aqua

Solution Brief

Securing Cloud Functions

It can be challenging to monitor and detect malicious activity in serverless functions because their footprint, in relation to other cloud native artifacts, is small, and they are ephemeral. Serverless functions do not persist for long periods of time. They contain dependencies to other services that can be hard to identify fully, making enforcement or fixing any security problems fraught with difficulty. And when the function is re-used, the same security issues are re-populated in different parts of development.

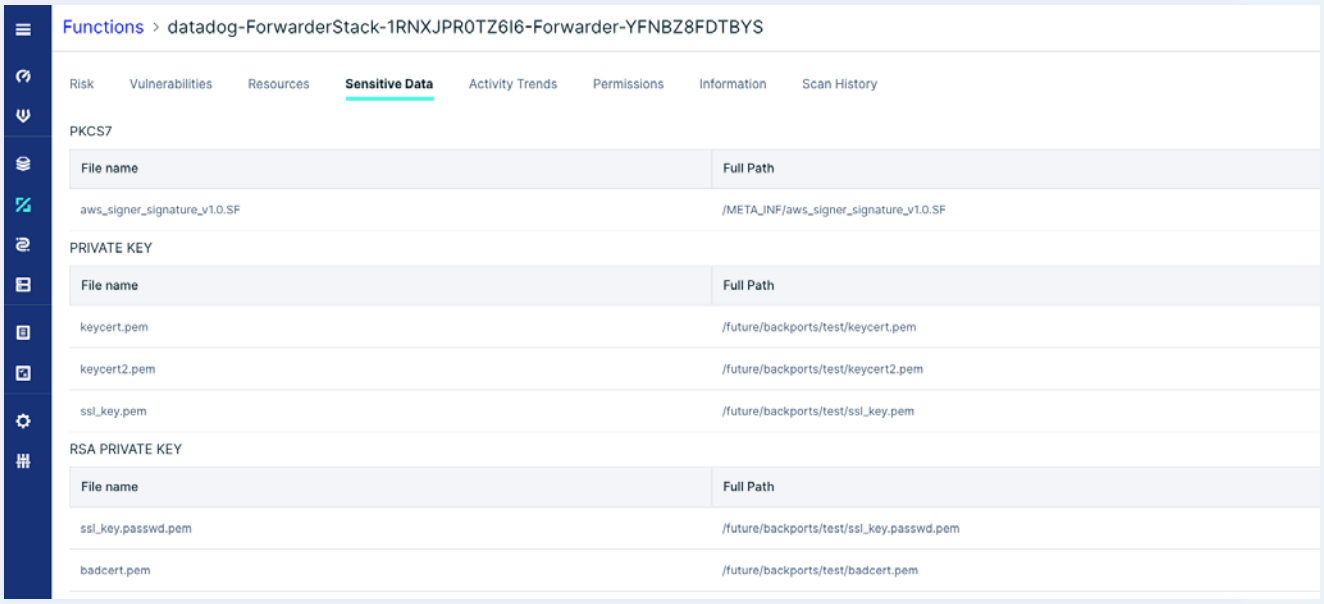
Therefore, it is critical to ensure functions are both secure before being launched into production as well as secured with a purpose-built enforcement mechanism specifically equipped for functions. Due to the speed and the vast number of functions, prevention of the most prominent issues should be done automatically using dedicated serverless security controls.

The unique security challenges of a serverless architecture

Malware, Vulnerabilities & Embedded Secrets

While the cloud provider handles the risk of vulnerable servers, the function may contain vulnerable code, dependencies (e.g., third-party libraries), and open-source packages, which an attacker can still exploit.

Ongoing Function Scanning
Aqua vulnerability scanning allows for the vulnerability of function code scans for open-source components and suspicious dependencies, as well as overprovisioned privileges. It creates an inventory of the installed packages for each function, making it easy to track which functions are influenced by vulnerable source code for fast and effective remediation. Further, Aqua scans for hardcoded secrets (e.g., SSH keys, RSA keys, access and security keys for cloud accounts, etc.) within functions. After running a scan, Aqua generates an inventory view of secrets and their locations.

