Barracuda Cloud Security Guardian

Build fast. Stay secure.

Barracuda Cloud Security Guardian is an agentless SaaS service that makes it simple and easy to stay secure while building applications in, and moving workloads to, public-cloud infrastructures. It provides end-to-end visibility across your public-cloud deployment, so you can better understand and reduce your risk posture. And it automatically optimizes and remediates security controls to ensure continuous compliance.

Barracuda Cloud Security Guardian watches over your security and compliance, so your builders can focus on what they do best—developing and deploying business applications.

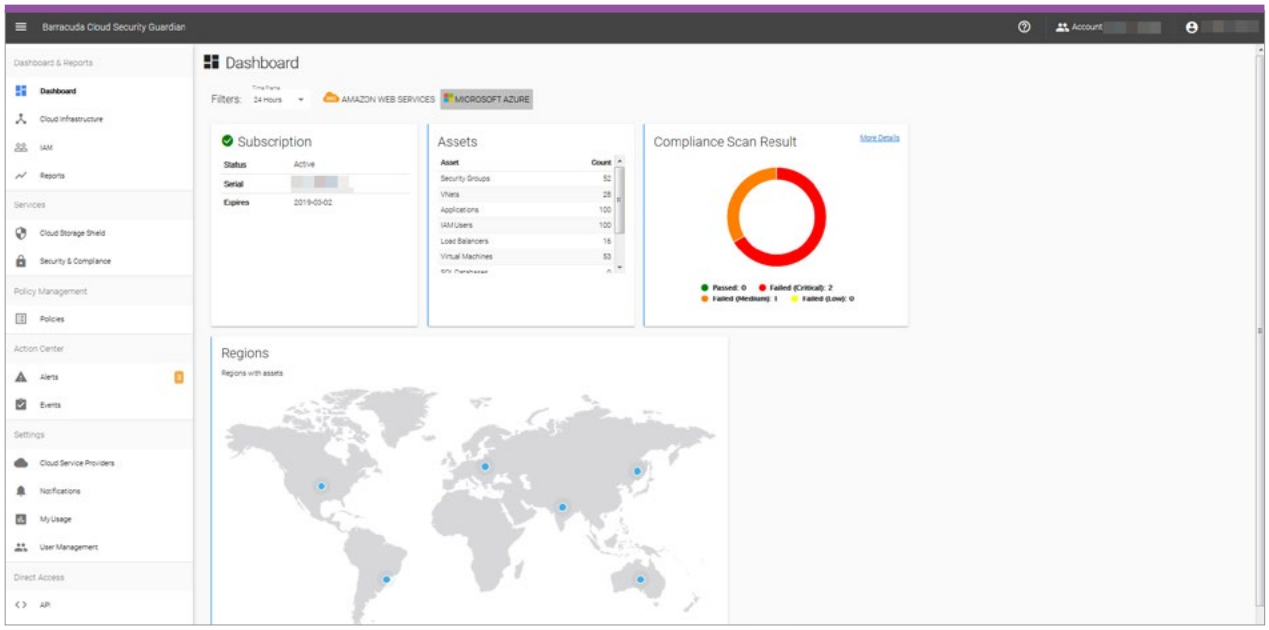


Figure 1 - Barracuda Cloud Security Guardian dashboard

Automated cloud security

Deploying and configuring Barracuda Cloud Security Guardian is simple. Within minutes of deploying it, the service will discover and analyze your entire cloud deployment and lay it out graphically before you—even if your deployment straddles multiple cloud infrastructures. From here, you can choose to use predefined

policy frameworks such as CIS, HIPAA, NIST, etc., or to create customized policy settings that best fit your business and security objectives. The system will then start assessing your deployment for policy violations. The assessment process continues to run in the background as Barracuda Cloud Security Guardian watches over your environment, remediating configuration drift and policy deviations that may get introduced over time. Remediation of policy violations and vulnerabilities is just a click away.

