SOLUTION BRIEF

RAPID7 LABS

Proprietary Cybersecurity Intelligence, Threat Data & Research

In an era of escalating cyber threats, staying ahead of adversaries requires more than just advanced tools—it requires the latest intelligence and collaborative insight.

Standing at the forefront of cybersecurity innovation, Rapid7 Labs provides teams with a community-driven approach to security with open-source tools and research-informed, curated intelligence to help you identify, assess, and mitigate threats more effectively.

Behind the Scenes
How Rapid7 Labs Delivers Intelligence

Rapid7 researchers gather real-world threat intel

Threat intelligence is gathered via:

- Proprietary research projects Project Lorelei & Project Sonar
- Incident Response engagements
- Commercial threat feeds
- Strategic government and industry partnerships
- Rapid7 open-source communities like Velociraptor and AttackerKB

Data analysis and content development

Our team of research experts:

- Leverage AI and ML to analyze threat data
- Conduct zero-day, ransomware, malware, APT, and other threat research
- Develop vulnerability and detection content

Intelligence delivered via our products & services

Expert intel provides customer & the Rapid7 services team with:

- The ability to better uncover threats and prioritize risks
- Enhanced threat detection
- Proprietary research reports and high-priority vulnerability analysis (Emergent Threat Response blogs, emails)
- Pro editions of open-source software like Metasploit
- Actionable threat intelligence for proactive defense, delivered via Intelligence Hub

Learn from—and contribute to—leading open-source communities & projects

We're committed to building a more secure future by fostering free, open-source communities and projects that unite insights and expertise from across the security industry.

- **Metasploit:** Simulate real-world attacks and gain unparalleled access to the latest exploits through **Metasploit**, the most trusted and expansive exploitation framework available.
- **AttackerKB:** Discuss, analyze, and expand your knowledge of conditions and characteristics of critical vulnerabilities being exploited in the wild.
- **Velociraptor:** Hunt for indicators of compromise, collect forensic evidence, and continuously monitor endpoint event data using Rapid7's advanced digital forensic and incident response (DFIR).
- **Project Sonar:** Access global exposure insights into common vulnerabilities through ongoing scans and analysis of public-facing internet assets.
- **Project Lorelai:** Stay ahead of threats with real-time intelligence from Rapid7's globally distributed honeypot network, which identifies potentially malicious inbound connections.

Stay ahead of emerging threats

Rapid7 Labs' Emergent Threat Response (ETR) team delivers fast, expert analysis and first-rate security content for the highest-priority security threats, enabling Rapid7 customers and the broader security community to assess their exposure and act quickly. Depending on threat severity, the ETR program provides mitigation guidance through a range of channels:

- **Blog post** summarizing the threat, Rapid7's perspective on impact, mitigation recommendations, and Rapid7 customer information
- **Proactive customer communications**, including customer emails, in-product notifications, and managed customer outreach from Customer Advisors
- **Prioritized vulnerability checks** to allow InsightVM and Nexpose customers to assess their exposure to the threat
- **New detection content** for InsightIDR and Managed Detection & Response customers
- **AttackerKB analysis**, delivering a full root cause analysis of the vulnerability in AttackerKB, with mitigation information and intelligence on attack likelihood

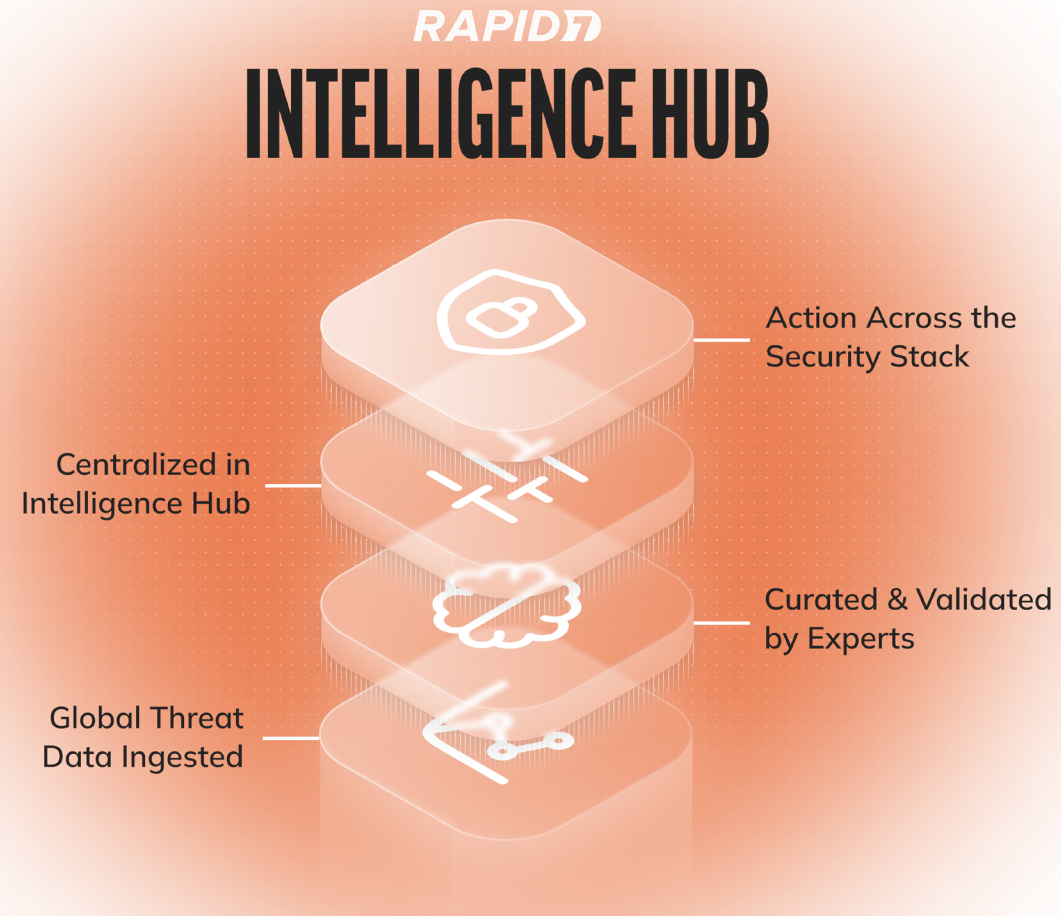
You guys are always providing the best content out there, letting us know, 'These are the biggest vulnerabilities that are out there. Make sure that you're patching this right away. This just happened. There's this zero-day threat that just came out."

