



Digital Security
Progress. Protected.

Zero Trust Security

Customized IT security
for every protection need



The current situation

Zero Trust in focus

For many companies and their employees, the COVID-19 pandemic has completely changed the world of work and business. Millions of people in Germany, Austria and Switzerland continue to work from home. But what else will change the reality? Which economic areas and IT segments will benefit from this digitalization and home office push? What does the situation look like in terms of data security? And above all, what holistic IT security approaches can companies use to ensure the security of their IT infrastructure and effectively protect their assets, despite the rapidly changing framework conditions?

The not entirely new Zero Trust approach is once again coming into focus for many organizations. The use of such “buzzwords” alone scares off many decision makers, while others capitulate early on for fear of excessive costs or because of a perceived lack of their own resources. However, the basic idea of “we do not trust any entity, neither inside nor outside our own perimeters” is extremely useful, especially against the backdrop of growing threats. ESET takes an approach here that is compatible for all organizations. We don't want to leave any users “behind” or even technologically dependent. With a simple maturity

model, implementation with us is possible in stages and makes sense for any size of organization.

Whether as a standard license or as a managed service, the ESET Multi-Secured Endpoint, i.e. the combination of endpoint security, encryption, multi-factor authentication and cloud sandboxing, forms the right foundation for Zero Trust. Depending on the requirements in the corresponding environment, an Endpoint Detection & Response (EDR) solution then complements the needs of a complete visibility (inside view) on one's own devices and processes. For organizations that also operate their own Security Operation Centre (SOC) and are often exposed to the risk of targeted attacks, it is important to operate a suitable early warning system (outside view) using Threat Intelligence (TI). Here, ESET's third stage of expansion helps to expose burgeoning or planned attacks at an early stage and to optimally monitor important assets.

CURRENT CHALLENGES



Our security maturity model

The three steps to Zero Trust

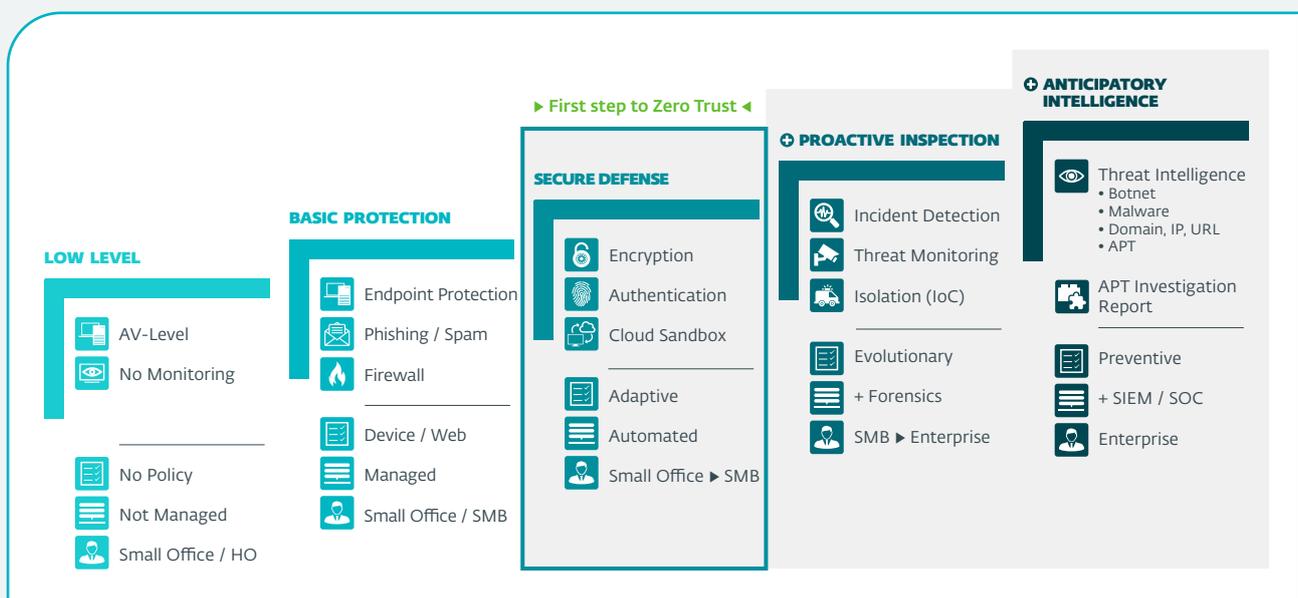
“Secure perimeters are obsolete; the transformation to post-pandemic standards began long ago.”

Michael Schröder, Security Business Strategy Manager, ESET DACH

Our strategic approach is based on the Zero Trust concept for IT security conceived by Harvard University. ESET has taken this conceptual basis, developed it further and tailored it to the needs of different organizational sizes. In short, it is a matter of classifying all internal and external devices, processes and people as potentially dangerous in principle. In times of COVID-19 and working from home, this has proven to be imperative.

ESET's Zero Trust security approach consists of a three-level maturity model that builds on each other. The higher the level, the more secure the protection - in other words, the more "mature". The model starts with the basic level "Basic Protection Plus", which follows the principle of ESET's Multi-Secured Endpoint approach. This is suitable as a foundation for Zero Trust for any organization, regardless of its individual protection needs. This is followed by two Zero Trust levels with complementary security technologies and services.

