SentinelOne

Einfach. Mehr Sicherheit.

Martin Knopf
Senior Systems Engineer

Einfach. Mehr Sicherheit.

Risiko reduzieren.

Moderne Angriffe
Breaches / Ransomware
Datenwachstum

Betrieb vereinfachen.

Fachkräftemangel
Zu viele Tools
Mangelnde Sichtbarkeit

Kosten senken.

Budgetlimitierung
Mehr mit weniger machen
Makroökonomische Herausforderungen

Einfach. Mehr Sicherheit.

Risiko reduzieren.

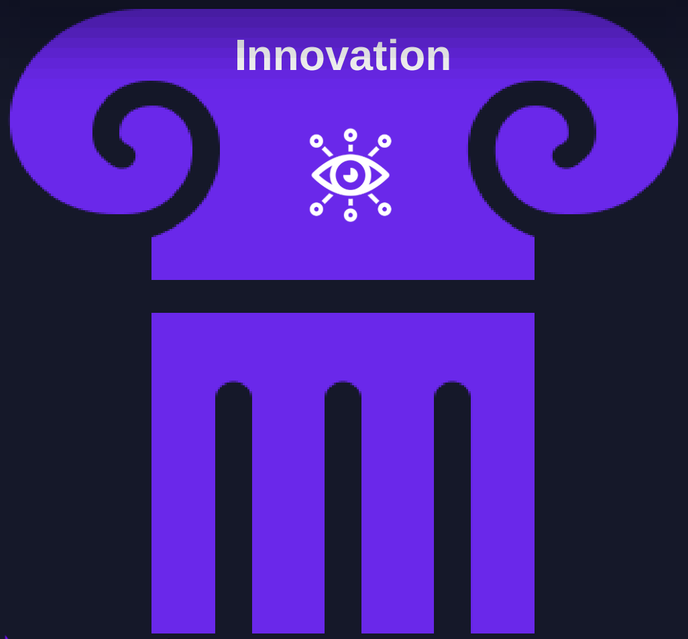
Moderne Angriffe
Breaches / Ransomware
Datenwachstum

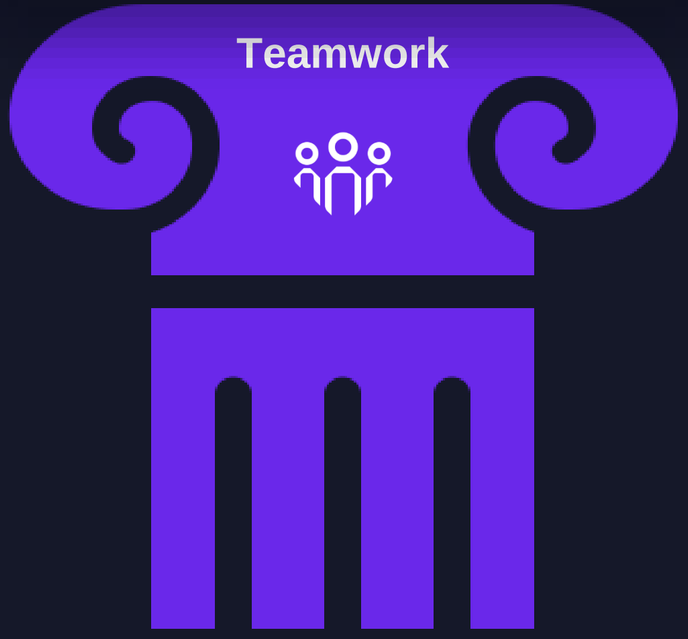
Betrieb vereinfachen.

Fachkräftemangel
Zu viele Tools
Mangelnde Sichbarkeit

Kosten senken.

Budgetlimitierung
Mehr mit weniger machen
Makroökonomische Herausforderungen







Wo können wir helfen?

Any Data

Cybersecurity – A Data Problem

Any Surface

Workstation, Server, Cloud, Storage, …

Any Time

Any process, any device, any time

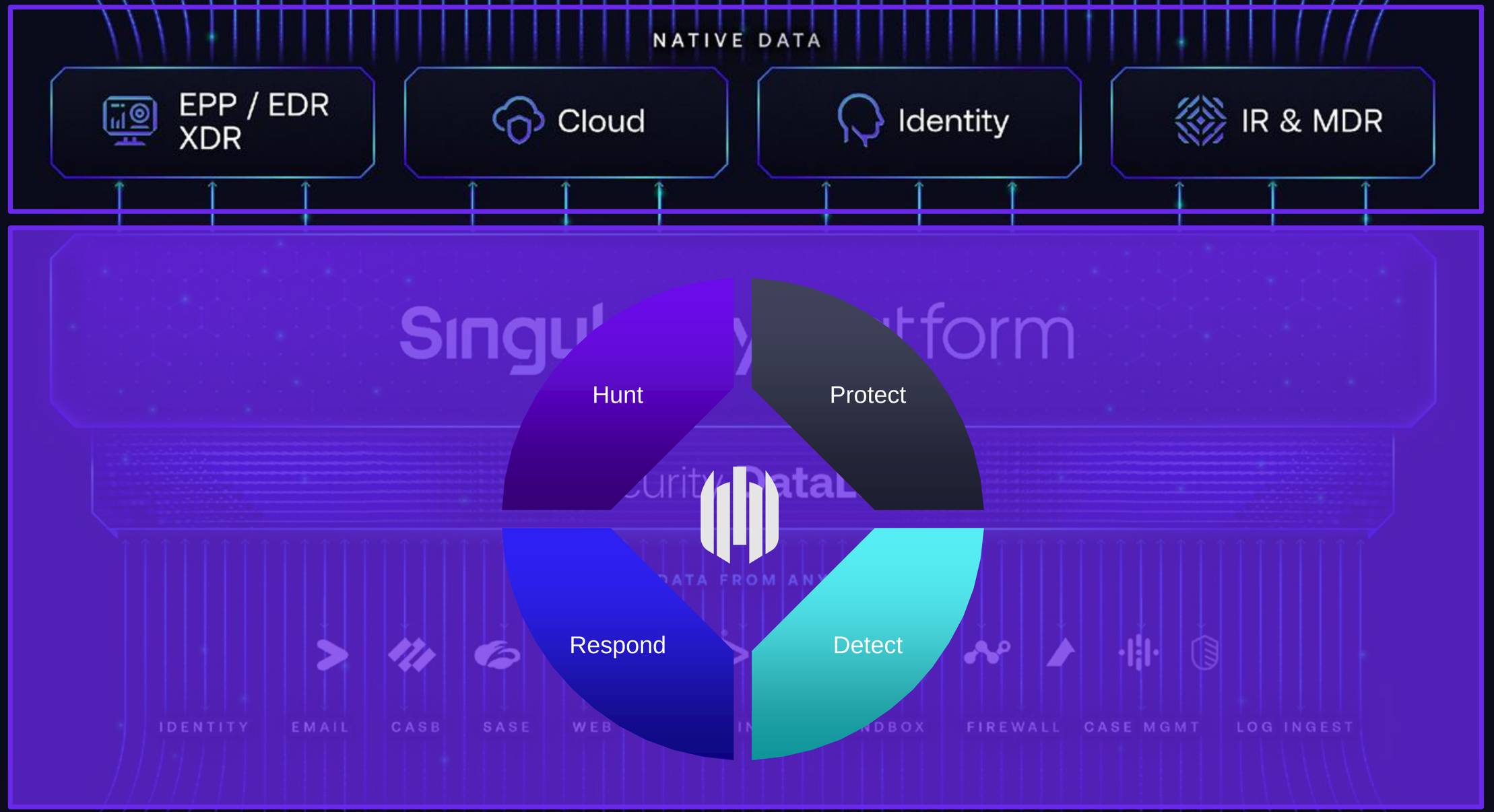
Einfach. Mehr Sicherheit.

