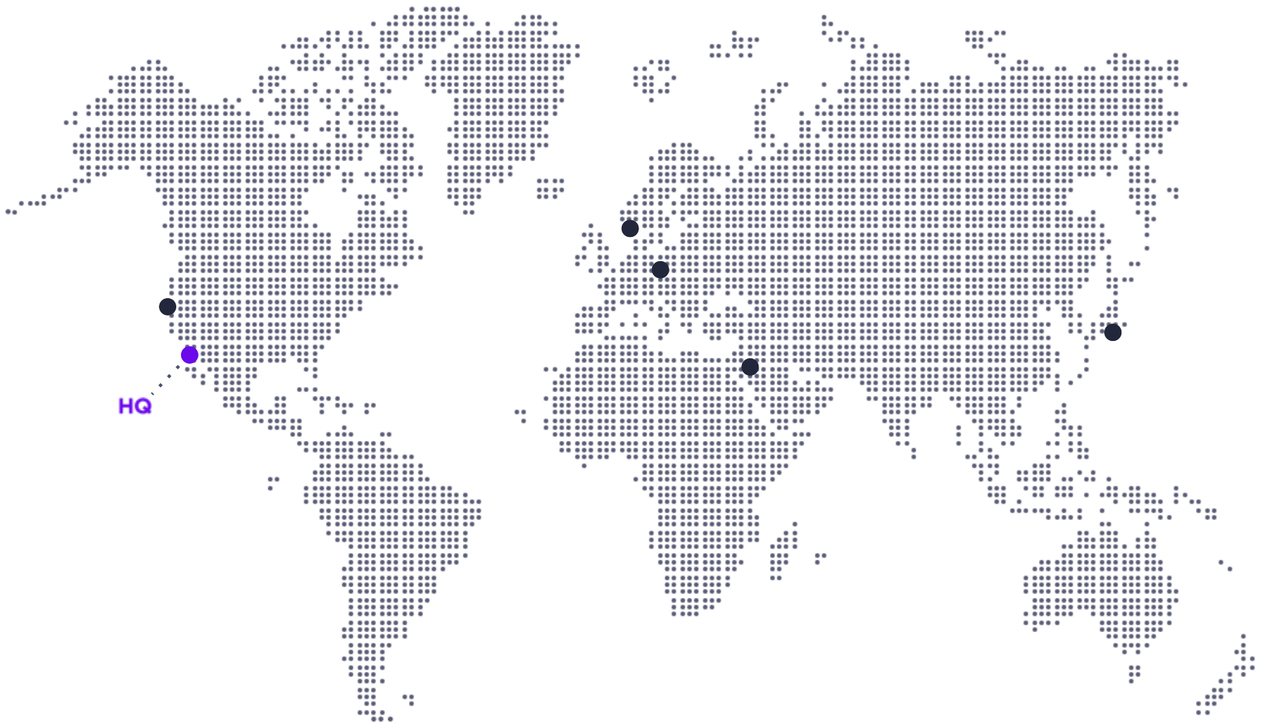
SentinelOne®

Singularity™ Platform

Overview, Design Objectives, Benefits

Global Scale. Global Readiness



>1,000
Employees

5,500+
Customers

$697M+
Funding

$3B+
Valuation

24/7

VIGILANCE
MDR Team
DF/IR Team

SUPPORT
Follow-the-Sun

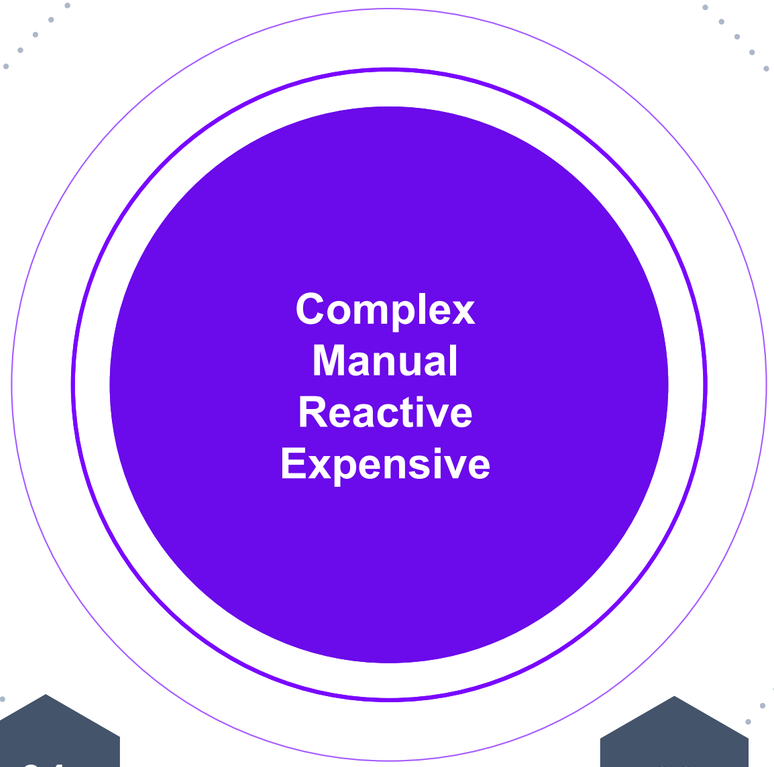
GLOBAL LOCATIONS
Mountain View, CA Tel Aviv, Amsterdam, Tokyo, Oregon

