SentinelOne®

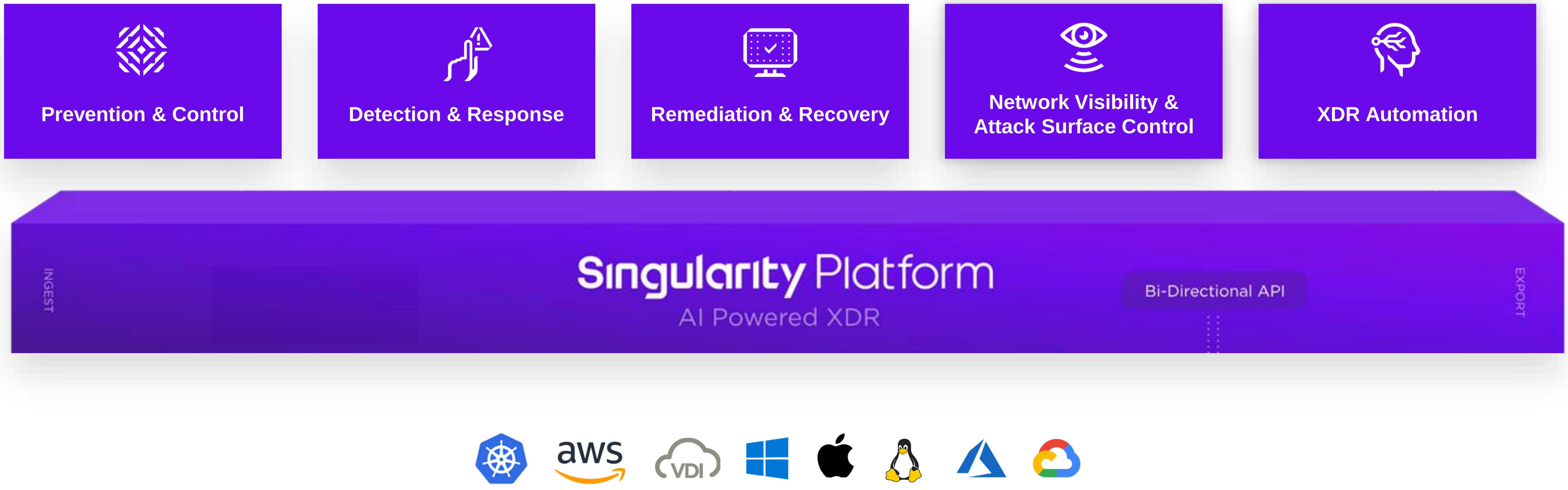
Endpoint Protection

Autonomous, AI-driven Prevention and
EDR at Machine Speed

March 2021

Singularity™ Platform

Platform Capabilities



Prevention & Control

Detection & Response

Remediation & Recovery

Network Visibility & Attack Surface Control

XDR Automation

Singularity Platform

