RAPID7

QUICK-START GUIDE

Driving Immediate Value with a Cloud SIEM

Explore how modern SIEMs are designed to get you deployed (yes, really) in no time.

Gartner predicts that in less than 5 years, 80% of SIEM solutions will have capabilities that are only delivered via the cloud—up from 20% previously.

“

INTRODUCTION

Detection and response is a critical piece in an ongoing journey to improve your security posture. As the threat landscape grows increasingly complex, an effective detection and response program will help you recognize threats early and minimize the likelihood of attacker success. For many SIEM vendors, solving these complex problems requires a complex solution. For us, there's a better way.

Yesterday's SIEMs were not built for today's hybrid, remote, and cloud environments. Setting up a traditional SIEM in your current tech stack can feel like navigating an endless maze of hardware, data sources, workarounds, and different interfaces. This complexity inherently contradicts what the actual goal of a SIEM should be: a focus on finding and eliminating threats. As a result, the promises most traditional SIEMs make are never realized, because these solutions are so complex they're never fully deployed (hello, shelfware).

We understand how important it is to have technology that you can actually deploy, that your team can actually use, and that will drive tangible ROI for your company and security program—especially when it comes to detecting and responding to threats.

A natively cloud SIEM, like Rapid7 InsightIDR, is purpose-built to get your team up and running quicker than ever before, while continuously up-leveling your capabilities as your needs and maturity evolve, whether you manage it or we do. Through faster implementation times and intuitive delivery of critical information, you'll see immediate value in days, not weeks or months. Let's look at how.

