



Egy félrekonfigurált felhő vállomásai –CTEM és Rapid7 InsightCloudSec

Foki Tamás
Senior System Engineer
tamas.foki@clico.hu



Agenda

- Attack Surface Management és CTEM dióhéjban
- Insight Platform
- InsightCloudSec
- Surface Command & Exposure Command

Attack Surface Management and CTEM

The Problem:

Only 17% of organizations can clearly identify and inventory a majority (95% or more) of their assets.”

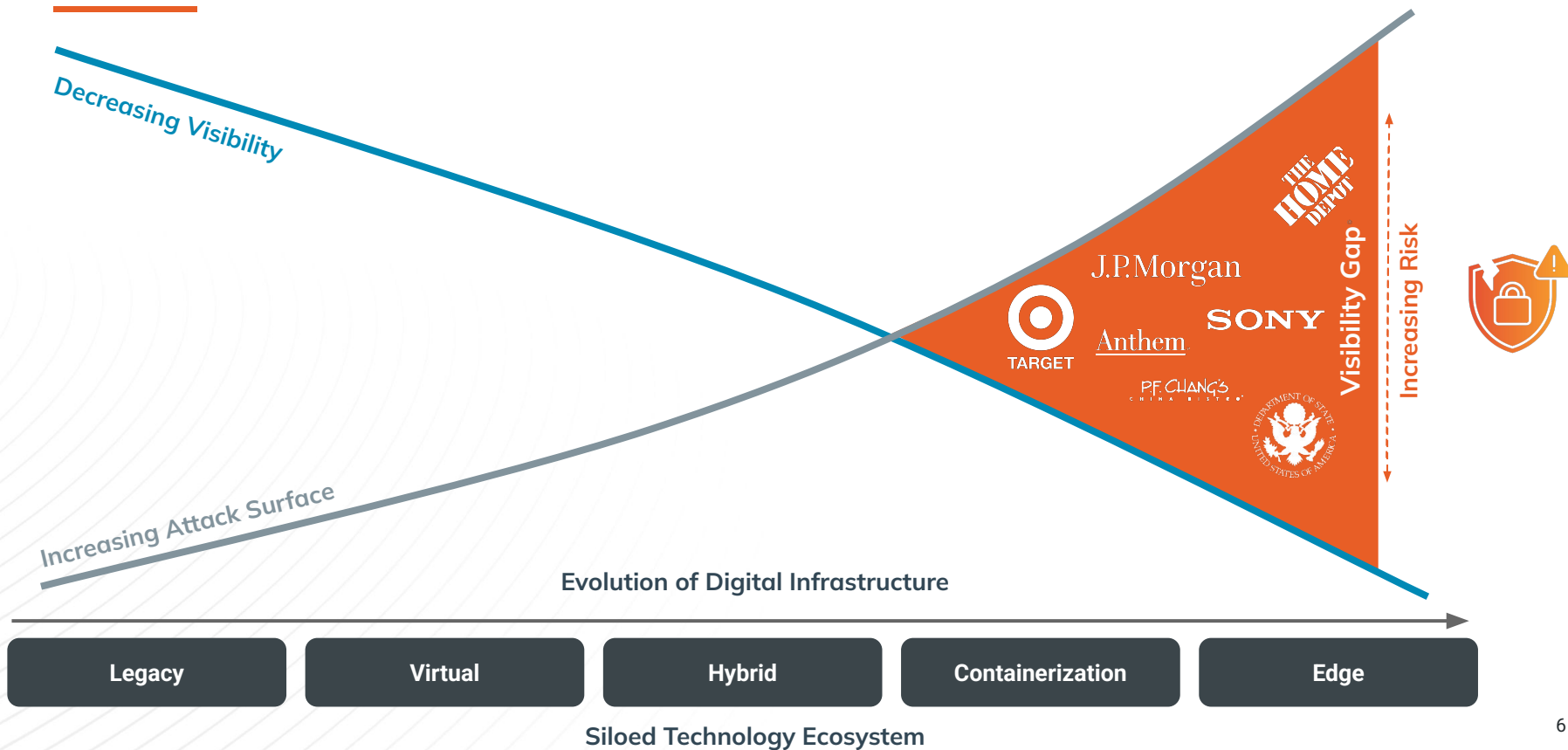
- Gartner's Cybersecurity Controls Assessment Benchmark 2023