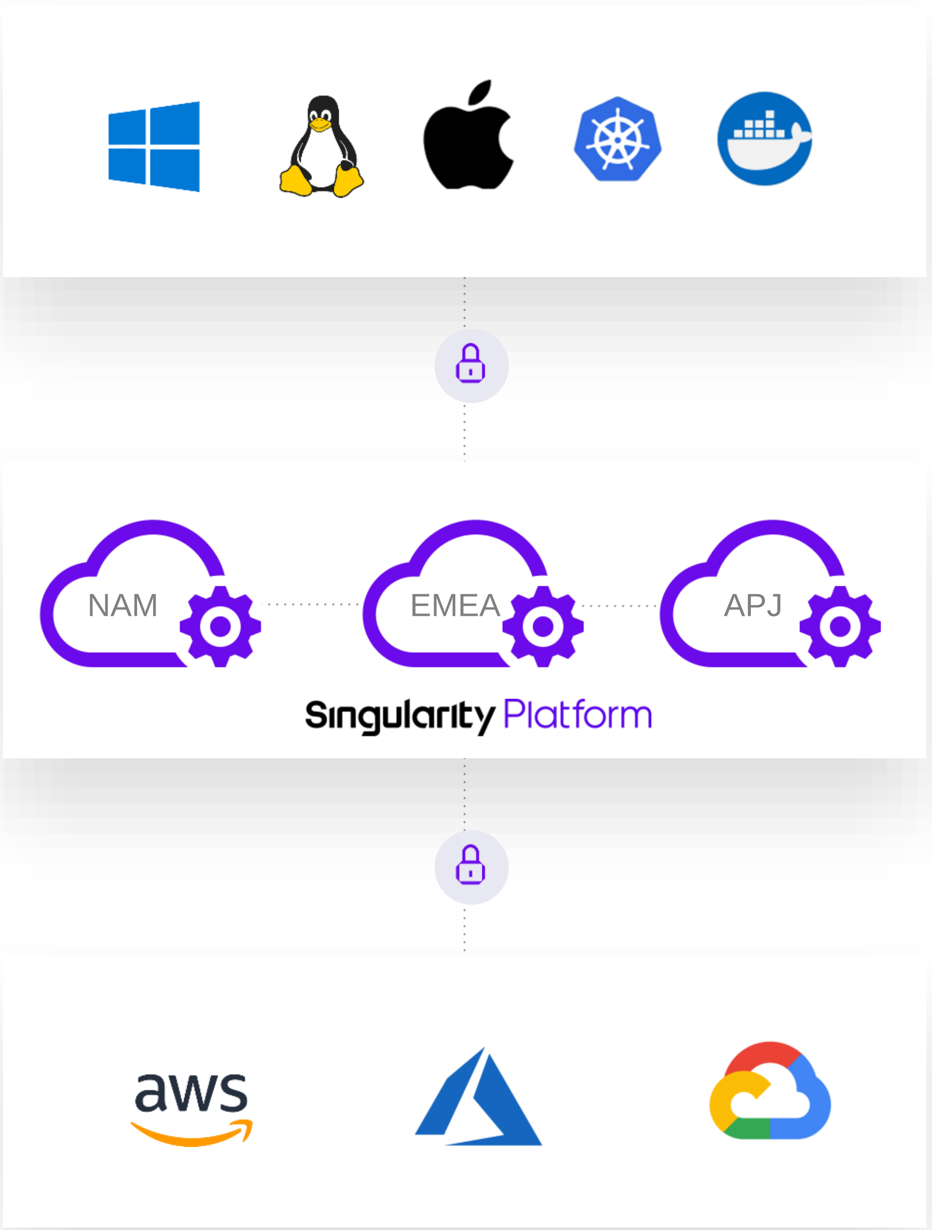
AI Powered XDR

SentinelOne®

Singularity™ Platform

Global Architecture

Standard Components to Support Organizations of Any Size



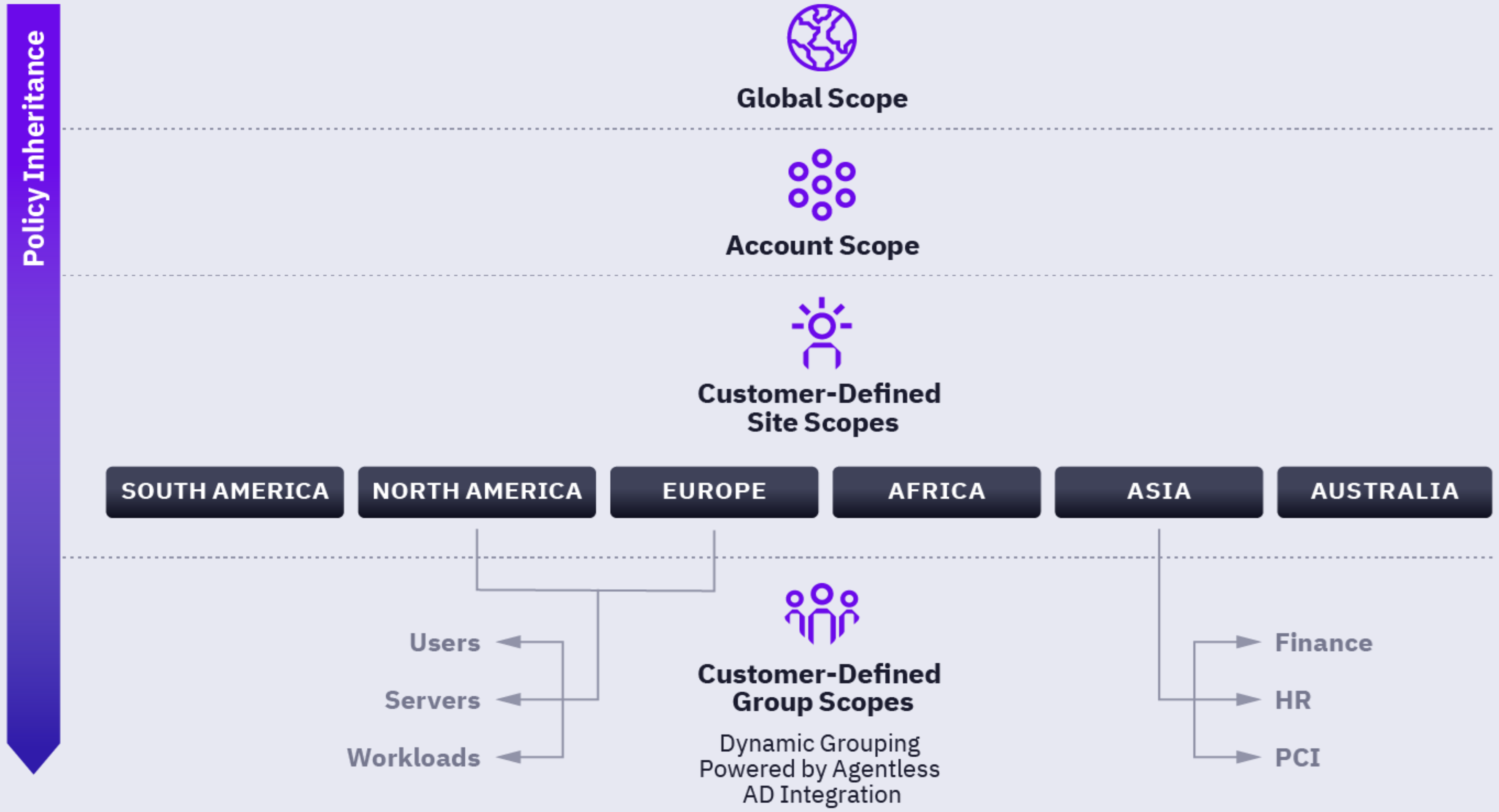
Autonomous Single agent
Distributed intelligence
Automatic EDR Context
Wide OS coverage + legacy
Physical or virtual

