Cloud Vulnerabilities & Hardening Cloud Posture

Whitepaper

2022

AGILEBLUE

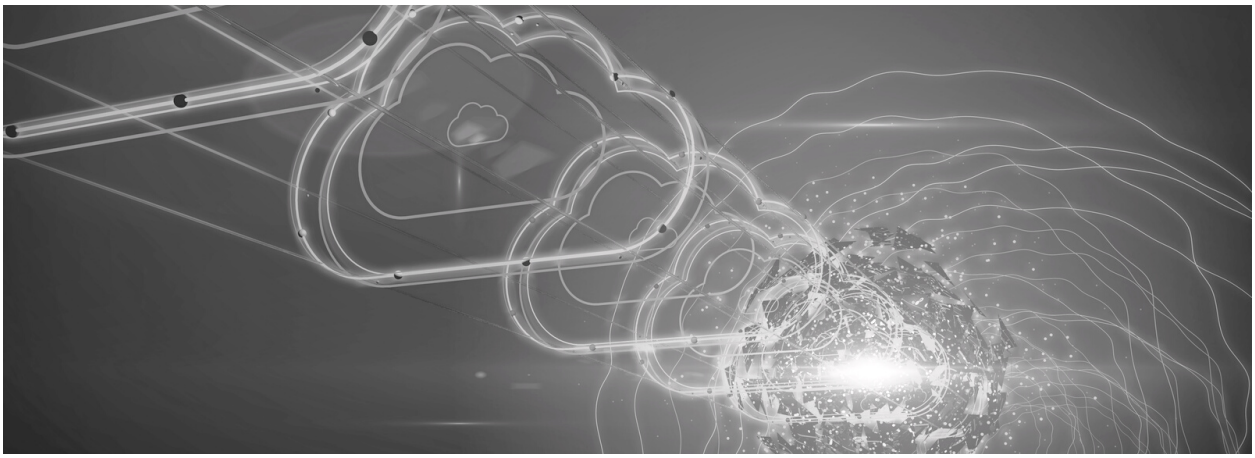
OVERVIEW

As cloud adoption accelerates, it's critical to manage your security risks within your growing number of cloud services. One single misconfiguration can lead to a serious data breach. Data shows that more and more breaches are happening, not because of people clicking on malicious links, but because of negligent misconfigurations.

The graphic below breaks down the biggest threats to an organization's cloud security. Misconfiguration of the cloud accounts for 62%.

> *"NEARLY ALL SUCCESSFUL ATTACKS ON CLOUD SERVICES ARE THE RESULT OF CUSTOMER MISCONFIGURATION, MISMANAGEMENT AND MISTAKES," - GARTNER, 2022*

Source: CB Insights



MISCONFIGURATION

At a general level, a misconfiguration could be anything from having storage not configured correctly, to not having access controls configured in a way that is controlling the access at the right levels. Some additional ways a cloud could be misconfigured include:

- lack of access restrictions
- lack of logging and monitoring
- lack of data protection
- lack of audit and validation
- over entitlement of access to some users

A common misconception is that the cloud is secure because businesses are using large cloud providers such as Amazon, Google, and Microsoft. While these providers are certainly some of the most secure in the world, it doesn't mean that an organization using these provides is secure. The set-up, data, applications, databases, etc., is a shared security model, and you, as a business, must run the security of your own installation.

The growing cloud usage has expanded the threat vector and introduces new challenges for security teams, thus making it impossible to manually manage and secure the cloud. Automating the cloud security assessment and management is a simple solution to the inevitable problem.

> *"95% OF ALL CLOUD SECURITY BREACHES ARE DUE TO MISCONFIGURATIONS. BY 2024, ORGANIZATIONS IMPLEMENTING A CSPM OFFERING AND EXTENDING THIS INTO DEVELOPMENT WILL REDUCE CLOUD-RELATED SECURITY INCIDENTS DUE TO MISCONFIGURATION BY **80%**" (GARTNER, 2021)*

CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

A cloud may connect and disconnect from hundreds or even thousands of other networks over the course of a day. This highly active nature makes clouds powerful, but it also makes them hard to secure. Cloud Security Posture Management (CSPM) is an automated technology that identifies misconfiguration issues and compliance risks in the cloud. An important purpose of CSPM programming is to continuously monitor cloud infrastructure for gaps in security policy enforcement.

