ESET MSP PROGRAM

6 TIPS TO MAKE YOUR MSP OFFER IRRESISTIBLE

As an MSP, you need to demonstrate your security expertise, offer a comprehensive portfolio of security solutions and services, and deliver added value to your clients.

1 Know your client

A good business partnership is built on trust. To foster a positive atmosphere, consider conducting an initial security audit of your client's IT systems. It will demonstrate your expertise, and generate the threat intelligence necessary to adjust your client's current security strategy — or allow you to create a new one from scratch.

This list is not exhaustive, but its outputs can highlight different needs that arise in different sectors. In agriculture, IT might be viewed as a "necessary evil" that just needs to work. By contrast, a customer operating in a health-care vertical will probably have a business model based on collecting and analyzing sensitive information from patients, so encryption or other technologies dedicated to data protection are essential.

Thanks to this initial survey, you can also identify the appropriate threat model to apply to your customer and and **help them craft a custom security package** that will help improve their level of protection.

Among many other aspects, such an assessment should provide answers to some elementary questions:

1. What vertical does the client operate in and what are the specifics of that vertical?
2. How and why does the client use their IT systems?
3. What is being stored on those systems?
4. Are the client's devices used solely on-premise or also remotely?
5. What types of users are logging into the network?
6. What IT problems has the client encountered in the past?

2 Apply cyber-hygiene

As a software and security provider, your own systems need to act as a model for your clients. Follow the best cyber-hygiene practices for your own systems, and then apply these to your clients' tech infrastructure too. By applying proper patch management and by keeping operating systems, apps and security solutions up-to-date, you can close many potential vulnerabilities.

You **can reduce attack surfaces** and avoid the creation of new cyber-security gaps by properly **managing your client's access rights** when it comes to installing new software. A similar approach should be stressed even in situations where the client wants their own IT department to maintain their software and security solutions.

The importance of cyber-hygiene was well-illustrated by the Wanna-Cryptor.D (aka WannaCry) 2017 incident. Despite the vulnerability in Windows being **known and patched** months before the attack, hundreds of thousands of machines didn't have the fix applied, many of which were in the SMB segment.

Clean up your IT practices

1. Reduce the attack surface by disabling or uninstalling any unnecessary services and software
2. Scan networks for risky accounts that use weak passwords, and ensure they are improved
3. Limit or ban use of Remote Desktop Protocol (RDP) from outside the network, or enable Network Level Authentication
4. Use a VPN for remote access
5. Review firewall settings and close any non-essential ports
6. Review rules and policies for traffic between internal company systems and outside network(s)
7. Password-protect the configurations of your security solutions
8. Segment the company LAN into subnets and connect them to firewalls to limit the potential impact of attacks within the network
9. Protect backups with multi-factor authentication
10. Train client staff to recognize cyber and social engineering attacks
11. Limit shared file / folder access only to those who need it, and make content read-only where possible
12. Enable detection of potentially unsafe/unwanted applications (PUSA/PUA)

3 Choose the right security solutions

Including antivirus and perimeter security features such as firewall and antispam in your offer is a must. However, based on your customers' needs, the verticals they operate in, and their regulatory requirements, offering additional products such as encryption, multi-factor authentication, or data leak prevention (DLP) can give you the edge.

All these **solutions should be low-maintenance, easy-to-deploy and easy-to-use**, as this will enable to focus your strength where it's needed, and allow your client to operate smoothly and undisturbed. ESET solutions are designed to fit your needs (and those of your clients) by working on an "install and forget" basis. To benefit from their full potential, here are some basics rules users should stick to:

- **Use the latest version** of each product
- **Keep security features** such as ESET LiveGrid® and real-time scanning **enabled**. These systems are designed to gather threat intelligence and increase the level of user protection
- If your internet connection allows it, **always update the scanning engine and detection database** to make sure managed endpoints are protected from new and emerging threats
- **Don't run scans manually**, as this consumes hardware power while needlessly duplicating the activity of real-time scanning

To learn more about ESET services for MSPs, see here.

ESET doesn't recommend that users run scans, except for the first scan after installation. After that, real-time protection takes care of any new items that your system might encounter. The only time when you should run a scan is after real-time protection was manually shut off.

