Controlware Security Day 2022

controlware

SentinelOne®

SentinelOne®

Singularity™ XDR

Konsolidieren Sie Ihre Cyber-Security für Endpoint, Workloads & Cloud in einer Lösung

Sascha Hyckel

Enterprise Account Manager

Global Scale. Global Readiness.

S
LISTED
NYSE
Most valuable
Cyber IPO

1500+
Employees

7,000+
Customers

3 of the Fortune 10

24/7

VIGILANCE
MDR Team
DFIR Team

SUPPORT
Follow-the-Sun

97% renewal rate

GLOBAL LOCATIONS

Mountain View, Tel Aviv, Amsterdam, Prague, London, Ft. Lauderdale, Eugene, Tokyo

GLOBAL DATA CENTERS

AWS US, Frankfurt, Tokyo, Canada, GovCloud

SentinelOne

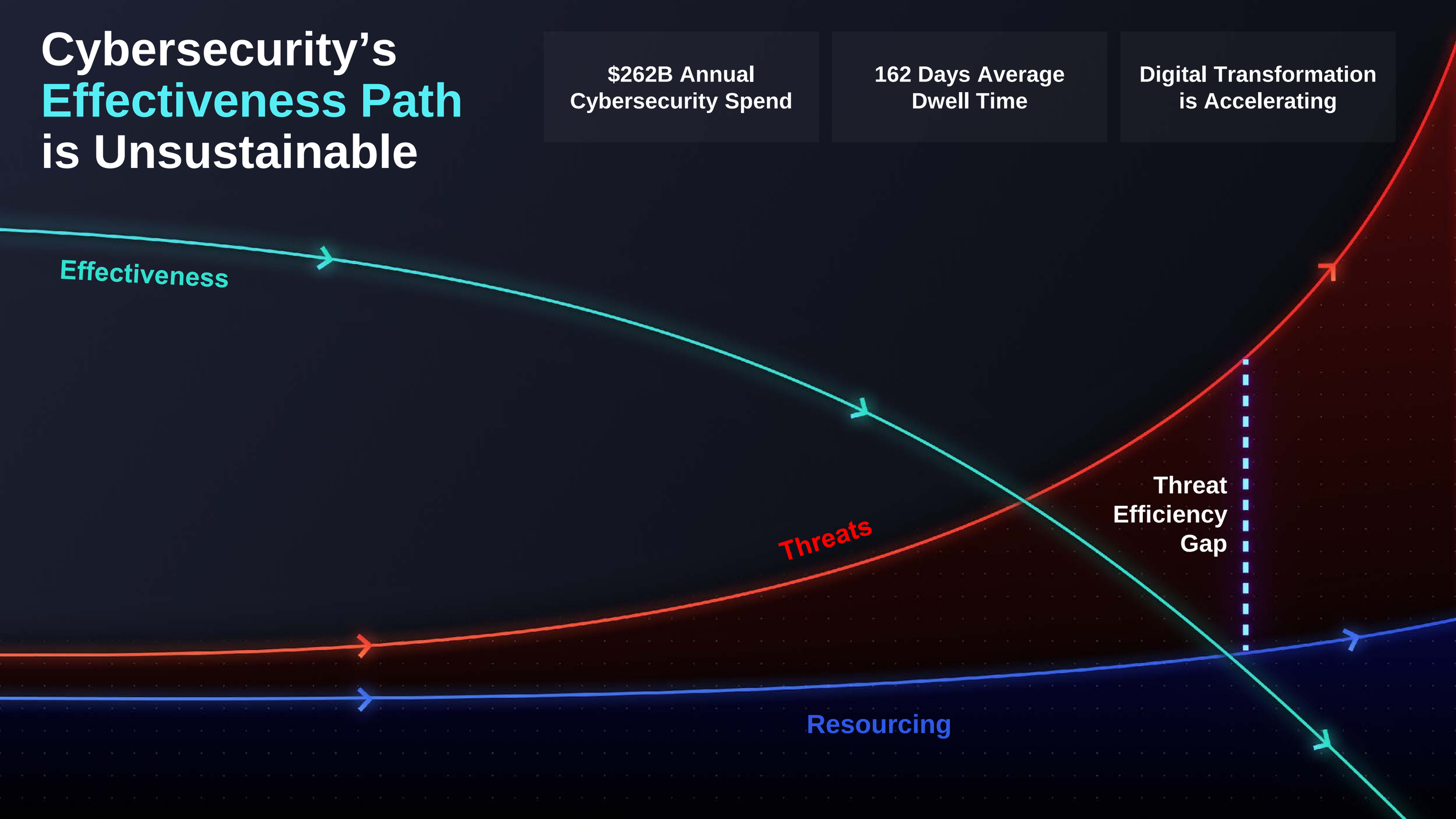
April 2022 statistics

Cybersecurity's Effectiveness Path is Unsustainable

$262B Annual Cybersecurity Spend

162 Days Average Dwell Time

Digital Transformation is Accelerating



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Outdated Solutions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

