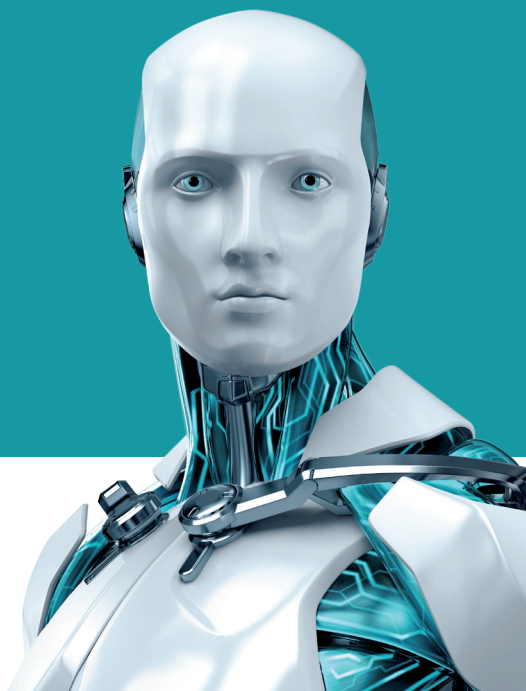
MAKE YOUR MSP OFFER IRRESISTIBLE WITH VALUE-ADDED IT SECURITY



ENJOY SAFER TECHNOLOGY™

CONTENTS

INTRODUCTION 2

THE WAVES THAT SHAPE TODAY'S IT SECURITY 3
- Ever-evolving cyberthreats 4
- Increasing regulatory requirements 4

HOW DO MANAGED SERVICE PROVIDERS FIT INTO THIS PICTURE? 5

WHERE AND HOW CAN MSPs DEMONSTRATE THEIR ADDED VALUE? . . . 6
- Know the client 6
- Apply cyber hygiene 6
- Choose the right security solutions 7
- Educate clients and their users 7
- Build proper infrastructure and engage with the client 7
- Avoid the break/fix model, be a modern MSP 7

ADVANTAGES OF THE ESET MSP PROGRAM 9

INTRODUCTION

Keeping the growing number of IT systems secure, patched, protected and compliant with various regulatory compacts is increasingly laborious for businesses of all sizes. This is especially true for small and medium businesses (SMB), for which cybersecurity incidents can have devastating consequences, ranging from data leaks, through reputational harm and on to the loss of clients.

However, with limits to their financial and human resources, it is natural that companies in this segment are looking for ways to manage risks and threats without compromising their primary goal: achieving growth while keeping daily operations smooth. To solve this dilemma and address their security needs, they increasingly turn to managed service providers (MSP).

To capitalize on this trend and grow rapidly, MSP vendors need to demonstrate their expertise in the field of security and knowledge of the threat landscape, present a comprehensive portfolio of security solutions and services, as well as offer added value to the client.

This whitepaper describes all the above-mentioned points in detail and brings additional information and tips in an actionable but easily digestible format. The last chapter is dedicated to the specifics of the ESET MSP program. It also explains why ESET is a powerful ally for the MSP segment, with its wide variety of complementary technologies and solutions able to address the most pressing security risks and challenges.description of the current trends connected to this cyberthreat. The main section details the most noteworthy Android ransomware examples since 2014 with focus on the most recent cases.

As has been a good tradition since we started publishing this report three years ago, the final chapter offers updated advice for Android users detailing best practice helping them to stay secure.

THE WAVES THAT SHAPE TODAY'S IT SECURITY

One of the significant factors MSPs have to take into consideration when building a custom security package for their clients are the threats faced by the given business sector.

Frequent phishing, social engineering and spying campaigns, doxing, distributed denial of service (DDoS) and ransomware attacks, leading to data leaks or data losses – those are just a few of "the waves" that currently shape the surface of business IT security. ESET systems process over 300.000 unique and possibly malicious samples every day, many of which have the potential to derail organizations' revenue streams and significantly disrupt their daily operations.

As shown by the ***ESET Business Security Survey 2016*** – conducted in seven European countries – cybersecurity incidents are no rare events. **In 2016, 71% of companies that took part in the survey experienced either an attack or a data breach**. Out of those, **75% faced a malware infection and one in three reported a social engineering attack**.

With the growing volume and value of data, breaches and leaks have also become a security risk that creates headlines almost on a daily basis. This is especially problematic for small and medium businesses (SMB). According to ***Aberdeen's analysis***, the **risk of a single data breach affecting up to a million records is higher for these companies by about 63% compared to larger organizations**.

"For SMBs there is a 90% likelihood of a singledata breach costing more than $216.000,".