STEP ONE

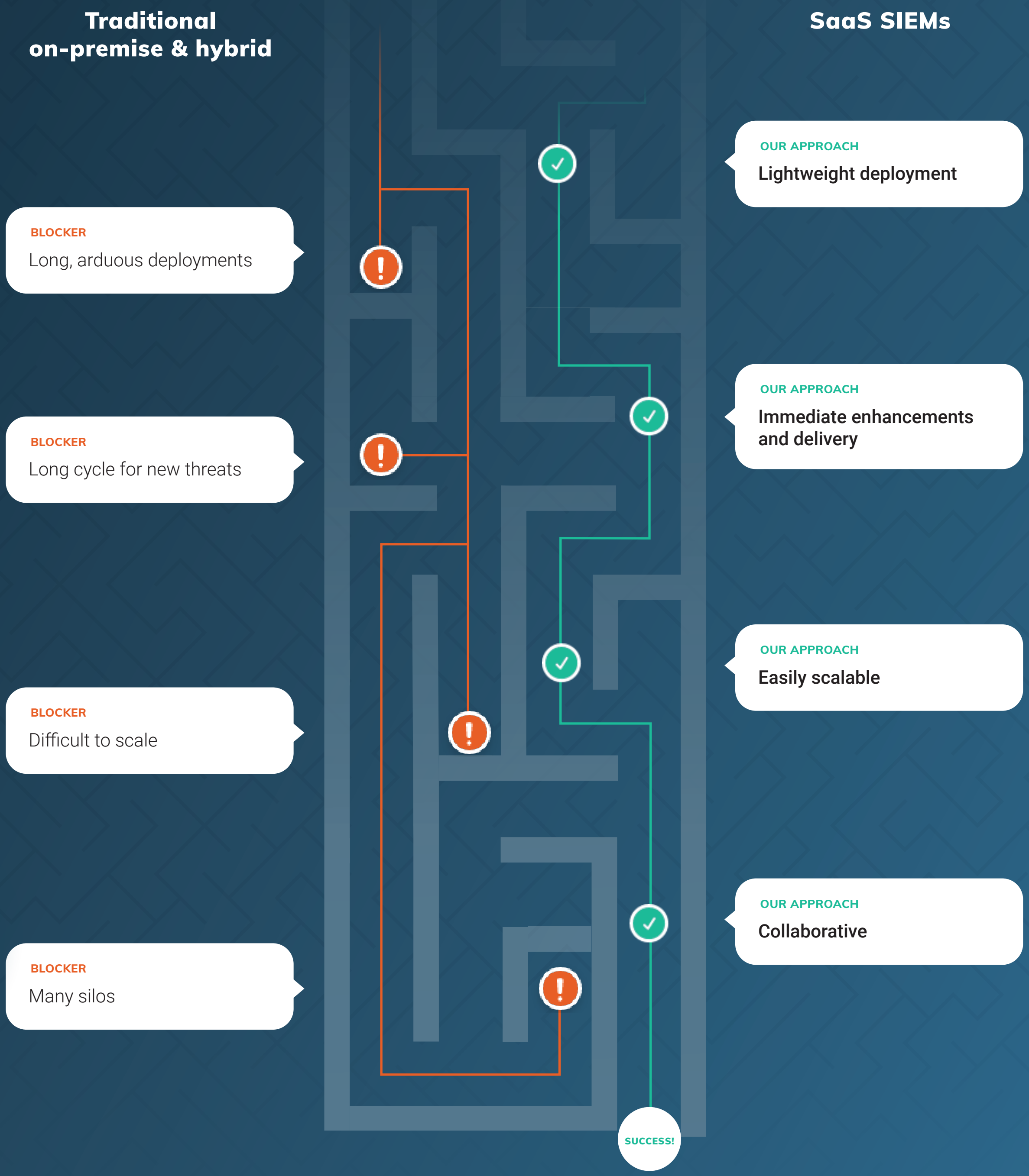
Deploy

No matter how you spin it, setting up a SIEM takes thought and time. But on the spectrum of setting up a traditional SIEM versus a modern SIEM, your efforts will be rewarded much faster by going straight to the cloud. A SaaS delivery model eliminates the arduous deployments and hardware updates that bog teams down, and it's more agile to scale with your organization as it evolves. Additionally, data storage costs are more predictable. Just be sure to evaluate your SIEM provider and their cloud hosting methods, to ensure you'll have the backups, controls, and other requirements you need.

As your environment changes—with new endpoints, domain controllers, cloud services, spikes in remote workforces, and more—a cloud SIEM like InsightIDR will continue to scale, providing the attack surface coverage and machine power required to keep up with modern environments. What that means for you: resiliency through change, with fewer dead ends.

> "Compared to the [previous] SIEM solution, I think we're saving a lot of time. A traditional SIEM platform would take five or six guys to get the job done."

Joost Dubbelman, Voogd & Voogd



Traditional on-premise & hybrid

BLOCKER
Long, arduous deployments

BLOCKER
Long cycle for new threats

BLOCKER
Difficult to scale

BLOCKER
Many silos

SaaS SIEMs

OUR APPROACH
Lightweight deployment

OUR APPROACH
Immediate enhancements and delivery

OUR APPROACH
Easily scalable

OUR APPROACH
Collaborative

STEP TWO

Ingest Data

Chances are, your modern tech environment includes pieces that didn't even exist when traditional SIEMs came around. Networks, endpoints, remote employees and offices, cloud applications and hosting, and more have pushed the limits of what a SIEM can (and should) be. They've also expanded the attack surface, creating new areas that organizations need to monitor to keep ahead of threats.

Traditional SIEMs focus on log ingestion alone and typically place the burden of figuring out (1) what data is most relevant to look at for recognizing security threats, and (2) how to get it into their product on the customer.

Cloud SIEMs like InsightIDR are designed to bring together data from disparate sources, so you can view critical information in one solution. First things first: take inventory of the tools and services you'll need data from, and the connectors available. This is where cloud solutions make life easier.

	TRADITIONAL BLOCKERS	INSIGHTIDR
Log Data	Data is stored on-premise, where you have to maintain additional infrastructure and ever-growing storage to accommodate network needs.	Collectors compress log data and push it to the cloud. It's then normalized and attributed, so you can run advanced queries and correlate user activity.
Remote Users & Assets	Manually monitor firewall logs, VPN logins, and network activity.	The Insight Agent provides real-time visibility across Windows, Mac, and Linux assets—no matter where they are.
Endpoint Data	On-premises agents are heavy and need to be installed for every endpoint device.	The lightweight Insight Agent centralizes and monitors data in the cloud.
Network Data	Manually maintain and monitor: firewalls, packet inspection tools, DNS tools, switches, routers, and more.	Network Sensors collect data from network aggregation points, like core switches. The Sensor captures raw network flow data and extracts rich medata.
Cloud	Unable to view cloud environments	Hosted in the cloud and connects to numerous third-party cloud solutions.

Need more resources or expertise?
Learn about Managed Detection and Response.