GLOBAL DATA CENTERS
AWS US, Frankfurt, Tokyo, GovCloud

SEQUOIA
Accel
SAMSUNG
TIGERGLOBAL
INSIGHT VENTURE PARTNERS
Redpoint

March 2021 statistics

The Security Condition



01

Too Many Tools

Functional overlap creates operational difficulties and expense

02

Too Much Noise

Raw, uncorrelated data slows down the ability to respond fast enough

03

Too Few Experts

Scarce high-end skills. Limited staffing.

04

Too Many Blind Spots

Poor coverage for modern threats

05

Too Many Bottlenecks

Coordination of people, processes, and technology creates scaling problems

Pervasive Challenges

Legacy AV products no longer work

Outdated Solutions

More agents. More tools. Not the answer.

Complexity

Manual tools waste valuable time

Productivity Drains

Work from home disrupts security architectures

Remote Work

Enterprise architecture cloud creep

Cloud Coverage

Singularity™ Platform

Platform Capabilities

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

Services Capabilities

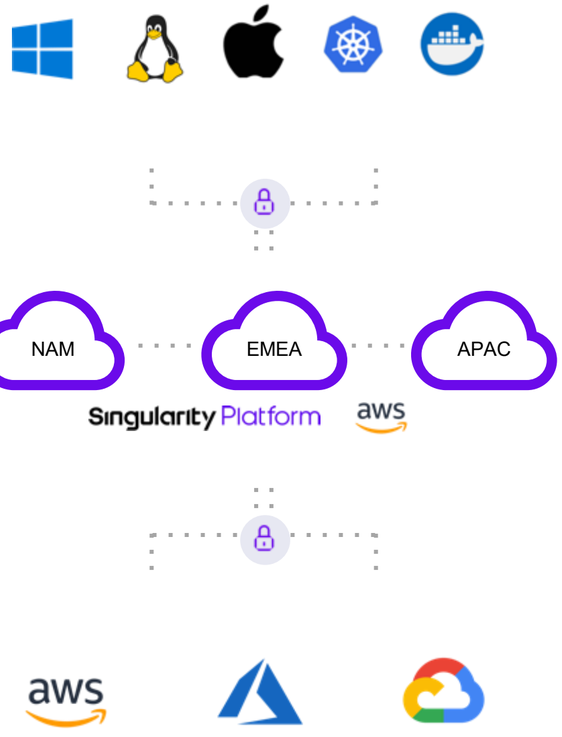
- Intelligence Driven Threat Hunting
- Managed Detection & Response
- Digital Forensics & Incident Response

Singularity™ Platform

Global platform | Prevention & control | Detection | Response | Hunting | XDR

Global Architecture

Standard Components to Support Organizations of Any Size



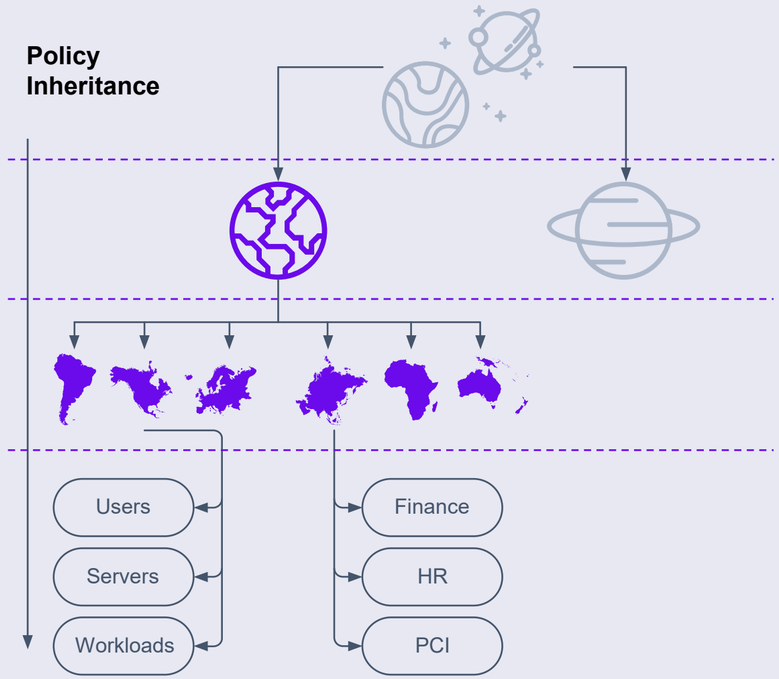
Autonomous Single agent
Distributed intelligence
Automatic EDR Context
Wide OS coverage + legacy
Physical or virtual

Regionalized SaaS in HA
SSO / MFA / RBAC
TLS 1.2+ end-to-end encryption
Marketplace Integrations
Agentless AD integration