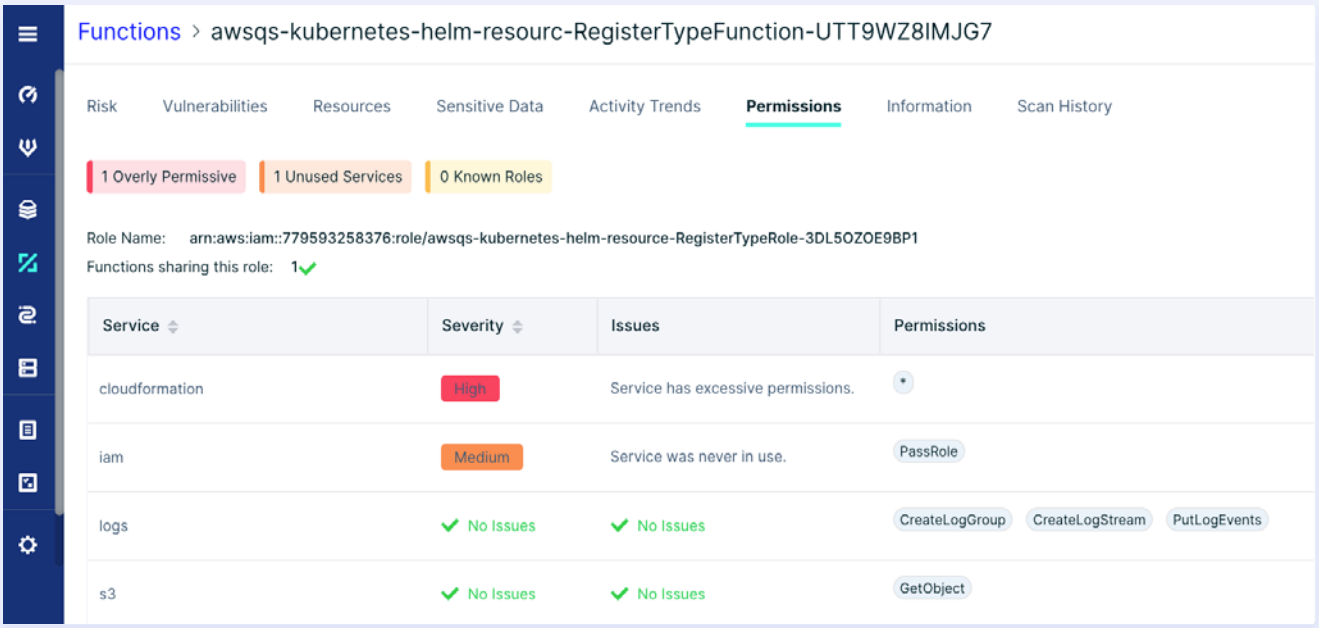


Over-Provisioned Access Permissons

Too often, serverless function accounts are over-provisioned by developers in the build phase. This, in turn, grants privileged access to other functions and resources beyond the scope of the task, which persist into production. When a function is launched, it is difficult to change and reduce its privileges due to the potential harm to other functions/service dependencies.

Applying Function Least-Privileges Enforcement

Aqua automatically discovers overprovisioned function permissions by scanning function IAM roles and highlighting risky permissions.

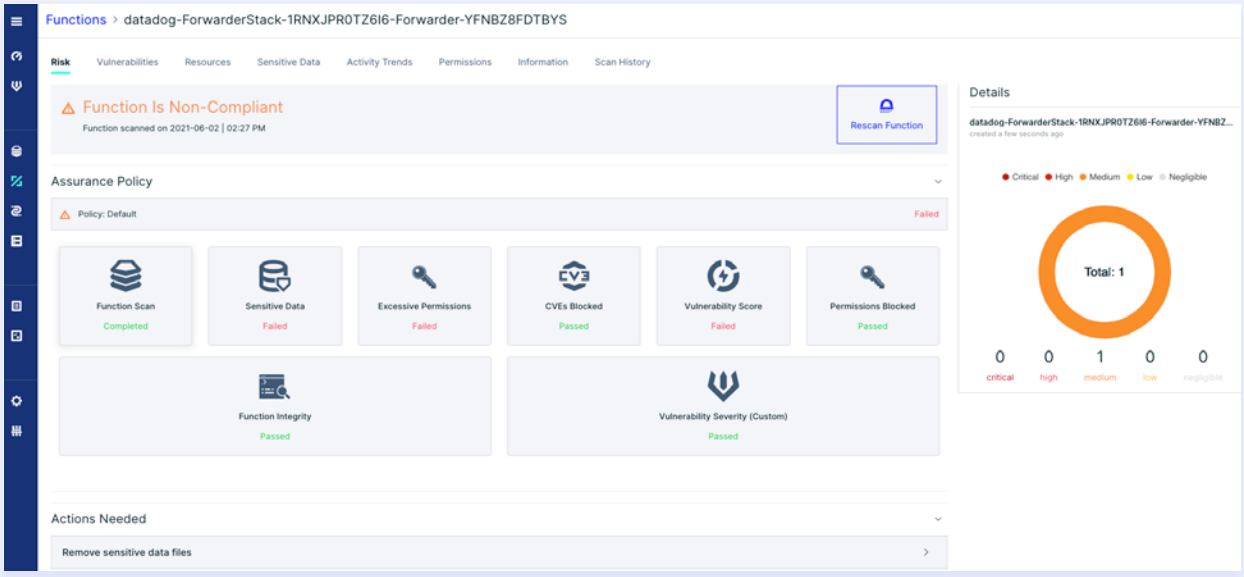


Limited Visibility

Compared to containers, it can be difficult to identify where and when a function runs. For example, two invocations of the exact function can run on completely different nodes. Therefore, it is critical to monitor and audit security data for functions.

