SentinelOne

Cloud Native Security

Agentless CNAPP with a unique Offensive Engine

Cloud security is broken and outdated. Traditional solutions offer siloed capabilities with inefficient outcomes resulting in security spending time on establishing context across alerts and eliminating false positives. Even then attackers find novel ways of infiltrating infrastructure and deal serious damage to an organization's IT. But what if a tool could imitate an attacker and highlight the most critical problems to address first?

Cloud Native Security (CNS) is an agentless CNAPP solution with a unique offensive engine that prioritizes vulnerabilities that are truly exploitable. Unlike other solutions that only list all theoretically exploitable alerts, CNS provides evidence of exploitability with every vulnerability to save time spent by security teams on validation and prioritization of alerts. Combine it with the AI-powered threat blocking of SentinelOne's agent-based Cloud Workload Security and organizations have a comprehensive security solution for their cloud environment.

Instant Visibility

Agentless onboarding creates asset inventory within minutes of connecting to cloud account.

Verified Exploit Paths™

Safely simulate harmless attacks on cloud infrastructure to move beyond theoretical attack paths to identify vulnerabilities that are truly exploitable.

Prevent Secrets Leakage

Identify more than 750 types of secrets hardcoded across code repositories.

Cloud Native Security delivers multi-cloud support for:

aws

Google Cloud

Azure

ORACLE
Cloud Infrastructure

DigitalOcean

Alibaba Cloud

>6 hours

Spent on average by issue owner on research and validation of an issue[1]

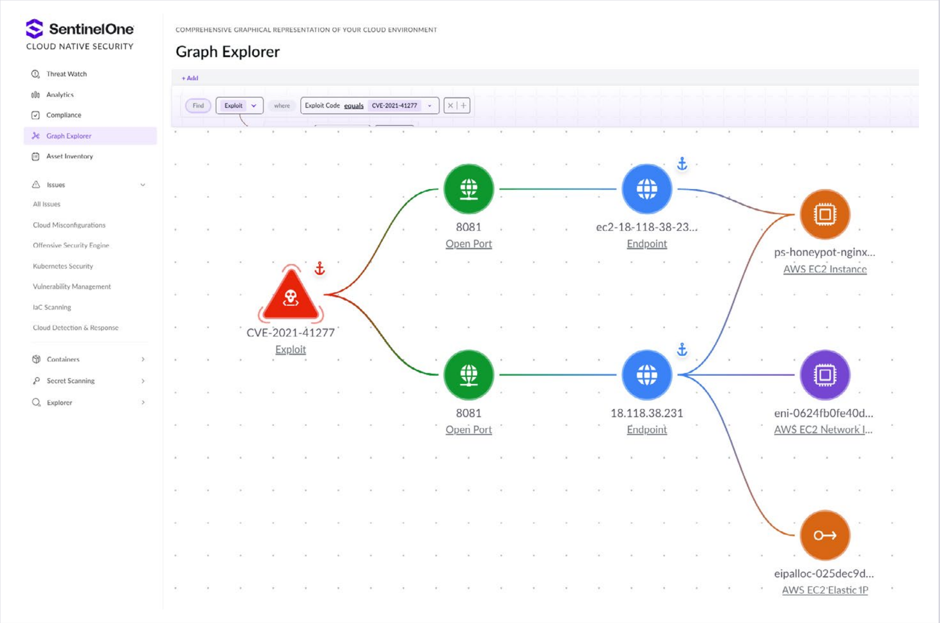
Key Features And Benefits

- + Offensive Security Engine
- + Secrets Scanning Engine
- + Cloud Security Posture Management (CSPM)
- + Cloud Detection and Response (CDR)
- + Software Bill of Materials (SBOM)
- + Agentless Vulnerability Scanning
- + Infrastructure as Code (IaC) Scanning
- + Kubernetes Security Posture Management (KSPM)
- + Compliance Dashboards
- + Enhanced by Security Graph

