UnderDefense
CYBERSECURITY

Managed SIEM
Pricing Guide

Managed SIEM Pricing Guide

As cyber threats become increasingly sophisticated, businesses must implement robust security measures to protect their sensitive data and maintain regulatory compliance. Managed Security Information and Event Management (SIEM) solutions have emerged as a vital component in the cybersecurity arsenal, offering advanced threat detection, real-time monitoring, and comprehensive incident response capabilities.

But how much does it cost? It depends on a range of factors. In this blog post, we will explore the common pricing models for Managed SIEM and provide a detailed breakdown to help you understand what to expect and how to budget effectively for this crucial service.

Table of contents

Managed SIEM common pricing models

When evaluating Managed SIEM pricing, it's crucial to consider factors such as service level requirements, customization needs, deployment preferences, and the service provider's reputation. Here's a pricing breakdown for Managed SIEM services based on different models:

Subscription-based:
In this model, clients pay a recurring subscription fee to access the Managed SIEM service. Pricing tiers can vary based on the level of service and the number of features included. Clients receive invoices either monthly or quarterly, depending on their preference.

Prepayment 100% upfront:
This approach often covers a specified contract duration, such as one year or more. By paying in advance, clients may benefit from discounts or other incentives the service provider offers. This model ensures that the service is fully funded from the outset, providing financial stability and predictability for both the client and the provider.

Per-user or per-device:
Some providers offer pricing based on the number of users or devices being monitored. This can be advantageous for organizations with a predictable user/device count and help tailor costs to actual usage.

The volume of data processed:
Pricing may be structured around the volume of data the SIEM platform processes. This could include logs from servers, applications, network devices, etc. Tiered pricing based on data volume ensures scalability and fair pricing based on usage.

Client-owned SIEM:
In this model, the client purchases and owns the SIEM software outright. Costs typically include upfront licensing fees, implementation, integration, and ongoing maintenance costs. The client is responsible for managing the infrastructure and security operations internally.

MSSP-owned SIEM:
With this model, the Managed Security Service Provider (MSSP) owns and operates the SIEM solution on behalf of the client. Pricing is usually subscription-based, with clients paying a recurring fee for access to the service. Costs may include subscription fees, customization, integration, and additional services such as incident response and support.

Custom pricing:
Custom pricing may be negotiated for organizations with unique requirements or larger-scale deployments. This could include specialized integrations, additional features, or extended support options.

Managed SIEM packages by UnderDefense

	SIEM Professional Services Expert guidance to help organizations effectively monitor, detect, and respond to cyber threats.	Co-managed SIEM A comprehensive solution for organizations seeking expert support and enhanced security.	SIEM as-a-Service A fully managed solution, including your choice of top-tier cloud-based SIEMs.
Security consulting	✓	✓	✓
SIEM architecture review	✓	✓	✓
Solving performance issues	✓	✓	✓
New custom data sources ingestion and normalization	✓	✓	✓
Effective garbage data filtering to optimize licensing	✓	✓	✓
Detection engineering - develop unique correlation taylored to your environment	✓	✓	✓
Eliminate alert fatigue	✓	✓	✓
Effective alerting and notifications engineering (Slack, Teams, Jlra etc)	✓	✓	✓
Unique dashboards and visualization	✓	✓	✓
Incident management with expert assistance in responding to security incidents		✓	✓
24/7 experienced SOC continuous monitoring of the SIEM environment for threats and anomalies		✓	✓
Automated detailed reports to meet compliance requirements		✓	✓
Automated incident enrichment			✓
Visibility testing performed by our experts			✓
All the sensors and log collectors you need to deploy are provided by UnderDefense			✓
Deployment, configuration, and licensing included			✓
Your choice of Gartner's top cloud-based SIEMs			✓

What is the average cost of Managed SIEM services?

Typically, the cost of a Managed SIEM falls within the range of **$5,000 to $10,000** per month. However, this estimate serves as a general guideline, and the actual pricing can fluctuate based on specific vendor and your individual needs as well as other factors:

1 Business size

The scale and complexity of the organization influence the pricing structure. Larger enterprises with extensive networks may incur higher costs compared to small or medium-sized businesses.

2 Data volume

The amount of data processed and monitored by the SIEM solution affects pricing. Higher data volumes often result in increased costs due to additional processing and storage requirements.