A Different Approach to Resolution

Data

Data to Insights

Tools

Tools to a Platform

People

Dependent to Efficiency

Automation

SHIFTING FOCUS TOWARDS DATA

SentinelOne

An Evolution Towards Improved Outcomes

Objectives
Mechanisms
Outcomes

XDR

Augment & Resolve

EDR + Cross Domain Integrations

Business Resilience

EDR

Detect & Respond

Behavioral AI + Full Visibility +
1 Click remediation

See More, Recover Faster

NGAV

Prevent

Autonomous AI Prevention

Reduce Device Impact

Device Focused

Incident Focused

Outcome Focused

Singularity™ Platform

Platform Capabilities

Prevention & Control

Detection & Response

Remediation & Recovery

Storyline

Network Visibility & Attack Surface Control

XDR Automation

INGEST

Singularity Platform

AI Powered XDR

Bi-Directional API

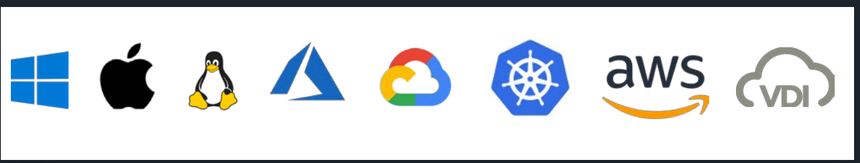
EXPORT

Services Capabilities

Intelligence Driven Threat Hunting

Managed Detection & Response

Digital Forensics & Incident Response

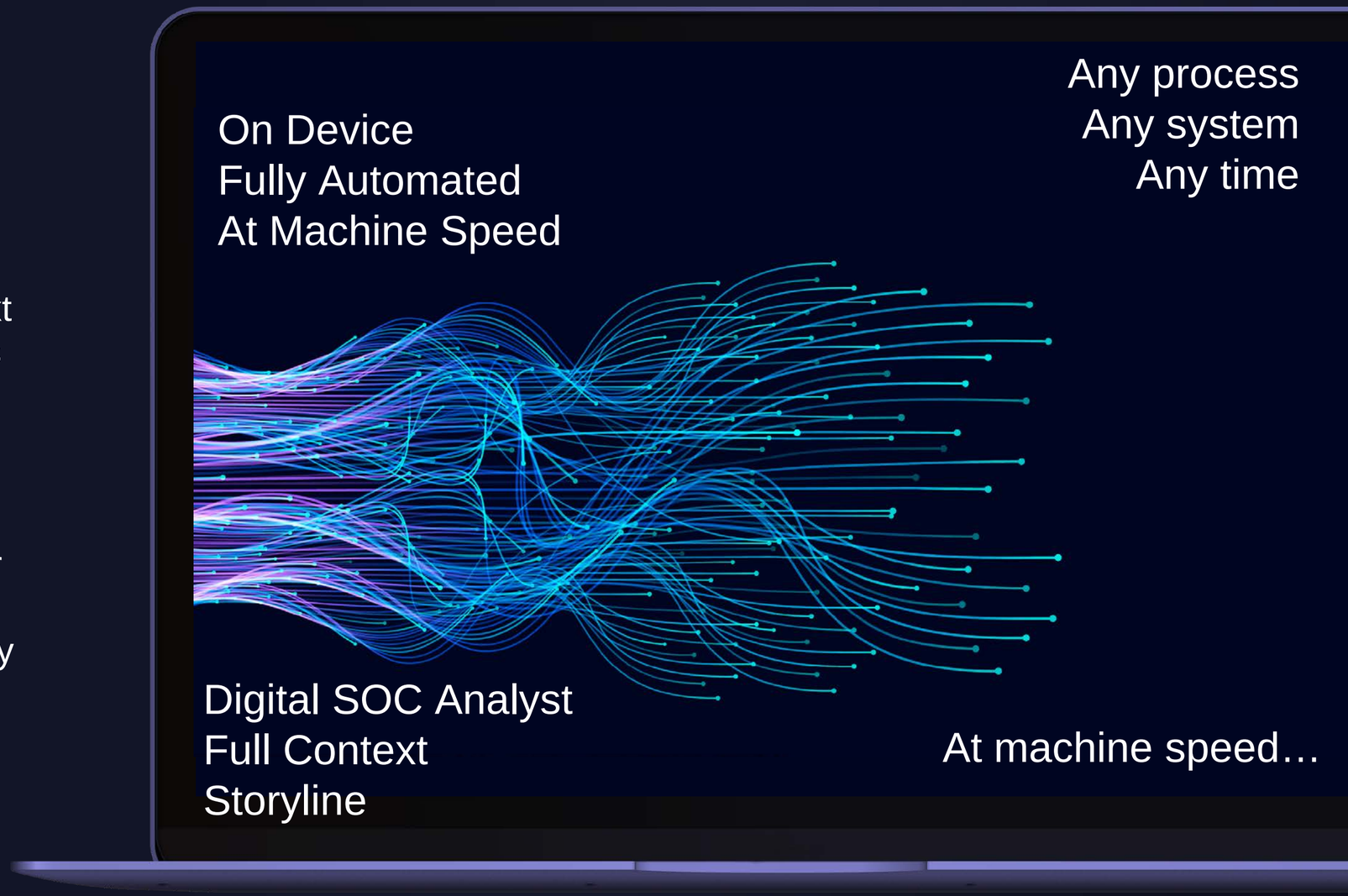


Singularity Platform

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



