

# Cloud Workload Protection Questionnaire

A cloud workload protection platform plays an important role in a cloud defense in depth strategy. CWPP stops what other security controls cannot or do not: runtime threats such as ransomware, cryptominers, zero days, and more. Behavioral AI detects and responds to these attacks as they occur, to protect your hybrid cloud infrastructure and keep your business running.

Enterprise CISOs are invited to use this questionnaire to lead conversation among their security and cloud architecture teams on how CWPP fits in their stack.

## Cloud Security Strategic Baseline

- ✓ On which clouds do we run workloads: AWS, Azure, Google Cloud, private data centers?
- ✓ What type of cloud infrastructure: cloud compute instances (VMs), containers, Kubernetes (managed or self-managed)?
- ✓ How do we secure the cloud control plane? Example: tiered admin with increasing levels of MFA, logging of admin accounts, etc.
- ✓ Which Linux distributions do our workloads use across all clouds?
- ✓ How do we reduce the attack surface of containerized workloads? Example: secrets management, private registry, SCA, etc.
- ✓ Do we have a cloud tagging policy, is it consistently followed, and does it help route security tickets immediately to the appropriate DevOps owner?
- ✓ Do we use IaC templates for infrastructure provisioning?
- ✓ How does my cloud security strategy support our 1, 3, and 5 year plans?

## CWPP: Real-Time Detection & Response

- ✓ Do we have CWPP in use today?
- ✓ Do my I&O counterparts understand the benefits of CWPP to our cloud business?
- ✓ Does my team have continuous runtime visibility at the OS-level?
- ✓ How long do we retain workload telemetry for use in investigation and threat hunting?
- ✓ Does our CWPP agent require kernel dependencies? If so, have my business stakeholders complained about workload outages? Friction in CI/CD pipeline?

Through comparative analysis of current and future cloud security states, a CISO can envision and quantify the benefits and incremental costs of new security initiatives. In so doing, security leaders are better able to make their case, secure funding, and position their team as an instrumental partner to the business.



# Singularity Cloud

Singularity Cloud Workload Security is a CWPP solution that transforms visibility into cloud workloads. Patented behavioral AI continuously checks for runtime threats, to respond in real time. Our cloud-native agent supports 13 Linux distributions and is built on eBPF, operating in user space for maximum stability. Workload telemetry is streamed to the Singularity XDR Platform for investigation and threat hunting.

**LEARN MORE AT**  
[www.sentinelone.com/platform/singularity-cloud/](http://www.sentinelone.com/platform/singularity-cloud/)

## Innovative. Trusted. Recognized.



**A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms**



**Record Breaking ATT&CK Evaluation**

- 100% Protection. 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays



**96% of Gartner Peer Insights™**

EDR Reviewers Recommend  
SentinelOne Singularity



### About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity Platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

### sentinelone.com

sales@sentinelone.com  
+ 1 855 868 3733