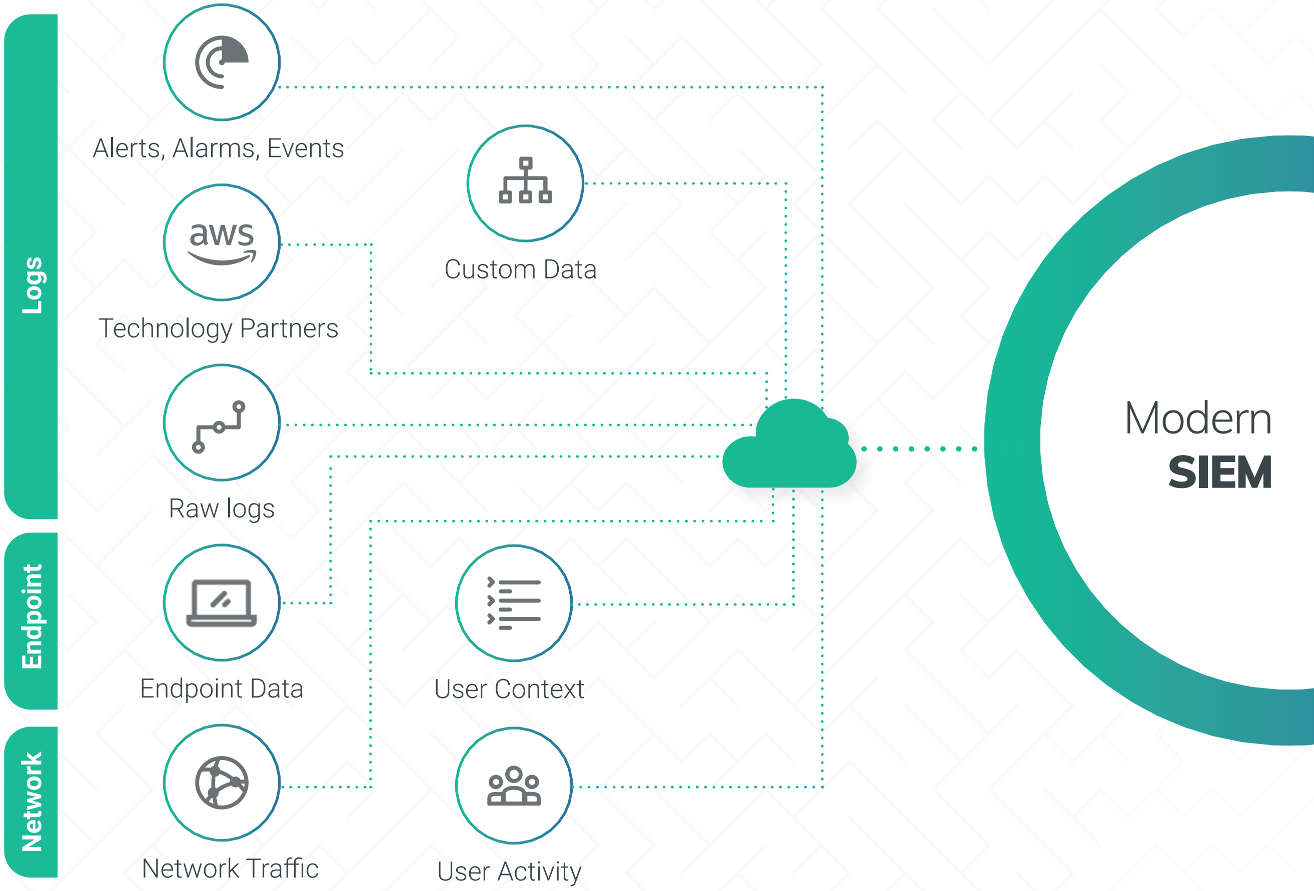
> “Within a week we had more event sources and more data flowing in than we could have imagined. We currently ingest more in three days than we did in three to four months previous in our traditional SIEM model.”