VMs & Kubernetes cloud-native
AWS EC2 & EKS
Google Cloud Compute Engine & GKE
Azure VM & AKS
Docker & OpenShift

Highly Flexible Management

Multi-tenant / Multi-site Hierarchy



Global Scope

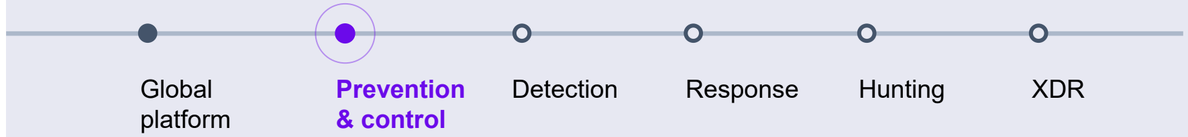
Account Scope

Customer-defined Site Scopes

Customer-defined Group Scopes

Dynamic grouping powered by agentless AD integration

Robust Prevention & Control



Use-cases

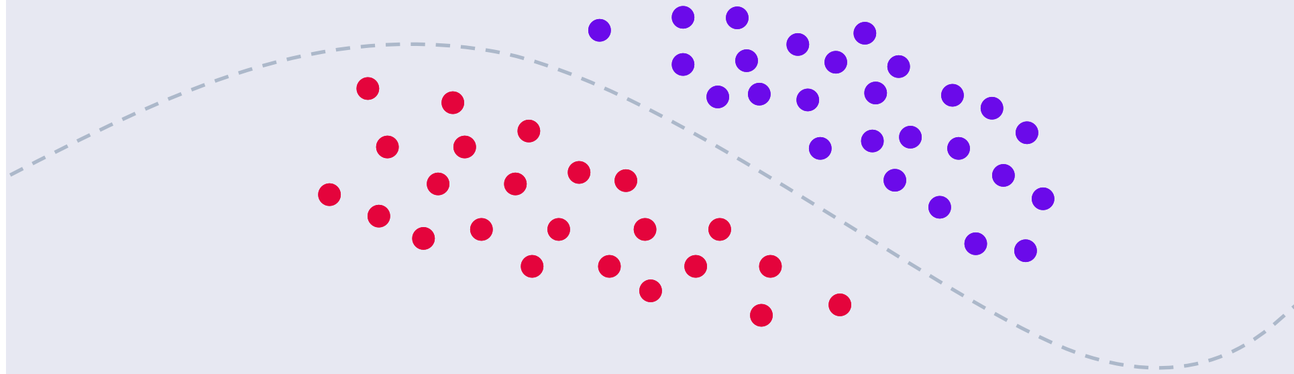
- AV/NGAV replacement
- Ransomware protection
- Endpoint hardware control & suite features

Benefits

- Modern protection
- Agent consolidation
- Broad platform support
- Fast time to value

Prevention And Control Capabilities

- Autonomous operation
- AI-based malware & ransomware protection. No signatures.
- Control USB & Bluetooth devices
- Control bi-directional network traffic + location awareness
- Discover rogue endpoints + remote agent push*
- Inventory all application
- AppControl preserves workload image immutability



Firewall

USB

Bluetooth

Rogues

App Inventory

Remote shell

Apps Control

Singularity™ Platform

Storyline™

Connects the Dots Automatically

- Patented, real-time, machine-built context across all major OSes & cloud workloads
- Distributed intelligence drives high-velocity, instantaneous protection
- Long time horizon EDR data retention for proactive custom queries, MITRE technique hunting, IR, or any EDR activity
- 1-Click recovery & response reverses unauthorized changes across the fleet

Enterprise-grade EDR

Threat Detection with Storyline™

Use-cases

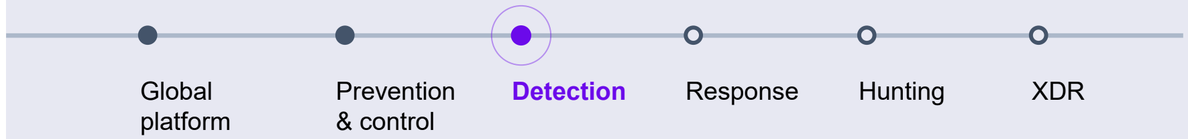
- Add, improve, consolidate EDR
- Reduce incident dwell time
- Uplevel staff skills with automation

