

# RAPID7 INCIDENT COMMAND: CONTEXT, CLARITY, AND CONFIDENCE TO ACT

## AI-Powered Next-Gen SIEM

### The context gap in security operations

Security teams today can't afford to look at threats in isolation. When an alert fires, it's not enough to know what happened—you need to know why it happened, what kind of asset is involved, how exposed it is, and what it means for the business. Without this context, teams are forced to react to symptoms instead of solving root causes, investigations slow down, and the window to act with confidence narrows.

Modern attacks move seamlessly across endpoints, cloud, SaaS, identity, and unmanaged assets - far beyond the reach of siloed security approaches. Responding effectively requires real-time, comprehensive context: the ability not just to see what's happening, but to understand why and have the tools to act on that insight, fast.

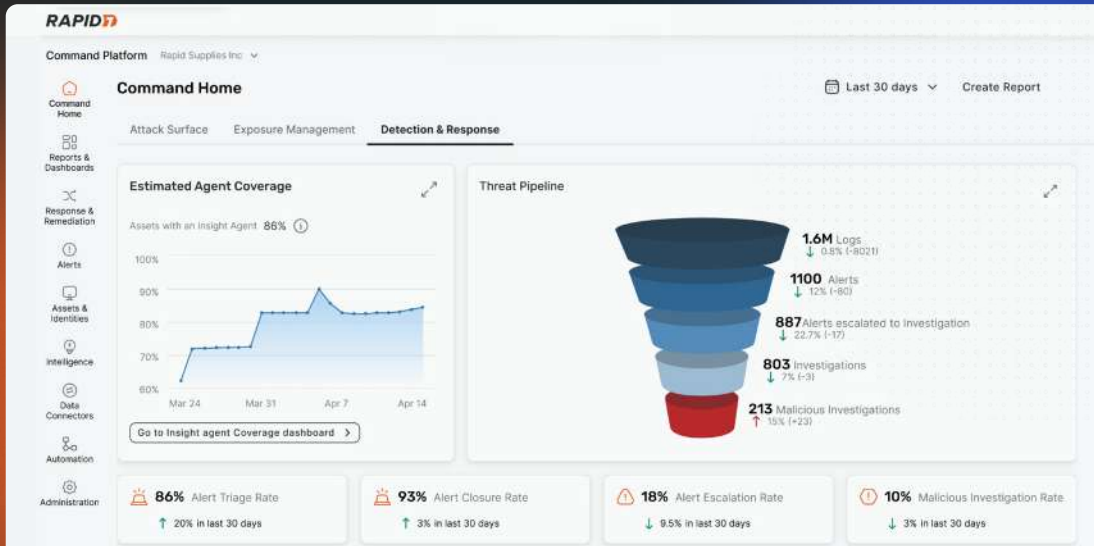
### Incident Command sets a new standard

Incident Command is the only AI-powered security operations platform that's purpose-built to deliver unified insight and deep environmental context **across your entire threat landscape**, with powerful analytics, investigation, response, and remediation functionality. By fusing internal and external asset context (ASM), threat intelligence, native and third party security telemetry, and vulnerability exposure into every alert and investigation, Incident Command empowers security teams to move with speed and confidence from first signal to decisive action. AI-powered investigation and automation transform this context into momentum, so analysts can cut through the noise, focus on what matters, and act fast to stop threats.



**76% of organizations have experienced some type of cyberattack due to an unknown, unmanaged, or poorly managed internet-facing asset. Identify unknown assets and secure your entire digital estate.”**