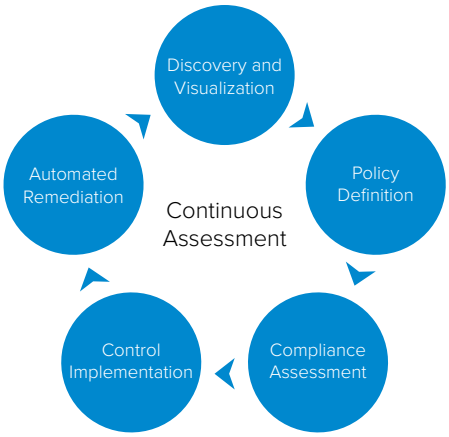


Figure 2 - Barracuda Cloud Security Guardian provides continuous, orchestrated remediation of policy violations across your entire cloud deployment

Barracuda Cloud Security Guardian automates your security processes, which has the practical benefit of eliminating the traditional friction between builders and security professionals. Your developers can work in the fast, agile way that gets you to your business goals quickly, while your security team monitors and remediates policy violations in real time *(see figure 2)*.

"Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials, or insider theft, not cloud provider vulnerabilities."

Neil MacDonald
Gartner Research

Barracuda Cloud Security Guardian advantages

Complete visibility of your cloud infrastructure

Public cloud environments change rapidly and constantly. The ability to change and grow elastically is a key benefit, but it also brings challenges from a security and compliance perspective. Complicate that further with a multi-cloud environment and it quickly becomes practically impossible to visualize your infrastructure clearly, drill down into detail, gather resource-level information, and understand the relationship and interconnections among those resources—which is critical to understanding how they affect compliance and your security posture.

Barracuda Cloud Security Guardian gives you a clear visualization of your cloud assets and their interrelationships from network, application, and access perspectives—so you can easily gather valuable insights *(see figure 3)*.

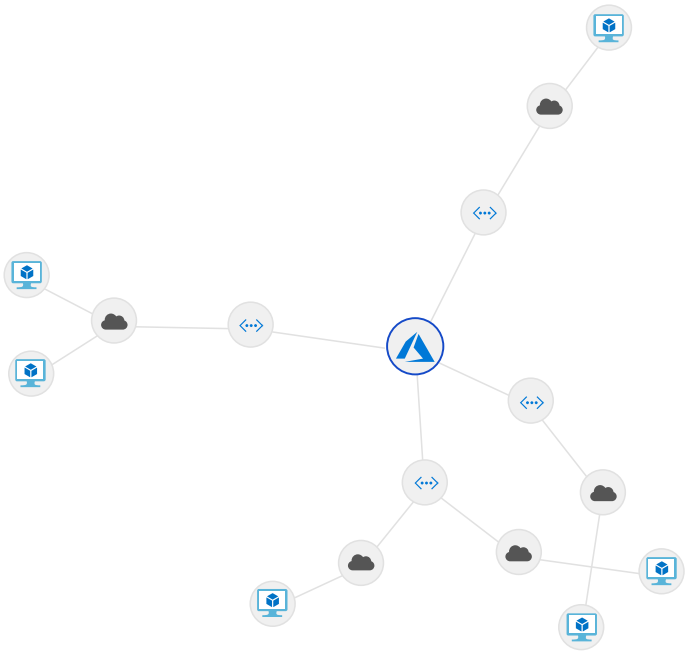


Figure 3 - Azure Visibility

Continuous compliance and automated security

Maintaining compliance across your cloud environment can be challenging. Your developers move fast to bring new services and applications online. But if they're also tasked with maintaining compliance with security frameworks such as PCI, CIS, NIST, and HIPAA, the result may be a loss of speed and agility.