3 Customization level

Organizations requiring extensive customization, tailored dashboards, correlation rules, or integrations with existing systems may face additional charges.

4 Feature requirements

The breadth of features and functionalities desired by the organization impacts pricing. Advanced threat detection capabilities, compliance management tools, and real-time alerting systems may incur higher costs.

The best way to get a precise quote is to contact potential Managed SIEM vendors directly. Clearly define your requirements (organization size, data volume, features needed, etc.) to receive the most relevant pricing information.

Managed SIEM common pricing models

- Subscription-based
- Prepayment 100% upfront
- Per-user or per-device
- Custom pricing
- The volume of data processed
- Client-owned SIEM
- MSSP-owned SIEM

Stop security headaches, not your budget.

With the UnderDefense Managed SIEM service, you can extend, simplify, and centralize your security visibility, consolidating disparate security data into a unified platform.

Calculate your Managed SIEM price

Your email*

email.@gmail.com

Number of Users*

101 - 200

Number of Endpoints*

101 - 200

Number of Servers

Your Number of Servers

Pick your attack surface(s)*

- [ ] Cloud infrastructure
- [ ] Endpoint
- [ ] SaaS apps
- [ ] Network
- [ ] Kubernetes
- [ ] Email

Get a Custome Quote

Key factors that influence Managed SIEM pricing

	HIGH SIGNIFICANCE
1	**The volume of data processed** Managed SIEM providers often charge based on the data ingested into the platform. This can include logs from servers, applications, network devices, and other sources. Higher data volumes typically result in higher costs.
2	**Deployment model** Whether the SIEM solution is deployed on-premises, in the cloud, or as a hybrid model can influence pricing. Cloud-based solutions often have subscription-based pricing models, while on-premises solutions may involve upfront hardware and software costs.
3	**Retention period** Some providers offer different pricing tiers based on the duration for which data needs to be retained. Longer retention periods typically incur higher costs due to increased storage requirements.
	AVERAGE SIGNIFICANCE
4	**Business size** The larger the business, the more data that needs to be monitored, which can increase costs, but the impact is not as direct as the high-significance factors.
5	**Customization and integration** Additional costs for customization or integration with existing systems may be incurred. Customized dashboards, reports, correlation rules, and integration with other security tools can contribute to overall pricing.
6	**Managed services vs. self-managed** Opting for fully Managed SIEM services, where the provider handles monitoring, maintenance, and updates, may cost more than self-managing the SIEM solution. Managed services often include additional features such as 24/7 support, threat intelligence feeds, and dedicated security analysts.
	LOW SIGNIFICANCE
7	**Additional features and support** Pricing may include threat intelligence feeds, compliance reporting, advanced analytics, and consulting services. Providers offering comprehensive support options may charge higher prices.
8	**Contract length and terms** Longer contract commitments may come with discounted pricing, but it's essential to evaluate the flexibility of the contract terms. Some providers offer month-to-month billing, while others may require annual commitments.
9	**Vendor reputation and expertise** Pricing may vary depending on the SIEM vendor's reputation and expertise. Established vendors with a track record of delivering reliable security solutions may command higher prices.
10	**Geographical location** Pricing can also be influenced by geographical factors such as regional market demand, labor costs, and regulatory requirements.

How to choose the right Managed SIEM provider

Choosing the right Managed SIEM provider is critical for any organization looking to enhance its cybersecurity posture. Here's how you can do it:

1 Define your requirements

Clearly define your organization's security objectives, compliance requirements, and budget constraints. Determine the specific features, functionalities, and level of service you need from a Managed SIEM provider.

2 Conduct market research

Research and identify reputable Managed SIEM providers. Consider industry reputation, customer reviews, analyst reports, and case studies to evaluate each provider's track record and expertise.

3 Assess capabilities and technology

Choosing the right Managed SIEM provider is critical for any organization looking to enhance its cybersecurity posture. Here's how you can do it:

4 Evaluate security expertise

Assess the expertise and qualifications of the provider's security team. Look for providers with certified security professionals, experienced threat hunters, and incident responders who can effectively monitor, analyze, and respond to security incidents.

5 Review compliance support

Ensure that the Managed SIEM provider has experience and expertise in supporting regulatory compliance requirements relevant to your industry, such as GDPR, HIPAA, PCI DSS, etc. Verify that the provider's services align with your organization's compliance obligations.

