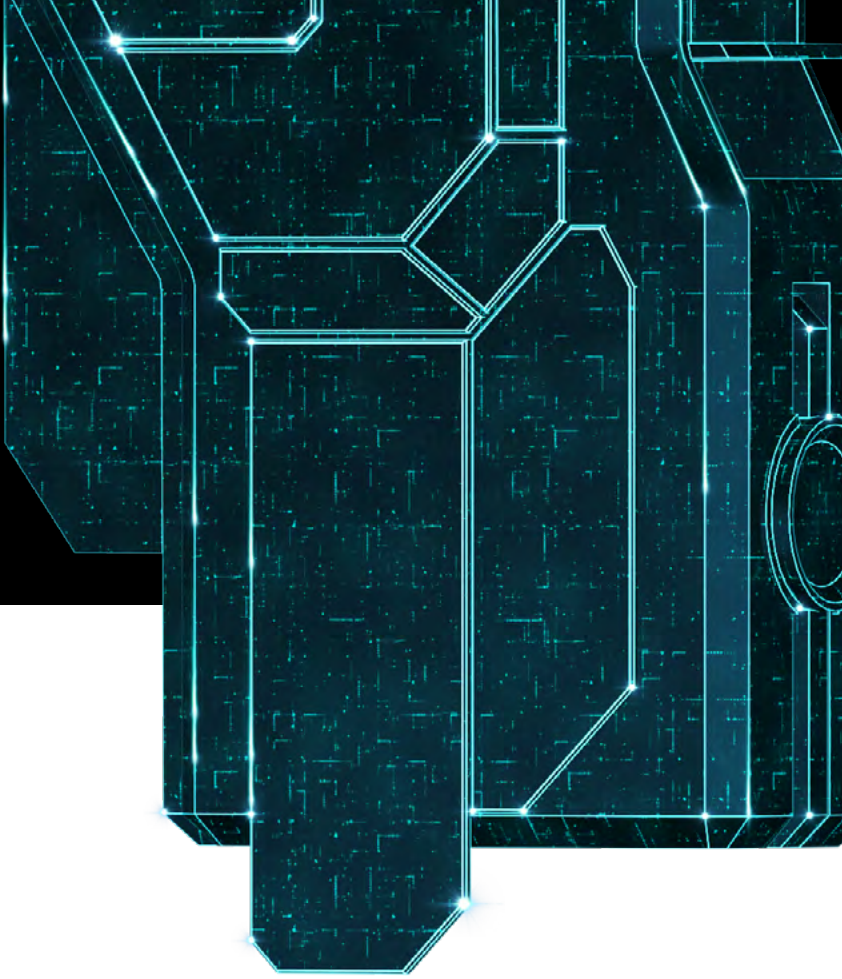
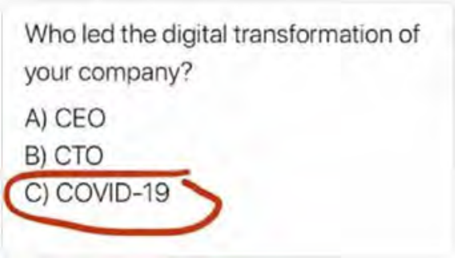
CYBERSECURITY
EXPERTS ON YOUR SIDE



DETECT, DEFEND AND DETER: THE 3 D'S OF SECURE DIGITAL TRANSFORMATION

Not long ago, the following image was circulating on social media, suggesting that unforeseen external factors could arguably be the best digital transformation accelerator:



Who led the digital transformation of your company?

A) CEO

B) CTO

[✓ C) COVID-19]

Digital transformation is the process of using digital technologies to create new, or modify existing, business processes and customer experiences to meet changing business and market requirements. Over the years, digital transformation has helped businesses to expand their digital presence, adopt new technologies and boost productivities.