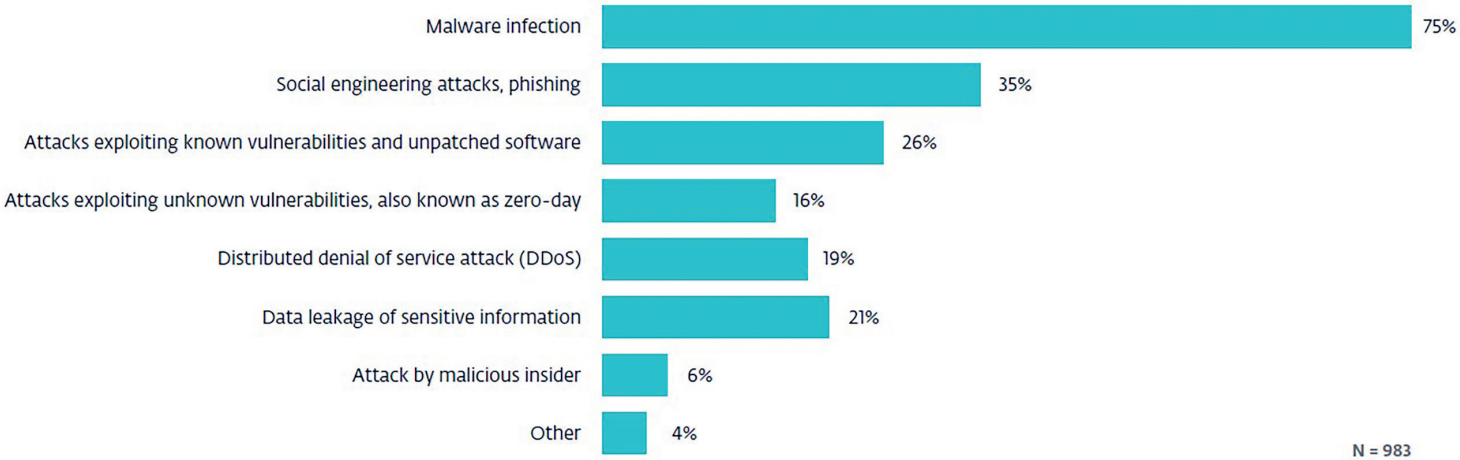


Figure 6
Which type(s) of cyber security incident has your company experienced in the past 12 months? (Multiple choice)

Ever-evolving cyberthreats

It's not only data breaches that keep the IT admins and security teams awake at night. Massive malware or ransomware campaigns seen in 2017 showcase the destructive impact that current cyberattacks can have on MSP clients.

In May 2017, a ransomware worm detected as **WannaCryptor.D (aka WannaCry)** spread rapidly using leaked NSA tools dubbed EternalBlue, which exploited a vulnerability in the most popular versions of Windows operating systems. Despite patches being issued by Microsoft more than two months prior to the attack, **hundreds of thousands of machines fell victim to the infection**. Files and systems of thousands of organizations around the planet – including critical sectors such as health care – ended up encrypted, with legitimate users unable to access crucial information.

Another massive incident with global consequences made headlines roughly a month later. At the end of June, malware detected as **Diskcoder.C (aka Petya or NotPetya)** started making rounds in Ukraine, but soon spilled over the country's borders, infecting businesses worldwide. At present, publicly ***admitted costs have surpassed one billion dollars.*** The attack disrupted the tax system of the entire country as Ukrainian authorities had to ***extend the country' tax-reporting deadline by several months.***

Increasing regulatory requirements

MSPs and their clients must also comply with the growing demands of legislation – the ***EU's General Data Protection Regulation (GDPR)*** being a perfect example of this trend. After the regulation comes into force in May 2018, all organizations operating within European member states, or holding the data of EU citizens, will have to follow strict policies and significantly increase the protection of their data records. If they fail to do so, they might face fines up to a maximum of 4% of the previous year's global revenue or €20 million (whichever is higher).

Apart from the high financial costs this might induce, GDPR also increases reputational risk for businesses of all sizes, as they have to publicly disclose all data breaches to the authorities and to all affected data subjects. This poses an opportunity for MSP vendors that can act as consultants to small and medium businesses (SMBs) struggling to fulfil the legislative requirements.

HOW DO MANAGED SERVICE PROVIDERS FIT INTO THIS PICTURE?

The above-mentioned threats and risks combined with the growing complexity of IT security technologies pose a great challenge for businesses, but at the same time represent new opportunities for MSP vendors. From the position of an external IT and security advisor, these providers can offer a better and more specialized service than an internal department could.