CSPM can help reduce your operational complexity in managing security across all your cloud applications, prevent data loss due to misconfigurations, and ensure the latest compliance guidelines – GDPR, CCPA, HIPAA, PCI, are adhered to in a multi-cloud infrastructure.

BENEFITS OF CLOUD CONFIGURATION & CSPM

1. CPSM provides discovery and visibility into cloud infrastructure assets and security configurations. Users can access a single source of truth across multi-cloud environments and accounts.

2. Misconfigurations management and remediation eliminates security risks and accelerates the delivery process by comparing cloud application configuration to industry and organizational benchmarks, so violations can be identified and remediated in real-time.

3. CSPM proactively detects threats across the application development lifecycle by cutting through the noise of multi-cloud environment security alerts with targeted threat identification and management approach. The number of alerts is reduced due to CSPM's focus on the areas adversaries are most likely to exploit.

4. Dev SecOps reduce the overhead expense and eliminate friction and complexity across multi-cloud providers and accounts via the centralization of controls.

MONITORING CLOUD INFRASTRUCTURE & THREATS

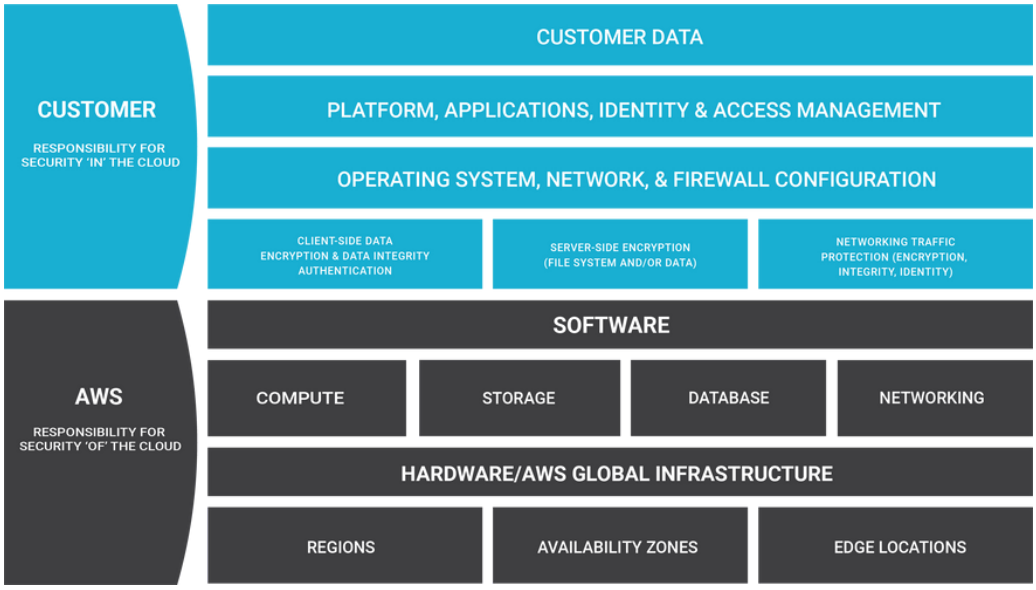
To securely enable business initiatives in a world of advanced, targeted attacks, security and risk management leaders must adopt a continuous adaptive risk and trust assessment approach to allow real-time, risk and trust-based decision making.

Organizations are overly dependent on blocking and preventing mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process that integrates predictive, preventive, detective, and response capabilities.

SECURING THE CLOUD

A cloud misconfiguration often occurs because of a misunderstanding of the shared responsibility model. This means that an organization may not fully understand the different layers of responsibility of what each third-party vendor is providing to the organization and what the organization as the consumer is responsible for.

