www.onesource.net info@ostcm.com

Managed Security Services (MSS) For Small And Mid-Sized Businesses

It's no secret that most small and mid-sized organizations with less than $1 billion in revenue (businesses, nonprofits, even some government agencies) lack the financial and personnel resources to administer vital cyber security functions. This is a problem in part because governments worldwide continue to impose strict regulations that enforce cyber security protections/controls within all companies, regardless of size, and because hackers and other threats have moved beyond large organizations to also target their smaller counterparts.

According to an oft-cited statistic from the U.S. Securities and Exchange Commission, 50 percent of small and mid-sized businesses have been the victims of cyber attack and more than 60 percent of small firms go out of business within six months of a data breach. But using Managed Security Services can – and should – prevent these events and their outcomes.

Managed Security Services take the best of enterprise-grade services, assets, and people to create customizable, affordable, and reliable packages for small and mid-sized businesses. A thorough offering, fully managed on the client's behalf, will include:

Proactive monitoring and detection

In this scenario, the Managed Security Services vendor protects against common threats and sophisticated attacks. Components include defenses at all points of entry, including endpoints, networks and email systems; detection of a full range of threats; and deployment of a Fortune 100-level security ecosystem.

Threat investigation

Here, the Managed Security Services vendor validates and priorities threats on behalf of clients, analyzing all security alerts using the latest intelligence. A proven Managed Security Services provider will also determine the scope of all incidents and the extent of any compromises. Finally, the vendor will diagnose and triage security alerts based on indicators of compromise (IOC), attackers' activities, and threat patterns.

Hunt

Next, the Managed Security Services provider proactively (and continuously) searches for malicious threats, indicators, and zero-day vulnerabilities. It then integrates threat intelligence throughout the customer's entire security ecosystem, while maintaining visibility across all traffic and endpoints.

Respond

Finally, the Managed Security Services provider should contain threats rapidly with automated threat notifications and orchestrated security responses. Some vendors will further develop immediate remediation plans and recommendations to minimize breach impact.

Organizations working with a Managed Security Services Provider (MSSP) should experience several benefits, chief among them enhanced capabilities, increased efficiency, and less worry. A good way of using an MSSP to create improved outcomes is through educating end users and changing their behavior. In other words, through a combination of automation and human expertise, a well-rounded MSSP will teach its customers how to protect the organization and themselves. Email serves as a prime example. More than 90% of cyber security attacks reach an organization through convincing phishing messages that trick employees into opening them. This then unleashes threats such as ransomware, malware, and viruses. Effectively combating these challenges calls for a complete security solution that combines human awareness, user education, and top-notch technology.

That is why One Source helps enterprises approach anti-phishing efforts in the following ways:

ONE SOURCE COMMUNICATIONS

Prioritizing risks across the entire organization with actionable remediation plans to all threats

Identifying organizational loopholes and increasing security awareness for all employees, thereby mitigating risks

Providing documented analytics to support the awareness program's financial goals and ensure compliance

Enabling customers to stay ahead of trends with real-time simulations that provide education and defend the client environment

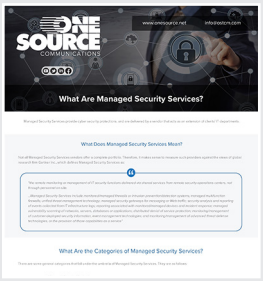
One Source delivers these capabilities alongside Cofense's PhishMe™ software as a service platform that distributes simulated phishing threats. The program has proven to reduce the number of employees falling victim to advanced cyber attacks by up to 95%.

And yet, still more is often needed to combat the growing sophistication of cyber threats – that's why One Source also leverages Cofense's Triage™ platform. Cofense Triage™ allows security analysts to respond to email-based attacks. It integrates with SIEM, malware and domain analysis tools, and features playbooks that helps IT teams respond in the most efficient way possible. Ultimately, Cofense Triage™ provides visibility into active phishing attempts and gives One Source the power to fight back.

Finally, One Source also teams with FireEye, a world-renowned company that pairs security technology with human intelligence. Through FireEye's unique next generation SIEM, Helix, One Source provides endpoint, network, and email security.

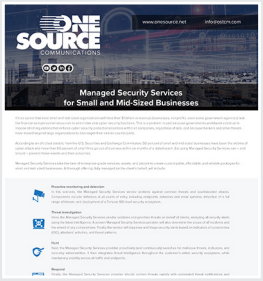
One Source's multifaceted approach closes gaps, bringing the latest, most thorough cyber security protections to clients with little effort on their part. And that last part is key. Small and mid-sized firms will gain the efficiencies that come with a fully outsourced Managed Security Services program. The vendor, through its professionals and partnerships, will deliver the expertise most small and mid-sized firms cannot afford on their own. This frees end users to focus on their competencies without having to worry about cyber security. Along the way, though, the Managed Security Services Provider will give customers full insight and visibility into all activity through a single interface, as well as around-the-clock security operations center support.

RESOURCES

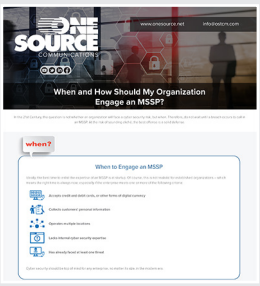


WHAT ARE MANAGED SECURITY SERVICES (MSS)?

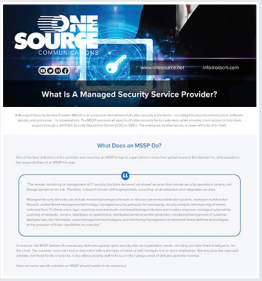
BENEFITS OF USING AN MSSP



MSS FOR SMALL AND MID-SIZED BUSINESSES



WHEN AND HOW SHOULD MY ORGANIZATION ENGAGE AN MSSP?



WHAT IS A MANAGED SECURITY SERVICE PROVIDER (MSSP)?