RAPID7 INSIGHTIDR CASE STUDY

Rapid7 InsightIDR Case Study: Medium Enterprise Retail Company

Introduction

This case study of a medium enterprise retail company is based on an October 2021 survey of Rapid7 InsightIDR customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> "InsightIDR has given us visibility across multiple security vectors that we did not have before."

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Rapid7 InsightIDR:

- Difficulty identify cyber security threats on endpoints
- Lots of jumping between different tools; leveraging multiple tools to look at different security telemetry
- Dealing with many blind spots across our environment
- Challenged to satisfy compliance and regulatory requirements around log retention and monitoring

Use Case

The key features and functionalities of InsightIDR that the surveyed company uses:

- User Behavior Analytics (UBA)
- Endpoint Detection and Response (EDR)
- Centralized Log Management
- Investigations and Incident Response
- Threat Hunting
- File Integrity Monitoring (FIM)

This organization leverages InsightIDR as both their SIEM and XDR.

They have deployed the Rapid7 Insight Agent across 76% – 99% of the assets in their environment. Outcomes realized by leveraging the Insight Agent with InsightIDR:

- Improved endpoint visibility
- Accelerated detection of targeted or compromised assets
- Accelerated time to contain threats on the endpoint

Results

The surveyed company achieved the following results with Rapid7 InsightIDR:

- Since they started using InsightIDR, they said that Threat detection and response is greatly improved.

The surveyed company agreed that InsightIDR helped them to:

- Level up and advance security program
- Greatly improve team efficiency

Since adopting InsightDR, they stated that they were able to reduce:

- Team time to address an incident by 50% or more
- Mean time to respond (MTTR) by 50% or more
- Mean time to resolution or containment (MTTC) by 50% or more
- Employee downtime as a result of incidents by 0-10%
- Occurrence of false positives by 0-10%

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:
Retail

About Rapid7 InsightIDR

Rapid7 is advancing security to accelerate innovation. Learn how our Insight Platform delivers shared visibility, analytics, and automation at www.rapid7.com.

Learn More:

Rapid7

Source: TechValidate survey of a Medium Enterprise Retail Company

Validated Published: Dec. 6, 2021 TVID: B92-EDA-E75

Research by TechValidate by SurveyMonkey