SentinelOne®

SentinelOne

Next Generation Endpoint Security & EDR

Vince Bourgeois
Regional Sales Director

Agenda

Who is SentinelOne?

Endpoint Protection Convergence

Customer Challenges

Ransomware

Why SentinelOne? What makes us different?

MITRE Engenuity ATT&CK evaluation – day 1 scenario

SentinelOne Solutions

Q&A

Global Scale. Global Readiness

900+
Employees

6,000+
Customers

$697M+
Funding

$3B+
Valuation

24/7

VIGILANCE
MDR Team
DFIR 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

McKESSON | flex | EA | KENNETH COLE new york

Gartner peerinsights™ EPP + EDR 4.9 ★★★★★ — "Highest rated EDR vendor in Voice of the Customer"

FedRAMP

jetBlue | ESTĒE LAUDER | carta | Kubota

Gartner peerinsights™ MDR 5.0 ★★★★★ — Perfect Score Last 12 Months

ISO 27001 CERTIFIED by schellman

POLITICO | norwegian | HITACHI Inspire the Next | CENGAGE

kuppingercole ANALYSTS — Featured EPDR Innovator

TEVORA™ — HIPAA Attestation, PCI DSS Attestation

AUTODESK | cars.com | ttec | SINGAPORE AIRLINES

FORRESTER® — Wave™ EDR "Strong Performer"

CNBC DISRUPTOR 50

NORFOLK SOUTHERN | havas | workday | Shutterfly

MITRE ATT&CK™ — Highest Data Correlation Across All Vendors

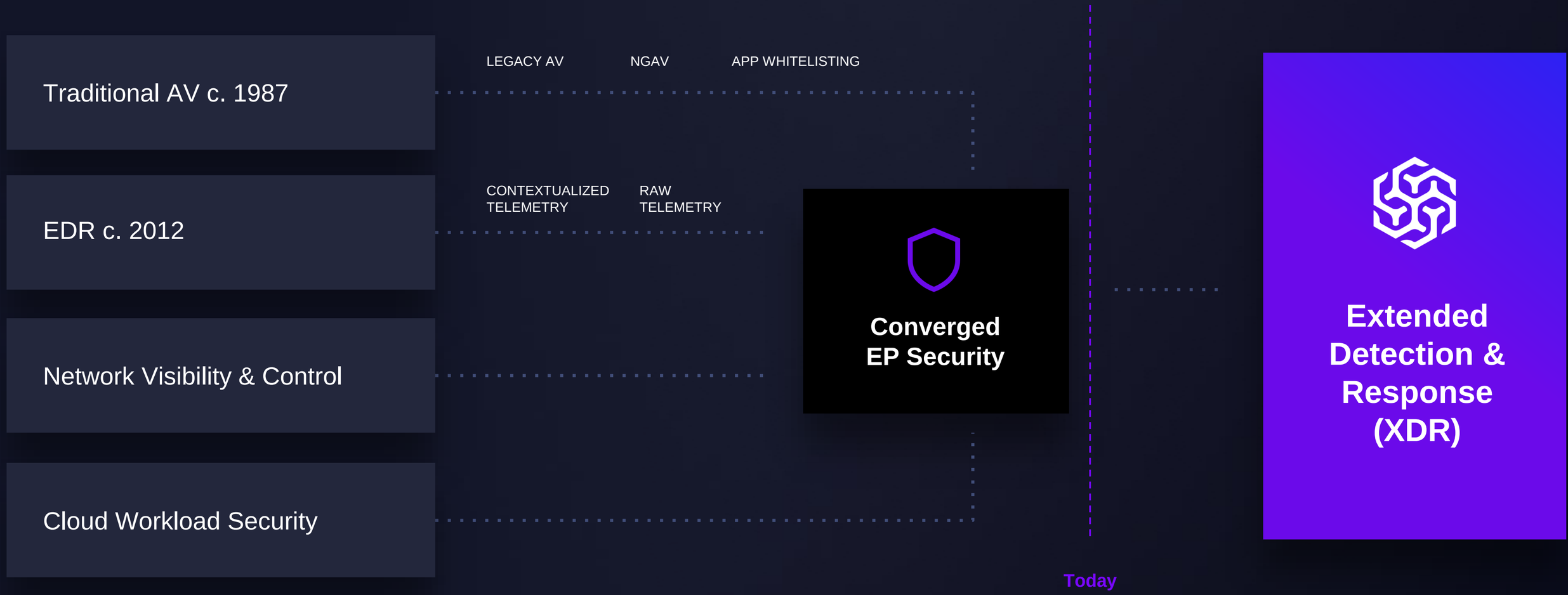
Forbes 2019 AI 50 MOST PROMISING AI FIRMS

SAMSUNG | O'NEILL | Sysco | ASTON MARTIN

SE Labs INTELLIGENCE-LED TESTING BEST New Endpoint WINNER 2020 — SE Labs Best New Endpoint

glassdoor 4.9 ★★★★★

Endpoint Protection (EP) Convergence
Market Overview



Common Challenges we hear from organizations

“We run traditional (signature based)

AV but we continue to get hit

with malware….”