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
Google GKE
Azure VM & AKS
Docker & OpenShift

Flexible Management Out-of-the-Box

Management Hierarchy Freedom of Choice to Fit Your Needs



Policy Inheritance

Global Scope

Account Scope

Customer-Defined Site Scopes

SOUTH AMERICA | NORTH AMERICA | EUROPE | AFRICA | ASIA | AUSTRALIA

Users
Servers
Workloads

Customer-Defined Group Scopes

Dynamic Grouping Powered by Agentless AD Integration

Finance
HR
PCI

SentinelOne

Robust Prevention & Control

Use-cases

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

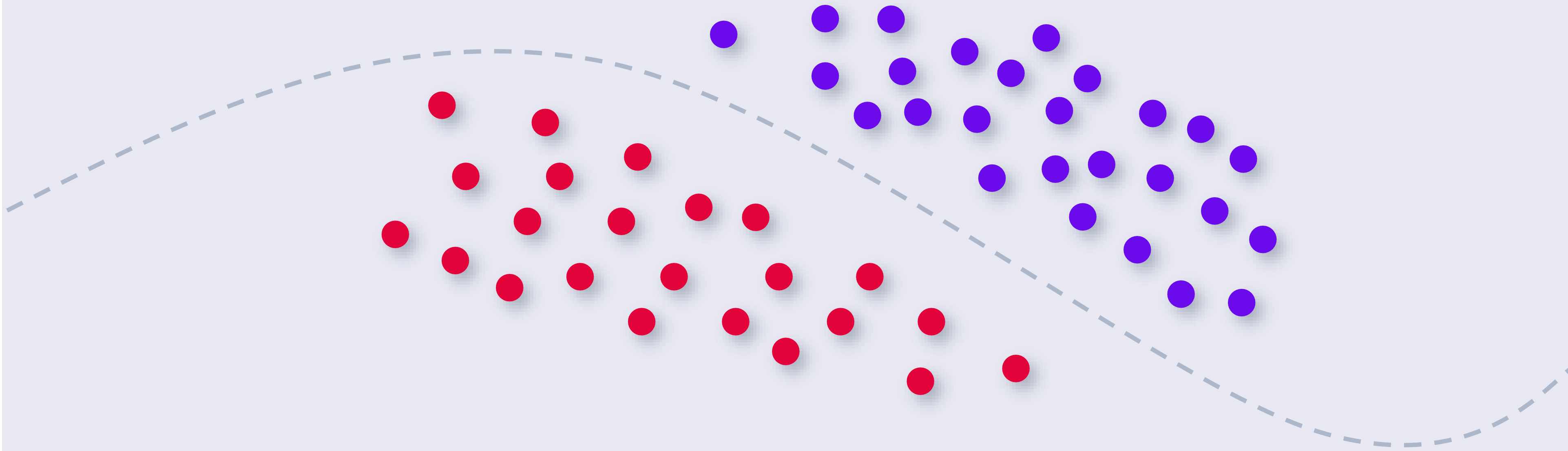
Benefits

- 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

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



