RAPID7

23/04/26

EVOLUTION OF RAPID7 : FROM SCANNING TO COMPLETE RISK AND INCIDENT MANAGEMENT


RAPID7


nexpose
insightVM


insightAppSec


metasploit


insightIDR

The Modern Security Challenge:

Gaps That Attackers Exploit

Exploding Attack Surface

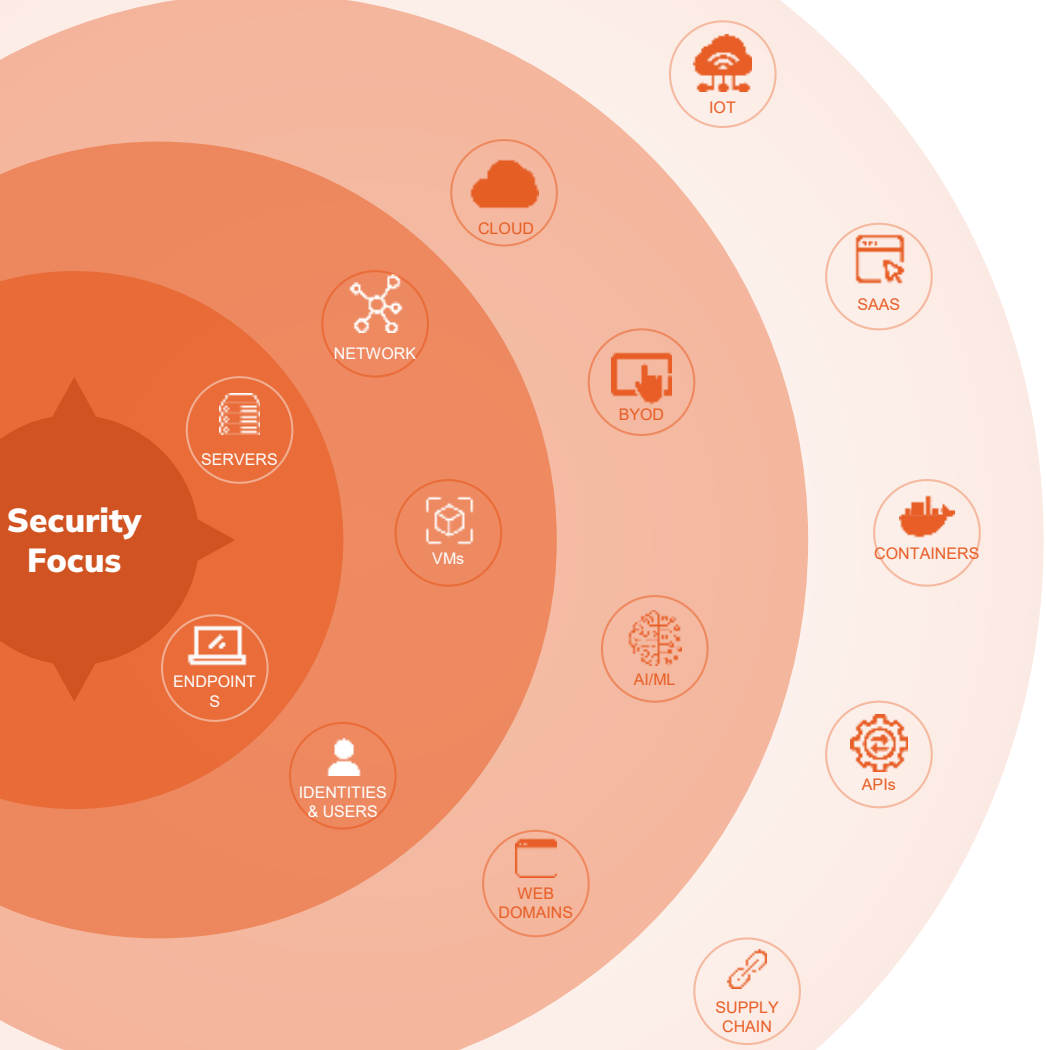
Organizations now manage endpoints, cloud, SaaS, shadow IT, and third-party connections creating blind spots attackers can easily target.

Inability to Scale SOC Outcomes

Security teams are strapped, and being asked to take on more. Manual processes can't keep pace with surging threat and alert volumes.

The SOC Context Problem

Traditional SIEMs and point products lack the context and visibility needed to keep up with today's pace and complexity, leaving dangerous gaps.



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

The Problem:

