respond

Respond Analyst Business Case

Table of Contents

The exponential growth in security-relevant data coupled with the ongoing challenge of finding training and retaining skilled security analysts to monitor and respond to that data creates a critical and vexing problem for security organizations.

Innovative Security Operations teams are evaluating Artificial Intelligence, Machine Learning and other modern technologies to mitigate risk by:

1) Increasing the coverage of security data analyzed
2) Better utilize their skilled and highly paid security resources

Respond Analyst provides an out of the box solution to effectively eliminate the need for security analysts monitor and analyze high volume, low signal alerts. As a software-based, expert system it applies consistent and complex analysis across multiple data sets.

How does the Respond Analyst Help You Reduce Detection to Response Time?

- Enable 7x24 networking monitoring and analysis without staffing a security team and doing so at a fraction of the cost of an MSSP.
- Add Automation to an existing Security Operations Centers, re-assigning skilled security analysts to hunting and investigating activities.
- Modernize and re-energize a SIEM workflow.

July, 2018

Working as a fully-trained, highly-skilled security analyst; Respond Analyst is a software application that works just like a skilled security analyst, providing a transparent explanation of why each incident is prioritized, along with escalation rationale. And unlike human security analysts, evaluates incoming data as it streams.

Respond Analyst provides a quick ROI because it is a pre-built expert system that works right out of the box, ready to process output from various security sensors with an initial accuracy rate of over 87%. Respond Analyst adapts to your company's environment and continually learns about your risk profile and what's critical to your business. More importantly, the feedback from your security teams will allow Respond Analyst to improve accuracy rates over a very short period of time.

Why we built Respond Analyst

Today it's clear that human security analysts are not physically capable of monitoring hundreds of thousands of events with the goal of protecting an organization from a malicious attack. A common but failed strategy is to attempt to filter data, using rules, to match analyst capacity. Or worse, ignore entire sets of data altogether. Both of these approaches leave organizations at risk. The fact is, the data that is filtered out is often relevant and can vastly reduce the time between detection and response.

With our team of experienced AI engineers and software developers, we took a step back and approached the problem from a different perspective. We asked ourselves, is it possible to teach software to emulate the judgement, reasoning and decision-making capability of the most skilled security analysts? And, if so, could we apply that automated capability to incept millions of alerts, as they stream?

The answer was just as clear as the problem. Yes…we can, and so we did.

Respond Analyst is not a detection product, case manager, an automation platform, nor a SIEM that requires management and maintenance. It's a complete solution, right out of the box. Respond Analyst doesn't interfere with but utilizes all of your technologies and acts as a decision-making partner for your security team – whether you've got one or fifty.

Technology and Implementation

At the core of Respond Analyst is Probabilistic Graphical Optimization (PGO™). PGO was developed by Respond Software's security experts and data scientists to analyze all network events, evaluate malicious attacks and determine which incidents should be investigated. PGO utilizes the most critical variables a SOC analyst considers relevant and decides if an event is malicious and actionable.

PGO is a multi-layered technology developed at the unique intersection of applied mathematics, security expertise and knowledge, and proprietary algorithms. With machine-level scalability, PGO utilizes all three of these elements to monitor, analyze, and determine which events are malicious across the organization's entire infrastructure. Through continuous learning and adaptation to an organization's environment, PGO becomes more efficient at prioritizing events and making actionable decisions. It is purpose-built to emulate the decision-making process of an experienced security analyst. PGO is foundational to Respond Analyst decision models, delivering efficient and effective security.

Security Architecture

Respond Software's enterprise-grade architecture framework is comprised of multiple layers to ensure your company's sensitive data is secure and confidential. Consisting of fundamental infrastructure specifications, data encryption and Respond's tokenization schema - each component plays a pivotal role in the security of Respond's architecture.

- Respond's cloud is hosted on top of AWS to provide the scalability to meet any organization's needs. Respond has numerous certificates of compliances with AWS:
  - Cloud Compliance – AWS
  - SOC Compliance – AWS
  - Respond Datacenter - PCI Compliant
- Everything within Respond Software is encrypted, whether the data is in-flight or at rest; Public Key Infrastructure encryption allows data to be securely exchanged over various networks. Respond encrypts data from your site to the Respond cloud. Mutual Authentication is used to validate and identify the communication between Respond and the client.
- Tokenization is another key component of Respond's security architecture. Regardless of the data protocol, everything that is sent to the Respond Cloud is de-identified, meaning we tokenize all sensitive data before it's in transit. The ability to look up a token value is stored securely on your organization's premise. One of the most powerful aspects of Respond Analyst is the Decision Engine with the capacity to process all these decisions with de-identified data, allowing economies of scale and compliance with corporate policies.