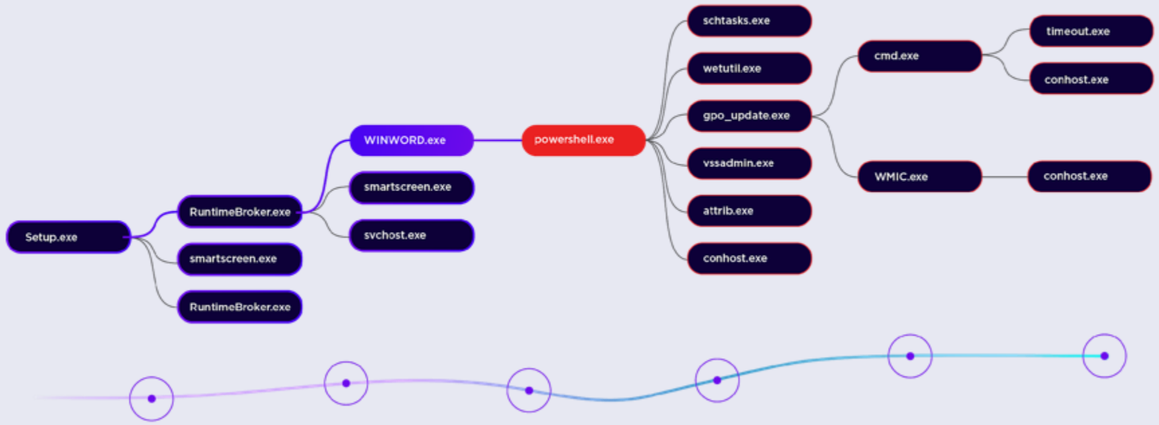
Benefits

- Machine-built stories amplify signals while reducing noise
- Machine-built stories reduce tedious tasks and errors
- EDR automation accelerates triage, response, and recovery
- Accelerate investigations with MITRE integration

Storyline: real-time detection / long term context

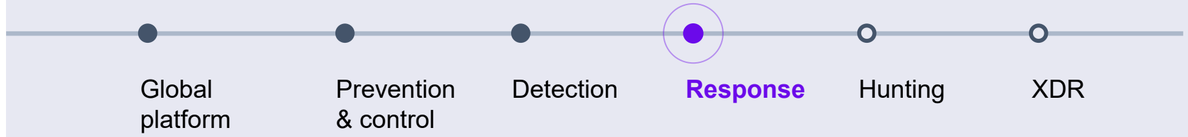
- Automatically correlates atomic events into rich story context.
- Up to 365 days context retention for all EDR activities.
- Behavioral AI pinpoints attack stories in real time: fileless attacks, lateral movement, actively executing rootkits, ++
- Mark as threat





Storyline™ is the reason why we correlate more telemetry than any other vendor

Enterprise-grade EDR



Response Actions

Use-cases

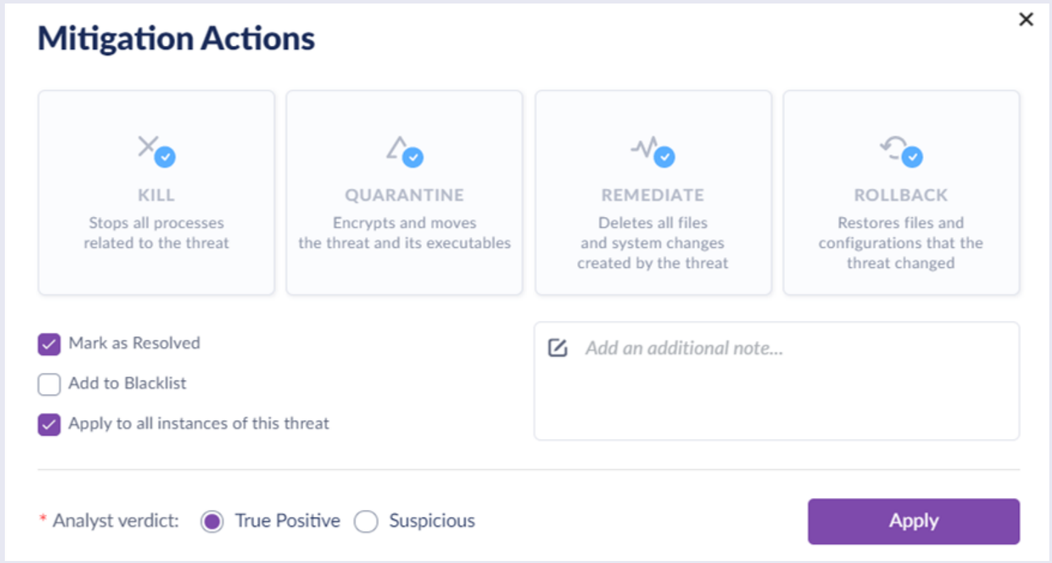
- Rapid threat containment
- Accelerated resolution
- Robust IT and SOC toolkits

Benefits

- Reduced Mean Time to Respond (MTTR)
- Automated remediation vs manual
- Best-in-industry response parity across OSes

Response capabilities

- Kill process or container
- Quarantine malicious file
- 1-Click Remediate & 1-Click Rollback
- STAR™ proactive, custom hunting and response rules
- Full Remote Shell on all platforms
- Device isolation
- Firewall control / Device control



Responses can be automated by policy, manually triggered, or orchestrated via API

Roadmap: Remote Script Orchestration is coming in Q2-2021

Enterprise-grade EDR

Proactive Threat Hunting at Scale

Use-cases

- SOC analyst investigative workflows
- Proactive threat defense
- Retroactive threat hunting

Benefits

- Uplevel SOC: Easily pivot and query
- Proactively detect and remediate low and slow attacks
- Lighten analyst load with automated hunting

