cybereason

THIS IS XDR

bwsecurity day 2022

09. März 2022

Alexandre Curty - Sales Director

About Cybereason

Founded in 2012

Headquartered in Boston

Privately held company

1300+ employees across the globe

75+ employees in the DACH region

$713.6M Total Funding

Gartner

Cybereason Named a **Visionary** in Gartner's 2021 EPP Magic Quadrant Report

FORRESTER®

Cybereason Named a Strong Performer With the **Highest Current Offering Score** in Forrester's 2020 EDR Wave

NSS LABS

Cybereason Received the **Highest Overall 'AA' Product Rating** in NSS Lab's 2020 Advanced Endpoint Protection Test

MITRE | ATT&CK™

Cybereason Leads the Pack in **Protection, Linux, and Actionable Coverage** in the 2021 MITRE ATT&CK Evaluation

This is for the Defenders:

VISION

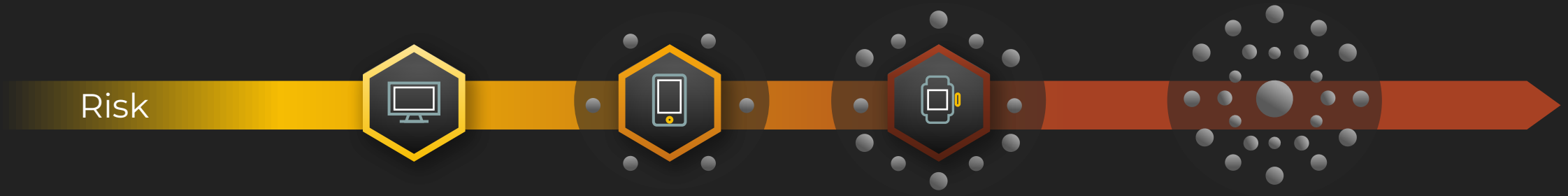
To protect people and information in the new and open connected world.

MISSION

To reverse the adversary advantage by empowering defenders with the ingenuity and technology to end cyber attacks.

We Meet This Challenge Together.

EVOLUTION OF THE ATTACK ENVIRONMENT



	2000	2007	2014	2021
Device	Desktop/Laptop	Mobile	IoT (Internet of Things)	IoE (Internet of Everything)
Applications	Client/Server	Web	Agile	Automation
Data	1 Exabyte	1.5 Zettabyte	12.5 Zettabyte	100 Zettabytes
Speed	2G	3G	4G	5G
Social Media	Instant Messenger	Facebook	Twitter	TikTok, Instagram
Perimeter	Controlled Access	Web Access	Hybrid Cloud	No Perimeter
Hackers	Script Kiddies	Criminal Ecosystem	Hacktivists	Nation-Affiliated Attackers, Ransomware Cartels
Attacks	Intrusive	Disruptive	Destructive	Cyber Armageddon

WE MUST EVOLVE TO ACHIEVE OUR MISSION

2000's

Reaction Centric

Perimeter

Static

Siloed

Legacy Vendors
Signature-based detection
for known threats

2010's

Alert Centric

Risk-based

Dynamic

Leveraged

Next-Gen AV/EDR
Evolved detection using
filtered endpoint data

2020's

Operation Centric

Dynamic Risk

AI/ML Driven

MalOps Focused

XDR Predictive detection across
all data, all endpoints and beyond.

Planetary Scale

Unrivaled ability to ingest and normalize petabytes of data from the entire IT environment.

Op-Centric

The whole picture and context of the malicious operation, not more alerts.