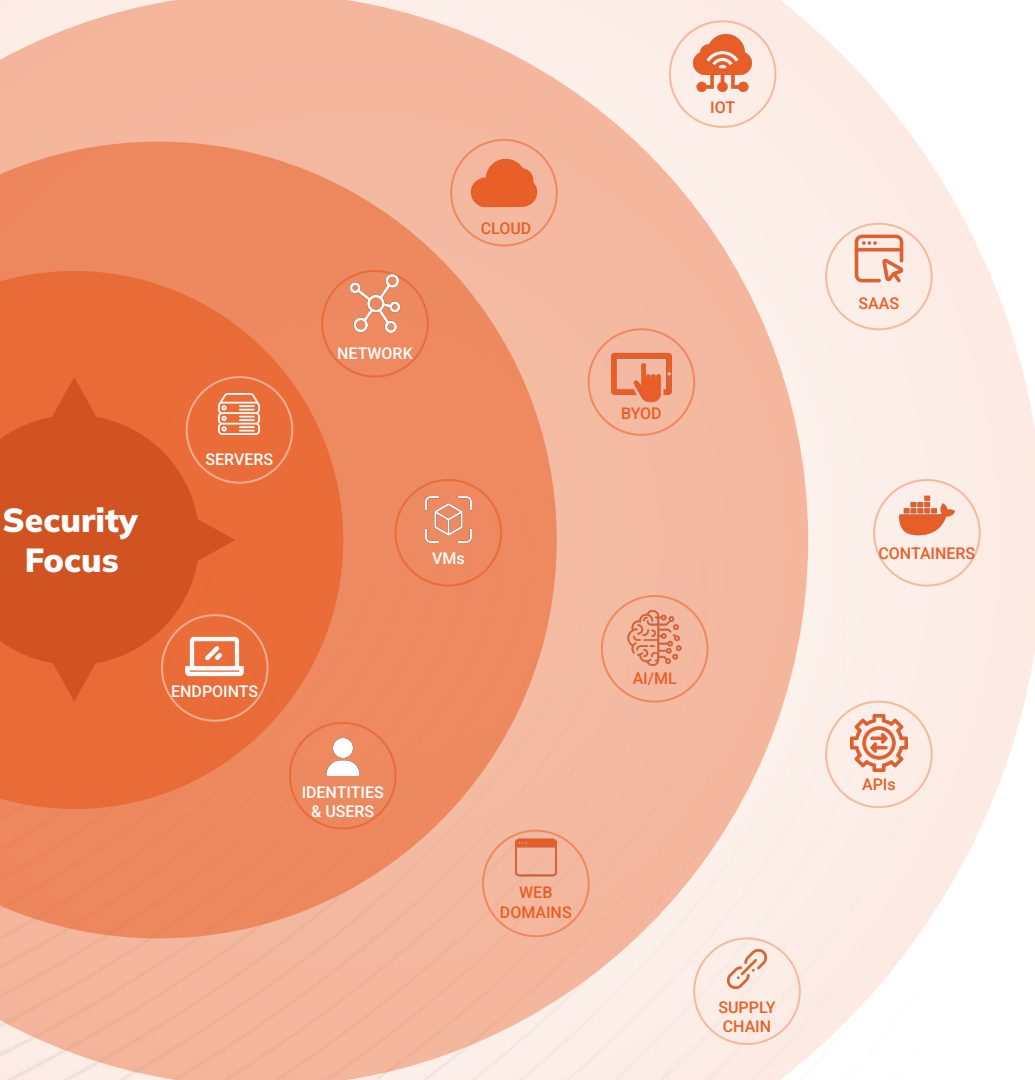
In Other Words:

More than 80% of organizations do not understand their attack surface.

- Gartner's Cybersecurity Controls Assessment Benchmark 2023

The Security Visibility Gap





Fragmented Attack Surface Challenges Productivity, Efficiency, Credibility

MORE DATA TO SYNTHESIZE

Challenged to keep up with volume of change to get a cohesive understanding of your total attack surface that you can trust

