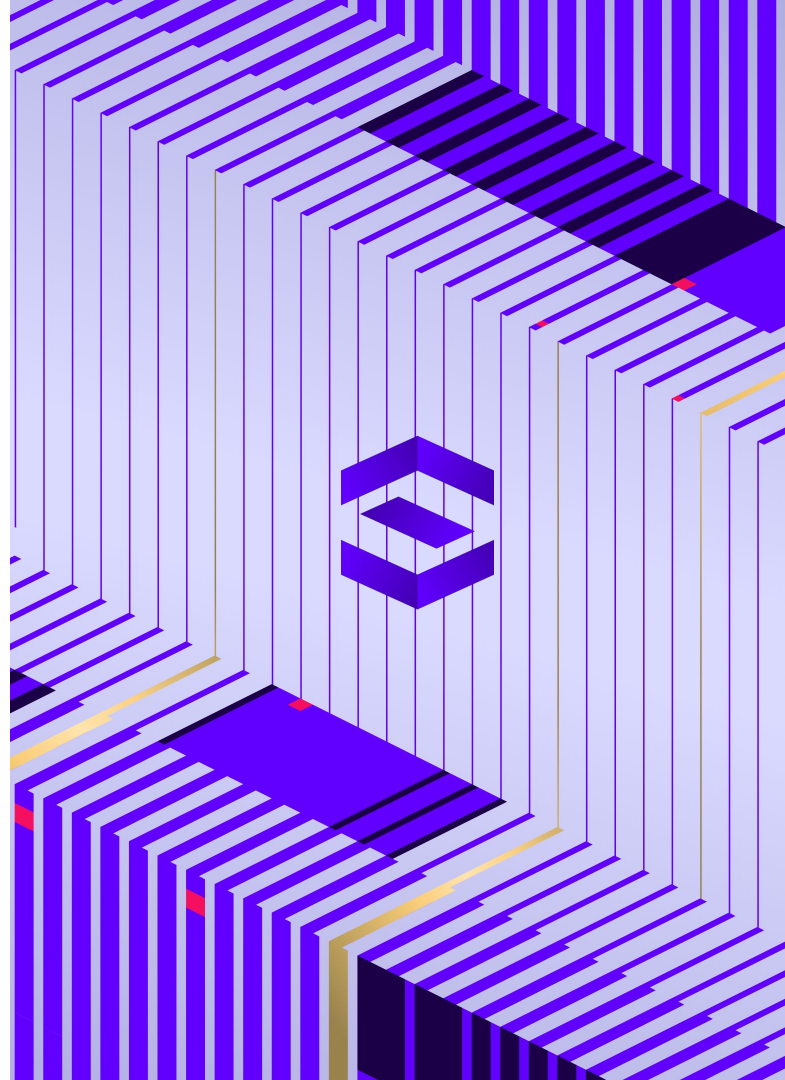


SentinelOne CNAPP – Know It. Secure It. Scale It.

Dora Beller

Product Manager

dora.beller@clico.hu



Cyber company with highest growth



2,500+ EMPLOYEES
12,200+ CUSTOMERS

Including 3 of the Fortune 10
10 of the CAC 40

GLOBAL DATA CENTERS

AWS US, Frankfurt, Tokyo,
Canada, Singapore, GovCloud

Google Cloud Platform



HQ in USA, Founded in 2013

S
LISTED
NYSE

Greatest Valued Cyber IPO in 2021
\$8B Valuation



40% ARR Growth YoY – with \$762 M ARR in 2024

Multiple acquisitions:

Scalyr, Attivo Networks, PinnacleOne,
PingSafe, etc...