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

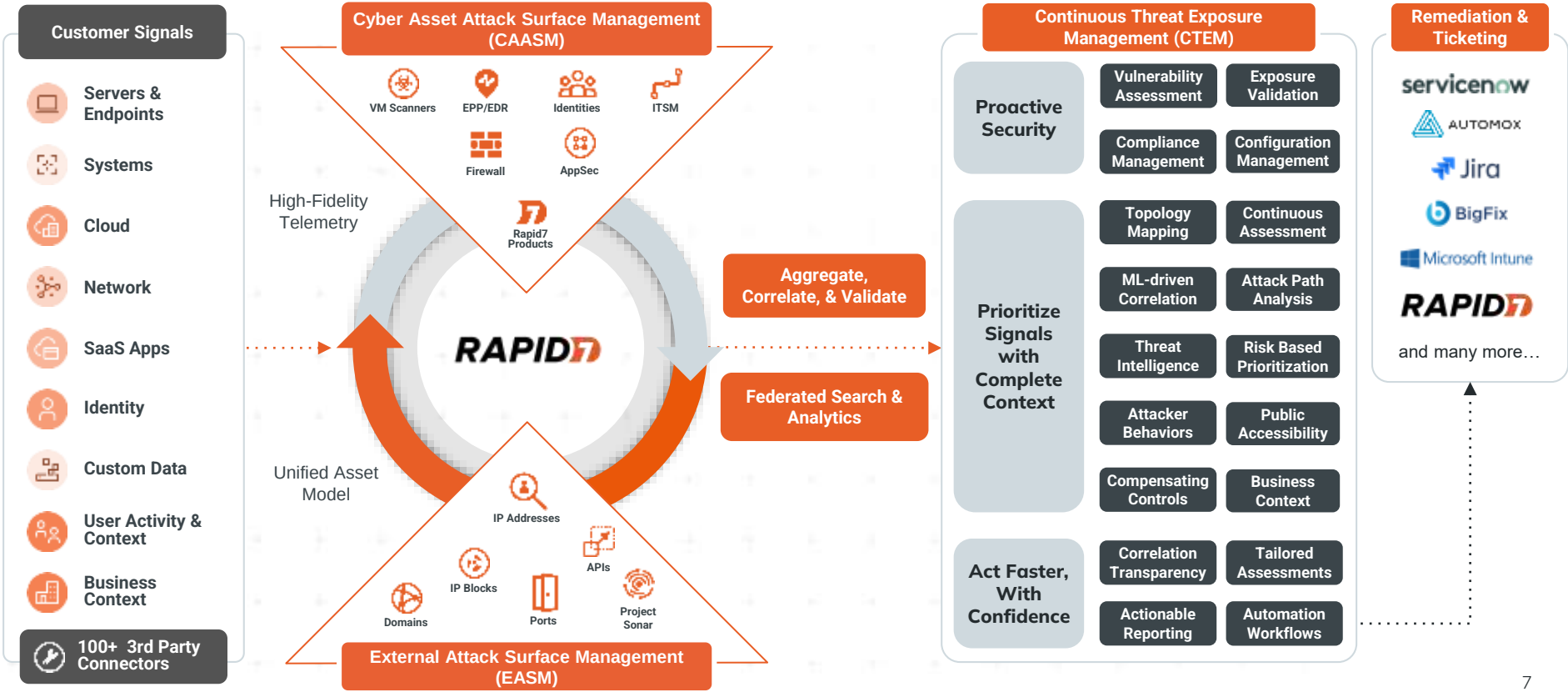
- Gartner’s Cybersecurity Controls Assessment Benchmark 2023

In Other Words:

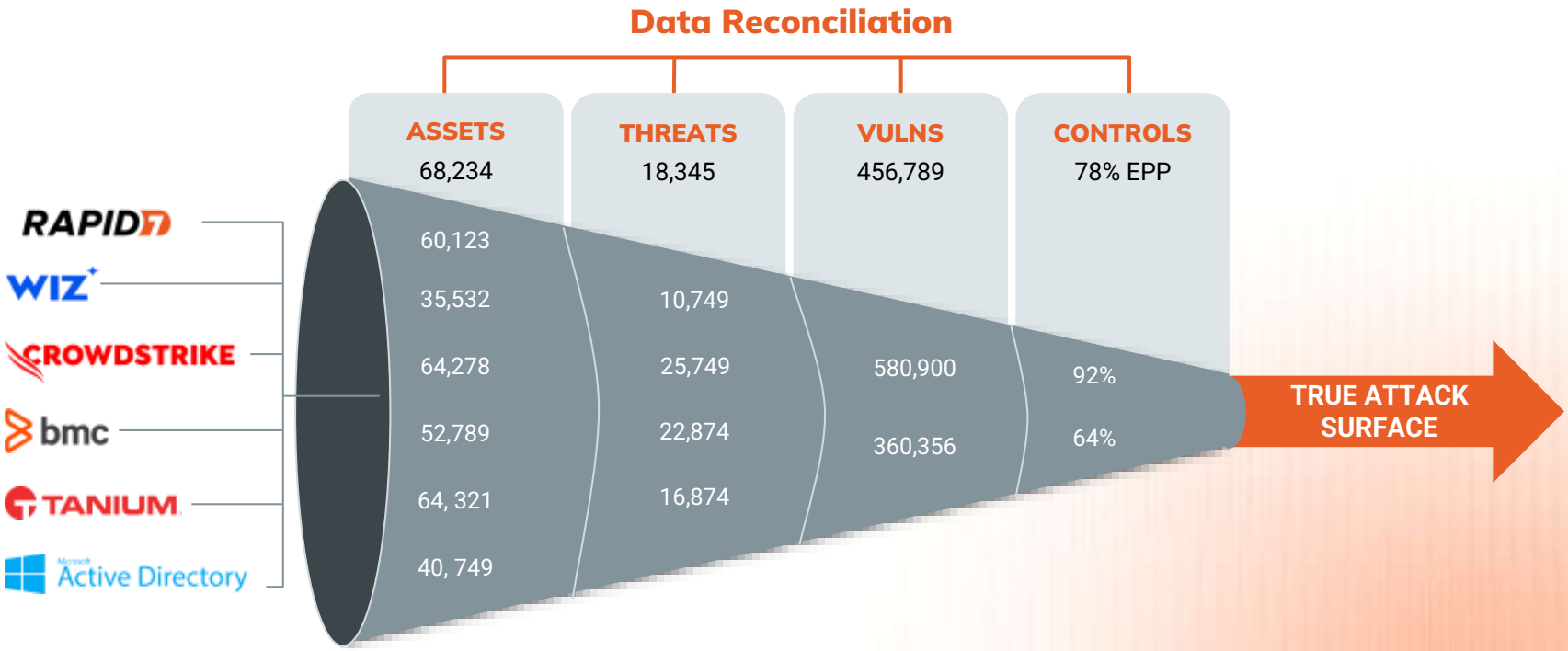
More than 80% of organizations do not understand their attack surface.