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

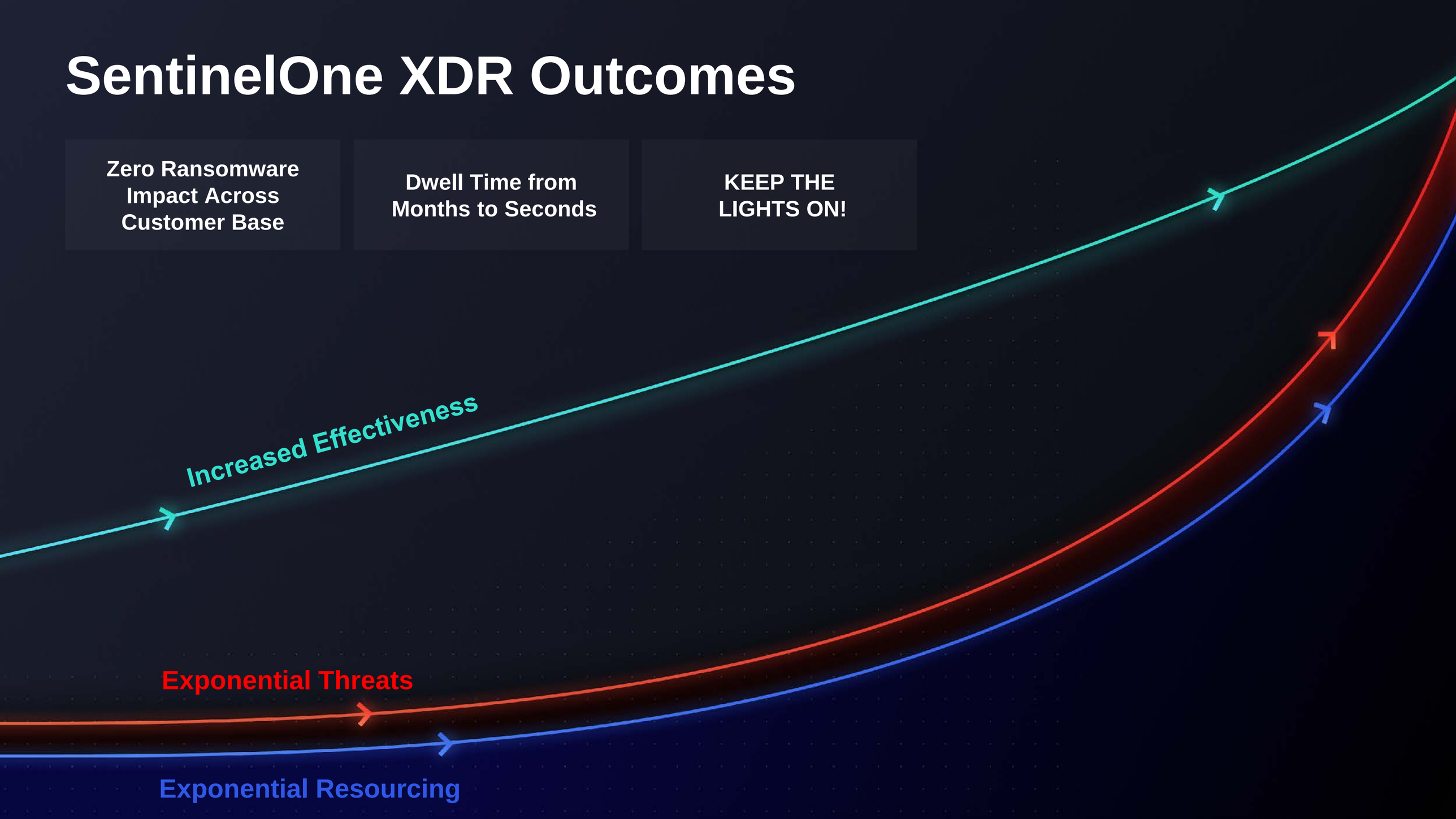
SentinelOne

SentinelOne XDR Outcomes

Zero Ransomware Impact Across Customer Base

Dwell Time from Months to Seconds

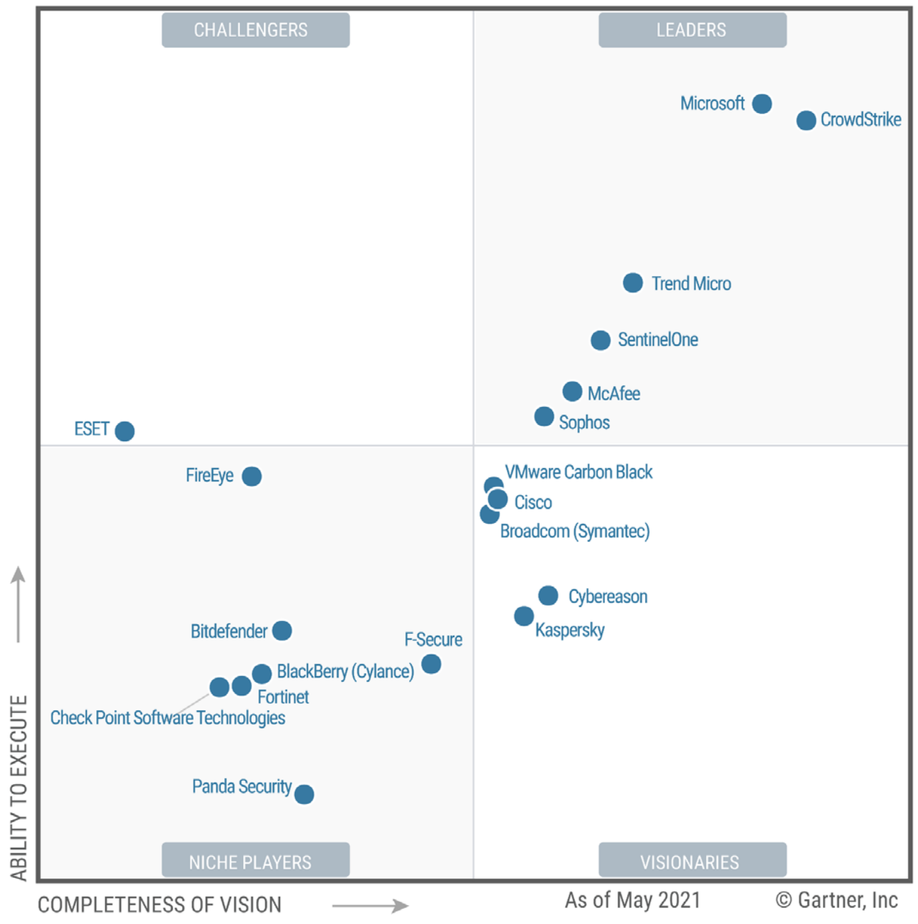
KEEP THE LIGHTS ON!



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	TYPE B USE CASE	TYPE C USE CASE
Lean Forward Organizations	Blended Approach Organizations	Prevention Focused Organizations
Highest Score	**Highest Score**	**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.