More info @ investors.sentinelone.com



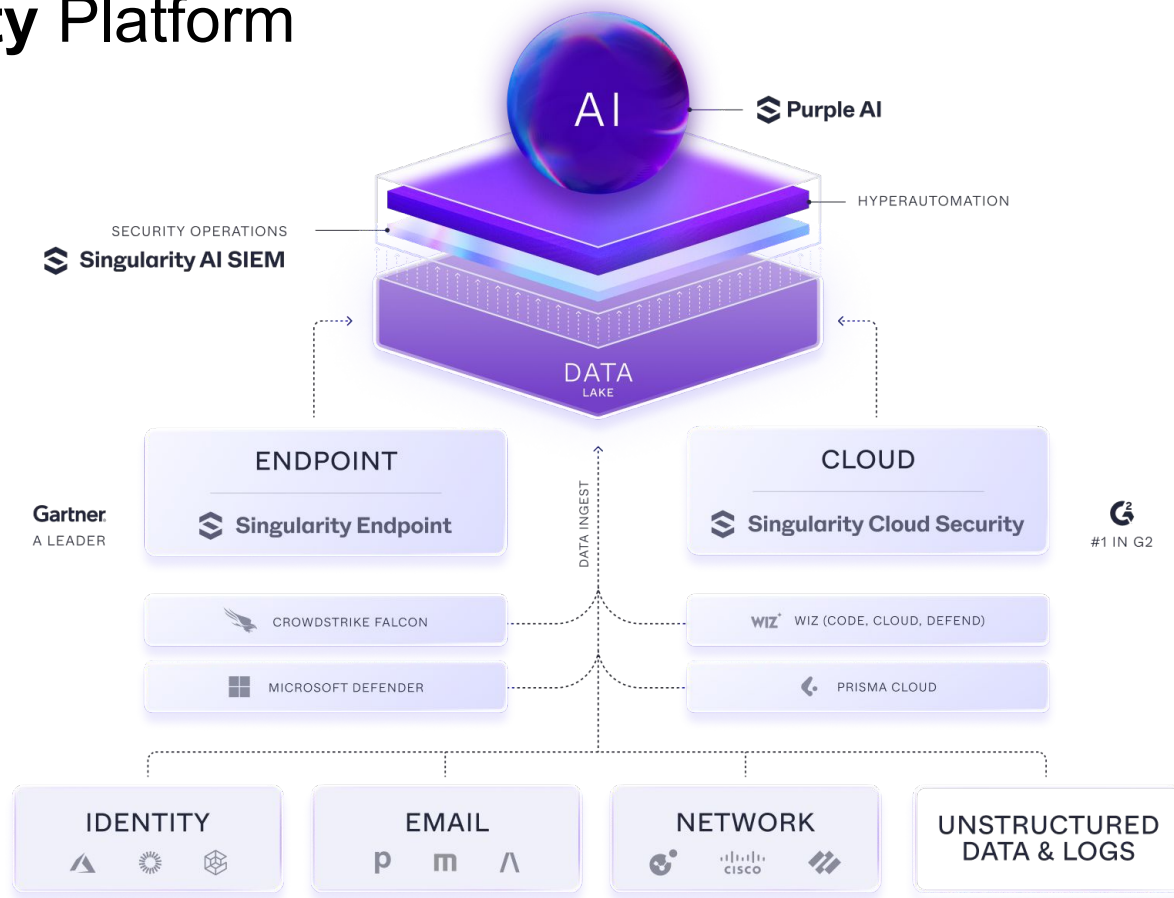
SentinelOne®

TO ACQUIRE



observo.ai

Singularity Platform

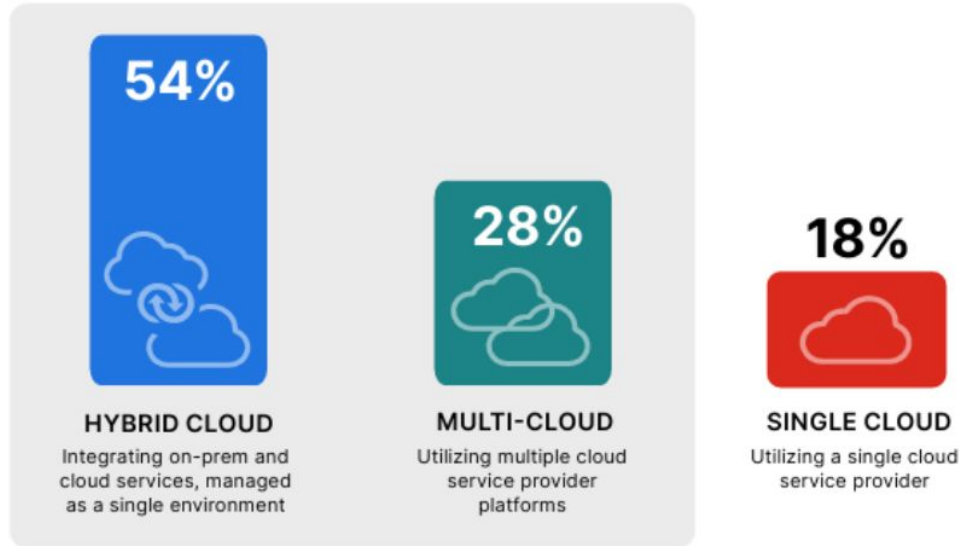


Operational Challenges in Cloud Security

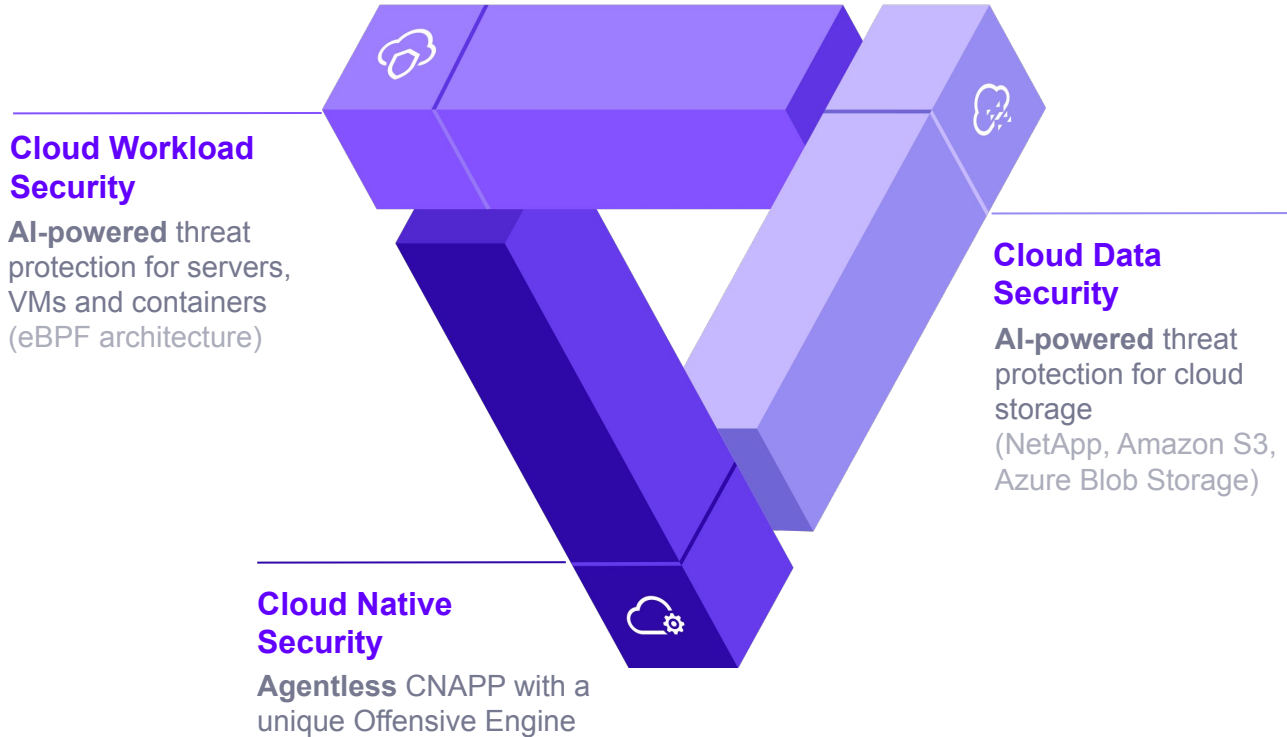


Shifting Cloud Deployment Strategies

82% of organizations are using a multi-cloud or hybrid environment



Cloud Native Application Protection Platform (CNAPP)



Cloud Workload Security



Stability and Performance

eBPF framework. No kernel dependencies. Low CPU and memory usage.



