RAPID7 VS EXABEAM

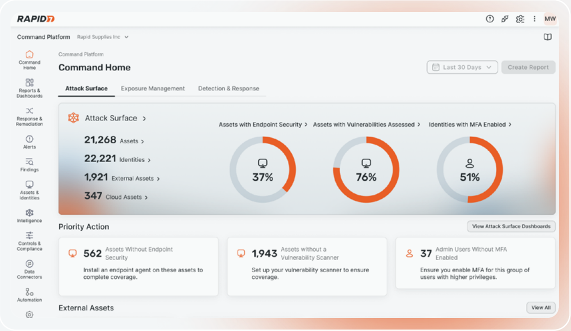
Why Rapid7 Beats Exabeam: A Unified Platform for the Modern SOC

The Security Information and Event Management (SIEM) market is undergoing a profound transformation, shifting from a collection of siloed tools to a unified platform-centric approach. This is being driven by escalating cyber threats, rapid cloud adoption, and the imperative for real-time threat detection and response. Perpetual SOC analyst frustration over other platform's lack of visibility into their entire threat attack surface remains a prominent issue and as a result, SOC performance continues to suffer.

Incident Command is an AI-native security operations platform that transforms how modern SOCs detect, investigate, and respond to threats. Unlike Exabeam, which is trying to cobble different capabilities together and integrate an entirely different LogRhythm platform, Rapid7's unified platform combines Attack Surface Management (ASM) with SIEM, Security Orchestration, Automation, and Response (SOAR), Digital Forensics and Incident Response (DFIR), and Threat Intelligence into a single, cohesive platform to eliminate fragmented tooling and quickly provide superior business value.

SOC-Proven All-in-One Solution for Detection and Response

Incident Command combines ASM and an award-winning SIEM, SOAR, DFIR, and Threat Intelligence into a single, scalable solution with superior detection and resolution, all in a single product interface. Unlike Exabeam's separate ASM offering with a different interface that provides limited integration with their SIEM.



Command Platform

Command Home

Attack Surface >

21,268 Assets >
22,221 Identities >
1,921 External Assets >
347 Cloud Assets >

Assets with Endpoint Security > 37%
Assets with Vulnerabilities Assessed > 76%
Identities with MFA Enabled > 51%

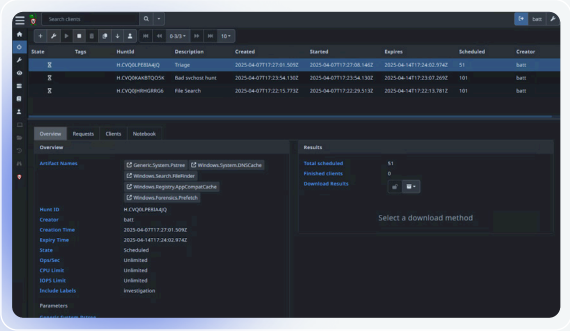
Priority Action

562 Assets Without Endpoint Security
Install an endpoint agent on these assets to complete coverage.

1,943 Assets without a Vulnerability Scanner
Set up your vulnerability scanner to ensure coverage.

37 Admin Users Without MFA Enabled
Ensure you enable MFA for this group of users with higher privileges.

External Assets



State	Tags	HuntId	Description	Created	Started	Expires	Scheduled	Creator
⧗		H.CVQ0LPE8IA4JQ	Triage	2025-04-07T17:27:01.509Z	2025-04-07T17:27:08.146Z	2025-04-14T17:24:02.974Z	51	batt
⧗		H.CVQ0KAKBTQO5K	Bad svchost hunt	2025-04-07T17:23:54.130Z	2025-04-07T17:23:54.130Z	2025-04-14T17:23:07.269Z	101	batt
⧗		H.CVQ0JHRHGRRG6	File Search	2025-04-07T17:22:15.773Z	2025-04-07T17:22:29.513Z	2025-04-14T17:22:13.781Z	101	batt

Overview

Artifact Names	Generic.System.Pstree Windows.System.DNSCache Windows.Search.FileFinder Windows.Registry.AppCompatCache Windows.Forensics.Prefetch
Hunt ID	H.CVQ0LPE8IA4JQ
Creator	batt
Creation Time	2025-04-07T17:27:01.509Z
Expiry Time	2025-04-14T17:24:02.974Z
State	Scheduled
Ops/Sec	Unlimited
CPU Limit	Unlimited
IOPS Limit	Unlimited
Include Labels	investigation

Parameters

Results

Total scheduled	51
Finished clients	0
Download Results	

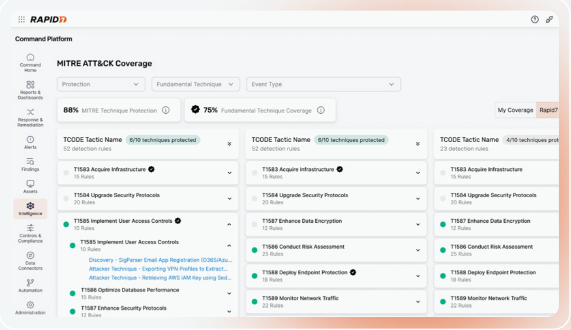
Select a download method

Dedicated Tool for Targeted Endpoint-Based Forensic Collection

Analysts directly perform the targeted collection of digital forensic evidence simultaneously across their endpoints with speed and precision thanks to the included DFIR tool, Velociraptor. This advanced DFIR tool enables investigators to hunt for live artifacts and remove malicious remnants of a breach. Exabeam's approach is primarily retrospective and log-centric; building a narrative from enriched event data.

Superior Business Value with Predictable Costs

Rapid7 is the only major SIEM provider with asset-based pricing, preventing billing surprises that can disrupt your security budget. Exabeam uses a complex pricing model with additional expenses for necessary add-ons, and ingest-based pricing, which can be variable and cause significant, unanticipated increased charges.



MITRE ATT&CK Coverage

88% MITRE Technique Protection

75% Fundamental Technique Coverage

TCODE Tactic Name 6/10 techniques protected
52 detection rules
- T1583 Acquire Infrastructure — 15 Rules
- T1584 Upgrade Security Protocols — 20 Rules
- T1585 Implement User Access Controls — 10 Rules
  - T1585 Implement User Access Controls — 10 Rules
    - Discovery - SigParser Email App Registration (O365/Azu...
    - Attacker Technique - Exporting VPN Profiles to Extract...
    - Attacker Technique - Retrieving AWS IAM Key using Sed...
  - T1586 Optimize Database Performance — 15 Rules
  - T1587 Enhance Security Protocols — 12 Rules

TCODE Tactic Name 6/10 techniques protected
52 detection rules
- T1583 Acquire Infrastructure — 15 Rules
- T1584 Upgrade Security Protocols — 20 Rules
- T1587 Enhance Data Encryption — 12 Rules
- T1586 Conduct Risk Assessment — 25 Rules
- T1588 Deploy Endpoint Protection — 18 Rules
- T1589 Monitor Network Traffic — 22 Rules

TCODE Tactic Name 4/10 techniques prot
23 detection rules
- T1583 Acquire Infrastructure — 15 Rules
- T1584 Upgrade Security Protocols — 20 Rules
- T1587 Enhance Data Encryption — 12 Rules
- T1586 Conduct Risk Assessment — 25 Rules
- T1588 Deploy Endpoint Protection — 18 Rules
- T1589 Monitor Network Traffic — 22 Rules

It’s Not Just About Checking the Critical Boxes, But We Do Anyway

USE CASE / FEATURE	DETAILS	RAPID7	EXABEAM
Full-Spectrum Visibility Across the Attack Surface	By integrating ASM, analysts have one centralized view of the entire threat attack surface that transforms how modern SOCs detect, investigate, and respond to threats.	✓	✗
Transparent, Asset-Based Pricing	Provides a clear-cut, predictable cost that scales with a tangible metric (the number of assets) that is easier for a CISO to track and budget for.	✓	✗
Cloud-Native SIEM, SOAR, and UBA	A true cloud-native SIEM, with integrated SOAR and UBA capabilities.	✓	✓
AI-Powered Log Search	AI log search query interface uses natural language to accelerate investigations with faster insights and no complex language learning curve.	✓	✓
AI Triage & Agentic AI Workflows	AI alert triage and agentic workflows reduce analyst workload and accelerate investigations.	✓	✓
Detection Library Mapped to MITRE ATT&CK®	Rich library of prebuilt detections mapped to the MITRE ATT&CK framework.	✓	✓
DFIR & Remote Remediation	Integrated digital forensics and endpoint interrogation tooling with malicious artifact clean up.	✓	✓
Deception Technology	Native deception tools lure adversaries and accelerate investigations.	✓	✗
Unified Navigation Across All Components	Streamlining every interaction, the Command Platform’s unified navigation helps security analysts move faster, stay focused, and get more done, reducing friction so they can spend less time finding what they need and more time taking action.	✓	✗

Driving Real-World Customer Impact

A major university faced significant cybersecurity challenges due to the lack of a centralized SIEM system, forcing its team to rely on time-consuming manual processes and leaving them with critical blind spots across their network. After evaluating several vendors, the university chose Rapid7 for its comprehensive capabilities and competitive, predictable pricing. The university was able to shift from a reactive to a proactive security posture, which has not only significantly reduced investigation times but also empowered the team to focus on strategic tasks, ultimately strengthening the university’s overall security.

Challenges Faced:

- **Lack of centralized visibility:** Without a SIEM, logs were scattered across multiple servers, making it impossible to see a complete picture of security activity leaving them flying blind against threats.

- **Time-consuming manual processes:** The team had to manually go through individual log files and cross-reference data. This slow and inefficient process limited their ability to quickly detect and respond to complex threats.
- **Cumbersome log management:** Logs were stored on a basic server, which limited their ability to correlate events and required team members to switch between different systems to document findings, slowing down their incident response.

Benefits of the Rapid7 Solution:

- **Centralized visibility:** The team gained a centralized platform to collect and correlate logs from various systems, eliminating fragmented data and providing a cohesive view of their network.
- **Faster, more efficient threat detection:** The user-friendly interface allowed the team to quickly access and analyze activity, drastically reducing the time it took to investigate security issues. A task that once took hours, like tracing VPN login activity, now takes only minutes.
- **Real-time response:** Rapid7's real-time alerting and response capabilities improved the team's ability to swiftly detect and respond to threats, making it faster and more accurate to identify compromised accounts.
- **Improved team focus:** By automating and streamlining manual processes, the security team can now reallocate time and resources to more strategic tasks, such as proactive threat hunting and fine-tuning alerts.
- **Enhanced security posture:** The shift from a reactive to a proactive threat management approach has significantly strengthened the university's overall security, empowering the team to protect the community's data with confidence.

"It was a top-tier product, worked really well, and met all of our requirements. And the Rapid7 team was great to work with, I've recommended the product to several other universities that I know that were looking for either their first SIEM or looking at potentially replacing their existing SIEM."
— Director of Information Security, Major University

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.

RAPID7

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**