This is especially the case for small and medium businesses (SMB) whose financial and human resources are limited and whose priorities lie with their business goals, namely growth and smooth daily operations. Unfortunately, this is often at the cost of neglecting security, regulatory compliance or privacy. MSPs can turn this to their advantage and offer SMBs an attractive alternative:

1. ***Better control over the IT budget:*** *While keeping costs at bay, MSP vendors can offer a wider scale of services and products compared to the portfolio that is affordable for a client using solely internal resources. Opting for the services of an MSP vendor also leads to a higher level of financial flexibility and more predictable costs. Thanks to adjustable billing plans, clients also have increased control over their IT and security budget.*

2. ***Expertise/Trusted Advisor Approach:*** *Clients looking to improve their level of protection often perceive MSPs as IT experts as well as experts in the field of security. An MSP can fulfil this expectation by employing and presenting seasoned experts for both of these areas.*

3. ***Market Overview and Broad Offering:*** *Thanks to their IT focus, MSPs also have a better overview of the security products available on the market. Based on this knowledge, MSPs can attract new clients by offering a custom security package. On top of that, MSPs with broader and more comprehensive security services have a better shot at customer retention, higher revenue and growth. A broad portfolio shouldn't only include basic endpoint protection for multiple platforms, but also additional services, such as backup and disaster recovery solutions, network and infrastructure monitoring tools as well as additional security products crucial for password and data protection, such as two-factor authentication and encryption.*

4. ***Innovation:*** *MSP specialized security teams can make adopting and implementing innovative solutions easier and help clients keep pace with current market developments.*

5. ***Prepared for change:*** *MSPs enable their clients to add or remove any software or hardware according to their current needs without having to go through the painstaking process of acquiring, implementing and maintaining new hardware and software resources. Especially in the SMB sector, such needs can arise unexpectedly. Outsourcing to an MSP shifts the burden of this process to the provider, freeing employees on the client side for other internal tasks.*

6. ***High-quality Support:*** *MSPs can provide clients with the necessary infrastructure and software. This includes maintenance of these resources as well as high-quality and quick support in case a security issue occurs.*

Despite all the advantages and rapid expansion of the MSP segment, vendors operating in this space have to adjust to the increasingly competitive environment, and quality of service is far from the only thing SMB clients are looking for only one point not...

WHERE AND HOW CAN MSPs DEMONSTRATE THEIR ADDED VALUE?

The main goal of every MSP is to generate revenue and growth, but to achieve it, the MSP has to demonstrate the added value represented in their security offer. Here are a few tips that can help to fulfill all of these goals:

Know the client

To build good business relationships, vendors need to create an atmosphere of partnership and trust. An **initial security audit** shows the MSP's expertise and interest in the state of the client's IT systems, and can produce the threat intelligence necessary to adjust the client's current security strategy or to create a new one from scratch.

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

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

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

Thanks to this initial questioning, MSPs can also identify the appropriate threat model to apply to a particular customer and craft a custom security package that will help improve the level of client's protection.

Apply cyber hygiene

MSPs as a software and security provider should follow best cyber hygiene practices for both their own systems as well as their clients'. By applying proper patch management and by keeping operating systems, apps and security solutions up-to-date, providers can close many potential vulnerabilities in the SMB's systems.

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

The importance of cyber hygiene was well-illustrated by the WannaCryptor.D (aka WannaCry) 2017 incident mentioned earlier in this report. Despite the vulnerability in the Microsoft operating systems 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[1].

1 Devices running ESET solutions were protected weeks before the incident, thanks to ESET network detection closing the EternalBlue vulnerability.

Choose the right security solutions

On today's threat landscape, antivirus and perimeter security features such as firewall and anti-spam are already a must. However, based on customer needs, the vertical they operate in and regulatory requirements, additional products such as ***encryption***, ***two-factor authentication*** or data leak prevention (DLP) might be necessary.

All of these solutions should be low maintenance, easy-to-deploy and easy-to-use, as this enables MSPs to focus their strength where needed and allows the client to operate smoothly and undisturbed.

ESET solutions are designed to fit these MSP (as well as client) needs, and thus work 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 the products*
- *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 the 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 manually run scans, as this consumes hardware power while only duplicating the activity of real-time scanning*

For more information about ESET products and technologies, refer to the ***final chapter of this paper***.

Educate clients and their users

MSPs acting in the role of an external security advisor can also present added value by offering employee cybersecurity trainings and education. These should be tailored with regard to the level of technical knowledge of the client's staff, differing for management, IT personnel and regular users.

If an MSP has limited human resources or doesn't have the capacity to provide such services for other reasons, they can utilize educational materials created by security professionals.

