

Barracuda Cloud Security Guardian

Build fast and stay secure, by automating public-cloud security compliance and remediation.

Barracuda Cloud Security Guardian is an agentless SaaS service that makes it easy to stay secure while building applications in, and moving workloads to, public-cloud infrastructures.

It provides security that firewalls cannot, including end-to-end visibility of your security posture in your public-cloud deployments and continuous, automated compliance monitoring and remediation of security controls.

“Guardrails” for developers

Cloud Security Guardian accelerates your public-cloud migration by delivering visibility, continuous compliance, and automated remediation. This lets your DevOps teams build applications faster, leverage cloud-native services, and shift more workloads to the cloud—all while ensuring security.

Full stack visibility for IT

Cloud Security Guardian provides real-time visibility into public cloud risk and compliance to policies and standards. IT gains visibility into the controls deployed to safeguard those environments, where the gaps are, and rich metrics and reporting.

Built on CIS Benchmarks—industry-leading best security practices

Cloud Security Guardian is built on, and certified by, CIS Benchmarks—industry-accepted best practices for cloud security policies. It provides real-time visibility into public cloud risk and compliance with policies and standards, and into reports that demonstrate how and why controls were applied.

CIS (Center for Internet Security) Benchmarks are the global standard and recognised best practices for security IT systems and data against cyber-threats, with specific benchmarks tuned to the major cloud platforms.



Product Features

Visibility

- Asset counter
- Datacenter usage
- AWS IaaS and PaaS
- Azure IaaS and PaaS
- Security posture

Compliance Assessment

- CIS benchmark
- NIST-800-53
- PCI DSS
- Custom ruleset

Alerting

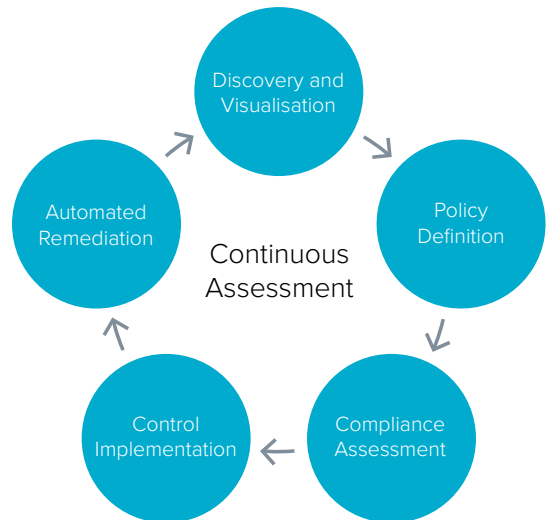
- Alerts on compliance violation
- Alerts on cloud native threat
 - Azure Security Center
 - Guard Duty
 - etc.
- Integration into SIEM and Alerting tools
 - Slack
 - Sumo Logic

Remediation

- One Click remediation
- JSON format edit
- API based

Cloud Storage Shield

- Advanced Threat Protection for S3 buckets
- Automated policy assignment
- Realtime notification



CIS-certified security posture solution

Cloud Security Guardian is certified by CIS Benchmarks, the gold standard for best practices in cloud infrastructures.

Multi-cloud visibility

Cloud Security Guardian maps and evaluates your security posture across multiple cloud instances, even from different cloud vendors—to give you a comprehensive view of your security.

Graphical map of all your cloud resources

Cloud Security Guardian draws—and continually updates—an infrastructure-wide map of your resource and how they are connected. Simple drill-downs provide more information and help identify root cause of security violations.

Built-in best practices

Cloud Security Guardian has already turned CIS Benchmarks best practices into rules that are pre-defined. PCI DSS rulesets are also included. Rules can be added and refined through simple JSON editing.

Eliminate latent threats from your cloud storage

Barracuda's Cloud Storage Shield, an optional feature of Barracuda Cloud Security Guardian, automatically scans the contents of your AWS S3 buckets or Azure Blob storage, and identifies and quarantines any latent threats.

Proactive security orchestration

Cloud Security Guardian can identify and automatically deploy Barracuda CloudGen WAFs and CloudGen Firewalls as needed to secure your applications and infrastructure in the cloud. Cloud Security Guardian can also deploy Azure Firewalls.