“We can’t see what is really happening on our endpoints…”

“We are currently dealing with agent fatigue,

and looking to consolidate…”

“We still find ourselves reimaging systems or using several other tools to clean up endpoints…”

“We know we need something more advanced, but a lot of the solutions we have seen are either too complex or are not flexible enough…”

“We were hit with a Ransomware attack…”

A New Ransomware Attack Occurs Every 11 Seconds…..

Hackers paralyzed a pipeline. Banks and stock exchanges are even bigger targets

By Matt Egan, CNN Business

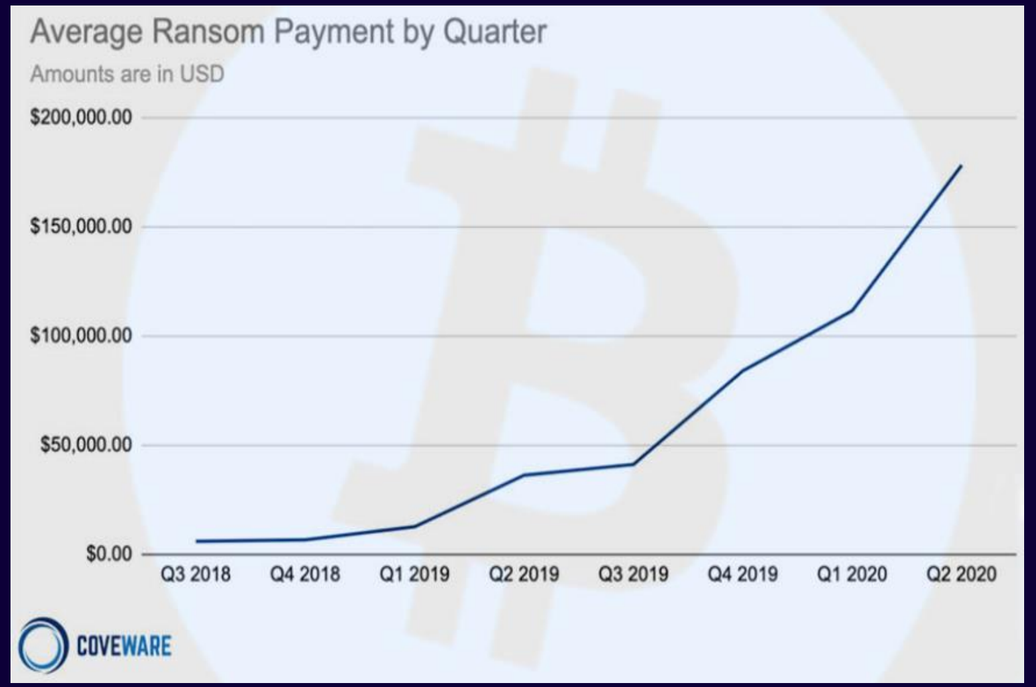
Updated 12:16 PM ET, Wed May 12, 2021

Ransomware on the rise

Cyberactivity that poses risks to the tech systems of banks and other companies increased significantly between March and June

- Ransomware and phishing attempts increased 64%
- Banks saw a 520% increase in ransomware and phishing attempts
- The number of connections to open Wi-Fi networks rose 243%
- Number of usernames and passwords exposed on dark web went up 429%

Source: Arctic Wolf's 2020 Security Operations Annual Report



Ransomware Payday: Average Payments Jump to $180,000

Ransomware attacks in numbers

- 51% of companies faced ransomware attacks.
- 26% of companies paid the ransom to cybercriminals.
- The average ransom amount in 2020 was $180,000 for big companies.
- The average ransom amount in 2020 for small businesses was $6,000.
- A set of software tools needed to launch a ransomware attack costs about $50 on the darknet.
- A new ransomware attack is detected every 11 seconds.

304 million

According to an annual report on global cyber security, there were a total of 304 million **ransomware** attacks worldwide in **2020**. This was a 62 percent increase from a year prior, and the second highest figure since 2014 with the highest on record being 638 million attacks in 2016. Apr 13, 2021

SentinelOne Ransomware Warranty

Protection **Visibility** **Simplicity** **Automation**

Protection Against Ransomware. Guaranteed.