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

- *Description of the **most common threats such as malware, social engineering and phishing***
- ***Rules of good password hygiene** – with useful tips about proper length, use of characters, regular changes and handling of passwords – and the importance of **two 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 and are thus more attractive targets for cybercriminals*

MSPs should also have a dedicated program for client's IT staff, including actionable tips and best practices for setting up the security products as well as networks and systems. Compared to trainings 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 setup of **password policies***
- *Correct setup of **admin and user profiles** on the company network*
- *Tips on how to **minimize the attack surface** of internal systems*
- *Specific settings for legitimate service that are often misused as attack vectors, such as remote desktop protocol (**RDP**), or **emails** and **email attachments***
- *Detailed **ransomware prevention** advice*

Build proper infrastructure and engage with the client

In the internet era, communication is key for almost any business sphere, including the MSP segment.

Today, organizations and especially SMB clients expect their security provider to **inform them in plain and easy to understand language** about what is happening in their IT systems. On top of that, MSPs also need to act as a filtering authority and notify the client only in key cases. Too many notifications about minor events can become a burden to the client and impair the trust in the provider's abilities.

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

In case of a security incident, an MSP has to be available and equipped to **act quickly** and **resolve** problems 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.

An MSP should also be **able to scale and adjust their systems**, infrastructure and software to fulfil ever evolving needs of the growing **SMB clients**.

Avoid the break/fix model, be a modern MSP

In the past, companies offering IT security services were often based on a break/fix model. This meant that the provider stepped in only when something went wrong, not to mention the time consuming on-site repairs. In this model, breakdowns, downtime and most importantly costly repairs were common and ended up on the client's bill as extra costs. On top of that, flagging problems and maintaining systems was often the responsibility of the customer, making it inconvenient and even more costly.

However, recent years have brought significant change to this outdated business model. To be a modern and instead MSP, providers should offer their clients:

- ***Value services:** It's not about selling products anymore. A modern MSP vendor needs to bring value to the table and persuade clients it is worth to invest in these services instead of building own 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 provided solutions. This lowers the burden on the client's side and enables the provider to stay constantly informed about both the state of and changes in the clients' 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 a higher flexibility and quickly deployable services and solutions.*
- ***Regular consultation with client:*** *As opposed to the former model, today's MSPs need to communicate and engage with customers regularly. This creates a closer relationship between both parties and helps avoid misunderstandings.*
- ***Remote troubleshooting:*** *Convenient, less time-consuming and most of all, faster ways to solve issues than provided by the older and mostly outdated on-site model*

ADVANTAGES OF THE ESET MSP PROGRAM

In a world of ever-evolving threats and growing risks, MSPs should be looking for reliable partners offering expertise and high-quality security solutions. ESET, as a well-known and established global cybersecurity player, is able to deliver on that front and enable its MSP partners to benefit from its experience in developing protective technologies.

As a full-fledged IT security vendor, ESET offers a number of innovative technologies that currently rank amongst the best in the world. Today, unique features such as UEFI scanner, DNA detections, its custom-built machine learning engine Augur, ransomware shield, advanced memory scanner, network attack protection module, exploit blocker or ESET's cloud based endpoint security are all part of its multi-layered solution. On top of that, ESET also offers separate technologies crucial for data and password security, namely encryption and multifactor authentication.

All of these can help providers in ESET MSP Partner Program meet the increased and ever growing demands of their clients by being:

- ***Lightweight:*** *ESET solutions have a low system footprint and minimal-hardware demandsEffective: High detection capabilities and low false positive rates*
- ***Easy to deploy:*** *ESET solutions also rank highly when it comes to rapid deployment compared with the competition*
- ***Tailored for MSPs:*** *ESET offers multitenant remote management via a specially crafted console tailored for MSP needs*
- ***Easy to integrate:*** *ESET offers support for a wide range of popular Remote Monitoring and Management (RMM) tools and PSA consoles*

And there are also business advantages to the ESET offering:

- ***Flexibility:*** *Within the ESET MSP Program, MSPs can flexibly add or remove seats instantly in a self-managed portal*
- ***Control over budget:*** *The ESET daily billing model allows MSPs to easily adapt to customer or market developments. MSP administrator can also generate handful of granular reports and performance tracking for each customer*
- ***Local support anywhere:*** *ESET products are available in 20 languages and offer support in 200 local languages, which helps MSPs achieve first class delivery to their customers*
- ***Marketing and sales support:*** *Content marketing tools and materials to help MSPs address the security needs of their customers*

January 2018

ESET, spol. s r.o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
Slovak Republic