

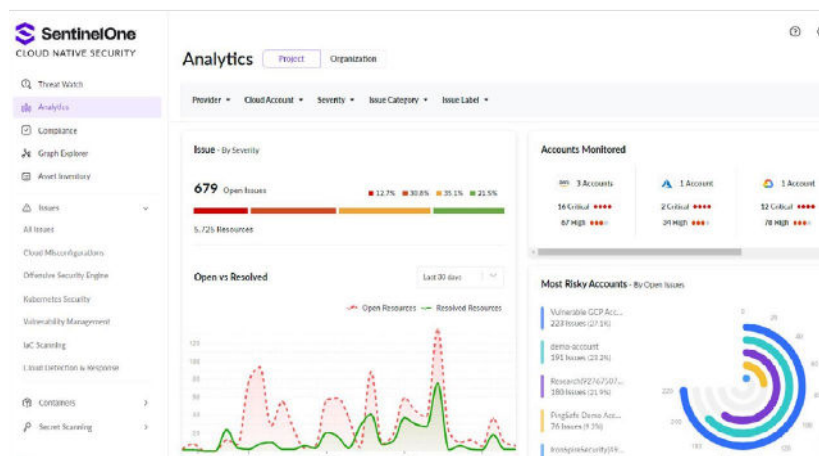
N-able Endpoint Detection and Response (powered by SentinelOne)

Cloud Native Security

Protect Modern Cloud Environments with Confidence

Cloud environments change fast, and so do cloud threats. For MSPs and IT teams, staying ahead requires more than visibility. It demands clarity, prioritization, and swift action on what matters most.

Cloud Native Security (CNS) extends N-able EDR Complete with **agentless cloud visibility, evidence-backed risk prioritization, and automated insights** that help service providers simplify cloud protection across AWS, Azure, and Google Cloud environments.



It is modern cloud security designed for real-world workloads, lean teams, and MSP scalability needs.

Why CNS matters for MSPs and IT Pros

✓ Instant value, no agents, no delays

Connecting a cloud account takes minutes, giving you an immediate inventory of cloud assets, configurations, and risks—no deployments, no performance impact, and no customer disruption.

✓ Less noise, more signal

CNS cuts through thousands of theoretical alerts by safely simulating attacker paths to confirm what is truly exploitable. Your teams spend less time validating alerts and more time fixing what matters.

✓ Proactive protection against credential-based breaches

With attackers increasingly “logging in instead of hacking in,” CNS helps stop leaked or hardcoded secrets before they become entry points into customer environments.

✓ Unified visibility to help you scale your services

One view across endpoints (via N-able EDR), cloud configurations, containers, identities, and workloads means you can reduce tool sprawl and spend less time stitching together context from multiple consoles.

Cloud Native Security

Key outcomes

1. Dramatically reduce cloud security noise

Most CNAPP tools drown teams in theoretical vulnerabilities. CNS shows you only what attackers can exploit so that your team knows what to fix first.

2. Strengthen customer defenses against leaked credentials

CNS detects 750+ types of hardcoded secrets across private and public repositories, including developer-associated repos many tools miss.

3. Improve compliance outcomes with less effort

CNS highlights misconfigurations mapped to frameworks like CIS, NIST, and MITRE,

giving you an effortless way to maintain and demonstrate continuous compliance.

4. Support multi-cloud environments without adding complexity

CNS delivers consistent detection, risk scoring, and reporting across AWS, Azure, and Google Cloud, making it ideal for teams managing mixed environments.

5. Shorten investigation and remediation time

Graph-based views and SentinelOne's Verified Exploit Paths™ clarify relationships between misconfigurations, workloads, and vulnerabilities, significantly speeding up triage

Technical capabilities

Cloud Native Security delivers multi-cloud support for:

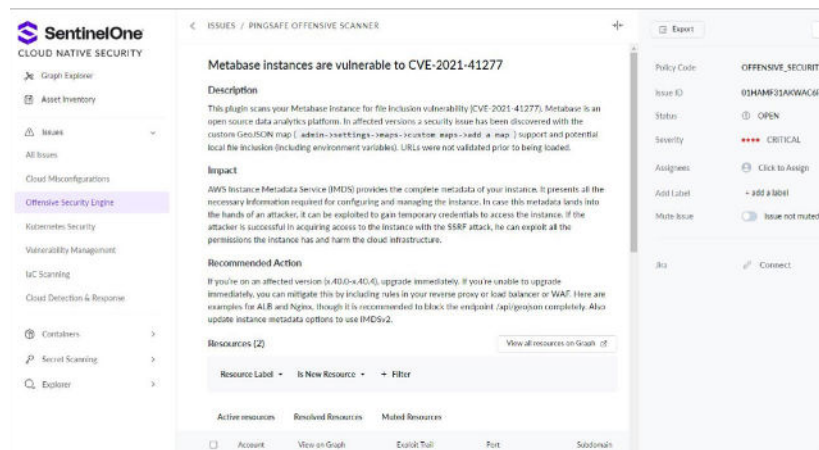
AWS	Oracle Cloud Infrastructure
Azure	Alibaba Cloud
Google Cloud	DigitalOcean

Agentless Cloud Security Posture Management (CSPM)

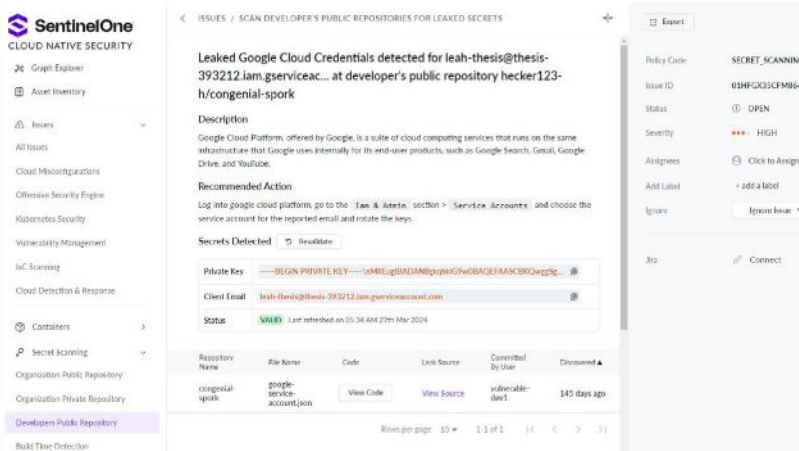
- ✓ 2,000+ configuration checks
- ✓ Near real-time detection of misconfigurations
- ✓ Custom policies with simple Rego scripting

Offensive Security Engine with Verified Exploit Paths™

- ✓ Safely simulates attacker behavior
- ✓ Validates exploitable vulnerabilities
- ✓ Prioritizes real-world risk vs. hypothetical findings



Cloud Native Security



Secrets Scanning

- ✔ Detects 750+ types of leaked secrets or credentials
- ✔ Scans both internal and developer-linked public repos

Kubernetes Security Posture Management (KSPM)

- ✔ Deep visibility into clusters, pods, workloads, and roles
- ✔ Benchmarks for EKS, GKE, and AKS

Agentless Vulnerability Scanning

- ✔ Generates SBOMs for container images
- ✔ Highlights affected services and dependency paths

Infrastructure as Code (IaC) Scanning

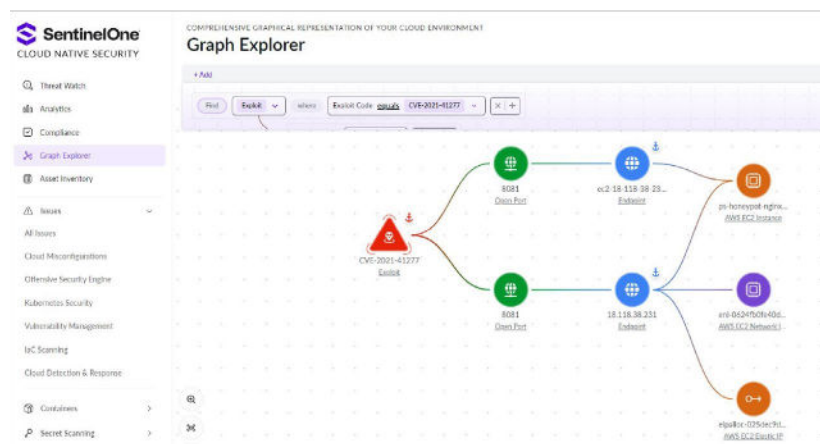
- ✔ Scans Terraform, CloudFormation, Helm, and K8s manifests
- ✔ Identifies misconfigurations before deployment