Response capabilities

- EDR built for massive scale, fast queries, and 14 - 365 days historical data retention.
- Intel-driven hunting packs for retrospective hunting
- Single pivot into RCA
- Threat activity visualization
- MITRE ATT&CK™ Technique & Tactic searching

Global platform | Prevention & control | Detection | Response | **Hunting** | XDR

365
Day available data retention

S1 Hunter
Chrome Extension

Ecosystem Integrations
Threat Intel, Sandbox, Orchestration, CASB, ++

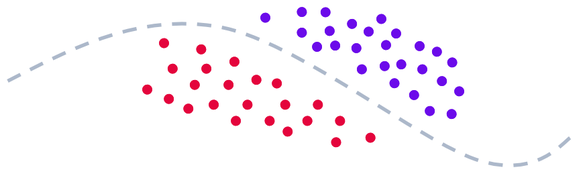
STAR Pro

Cloud Funnel

Binary Vault

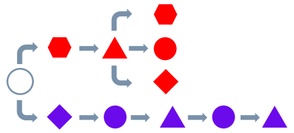
The SentinelOne Solution

Real-Time File Analysis



ML for PEs & Docs

Behavioral Analysis



Dynamic Behavioral Models

Automated Remediation

- Kill & Quarantine
- App Control
- Disconnect / Isolate
- Attack Story Cleanup
- Full Rollback
- Works online & offline

Deep Visibility & Response

- Threat Hunting
- STAR Watchlists
- Fast queries. Highly scalable.
- Full attack storyline
- Mark entire story as threat
- MITRE ATT&CK™ TTP hunt
- Full remote shell

AUTONOMOUS REAL-TIME DETECTION & PREVENTION + REMEDIATE & RECOVER

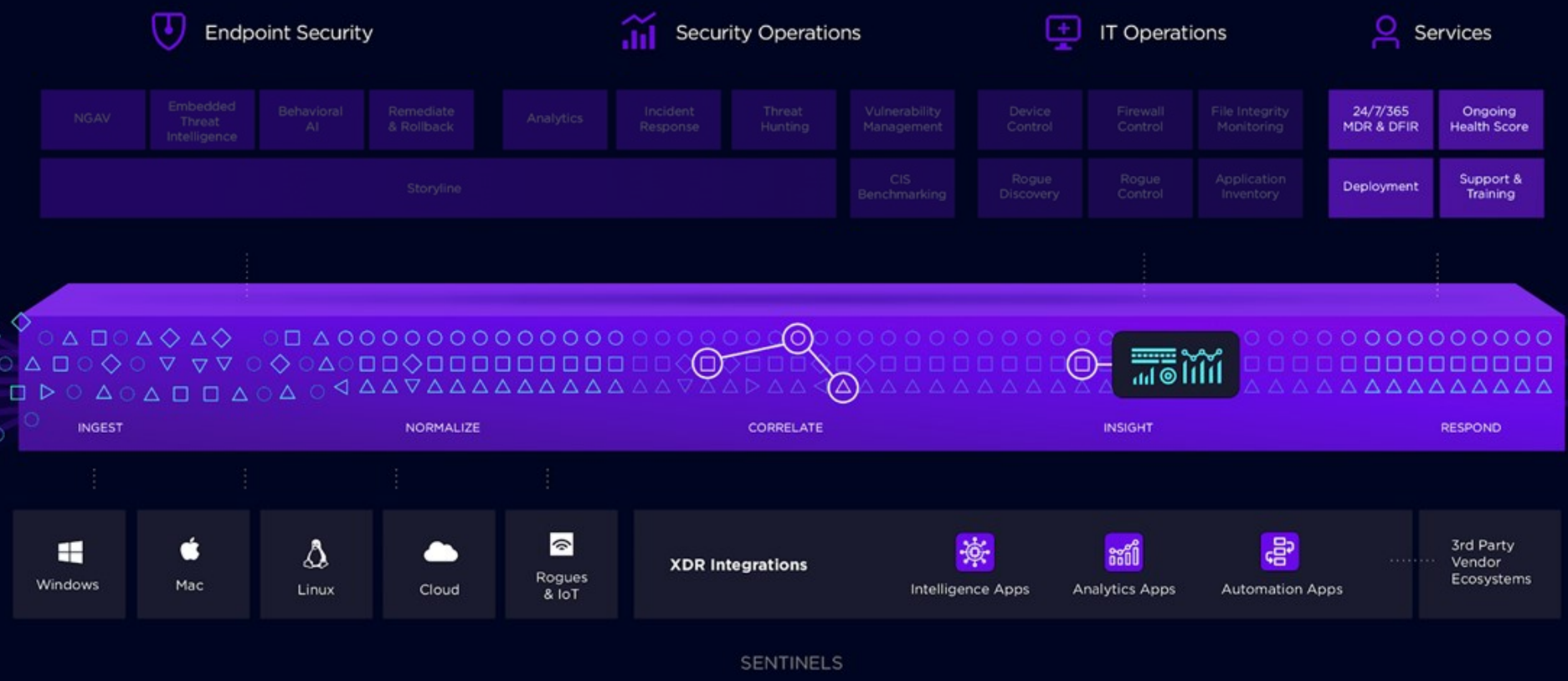
INVESTIGATE HUNT RESPOND

Timeframe = Seconds
Single Lightweight Agent
Autonomous Agent Operation + Cloud
Windows, Mac, Linux, VDI, Cloud, Kubernetes/Docker