MITRE ATT&CK Results Data

100% Protection

9 of 9 MITRE ATT&CK Tests

100% Detection

19 of 19 Attack Steps

100% Real-Time Protection

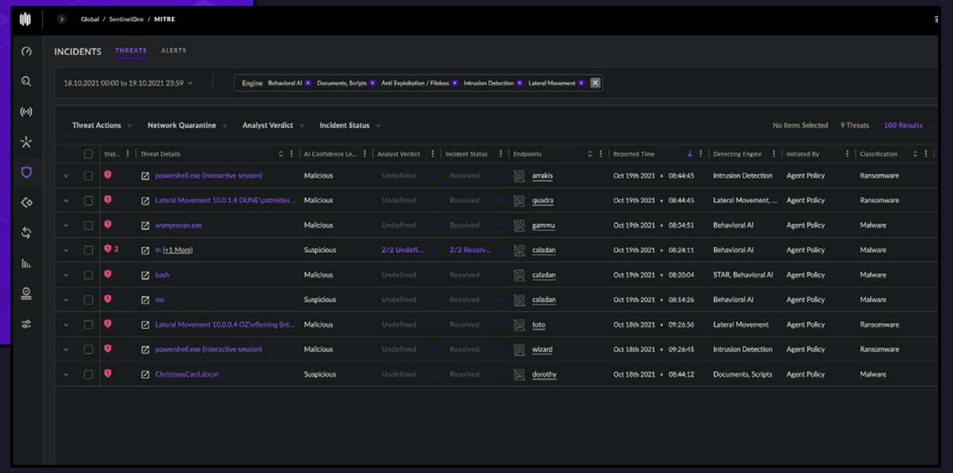
0 Delays

99% Visibility

108 of 109 Attack Sub-Steps

99% Highest Analytic Coverage

108 of 109 Detections



S1 AVERAGED 300% FEWER DISTINCT ALERTS THAN OTHER VENDORS

SentinelOne


Endpoint, Storage & Servers
Cloud, Containers
Mobile
IoT & Network
Identity
Active Directory
Endpoint Protection
Endpoint Detection & Response
Incident Response Tooling
Cloud Workload Security
Identity, Detection & Response
Insider Threat & Deception
Attack Surface Management
Security Data Analytics
Managed Services
Singularity XDR
T1113
T1078
T1037
Powered by STORYLINE
aws
Singularity Marketplace

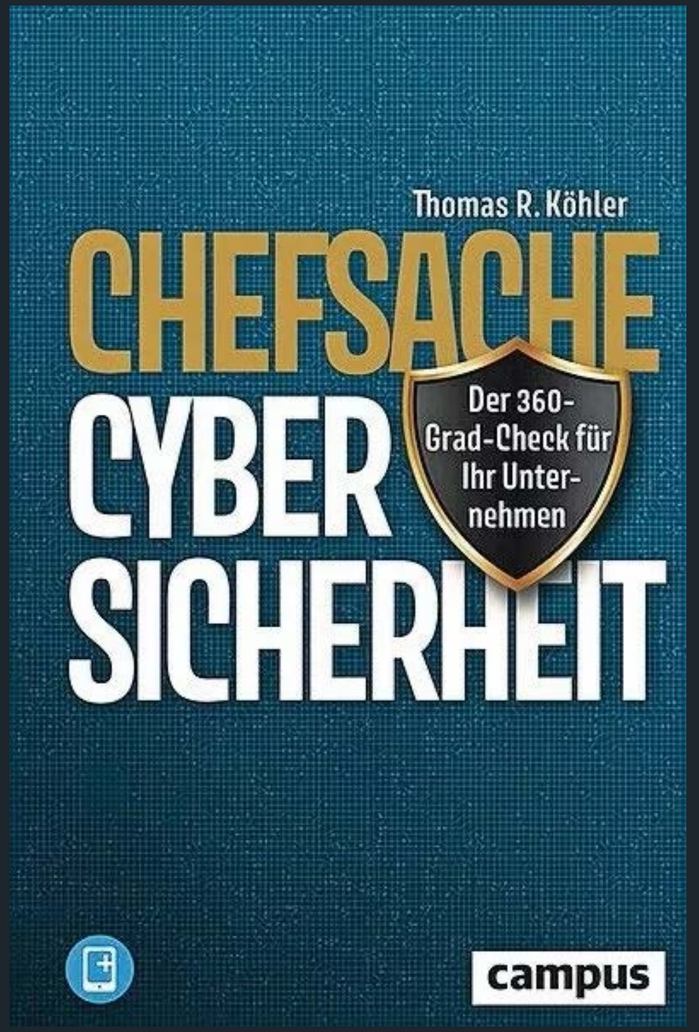
SentinelOne®

Autonomous Cybersecurity

Einladung zur technischen Demo

- Vereinbaren Sie eine technische Demo bei uns am Stand

- Die ersten 15 Registrierungen erhalten das Buch „Chefsache Cybersicherheit“ von Prof. Thomas R. Köhler



Prof. Thomas R. Köhler:
- Technologieexperte mit Fokus auf Cybersicherheit
- Forscher, Autor und Keynote Speaker
- Bekannt aus TV, Radio und Print-Medien


Thank you