4 Educate your clients and their users

As an external security advisor, you can also add value by offering your clients' employees cybersecurity training and education. This should be tailored to the employees' level of technical knowledge, with different training for management, IT personnel and regular users.

In regard to ongoing training, **regular users are often described as the most vulnerable** to simple social engineering and phishing techniques, as well as to other cyberattacks. Therefore, their training should be as broad as possible, starting with the basics:

- Description of the most common threats such as malware, social engineering and phishing
- Rules of good password hygiene and the importance of multi-factor authentication
- Best practices when connecting to networks
- Tips and rules for secure browsing
- Explanation of spearphishing, whaling and targeted cybercriminal campaigns – mainly for management and employees who work with sensitive materials

MSPs should also have a dedicated program for their clients' IT staff, including actionable tips and best practices for setting up security products as well as networks and systems. Compared to training for management or end-users, programs for IT staff should go into more technical detail and cover a different range of topics:

- Minimal password requirements, frequency and set-up of password policies
- Correct set-up of admin and user profiles on the company network
- Tips on how to minimize the attack surface of internal systems
- Specific settings for legitimate services that are often misused as attack vectors, such as remote desktop protocol (RDP), or emails and email attachments
- Detailed ransomware prevention advice

ESET offers educational materials, guides and tips to MSP partners, designed for you to share with your clients.

5 Build proper infrastructure and engage with the client

Communication is key, but sometimes less is more. Clients expect you to inform them in plain and easy-to-understand language about what is happening in their IT systems – but only when necessary. Too many notifications about minor events can become a burden on your client and affect their trust in your abilities.

An MSP should use proper security tools that supply detailed information and an overview of anomalies on endpoints or other parts of the system that might require attention.

In the event of a security incident, an MSP has to be available and equipped to **act quickly** and resolve problems that the incident might cause. If possible, the situation should be handled and resolved **remotely**. To achieve this goal, properly scaled and highly **resilient infrastructure** as well as **reliable network connectivity** are necessary.

As an MSP, you should also be **able to scale and adjust your systems**, infrastructure and software to fulfill the constantly evolving needs of your SMB clients.

ESET offers a robust, multi-tenant ESET Security Management Center console. It lets you automate the resolving of security issues, and automatically generate reports with your logo, which you can send to your customers. It's easy to integrate: we provide support for a wide range of popular Remote Monitoring and Management (RMM) tools and PSA consoles.

6 Avoid the break/fix model, be a modern MSP

Offering IT security services on the old "break/fix" model is quickly becoming a thing of the past. Your clients want to avoid time-consuming – and expensive – on-site repairs, or the inconvenience of having to flag problems and maintain their own systems.

As a modern MSP, consider offering your clients following:

- **Added value services:** It's not about selling products anymore. A modern MSP needs to bring value to the table and persuade clients it is worth investing in these services instead of building in-house capacities.
- **Regular monitoring of on-premise IT:** Instead of just installing and passing control over IT and security to the client, a modern MSP offers constant monitoring and maintenance of the solutions they provide. This lowers the burden on the client's side and enables the MSP to stay constantly informed about both the state of and changes in their client's systems and networks.
- **Open-ended and recurring billing:** As with many other online services, even MSPs have adopted the model of open-ended and recurring billing. This offers clients greater flexibility and quickly deployable services and solutions.
- **Regular consultations with clients:** As opposed to the former model, today's MSPs need to communicate and engage with customers regularly. This creates closer relationships and helps avoid misunderstandings.
- **Remote troubleshooting:** A convenient, less time-consuming and above all, faster way to solve issues compared to the mostly outdated on-site model.

Your clients should always have an easy way to contact you. If you want to make sure that this is clear, create a series of custom desktops that incorporate your contact details. This will make your support team available and accessible in case of IT emergency.

6 TIPS TO MAKE YOUR MSP OFFER IRRESISTIBLE

As an MSP, you need to demonstrate your security expertise, offer a comprehensive portfolio of security solutions and services, and deliver added value to your clients.

LEARN MORE

ESET, North America
610 W. Ash Street, Suite #1700
San Diego, CA 92101

partnerservices@eset.com
(619) 876-5489
https://www.eset.com/us/

CYBERSECURITY EXPERTS ON YOUR SIDE