Brett Deroche, Amedisys

✓ See why we were named a leader in the 2020 Gartner Magic Quadrant for SIEM

READ THE REPORT

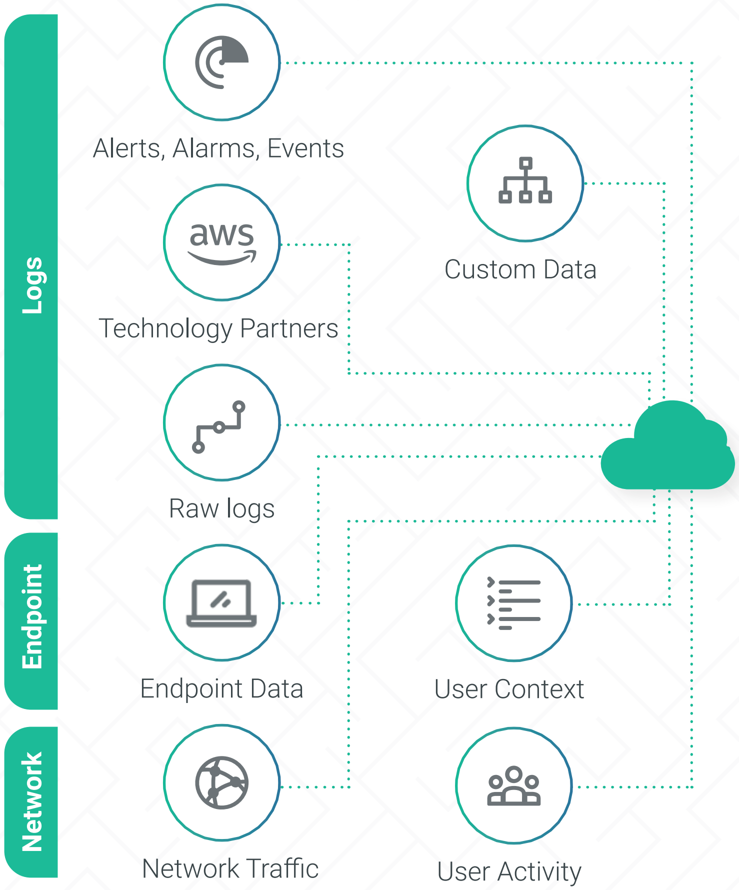
Data Ingestion Environment



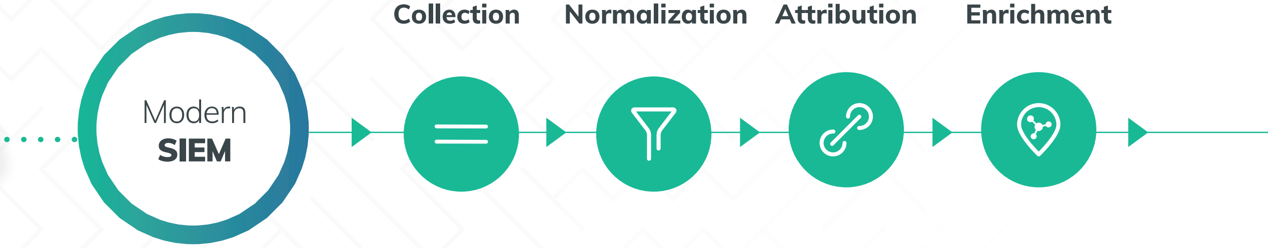
Transform Data

Data alone means nothing. It offers no real visibility into your environment until it's transformed into actionable information. There are two ways to transform your data: manually and automatically. With traditional SIEMs, the burden of making data useful is placed on the user; it would be a manual process to configure every event source, log, network switch, etc.

Most modern SIEMs streamline this process by ingesting and transforming data at scale. A SIEM like InsightIDR does even more to go beyond just log collection and management. Once InsightIDR collects data, it's normalized, attributed to users and systems, and then enriched. This approach structures the data and analytics for investigations, empowering analyst visibility and action. With just a few foundational event sources set up, you'll immediately see impactful takeaways.



Modern Data Transformation



> “SIEM implementations often fail to deliver full value — not only due to “broken tools,” but also due to broken processes and practices. SIEM solutions are not a set-and-forget type of security technology.”
>
> Gartner