COMPLEX SYSTEMS INTEGRATIONS

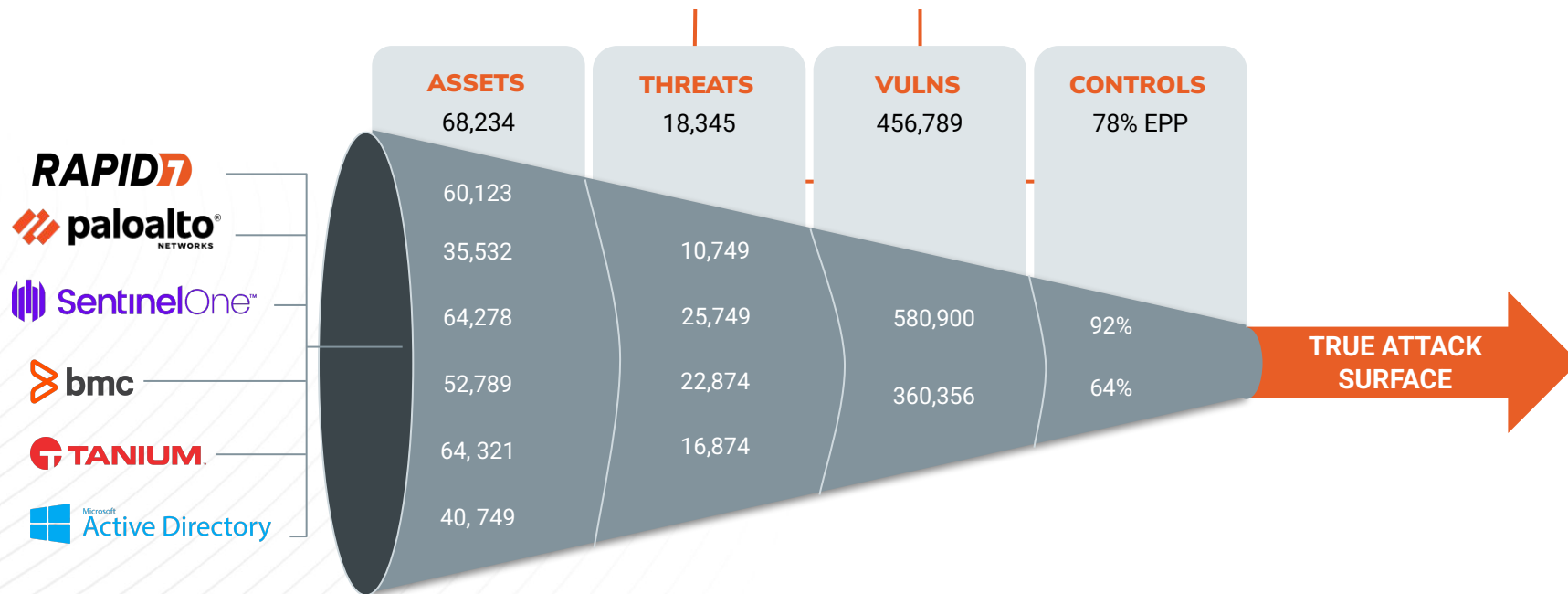
Caught in a web of disparate, conflicting sources to try to get effective context, make decisions, and know where to focus

INCREASING BUDGET DEMANDS

Escalating investments in technologies and training, as teams become more burnt out and struggle to point to ROI

Organization's Lack Accurate Visibility

Data Reconciliation



Insight Platform

Deep visibility, high-fidelity detections, and end-to-end automation in one unified platform.

- Lightweight single endpoint agent
- Cloud-based global deployment
- Security automation and customization
- Comprehensive API and 3rd-party integrations



Enable Better
Decisions

Contextualized data and analytics help you make smarter decisions with more speed.



Improve
Collaboration

Reduce complexity with integrated data that leverages existing security and IT systems across the platform.



Streamline
Everything

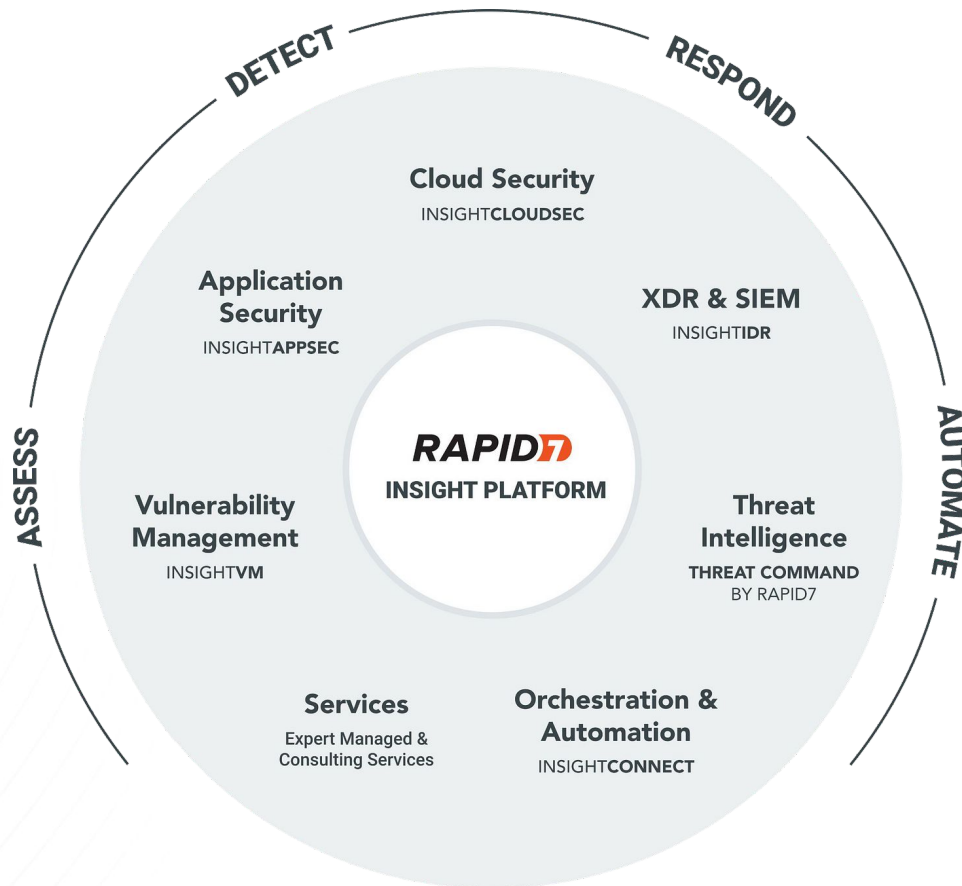
Simplify time-intensive, highly manual tasks with comprehensive automation and centralized controls.



