



Singularity™ Platform

Overview, Design Objectives, Benefits

Daniel Bachofen, Sales Engineer Switzerland
dbachofen@sentinelone.com

ISSS WEBINAR: WIE SIE MIT HILFE VON KI UND AUTOMATISIERUNG RANSOMWARE ANGRIFFE ABWEHREN KÖNNEN.

Today's reality (RaaS)

Darknet-Leak betrifft Kundinnen und Kunden der Emil Frey Gruppe – das musst du wissen

Die Comparis-Hacker schlagen schon wieder zu – und erneut trifft es eine Schweizer Firma

Matisa, Westschweizer Hersteller von Gleisbaumaschinen, steht im Fadenkreuz von Internet-Erpressern. Offenbar wurden Daten gestohlen und verschlüsselt. Die Firma wird wie zuvor Comparis von der Hackergruppe «Grief» erpresst.

Swisswindows AG macht per sofort dicht: 170 Mitarbeiter entlassen

Hacker-Angriff versetzte den Todesstoss!

Ransomware-Attacke 15.07.2021, 11:03 Uhr

Beim Comparis-Hack wurden offenbar Daten entwendet

Bei der kürzlichen Attacke auf Comparis.ch wurden nicht nur deren Systeme blockiert – offenbar sind auch Kundendaten entwendet worden.



INSTRUCTIONS

CHAT SUPPORT

ABOUT US

4 minutes ago

to all my files and also for my backup data?
3 minutes ago

Yes. For all files
2 minutes ago

ok thanks for the info.
15 seconds ago

I see you want 1.9 mio usd. can we negotiate on it?
1 second ago

Type your question here

[Browse files](#) for attach (maximum 3 files, less than 10MB) **SEND**

We will wait 65,95 BTC, btc amount freezed

3 minutes ago

thanks. so you provide me 24 hours more and i will call the co-founder of anycoindirect

2 minutes ago

Yes, you have 24 hours more.

2 minutes ago

thanks

19 seconds ago

Type your question here

[Browse files](#) for attach (maximum 3 files, less than 10MB)

SEND

* Current price 9070.57179753 XMR will be doubled in

1 day, 00:57:18

- If you do not pay on time, the price will be doubled
- Time ends on **Jul 10, 16:56:23**

After time ends

≈ 608,653 USD

131.9 BTC

≈ 1,217,306 USD

Bitcoin address: 3QNPKUS1DsEGDMur42LdeoeLw9YXofJGsF

* USD will be recalculated in 3 hours with an actual rate.

INSTRUCTIONS

CHAT SUPPORT

ABOUT US

Payment method **MONERO** **BITCOIN (+10%)**

Yes

2 minutes ago

Wait for 3 confirmations

2 minutes ago

can you please provide me the transaction id?

1 minute ago

612b4 [REDACTED] fd048ade

1 minute ago

Type your question here

Browse files for attach (maximum 3 files, less than 10MB)

SEND

Instructions for using General-Decryptor you can find below.

Download

INSTRUCTIONS

CHAT SUPPORT


ABOUT US

Payment method MONERO **BITCOIN (+10%)**

1. Decryptor looking for encrypted file
2. creating backup of file
3. decrypting file
4. removing the backup
5. looking for a next file and loop repeating.

You can collect list of extensions, input to the textarea above the chat and click "Download" to generate General decryptor to decrypt files with these extensions.

But this way is not necessary, because we provide you the universal decryptor. It just works slowest but you don't need collect anything, just download it and use on any system with admin rights. DOWNLOAD:

 uni_dec.exe
68.1 KB

Type your question here

[Browse files](#) for attach (maximum 3 files, less than 10MB)