STEP FOUR

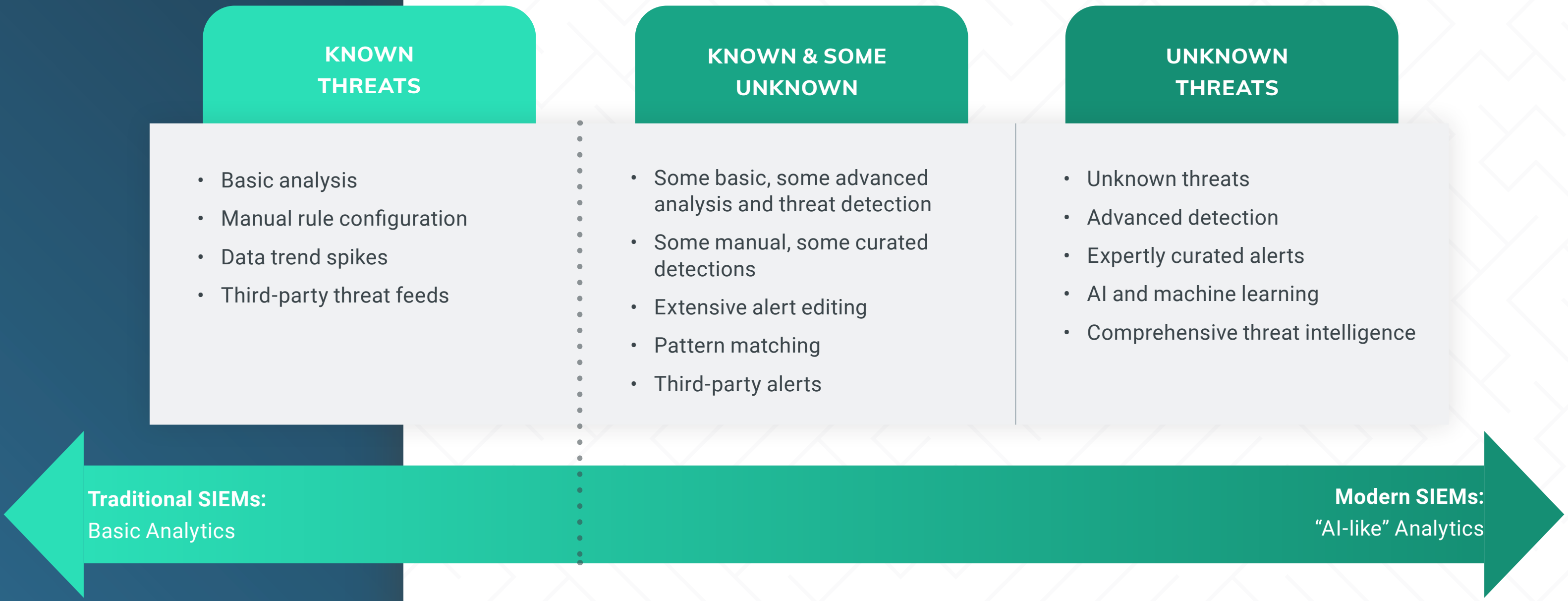
Cloud Analysis

Once your data is in a usable format, it's time for analysis. Traditional SIEMs focus on reading data to find known threats, and they require analysts to manually filter and configure the settings based on what users or assets "should" do. This includes basic analytics, pattern-matching, and similar tactics for finding predictable behaviors. The problem? Today's threat landscape is anything but predictable.

To combat this, modern SIEMs have the analytical and compute power needed to look for more advanced and elusive threats. Combined with out-of-the-box detections, visual timelines, and advanced behavioral analytics, users will view and analyze data holistically, resulting in greater context and visibility into your environment.

At Rapid7, we take it even further. We combine the power of our threat intelligence community, Managed Detection and Response analysts, machine learning, and additional filtering and data science to build on traditional out-of-the-box detections and baseline user behavior. InsightIDR looks for further indicators of compromise, such as logging in from unknown domains as opposed to simply a different office location, to alert on true threats.

Threat Analysis Spectrum



KNOWN THREATS

- Basic analysis
- Manual rule configuration
- Data trend spikes
- Third-party threat feeds

KNOWN & SOME UNKNOWN

- Some basic, some advanced analysis and threat detection
- Some manual, some curated detections
- Extensive alert editing
- Pattern matching
- Third-party alerts

