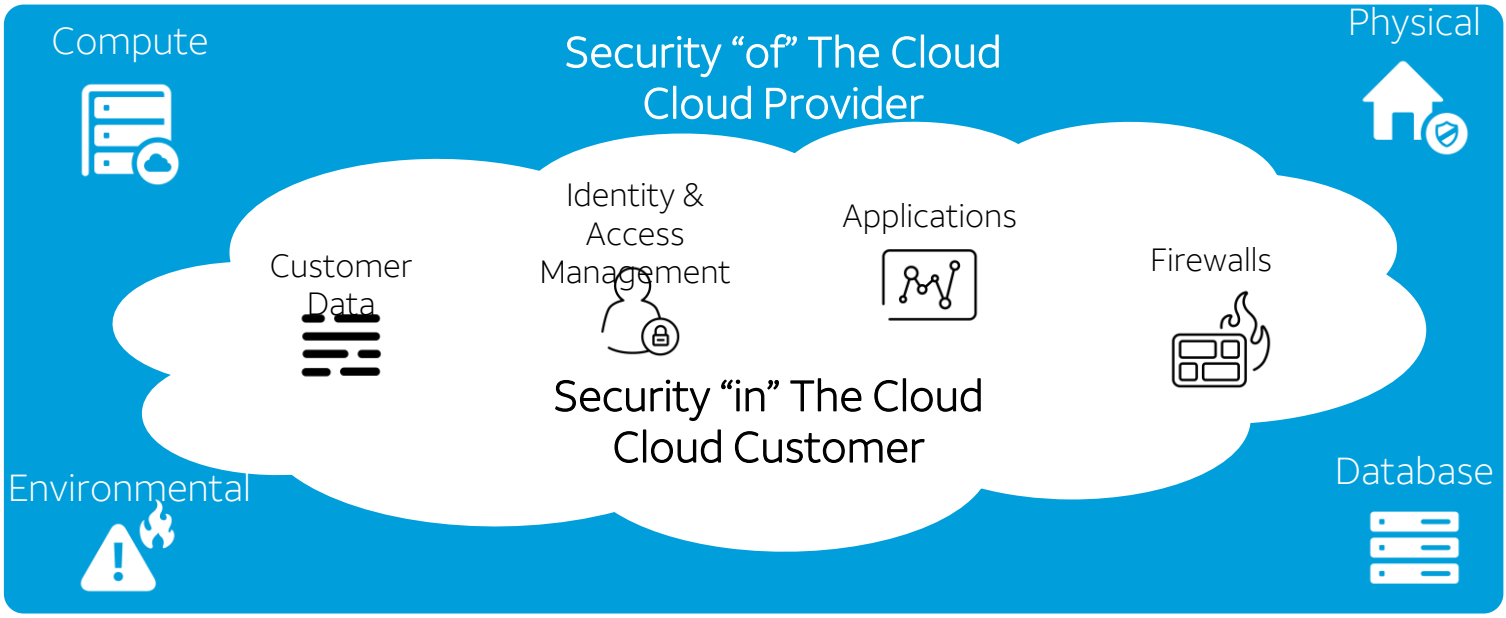
AT&T Business

AT&T Cybersecurity Consulting – Cloud Security Threat and Vulnerability Management

Continuously monitor and assess your cloud assets and resources for vulnerabilities, misconfigurations and non-standard deployments.



The responsibility of security is shared between the cloud provider and their customer and will vary by service type.

As you aggressively move workloads into the public cloud, you need to protect them. You want to take advantage of the cost and development benefits afforded by migrating your applications and data from on-premises to public cloud environments.. For starters, it's key to understand that public cloud platform providers operate on a "shared security responsibility" model: The burden is split between the cloud provider and their customers. These vendors take care of the security of the cloud. Customers, in turn, are responsible for defining their controls to protect their instances, data and software on these platforms.

As more and more business units migrate to the cloud, InfoSec teams lose sight of who's doing what, and what resources they're using. This problem gets compounded if the organization is using cloud platforms from more than one vendor.

Benefits

- Helps boost the security of your public cloud deployments
- Helps identify threats caused by vulnerabilities, misconfigurations, and non-standard deployments
- Helps run continuous security checks on your cloud instances, containers, and assets

Cloud Security Assessment gives you an "at-a-glance" comprehensive picture of your cloud inventory, the location of assets across global regions, and full visibility into the public cloud security posture of all containers, assets and resources. It provides a quick overview of inventory and their associated security posture via dashboards.

The reporting capability lets you personalize your dashboard with custom widgets based on queries or on other criteria, such as "Failures by Control Criticality" and "Security Postures by Region".

Cloud Security Threat and Vulnerability Management Solutions

Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes. High levels of automation and user self-service in public cloud infrastructure as a service (IaaS) and platform as a service (PaaS) have magnified the importance of correct cloud configuration and compliance. Organizations should invest in cloud security posture assessment and management processes and tools to proactively and reactively identify and remediate these risks.

Approach:

- Help identify, classify, and monitor assets and vulnerabilities;
- Help comply with internal and external policies;
- Help prioritize vulnerability remediation;

In addition, you can generate a continuously updated inventory of your public cloud instances and infrastructure, as well as continuously monitor and assess your cloud instances, containers, assets and resources for misconfigurations and other mistakes.

Insight and threat prioritization

The elastic nature of the cloud makes it difficult to track and prioritize threats. With this service we offer a 360-degree view of cloud assets' security posture, which includes cloud vulnerabilities associated with instances, containers, and assets, compliance requirements and threat intelligence insights, so users can contextually prioritize remediation.