OUR SERVICES

Expel MDR &
Security Data Lake

Cut costs while crushing your compliance goals

Your challenge

Meeting security demands while also keeping your CFO happy is a struggle for many security leaders. Storing high-volume data in your SIEM can be costly, but may feel necessary to meet long-term data storage requirements. If you are looking for a solution to lower storage costs while still keeping your data accessible for investigations and compliance purposes, we can help.

How we help

Expel and Sumo Logic have joined forces to bring you a unified solution: 24x7 expert-managed detection and response (MDR) paired with an affordable, scalable data lake—all under a single contract. Whether you're looking to cut costs by offloading lower-priority data from your current SIEM or just need a straightforward, budget-friendly solution for compliance and data retention, this solution has you covered.
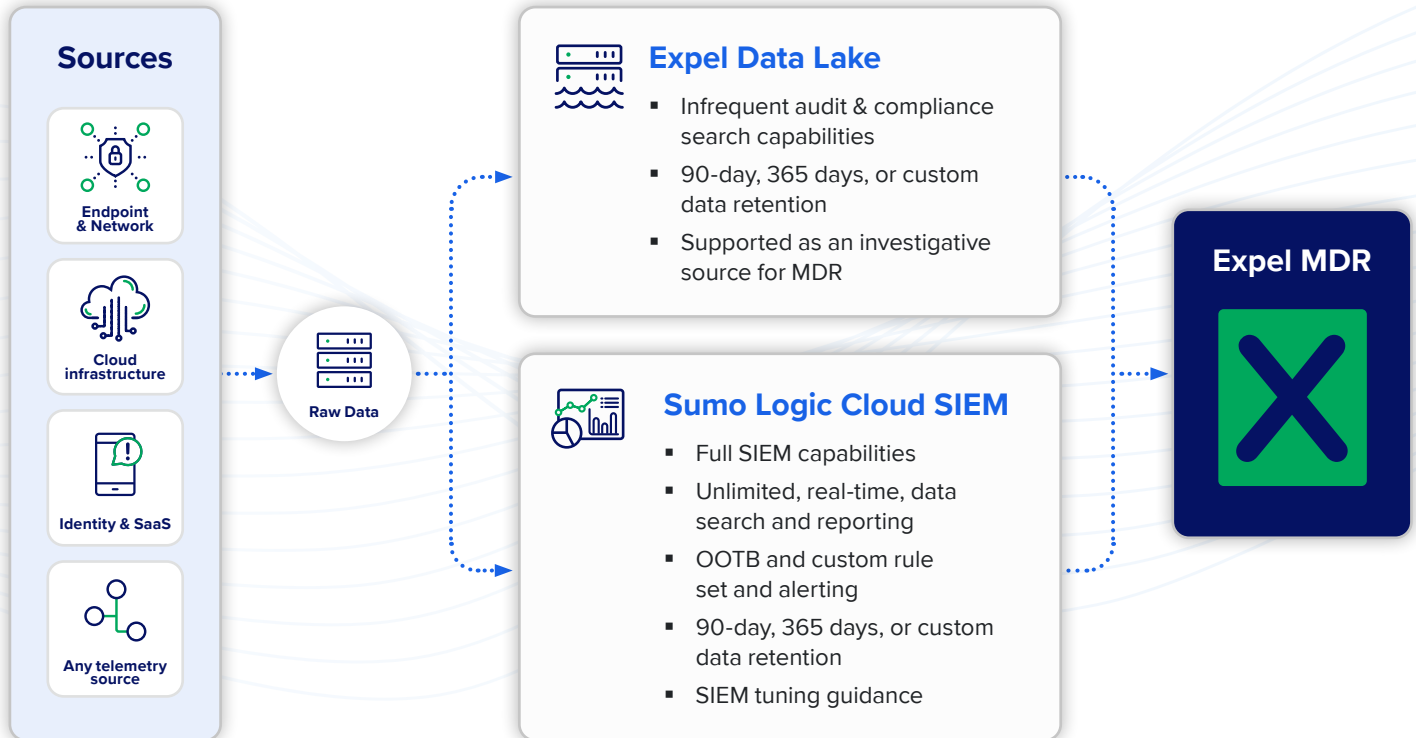
With our joint solution your data is readily available for audits and for Expel analysts to access as an investigation source. And lowering SIEM costs doesn't mean starting over with a new vendor. Expel can integrate seamlessly with your existing SIEM, while also giving you access to store low-fidelity data in a cost-effective data lake. Meanwhile, our expert analysts manage detection and response, boosting your team's efficiency and helping you get the most out of your security investments.

Trends driving data lake adoption

- **Increasing data volume**
  Organizations struggle with unsustainable SIEM pricing as log volumes and retention needs increase.

- **Rising data costs**
  It is getting more expensive to meet long-term data retention goals and satisfy audit and regulatory mandates.

- **Inadequate data availability**
  Maintaining readily available data for investigations and audits is expensive and cumbersome with traditional SIEMs.

expel.com

Expel MDR + Data Lake

Expel offers flexible options to support you—no matter where you are on your SIEM and data retention journey.

1. **Store long-term data in the Expel Data Lake** where Expel can leverage it as an investigative source for MDR.

2. **Looking for a full Service SIEM?** You also have the option to bundle Expel MDR with Sumo Logic's full Cloud SIEM to unlock advanced support, SIEM tuning guidance, advanced detection logic out-of-the-box and custom rules for advanced detection and response.

Sources

- Endpoint & Network
- Cloud infrastructure
- Identity & SaaS
- Any telemetry source

Raw Data

Expel Data Lake
- Infrequent audit & compliance search capabilities
- 90-day, 365 days, or custom data retention
- Supported as an investigative source for MDR

Sumo Logic Cloud SIEM
- Full SIEM capabilities
- Unlimited, real-time, data search and reporting
- OOTB and custom rule set and alerting
- 90-day, 365 days, or custom data retention
- SIEM tuning guidance

Expel MDR

Why Expel

Lower SIEM costs
Offload high-volume data to reduce storage expenses without losing insights—all while Expel handles your detection and response.

Meet compliance with ease
Use our affordable data lake to retain security logs and meet audit or regulatory mandates without a full SIEM.

Accessible data on demand
Retrieve stored data quickly for investigations or audits while keeping costs under control and workflows simple.

Gartner Peer Insights™
4.7/5 Stars
Gartner Peer Insights

CUSTOMER NPS
75+

G2
4.8/5 Stars
on G2 Peer Review

Learn more at expel.com

02/05/25