Cloud Detection and Response (CDR)

- ✔ Out-of-the-box rules
- ✔ Custom policies for cloud events

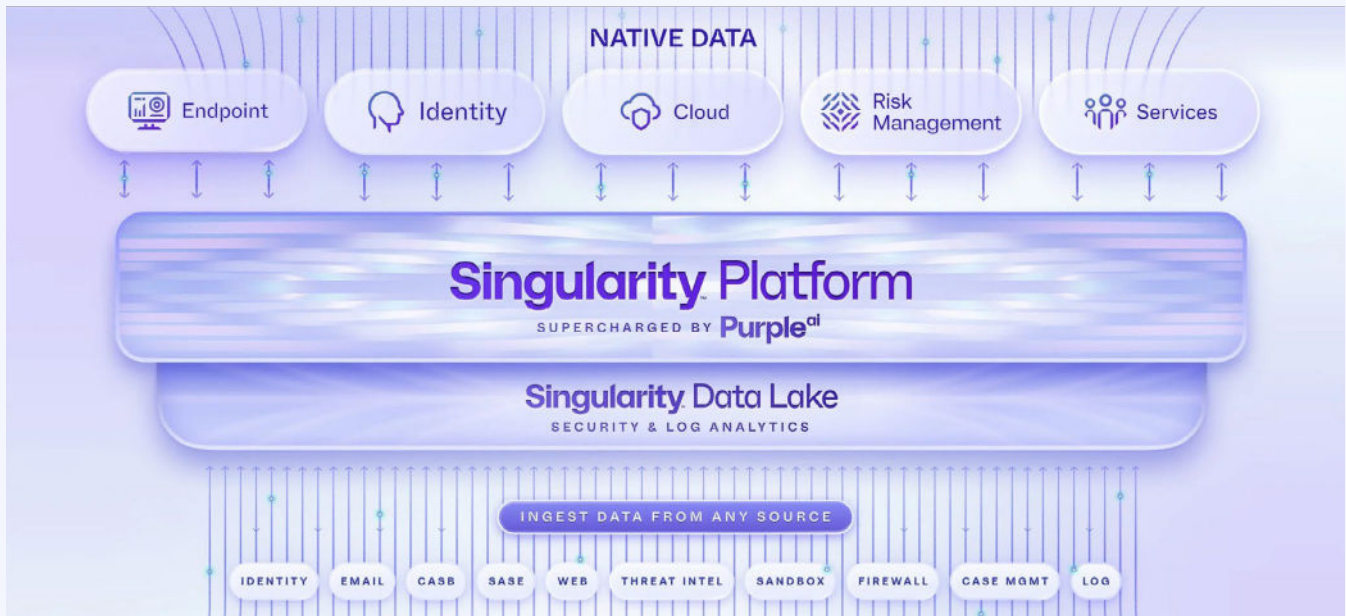
Graph Explorer

Graph Explorer facilitates the investigation of Verified Exploit Paths through visual analysis of the potential blast radius of cloud resources affected by an identified vulnerability. It also includes a convenient means of intuitively writing queries via the visual interface to quickly create and apply custom policies to a specific resource group with a few simple clicks.



Cloud Security in the Singularity™ Platform

The Singularity Platform offers comprehensive threat prevention, detection, and response that is easy to use and spans complex enterprise environments.



Innovative. Trusted. Recognized



Record Breaking ATT&CK Evaluation

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



N-able protects businesses from evolving cyberthreats. Our AI-powered cybersecurity platform delivers business resilience to more than 500,000 organizations worldwide, leveraging advanced end-to-end capabilities, simplified workflows, market-leading integrations, and flexible deployment options to improve efficiency and drive critical security outcomes. Our partner-first approach pairs our technology with experts, training, and peer-led events that empower customers to be secure, resilient, and successful.
n-able.com

This document is provided for informational purposes only. Information and views expressed in this document may change and/or may not be applicable to you. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein.

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.