- Gartner's Cybersecurity Controls Assessment Benchmark 2023

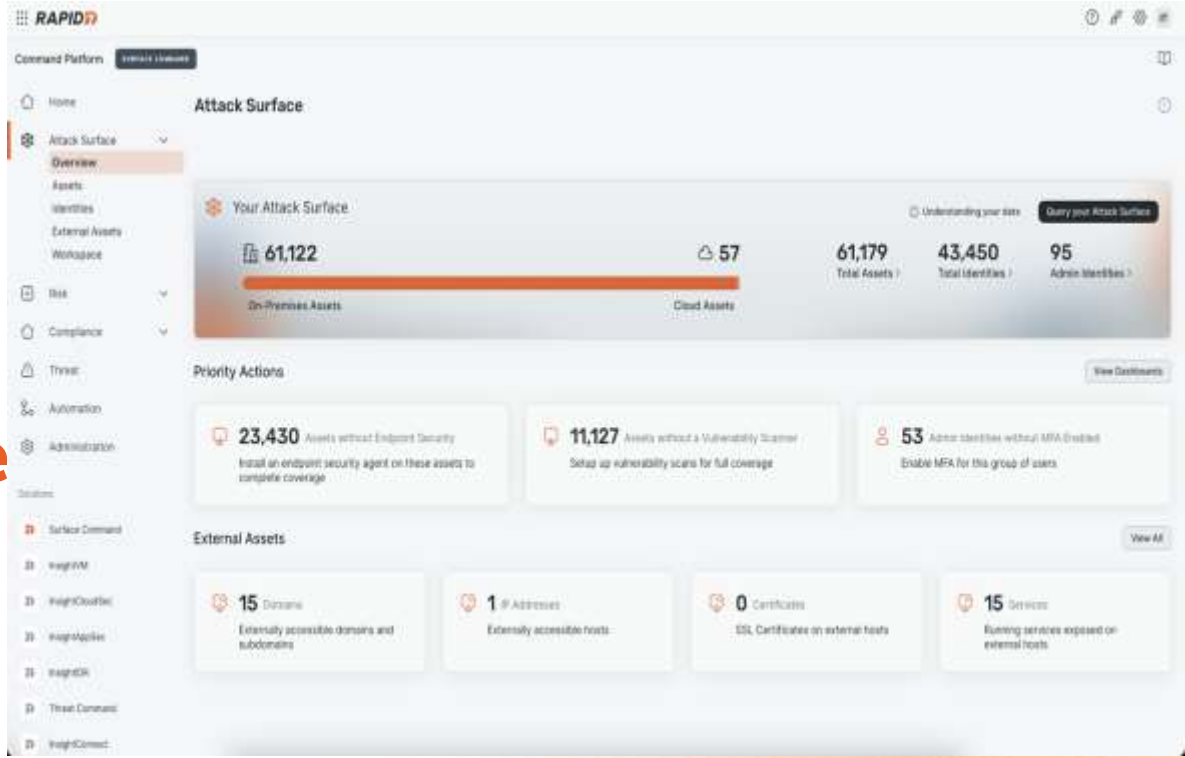
Rapid7 Surface Command



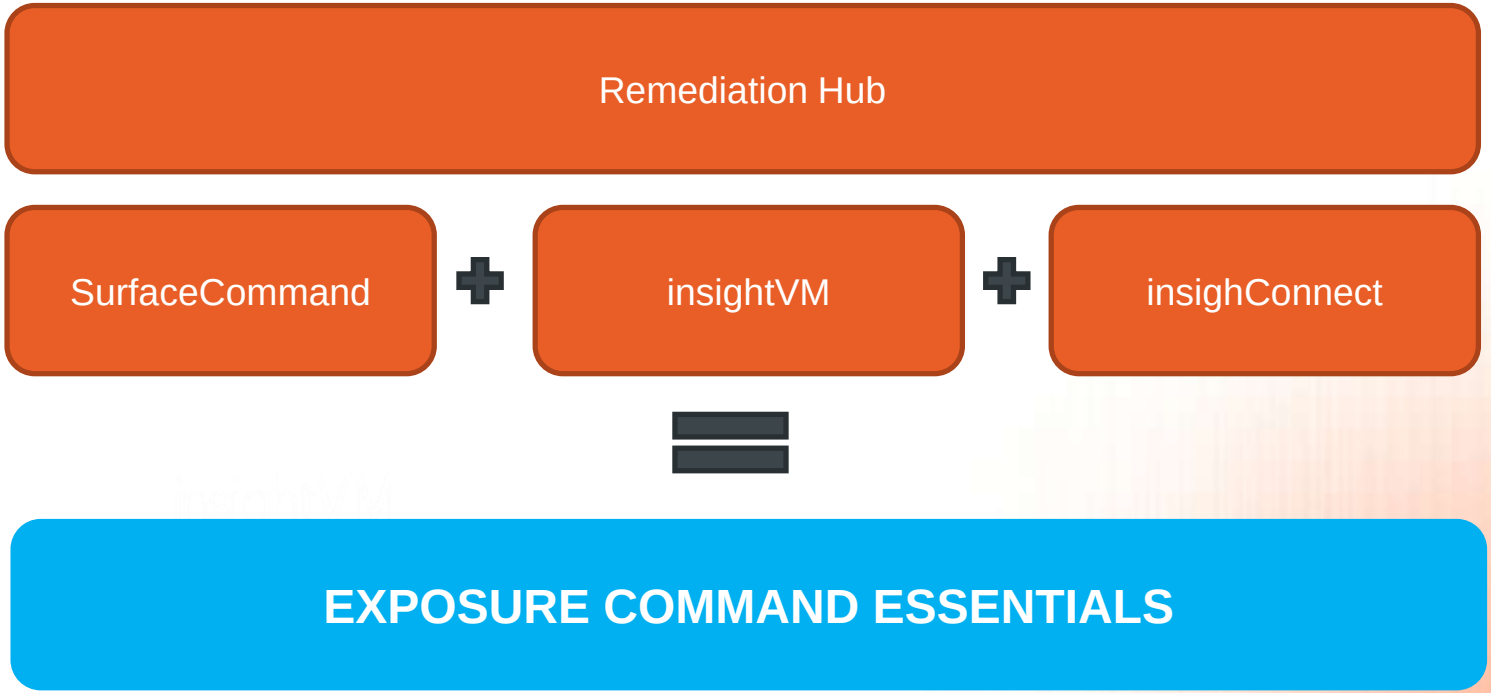
Organization's Lack Accurate Visibility

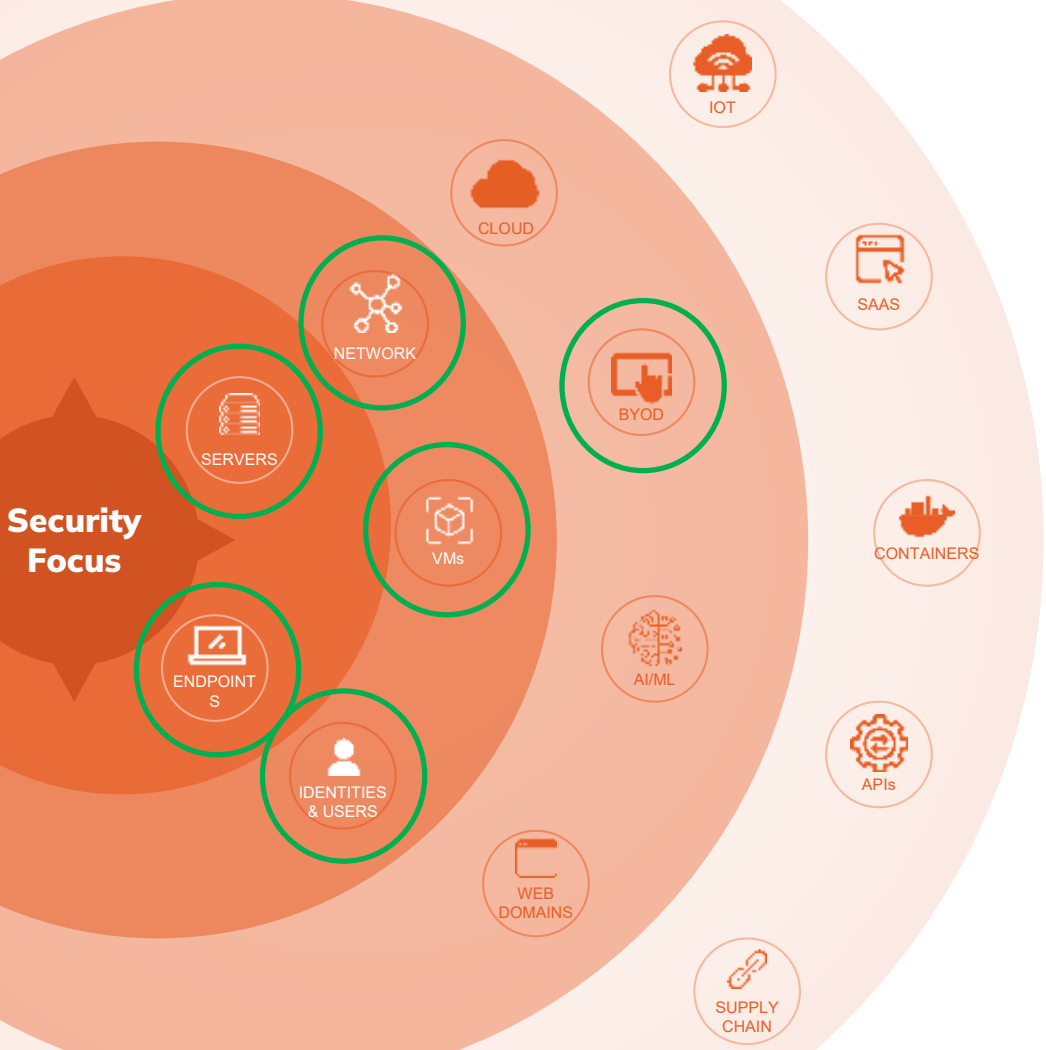


