Fedd fel kitettséged a Rapid7-tel:

ASM és CTEM új megközelítésben

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

Attack Surface Management and CTEM

More innovation.
Increasingly complex attack surface.

17% Of organizations can clearly identify and inventory a majority (95%+) of their assets. [1]

40% Of SecOps leaders think AI will have the most impact on security in the next 12 to 24 months. [2]

43 Average number of security tools, with 69% of leaders noting a significant increase in the last few years. [3]

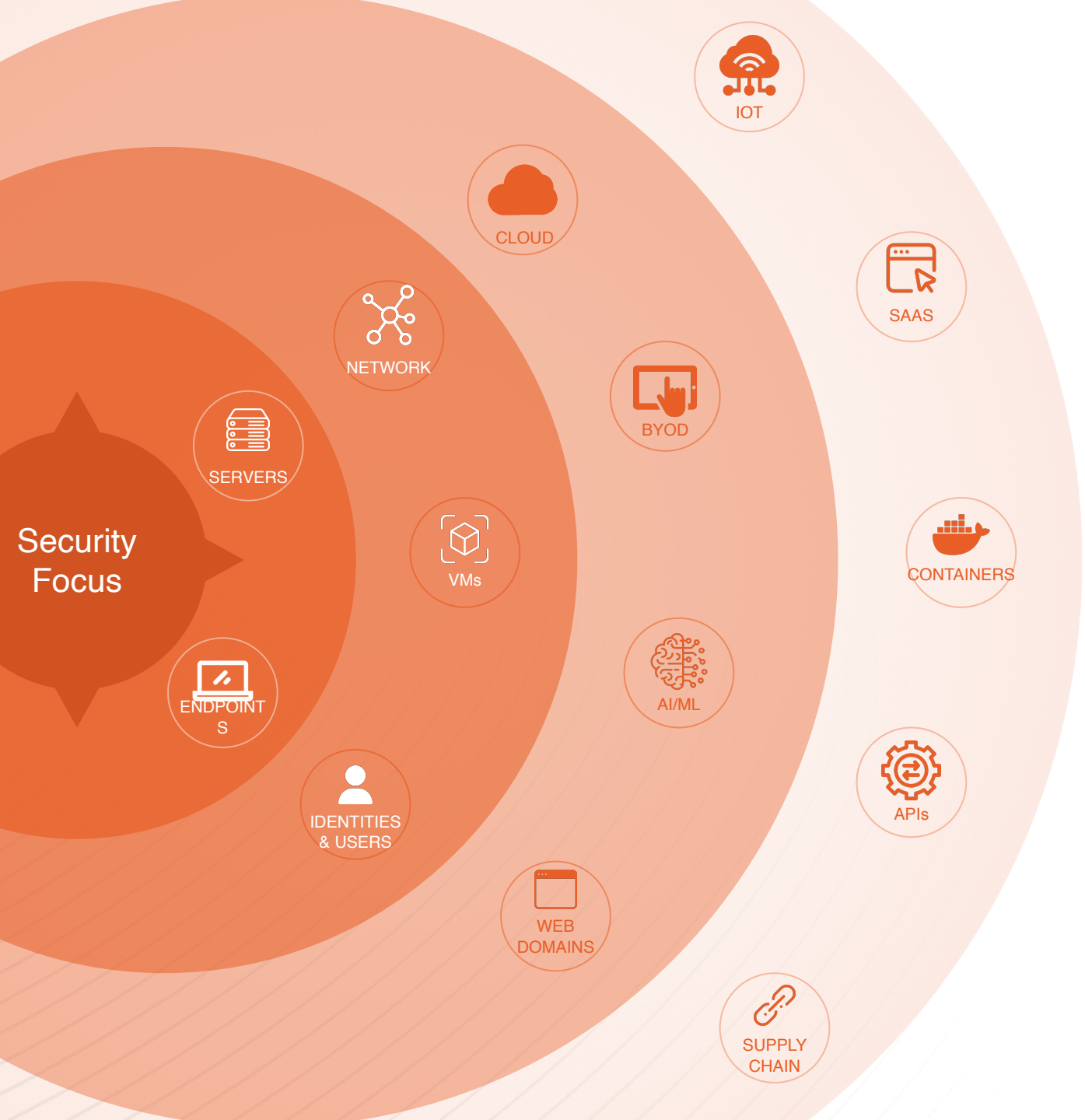
80% Of organizations attest that they do not fully understand their attack surface. [1]

Strategic Goals

- Enhance customer experiences
- Increase cloud adoption
- Fuel automation with AI
- Eliminate operational silos

Common Situation / Barriers

- Multi-cloud, hybrid stack
- Distributed workforce
- Constant regulations and audits
- Growing attack complexity