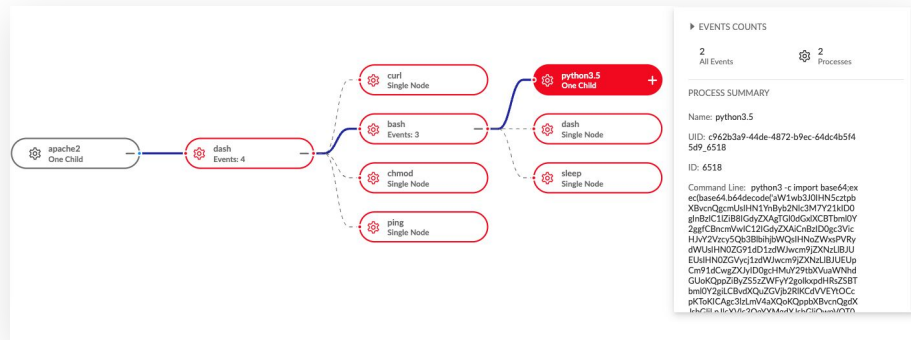
Broad support

for 17 Linux distros. Popular container runtimes (Docker, containerd, cri-o), with / without orchestration.



Hunting and Forensics

Unified XDR integration into Singularity Data Lake. AI-powered insights.



Cloud Data Security



Local and Compliant

Scan objects directly in your storage, no sensitive data leaves your environment



Automated Response

Automated quarantine of malicious objects.



Detection Without Delay

Detect malware and zero-day exploits in milliseconds.

doki_modified detected as Malware

Mitigated Medium Malware Mar 2, 2024, 13:50:33

Alert Status: New Assigned To: Analyst Verdict: Undefined

Alert Description and Recommendations

Windows file events analysis detected a malicious file known to SentinelOne's Cloud Intelligence

[More Details](#)

Threat Intelligence 0 events scanned, 0 Threat intelligence indicators detected

Detection Details		Target Asset	
Confidence Level	Malicious	Target Name	TheBorg-KVNV
Detection Engine	SentinelOne Cloud	Scope	tkaspar/UFP/Storage
Detection Type	Learning	OS Type	Unknown
Storyline ID	8cc04263-f490-8abd-d0...		More Details
Process User	192.168.192.10		

Cloud Native Security



Offensive Security Engine

Prioritize cloud health and remediation. More than ~2,100 checks, including CVEs



Secret Scanning

Identify more than 750 types of secrets hardcoded across code repositories



Container and K8s Security (KSPM)

Shift-left scanning of container-related misconfigurations in IaC, such as Helm Charts.

The screenshot displays the SentinelOne Operations Center interface. The main panel shows a list of vulnerabilities under the 'EXPOSURES' tab, filtered by 'Last Year'. The table includes columns for CVE ID, Description, Severity, and Status. A detailed view of CVE-2023-29405 is shown on the right, titled 'The go command may execute arbitrary code at build time when using cgo. This may ...'. The detailed view includes a severity of 'Critical', a date of 'Apr 9, 2025 4:07:27 PM', and a description of the vulnerability. Below the description, there is a section for 'Affected Asset' with details about the cloud account, asset name, and other relevant information.

CVE ID	Description	Severity	Status
CVE-2023-29405	Malicious Code Execution ...	Critical	Now --
CVE-2023-29402	Unexpected Code Genera...	Critical	Now --
CVE-2023-29404	Arbitrary Code Execution ...	Critical	Now --
CVE-2023-29402	Unexpected Code Genera...	Critical	Now --
CVE-2022-1664	Directory Traversal Vulner...	Critical	Now --
CVE-2023-29405	Malicious Code Execution ...	Critical	Now --
CVE-2022-37434	Heap-based Buffer Over-r...	Critical	Now --
CVE-2023-45853	Integer and Heap-Based B...	Critical	Now --
CVE-2024-24790	Malfunction in 'tr' Method...	Critical	Now --
CVE-2022-37434	Heap-based Buffer Over-r...	Critical	Now --
CVE-2022-23806	Go Crypto/Elliptic Library ...	Critical	Now --
CVE-2023-45853	Integer and Heap-Based B...	Critical	Now --
CVE-2024-38428	Insecure Data Handling in ...	Critical	Now --
CVE-2022-23219	Buffer Overflow Vulnerabi...	Critical	Now --




