PeerSpot

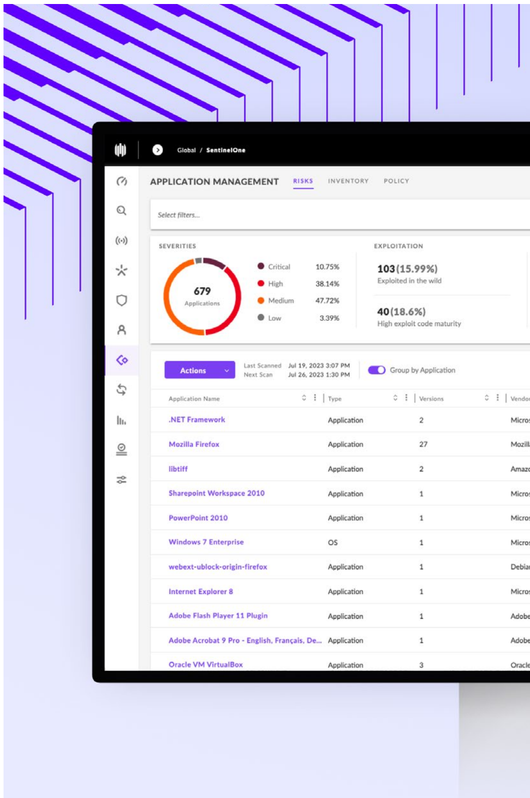
> “
>
> The offensive security feature is something no other product offers.
>
> **Cloud Security Engineer**
>
> FINANCIAL SERVICES, 10K+ EMPLOYEES

[1] The State of Security Remediation 2024, Cloud Security Alliance



COMPREHENSIVE GRAPHICAL REPRESENTATION OF YOUR CLOUD ENVIRONMENT

Graph Explorer



Application Name	Type	Versions	Vendo
.NET Framework	Application	2	Micros
Mozilla Firefox	Application	27	Mozill
libtiff	Application	2	Amazo
Sharepoint Workspace 2010	Application	1	Micros
PowerPoint 2010	Application	1	Micros
Windows 7 Enterprise	OS	1	Micros
webext-ublock-origin-firefox	Application	1	Debiar
Internet Explorer 8	Application	1	Micros
Adobe Flash Player 11 Plugin	Application	1	Adobe
Adobe Acrobat 9 Pro - English, Français, De...	Application	1	Adobe
Oracle VM VirtualBox	Application	3	Oracle

Offensive Security Engine

CNS' Offensive Security Engine automatically and safely simulates harmless attacks on cloud infrastructure to validate the exploitability of vulnerabilities. With a single click of a button evidence of exploitability is generated to prioritize the truly critical alerts from theoretically exploitable attack scenarios . By incorporating CNS' capability to provide Verified Exploit Paths™ security teams can significantly increase their efficiency and focus on remediating the truly critical alerts.

Secure your cloud environments from code to deployment

✓ Secret Scanning

- CNS scans public and private repositories of the organization AND public repositories of the associated developers to prevent leakage of secrets and credentials
- CNS identify over 750 types of hard coded secrets

✓ Shift Left

- Shift left to identify pre-production issues in IaC templates and container configuration files like Terraform, CloudFormation, and Kubernetes (both helm and manifests)
- CNS lists SBOM at a container image level to identify and eliminate vulnerabilities before they reach production

✓ Cloud Detection & Response

- Use out of box rules and create custom policies for cloud resources via simple rego script to cover events specific to your environment
- Using Security Graph to write and export queries to apply custom policies to specific group of resources with a single click of a button

Singularity Platform

Proactively resolve threats in real-time at the site of the cybersecurity battle: the computing and cloud edge.

Ready for a Demo?
Visit SentinelOne.com for more details.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights™

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FR FedRAMP — TEVORA PCI DSS Attestation HIPAA Attestation — AICPA SOC — STAR LEVEL ONE — vb 100 VIRUS virusbtn.com — SE Labs BEST Innovator WINNER 2021 — SE Labs AAA — Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733