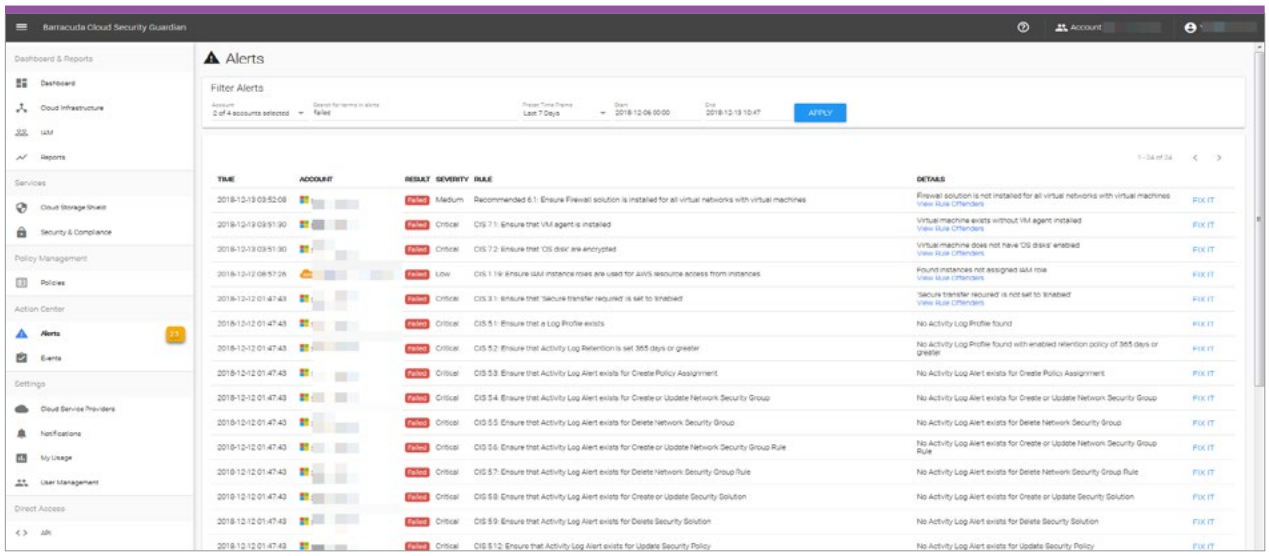


Figure 4 - Barracuda Cloud Security Guardian compliance alerts

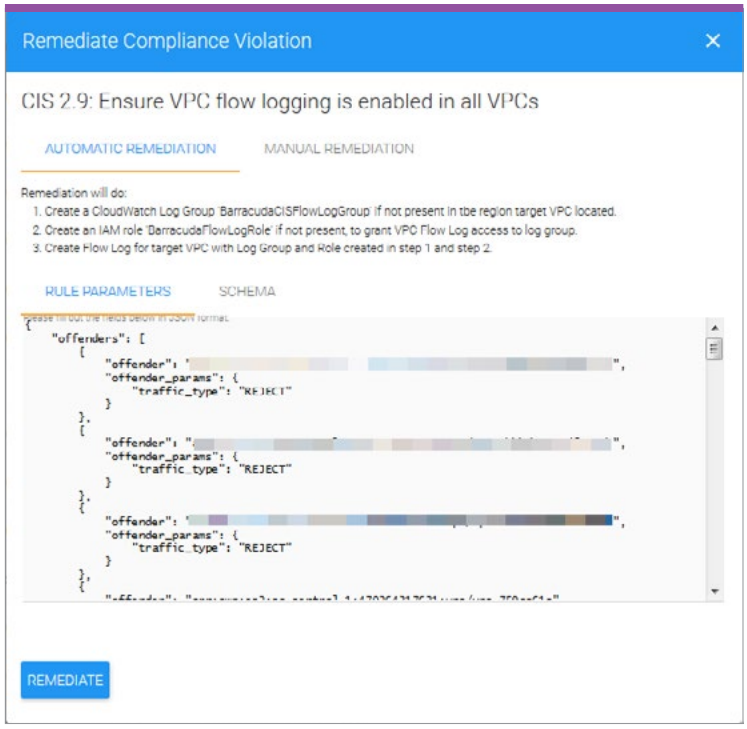
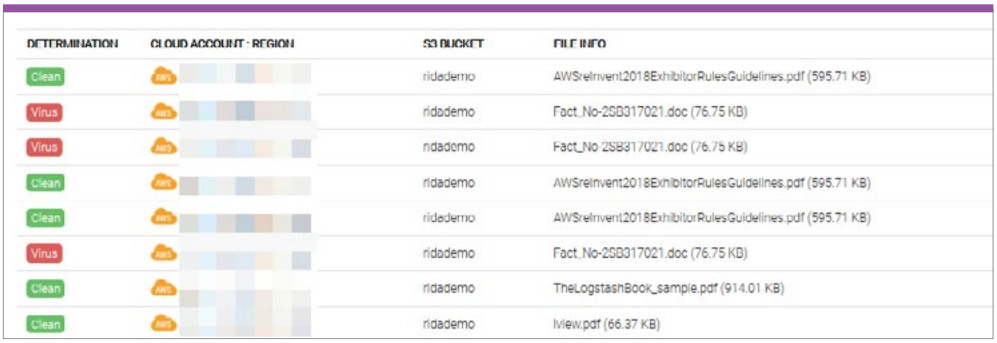


