insightIDR

Log Storage and Retention with InsightIDR and Managed Detection and Response

Answering Questions About Your Data

RAPID7

InsightIDR helps you detect and respond to all of the top attack vectors behind breaches by unifying your data, applying analytics, and giving you the power to directly respond. While we're focused on helping you find and stop malicious behavior as early as possible across the ATT&CK framework[1], InsightIDR's SIEM capabilities also give you full, centralized log management for search, dashboards, and compliance.

Rapid7 Managed Detection and Response (MDR) service combines InsightIDR with our passionate, veteran SOC teams to enhance your security maturity with hands-on 24x7x365 threat monitoring, hunting, and customized security guidance to move your environment from risk to remediation.

Keep reading to learn how you can escape the drudgery of managing, indexing, and interpreting mountains of logs with our thorough and secure approach to data collection.

Answering Questions About Your Data

What kind of data does the InsightIDR technology collect?

InsightIDR integrates with your existing infrastructure, ranging from network sources such as Active Directory, LDAP, and DHCP, to your remote endpoints, cloud services, and IaaS. This data is normalized, enriched, and correlated to the users and assets behind them, providing your team value across your incident response lifecycle. InsightIDR does not collect or require any of your customer data.

Do I need to purchase additional hardware to store logs with InsightIDR?

No. The logs from your existing network and security stack are collected through an on-premise collector and sent to Rapid7's secured Simple Storage Service within Amazon Web Services (AWS). AWS delivers a secure, scalable cloud computing platform with high availability, offering flexibility for us to build a wide range of additional layers of security for data at rest, in transit, and in use.

How is my data used within InsightIDR?

InsightIDR uses the data collected across your network to reliably detect earlier in the Attack Chain. All of the actions taken on your network are correlated back to the users and assets involved, enabling your team to detect stealthy attacker behavior such as the use of stolen passwords and lateral movement. In addition to the pre-built analytics in InsightIDR, you can also create custom alerts using a simple search query language.

With the SIEM capabilities in InsightIDR, any syslog can be ingested for use in log search and data visualizations, such as dashboards to measure and report on compliance.

[1] MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. You can learn more at: https://attack.mitre.org/wiki/Main_Page.

How long is the log data stored for?

For a standard InsightIDR subscription, any ingested logs are stored and available for search, visualization, and investigations for one year. This data retention time is entirely flexible; your subscription can be tailored to exactly meet your business and compliance needs.

With Rapid7 Managed Detection and Response, your logs are retained for audit, compliance, and search for 365 days in hot storage, 30 days cold storage with the standard subscription. Longer retention periods are available—just let us know your needs.

How is the data at rest protected?

Data is encrypted before it is pushed from the collector to the cloud. InsightIDR employs public key cryptography and challenge-response handshakes to ensure the security of your data and the integrity of the credentials entrusted to the platform. User credentials are encrypted with bcrypt; credentials to connect with your event sources are encrypted using RSA PKI (4096 bit keys). Other database contents are not encrypted at rest. Data is protected by strict access controls.

InsightIDR is designed as a multi-tenant application. Each customer's user data is isolated in its own individual database, preventing other customers from accessing your user data. As an additional safeguard, each customer's log data is tokenized using a unique UUID that walls the data off from other customers, isolating your company's data.

Can I have a separate, or backup copy of my log data?

Yes. While delivering the data to InsightIDR, you are welcome to generate copies of that log data to store on-premise or elsewhere as a backup.

How does Rapid7 ensure stability and redundancy with my data in InsightIDR?

InsightIDR is hosted in Amazon Web Services (AWS) for all data storage and processing for analytics. Rapid increases in CPU, memory, storage, and networking capacity are performed on demand to meet the scaling and performance needs of enterprise customers. We leverage AWS to guarantee backup, redundancy, and high availability. AWS has SOC1, 2 and 3 reports to attest to their backup methodology https://aws.amazon.com/security/. If needed, we can work with AWS to provide you with these reports.

On the Rapid7 side, we have carefully designed our network to build in redundancy, backup, and recovery capabilities. Our data centers have disaster recovery plans and their own risk assessments.

What is the Rapid7 licensing model for data retention and volume for InsightIDR?

InsightIDR is priced by total number of assets in your organization. This is in deliberate contrast to data volume, "consumption-based" pricing models. We've heard a lot of dissatisfaction from customers and security teams about data costs rising unpredictably (overages) and exponentially (huge upsells) over time. With InsightIDR, you get a transparent model that allows for consistent budgeting and no surprises. You aren't forced to choose between ingesting different types of security data due to prohibitive costs.

Should you have specific needs aside from data analysis for comprehensive threat detection and response, such as extended retention or anomalously large data volume, we can build a custom package to ensure those needs are met.

What is the definition of an asset for InsightIDR?

A billable asset is defined as a system that is monitored for activity. This includes servers, desktops, and laptops (physical and virtual), and any system with a static IP address. The per asset fee comes with an allocated data storage that meets 90% of all customer data volume needs. If needed, additional data can be purchased separately.

If I use Rapid7 Managed Detection and Response (MDR), can I still search and report on my data?

Yes. With your MDR subscription, your team is provisioned credentials to login and use InsightIDR. While our experts are monitoring and hunting across your network, you may use InsightIDR for log search, data visualization, and reporting. This combination means you're getting both managed detection, SIEM capabilities, and a bundled response plan in a single subscription.

What happens in the event of contract cancellation? Can the team get their logs back?

You own the data you collect—you control access to that data. If you opt to leave a Rapid7 service, you'll have the opportunity to collect and transfer any data possible to export. Should you request deletion of the data, we'll process that request within 14 days. For more, please visit www.rapid7.com/trust.

Learn More about InsightIDR

At Rapid7, we're obsessed with detecting intruders in your ecosystem. From our continued research from the Metasploit project, our red & blue teams, and collaborative research, we understand how attacker tactics, techniques, and procedures continue to evolve. For example, attackers are moving away from malware as stolen & default credentials are getting the job done. That's why we pioneered the User Behavior Analytics space and start with an approach of simple, but thorough data collection. Unify your existing data sources, then leverage the right analytics to provide your team with answers.

We understand you're getting too many alerts, incident investigations are a hassle, and you have an increasingly dizzying security stack. InsightIDR was built hand-in-hand with teams like yours to unify and augment existing technologies, reliably detect attackers, and prioritize your search. By combining SIEM, UBA, and EDR with your existing tools, you'll find intruders fast and meet regulatory compliance – no deployment headaches or data degree required.

RAPID7

If you have additional questions or are ready for next steps, contact us at sales@rapid7.com or +1-617-247-1717.

© 2018 Rapid7