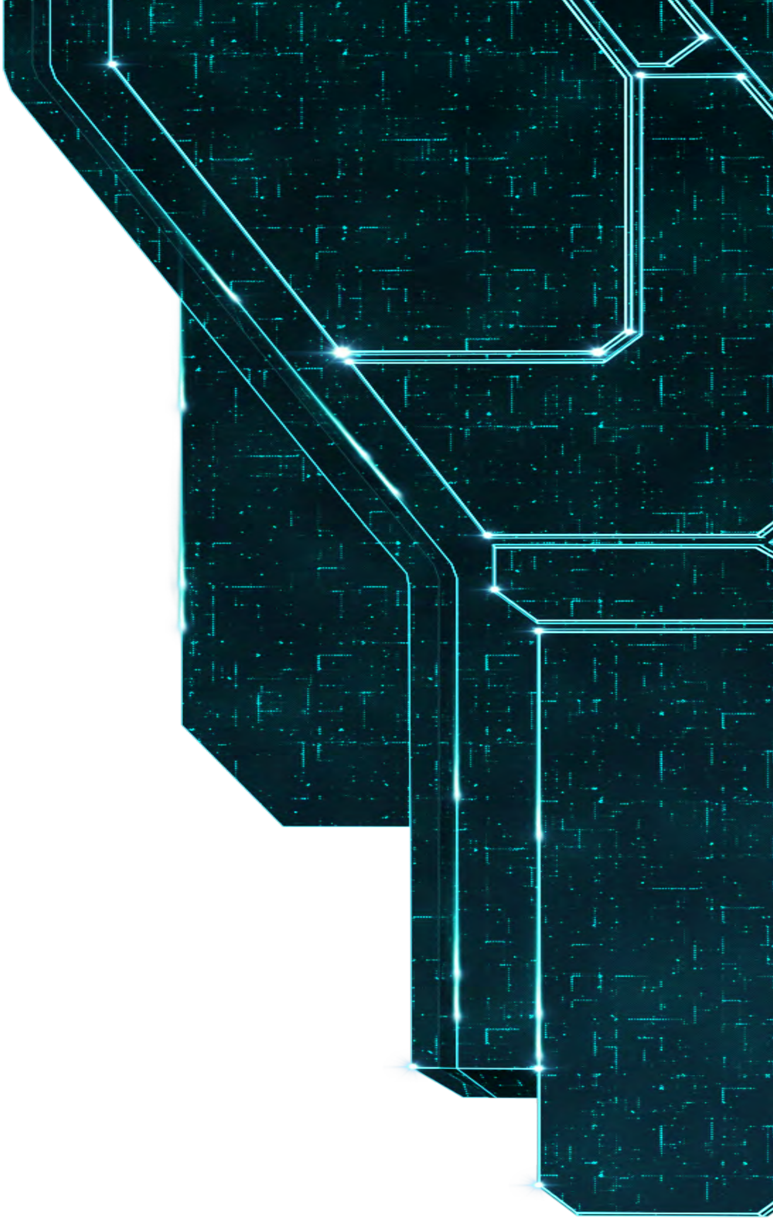
More recently, it has allowed organizations to swiftly migrate their operations to a work-from-home (WFH) model in response to the Covid-19 pandemic.

As a result of this, endpoints have gone beyond the boundary of corporate firewalls with more employees staying connected remotely. This, in turn, has widened the attack surface.

Without proper security in place, cyberthreats such as zero-day exploits, phishing, fileless malware attacks and ransomware can bring SMBs and enterprises alike to their knees. Successful cyberattacks can result in reputational, monetary and productivity losses—so endpoint security is an area that businesses should not take for granted.

Endpoints must be kept secured to ensure sensitive data doesn't fall into the hands of bad actors. Such data is increasingly prized by ransomware gangs out to steal and then encrypt trade secrets, credit card details and other invaluable information—rendering it inaccessible to a business unless a steep ransom is paid. Often, even paying the price doesn't ensure the return of the data.

Selecting the right combination of products to protect your business, regardless of size, can be difficult given the plethora of endpoint security products and services in the market. To determine which are the best solutions for your organization, you must consider the 3 Ds: **Detect, defend and deter.**



1. DETECT MALICIOUS ACTIVITIES

The ideal endpoint security product will be able to detect and block close to 100% of in-the-wild malware; have near-zero false positive rates; 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 without requiring much human intervention to investigate false alarms. Alex Teh, CEO of Chillisoft, has written a great **article** about why these factors are the trifecta of a good endpoint security software.

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

You can easily augment your detection and analytic capabilities with **ESET Enterprise Inspector**, our endpoint detection and response (EDR) solution. This sophisticated tool uses real-time data to evaluate everything happening on endpoints and networks, including user, file, process, registry, memory and network events.

Knowing how a threat infiltrated your network enables you to prevent future attacks, as well as isolating developing threats and identifying risky user behaviors.

This brings us to the second 'D' in the basics of cybersecurity: **Defend.**

2. DEFEND ENDPOINTS AND DATA

To use a sports analogy, 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 sandboxing, nothing beats the prowess and speed of **ESET Dynamic Threat Defense** (EDTD), a cloud-based sandboxing technology.

