



Scale Up Your Security with a Managed Security Service Provider



1. Introduction	03
2. What is a managed security service provider?	03
3. 8 benefits of a managed security service provider	04
a. Add Extensive Knowledge and Experience to Your Team	04
b. Constant Vigilance with 24/7 Security Operations Center	05
c. All-in-one Bundled Services for Multilayered Security	05
d. End Response Fatigue with Instant and Accurate Responses	06
e. Stay Stress-free with Automated Compliance	06
f. Pocket-Friendly Security Solution	06
g. Never Have a Blind Spot with Vulnerability and Risk Assessment	07
h. Stay Ahead of Attacks with Threat Prediction and Proactive Hunting	07
4. MSSP: The Only Line of Defense You Need	08
5. About Ace Cloud Hosting	09

Introduction

Most of your work takes place over the cloud these days. So why is your security still traditional?

Cyberattacks have unfortunately become common in the business world. You might think that small and medium-sized enterprises are safe, but that's not true! Cyberattacks against small and medium-sized businesses are increasing every day. Research shows that 43%¹ of cyberattacks target small businesses.

Putting together a fully-equipped security team is difficult for small and medium enterprises. The challenges are several:

- **High expenditure of procuring and maintaining the latest technologies**
- **Cost and effort involved in hiring and training skilled professionals**
- **Overseeing the smooth functioning of a Security Operations Center (SOC)**
- **Keeping up with advanced threats**
- **Securing multiple endpoints, especially in a remote work set-up**

A managed security service provider is your solution to all of these problems.

Continue reading this eBook to find out how managed security services benefit your enterprise.

What is a Managed Security Service Provider?

A managed security service provider (MSSP) is an IT vendor responsible for managing and monitoring your security process. Their services incorporate constant monitoring of your network and endpoint devices, processing vast data, instant response in case of attacks, and remediation recommendations.



A qualified MSSP incorporates a wide variety of technologies as a part of their services. Some of these technologies are:

- Cloud Firewall Management
- Web Filtering
- Endpoint Detection and Response (EDR)
- Vulnerability Management
- Data Loss Prevention
- Disaster Recovery
- Email Security and Spam Protection

An MSSP takes your security operations to the next level. Read on to see how.

8 Benefits of a Managed Security Service Provider



1. Add Extensive Knowledge and Experience to Your Team

Have you found it difficult to hire experienced professionals with cybersecurity skills? You're not alone.

While the cybersecurity domain has been expanding rapidly, there is a skill gap in the industry. People with exceptional cybersecurity knowledge can be hard to find. As a result, many small and medium businesses are unable to adequately equip their security teams.

With an MSSP, you benefit from the expertise of people entrenched in the cybersecurity domain for decades. They add a global perspective to your team. The cherry on top is that you get this world-class experience at no extra cost. An MSSP also eliminates the hassle of recruiting



2. Constant Vigilance with 24/7 Security Operations Center

Are you able to actively monitor your network 24/7? None of us can. Monitoring a network involves various interrelated activities. Several technologies are a part of the process. And all this can be complex for a novice to understand.

Cyberattacks don't wait for you to be active. They can happen at any time. With every passing second, a malicious agent stays undetected in your network, the risk of long-term damage and data loss increases.

A 24/7 SOC constantly monitors your network for intrusions and runs deep investigations and analyses. Even if an attack occurs, it gets detected instantly. The attacker's "dwell time" on your system is minimal.



3. All-in-one Bundled Services for Multilayered Security

An effective cybersecurity operation works on multiple levels. Cyberattacks can take a wide variety of forms, and their paths inside your system are also diverse. An array of security solutions will work in tandem to counter this.

An MSSP provides multi-layered services. You can leverage their existing security investments. The providers also customize their services according to your business environment.

The security technologies bundled with ACE Managed Security Services are:

Managed SIEM – A Security Information and Event Management system provides real-time analysis of the security alerts generated within the system

Next-Gen Firewall – A cloud firewall combines network protection with next-level intrusion detection and forensic analysis of alerts.