Data Ingest

Platform Management

Unified Security DataLake

Einfach. Mehr Sicherheit.


NATIVE DATA
EPP / EDR
XDR
Cloud
Identity
IR & MDR
Hunt
Protect
Respond
Detect
IDENTITY
EMAIL
CASB
SASE
FIREWALL
CASE MGMT
LOG INGEST
Data Ingest
Platform Management
Unified Security DataLake

NATIVE DATA

EPP / EDR
XDR

Cloud

Identity

IR & MDR

Single Agent

Any Surface (Worksations, Server, Mobile,…)
Any OS (Windows, Mac, Linux)

Autonomous

Storyline (any process, any time, any device)
Response and Rollback

AI-Powered

Digital Behaviour
Fast & Transparent

Data Ingest

Platform Management

Unified Security DataLake

NATIVE DATA

EPP / EDR
XDR

Cloud

Identity

IR & MDR

Cloud Workloads

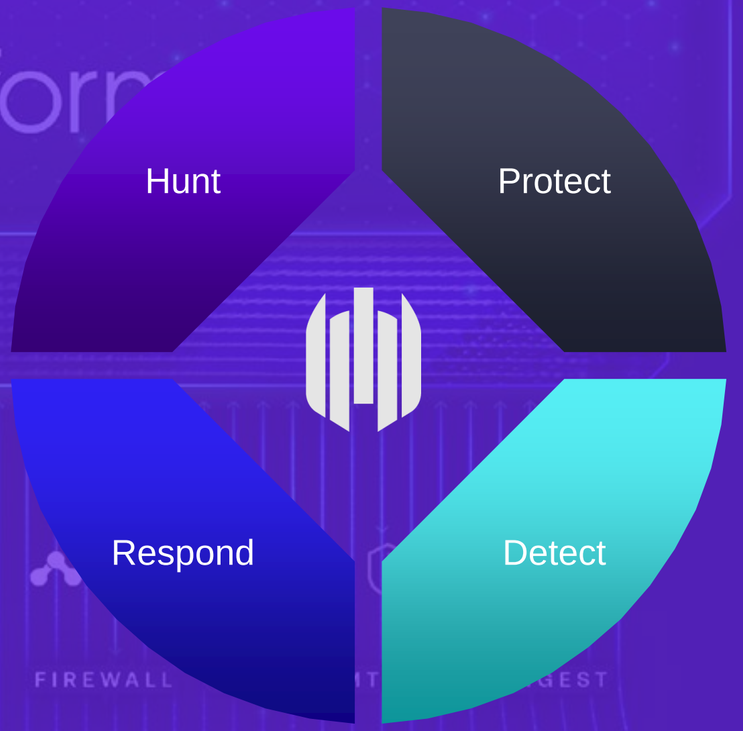
Virtual Machines, Containers, physical machines
Across clouds and data centers

S3 Buckets

Threat Detection for amazon S3
Detect Malware & Zero Days in milliseconds

NetApp Filer

Threat Detection for NetApp
Stops file storage from spreading malware



Data Ingest

Platform Management

Unified Security DataLake

NATIVE DATA

EPP / EDR
XDR

Cloud

Identity

IR & MDR

Attack Surface Management

Spot misconfiguration within your AD
Pinpoint Vulnerabilities and shift left

ITDR

Real-time Identity Threat Detection & Response
Guard against identity infrastructure misuse

Network Deception

Lures in-network threat actors (insider attacks)
Using system decoys to attract and reveal attackers

Data Ingest

Platform Management

Unified Security DataLake

NATIVE DATA

EPP / EDR
XDR

Cloud

Identity

IR & MDR

Managed Detection & Response

24/7 Managed Detection & Response
Shorter MTTR, Fewer Alerst, More Control

Threat Hunting Services

Deep Dive Threat Hunting & Assessment Service
Custom Reports & Recommendations

Incident Response

Preset incident response retainer hours
React and recover with dedicated case manager

