CYBERSECURITY
EXPERTS ON YOUR SIDE

THE '3DS' OF ENDPOINT SECURITY TO SECURE YOUR DIGITAL TRANSFORMATION

Not long ago, there was an image circulating on social media suggesting that unforeseen external factors could arguably be the best digital transformation accelerator. Even IDC, a leading market intelligence analyst, has stuck to their forecast that **digital transformation spending will continue its double-digit growth in 2020** amid the pandemic.

This doesn't come as a surprise as businesses understand the importance of digital transformation and the role cybersecurity in safeguarding IT infrastructure. Digital transformation has helped businesses to expand their digital presence, adopt new technologies, boost productivities and in recent time, to swiftly migrate their operations to a work-from-home (WFH) model. As a result of this, endpoints have gone beyond the boundary of corporate firewalls with more employees stay connected remotely, and this has widened the attack surface.

Without proper security in place, cyber threats such as zero-day exploits, phishing, fileless malware attacks and ransomware amongst many others, could bring SMBs and enterprises to their knees. This would lead to reputational, monetary and productivity losses. Based on our **study**, cybersecurity breaches had cost companies within the APAC region an average of more than US$100,000 in losses a year. Endpoint security is an area that businesses should not take for granted.

Endpoints must be kept secured to ensure sensitive data do not fall to the hands of bad actors. Such data is highly prized by ransomware gangs as businesses are more likely to pay for ransom if sensitive data, such as trade secrets and credit card information, are encrypted and rendered inaccessible to businesses.

As easy as it sounds, selecting the right combination of products to protect your business, regardless if you are an SMB or enterprise, can be a difficult task given the plethora of endpoint security products and services in the market. To determine which are the best solutions, you must consider the 3Ds: **detect**, **defend** and **deter**.

Detect malicious activities

The ideal endpoint security product should have the ability to detect and block near 100% of in-the-wild malware, have close-to-zero false positives and hardly consume any computing power. The rationale here is quite simple: this will give you adequate protection against cyberattacks without affecting your endpoints' performance and require minimal human intervention to investigate false alarms. Alex Teh, CEO of Chilisoft, has recently written a great **article** about why these factors are the trifecta of a good endpoint security software.

Our security software, **ESET Endpoint Protection Platform**, had achieved **high scores** in these three aspects, as validated by a leading independent testing laboratory. This was thanks to the effectiveness of our **multilayered approach** in mitigating cyberattacks. Our products are powered by various technologies ranging from machine learning, DNA detections, behavioural blocking to cloud malware protection system and UEFI scanner. A single line of defence is simply not enough today when bad actors are getting increasingly creative.

Also, you might have heard of instances where vendors or resellers are positioning their endpoint security products side-by-side with Endpoint Detection and Response products (EDR), saying that when using together, these two solutions can thwart every single type of cyberattack. Such statement must be taken with a pinch of salt as not all businesses, especially SMBs and small enterprises, have the resources to deploy EDR.

To realise the full potential of EDR, you would need a team of highly trained cybersecurity engineers that can perform sophisticated investigations and remediations when the endpoint security product failed to block malware and flagged potential breaches, both real and false positives. You would not end up in this position if you are using an endpoint security product that could effectively stop the malware in the first place without requiring further actions by an expert. At ESET, we have been advocating that our EDR solution, **ESET Enterprise Inspector**, as an additional layer of defence and not a substitute to plug the gaps in endpoint security products that are providing inadequate protection.

Now, this brings us to the second 'D' in the basics of cybersecurity: **defend**.

Defend endpoints and data

Like in any team sports, the ability to defend your endpoints quickly as a unit forms the foundation of a winning formula. While ESET Endpoint Protection Platform offers in-product sandbox, nothing beats the prowess and speed of **ESET Dynamic Threat Defense** (EDTD), a cloud-based sandboxing technology.

Time is of the essence in cybersecurity as cyberattacks can cause outages in areas that are critical to business operations. **In the case of a South African power company, a ransomware attack in 2019 had made it impossible for its customers to refill their accounts and buy electricity, leaving some residents without power.**

In addition, a ransomware attack usually also means a lengthy IT downtime. A company that is specialised in ransomware settlement and recovery had recently published a report highlighting the **average days of downtime caused by the ransomware was 16 days in Q1 2020**. They had also reported the average ransom paid by affected businesses was a whopping USD 178,254 in the same quarter.

EDTD adds value to our endpoint security products by **undertaking the analysis of suspicious files via a vastly more powerful, dedicated system that resides in the cloud**. This reduces the analysis time of never-before-seen threats (zero-day) from hours and even days to under five minutes while protecting 'patient zero', the device where the suspicious file is detected. If a threat is identified, computers within the same company will then be updated and protected within around two minutes of the patient zero.

As employees are taking home with them valuable company's data that resides in their work computers, you should also consider using **ESET Full Disk Encryption**. This ensures that every data stored on each endpoint is locked down and secure, protecting you against loss or theft. Besides, the solution enables you to comply with data protection regulations.

Having all these safeguards will not mean anything if you cannot ensure they are being properly used 24/7. This brings us to the third and last 'D': **deter**.

Deter bad actors and prevent data breaches

Endpoint security products should not be approached with an install-and-forget attitude. Businesses might try to deter bad actors and preventing data breaches by coming up cybersecurity policies and sharing them with employees. This is not sufficient as **human error is one of the leading causes of data breaches**.

Businesses need not only the right security policies but also the ability to enforce them to deter bad actors and prevent data breaches from happening. Remote working has made this harder, but it not an impossible task to achieve. Here is where cloud-based remote management tools like ESET Cloud Administrator come in handy.

These solutions allow you to remotely manage the security of all endpoints from one single pane of glass, as well as to automate policies and tasks for specific computers or static or dynamic groups. Besides, they provide real-time visibility for on-premise and off-premise endpoints, which is perfect for the WFH environment. In other words, you can ensure the endpoint security software in all of your company's devices, regardless of location, are always updated and running without the risk of being disabled.

CYBERSECURITY
EXPERTS ON YOUR SIDE

All the endpoint security solutions that you need in a single bundle

ESET has put together bundled solutions consisting of endpoint security products that are essentials to protect your endpoints and safeguard your digital transformation. These bundled solutions offer great savings, as well as feature industry-leading customer experience and unparalleled IT security performance.

Designed for Small and Medium Enterprises, **ESET PROTECT Advanced** features:

- Endpoint Protection,
- File Server Security,
- Cloud Sandbox,
- ESET Full Disk Encryption
- Cloud or On-premise Console

Designed for Enterprises, **ESET PROTECT Complete** features:

- Endpoint Protection,
- File Server Security,
- Cloud Sandbox,
- ESET Full Disk Encryption,
- Mail Security,
- Cloud app protection,
- Cloud or On-premise Console,

TAKE THE NEXT STEP

Want to find out more about ESET's security solution to secure your digital transformation? Click on the "LEARN MORE" button below.

LEARN MORE

CYBERSECURITY EXPERTS ON YOUR SIDE

For over 30 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit ***www.eset.com****.*

Copyright © 1992–2019 ESET, spol. s r. o. ESET, ESET logo, ESET android figure, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo and/or other mentioned products of ESET, spol. s r. o., are registered trademarks of ESET, spol. s r. o. Windows® is a trademark of the Microsoft group of companies. Other here mentioned companies or products might be registered trademarks of their proprietors. Produced according to quality standards of ISO 9001:2015 and information security standards of ISO 27001:2013.