Visualize Your Attack Surface from Inside and Out with Surface Command



What is Exposure Command





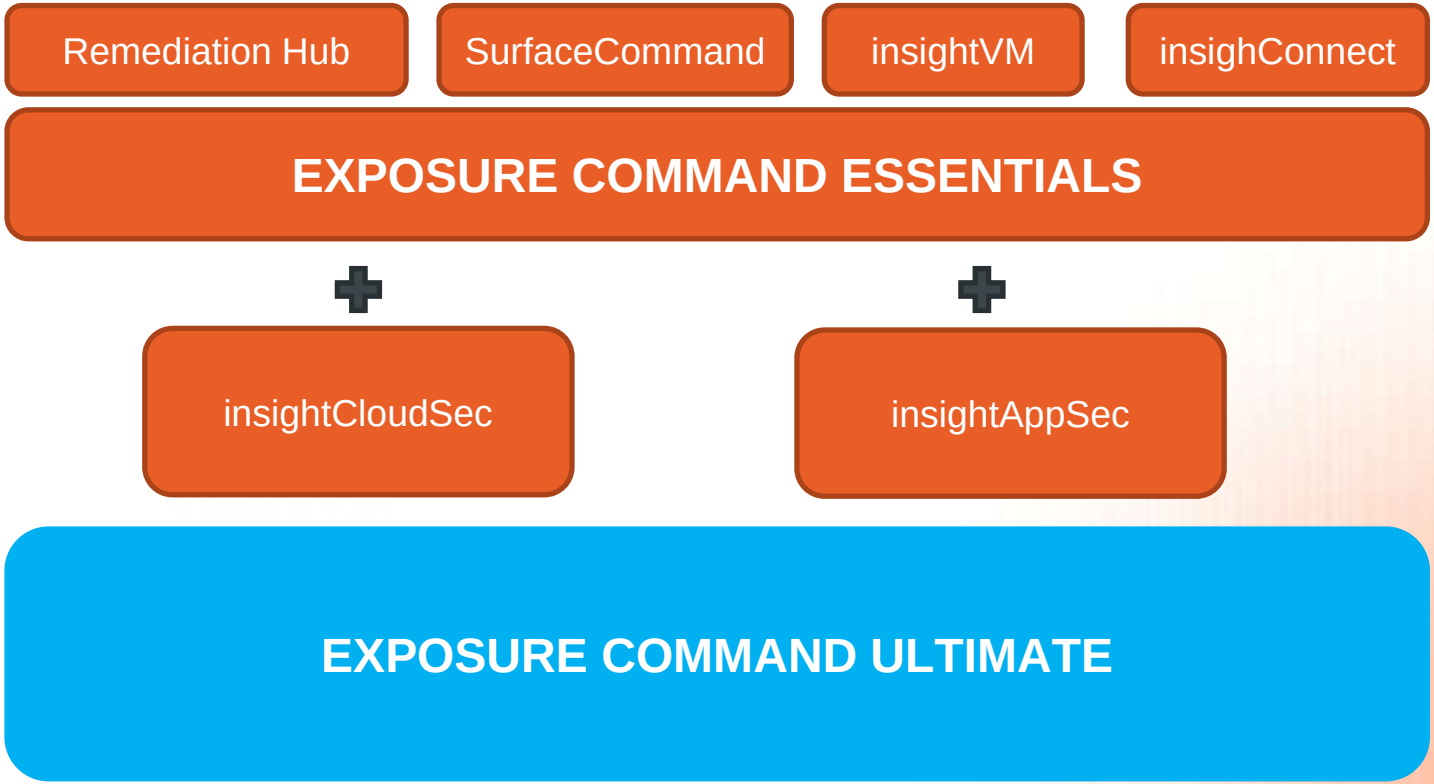
Fragmented Attack Surface Challenges Productivity, Efficiency, Credibility