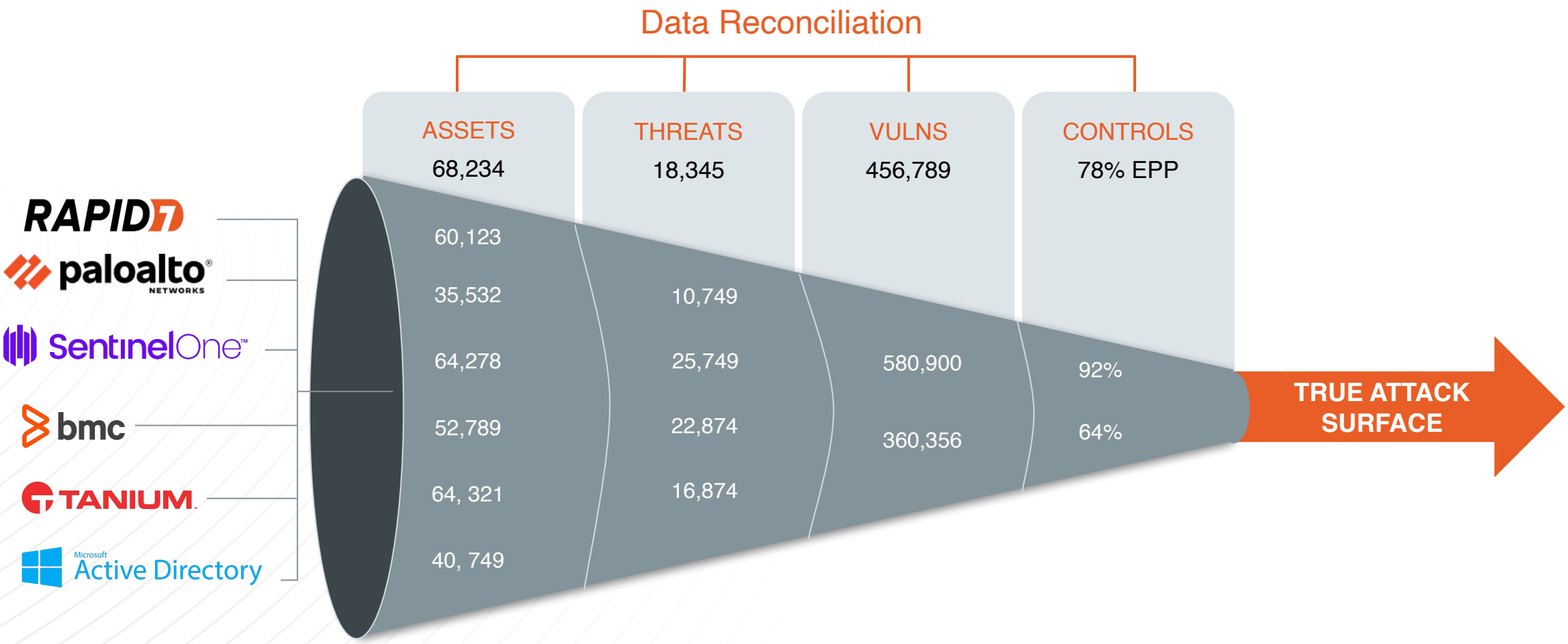
Fragmented Attack Surface Challenges Productivity, Efficiency, Credibility

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

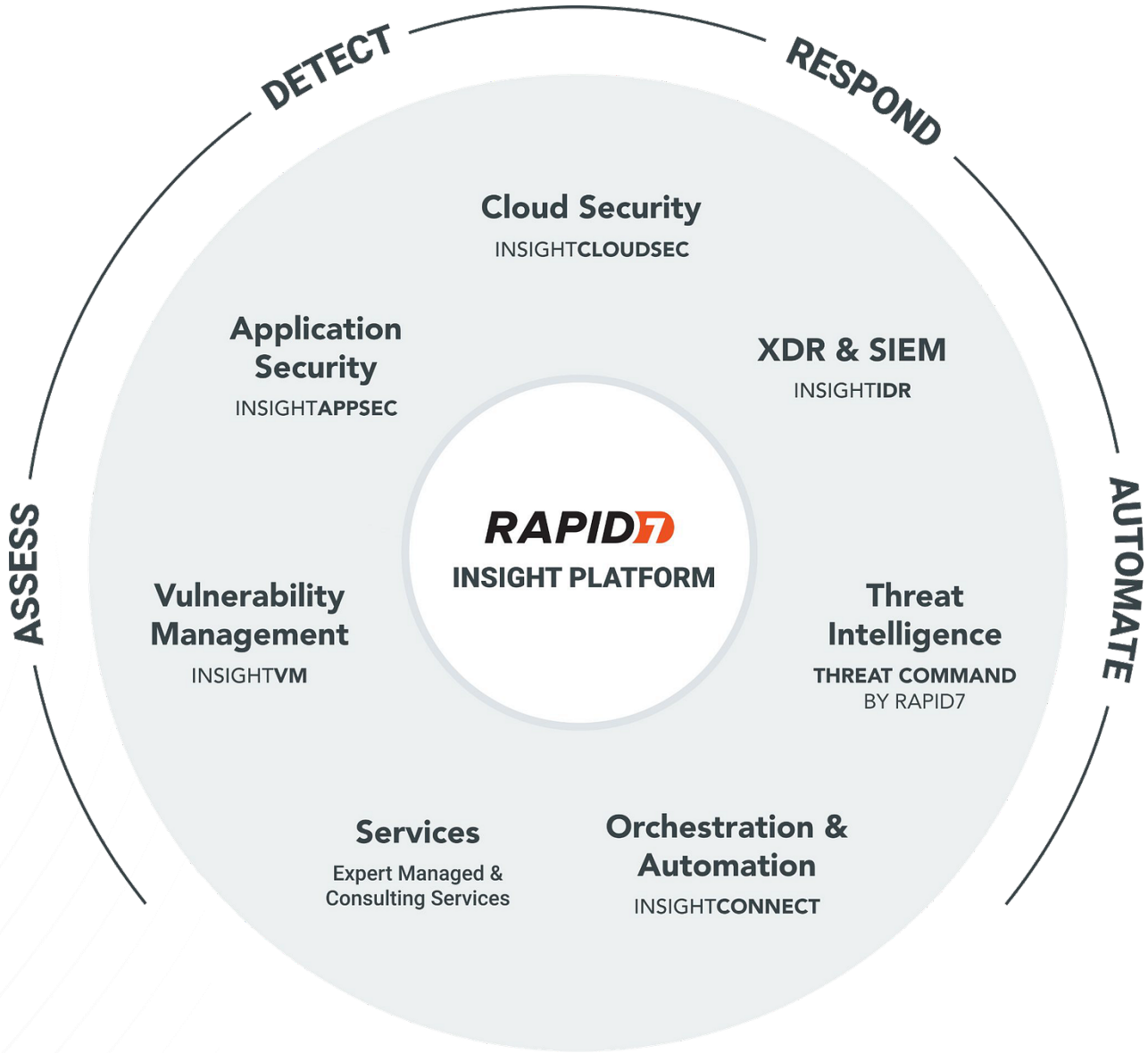
COMPLEX SYSTEMS INTEGRATIONS
Caught in a web of disparate, conflicting sources to try to get effective context, make decisions, and know where to focus