Firewall · **USB** · **Bluetooth** · **Rogues**

App Inventory · **Remote shell** · **Apps Control**

SentinelOne

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

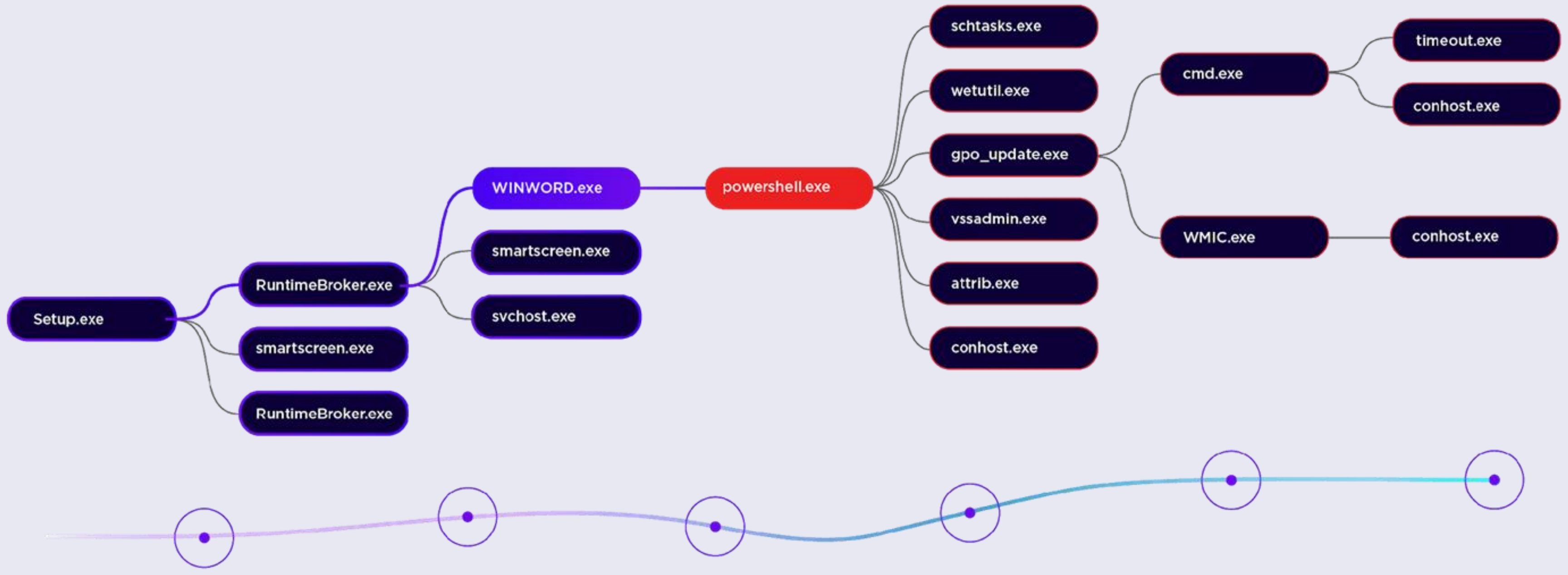
- Add, improve, consolidate EDR
- Reduce incident dwell time
- Uplevel staff skills with automation

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

MITRE ENGENUITY™ | ATT&CK® Evaluations

2 days of emulated APT testing in 174 phased steps

The Results: SentinelOne automatically correlated the entire test into 7 campaign-level alerts

SentinelOne excels across major customer KPIs and delivers business value:

100% Visibility Zero Misses

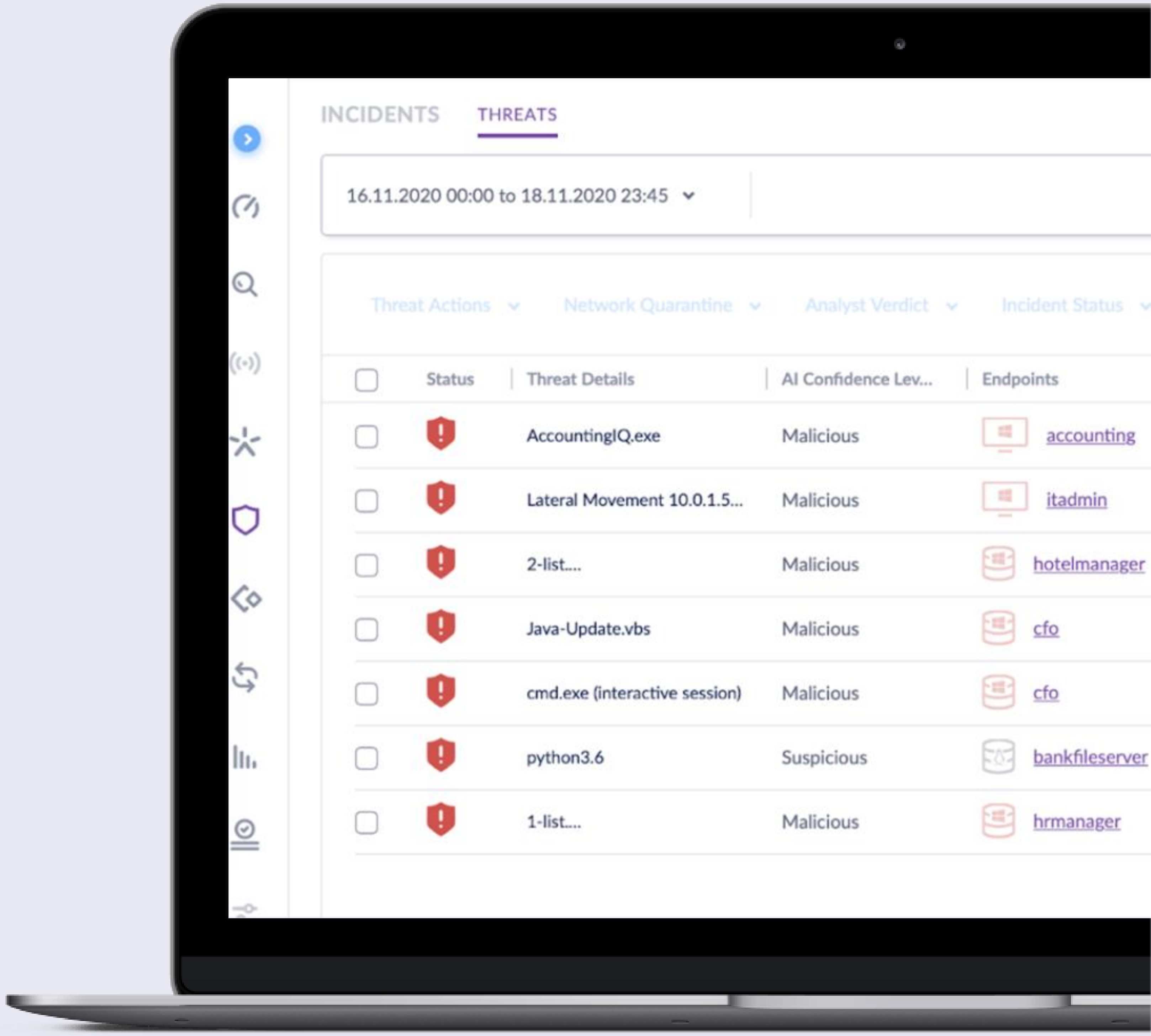
SentinelOne is the only vendor to achieve full visibility with no missed detections.