The go command may execute arbitrary code at build time when using cgo. This may ...
24 Critical Vulnerability Apr 9, 2025 4:07:27 PM
Actions Automate Event Search

Evidence
CVE-2023-29405 NVD Base Score 9.8 EPSS Score 3% EPSS Percentile 86%
The go command may execute arbitrary code at build time when using cgo. This may occur when running "go get" on a malicious module, or when running any other command which builds untrusted code. This is can be triggered by linker flags, specified via a "Rgo LDFLAGS" directive. Flags containing embedded spaces are mishandled, allowing disallowed flags to be smuggled through the LDFLAGS sanitization by including them in the argument of another flag. This only affects usage of the...

Affected Asset
Cloud Account Demo
Cloud Account ID 867902650518
Asset Name 867902650518.dkr.ecr.us-east-1.amazonaws.com/hugob...
Asset Type Container Image
Cloud Provider AWS
Cloud Resource ID 867902650518.dkr.ecr.us-east-1.amazonaws.com/log4...
Software stdlib
Software Version go1.16.7
Software Fix Version 1.19.10, 1.20.5

Cloud Native Security

Security ecosystem integrations to enable seamless onboarding and security value in minutes

Cloud Providers	Container Registry	Container Orchestrators	Version Control	CI/CD & Git Hooks	Alerting
 AWS Cloud	 ECR (AWS)	 ECS	 Github Cloud	 Pre-commit Hook	 Email
 Google Cloud Platform	 GCR (GCP)	 EKS	 Github Enterprise	 Github Action	 Jira
 Azure	 Azure Registry	 GKE	 Gitlab Cloud	 Gitlab Pipeline	 Slack
 DigitalOcean	 SonaType Nexus	 AKS	 Gitlab Enterprise	 Bitbucket Pipeline	 OpsGenie
 Oracle Cloud	 Docker Hub		 Bitbucket Cloud	 CNS CLI	 PagerDuty
 Alibaba Cloud	 JFrog Artifactory		 Azure Pipeline		 Webhook
	 Harbor				 AWS SQS

The Q2 logo is a stylized white 'Q' with a '2' inside it, positioned in the upper left quadrant of the image. The background is a wide-angle photograph of a large sports stadium with green seats and a large roof structure. The text 'Q2' is also visible on the stadium's facade in the background.

Q2

Q2 Boosts Efficiency and Reduces
Attack Volume by 97% with
SentinelOne and AWS

Industry Recognition

Gartner

**100% detection.
Zero delays.
5 years running.**

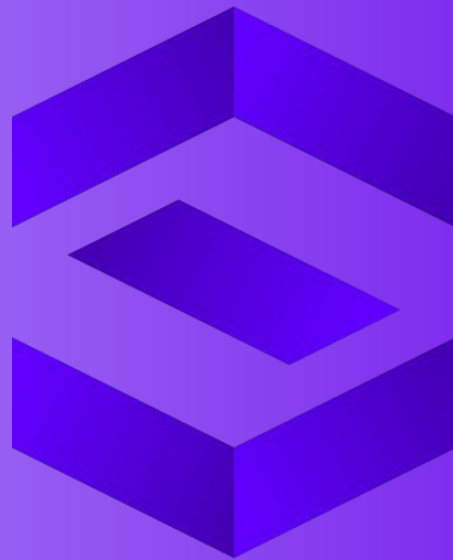
 **PeerSpot**

**98% willing to
recommend.
CNAPP customers
rank SentinelOne
highly in satisfaction,
innovation, and
performance.**

Gartner
Peer Insights™

**4.7 out of 5 stars as of
12 August 2025,
based on 359 ratings,
Cloud-Native
Application
Protection Platforms
(CNAPP)**

**Secure the cloud.
Avoid the storm.**



Demo oldal

<https://engage.sentinelone.com/viewer/4f8796b0f7f2dc6be9d13da422d67cf7>