CloudSploit by aqua

Automated Cloud Security Monitoring

CloudSploit keeps your cloud accounts configured securely

AWS | Azure | GCP | Oracle Cloud | GitHub

Adhering to security best practices can be difficult and time consuming.
The problem grows exponentially as the environment and the number of people with access to it increases.
Don't let a single misstep compromise your entire infrastructure.

Free Your Developers

CloudSploit offers best practices as a service. We update and automate risk detection safely without accessing the contents inside your network and with no agents to install. This can easily save hours of your developers' time each week.

Make Compliance A Priority

The scan reports generated by CloudSploit can be used to automatically assess risks, plan for remediation, and audit changes over time. Legal's happy. You're happy.

Protect Your Customers

Undetected issues put your customers' data and your business's reputation at risk. CloudSploit detects risks before they are exploited. If you have any questions, our fast-acting support team is at your service—even for our Free Plan.

CloudSploit is the tool of choice for security-minded companies

We are honored to be included on the SANS Secure DevOps Toolchain.
Our engine is open source and offers custom plugins for your infrastructure.

aws partner network
Advanced Technology Partner

cloudsploit.com

CloudSploit by aqua

Continually Monitor Security and Configurations Across Cloud Environments

CloudSploit's open source engine scans EC2, ELB, IAM, KMS, VPC, S3, and other AWS infrastructure in search of configurations that do not adhere to best practices. Alerts, which include remediation advice, are routed by you via email, SNS, and several other integrations such as Slack, OpsGenie, and PagerDuty.

Secure Access

With a cross-account AWS Security Audit IAM role, CloudSploit can only see infrastructure configurations.

Automated Detection

Run configuration scans as often as hourly to be constantly updated on configuration changes with each deployment. With real time event streams, DevOps teams can be instantly alerted to potential issues before vulnerabilities are exploited.

Custom Plugins

Comply with your company's policies by developing custom Node.js plugins that are open source or private and custom to your particular needs.

Minimal Blast Radius

CloudSploit priotizes user security and anonymity. Scans only have access to service metadata, so we cannot see your data or make modifications.

Workflow Integration

Connect with CI/CD environments, custom scripts, and more. Our APIs are available at cloudsploit.com/api/documentation.

Secure Infrastructure As Code

Detect insecure configurations within your CloudFormation templates via CloudSploit's API-accessible scanner.

Serverless

Our infrastructure is based on Lambda functions. We can scale to meet any workload.

How It Works - Get set up in seconds

01 Create a secure, cross-account IAM role
This allows CloudSploit to query the cloud's API on behalf of your account

02 Give the role read-only permissions
CloudSploit only has read access to your account metadata. Simply use the built-in Security Audit policy

03 Integrate your IAM role with CloudSploit
Connect a new role through the CloudSploit dashboard in just a few minutes

04 Begin scanning
You can initiate on-demand scans immediately or enable continuous background scanning

05 Configure your account. Set limits for configurations and suppress plug-ins
Add integrations to route notices and avoid notification fatigue

aws partner network
Advanced Technology Partner