Is Your Public Cloud Too Public?

Follow this checklist to see how well your cloud workloads are protected

Are you properly securing your workloads in public cloud infrastructure, such as Amazon Web Services, Microsoft Azure, or Google Cloud Platform? There are many threats to public cloud workloads, some similar to traditional environments and some specific to the cloud. We've identified the most pertinent threats to workloads in public cloud environments.

Are you able to detect these threats in your public cloud?

○ **Misconfigured resources**

The public cloud gives you enough control to create your own security problems. Misconfigured assets, such as databases of customer data left open to the Internet, can leave you open to a breach.

○ **Compromised resources**

When a cloud resource is compromised through credential abuse, application vulnerability, or some other method, security staff need to identify it quickly to prevent a breach.

○ **Credential abuse**

Compromised credentials are one of the primary ways an attacker can penetrate your cloud infrastructure. Identifying logins from unusual locations or risky behavior such as disabling two-factor authentication can help detect credential abuse.

○ **Bad ephemeral resources**

The dynamic nature of the cloud means that attackers with cloud access can spin up a new server, use it to perform a bad activity such as data exfiltration, and remove it before the security team notices something is wrong.

○ **Unusual account behavior**

Since cloud infrastructure is highly automated, many aspects of its operation should be consistent and predictable. Abnormal behavior, such as the appearance of new resources in previously unused regions or API calls from unusual countries, can be indicators of compromise.

Cloud infrastructure is an increasingly important component of the modern business. If you cannot detect these threats in your public cloud infrastructure, you are leaving yourself open to attack.

Cisco Stealthwatch Cloud can help you secure your cloud by detecting early stage indicators of compromise, monitoring your cloud and network traffic, and identifying compliance and policy violations. Stealthwatch Cloud can protect your public cloud infrastructure, private network, and hybrid network environments.

Try Stealthwatch Cloud free for 60 days

Learn More