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

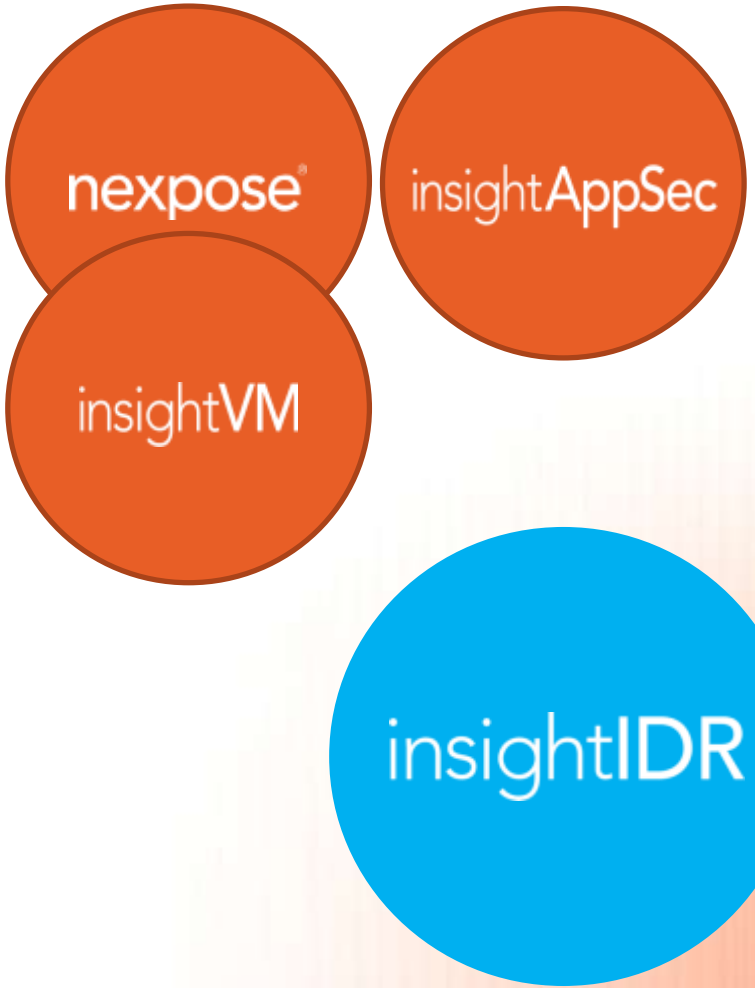
COMPLEX SYSTEMS INTEGRATIONS
Caught in a web of disparate, conflicting sources to try to get effective context, make decisions, and know where to focus