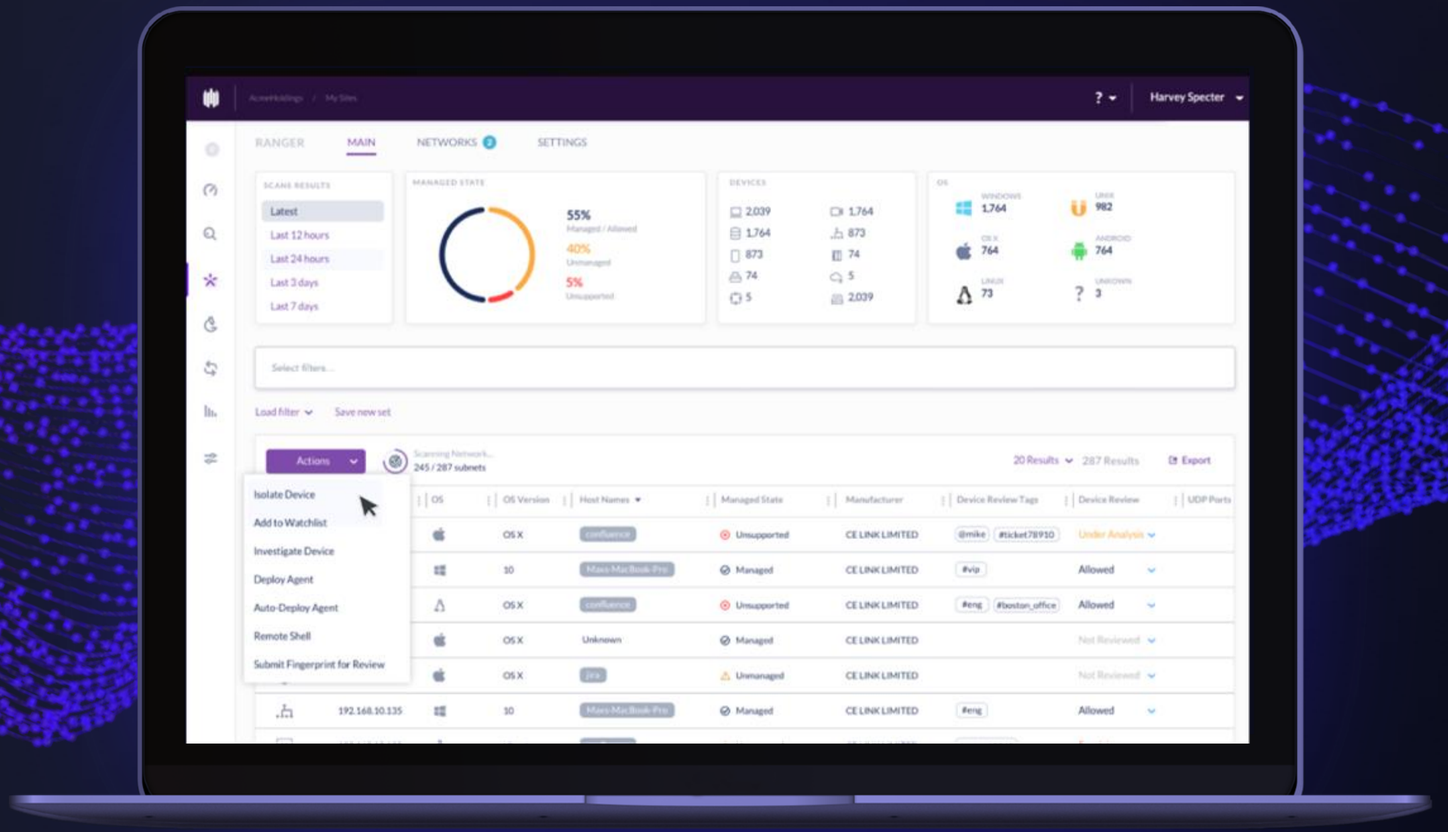
SentinelOne™

- $1,000 per endpoint
- $1M per client

Singularity is a Data Platform

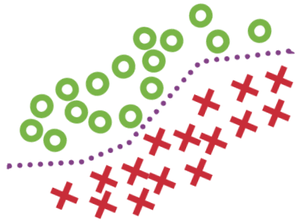
Designed to consume, understand, and action limitless data sets.