SEND

Cybersecurity is Reactive

Cybersecurity's Effectiveness Path is Unsustainable

\$262B Annual
Cybersecurity Spend

162 Days Average
Dwell Time

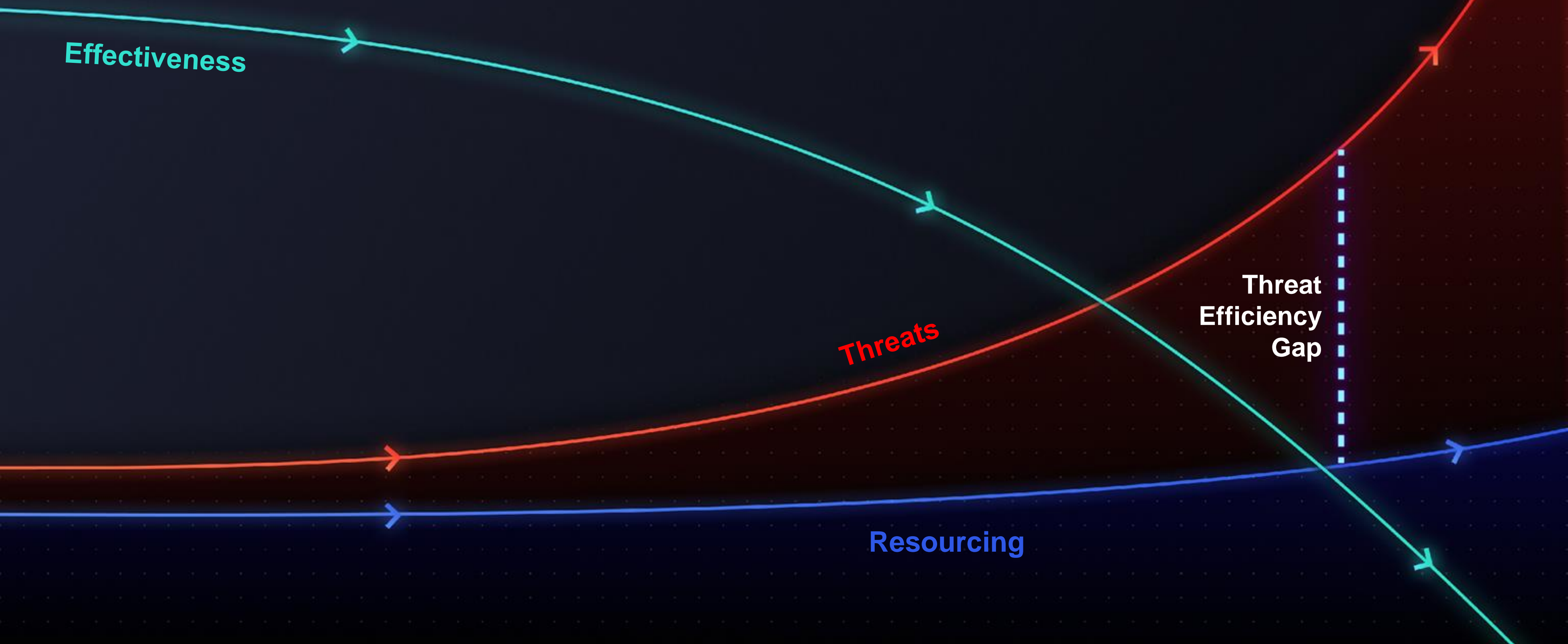
Digital Transformation
is Accelerating

Effectiveness

Threats

Threat
Efficiency
Gap

Resourcing

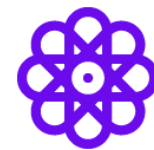


Challenges



**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

Singularity Platform
AI Powered XDR

INGEST EXPORT

Bi-Directional API

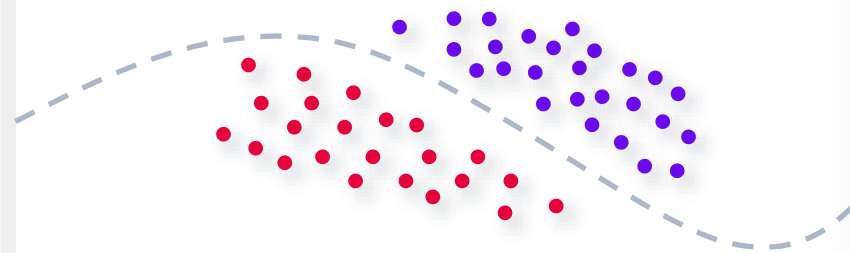
Services Capabilities

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



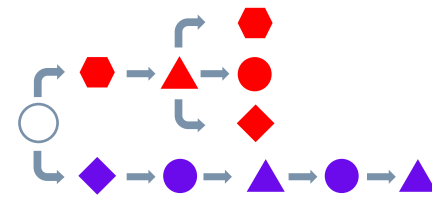
The SentinelOne Solution

Real-Time File Analysis



AI 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, **NetApp**



Singularity Mobile

Retention:

14 days - 1 year

Full context and correlation

Integrated response

workflow

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



An Evolution Towards Improved Outcomes

Objectives
Mechanisms
Outcomes

XDR

Solving Cyber End-to-End

Augment & Resolve

EDR + Cross Domain Integrations

Business Resilience

EDR

Solving the Breach

Detect & Respond

Behavioral AI + Full Visibility + 1 Click remediation

See More, Recover Faster

NGAV

Solving the AV Problem

Prevent

Autonomous AI Prevention

Reduce Device Impact

Device Focused

Incident Focused

Outcome Focused

How Singularity XDR Solves the Problem

Ingest All Data



Deliver Any Outcome



See

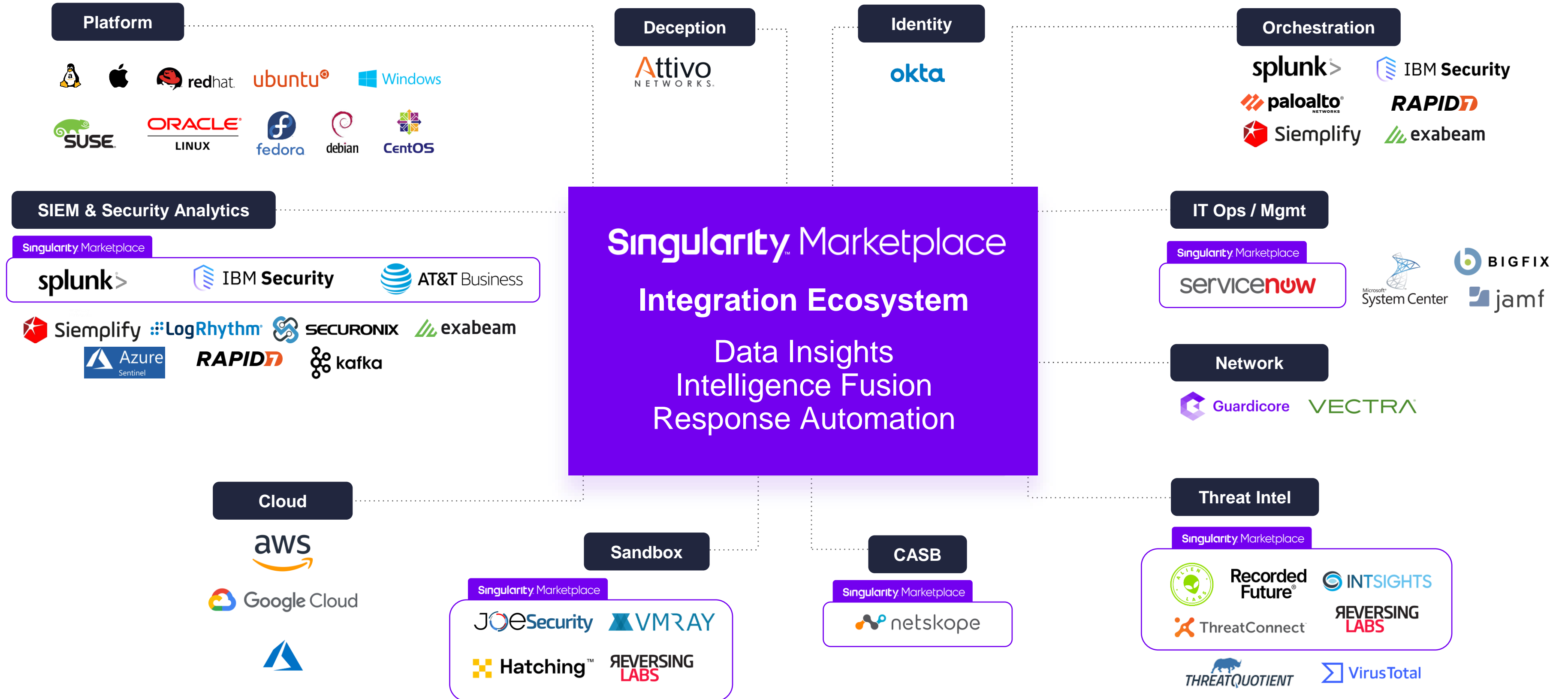


Protect



Resolve

Singularity Marketplace & Technical Integration Ecosystem



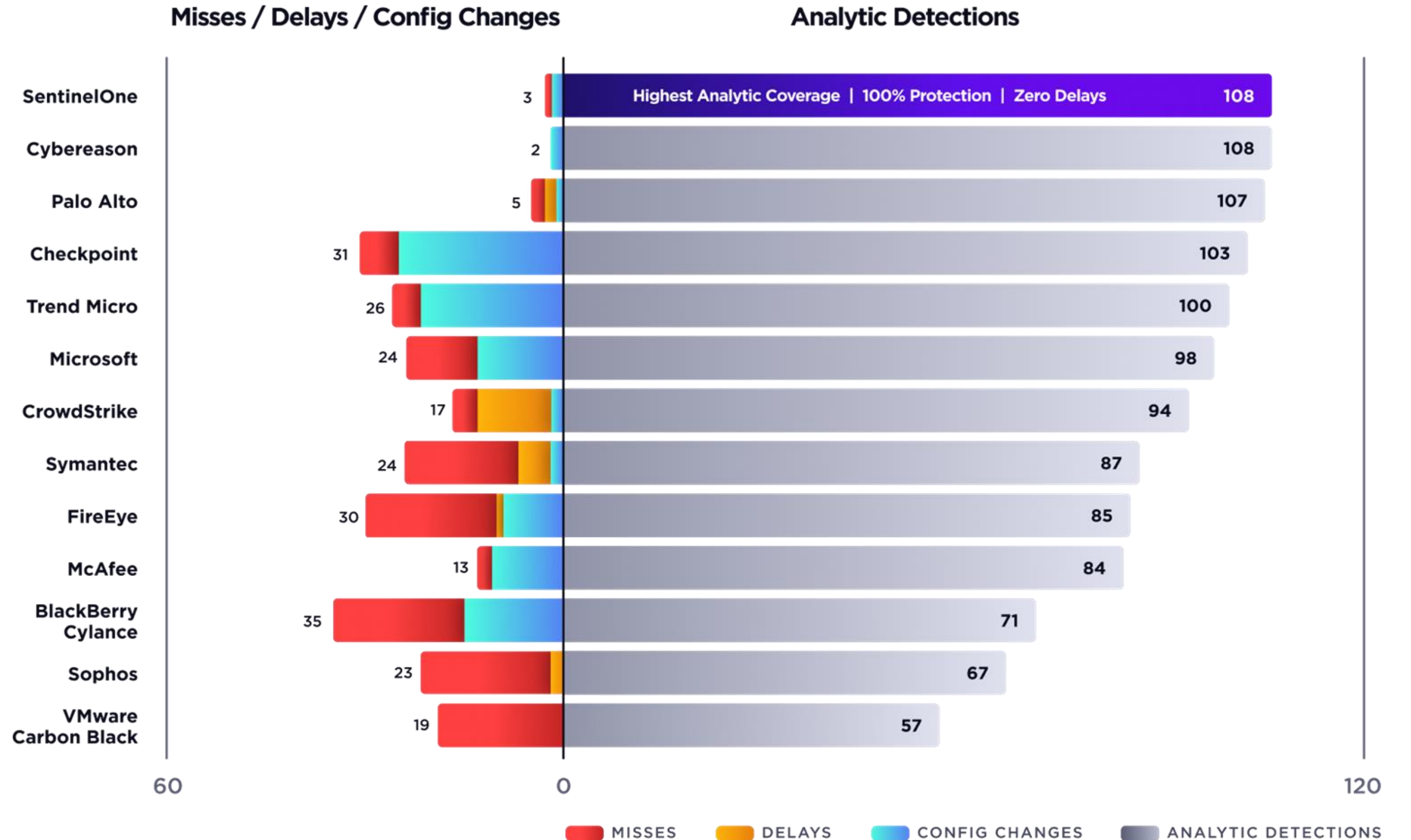
MITRE ATT&CK Results Data

Highest Analytic Coverage

Delivering 100% protection and highest quality context & insights without the noise

- ✔ INSTILLS CONFIDENCE
HIGHEST Analytic Coverage
- ✔ WORKS OUT-OF-THE-BOX
100% Protection
- ✔ MOVES AT MACHINE SPEED
ZERO Delayed Detections

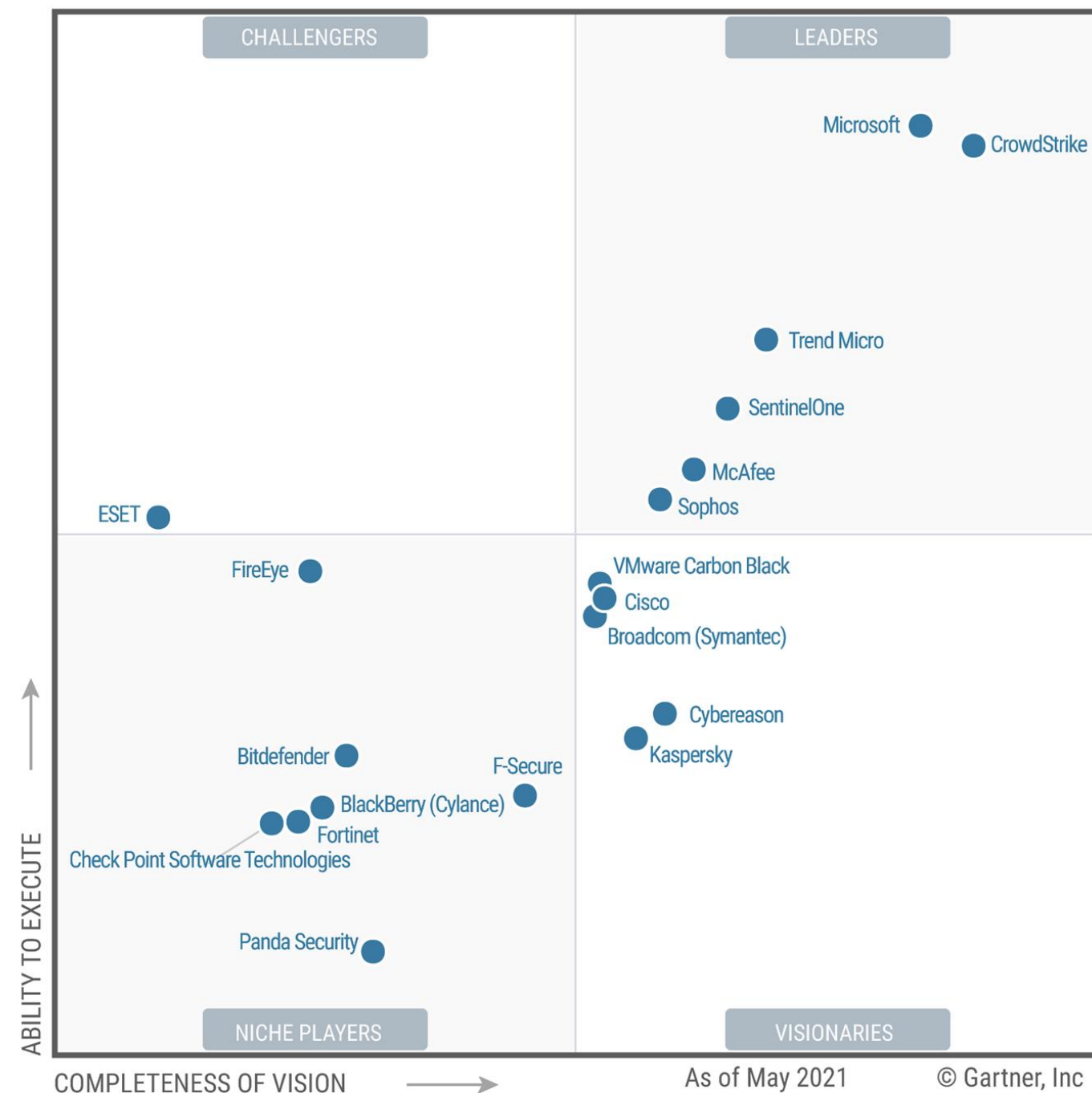
[MITRE ATT&CK Results Data](#)



Named a Leader.

2021 Gartner Magic Quadrant for Endpoint Protection Platforms

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (May 2021)

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 2021 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>

Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Thank you



sentinelone.com