Retention:
14 days - 1 year
Full context and correlation
Integrated response workflow

Singularity™ Platform

AI Powered XDR with SCALYR



Why SentinelOne?
Automation

Storyline™

Autonomously connecting the dots to reduce labor and error

ActiveEDR®

AI real time response. Proactive EDR and recovery

Ranger®

Network attack surface learning & control in the same agent

Singularity™ XDR

Integrate EPP+EDR with other security stack components

ONE Console

Manage all workloads in a single console across GEOs

Singularity Platform Products

Singularity Complete

Enterprise EDR
Endpoint Control
NGAV

Optional Components:

- Data Retention Upgrade: 14, 30, 90, 365
- STAR Pro
- Binary Vault
- CloudFunnel Data Streaming

Singularity Cloud

Cloud Workload Security

Singularity RANGER

Network Visibility & Control

Singularity Control

NGAV + Endpoint Control

Singularity Core

NGAV

FedRAMP® Compliant GovCloud Hosting

Software Development Kit (SDK)

Augment the Singularity™ Platform with:

Tiered Threat Services

VIGILANCE Respond PRO

Digital Forensics & Incident Response Expertise (DFIR)
Directed Investigation & Threat Hunting
Managed Detection & Response (MDR)
Intelligence-led Threat Hunting

Augment Your Team with SOC Expertise

VIGILANCE Respond

Managed Detection & Response (MDR)
Intelligence-led Threat Hunting

Accelerate Triage & Resolution

WATCHTOWER

Intelligence-led Threat Hunting
*Included as part of the Vigilance services above

Adapt to Today's Global Threat Landscape

Support & Deployment Services

Tiered Support Services

Professional Support
Enterprise Support + Technical Account Management

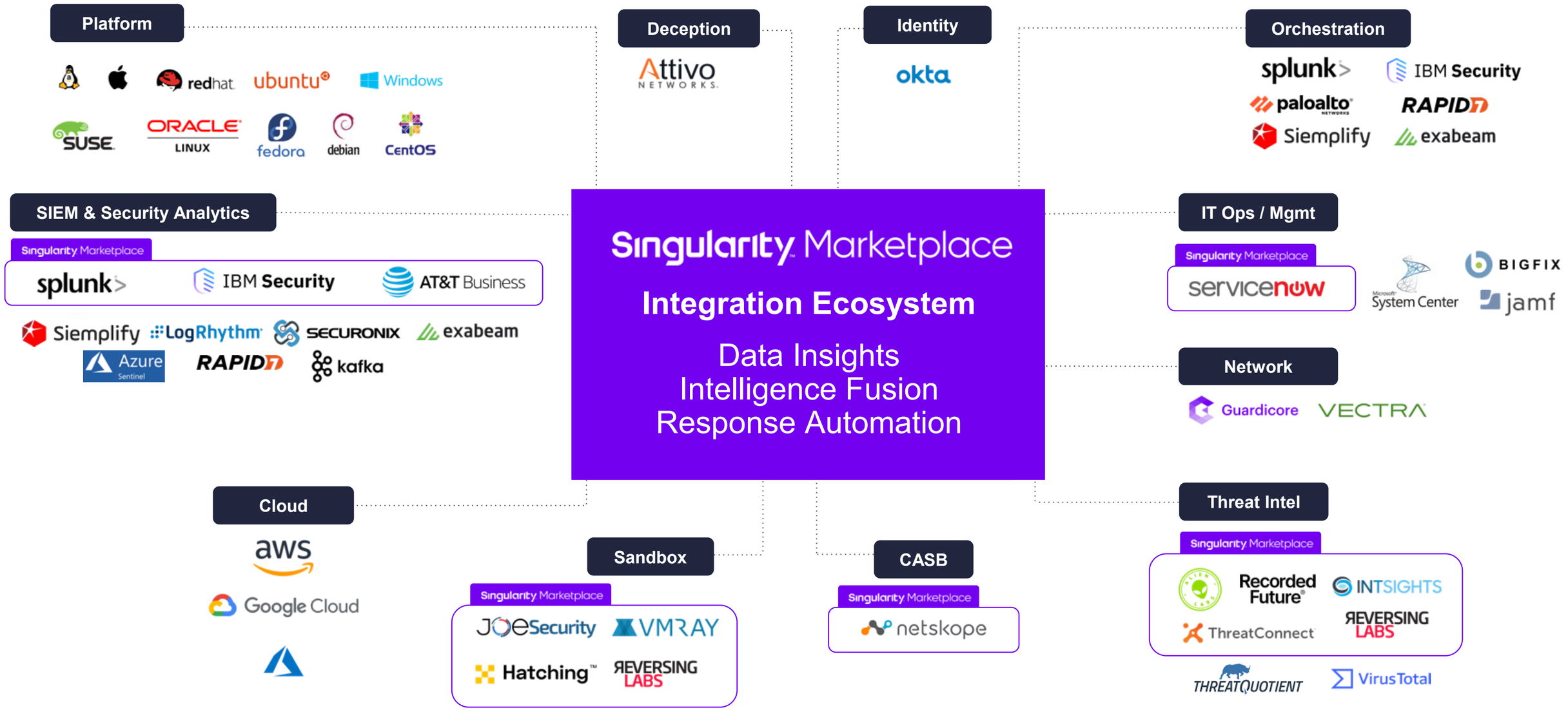
Receive White Glove Treatment & Follow-the-Sun Support