The impact of not understanding your responsibility as an organization can lead to the inaccurate inventory of your cloud resources, inadequate encryption of sensitive data, and flawed assumptions about business continuity and disaster recovery. The below graphic outlines responsibilities of the customer vs. AWS, a third-party vendor. It is important to note that an organization is responsible for the security *in* the cloud while AWS is responsible for the security *of* the cloud.



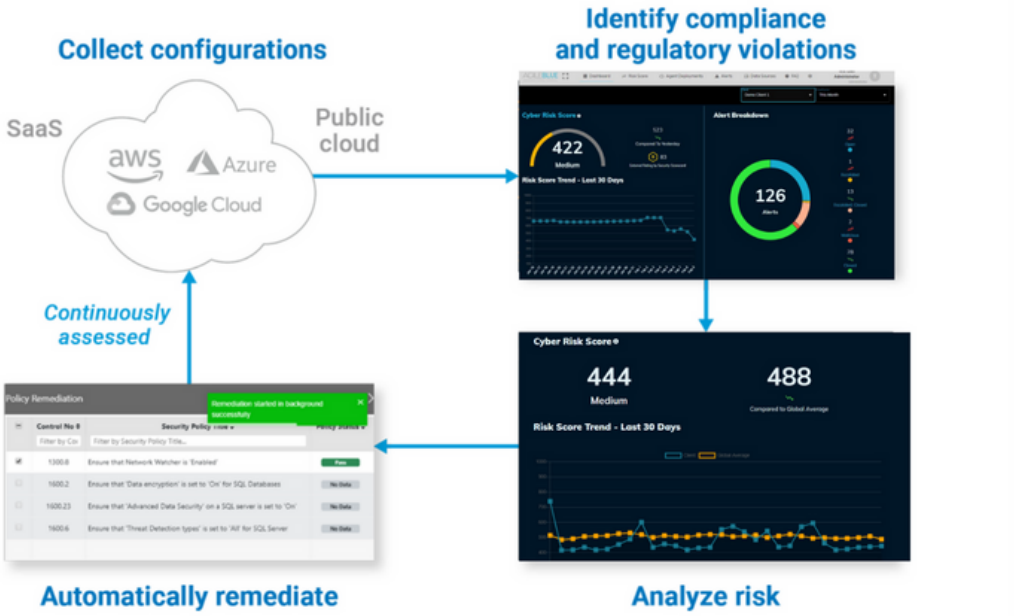
Source: Amazon Web Services

While many security professionals are highly skeptical about the secureness of cloud-based services and infrastructure, it's important to implement best practices and guidelines that should be used to securely leverage the benefits of the cloud. Some best practices are outlined below:

- Encryption of data in transition should be end to end
- Encryption of sensitive data should be enabled at rest
- Implement and enforce a defined data deletion policy
- Complete ongoing vulnerability testing
- Add protective layers with user-level data security

SIMPLIFING YOUR CLOUD SECURITY

AgileBlue's Cloud Security Posture Management (CSPM) provides discovery and visibility into your cloud infrastructure assets and security configurations allowing you to access a single source of truth across multi-cloud environments and accounts. Our CSPM eliminates security risks and accelerates the delivery process so violations can be identified and remediated in real-time. We help reduce overhead expenses and eliminate friction and complexity across multi-cloud providers and accounts through centralization of controls.



AGILEBLUE

AgileBlue is a SOC|XDR platform that's proven to detect cyber threats faster and more accurately across your entire digital infrastructure and cloud. We provide 24/7 monitoring, detection and response to identify cyber threats before a breach occurs.

Our tech is intelligent and automated, but we take a custom approach for every client we work with, analyzing and detecting exactly what you need it to. Our products are 100% cloud-based including advanced machine learning and user behavior analytics backed by our team of cyber experts who are always just a call away.

For more information, visit our website: AgileBlue.com.

Ready to start protecting your company?

REQUEST A DEMO