6 Consider deployment options

Evaluate the deployment options offered by each Managed SIEM provider, such as on-premises, cloud-based, or hybrid deployments. Choose a deployment model that aligns with your organization's infrastructure, security policies, and budgetary constraints.

7 Compare pricing and contract terms

Request pricing quotes from multiple Managed SIEM providers and compare them based on subscription fees, data volume pricing, customization costs, and contract terms. Pay attention to hidden costs and ensure the pricing structure is transparent and scalable.

8 Assess support and Service Level Agreements (SLAs)

Evaluate each provider's level of support, including response times, incident escalation procedures, and the availability of dedicated security analysts. Review the provider's SLAs to ensure they meet your organization's uptime and performance requirements.

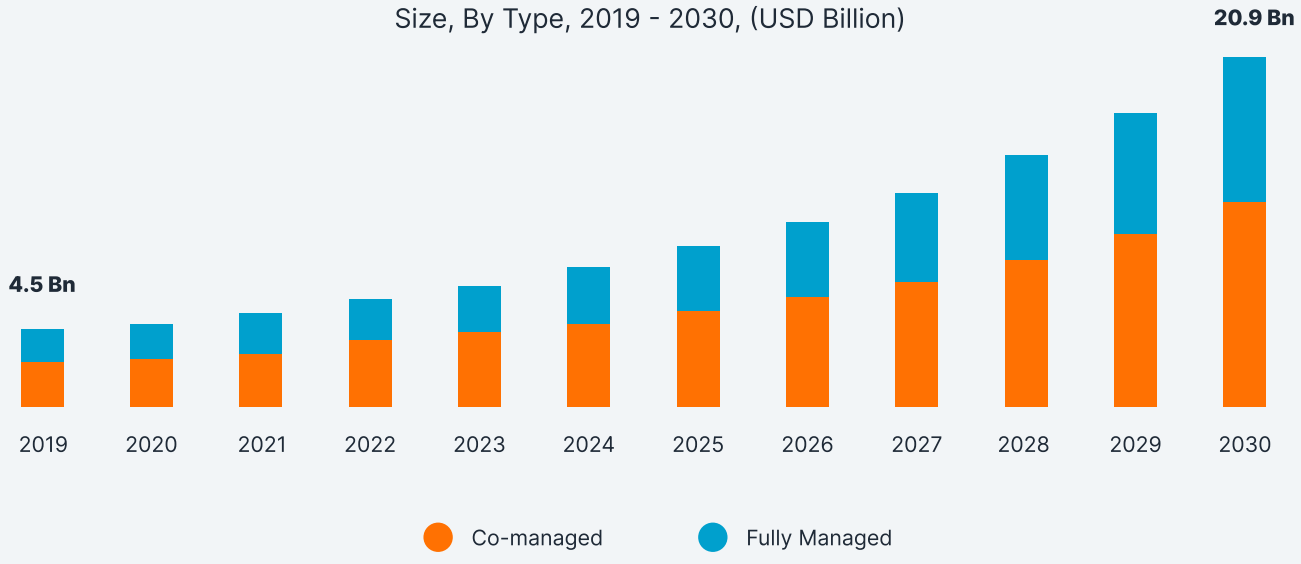
9 Request references and demos

Ask each Managed SIEM provider for customer references and case studies to validate their track record and customer satisfaction levels. Request product demos or trials to assess the provider's SIEM platform's usability, functionality, and effectiveness.

10 Consider long-term partnerships

Choose a Managed SIEM provider willing to establish a long-term partnership and collaborate closely with your organization to address evolving security threats and business needs. Ensure that the provider is responsive to feedback and committed to continuous improvement.

Global Managed SIEM Services Market



Source: www.kbvresearch.com

Choosing the right Managed SIEM provider

- Define your requirements
- Conduct market research
- Assess capabilities and technology
- Evaluate security expertise
- Review compliance support
- Consider deployment options
- Compare pricing and contract terms
- Assess support and SLAs
- Request references and demos
- Consider long-term partnerships

Interested in Managed Services for Your Organization? Contact UnderDefense Today

Get a Quote

Maximize tech ROI with Managed SIEM services

UnderDefense provides a Managed SIEM solution that fits your budget and gives you confidence in your organization's security posture. Here's how our Managed SIEM service can help you overcome common challenges:

- Rapid security implementation
- Comprehensive threat coverage
- SIEM performance optimization
- Adaptable service options
- Simplified compliance

Talk to Expert