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

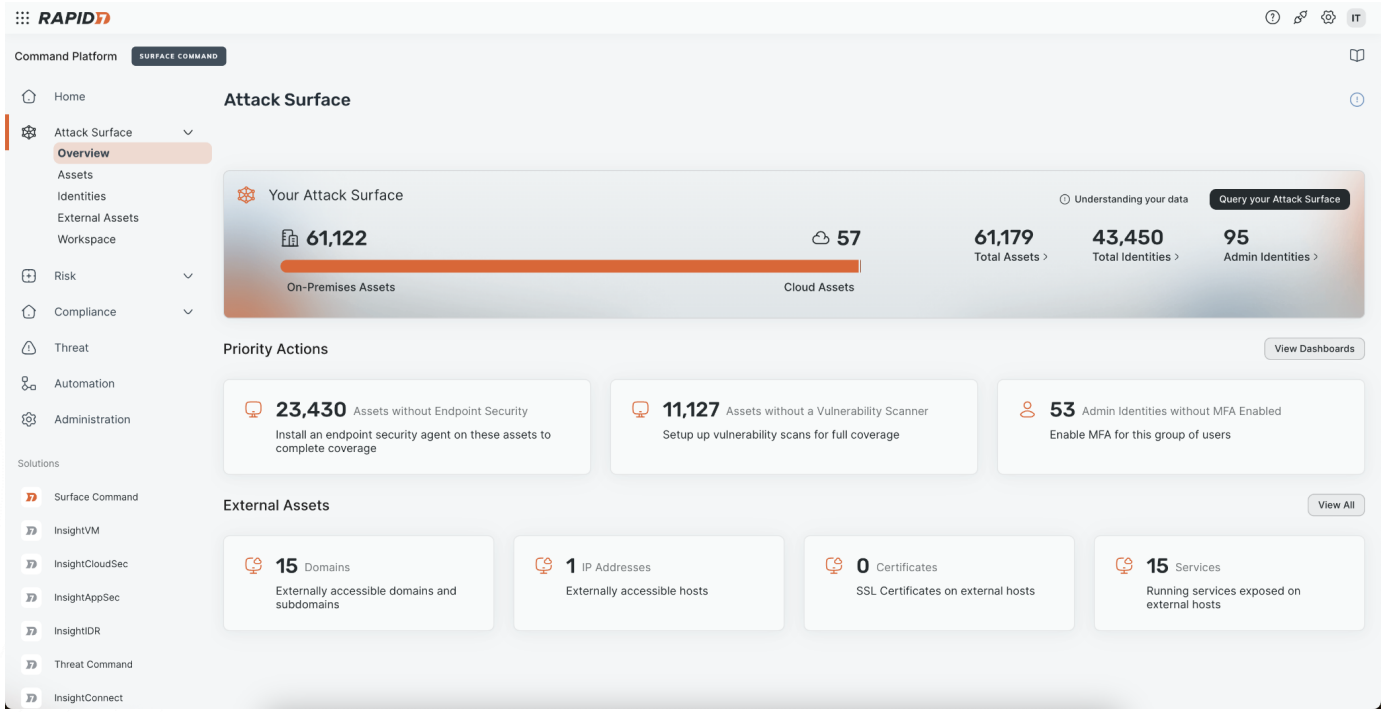


Rapid7 Insight Platform



Exposure Command and Surface Command

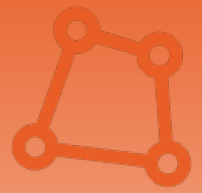
Visualize Your Attack Surface from Inside and Out with Surface Command



SURFACE COMMAND

Eliminate Exposures. Everywhere.

Confidently Prioritize Exposures From Endpoint to Cloud



Synthesize your entire attack surface

Gain an accurate, deep, and continuous view of your total attack surface, enabling you to stay ahead of known entities, shadow IT, and new resources.

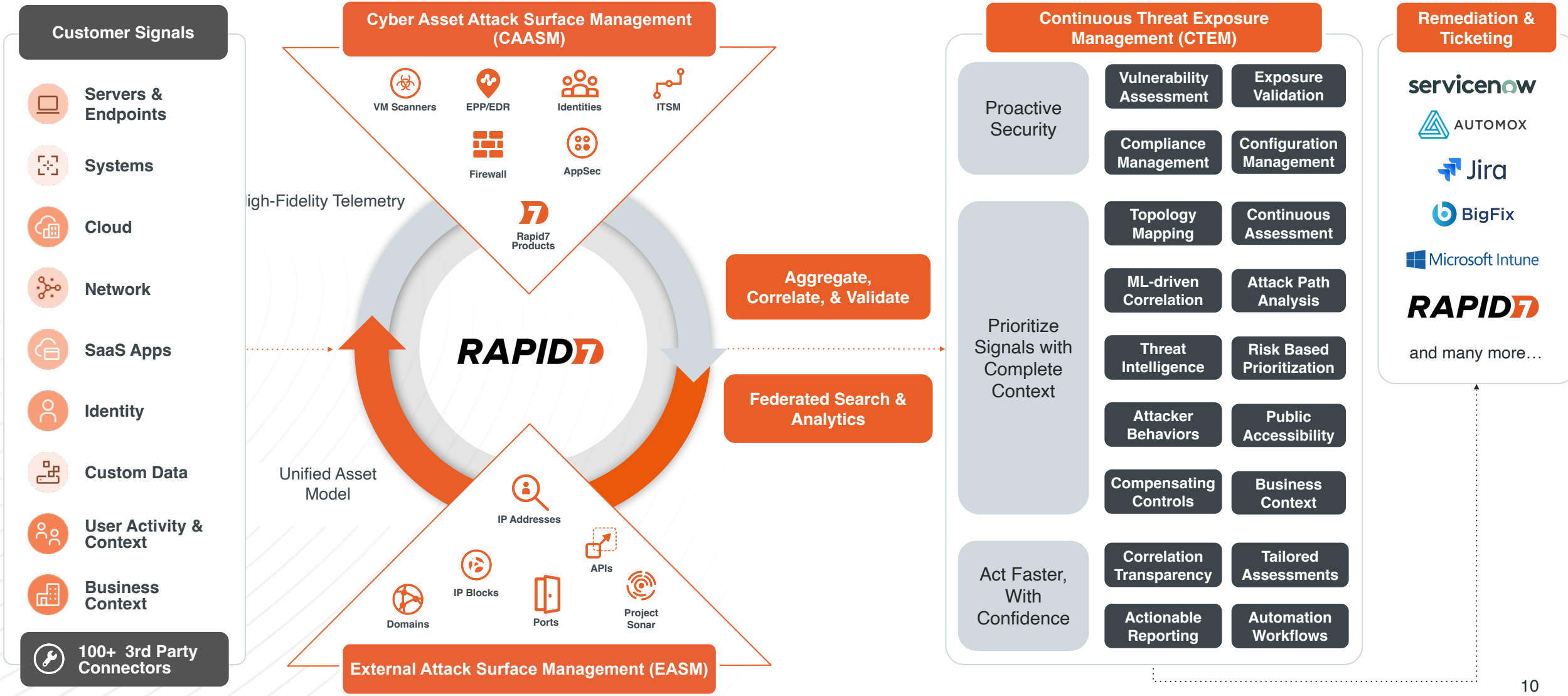
Uncover the riskiest, most imminent exposures

Instantly assess the true security of your technology stack to identify the assets and attack paths attackers are most likely to exploit.