Predictive Response

We predict and automatically respond to end the attack

THIS IS XDR

MORE **SCALE**
10X

MORE **SPEED**
10X

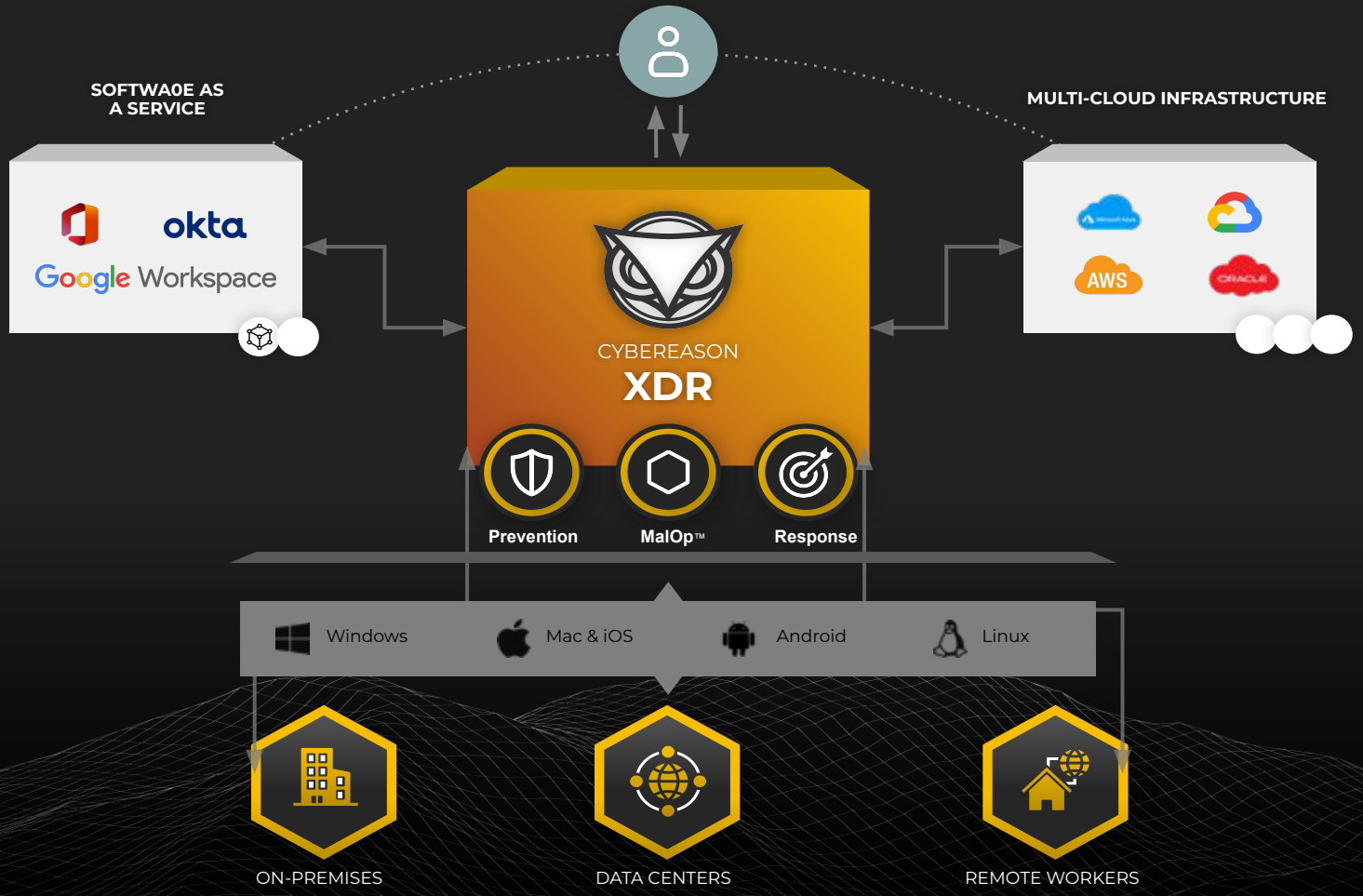
MORE **VALUE**
10X

XDR

Planetary-Scale eXtendability

Operation-Centric Detection

Predictive Response



Analyze

9.8PB

of threat intelligence weekly.