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

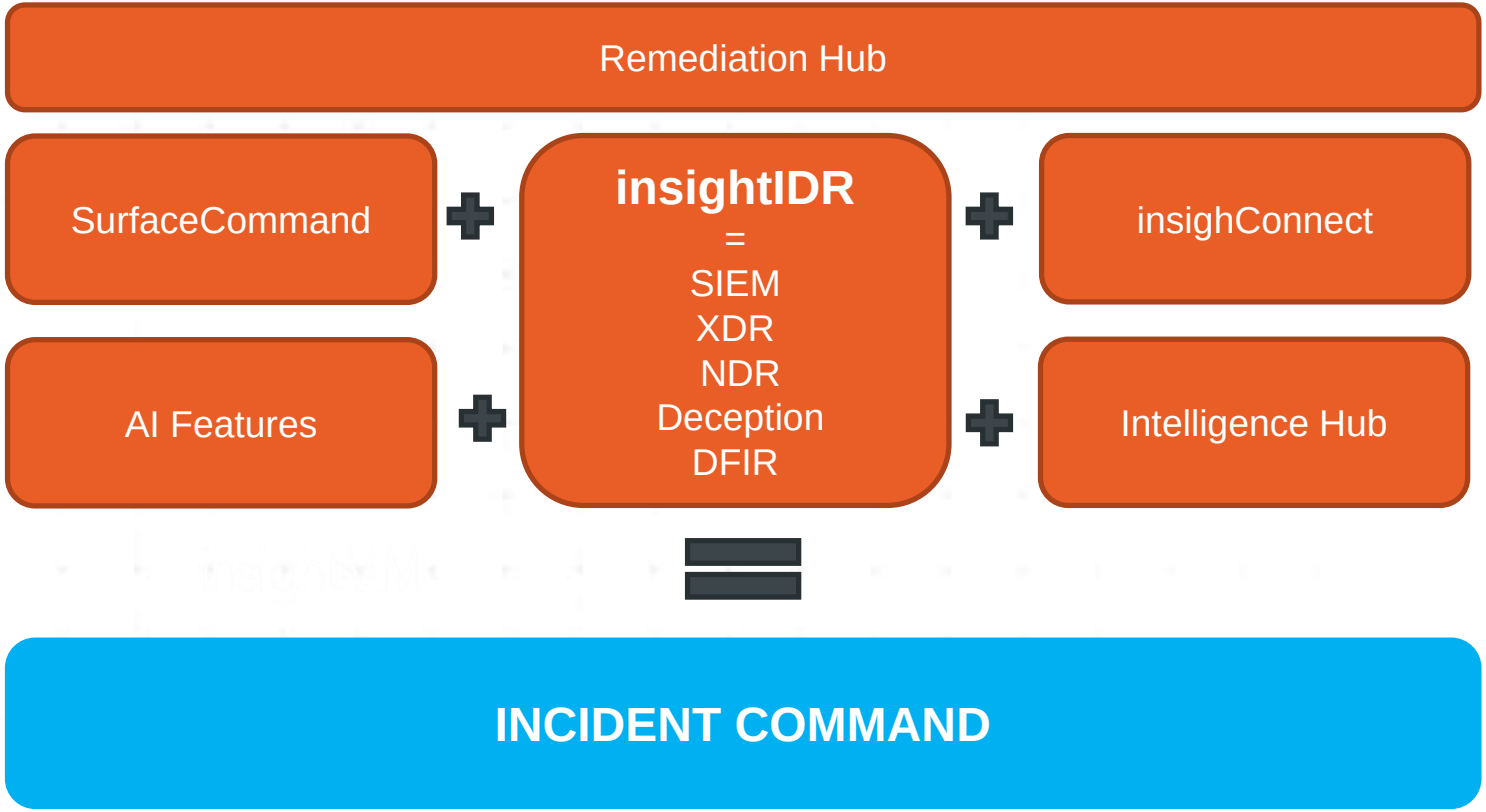
What is Exposure Command



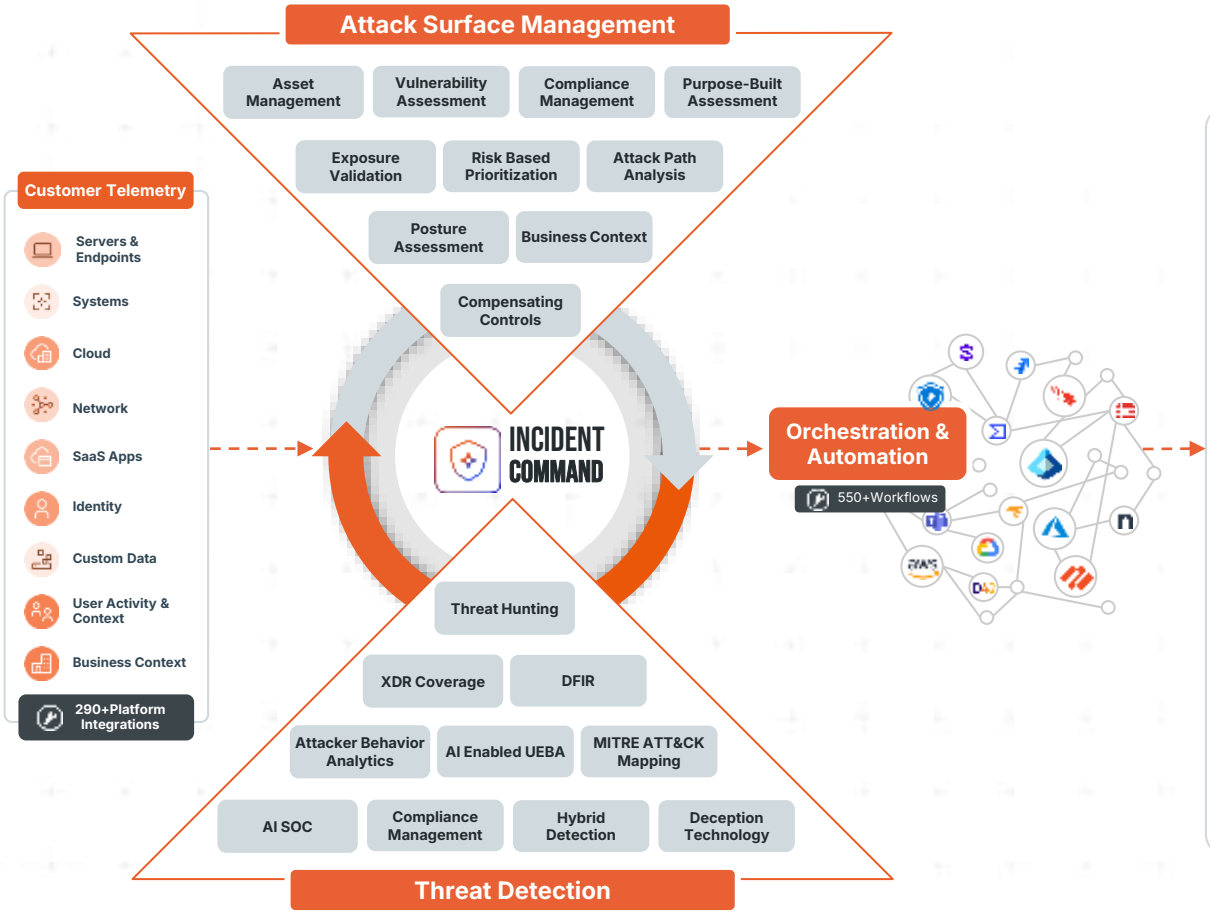
RAPID7



What is Incident Command



Incident Command: Scaling your SOC with Speed and Confidence



Complete Risk & Threat Coverage

Bridge The Context Gap	Instantly connect risk, asset, and threat intelligence to eliminate blind spots and drive decisive action.
Accelerate with the AI SOC	Triage and analyze more alerts, faster and with less noise and more focus.
Prevent & Detect Early & Reliably	Detect threats sooner and with greater precision before they escalate.
Eradicate Threats Faster	Automate investigations and response to contain threats in minutes, not hours.

