insightIDR

Log Storage and Retention with InsightIDR

Answering Questions About Your Data

RAPID7

InsightIDR helps you relentlessly hunt threats across your environment by combining SIEM, User Behavior Analytics (UBA), and Endpoint Detection and Response (EDR) capabilities with your existing network and security stack. While we're obsessed with helping you detect and investigate intruders early in the Attack Chain, we can also help with your log centralization needs, whether it be for search and visualization, or to ensure you're compliant with the regulations for your business.

When storing your data in the cloud, it's natural – and important – to have questions. Read on to learn about our thorough and secure approach to data collection. Our goal is not to just give you confidence, but to give you answers.

What kind of data does InsightIDR collect?

InsightIDR integrates with your existing stack, ranging from network sources such as Active Directory, LDAP, and DHCP, to endpoint, cloud service data, and other existing security solutions. This data is normalized, enriched, and correlated to the users and assets behind them to provide your team answers during incident detection and investigation. InsightIDR does not collect 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 (S3) buckets within Amazon Web Services (AWS). AWS hosts 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.

How long is the log data stored/retained for?

With the standard InsightIDR subscription, 13 months. Ingested logs over that time window are retained and available for search, visualization, and investigations. Should you need a longer retention time, we can tailor a plan 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. During this term, any ingested logs will be available for search. For export functionality, Customer must stand up an S3 instance for logs to be transferred to. Upon connecting to the customer's S3 instance, all logs generated from that point forward will be available for export via the S3 instance.

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). Data is protected by strict access controls – each customer's log data is tokenized using a unique UUID that walls the data off from other customers, isolating your company's data.

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 SOC 1, 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 infrastructure to build in redundancy, backup, and recovery capabilities. Our data centers have disaster recovery plans and their own risk assessments.

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 log in 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 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?

If you opt to leave a Rapid7 service, you will have access to the platform until your end date. All data, including backups, will be deleted after 90 days. Should you request deletion of your data prior, we'll process that request within 14 days.

If you choose to retain Managed Services reports, you should download them from the Services Portal prior to the last day of service. Your final report will be delivered via secure email.

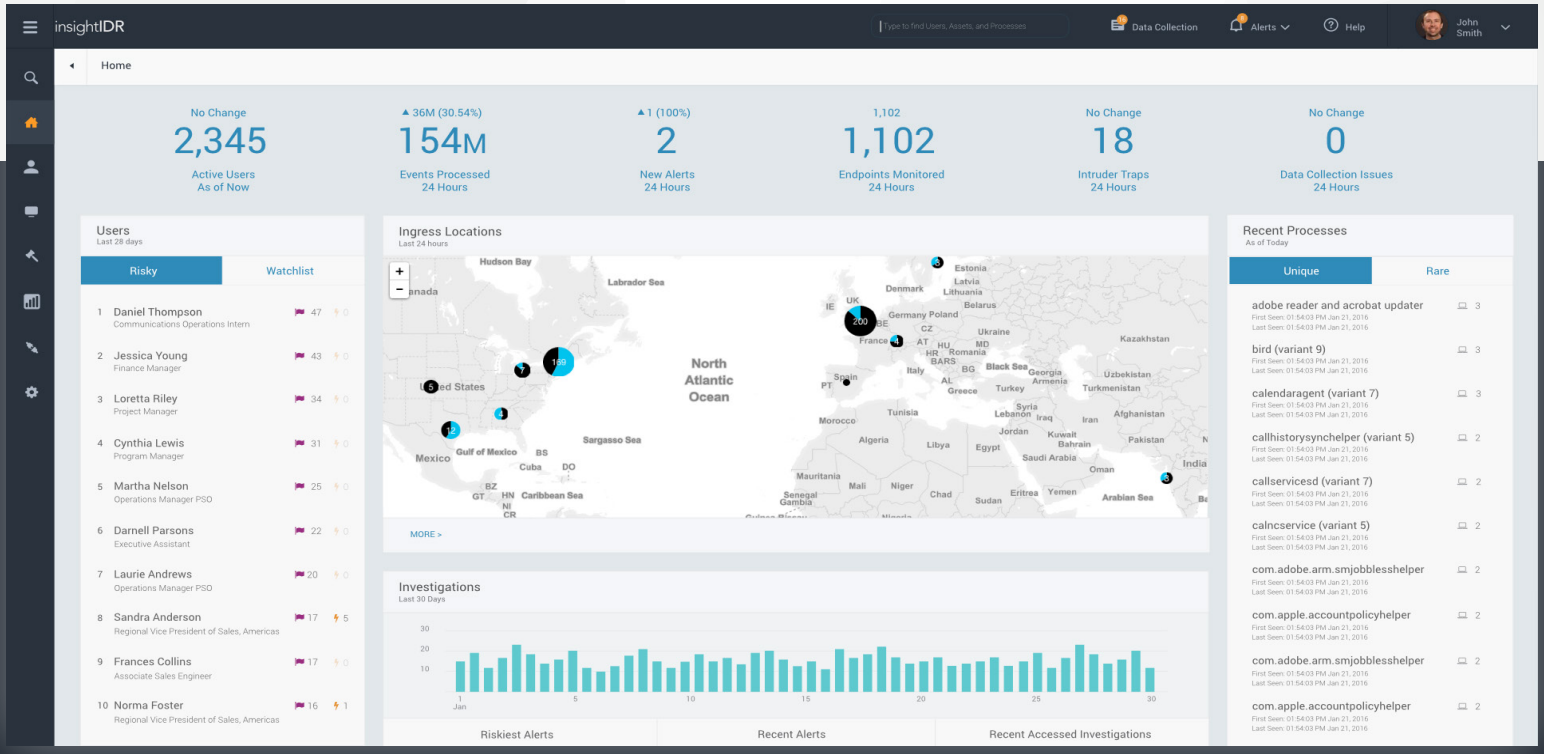
If you wish to retain your log data, you will need to have previously setup the S3 Archiving feature. This will carry out a daily backup of the log data ingested on that day. These backups are stored in an Amazon S3 bucket that you own. A retrospective export-on-demand option is not available at this time.

For more information about our data privacy policy, please visit www.rapid7.com/trust.

Learn More about InsightIDR

InsightIDR cuts through complexity and noise to accelerate detection and response with reliable alerts, high-context investigations, and automation. Powered by insights from our MDR, research, and threat intelligence teams, InsightIDR aggregates and analyzes data sources across logs, users, endpoints, and network to notify teams at the first signs of attack. 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.

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, NTA, 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.