Data Ingest

Platform Management

Unified Security DataLake

NATIVE DATA

EPP / EDR
XDR

Cloud

Identity

IR & MDR

Managed Detection & Response

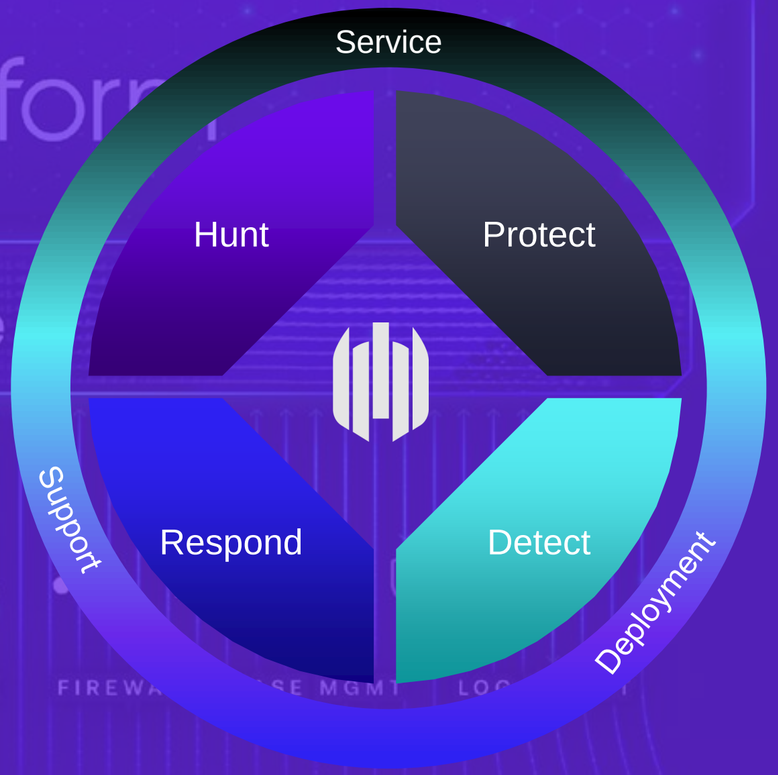
24/7 Managed Detection & Response
Shorter MTTR, Fewer Alerst, More Control

Threat Hunting Services

Deep Dive Threat Hunting & Assessment Service
Custom Reports & Recommendations

Incident Response

Preset incident response retainer hours
React and recover with dedicated case manager



Data Ingest

Platform Management

Unified Security DataLake

Any Data

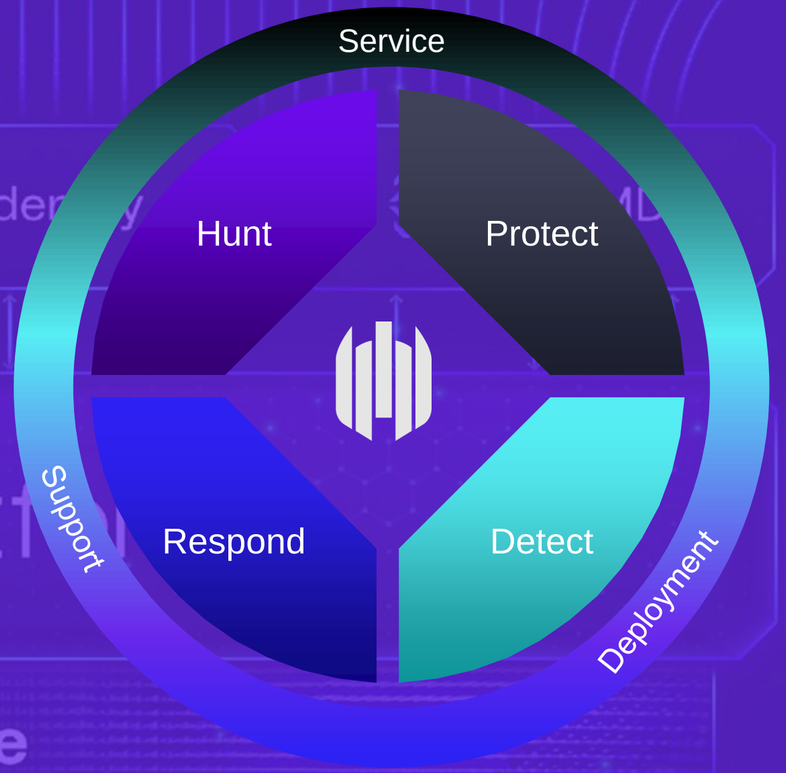
Ingest security relevant Data from any source
Marketplace for predefined interfaces