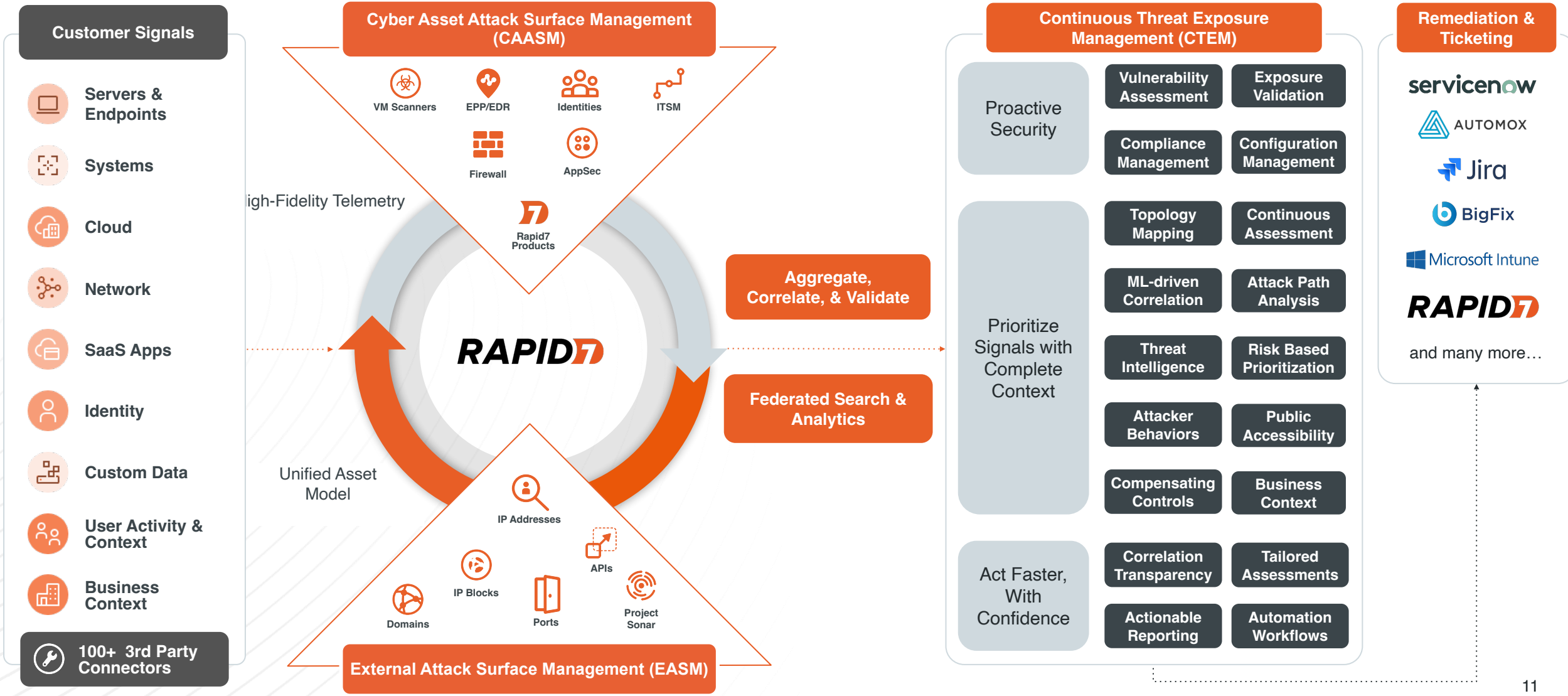
Empower teams to mitigate threats together

Accelerate remediation and track progress across teams with trusted guidance that integrates with existing tools and workflows.

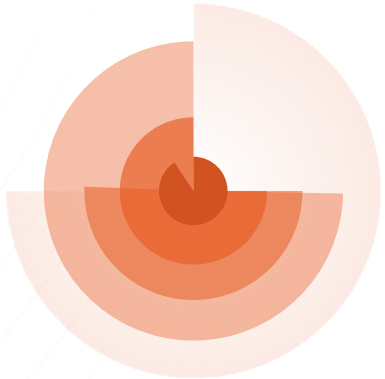
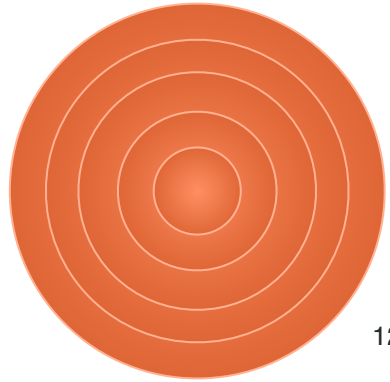
Rapid7 Attack Surface Management