Incident Command

Ingest, Correlate, and Respond at Scale

RAPID7

COLLECT	DETECT	ENRICH	TRIAGE	INVESTIGATE	RESPOND
Ingest security data from across your diverse ecosystem.	Identify suspicious activity with analytics and threat intelligence.	Gather asset, exposure, and user context for alerts.	Assess alert severity and determine investigation urgency.	Correlate events to understand scope, impact, and root cause.	Take containment, remediation, and notification actions.
Ingest all security data without compromise.	**Surface real threats across your entire ecosystem.**	**Add deep context to every investigation.**	**Accelerate triage and eliminate alert fatigue.**	**Correlate, reconstruct, and understand every attack.**	**Orchestrate fast, consistent response and remediation.**
● Ingest **logs** and telemetry from all major sources ● **Capture** endpoint, cloud, network, and identity **data** ● Integrate with **290+ platforms** and apps	● **Identify threats** with advanced analytics and correlation ● **Use MITRE ATT&CK® mapping** for detection confidence ● Spot **lateral movement**, **credential misuse**, and unknown attacks ● **Reduce false positives** with behavioral analytics	● **Add** asset and exposure **context** to every alert ● Link detections to business-critical systems ● See **user**, **vulnerability, and risk details** ● Surface impacted assets **for faster decisions**	● **Filter noise** with AI-driven alert scoring ● **Prioritize true threats**, not routine events ● Streamline analyst workflow with **automation** ● Escalate urgent incidents immediately	● Correlate events across all telemetry in one timeline ● Trace **attack paths** and **lateral movement** ● Visualize user, asset, and **network relationships** ● **Access all context without** tool switching	● **Trigger playbooks** to contain or remediate ● **Automate** common **response** actions ● Document **investigations and evidence** ● **Integrate with ITSM** and **case management tools**

Security Operations:

Vetted and Continuous Threat Intel

Rapid7 Intelligence Hub takes raw threat data and transforms it into curated, actionable threat intelligence:

- **Proactively Respond to Real-World Threats:** Aggregated, context-rich intelligence focuses analysts on high-confidence threats and enables proactive defense by tracking top adversaries targeting your industry.
- **Enhance Detection Coverage and Threat Hunting:** Actionable threat intelligence enables reliable attribution with mapped threat actor profiles and increases precision.
- **Prioritize Remediation:** Prioritize and justify remediation by targeting the highest-risk threats with real-world intelligence and business context.

The Rapid7 AI SOC

Powering Scalable Security Operations

- **AI Alert Triage**
  Automated alert analysis triages with 99.93% benign alert accuracy, reducing noise and improving response times.
- **Agentic AI Workflows**
  Autonomous investigative intelligence that scales investigation capacity and accelerates human decision-making.
- **AI for Log Search**
  Search logs and hunt for threats using natural language to query logs and surface the insights that matter without complex LEQL queries.

3 CORE TENETS OF AI DEVELOPMENT

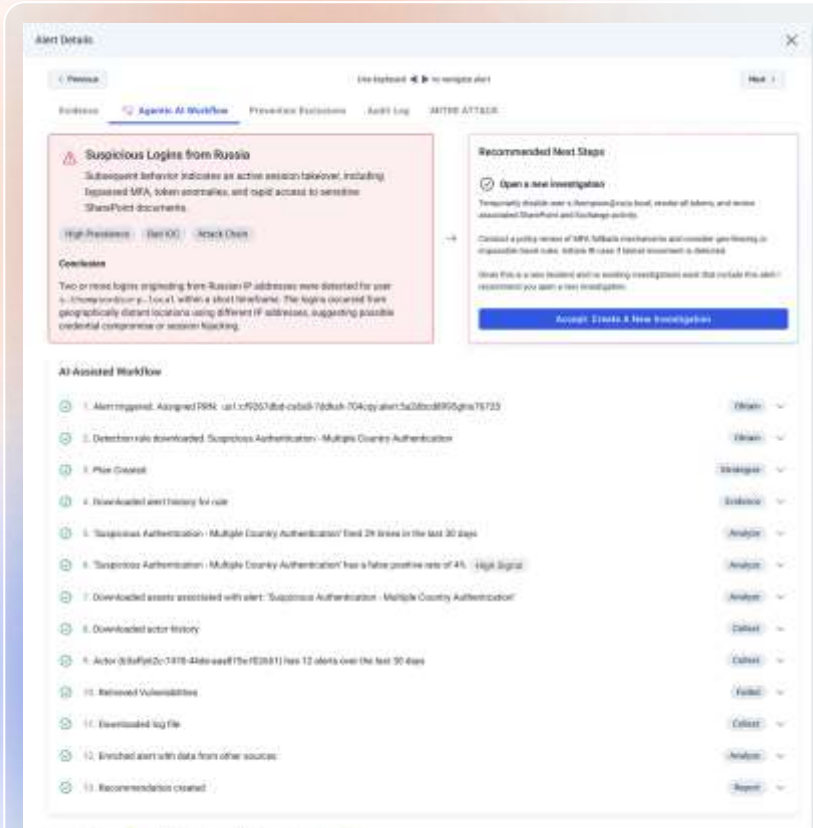
1. **Human Centric:**
   Enhance human capabilities without ever replacing human judgment. Empower, but never override, the human analyst.
2. **Transparent & Accountable:**
   Understand and clearly see when and how AI is used to impact decision-making and drive security outcomes.
3. **Built on Analyst Experience:**
   Reflect the rigor and experience of analyst-led detection and response in every AI-powered action or output.

Security Operations:

Faster SOC Outcomes with AI

Agentic AI Workflows add speed and a repeatable framework to collect information, correlate context, analyze, and strategize within seconds:

- **Investigate More Alerts, Faster:** Accelerate triage by autonomously enriching alerts and surfacing context in seconds.
- **Ensure Consistent, High-Quality Investigations:** Applies structured, repeatable analysis – in line with the OSCAR framework to deliver reliable outcomes across every alert.
- **Autonomous Intelligence, Human-Centered Control:** Acts independently but defers decisions to analysts, preserving expert oversight.



THANK YOU!