Figure 5 - Barracuda Cloud Security Guardian policy remediation

Barracuda Cloud Security Guardian installs in minutes and scans your entire cloud infrastructure for vulnerabilities, including the CIS AWS Benchmarks. Using predefined or custom profiles, you can quickly remediate and maintain continuous compliance while letting your builders to do what they do best—build fast!

Eliminate latent threats from your cloud storage

Latent threats and malware can have devastating effects on any business. Barracuda's Cloud Storage Shield, a function of Barracuda Cloud Security Guardian, automatically scans the contents of your AWS S3 buckets or Azure Blob storage, then identifies and removes any latent threats *(see figure 6)*.



DETERMINATION	CLOUD ACCOUNT : REGION	S3 BUCKET	FILE INFO
Clean		ridademo	AWSreInvent2018ExhibitorRulesGuidelines.pdf (595.71 KB)
Virus		ridademo	Fact_No-2SB317021.doc (76.75 KB)
Virus		ridademo	Fact_No-2SB317021.doc (76.75 KB)
Clean		ridademo	AWSreInvent2018ExhibitorRulesGuidelines.pdf (595.71 KB)
Clean		ridademo	AWSreInvent2018ExhibitorRulesGuidelines.pdf (595.71 KB)
Virus		ridademo	Fact_No-2SB317021.doc (76.75 KB)
Clean		ridademo	TheLogstashBook_sample.pdf (914.01 KB)
Clean		ridademo	Mew.pdf (66.37 KB)

Figure 6 - Cloud Storage Shield Report

Eliminate configuration drift

Ensuring that you maintain the correct rights and privileges to cloud services across environments can be challenging when your builders move fast. Should a resource change and deviate into non-compliance, Barracuda Cloud Security Guardian will automatically alert, remediate, and present activity reports for that user while quarantining the user or application from making any further changes that affect your security posture.

Protect the data plane of your cloud deployment

One of the benefits of Barracuda Cloud Security Guardian is its ability to identify and deploy Barracuda CloudGen WAFs and CloudGen Firewalls as needed to secure your applications and infrastructure in the cloud. An integral function of these firewalls is Barracuda Advanced Threat Protection, a service that scans uploaded files for malware. With Barracuda Cloud Storage Shield enabled, you'll keep even the newest, most evasive threats out of your environment.

The Barracuda difference: A full-stack security solution

Today, attackers move fast by automating the exploitation of misconfigured resources, and your public cloud environment is no exception. Barracuda Cloud Security Guardian polices the management plane and the data plane, fixing vulnerabilities by instrumenting and configuring native controls and by deploying our market-leading CloudGen WAF or CloudGen Firewalls as and where needed.

Barracuda
Your journey, secured.