Cybereason

XDR

Planetary-Scale eXtendability

Operation-Centric Detection

Predictive Response

AI-Driven Protection To End Attacks Everywhere

Exponential Improvement Over Existing Solutions

Malicious Operation (MalOp) Engine For Unmatched Productivity

Dramatic Increase In Security Efficiency and Effectiveness

Alert Centric	
Days (Time to detect & respond)	
80-150 (Avg. # of security vendors for large enterprises)	
24 Days (Dwell time)	
10 Million (Events analyzed per day)	Alert Based (Requires analyst)

MalOp

Operation Centric	
Seconds (Time to detect & respond)	93% (Reduction in Detection Time)
308% (ROI)	75% (Reduction in Platform Mgmnt)
Hours (Dwell time)	1:200K (Analyst to Endpoints)
7 Trillion (Events analyzed per day)	Real Time (Automated Response)

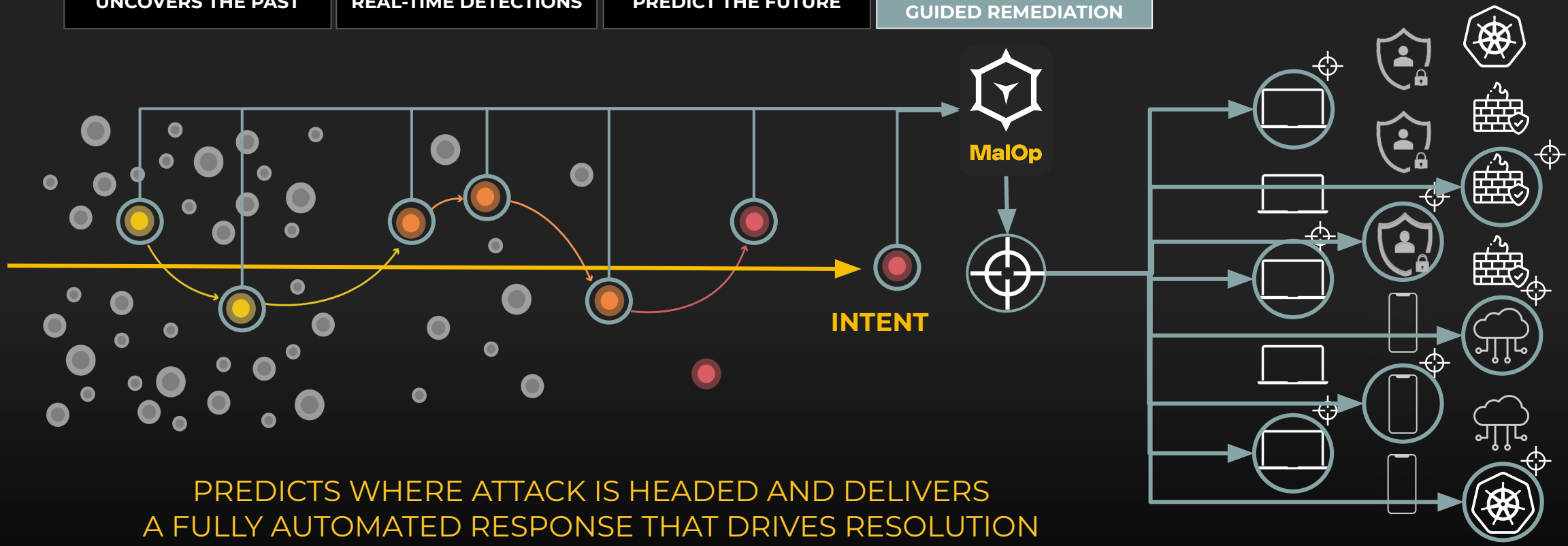
XDR

Planetary-Scale eXtendability

Operation-Centric Detection

Predictive Response

UNCOVERS THE PAST | REAL-TIME DETECTIONS | PREDICT THE FUTURE | ONE-CLICK / AUTOMATED GUIDED REMEDIATION

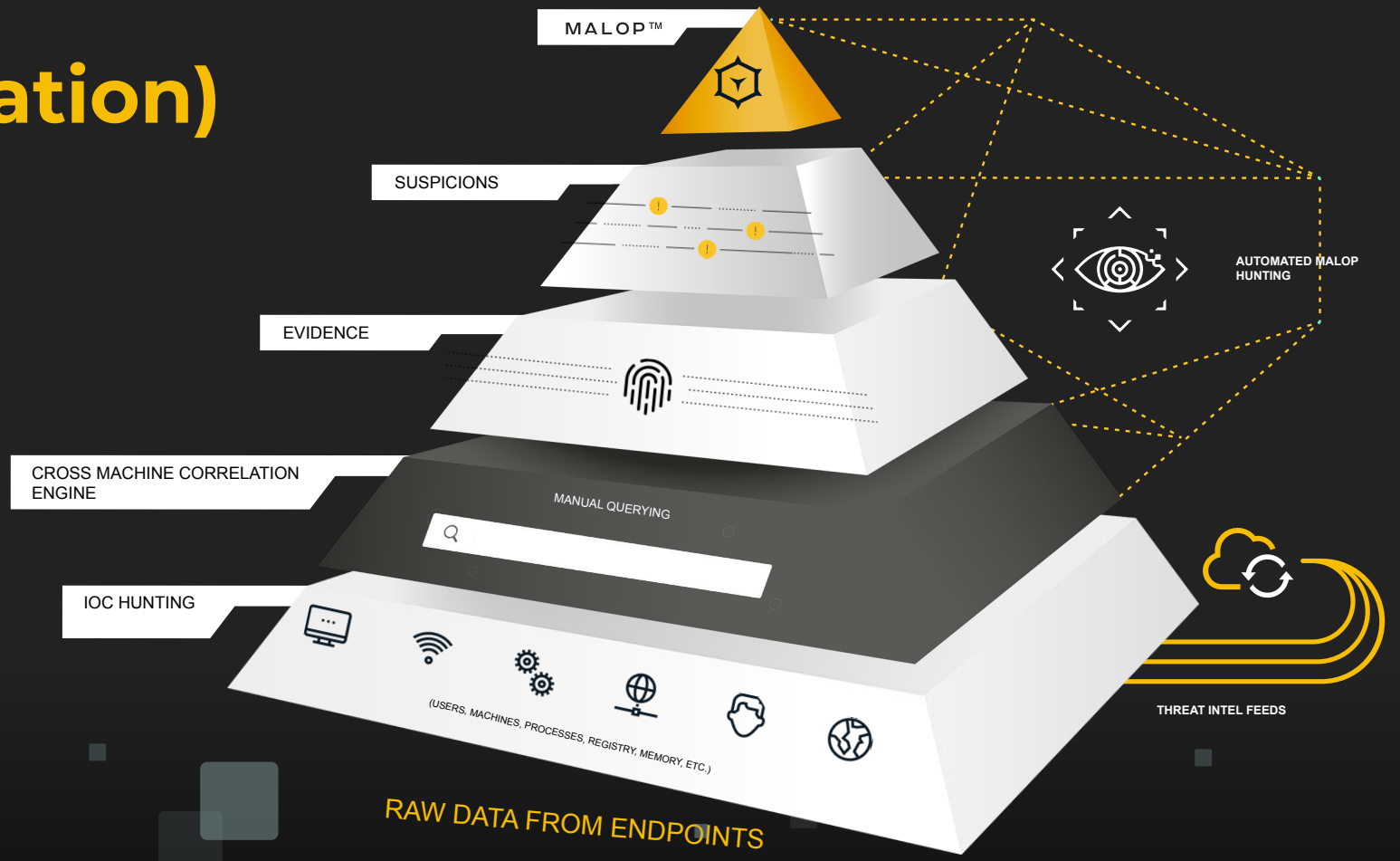


PREDICTS WHERE ATTACK IS HEADED AND DELIVERS
A FULLY AUTOMATED RESPONSE THAT DRIVES RESOLUTION

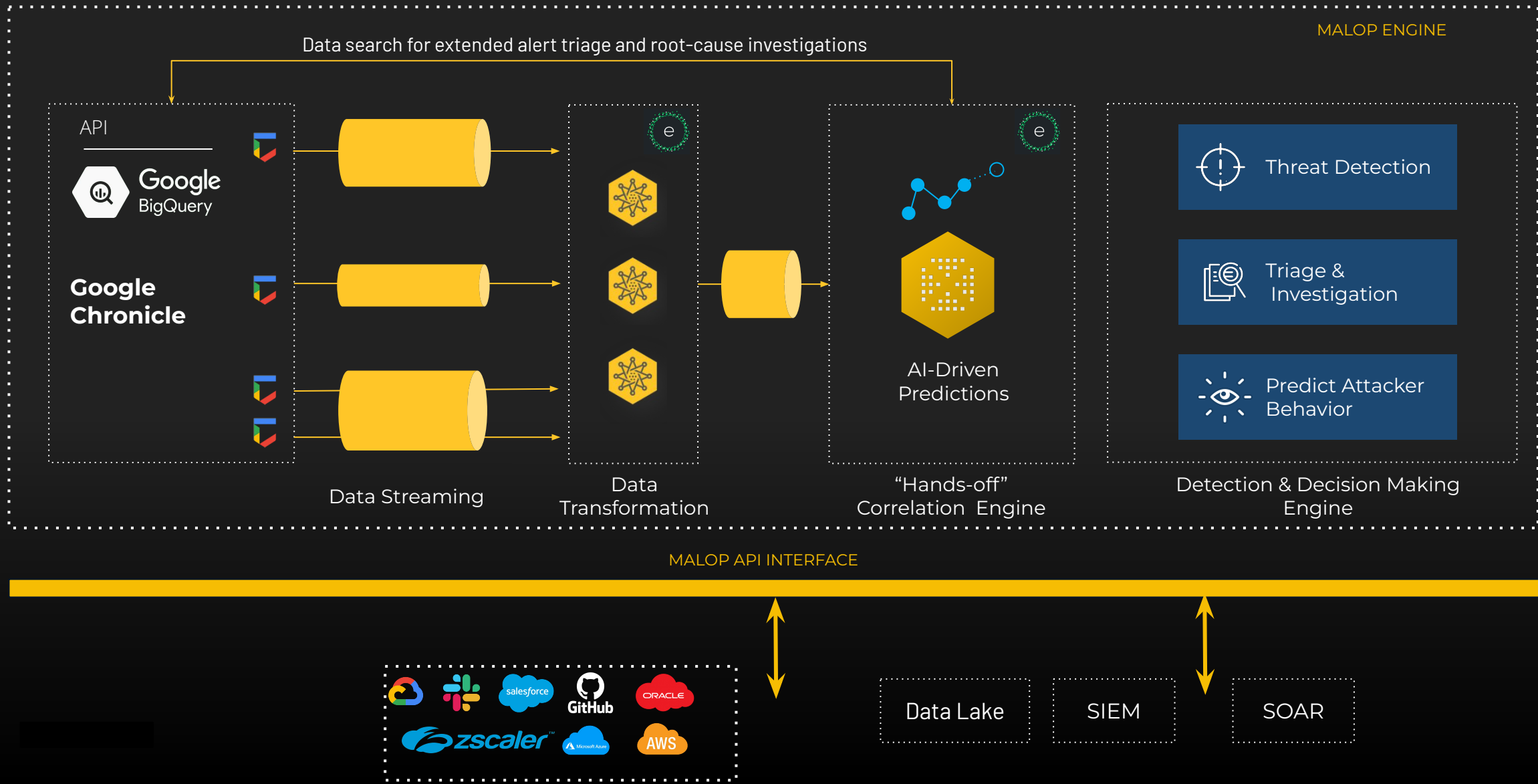
93% FASTER.

The MalOp™ (Malicious Operation)

Operation-Centric Security



Cybereason MalOp: Technical Architecture



Cybereason XDR Powered by Google Chronicle

Predict, understand and end attacks at planetary scale.

Powered by Google Cloud Security

EASY PETABYTE-SCALE ONBOARDING

CYBEREASON CONNECT

Endpoint

Windows · Apple · Linux · iOS · Android

Cloud

Microsoft Azure · Google Cloud · AWS Cloud · Oracle

Workspace & Identity

Slack · Salesforce · GitHub

Network

Cisco · F5 Networks · Google Cloud · Checkpoint · Amazon Web Services

PLANETARY-SCALE DATA MANAGEMENT

GOOGLE CHRONICLE

- Sub-Second Search at Petabyte Scale
- Google Threat Intelligence
- Cost Effective Data Retention

THREAT INVESTIGATION AND PREDICTION

MALOP ENGINE

ROOT CAUSE & EFFECT	VISUAL TIMELINE

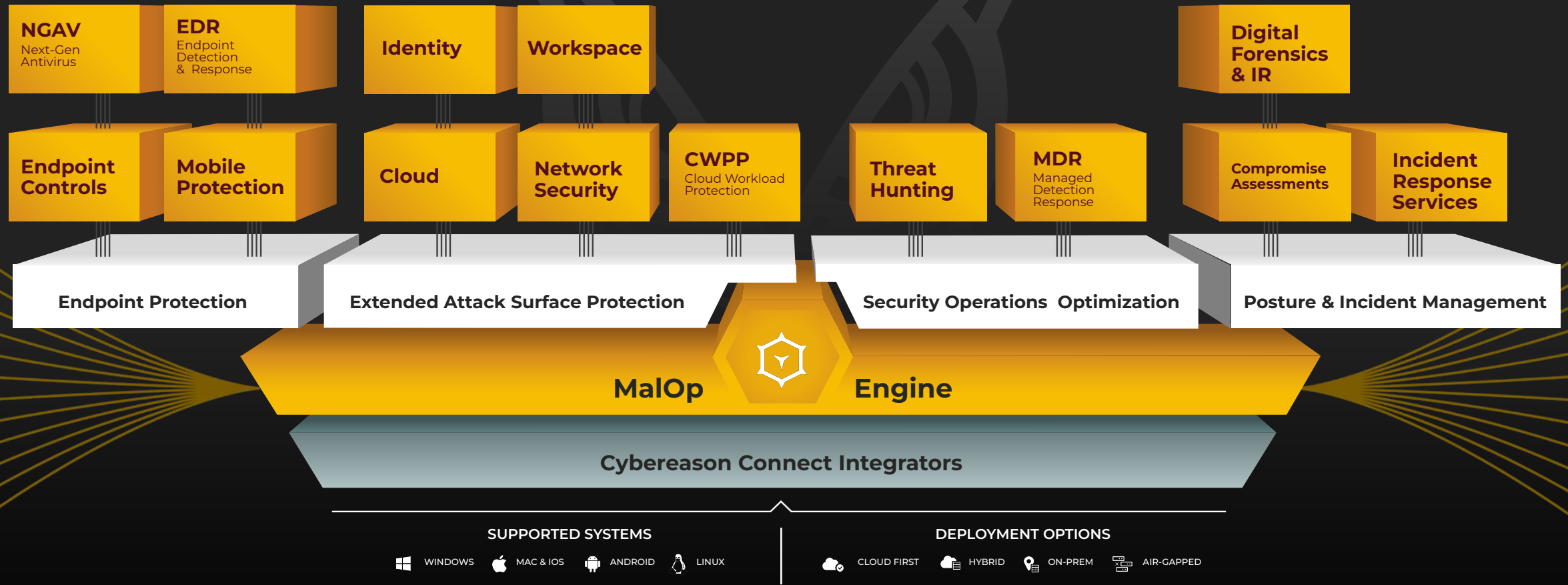
- AI-Powered Threat Detection
- Triage & Investigation
- Predict Attacker Behavior

INCIDENT RESPONSE

GUIDED RESPONSE

- Prevention
- Orchestration
- Autopilot Response
- Custom Detections

CYBEREASON XDR PLATFORM



SUPPORTED SYSTEMS

WINDOWS · MAC & IOS · ANDROID · LINUX

DEPLOYMENT OPTIONS

CLOUD FIRST · HYBRID · ON-PREM · AIR-GAPPED


cybereason
THANK
YOU.