Endpoint Cloud IoT XDR



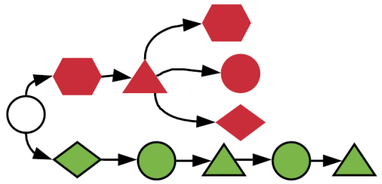
The Solution

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

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

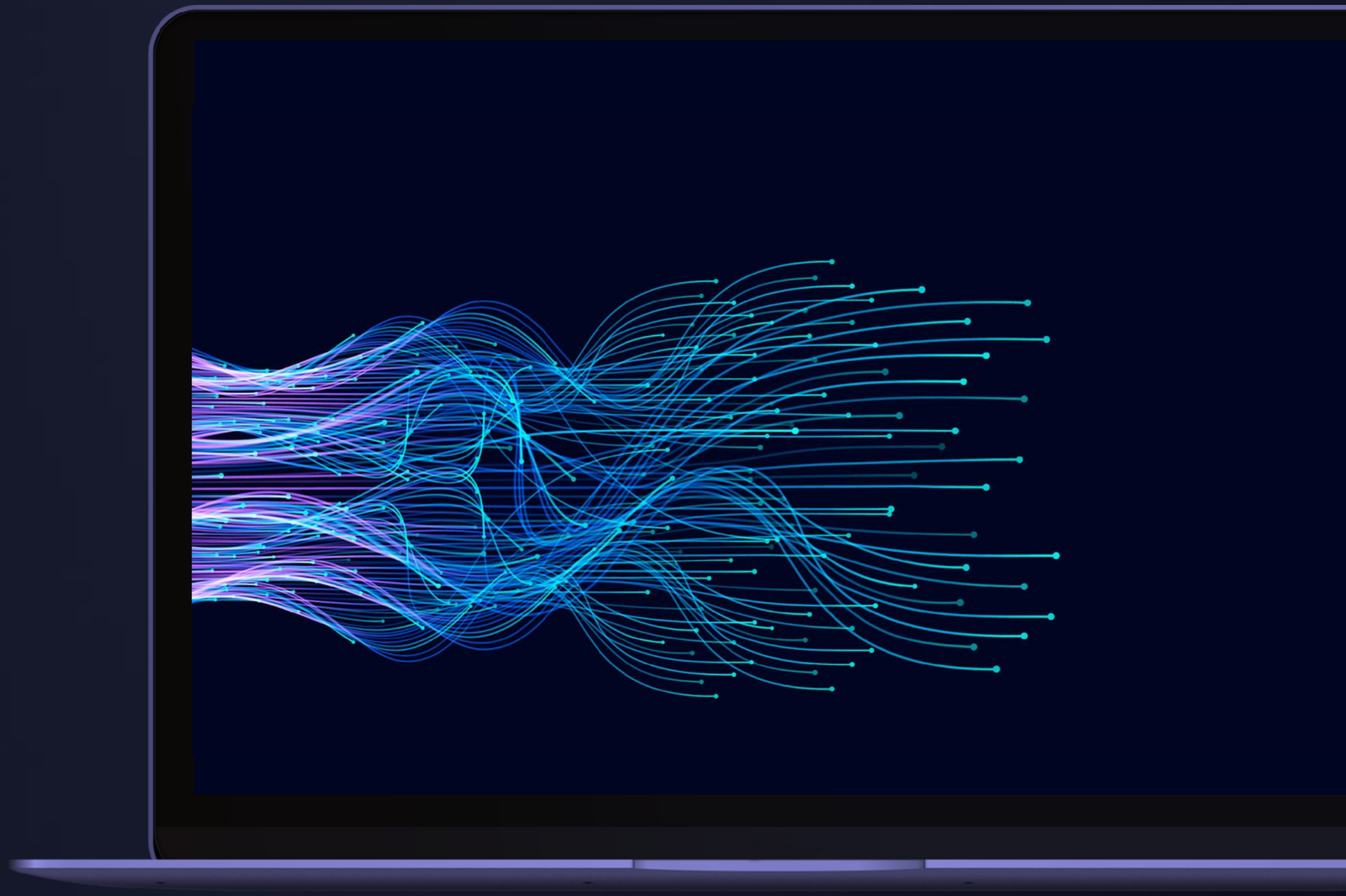
Retention: 30 days - 1 year
Full context and correlation
Integrated response workflow