Readiness

Deployment & Quarterly Health Checks

Set Up for Success, Sustain That Success

Singularity Marketplace & Technical Integration Ecosystem



MITRE ATT&CK Results Data

Highest Analytic Coverage

Delivering 100% visibility and quality context & insights without the noise

INSTILLS CONFIDENCE

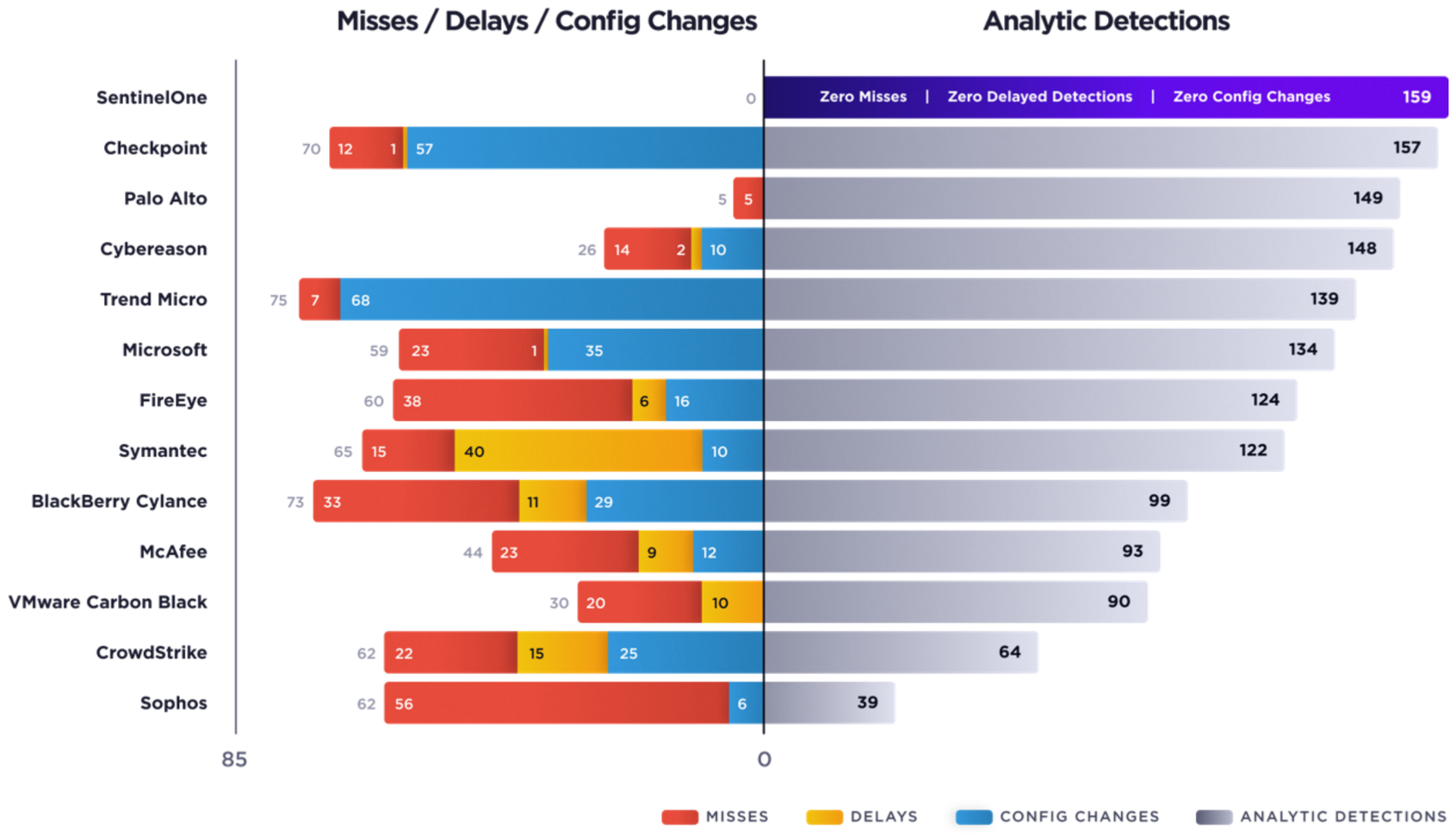
ZERO missed detections

WORKS OUT-OF-THE-BOX

ZERO configuration changes

MOVES AT MACHINE SPEED

ZERO delayed detections



[MITRE ATT&CK Results Data]