Respond Analyst at Work

Here are some real-world examples of the Respond Analyst at work at U.S. companies. Contact your Account Team for specific customer references.

Fortune 500 Company

- Challenge: Upcoming business expansion requires additional staffing and monitoring capability. Existing solution produces a significant amount of inaccurate escalations resulting in wasted time and energy
- Results: Ability to scale to meet increased data volumes, with accurate and consistent incident escalation.
  - 242,246,182 alerts analyzed per month
  - 12 escalations scoped and prioritized
  - 92% accurate verified by incident response

Financial Technology Provider

- Challenge: Spending a significant amount of time, money and resources to deploy and configure SIEM technology, while maintaining compliance.
- Results: Recognized significant savings in engineering resource costs to building and maintaining SIEM content, while adding more capacity and efficiency.
  - 21,274 events analyzed per hour
  - 1.5 security Analysts re-assigned to new projects
  - 50 hours eliminated each quarter

Large Communication Network Provider with an MSSP

- Challenge: MSSP is continually failing to identify critical incidents and while escalating a high-number of false-positives. MSSP is unable to analyze the high-volume of data, which has forced them to tune down devices and signatures, greatly reducing visibility into their environment. Additionally, MSSP did not provide monitoring during off-hour and weekends.
- Results: Respond Analyst's unlimited virtual analyst capacity provides greater visibility into events and higher-fidelity incidents. RA greatly reduced false-positive escalations and allows the organization to better utilize customer time. Ultimately replacing their existing MSSP with Respond Analyst.
  - 284k IPS events analyzed
  - 4 incident escalations from Respond Analyst
  - Equivalent to ~12 analysts working 24x7 over 60 days

Calculating Return on Investment

Our ROI calculator factors in multiple variables that are unique to each Security Operations Program. Reach out to your account manager to discuss Respond Analyst will impact your business.

Awards/Recognition

- Gartner Cool Vendor 2018 - Security Operations and Vulnerability Management ↗
- Cyber Defenders 2018 — CBInsights ↗
- 20 Cyber Security Companies to watch in 2018 — eSecurity ↗
- CyberSecurity Ventures Top 500 CyberSecurity Companies — CyberSecurity ↗

Customer Quotes

"We need more than yesterday's SOC. Respond can enable capabilities that vastly increase the comprehensiveness and efficacy of our efforts."

Kirsten Davies, CISO, Absa / Barclays Africa Group, Ltd.

"Good analysts keep the SOC operating at peak efficiency – but it is tough to find and retain them. Respond provides an always-on, expert-in-a-box."

-Izak Mutlu, former CISO, Salesforce.com

Respond Software Team

When it comes to selecting IT security solutions, you need to partner with teams that you trust to understand the real challenges facing security teams and deliver on what they sell.   Our experience comes from decades of security operations– from performing individual security operations assessments to leading the design, training and hands-on management of security operations teams at companies such as IBM, Shell, Sony, Walmart, Vodafone, and close to 150 others. We balance that with experience and knowledge in building industry-leading enterprise software solutions.

Our combined Security Operations Experience includes:

- 100+ years of security experience
- 35+ Complete SOCs built (people, process & technologies)
- 150+ SOC Engagement
- 1,000+ Security Analysts Trained
- 10,000 investigations (40+ counter nation-state investigations)

Our collective product experience includes commercially successful and marketing defining software solutions from:

ArcSight
Borland
Fortify Software
HPE
IBM
Oracle
Pure Software
Siemens

The company is led by experienced domain leaders, supported by a first-class Board of Directors and Advisory Board and backed by two respected Silicon Valley Venture Firms.

Leadership Team

Mike Armistead, Co-founder and CEO

Chris Calvert, Co-founder and VP Product Strategy and Research

Robert Hipps, Co-founder and VP of Engineering

Steve Dyer, CTO

Chris Triolo, VP of Customer Success

respond

Please contact us at: respond-software.com/company/

July, 2018