Singularity™ Platform

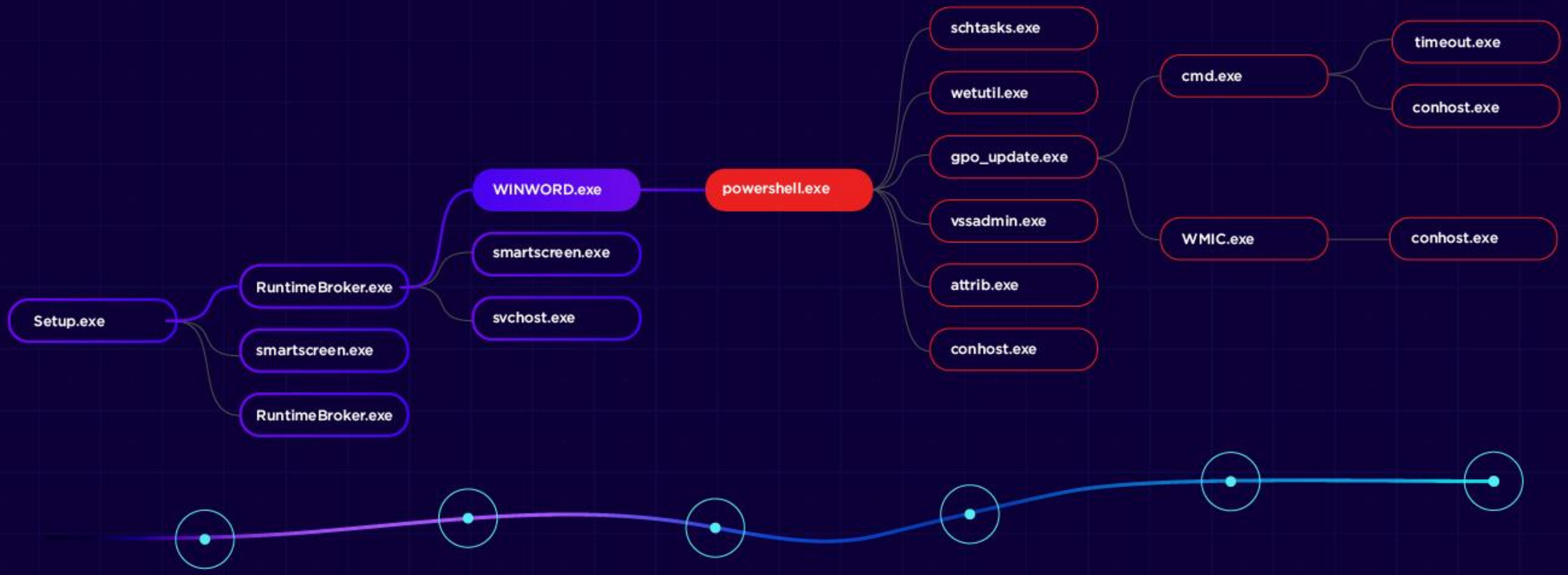
Storyline™

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



The Real Storyline & ActiveEDR



SentinelOne®

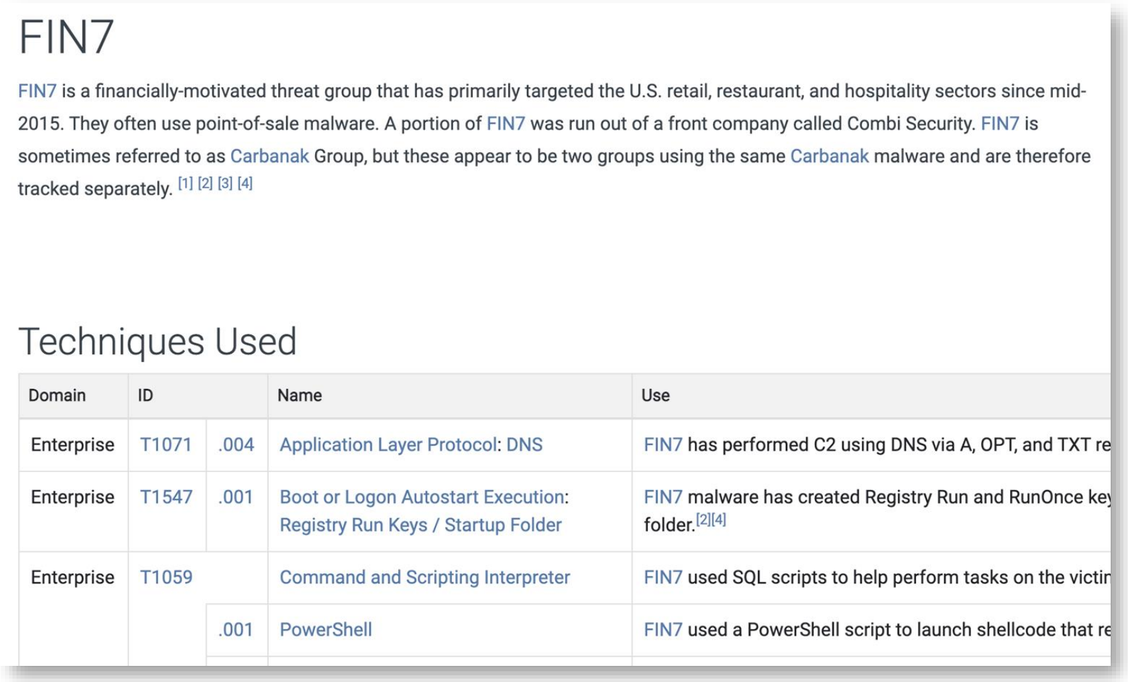
MITRE ENGENUITY™

ATT&CK 2020

Evaluation Testing Performed November 2020
Results Released April 2021

Threat Group Test Emulations

FIN7 → retail, hospitality



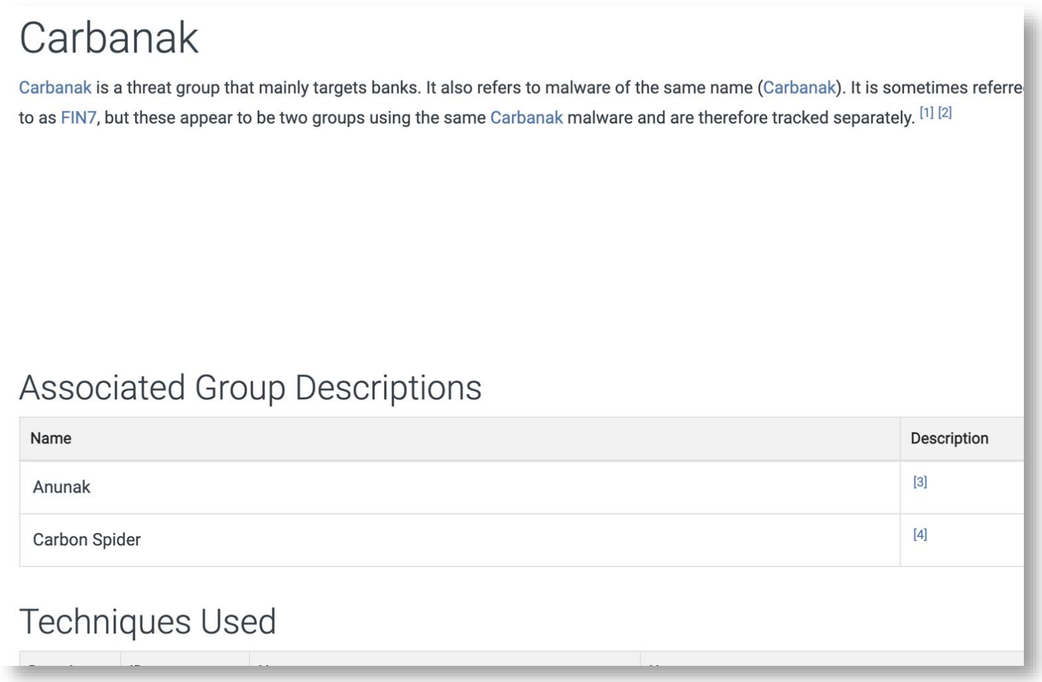
FIN7

FIN7 is a financially-motivated threat group that has primarily targeted the U.S. retail, restaurant, and hospitality sectors since mid-2015. They often use point-of-sale malware. A portion of FIN7 was run out of a front company called Combi Security. FIN7 is sometimes referred to as Carbanak Group, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. [1] [2] [3] [4]

Techniques Used

Domain	ID		Name	Use
Enterprise	T1071	.004	Application Layer Protocol: DNS	FIN7 has performed C2 using DNS via A, OPT, and TXT re
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	FIN7 malware has created Registry Run and RunOnce key folder.[2][4]
Enterprise	T1059		Command and Scripting Interpreter	FIN7 used SQL scripts to help perform tasks on the victir
		.001	PowerShell	FIN7 used a PowerShell script to launch shellcode that re

Carbanak → banks



Carbanak

Carbanak is a threat group that mainly targets banks. It also refers to malware of the same name (Carbanak). It is sometimes referre to as FIN7, but these appear to be two groups using the same Carbanak malware and are therefore tracked separately. [1] [2]

Associated Group Descriptions

Name	Description
Anunak	[3]
Carbon Spider	[4]

Techniques Used

More info → https://attack.mitre.org/groups/

Testing Flow

MITRE Engenuity ATT&CK Evaluation

All remote testing due to COVID

Schedule

Two emulations over 3 days

November 2020 with results released April 2021

Lab Setup

Multiple computers in a controlled environment

Test Execution

Step-by-step Carbanak + FIN7 emulation

20 stages comprising 174 steps

2 New Options for 2020: ✓ Linux, ✓ Prevention

Results Checking

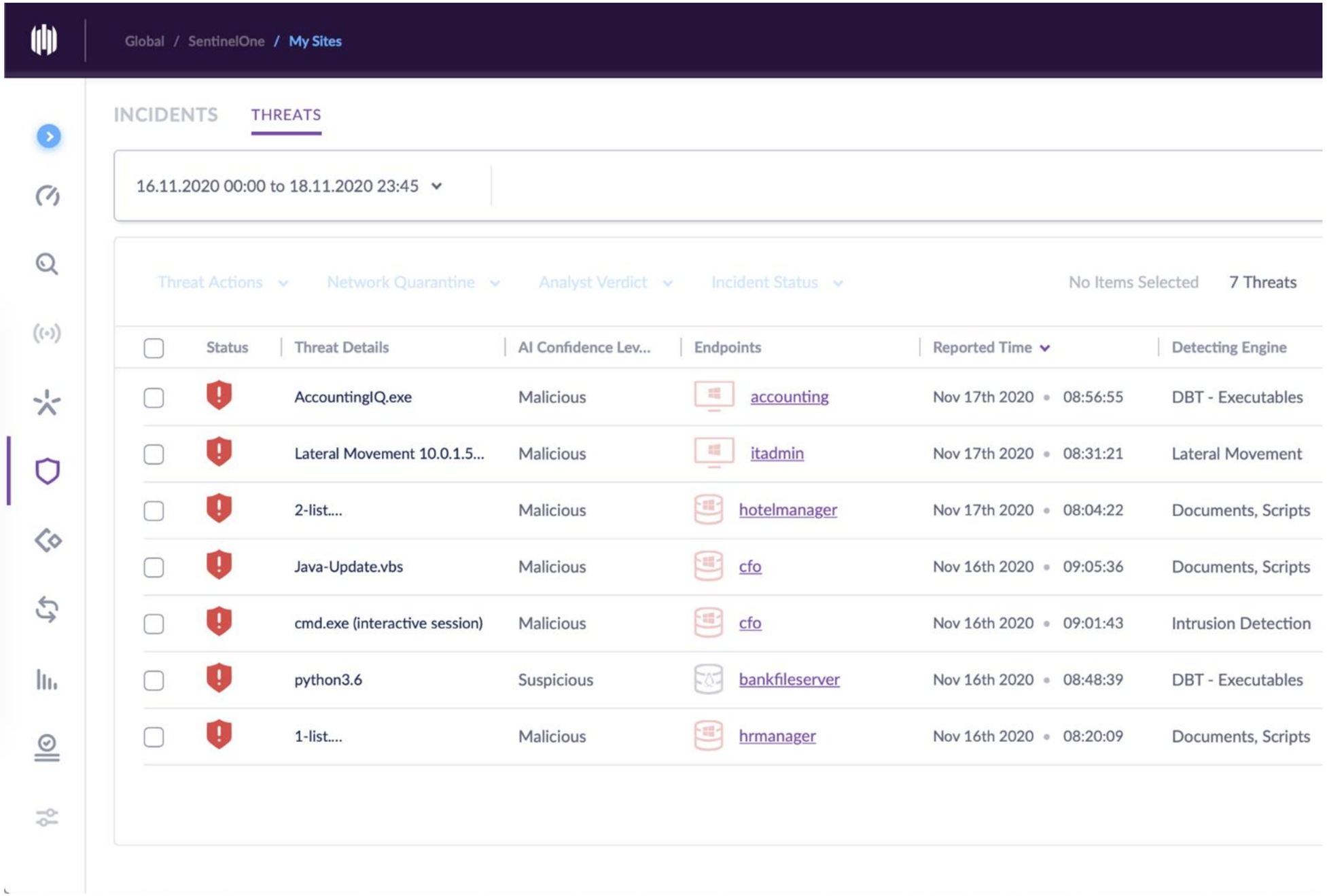
Stepwise results checking

MITRE Engenuity ATT&CK – Day 1 simulation

Unprecedented Simplicity

S1 summarized 2-days of testing into 7 Campaign Level console alerts.

Singularity proves its ability to correlate & contextualize making this EDR truly capable of alleviating common SOC burdens.



SentinelOne

S1 Core Endpoint Protection

Core

Control

Complete

Unifies Prevention, Detection & Response

- ✓ Autonomous decisions + Automatic, instant responses
- ✓ Global Intel + Static AI + Behavioral AI
- ✓ Full forensics & indicators. Easy pivot to EDR.

Protection Differentiators

- ✓ Holds up to high velocity & stealthy attacks
- ✓ Clean, simple management UX provides context
- ✓ Feature parity across OSes

ONE One Agent & Console

VDI

MITRE ATT&CK™

SentinelOne™

S1 Core Endpoint Recovery

Core

Control

Complete

Painless, fast attack recovery keeps users working

Recovery Differentiators

- ✓ Easy reversal of unauthorized changes
- ✓ One-click remediation & Windows rollback
- ✓ Device isolation & triage
- ✓ Less re-imaging. Less operational work.