Gartner

2021 Gartner Magic Quadrant for Endpoint Protection Platforms

- Named a Leader
- Highest Scored Vendor Across All 3 Use Cases in the Critical Capabilities Report

MITRE ENGENUITY ATT&CK® Evaluations

SentinelOne Leads in ATT&CK Evaluation Performance

- Only Vendor with 100% Visibility
- Highest Analytic Detection Coverage Delivers Quality Insights, Not Noise
- ZERO: Misses, Configuration Changes, or Delays

Gartner peerinsights™

4.9 ★★★★★

EPP + EDR
Highest rated EDR vendor in Voice of the Customer report

5.0 ★★★★★

MDR
Nothing short of 5-star reviews in the past 12 months

TEVORA™
HIPAA Attestation
PCI DSS Attestation

ISO 27001 CERTIFIED by schellman

FedRAMP

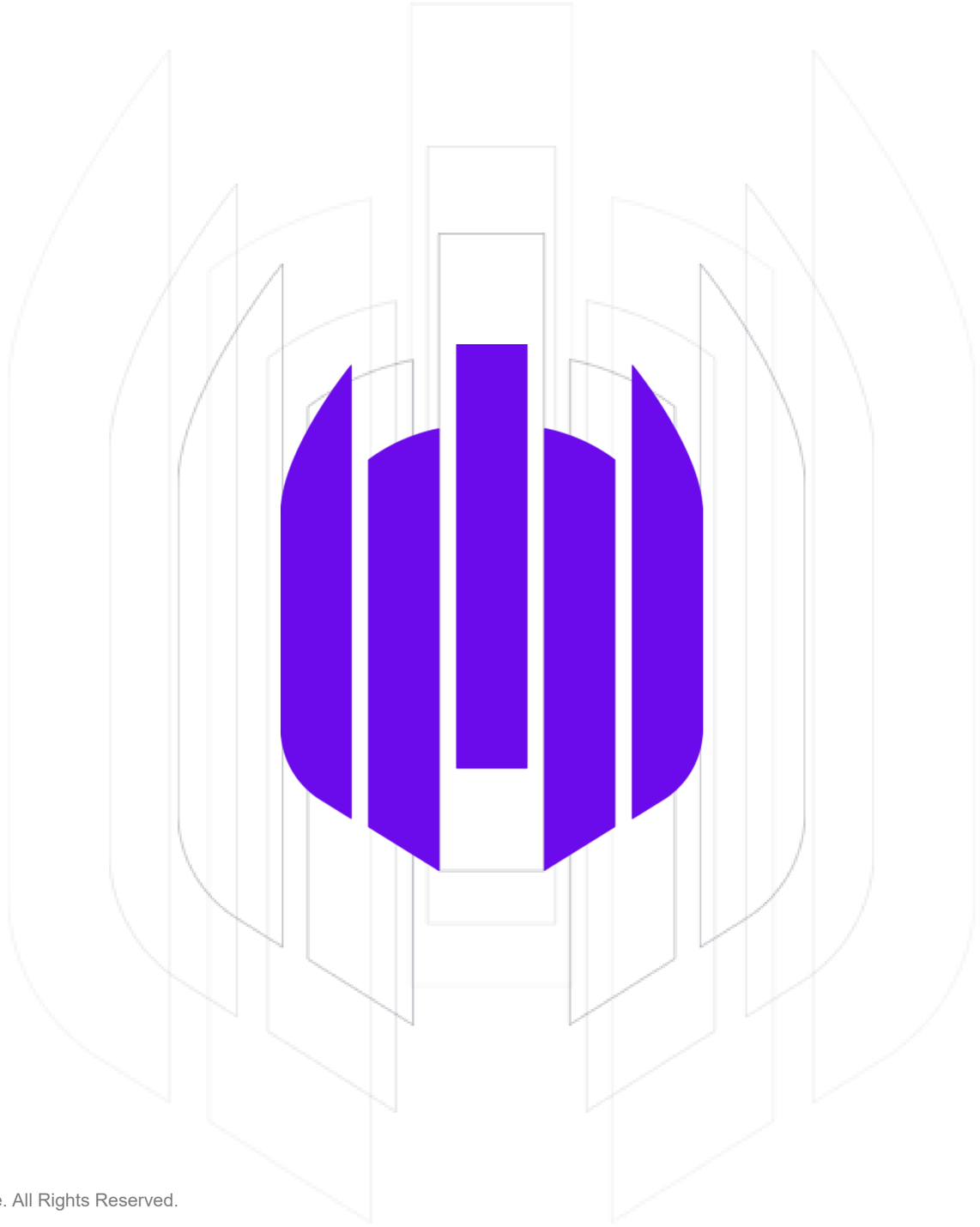
SE Labs INTELLIGENCE-LED TESTING BEST New Endpoint WINNER 2020

SE Labs AAA AUGUST 2020 BREACH RESPONSE (PROTECT)

SE Labs AAA JAN-MAR 2021 ENTERPRISE ENDPOINT PROTECTION

glassdoor 4.9 ★★★★★

Proactive.
Cybersecurity.
Now.



Thank you

SentinelOne®

sentinelone.com