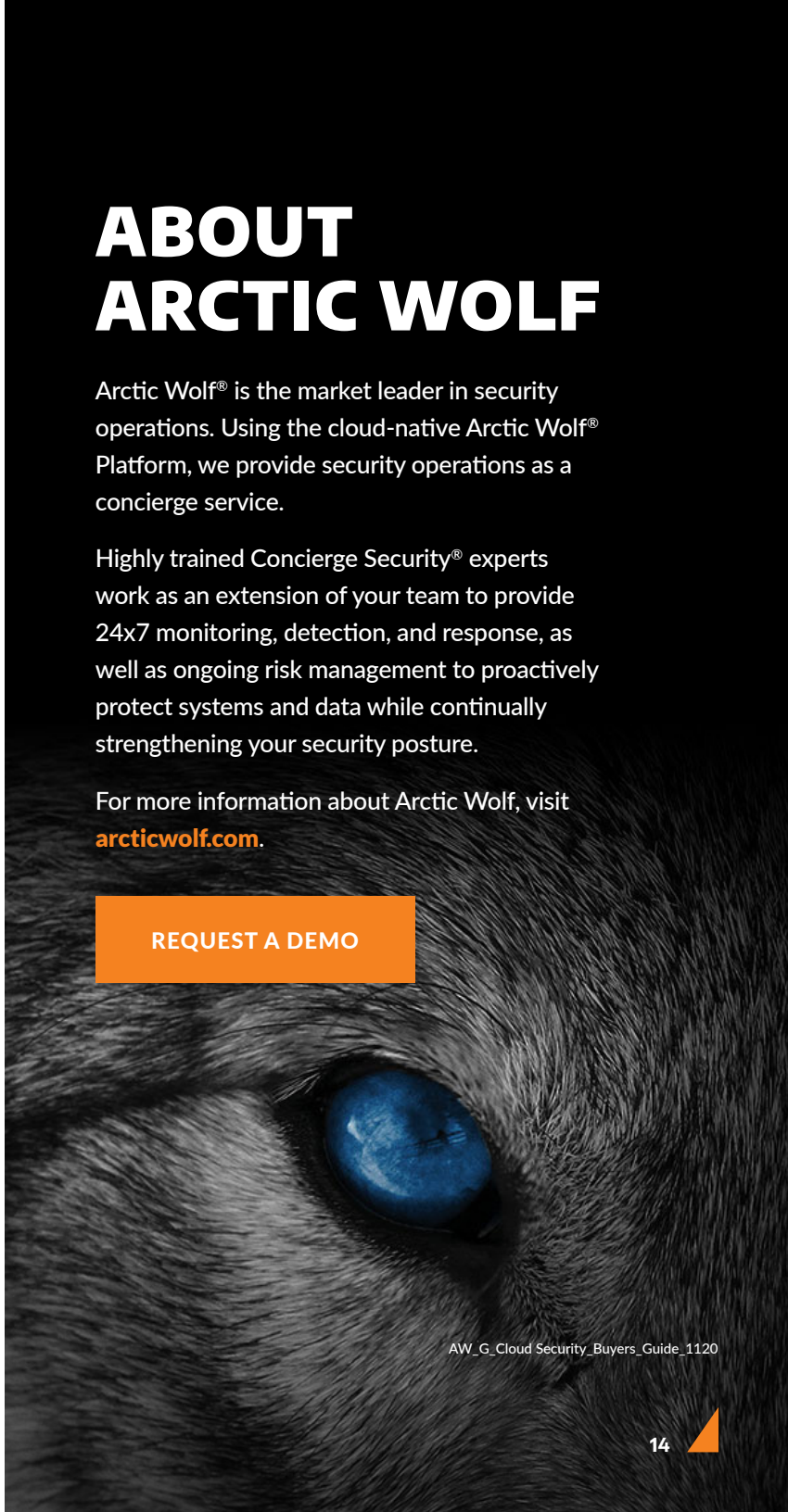
ABOUT ARCTIC WOLF

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



AW_G_Cloud Security_Buyers_Guide_1120