Start Anywhere,
Scale Anytime

Expand your security program, and extend your team and capabilities as your business evolves.

Rapid7 Insight Platform



Cloud Adoption Is Disrupting Security Programs



CLOUD SECURITY

InsightCloudSec

Continuous security and compliance for cloud environments.

USE CASES

- Cloud inventory and asset management
- Misconfiguration and data breach prevention
- Full CI/CD lifecycle security
- Governance, risk management, and compliance



Full Coverage and Unified Visibility

Get a unified inventory to track risk across even the most complex cloud and container environments.

Real-time Risk Assessment

Dynamically gather data on configuration changes for up-to-the-minute cloud risk assessment.

Best-in-Class Automation

Reduce dwell time and manual effort with automated notification and remediation workflows.

Adaptability and Extensibility

Operationalize cloud security through enterprise-grade flexibility and extensibility.

CAPABILITIES



Cloud Security
Posture Management


Kubernetes
Security

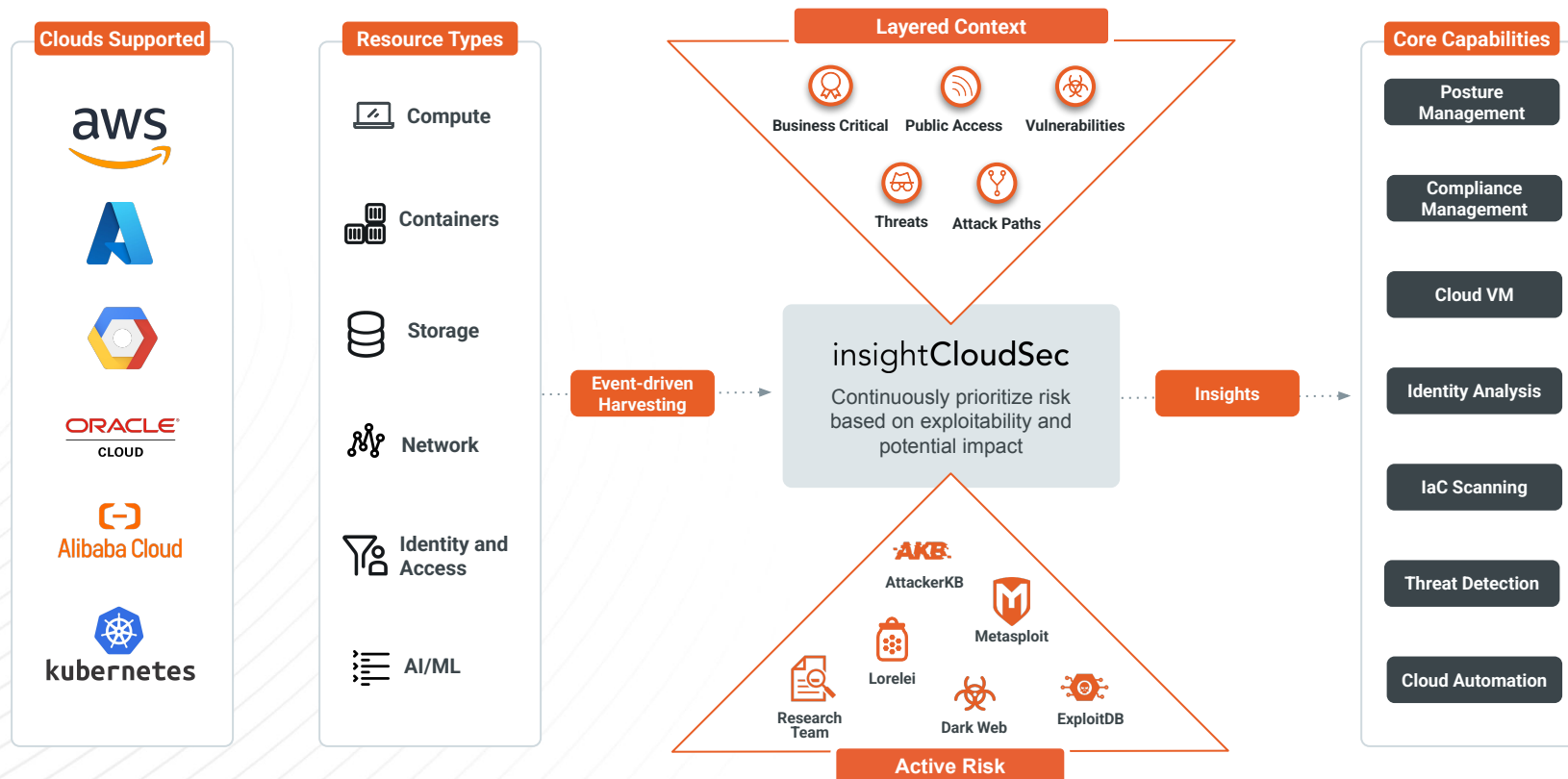

Cloud Workload
Protection


Infrastructure-as-Code
Analysis

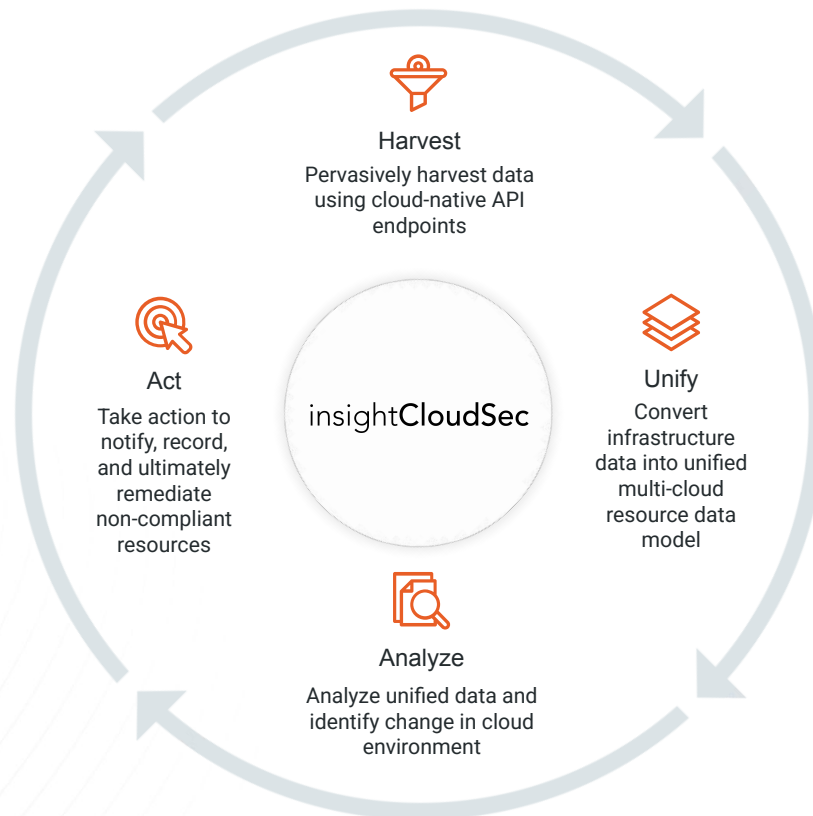

Cloud Identity and
Access Management


Customizable
Reporting

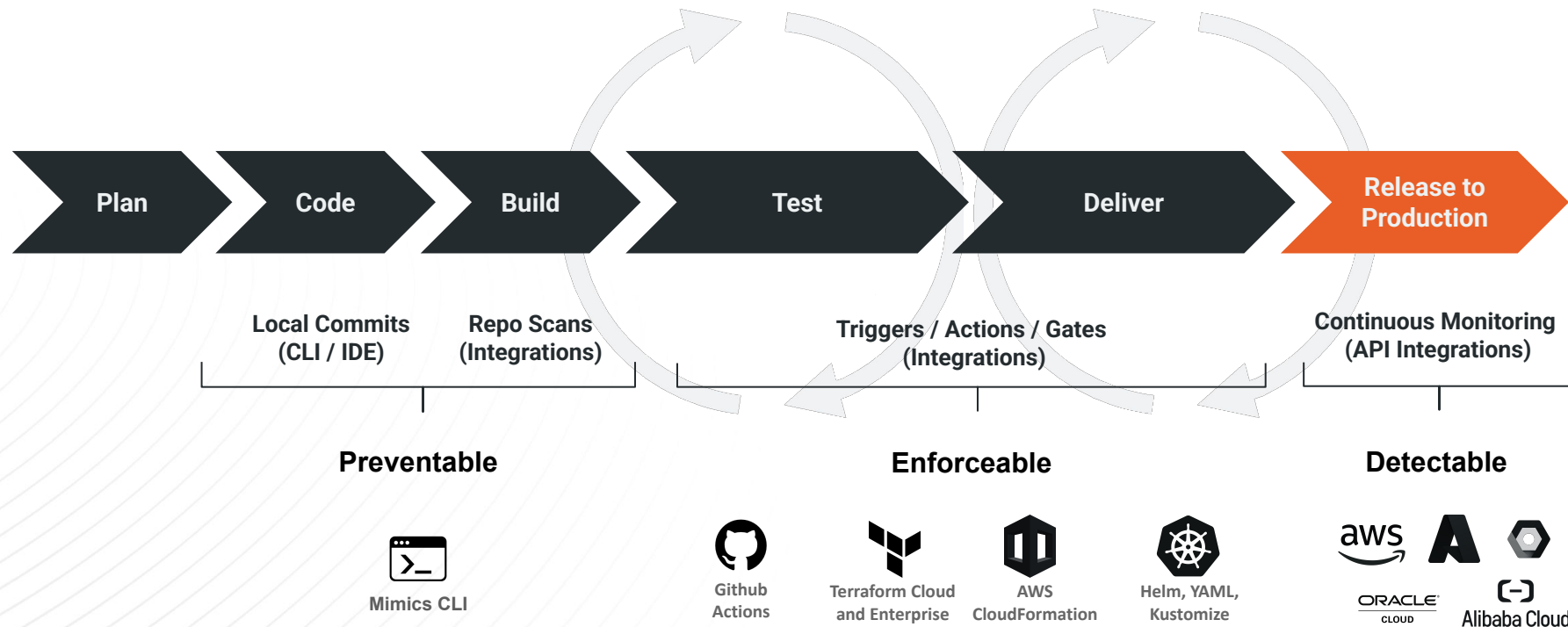
Extensive Multi-Cloud Breadth and Depth



How It Works



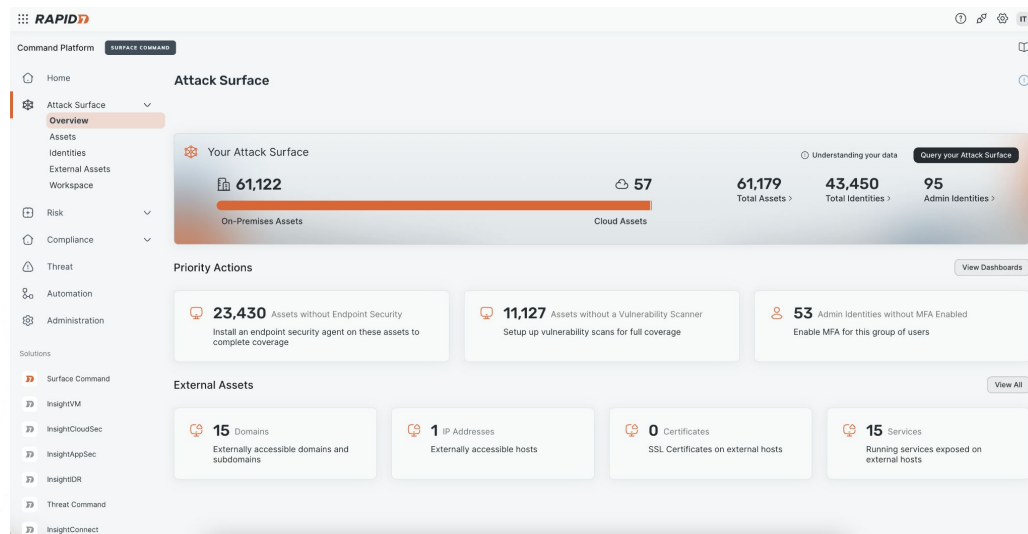
Stop issues before they're created with **IaC Scanning**