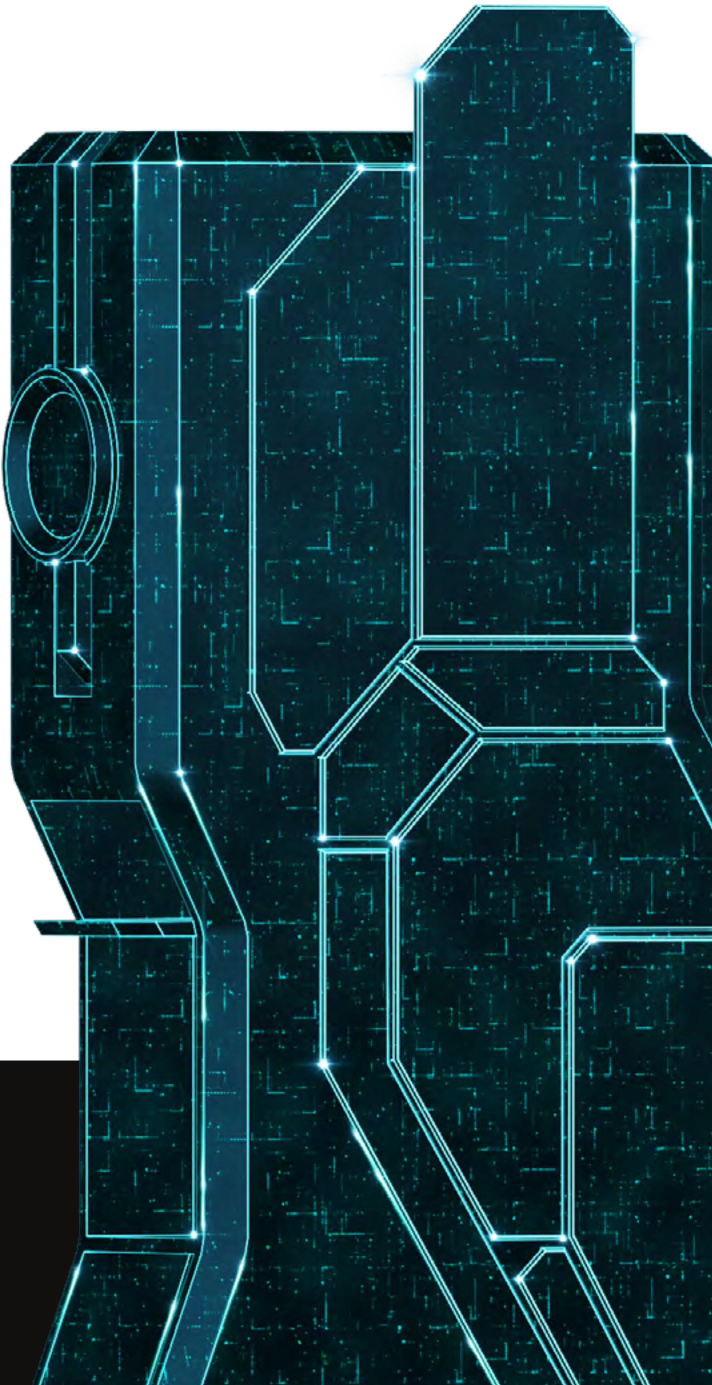
Time is of the essence in cybersecurity as cyberattacks can cause outages in areas that are critical to business operations. In the case of a South African power company, a **ransomware attack** in 2019 made it impossible for its customers to refill their accounts and buy electricity, leaving some residents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

In addition, a ransomware attack usually also means a lengthy IT downtime. A company that specializes in ransomware settlement and recovery published a **report** last year noting the average downtime caused by ransomware was 16 days in Q1 2020. They also reported the average ransom paid by affected businesses was a whopping $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 exploits) 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.

As employees take home valuable company data that resides in their work computers, you should also consider using **ESET Full Disk Encryption**. This ensures that data stored on each endpoint is locked down and inaccessible to unauthorized users, protecting you against loss or theft. This solution also helps you comply with data protection regulations.

Of course, 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.**



3. DETER BAD ACTORS AND RISKY BEHAVIORS

When it comes to endpoint security, businesses need not only the right security policies—but also the ability to enforce them to deter bad actors and prevent risky behaviors by users that could lead to data breaches.

Remote working has made this type of supervision more difficult, which is where a cloud-based remote management tool like **ESET PROTECT Cloud** comes into play.

This solution allows 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. This easy-to-use console provides real-time visibility for both on- and off-premises endpoints, which is perfect for the WFH environment. The console is also available as an on-premises management solution.

GET ALL THE ENDPOINT SECURITY SOLUTIONS YOU NEED IN A SINGLE BUNDLE

ESET offers bundled solutions with the essential elements for protecting your endpoints and safeguarding your digital transformation. These solutions offer great value, combining unparalleled IT security performance with friendly U.S.-based tech support.

ESET PROTECT Advanced, suitable for businesses of all sizes, includes:

- Advanced protection against ransomware and zero-day threats via cloud-based sandboxing
- Full disk encryption for system disks, partitions or entire devices
- File server security
- Cloud-based management console you can access anytime, anywhere

See how ESET security solutions will secure your digital transformation today.

GET STARTED

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.