ONE One Agent & Console

VDI

MITRE ATT&CK™

SentinelOne™

S1 Control

Core
Control
Complete

Adds security suite features to further support agent consolidation

Firewall for all OSes

Bluetooth & BLE Control

Full Remote Shell for all OSes

USB Device Control

Unpatched Apps

ONE One Agent & Console

VDI

MITRE ATT&CK™

SentinelOne™

S1 Complete EDR

Core

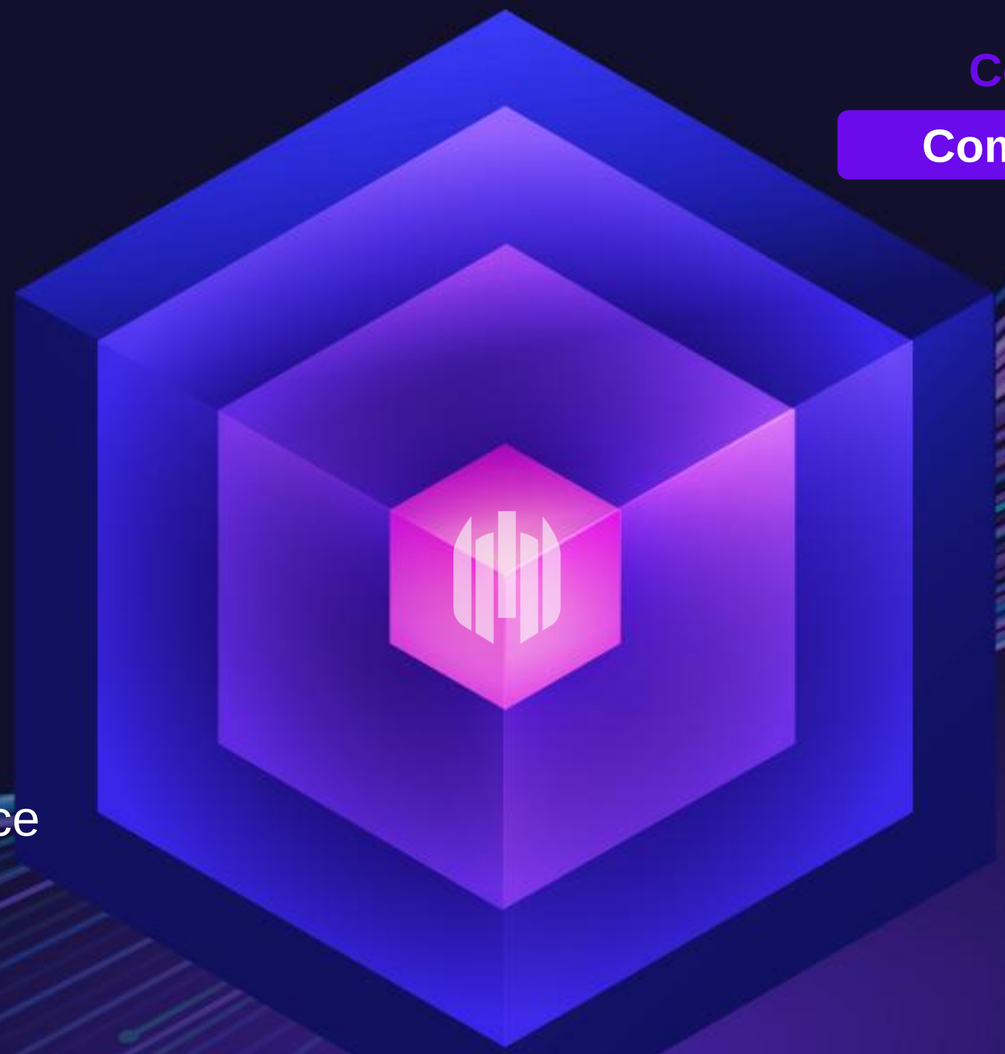
Control

Complete

Adds Deep Visibility™ Endpoint Detect & Respond

EDR Differentiators

- ✓ Combines enterprise features + ease-of-use
- ✓ Deeply coupled with Prevention enforcement
- ✓ MITRE ATT&CK™ technique searching
- ✓ ActiveEDR™ mark entire story as threat
- ✓ Built for massive data retention, scale, performance



ONE One Agent & Console

VDI

MITRE ATT&CK™

SentinelOne™

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

1 ONE Console

Manage all workloads in a single console across GEOs

Why SentinelOne?

Value

Critical features drive consolidation. Simple packaging.

Easy to deploy. Compatible. Fast time to value.

Empower staff with superior usability. Uplevel skills

Best in class customer service

97% Customer Satisfaction

97% Would Recommend S1

Net Promoter Score in the “great” to “excellent” range

353% ROI

Forrester TEI

Thank you

SentinelOne®

sentinelone.com