Rapid7 Surface Command - Exposure Command

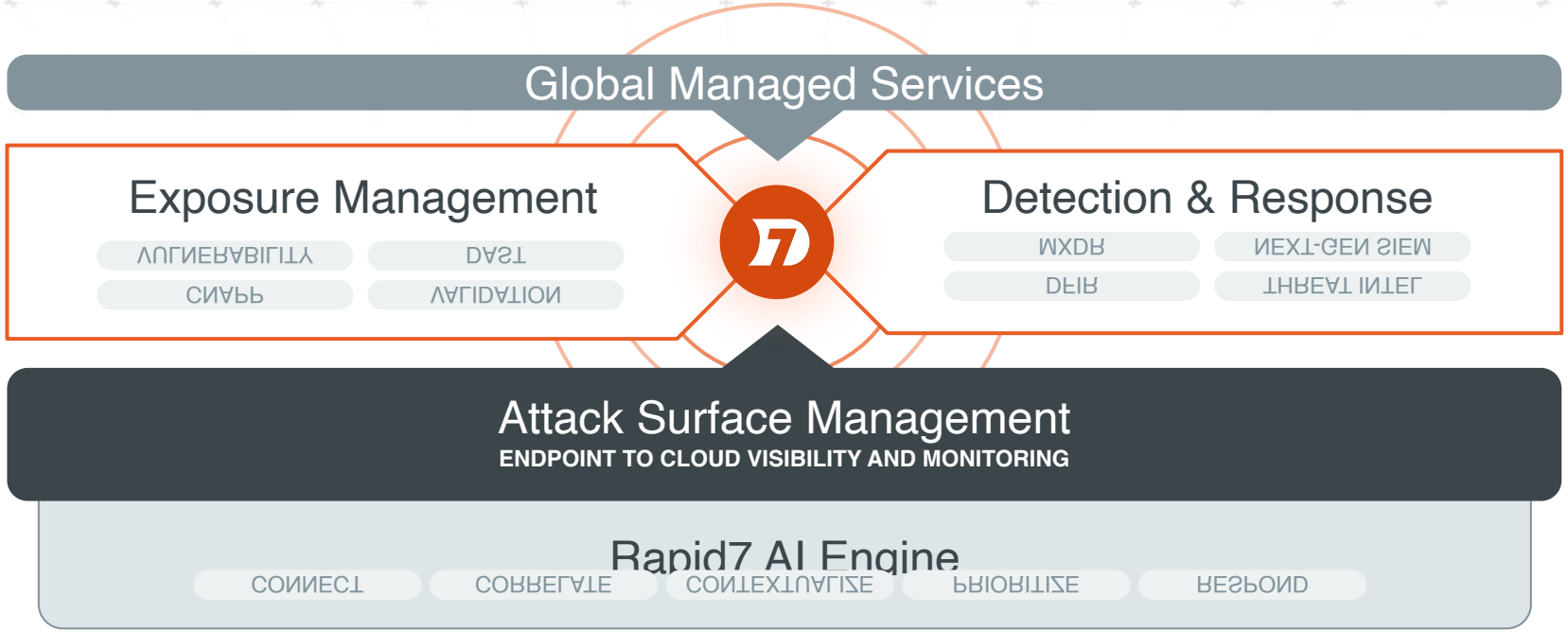


Attack Surface & Adjacent Tooling Comparison

Category	Asset Inventory	EASM	CAASM	RBVM	Rapid7 Surface Command
Scope	• Limited to data from vendor's agent or vulnerability scanner • Lacking larger ecosystem context and telemetry • "Free" offerings focuses only on vendor's native data	• Limited to external assets - important, but represents only a small percentage of an organization's overall attack surface	• Primarily focused on internal assets, identities, and compensating controls • Missing telemetry from threats, vulns & exposures • Lacking native EASM, requires a separate solution	• 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.	• 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)					

RAPID7

Command Your Attack Surface



RAPID7 CommandPlatform

R7 NATIVE DATA COLLECTION

YOUR CRITICAL SECURITY ECOSYSTEM

R7 Labs · External · Scans · Agent · Network · APIs · Collectors · Applications · Cloud · Identity · Containers · SaaS · IaC · Supply Chain

aws

TAKE COMMAND WITH

Comprehensive Attack Surface Management

Establish a Single Source of Truth

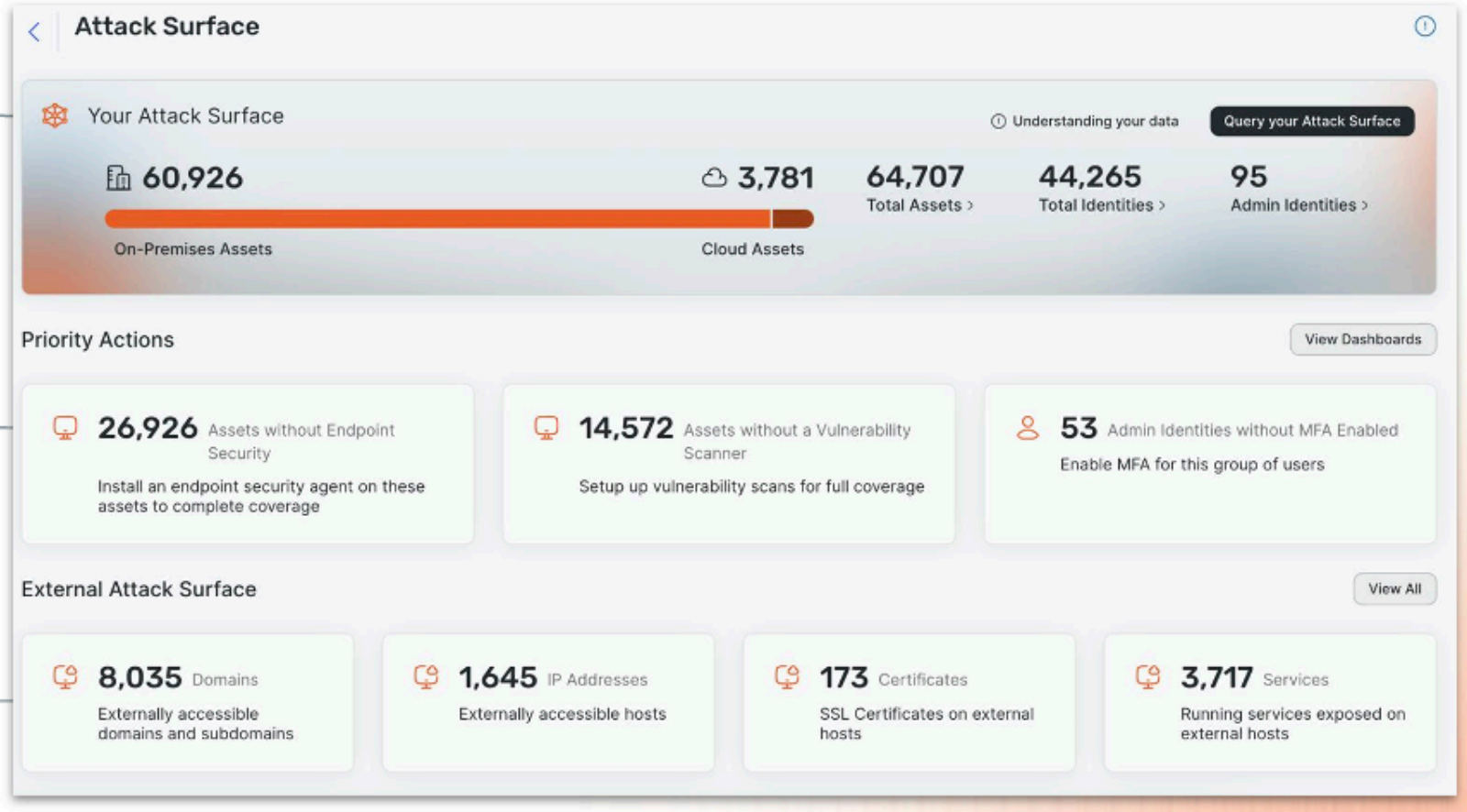
Consolidate asset inventory and identities across all internal tools to create a unified, reliable data source.