Most Analytics Detections 2 Years Running

SentinelOne leads the pack in automatic correlation & contextualization of alerts.

Zero Config Changes Zero Delays

SentinelOne detections deliver on their promise out of the box, in real time, without delay.



□	Status	Threat Details	AI Confidence Lev...	Endpoints
□	!	AccountingIQ.exe	Malicious	accounting
□	!	Lateral Movement 10.0.1.5...	Malicious	itadmin
□	!	2-list....	Malicious	hotelmanager
□	!	Java-Update.vbs	Malicious	cfo
□	!	cmd.exe (interactive session)	Malicious	cfo
□	!	python3.6	Suspicious	bankfileserver
□	!	1-list....	Malicious	hrmanager

MITRE ATT&CK Results Data

Highest Analytics Coverage

Delivering quality context & insights without the noise

GAIN CONFIDENCE

✓ **ZERO Missed Detections**

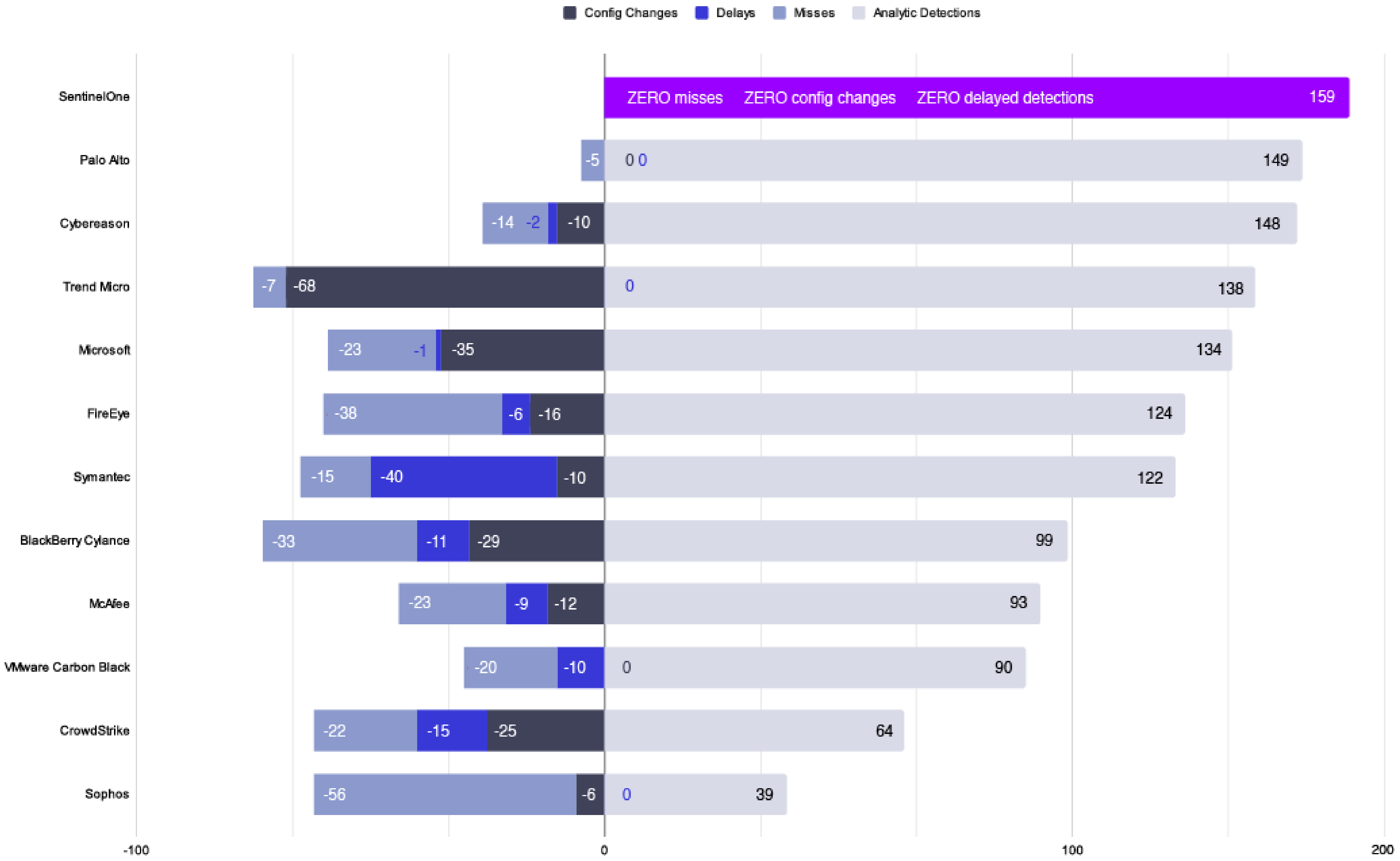
GET STARTED OUT-OF-THE-BOX

✓ **ZERO Configuration Changes**

MOVE AT MACHINE SPEED

✓ **ZERO Delayed Detections**

MITRE ATT&CK Results Data



Enterprise-grade EDR

Response Actions

Use-cases

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

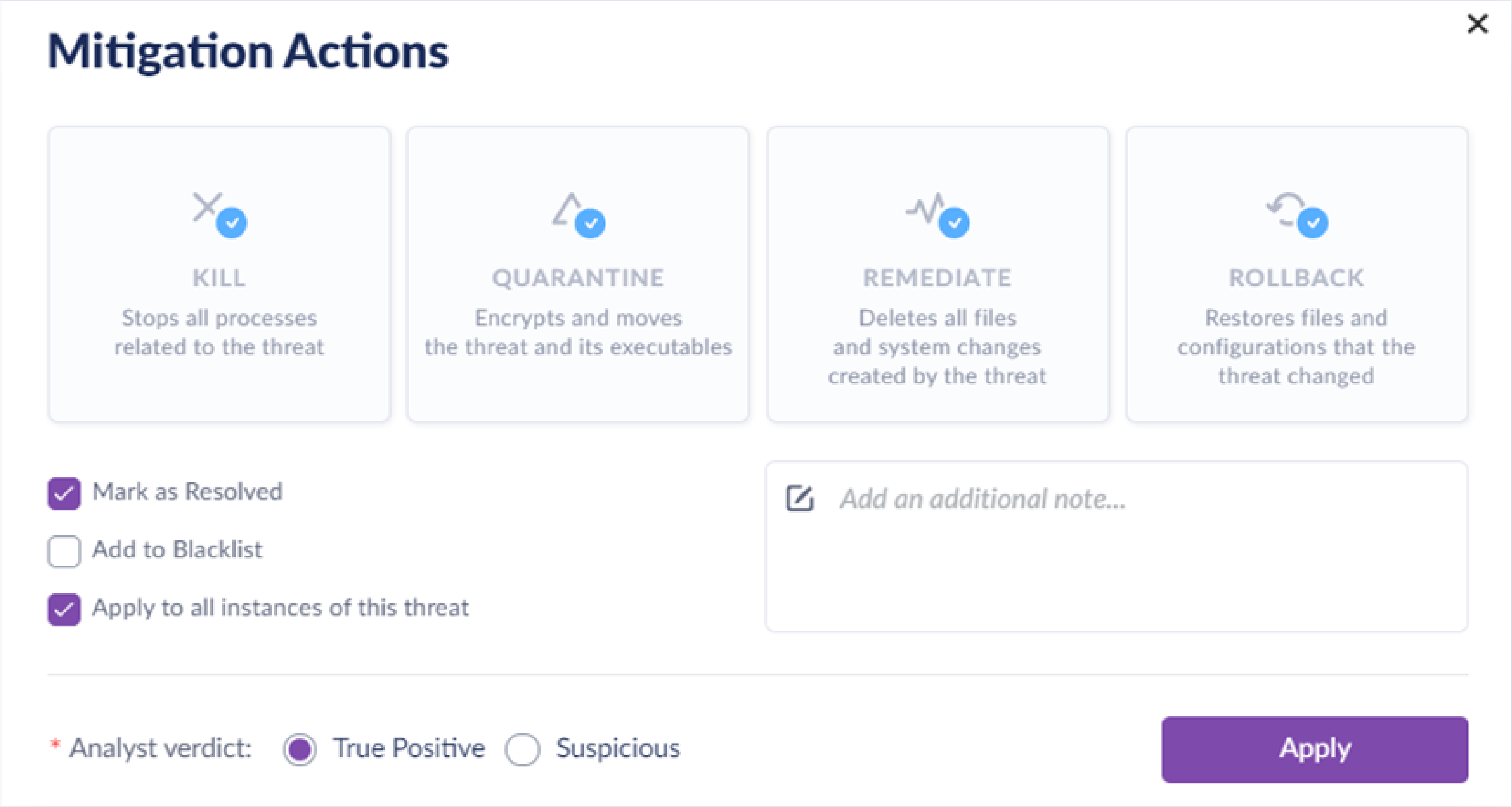
Benefits

- 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
- Remote Script Orchestration
- Full Remote Shell on all platforms
- Device isolation
- Firewall control / Device control