Managed EDR - Endpoint Detection and Response manages the security of your endpoint devices.

All the advanced technologies you need to protect your environment are available on one platform.





4. End Response Fatigue with Instant and Accurate Responses

Detecting threats and intrusions are just half the battle. How rapidly and efficiently you respond to those threats plays a significant part in minimizing damage. If an attacker is present in your network for a long time, it can steal sensitive information and trigger irreversible damage.

Incident response requires a specialized skill set. Each attack requires a different understanding. For instance, a wiper malware attack warrants a response to protect your data and identify the scope of the malicious code.

An MSSP has a dedicated incident response team responsible for instant remediation. They investigate all the alerts produced by the system. And only legitimate alerts are forwarded to you. It saves you from receiving too many redundant alerts and lowers your alert fatigue. False positives also diminish due to thorough investigations



5. Stay Stress-free with Automated Compliance of Industry Regulations

Keeping up with industry compliance can be a chore, especially for a small enterprise that can't afford a dedicated team to oversee compliance with regulations. Rules and regulations are also constantly changing. It is easy to miss an update and face trouble with regulators.

MSSPs conduct data collection per regulations such as HIPAA, PCI DSS, GDPR, and CCPA, to name a few. They implement the required security controls and maintain visibility in the network. They generate audit-ready reports when needed. They are responsible for alerting data breaches and other cybersecurity incidents to regulators. This feature cuts down on the efforts required from your team.



6. Pocket-Friendly Security Solution

An in-house dedicated security team is a considerable expense. It is out of reach for small businesses. The hardware and software required to run a security operation are costly. Its maintenance is also an added cost. Keeping up with rapidly evolving threats requires a high level of expertise. All this is impossible to achieve on a limited budget.

An MSSP gives you the level of security expertise that large businesses can build up. And it does so at a fraction of the cost involved. All the hassles with hardware, software, and human resources are taken care of by the provider. Also, you can quickly scale up or down with an MSSP. The cloud also eliminates the cost and effort involved in



7. Never Have a Blind Spot with Vulnerability and Risk Assessment

All systems have dynamic vulnerabilities. When your environment keeps changing, your risk profile keeps changing as well. It's critical for any security operation to check vulnerable areas constantly.

An MSSP conducts regular automated internal and external scans across your network and all your IT assets. Resource needs are adjusted according to the outcome of the vulnerability scans. MSSPs also offer configuration changes and patch management via an interactive dashboard



8. Stay Ahead of Attacks with Threat Prediction and Proactive Hunting

Cyber threats become more advanced and sophisticated as each day passes. There are probable threats hidden in your system that traditional cybersecurity solutions cannot detect. Proactive threat hunting compliments the constant monitoring of your network.

Effective threat hunting is powered by artificial intelligence. Pattern analysis and deep behavioral analysis are employed to detect potential threats.

Your security operation converts from just prevention to active hunting. An MSSP helps you stay one step ahead of malicious agents

Managed Security Service Providers: The Only Line of Defense You Need



Small and large businesses face the same level of cyber-attacks. So why should a small business's cyber defense be lacking?

Managed security service providers make your security operation more effective, affordable, and sophisticated. All the know-how and equipment you would need to defend against the myriad of threats are at your fingertips.

Ace Cloud Hosting's Managed Security Service gives you all-around protection from cyber threats. As a part of our services, you have access to **managed SIEM**, **managed cloud firewall**, and **managed EDR** that protect your endpoints. Try out the ACE way of keeping your network safe.

GET A CUSTOM QUOTE NOW!

About Ace Cloud Hosting

ACE is a renowned cloud service provider having won 16 awards over 14 years of expertise. Our success attributes to innovative services of Public Cloud, VDI, Managed Security & Application Hosting that simplify cloud adoption for large to SMEs by meeting their unique requirements. We provide high-performing solutions checking every box on quality, security, and availability.



Reference

- 1) <https://www.fundera.com/resources/small-business-cyber-security-statistics#:~:text=43%25%20of%20cyber%20attacks%20target,business%20cyber%20breaches%20last%20year>