Next-Generation Security Information and Event Management

Minnesota IT Services (MNIT) offers a Next-Generation Security Information and Event Management (Next-Gen SIEM or NGS) solution through a trusted vendor partner.

This solution collects and aggregates log data from multiple sources, centralizing information for faster detection, analysis, and response. By uniting data across the enterprise, NGS creates a more complete and connected view of an organization's IT environment. This holistic visibility empowers security teams to act more quickly, strengthen their defenses, and support more informed decision-making.

Benefits

After enrolling in MNIT's Managed Detection and Response (MDR) program, entities participating in MNIT's NGS will have:

- Centralized security visibility across endpoints and third-party sources.
- CJIS, MNJIS, FedRAMP High, HIPAA, and PCI DSS compliance support.
- Flexible and scalable ingest model with a 10 GB free allowance.
- 365-day data retention for investigations and compliance.
- MDR-managed endpoint data, with partner control of third-party data.

Compliance

MNIT's Next-Gen SIEM solution is designed to simplify compliance for Minnesota's state, local, and tribal partners by aligning with some of the most stringent security standards in the country.

The platform:

- Is fully compliant with Criminal Justice Information Services (CJIS) and Minnesota Justice Information Services (MNJIS) controls.
- Meets Federal Risk and Authorization Management Program (FedRAMP) High controls.
- Supports compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Note: Compliance is a shared responsibility. While the technology supports CJIS compliance requirements, customer entities are responsible for identifying and configuring log sources, access controls, and retention in alignment with relevant compliance standards in place.

Data ingest and retention

Each NGS participant receives 10 GB of third-party data ingest at no cost. This allows organizations to begin sending their most critical log sources into the platform right away without worrying about initial costs.

Vendor-provided endpoint data

This is not counted toward this allowance, ensuring partners get the full benefit of the free allocation.

Third-party data

There is no cap on the amount of third-party data that can be ingested. Instead, billing is based on each organization's average daily ingest volume and endpoint counts, providing flexibility to scale usage as security and operational needs grow.

Data retention

All data ingested into the platform is retained for 365 days, supporting deeper investigations, compliance obligations, and long-term visibility.

Endpoint data

This is fully managed through MNIT's MDR program, ensuring strong oversight of security telemetry. However, MDR Complete services are not included with the NGS module, providing a clear distinction between what MNIT manages centrally and what remains the responsibility of the partner organization.

Eligibility and cost

Eligible entities must be enrolled in MNIT's MDR program prior to using NGS. This allows all data to be processed and avoids duplication of efforts and cost.

- NGS pricing is based on the amount of third-party data ingest (external sources) and number of endpoints.
- The vendor for MDR and NGS dashboard provides daily ingest data. MNIT and the vendor use this data to determine an average daily ingest each month for billing purposes.
- Billing is based on each organization's average daily ingest volume and endpoint counts, providing flexibility to scale usage as security and operational needs grow.
- Each partner receives 10 GB of external ingest free each month. Vendor endpoint data does not count toward this total. There's no cap on how much data you can send. You only pay for what you use above the free 10 GB.

Training and information

- MNIT's Cyber Navigator team supports the enrollment and onboarding process to ensure partners are comfortable with the initial implementation process.
- All users have access to the vendor's training portal, a SIEM-100 course, and recorded webinars.
- Contact MNIT's Cyber Navigator team for specific costs and information: **CN.MNIT@state.mn.us**
- Refer to MNIT's Whole-of-State participant page for more information. **mn.gov/mnit/about-mnit/security/whole-of-state-cybersecurity-plan/wos**

Whole-of-State Participant Information