

Medium Enterprise Wholesale Distribution Company

Introduction

This case study of a medium enterprise wholesale distribution company is based on a February 2022 survey of Rapid7 Managed Detection and Response (MDR) Services & Solutions customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.



“We don’t have to worry about piecing together solutions anymore and then try to find time to dig through the findings that those solution require. It’s valuable that we have a team of security experts and tools reviewing our environment rather than our small team trying to do so in our spare time.”

“Without Rapid7 MDR, our team would not be able to serve the business properly or feel as confident that our systems are protected as they are with Rapid7.”

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Rapid7 Managed Detection and Response (MDR) Services & Solutions:

- They decided to adopt a managed detection and response solution because:
 - They had no existing D&R Program
 - They didn’t have a large enough team to do it in-house
 - They didn’t have the right technology
 - They didn’t have the resources/budget to do it in-house
 - They were unable to keep pace with organization’s security needs
 - They needed expert support and guidance
- Confirmed that prior to implementing Rapid7 MDR, they had approximately 5 dedicated FTEs as part of their organization’s in-house cybersecurity team.

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
Medium Enterprise

Industry:
Wholesale Distribution

Use Case

- The criteria most important in their decision to select Rapid7 MDR was:
 - Team augmentation
 - Technology stack in use
 - Investigation capabilities
 - Containment/Incident response
 - Proactive threat hunting
 - Correlation and triage of alerts
 - Threat intelligence
 - Visibility and reporting
 - Cybersecurity expertise
 - Forensics
 - Cost/ROI
 - IR Automation

About Rapid7 Managed Detection and Response (MDR) Services & Solutions

Rapid7 is advancing security to accelerate innovation. Learn how the MDR service provides round-the-clock expert monitoring to defend against threats and stop attackers in their tracks at rapid7.com/mdr.

Learn More:

[!\[\]\(bff896c19919791b89ab521f039b410a_img.jpg\) Rapid7](#)

Results

- Aspects of Rapid7 MDR most impactful to their organizations’ security success:
 - 24 × 7 × 365 SOC team
 - Automated attack containment provided by MDR Active Response
 - Predictable, asset-based pricing
 - Ability to pivot to engage Rapid7 in Incident Response if breached
 - Proactive threat hunting
- They said “Our detection and response program has substantially improved since partnering with Rapid7 MDR.”
- How they rate the following capabilities based on experience with Rapid7 MDR:
 - SOC Expertise: Excellent
 - Technology: Excellent
 - Threat detection: Excellent
 - Incident Response: Excellent
 - Reporting: Excellent
 - Customer Advisor Guidance: Excellent
- Since we’ve implemented Rapid7 MDR, our team has:
 - Spent less time doing investigations
 - Improved their Mean Time To Detect (MTTD)
 - Improved their Mean Time To Respond (MTTR)
 - Received less false positives
 - Had more time to focus on other security initiatives
 - Had more time to focus on professional development/skills
 - Improved their coverage outside the 5x8 work week
 - Have improved our overall security posture
 - Have been able to engage more with the business