Teamwork

Not only ingest, but also share information
with your existing ecosystem to further improve

Use Cases

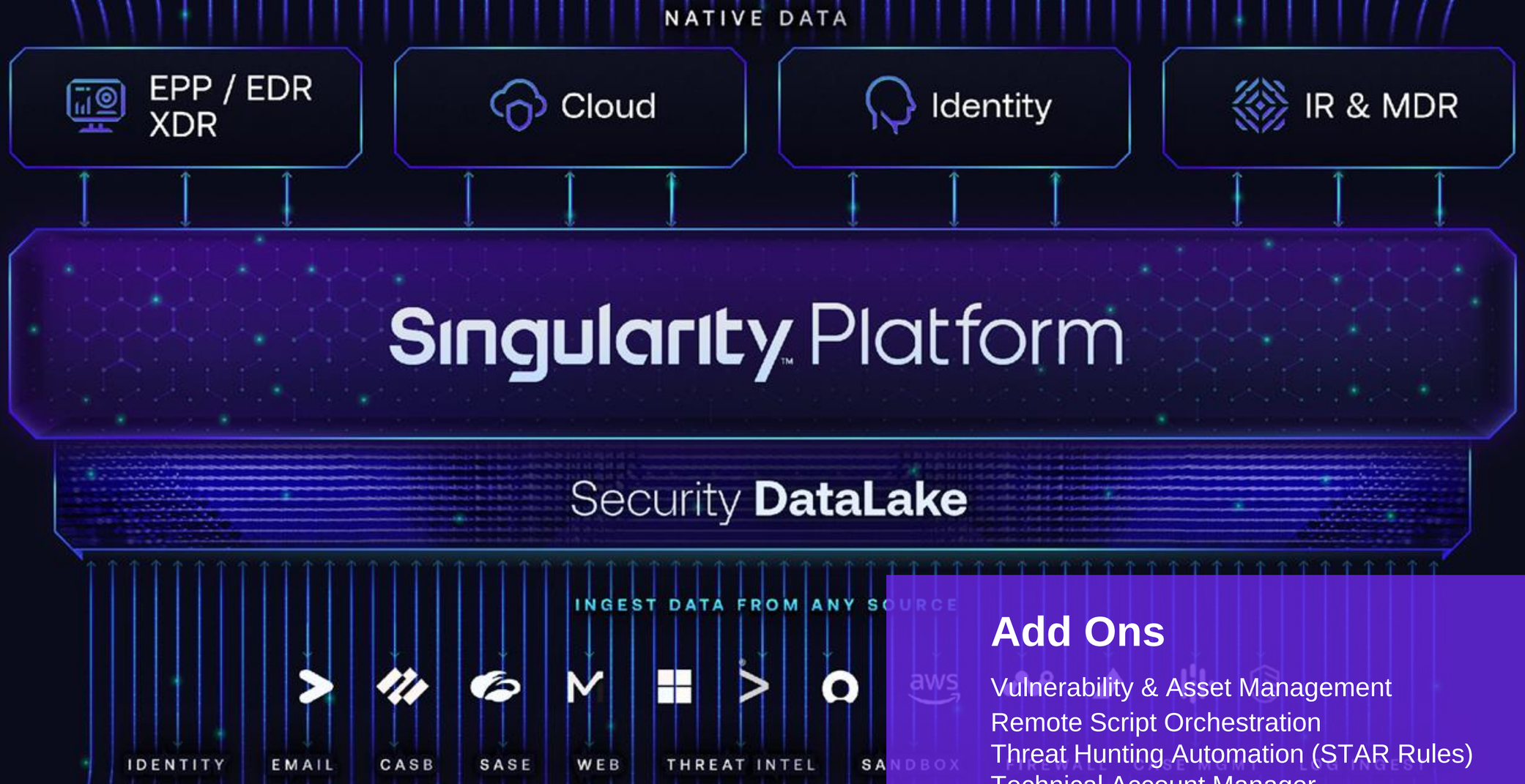
Okta
Netskope
ZScaler



INGEST DATA FROM ANY SOURCE

IDENTITY EMAIL CASB SASE WEB THREAT INTEL SANDBOX FIREWALL CASE MGMT LOG INGEST

Data Ingest | Platform Management | Unified Security DataLake



Add Ons

Vulnerability & Asset Management
Remote Script Orchestration
Threat Hunting Automation (STAR Rules)
Technical Account Manager
…

Einfach. Mehr Sicherheit.

NATIVE DATA

EPP / EDR
XDR

Cloud

Identity

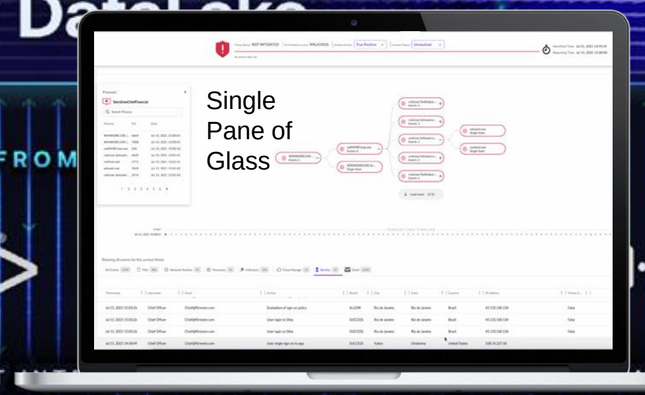
IR & MDR

Singularity™ Platform

Security Data

INGEST DATA FROM

IDENTITY EMAIL CASB SASE WEB THREAT



vs.

LOG

Data Ingest

Platform Management

Unified Security DataLake



Wo können wir helfen?

Wo können wir helfen?

Innovation

Moderne Technologien / KI
Automatisierung
”Single Pane of Glass”

Teamworking

Erkenntnis Teilen (Ökosystem)
Konsolidierung
Managed Services

Konsolidierung

Weniger Tools
Mehr Sichtbarkeit
Weniger Komplexität

Markt, Technologie, Kunden

Gartner

Magic Quadrant

A Leader.

SentinelOne is a Leader in the 2023 Gartner Magic Quadrant for Endpoint Protection Platforms.

Gartner Ranks SentinelOne Highest Among All Vendors in Critical Capabilities

MITRE ENGENUITY™

100% Protection Zero Misses

SentinelOne delivered full protection and was fastest to detect and block attacks.

Zero Delays

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

Highest Analytic Coverage 3 Years Running

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

Gartner Peer Insights™

4.8 Rating

★★★★★

Across EPP, EDR, and CWPP

96% Would Recommend

SentinelOne - Global Scale. Global Readiness

S
LISTED
NYSE

GLOBAL LOCATIONS

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

GLOBAL DATA CENTERS

AWS US, Frankfurt, Tokyo, Canada, GovCloud

>2,500
Employees

10,000+
Customers

4 of the Fortune 10

97% renewal rate

24/7

VIGILANCE
MDR Team
DF/IR Team

SUPPORT
Follow-the-Sun

SentinelOne®

Einfach. Mehr Sicherheit.

RoundTable um 15:30 Uhr:

Deep Dive: Einfach. Mehr Sicherheit mit der SentinelOne Singularity Platform

Vielen Dank!

SentinelOne®

Additional Slides

Icons

Einfach. Mehr Sicherheit.

SentinelOne®

Vielen Dank!