ESET® MSP PROGRAM

YOUR NEW PROPOSITION
DATA PROTECTION

Help your customers solve their data protection challenges by offering solutions that prevent data breaches and the resulting penalties now mandated by law. Save your customers money, and unlock new revenue streams for your business.

Solve real customer problems, unlock new revenue streams

As their trusted MSP, you can help your customers to take the right security steps and block potential attackers.

### Turn compliance concerns into revenue

Data protection legislation is an ongoing obligation for both you and your clients. Evolving regulations require organizations of all sizes to adopt new processes and policies. Your clients will need assistance to ensure compliance, and ESET can help you provide this.

Strengthen your security offering

To differentiate your offer, endpoint protection alone is no longer enough. By adding **encryption** and **multi-factor authentication (MFA)** to your portfolio you will significantly improve your competitive edge.

ENDPOINT + **ENCRYPTION** + **MFA**

According to a survey ESET carried out among MSP partners, current client IT security challenges also include:

66%
Spam and phishing

61%
Ransomware

26%
Compliance
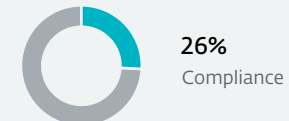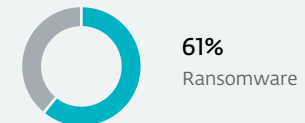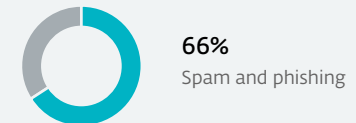
Source: ESET polled 488 MSP partners in 14 countries during July 2019 an via online questionnaire

Why should your clients care about encryption?

Endpoint encryption is an essential data security tool, providing full disk encryption on endpoint devices. It prevents stolen data from being read and misused if they fall into the wrong hands.

Over 80% of companies hold personally identifiable information (PII) on their customers, as well as on their own employees.

Data collected from over 27,000 participants – mostly from European Union (EU) via ESET's GDPR compliance check form (2018).

Data breaches

Unencrypted data breaches put data at risk of being released, publicized, or used for malicious purposes. All companies have sensitive data, such as customer lists, proprietary information, sales-related data, staff and HR information. By implementing an encryption solution, businesses **make it virtually impossible for hackers to read stolen data**.

The security challenges of remote working

Allowing employees to work from home has become the norm for many businesses. Also, the need for remote users always to be online, working out of coffee shops, airports and at client premises, increases the risk of data misuse or device loss.

However, an encryption solution gives your clients the ability to immediately terminate remote users and **render data on any device inaccessible**, thus effectively mitigating the risk.

Compliance

When it comes to encryption, many regulations and laws, such as GDPR, PCI-DSS, HIPAA, SOX and GLBA, recommend its implementation. If a company's data, including personal information are properly encrypted, **data breach incidents are much less likely to be regarded as compliance failures**.

ESET encryption is powerful, and simple to deploy

ENCRYPTION

How easy is it for you?

- ✓ **ESET Full Disk Encryption** is available via a convenient monthly MSP model

- ✓ Add and remove licenses as client needs change

- ✓ Remotely managed via ESET PROTECT

- ✓ Extremely simple deployment

- ✓ Can be deployed independent of ESET Endpoint Security

How easy is it for your clients?

- ✓ Zero impact on employee productivity

- ✓ Fast, seamless deployment without any downtime

- ✓ No employee training required

- ✓ No special hardware required (TPM chips are supported, but not required)

Full disk encryption is a large opportunity for MSPs - either as a cross-sell, or as a standalone product:

1/3
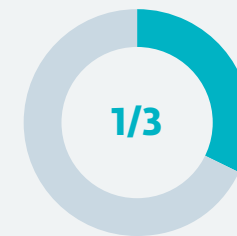
Only one-third of companies have implemented encryption, according to 488 MSPs surveyed by ESET in 2019

Add another layer of data access protection

MFA

Multi-factor authentication (MFA) solutions, like ESET Secure Authentication, that require two or more independent pieces of information to verify a user's identity. MFA is much stronger **than traditional, static password or PIN authentication.**

80% of hacking-related breaches involve compromised an weak credentials.

Source: Verizon 2017 Data Breach Investigations Report, 10th Edition

Poor password hygiene

Weak password practices are a significant cybersecurity risk for your clients. Not only do employees utilize identical passwords across multiple websites and applications, they sometimes share their passwords with friends, family and co-workers. Even where businesses enforce password policies, this can lead employees just to use variants of their previous password, or write their passwords on sticky notes. **MFA protects business against poor password hygiene** by implementing an additional authentication element, e.g. a unique code generated by the employee's phone. Having an MFA solution in place can prevent attackers from gaining access to company systems by simply guessing weak passwords.

Data breaches

One of the most common ways hackers can gain access to your clients' data is through stolen passwords, or a targeted attack. By adding an MFA solution businesses make it much more difficult for hackers to gain access to their systems. Traditionally, **the top targets** for data breaches are **financial, retail, healthcare and public sector organizations**. But hackers are now targeting other sectors too.

Compliance

Several compliance regulations mandate MFA, and most stress the need for stronger authentication practices, including GDPR and HIPAA. Multi-factor authentication is no longer an optional solution. **Regulation agencies** such as ENISA **strongly recommend it for businesses that handle credit cards or financial transactions**. All organizations should evaluate their compliance. With ESET's support, you can help them.

Implementing multi-factor authentication

MFA

33%
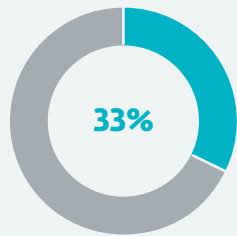
33% of MSPs consider MFA their fastest growing service

Source: ESET polled 488 MSP partners in 14 countries during July 2019 via online questionnaire

ESET Secure Authentication provides an easy way to implement MFA across commonly utilized systems such as VPNs, Remote Desktop, Outlook Web Access, operating system login, and web/cloud services such as Office 365, Google Apps, Dropbox and many others, via ADFS 3.0 or SAML protocol integration.

How easy is it for you?

- ✓ Convenient monthly payment model
- ✓ Add and remove licenses as client needs change
- ✓ Completely intuitive remote deployment and management
- ✓ No additional infrastructure costs
- ✓ Supports numerous VPNs

How easy is it for your clients?

- ✓ Prevents user frustration caused by the need for ever more complex passwords
- ✓ Works with existing smartphones
- ✓ Single-tap solution, no need to retype passwords
- ✓ No additional hardware needed
- ✓ No employee training required

Set yourself apart from the competition

Your new proposition can be to offer your clients data protection solutions **rather then simple endpoint protection. Introducing added value solutions does not have to be difficult. ESET offers hassle-free solutions that help you to:**

Increase your product line offering and open additional selling opportunities

Help customers address their compliance challenges

Break into new verticals and market sectors

Complement your current pricing structure using ESET's pay-as-you-go model

YOUR NEW
PROPOSITION
DATA PROTECTION

Help your customers solve their data protection challenges
by offering solutions that prevent data breaches.

ESET
CYBERSECURITY
EXPERTS ON YOUR SIDE