Contact: Khvorstyna Dmytro

khvorostyna@softprom.com

APPENDIX

Rapid7 Insight Agent

The Power of the Agent

See speaker notes for
risks of not using the In

Continuous, Real-Time Visibility

- Continuously collects data from endpoints instead of scheduled snapshots
- Crucial for assets that are frequently off the corporate network, such as laptops used by remote workers
- Ensures that security teams have up-to-date information on vulnerabilities and threats at all times

Extended Threat Detection and Response (EDR) Capabilities

- Collect process, log, and user activity data from the endpoint, essential for detecting the early signs of an attack
- Allow security teams to identify suspicious behaviors and respond to threats before they escalate into a full-blown breach

Deeper Context and Analytics

- Data collected by the agent fuels the analytics within Incident Command
- Provides rich context, such as which user is running a process, which can be critical for an investigation
- Enables more accurate threat detection rules and helps prioritize vulnerabilities based on real-world risk and attacker behavior

Simplified Deployment and Management

- Designed to be lightweight and easy to deploy at scale and installed on a wide range of operating systems (Windows, Linux, MacOS)
- Can be mass-deployed using standard management tools and also updates automatically, reducing the administrative overhead for security teams
- Usable by both Incident Command and Exposure Command, no duplicate installation

Defense in Depth

- Supplement existing EDR agents when those agents are compromised or bypassed

On average, there are over 15 million Insight Agents in daily use

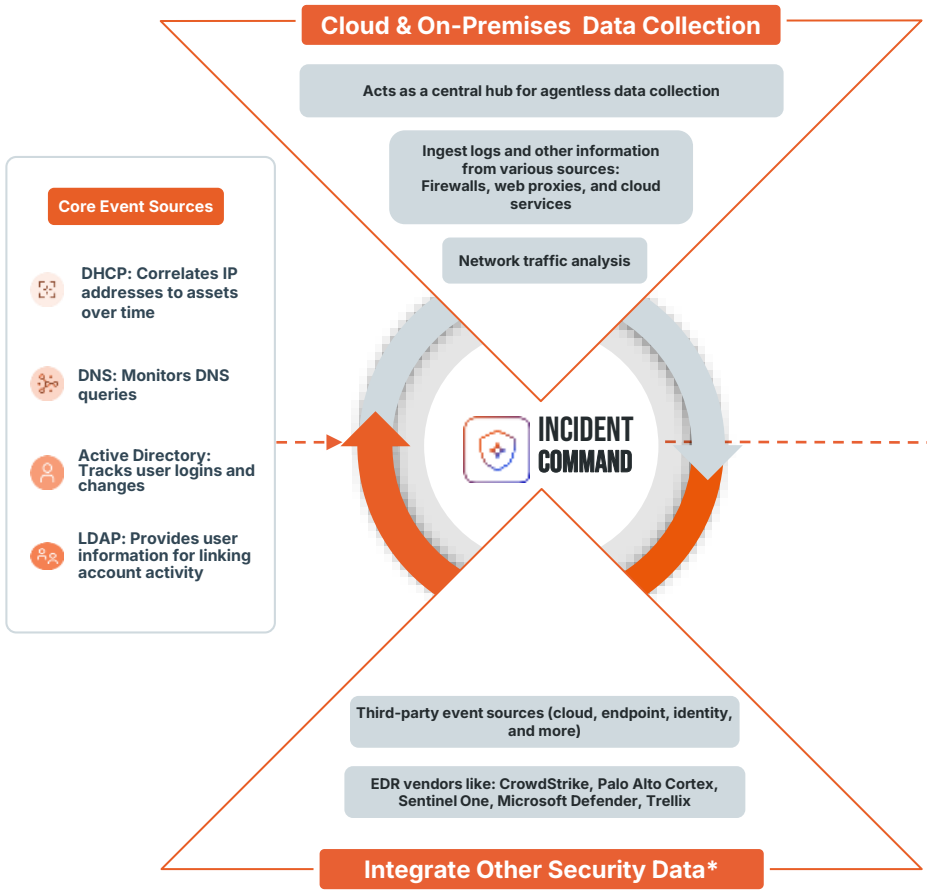
> "Immediately, the information began flowing in a very manageable way. It was easy to see the value in the product – it alerted us to the presence of malware that was easily eliminated, but that we might not otherwise have known about."

Søren Hansen, IT Security Manager
Chr. Hansen

Small footprint. Big insights.	
Footprint	~50-100 MB
RAM	<100-200 MB
CPU	<6-8%

Data is approximated; reflects Incident Command only, does not include InsightVM.

Incident Command: Security without the Insight Agent



Core Security Capabilities:

- Log Search and Analysis
- UBA
- Threat Detection
- Deception Technology
- Investigations and Reporting
- Network Detection and Response

*Without the Insight Agent, no layered security

In 2025, compromise starts with credentials

50%

of incidents responded to by the Rapid7 SOC were initiated via valid accounts without MFA or social engineering[1]

50 : 1

Ratio of non-human to human identities[2], expected to balloon with greater adoption of generative and agentic AI

80%

of global social engineering attacks now involve AI-generated content[3]

292 DAYS

to identify and contain breaches involving stolen credentials, the longest of any attack vector[4]

IDENTITY IS THE MODERN CYBER BATTLEGROUND

Traditional detection and access controls can't keep pace with adversaries who can generate trust on demand

Security teams must evolve from static credential defense to continuous identity verification and behavior-based detection

[1] Q3 2025 Incident Response Data, Rapid7 [2] DarkReading [3] ENISA [4] IBM

How We Detect Identity Threats in Incident Command

Identity Data in, Fast

Native event sources for Okta, Entra ID/Azure AD, VPNs, and more, like feed authentication, admin actions, and ingress activity into a common schema that allows for rapid identity detection and response.

Common Schema

Incident Command learns normal user patterns (devices, geos, access times) and flags anomalies as notable events or alerts.

Identity Alerts

Prioritize High-Value Signals

Rule actions, priorities, exceptions, and throttles help reduce noise while preserving coverage.

- ✓ Account Takeover
- ✓ Privilege Escalation
- ✓ Lateral Movement
- ✓ Insider Threat or Unauthorized Access
- ✓ Automated Credential Attacks