SentinelOne™

The Singularity platform

George Saftoiu, Technical Team Lead, Clico Romania

Pervasive Challenges

SentinelOne Design Goals

Legacy AV products no longer work and provide zero visibility

Outdated Solutions

More agents. More tools. Not the answer.

Complexity

Manual tools waste valuable time and delay recovery

Productivity Drains

Remote work disrupts traditional security architectures

Remote Work

Cloud workload transition introduces new risks

Cloud Coverage

Must have‘s…

Automation

Machine speed instead of human speed

Autonomy

Detection without prior knowledge /cloud connection

Correlation

Automated correlation to combat alert fatigue

Visibility

Visibility across whole life cycle for every incident

One Platform / One Agent

No context switches in response between tools

An Evolution Towards Improved Outcomes

Objectives
Mechanisms
Outcomes

NGAV

Solving the AV Problem

Prevent

Autonomous AI Prevention

Reduce Device Impact

EDR

Solving the Breach

Detect & Respond

Behavioral AI + Full Visibility + 1 Click remediation

See More, Recover Faster

XDR

Solving Cyber End-to-End

Augment & Resolve

EDR + Cross Domain Integrations

Business Resilience

Device Focused

Incident Focused

Outcome Focused

Singularity™ Platform

Platform Capabilities

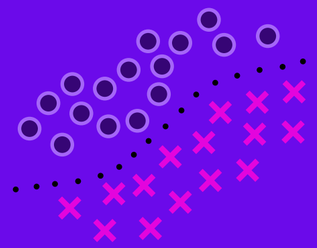
- **Prevention & Control**
- **Detection & Response**
- **Remediation & Recovery**
- **Network Visibility & Attack Surface Control**
- **XDR Automation**

Services Capabilities

- **Intelligence Driven Threat Hunting**
- **Managed Detection & Response**
- **Digital Forensics & Incident Response**

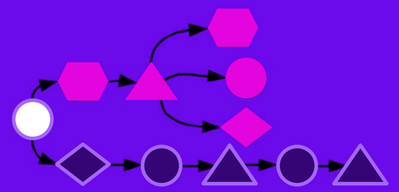
How the agent operates

Real Time File Analysis



AI-ML Static File Models

ActiveEDR™ Code Analysis



AI Dynamic Behavioral Models

Automated Remediation

- Kill & Quarantine
- One-click Cleanup
- One-click Rollback
- Disconnect from Network
- Local firewall control
- Anti-tamper

Deep Visibility Response

- Threat hunting / Watchlists
- Fast queries. Highly scalable.
- Single pivot storyline built with Storyline™
- Mark entire story as threat
- MITRE ATT&CK™ TTP hunt

REAL TIME PREVENTION + REMEDIATION & RECOVERY

DETECTION & RESPONSE

Timeframe = Seconds
Autonomous Agent Operation / Not Cloud Reliant

Timeframe = 14 - 365 Days
Incl. Data Context/Storyline

Use the cloud - Don‘t rely on it!

Named a Leader.

2022 Gartner Magic Quadrant for Endpoint Protection Platforms

SentinelOne Characteristics

- Easy deployment
- Effective protection
- Options to suit all organizations
- Cloud workload ready
- Strong MITRE ATT&CK results
- Timely, quality customer support

Gartner Critical Capabilities:

TYPE A USE CASE

Lean Forward Organizations

Highest Score

TYPE B USE CASE

Blended Approach Organizations

Highest Score

TYPE C USE CASE

Prevention Focused Organizations

Highest Score

Highest Score in All Use Cases

SentinelOne Receives Top Scores for Type A, B, and C Uses Cases in Gartner's 2022 Critical Capabilities for Endpoint Protection Platforms. SentinelOne meets you where you are with options to suit each type of organization.

Read the full report at https://s1.ai/gartnermq

Why SentinelOne?

PERFORMANCE

- Lightweight Agent
- Unique machine learning data models – no signatures
- Showing the full story while creating less alerts

SIMPLICITY

- Full on-device security, no matter if on- or offline
- Full multi tenancy
- Easy to deploy and manage

VISIBILITY

- Correlate any process on any system in real time
- Response mechanisms such as mitigate, remediate, rollback
- High performance Data Platform to generate insights from multiple data sources

SentinelOne

Thank you

SentinelOne®

sentinelone.com