Focus on High-Impact Actions

Focus your team on the highest impact tasks by prioritizing signals with full context.

Enhance Attack Surface Visibility

Get a complete view of your external attack surface to proactively detect and mitigate risk before exploitation.



ONE CENTRALIZED HUB

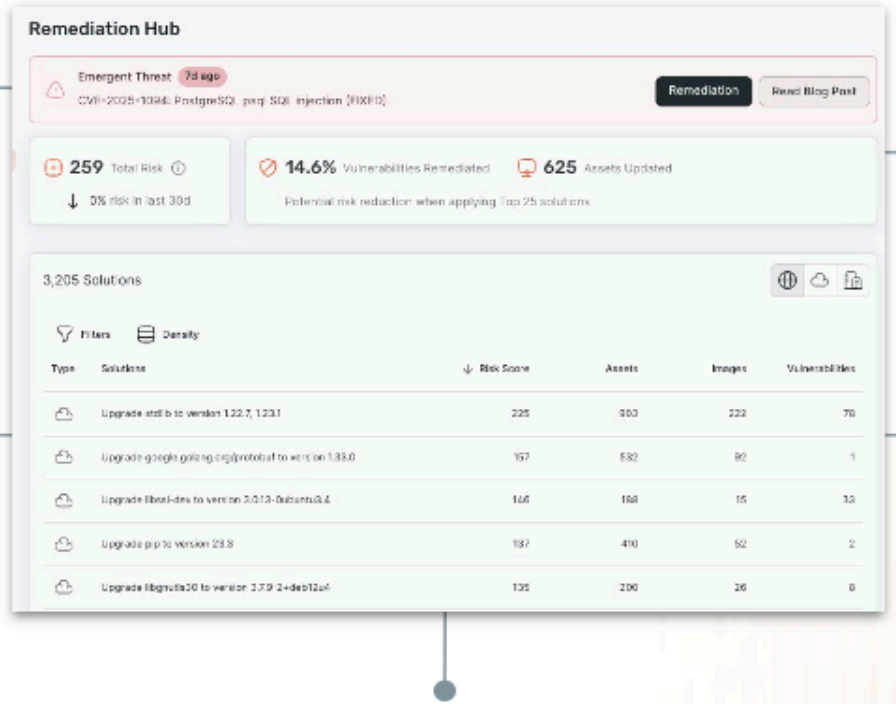
For Exposure Prioritization and Remediation

Solution-Oriented

Look for solutions, not problems
Understand the actions your team can take to make the biggest impact on organizational risk reduction.

Holistic Management

Break down silos between on-prem and cloud environments, taking a **comprehensive approach across your entire hybrid estate.**



Context-Enriched

Ensure remediators have access to **relevant business, environment and asset context** to make informed decisions and act fast.

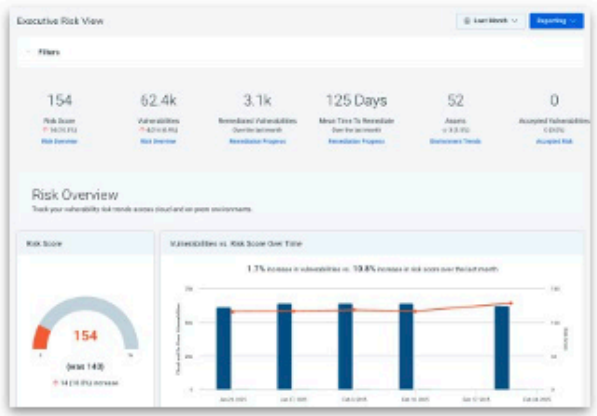
Deeply Integrated

Leverage 290+ out-of-the-box integrations with popular security and ITOps tools, allowing teams to weave exposure remediation into their existing workflows without adding friction.