-ESG



## From overwhelmed to taking command

CHALLENGE	HOW INCIDENT COMMAND SOLVES IT
Relentless alert volume and alert fatigue	AI-powered triage eliminates noise by automatically classifying 99.93% of benign alerts, so your team spends time only on true threats.
Fragmented environment visibility	Unified platform brings together asset, attack surface, risk, and third-party insights for continuous, full-spectrum visibility.
Siloed context; lack of asset risk awareness	Asset context enriches alerts with full context asset, identity, threat, and vulnerability - so action is always risk-driven and business-aligned.
Slow, manual investigation and response	Automation and SOAR workflows accelerate triage, investigation, and response to cut MTTR and analyst workload.
Difficulty scaling threat hunting and detection	Analysts can hunt for threats across all sources with easy-to-use log management and AI-powered natural language search.
Manual, error-prone triage and incident management	Agentic AI recommends next actions, links evidence, and streamlines investigations with unified timelines and playbooks.
Complex, hard-to-tune detection rules	Continuously updated MITRE ATT&CK®-mapped detections deliver immediate protection against new threats, with the ability to write custom detections based on environment needs.
Vendor lock-in and costly ingestion-based pricing	Ecosystem-agnostic SIEM with 180+ integrations and our own detection library, and asset-based pricing provide flexibility, transparency, and rapid time-to-value.
Difficulty proving progress and ROI to stakeholders	Detection & response dashboard provides at-a-glance, real-time reporting and drill-downs, making it easy to track, demonstrate, and share program progress and results.

## Core use cases across the detection & response lifecycle:

### VISUALIZE



Unify asset, risk, and telemetry data into one view. Eliminate blind spots with native Attack Surface Management (ASM), cloud, and third-party ingestion.

### DETECT



Behavioral analytics, user behavior analytics (UBA), and detection-as-code workflows reduce alert noise and highlight stealthy threats.

### IDENTIFY



AI-based triage, exposure context, and threat enrichment focus the team on high-risk issues.

### INVESTIGATE



Correlate evidence across users, assets, and environments. AI technology correlates data and recommends next steps in the process with speed, accuracy, and transparency.

### CONTAIN



Trigger response actions directly from investigations. Automated workflows and playbooks make response consistent, auditable, and fast.

### RESPOND



Built-in response playbooks, automated documentation, and analyst feedback loops continuously tune the system and improve outcomes.

## Lead with insight. Respond with precision. Prove your impact.

The attack surface is getting bigger, the data is getting louder, and the stakes are higher than ever. Incident Command turns fragmented noise into unified intelligence to deliver real-time context, machine-speed triage, and AI-powered triage, hunting, and investigation at enterprise scale. Move beyond traditional SIEMs, shrink dwell time, automate away the grunt work, and give your SOC the platform to see everything, understand anything, and act before attackers do.



**THIS IS NEXT-LEVEL DETECTION AND RESPONSE. THIS IS TAKING COMMAND.**

# INCIDENT COMMAND PACKAGES:

## Tiered capabilities and market value for today's SOC

PACKAGE	WHAT'S INCLUDED
<b>ESSENTIAL</b>	<b>Rapid7 Agent</b> <ul style="list-style-type: none"><li>• SIEM (Log Management, Rules, UBA)</li><li>• Asset &amp; Attack Surface Discovery (ASM)</li><li>• Active Risk Prioritization</li><li>• Remediation Hub &amp; SOAR</li><li>• Embedded Threat Intelligence</li></ul>
<b>ADVANCED</b>	<b>Everything in Essentials, plus:</b> <ul style="list-style-type: none"><li>• AI-Powered Alert Triage</li><li>• Agentic AI Workflows</li><li>• Intelligence Hub</li><li>• Deception Technology</li><li>• Extended Retention</li></ul>
<b>ULTIMATE</b>	<b>Everything in Advanced, plus:</b> <ul style="list-style-type: none"><li>• Endpoint Detection &amp; Response (EDR)</li><li>• Network Detection &amp; Response (NDR)</li><li>• Intrusion Detection (IDS)</li><li>• Hosted DFIR &amp; Velociraptor</li></ul>

### ABOUT RAPID7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open-source communities and cutting-edge research—using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.



### SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

### ACCELERATE WITH

[Command Platform](#) | [Exposure Management](#) |  
[Attack Surface Management](#) | [Vulnerability Management](#) |  
[Cloud-Native Application Protection](#) | [Application Security](#) |  
[Next-Gen SIEM](#) | [Threat Intelligence](#) | [MDR Services](#) |  
[Incident Response Services](#) | [MVM Services](#)

### SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free -  
start your trial at [rapid7.com](https://rapid7.com)