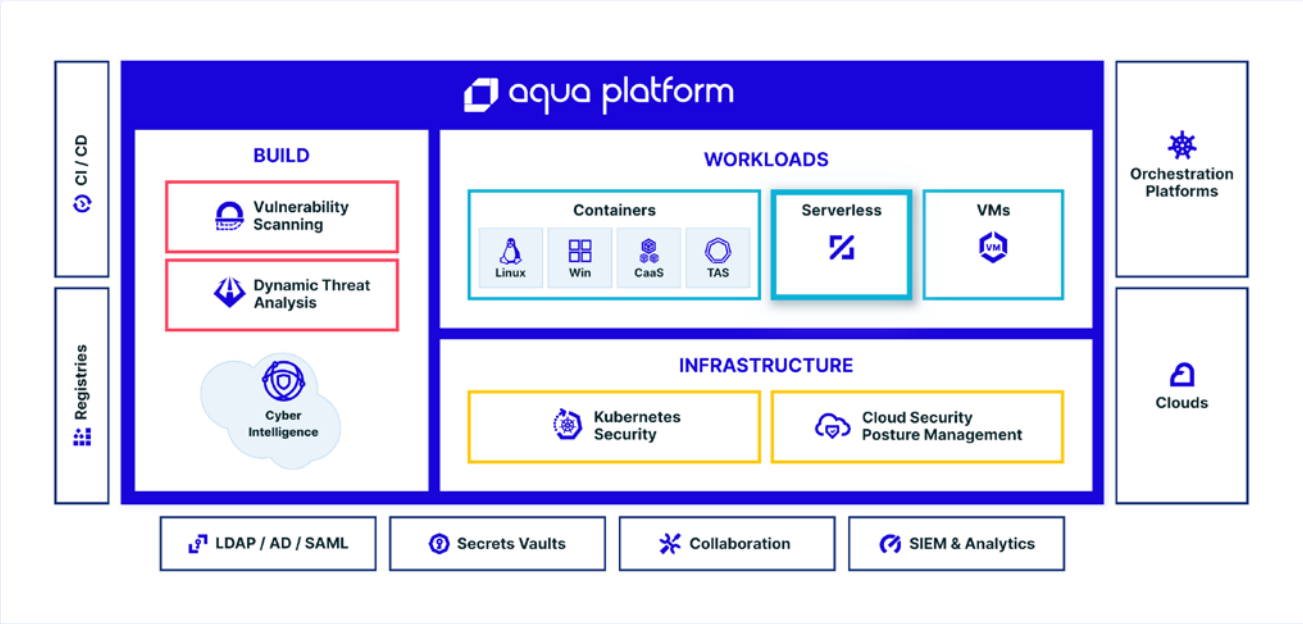
Ongoing Monitoring & Reporting

Aqua generates audit data of scanned functions for malware, vulnerabilities, sensitive data, and secrets, tracking changes in vulnerability status, timeliness of scan, and remediation trends. In addition, Aqua's function dashboard enables live monitoring so functions can be mapped by region, application, account, or any type of configured parameter.



A single pane of glass across all three major cloud providers

Aqua provides you with a single pane of glass for all three leading brands, providing complete security coverage for multi-tenant environments. Ensure you enforce a single security policy in all your environments, with full lifecycle security controls and management for multiple team deployments from a central console.



Ensure that your serverless environment is free from known security risks through continuous discovery, scans, and monitoring.

Risk Posture Discovery

- Automatically retrieve and scan inventory of serverless functions from your cloud accounts
- Gain holistic visibility of your functions' risk posture
- Send scan results and security events data to your existing SIEM and analytics tools

CI/CD Integrations

- Scan serverless functions as they are built in your CI pipeline, providing feedback to developers on security issues
- Automatically fail the build of serverless functions based on a preconfigured assurance policy
- Integrate with the CI tool of your choice: Jenkins, Bamboo, CircleCI, TeamCity, Gitlab, and more

Function Risk Assessment

- Scan for known vulnerabilities based on multiple public, vendor-issued, and proprietary sources
- Detect over-provisioned or unused permissions or administrative roles that should be reduced or eliminated
- Discover sensitive data (access credentials, keys) embedded in functions or their environment variables

Function Assurance

- Prevent execution of functions that present an unacceptable risk according to your organization's regulations
- Define assurance policies based on vulnerability scores, detected permissions, and sensitive data
- Get notifications and generate audit events when functions are blocked from executing

Runtime Protection (Lambda)

- Deploy Aqua's NanoEnforcer by injecting it automatically as a Lambda Layer with no modifications to the function code or its runtime
- Maintain function's integrity and prevent drift, validate that it has not been changed or updated during its lifecycle in the cloud
- Protect the function's "/tmp" directory against unauthorized abuse, blocking code injection
- Control the types of executables that can be used in functions by listing blocked executables

Honeypot Malicious Actors (Lambda)

- Insert an AWS account credentials into Lambda functions where attackers would likely seek them. It is recommended that this user be assigned an empty role (therefore having no access to resources)
- Continuously monitor the accounts to detect attempts to use the credentials as a clear indicator of compromise of your Lambda environment