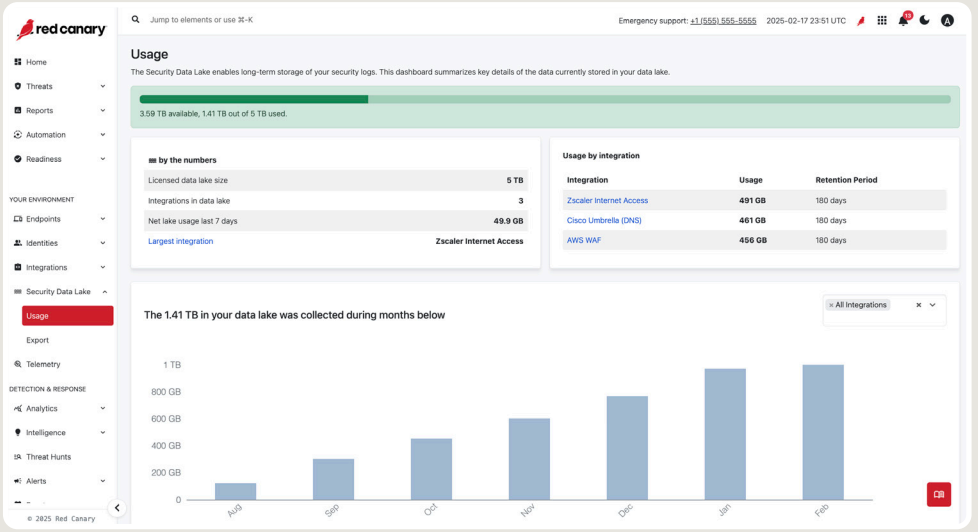
red canary

Red Canary Security Data Lake

Cost-effective storage that improves your security posture.

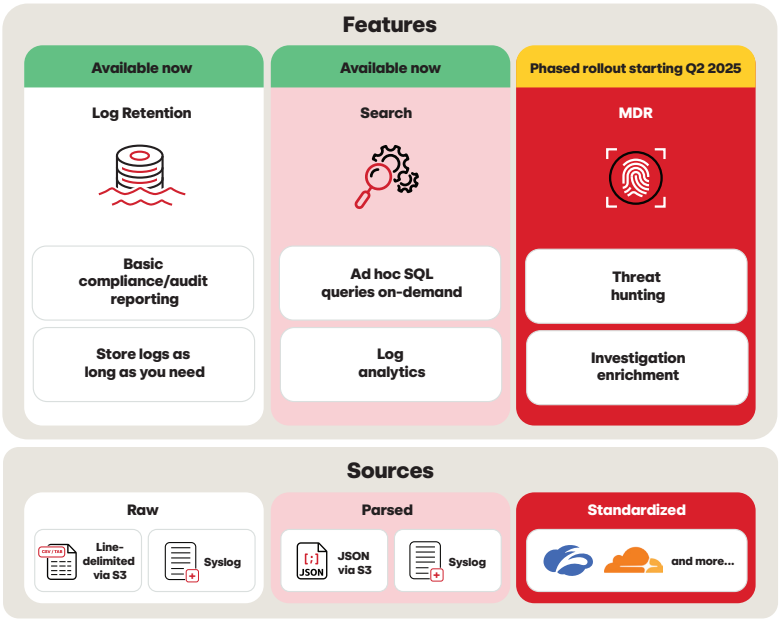
The challenge

Security leaders face tough tradeoffs when managing security data. Storing too much in a SIEM results means you're overpaying on infrequently searched, low-value data, while managing a data lake adds infrastructure headaches. You need a solution that reduces overhead and keeps data accessible at all times.



Capabilities

The Red Canary Security Data Lake provides cost efficient storage for data that your organization and Red Canary can simultaneously leverage for investigation. You send us your raw data—JSON strings, Syslog messages, anything that's line delimited that you can write to an S3 bucket—for any length of time specified by you. You can analyze that data today, and soon Red Canary will begin leveraging stored data during MDR investigations.



Reduce SIEM costs

Pay a fraction of SIEM storage costs for high-volume, low-fidelity data sources like firewall, DNS, and SASE logs. If a log source doesn't help you detect threats, don't pay a premium to store it.

Meet retention requirements

Prove to auditors that your data is retained and can be retrieved on-demand. If you need to export specific logs, you can do so at any time.

Investigate stored data

Ensure visibility into your data for your team's and Red Canary's investigations. Your team can flexibly filter, correlate, aggregate, and analyze their stored data, and our team can leverage the data as part of our MDR workflows.