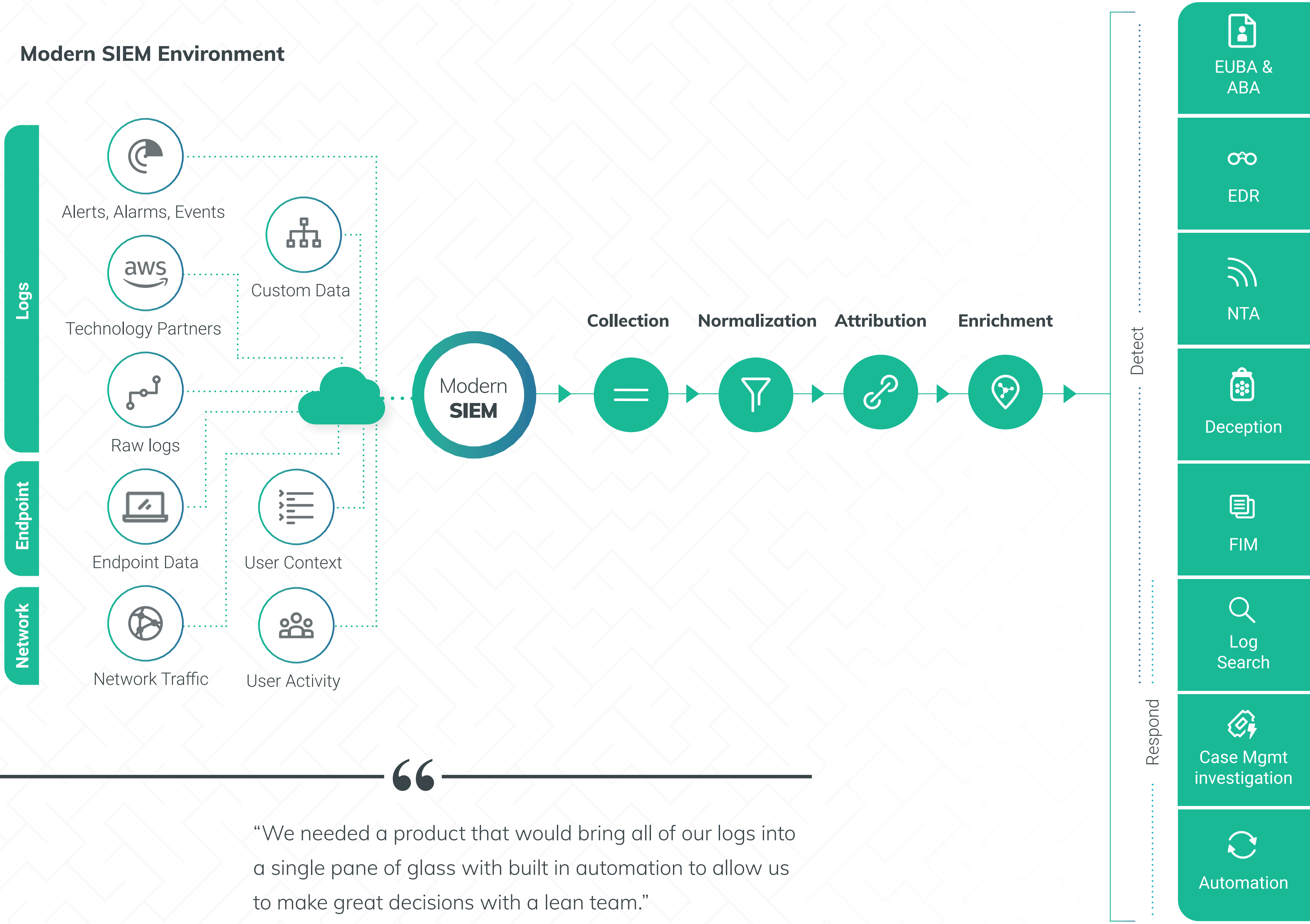
UNKNOWN THREATS

- Unknown threats
- Advanced detection
- Expertly curated alerts
- AI and machine learning
- Comprehensive threat intelligence

Traditional SIEMs:
Basic Analytics

Modern SIEMs:
"AI-like" Analytics

Modern SIEM Environment



> “We needed a product that would bring all of our logs into a single pane of glass with built in automation to allow us to make great decisions with a lean team.”

Sr. Cyber Security Engineer, via Gartner Peer Insights

LEARN MORE

About Rapid7 InsightIDR and Managed Detection & Response

Rapid7 is defining the complete approach to threat detection and response. By combining the most impactful components of our technology and services, we've developed a SIEM you can actually deploy, that your team can actually use, and that will drive tangible ROI for your company and security program.

Whether you're new to detection and response or you've outgrown your current model, we have the answer to your evolving needs. The **InsightIDR** ecosystem is built to help you get up and running quicker than ever, while continuously up-leveling your capabilities (whether you manage it, or our MDR team does). We've infused expertise from our SOC analysts and Rapid7's global threat intelligence network into our offerings. This streamlined approach ensures you can reduce attacker success, respond to events quickly and confidently, and advance your security posture.

Unlike traditional SIEMs, InsightIDR is natively cloud, meaning customers are deployed in days, not months. With expertise built into every step—from prescriptive event source collection wizards, to highly curated pre-built detections and intuitive UI—InsightIDR delivers actionable insights and tangible return on investment.

Don't just take our word for it.

Hear from your peers

HERE

Explore how fast you'll see value

FREE TRIAL

CONTACT MDR