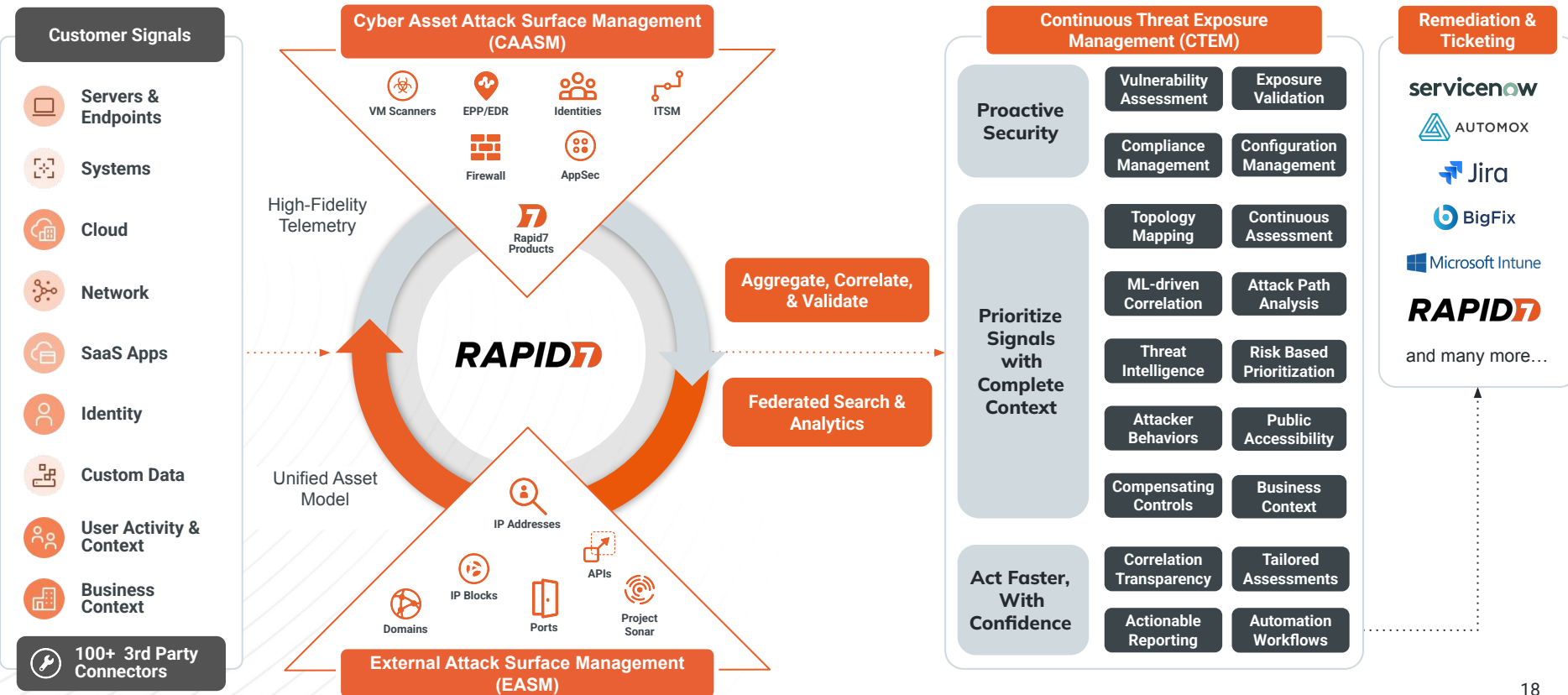
RAPID7

Surface Command

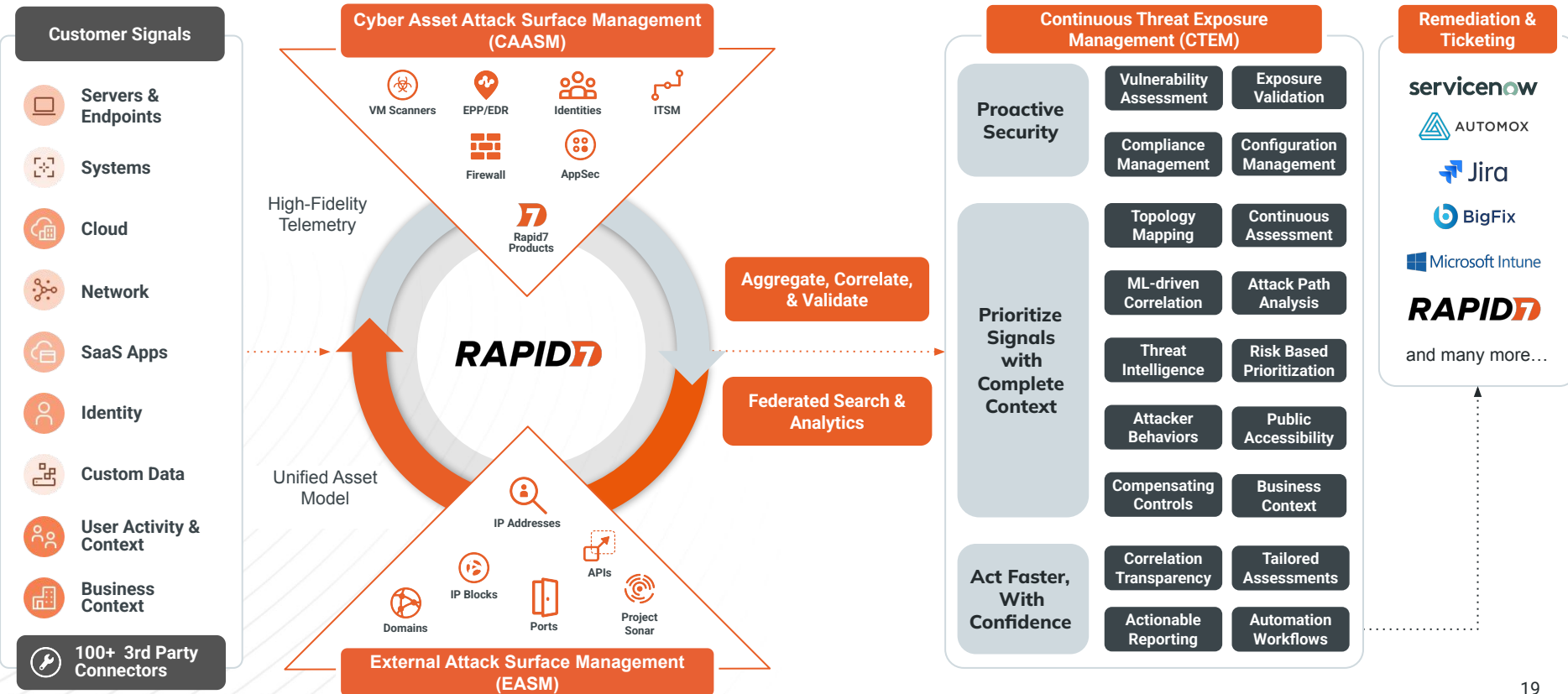
Visualize Your Attack Surface from Inside and Out with Surface Command







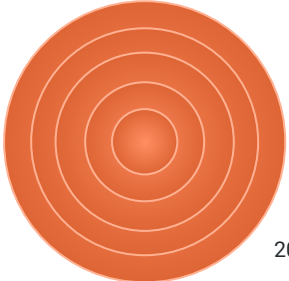
Rapid7 Attack Surface Management



Rapid7 Surface Command - Exposure Command



Attack Surface & Adjacent Tooling Comparison

Category	Asset Inventory	EASM	CAASM	RBVM	Rapid7 Surface Command
Scope	<ul style="list-style-type: none"> Limited to data from <i>vendor's</i> agent or vulnerability scanner Lacking larger ecosystem context and telemetry "Free" offerings focuses only on vendor's native data 	<ul style="list-style-type: none"> Limited to external assets - important, but represents only a small percentage of an organization's overall attack surface 	<ul style="list-style-type: none"> Primarily focused on internal assets, identities, and compensating controls Missing telemetry from threats, vulns & exposures Lacking native EASM, requires a separate solution 	<ul style="list-style-type: none"> Limited to data from vulnerability scanners & CSPM Context comes from vulnerabilities, exposures, and some business tools - missing the larger ecosystem data to be more actionable and complete. 	<ul style="list-style-type: none"> Comprehensive visibility across ecosystem to deliver most complete view of the attack surface Native telemetry support, but also vendor agnostic Context from vulnerabilities, exposures, business applications, assets, and threat data
Environment Visibility (illustrative)					



Command Your Attack Surface

Global Managed Services

Exposure Management

VULNERABILITY
CNAPP

DAST
VALIDATION

Detection & Response

MXDR
DFIR

NEXT-GEN SIEM
THREAT INTEL



Attack Surface Management

ENDPOINT TO CLOUD VISIBILITY AND MONITORING

Rapid7 AI Engine

CONNECT

CORRELATE

CONTEXTUALIZE

PRIORITIZE

RESPOND



RAPID7
CommandPlatform

R7 NATIVE DATA COLLECTION



R7 Labs



External



Scans



Agent



Network



APIs



Collectors



Applications



Cloud



Identity



Containers



SaaS



IaC



Supply Chain



KÖSZÖNÖM

Foki Tamás
Senior System Engineer

rapid7@clico.hu

tamas.foki@clico.hu