Red Canary Cloud Protection

The cloud has enabled every organization to innovate faster, transforming development processes and decentralizing infrastructure ownership. However, as businesses move to the cloud, security teams are tasked with solving one of the biggest problems they've encountered in decades—reducing cloud risk as their attack surface expands. Compounding this problem is the fact that 92 percent of organizations use more than two public clouds, according to Cisco research. This requires security teams to develop even greater knowledge and expertise in order to protect their multi-cloud environment.

Cloud Protection Bundle Summary

Red Canary integrates directly with your IaaS environment, the cloud workloads you have created, as well as third-party cloud security tools to help secure the entirety of your cloud. The bundle is broken down into three primary components based on coverage type:

Control Plane

Red Canary helps prevent the malicious monetization of your cloud environment via ransomware or data exfiltration/extortion threats. We identify and stop credential based attacks (account compromise, social engineering, brute force, etc), cloud token theft, and system/policy misconfigurations. We support:

- AWS CloudTrail and GuardDuty
- Microsoft Azure Audit Logs and Defender for Cloud
- Third-party cloud security tools like Lacework and Wiz
- GCP Audit Logs coming soon

Cloud Instances

Our team of Linux and cloud workload security experts monitor your environments to identify threats to your virtual machines, containers, kubernetes, and other cloud resources.

Red Canary Linux EDR

Red Canary's Linux EDR agent was built from the ground up by Linux experts. Lightweight and designed specifically for production environments, our agent protects you with minimal performance impacts or downtime.

> "Red Canary's detection capabilities allow us to sleep better at night, as well as free up my team to focus on other projects."
>
> **CHIEF INFORMATION SECURITY OFFICER, GLOBAL ACCOUNTING FIRM**

Cloud Protection Benefits

- Get 24x7x365 monitoring across both your cloud control plane and runtime instances to secure your multi-cloud environment.
- Find cloud threats others miss as Red Canary ingests raw event data correlated with posture management based alerts from tools like Wiz and Lacework.
- Add multi-cloud threat intelligence, threat hunting, and a rapidly expanding library of cloud detectors to your SOC.
- Detect cloud runtime threats across your workloads and containerized environments with the help of our Linux security experts.
- Deploy in minutes to close visibility gaps, reduce the complexity of securing your cloud environment, and detect threats faster.
- Respond quicker with Red Canary's automated response capabilities and guided remediation.