Chris Hippensteel, New Resources Consulting's Director of IT

Intelligence Hub: Safeguard your organization against emerging vulnerabilities and threats with curated, actionable intelligence

2024 saw over 40,000 published CVEs and an average of 14 publicly-claimed ransomware incidents per day—an impossible number of vulnerabilities and threats for organizations to keep up with. Security teams need visibility into the risk signals relevant to their specific organization to ensure they stay safe against rising threats—**enter Rapid7 Intelligence Hub.**

Intelligence Hub delivers high fidelity, actionable threat intelligence with significantly less noise than traditional Threat Intelligence Platforms (TIP). Infused with intelligence from Rapid7 Labs proprietary threat and vulnerability research and community-driven tools, teams can easily focus on the most meaningful risk signals and take high priority actions (like patching systems with vulnerabilities that are being actively exploited in the wild) to stay ahead of critical threats most relevant to their organization.

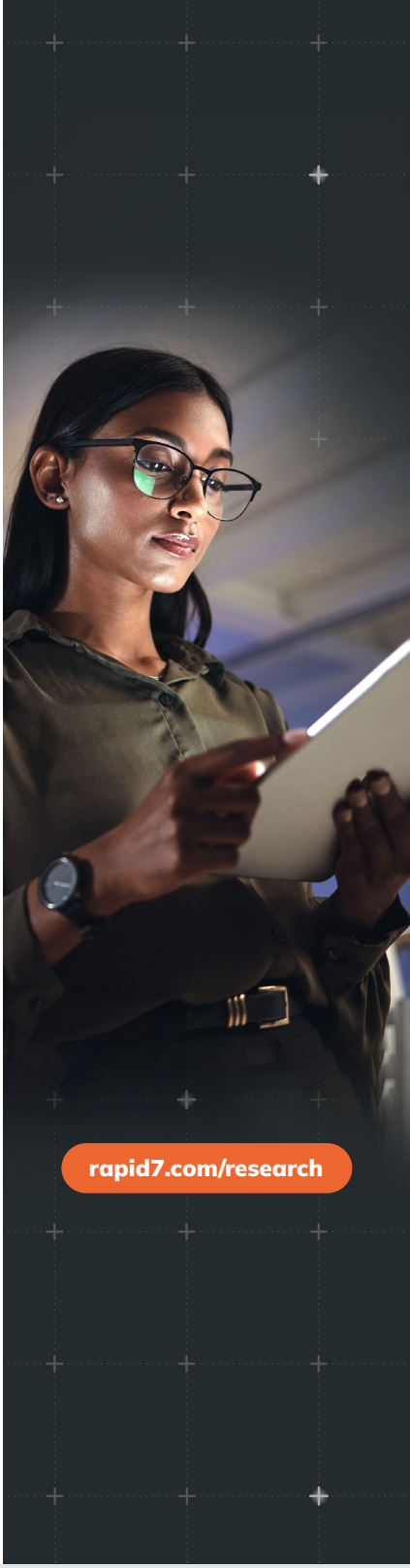


Fortify your defenses with our proprietary research findings

Our expert researchers dig into the latest data across the security landscape to bring you crucial insights into attacker intelligence trends and practical guidance. Rapid7 customers benefit directly from this intelligence within products like InsightIDR, InsightVM, and Exposure Command, as well as through Managed Detection and Response services, where insights support Rapid7 SOC analysts in threat hunting and incident response.

However, our research **extends beyond supporting solutions for our customers**. Rapid7 Labs research reports are free to all, supporting the greater security community by providing access to key findings and takeaways to keep their organizations safe.

RAPID7 LABS ISN'T JUST A SUITE OF TOOLS AND RESOURCES— IT'S A COLLABORATIVE APPROACH TO CYBERSECURITY.



rapid7.com/research

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

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact