



# RAPID7 VS AXONIUS

See everything, know what matters, and take action — all in one powerful platform.

When it comes to managing your attack surface, partial visibility creates real risk — blindspots, unmanaged assets, shadow IT, and exposures that attackers will exploit. Rapid7's Exposure Command gives you a complete, continuously updated view across internal and external assets, enriched with native telemetry and threat intelligence to ensure risks are identified, prioritized, and acted on fast.

Axonius relies entirely on third-party data, lacking native discovery, context, and workflows — and charges extra for add-on modules to get value from those sources. With this lack of visibility, networks are left vulnerable. Rapid7 delivers stronger coverage, smarter prioritization, and faster risk reduction, all in one integrated platform instead of multiple point solutions.

## Proactive Exposure Discovery

Rapid7 continuously discovers known and unknown assets, misconfigurations, permissions issues, and exposures so you can eliminate risks before attackers find them. With native EASM, CAASM, and RBVM in one platform, we deliver a complete, real-time view of your attack surface.

Axonius centers on aggregated CAASM data and ingests external findings from third-party tools, which can leave gaps if upstream sources miss assets.



## Actionable Security Intelligence

Rapid7 doesn't just show you what's out there, we tell you what matters most. By pairing real-world vulnerability intelligence with business context, we deliver clear, prioritized risks you can act on immediately. This includes native threat intelligence from our research teams, exploit monitoring, and adversary behavior analysis for timely, first-party context.

Axonius only supports threat intelligence through third-party feeds, but without native capabilities it can't match Rapid7's depth, context, and immediacy, backed by decades of industry leadership in vulnerability research and threat intelligence.



## One Platform, Less Complexity

Rapid7 unifies exposure management and detection and response in a single platform, replacing multiple tools to cut complexity and reduce risk faster. Asset visibility, vulnerability management, cloud security, application security, and incident detection seamlessly work together in one platform.

Axonius centralizes asset data but still relies on separate products for these capabilities. This tool sprawl not only creates complexity but also drives up costs, slows response, and leaves visibility gaps.



## It's Not Just About Checking More Boxes, But We Do Anyway

USE CASE / FEATURE	DETAILS	RAPID7	AXONIUS
<b>Aggregate and normalize asset data into a single source of truth</b>	Correlates asset data from multiple sources to create a unified inventory and asset relationship map.		
<b>Connect to tools and clouds to expand coverage</b>	Offers broad integration support with deep connections across the platform ecosystem.		
<b>Manage the entire attack surface</b>	Provides visibility into both internal (CAASM) and external (EASM) attack surfaces in a single view for comprehensive coverage.		Ingests third-party external findings; no native scanning.
<b>Continuously discover assets and exposures</b>	Natively discovers unknown internet-exposed assets, internal assets, misconfigurations, and exposures to eliminate blind spots.		
<b>Find vulnerabilities at scale</b>	Includes built-in vulnerability management for scanning, prioritization, and remediation.		
<b>Layer first-party security telemetry into your inventory</b>	Combines native security telemetry with other data sources to create a unified, contextualized view of risk and reduce tool sprawl.		
<b>Manage software asset inventory and lifecycle</b>	Provides strong software asset inventory and lifecycle management capabilities.	Limited	 Additional cost
<b>Prioritize risk with business and threat context</b>	Combines vulnerability data with environment, business context, and native threat intelligence to produce clear, action-oriented risk scores, incorporating both first- and third-party intel sources.		Third party feeds only.
<b>Validate exploitable application weaknesses</b>	Delivers dynamic application security testing to identify runtime vulnerabilities during active operations.		
<b>Automate and orchestrate remediation</b>	Delivers no-code workflows and an action library to trigger notifications, open tickets, quarantine devices, update cloud resources, and validate fixes.		 Additional cost
<b>Track and validate compliance cow</b>	Continuously checks controls against benchmarks and produces audit-ready reports, with workflows to address gaps.		 Additional cost

## Exposure Command in Action: Driving Real-World Customer Impact

A global manufacturing company strengthens security operations and supports rapid mergers and acquisitions activity with Rapid7, achieving near-total network visibility.

### Challenges Faced

- The security team was building its program from the ground up while navigating constant mergers and acquisitions - about 120 transactions over five years.
- They lacked the tools needed to understand their true risk and exposure.
- Their rapid growth outpaced the capacity of their initial security services provider, creating urgent visibility and response needs.
- An ever-changing IT network from mergers and acquisitions activity created continuous blind spots and vulnerability risks.

### Benefits of the Command Platform

- A lightweight, always-on agent provides near-complete coverage of the organization's constantly changing network, delivering comprehensive visibility into vulnerabilities, exposures, and attack surface risks.
- Unified attack surface mapping gives the organization a clear, single view of all assets — internal and external — enabling faster, more effective communication of risk posture across the business.
- Integrated risk management capabilities streamline and clarify security alerts, reducing fatigue and enabling proactive controls to prevent misconfigurations.

**“Before Rapid7, we didn’t have the tools to fully understand our vulnerabilities or exposures. Now, with these solutions in place, we have a clear picture of our risk and the ability to address it before it becomes a problem.”** — Global Chief Information Security Officer, Global Manufacturing Company

### 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)

