overwatch
CYBER SECURITY

Managed Detection and Response Pricing

Our Managed Detection and Response (MDR) service for Microsoft Sentinel offers comprehensive security monitoring and threat response. The following table outlines our pricing tiers based on the number of endpoints.

Endpoints	Monthly MDR Service Fee:
1-15	**$1,500**
1-25	**$2,000**
26-50	**$3,200**
51-250	**$4,800**
251-500	**$6,667**
501-1000	**$12,000**

Note: We will apply a 15% discount to customers who sign up for annual billing

Incremental Add-On Pricing

Need to scale up your coverage? Here's the per-endpoint cost for before upgrading to the next tier:

Tier Jump	Per Endpoint Cost
1-25	$25 per endpoint beyond 25 - up to 38
26-50	$25 per endpoint beyond 50 - up to 150

Note: *Per the example above, If you exceed halfway into the next tier, you will move to that tier's full price. For example, from Tier 1 (1–15 endpoints), adding beyond 20 endpoints switches you to Tier 2 pricing.*

What You're Paying For

- **Active Response by Experienced Cybersecurity Experts**

- **Initial Setup Support**

- **24/7 Threat Monitoring & Incident Response**

- **Automated Playbooks & SOAR Integration**

- **Microsoft Sentinel Tuning & Management**

- **Threat Intelligence Enrichment**

- **Custom detection rules tailored to your environment**

Additional Pricing Considerations – Azure Infrastructure

- **Microsoft Sentinel Pricing is Usage-Based:**
  Sentinel charges by data ingestion (GB/day) and retention beyond 90 days. More logs = higher costs.

- **Ingestion is The Main Driver of Cost:**
  Continuous ingestion of Windows event logs, Defender alerts, network logs and application logs can become expensive in traditional Sentinel-only models.

- **Our Hybrid Data Lake Model Strategy Saves Money:**
  We promote only critical security logs (e.g., SecurityEvent, SignInLogs, Defender data) into Sentinel for real-time monitoring, while archiving less critical logs to Azure Data Lake Storage at a fraction of the cost.

- **Cost Efficiency:**
  - **Sentinel ingestion: ~$2.76 per GB.**
  - **Azure Data Lake storage: ~$0.02 per GB (cool tier).**
  - **This hybrid strategy has the capacity to reduce Sentinel storage and ingestion costs by 40–60% once full support is rolled out by Microsoft - with immediate cost savings projections being between 10-20%**

- **Licensing Costs Separate:**
  Defender P2 or Microsoft 365 E5 licenses are billed separately by Microsoft or your CSP.

Example Estimate (25 Endpoints with Hybrid Data Lake Model)

- **We are assuming here that:**
  - **Average log volume per endpoint: ~0.2 GB/day.**
  - **25 endpoints = 5 GB/day.**
  - **Monthly = ~150 GB.**
- **Traditional Sentinel-Only Model:**
  - **150 GB × $2.76 = $414/month just for ingestion.**
- **Hybrid Model:**
  - **Promote ~40% of logs to Sentinel (~2 GB/day = 60 GB/month).**
  - **Sentinel cost = 60 × $2.76 = $165/month.**
  - **Archive remaining logs to Azure Data Lake = (90 GB × $0.02) = $1.80/month.**
- **Total Estimate:**
  $166.80/month vs $414/month ~60% savings on storage.

Note: *This is an estimate and prices vary depending on the region resources are deployed and how many gigabytes are being ingested through sentinel in analytics tier ingestion/storage. Microsoft is also phasing in additional table support for data lake only ingestion and is currently limited.*

Next Steps

Sound like a good fit? Book your consultation here!