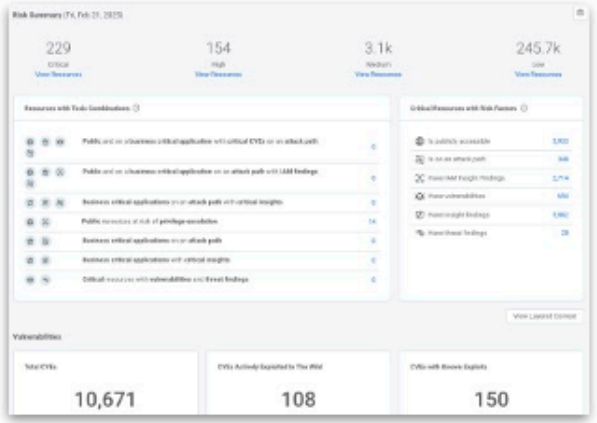
Act Once, Solve Many

Group remediation activity across your entire estate, allowing teams to work smarter, not harder, applying a solution globally ensuring risk is addressed in bulk

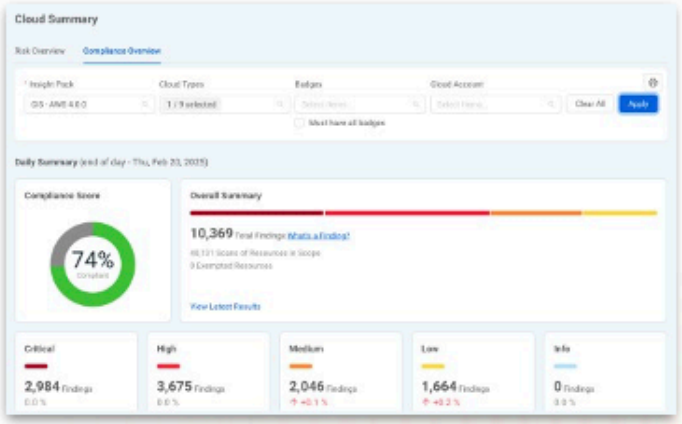
Flexible Reporting Options, Tailored to End-Users



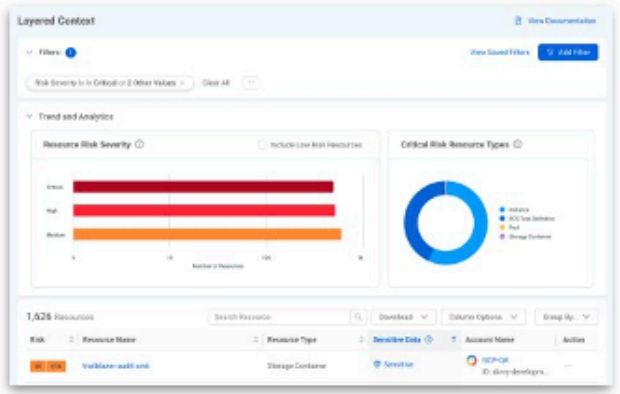
Executive Risk View



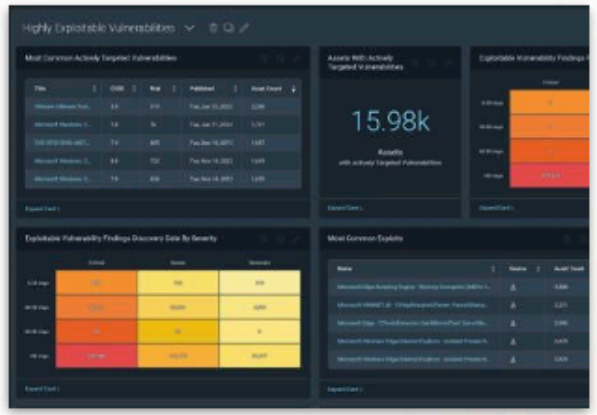
Cloud Risk Summary



Cloud Compliance Summary



Layered Context



Vulnerability Prioritization Dashboard

Actionable Remediation Planning

View all reports: https://docs.rapid7.com/services/mtc-welcome#report-you-can-access

NEW EXPOSURE COMMAND FAMILY

DEFAULT LAND MOTION

Exposure Command *Essentials*

Complete, single source of truth with actionable detection & validation

Risk-based exposure management

- Stay ahead of zero-days
- Eliminate blind spots
- Automate remediation

Vulnerability management

- Detect critical risk
- Harden on-prem devices
- Deliver defensible analysis

Exposure Command *Ultimate*

Full stack exposure management with proactive, end-to-end remediation

Cloud Security

- Close cloud breach patterns
- Detect threats at runtime
- Drive cloud compliance

Application Security

- Shift left
- Cover emerging risk
- Protect modern apps

Optional Add-ons:

- Intelligence Hub
- Active Patching
- Controls Monitoring
- DSPM

A more detailed look is available here.

Exposure**Command**

Complete Attack Surface Management

Complete attack surface visibility from insight and out - powered by **Surface Command**

Hybrid Vulnerability Management

Detect and prioritize vulnerabilities with purpose-built assessment from endpoint to cloud.

Cloud-Native Application Protection

Proactive risk and compliance management for modern cloud workloads

Continuous Application Security Testing

Automatically identify, triage, prioritize and remediate application risk

KÖSZÖNÖM

Foki Tamás
Senior System Engineer
rapid7@clico.hu
tamas.foki@clico.hu