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



Mitigation Actions

KILL
Stops all processes related to the threat

QUARANTINE
Encrypts and moves the threat and its executables

REMEDIATE
Deletes all files and system changes created by the threat

ROLLBACK
Restores files and configurations that the threat changed

☑ Mark as Resolved
☐ Add to Blacklist
☑ Apply to all instances of this threat

Add an additional note...

* Analyst verdict: ● True Positive ○ Suspicious

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

SentinelOne

Enterprise-grade EDR

Proactive Threat Hunting at Scale

Use-cases

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

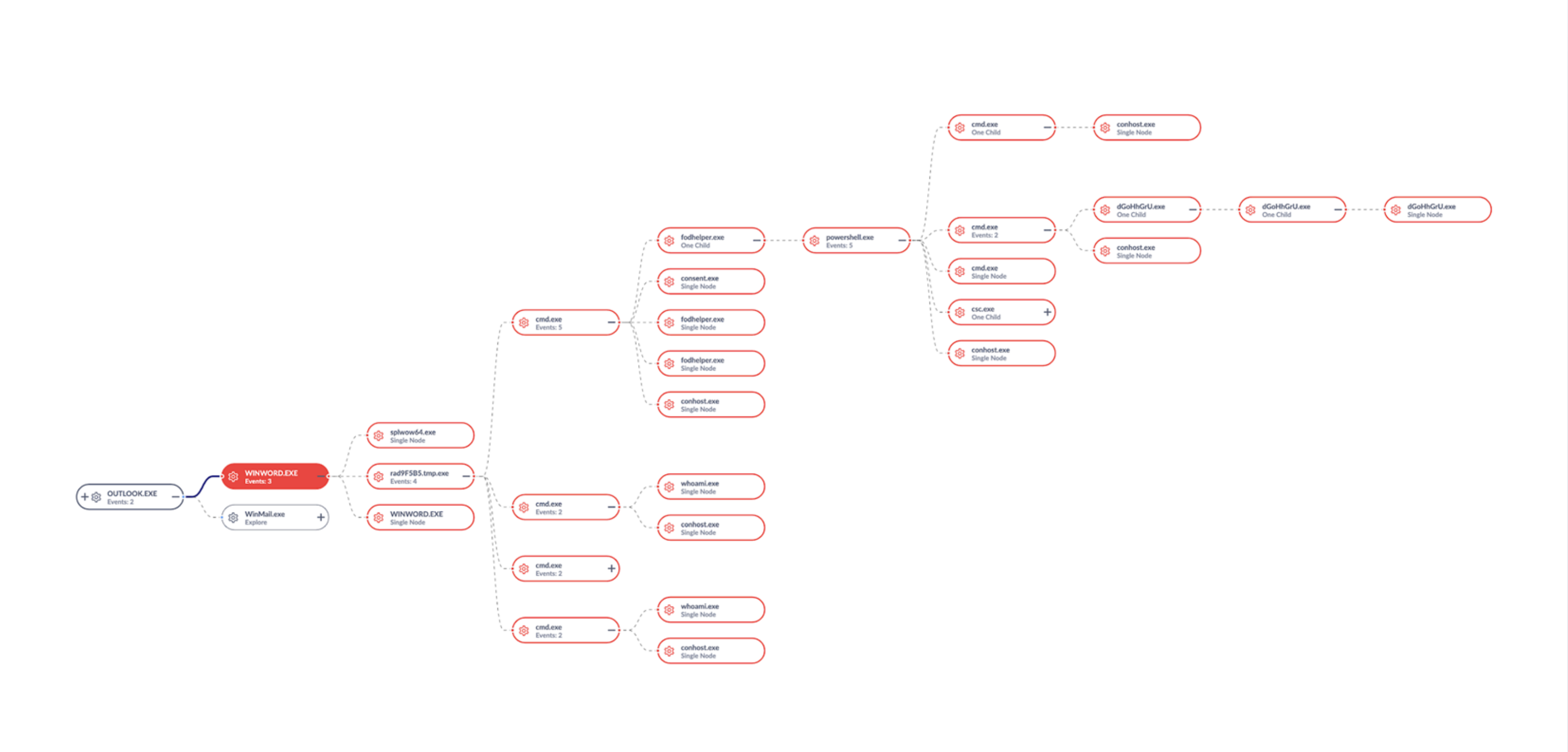
Benefits

- 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, ++

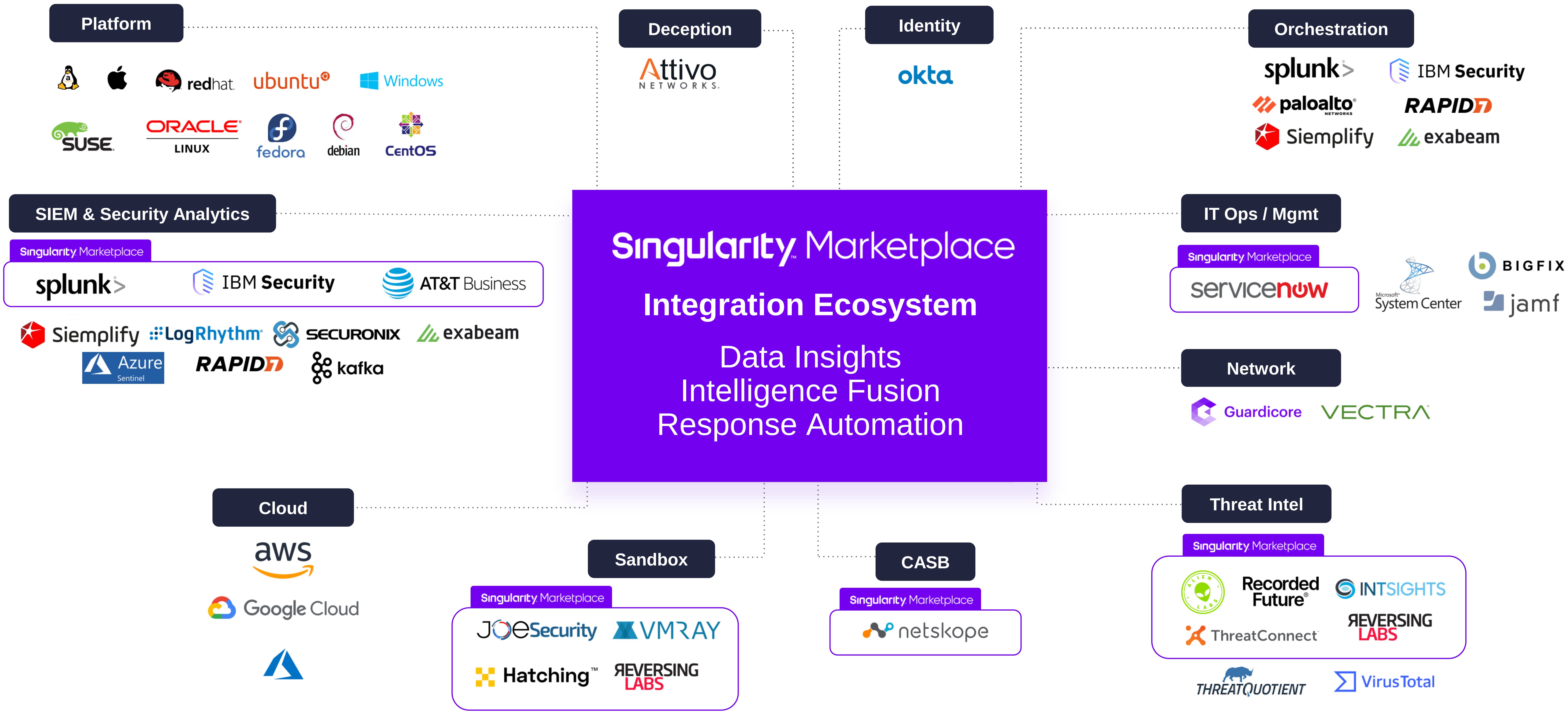
STAR Pro

Remote Script Orchestration

Binary Vault

Cloud Funnel

Singularity Marketplace & Technical Integration Ecosystem



Singularity Marketplace

Integration Ecosystem

Data Insights
Intelligence Fusion
Response Automation

Platform

redhat · ubuntu · Windows · SUSE · ORACLE LINUX · fedora · debian · CentOS

Deception

Attivo NETWORKS

Identity

okta

Orchestration

splunk> · IBM Security · paloalto NETWORKS · RAPID7 · Siemplify · exabeam

SIEM & Security Analytics

Singularity Marketplace: splunk> · IBM Security · AT&T Business

Siemplify · LogRhythm · SECURONIX · exabeam · Azure Sentinel · RAPID7 · kafka

IT Ops / Mgmt

Singularity Marketplace: servicenow

Microsoft System Center · BIGFIX · jamf

Network

Guardicore · VECTRA

Cloud

aws · Google Cloud

Sandbox

Singularity Marketplace: JOESecurity · VMRAY · Hatching · REVERSING LABS

CASB

Singularity Marketplace: netskope

Threat Intel

Singularity Marketplace: ALIEN LABS · Recorded Future · INTSIGHTS · ThreatConnect · REVERSING LABS

THREATQUOTIENT · VirusTotal

SentinelOne

Thank you

SentinelOne®

sentinelone.com