cybereason® | PRODUCT BRIEF

# Cloud Workload Protection

## EXTEND PROTECTION TO CLOUD WORKLOADS

### KEY BENEFITS

**Secure** workloads in public clouds, private clouds, on-premises, or in hybrid infrastructure

**Highly performant** runtime protection; minimal resource consumption

**Simple** and automated deployment

**Business Context** Tagging that accelerates collaboration with DevOps

**Comprehensive** understanding of threats with the MalOp view

**Automated** Response Actions

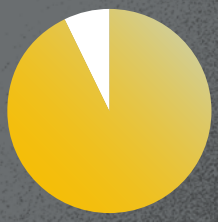
**Unified protection** across cloud workloads, endpoints, and extended resources

### Protect Workloads Everywhere with Minimal Impact

Organizations today operate in a complex world with data and workloads on-premises, in the public cloud, at the edge, and in hybrid configurations. Cybereason Cloud Workload Protection is designed to protect workloads and containers wherever they reside or move across infrastructure. This cloud-native solution extends Kubernetes integration and powerful sensors across the environment, providing the most effective threat detection and prevention available. All while reducing performance impact by deploying highly-tuned sensors across the environment that offer significantly better performance than competitors.

### Visibility That Bridges DevOps & SecOps

Traditional silos that exist between SecOps and DevOps teams increase operational friction and decrease response times. Built from the ground up to bridge the gap between DevOps and SecOps teams, Cybereason Cloud Workload Protection is designed to deliver frictionless deployment that automatically updates and scales, improves understanding, and causes minimal impact to consumption costs. Business Context Tagging decreases remediation time and facilitates effective cooperation between DevOps and SecOps teams by ensuring a universal understanding of impacted resources.



93%

**Reduction in time spent on detection and response to threats.**

Forrester Total Economic Impact Report

## SIMPLE AND AUTOMATED DEPLOYMENT

Automate deployment with your existing orchestration tools such as

- CHEF
- PUPPET
- ANSIBLE
- TERRAFORM

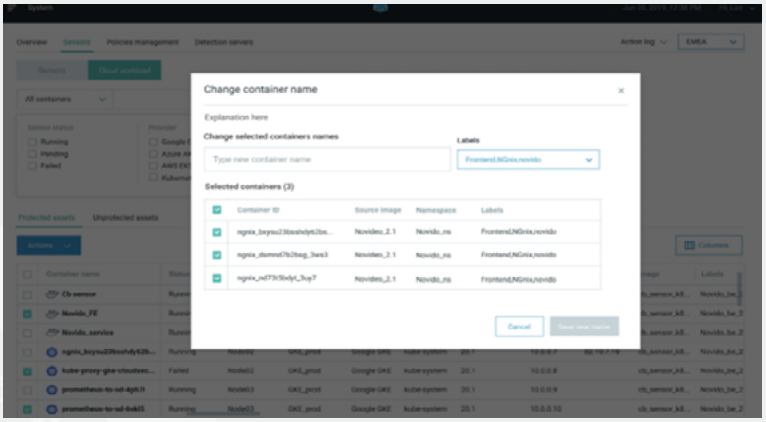
A Kubernetes Helm Chart and single-line installation scripts enable automated continuous deployment.

## Deep Detection & Automated Response at Petabyte Scale

Leveraging AI, the Cybereason MalOp™ Detection Engine transforms petabytes of data every day from the public cloud, on-premises, and hybrid environments into visual attack stories that provide a comprehensive view of the threat. Broad visibility across workload telemetry and the Kubernetes control plane provide a complete threat picture in a simple to understand and actionable platform. Single-click threat remediation actions, and unique automatic response rules result in a 93% reduction in time spent to detect and respond.

## Business Context Tagging

Effective collaboration requires that all parties are working off of the same information. Frequently, security teams refer to resources with different identifiers than those used by DevOps, creating friction and slowing resolution. Business Context Tagging in Cybereason Cloud Workload Protection pulls in the tags the DevOps team has implemented through Kubernetes directly into the view the Security team uses, ensuring a common understanding of impacted resources and accelerating response.



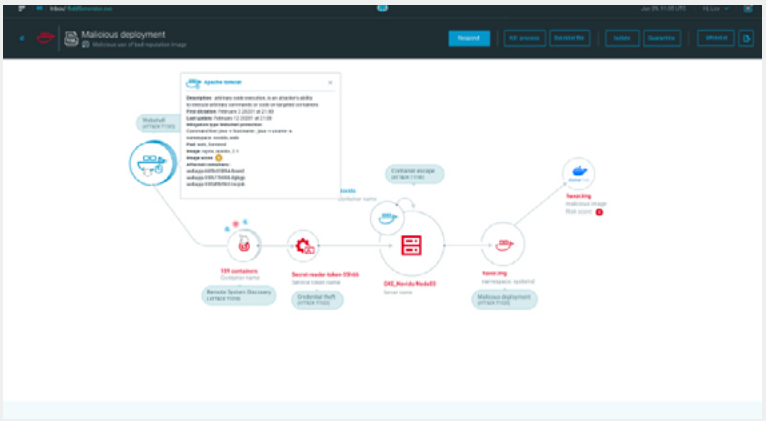

Business Context Tagging

## MalOp™ View

Most solutions rely on an alert-centric approach to security, creating a deluge of piecemeal and unactionable alerts. Cybereason takes an operation-centric approach, where all the disparate pieces of an attack across all cloud and on-premises resources are collated into a single notification—what we call a MalOp view, short for malicious operation. Automation and machine learning ensures that all relevant data is collected, processed, and analyzed in real-time so that the details of an attack are delivered as a fully contextualized and correlated insight into the attacker's holistic malicious operation.

## Automated Response Actions

Threats evolve rapidly in cloud workloads making fast and efficient response imperative to avoiding disruptions of mission-critical applications. With Cybereason Cloud Workload Protection, analysts can confidently execute a full suite of remediation actions—from container or host isolation to killing processes—with a single click all from within the MalOp view. Furthermore, Automatic Response Rules enable the resolution of common issues without analyst intervention.




MalOp View

## PART OF THE CYBEREASON DEFENSE PLATFORM

The Cybereason Defense Platform represents the first time the security industry has combined threat activity across endpoints, workstations, workspace and productivity tools together with the threat activity occurring in cloud workloads. Only the Cybereason Defense Platform can give you a fully contextualized view of a malicious operation—called the MalOp view—happening across resources operating on-premises, remotely in employee homes, and in the cloud. A drastic reduction in security tooling fragmentation means streamlined management and most importantly fewer security events.

## ABOUT CYBEREASON

Cybereason partners with Defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the Cybereason Defense Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.