THE ESET SECURITY MATURITY MODEL

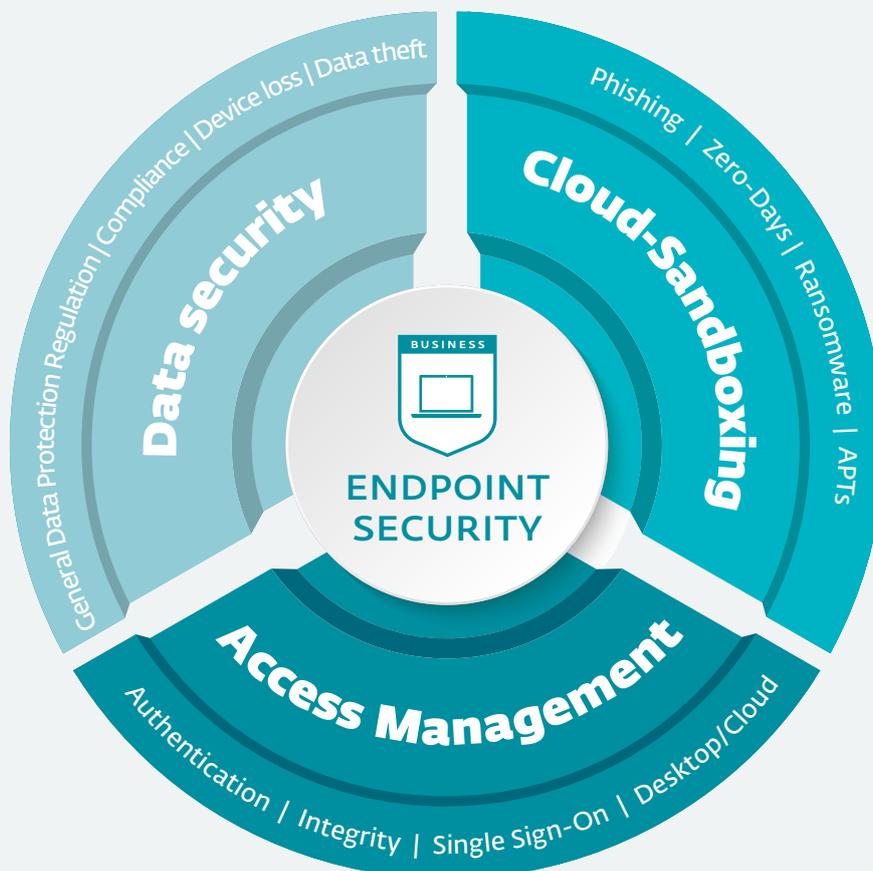


Level 1: Secure Defense

The Multi-Secured Endpoint as the foundation for Zero Trust Security

IT managers have to meet more and more demands against the backdrop of the current situation with unchanging resources. Implementing much-needed solutions to protect against data/password theft, ransom ware, APTs, and zero-day threats in a remote situation presents immense challenges to organizations of all sizes. The Multi-Secured Endpoint protects all endpoints and servers across operating systems with award-winning multi-layered technology, secures access management

with multi-factor authentication, supports organizations in data security (including GDPR and compliance requirements) with certified encryption products, and keeps the corporate network free from all kinds of threats thanks to cloud sandboxing.



Data security and integrity application example

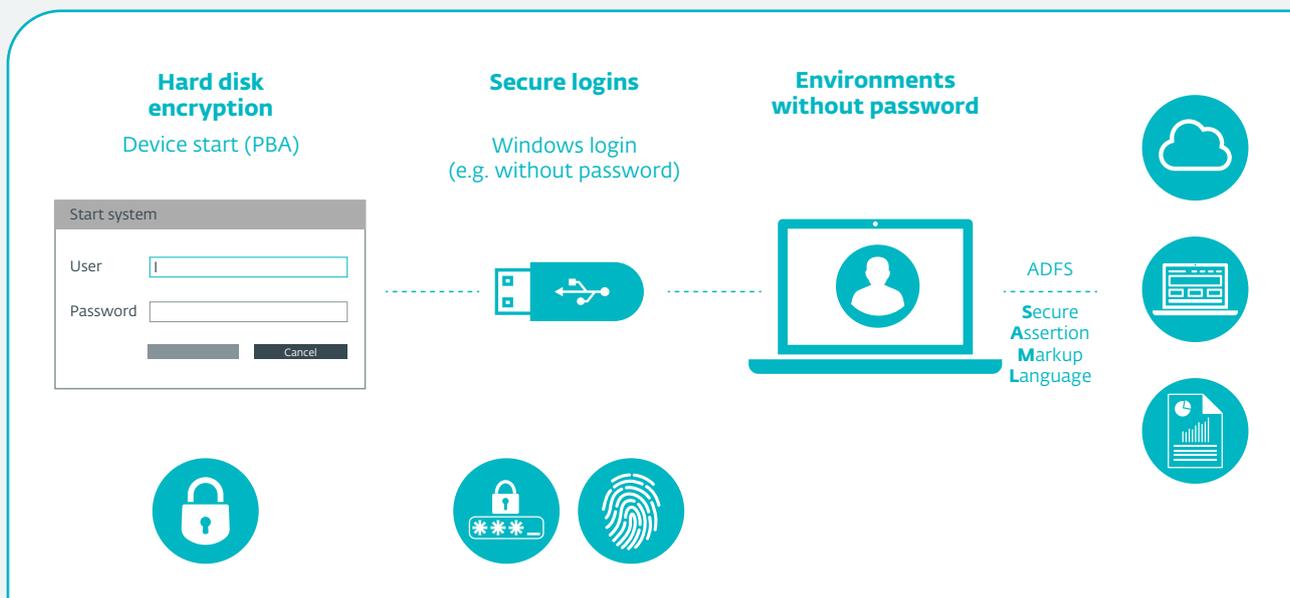
FULL DISK ENCRYPTION

ESET Full Disk Encryption (EFDE) is a hard disk encryption with preboot authentication (PBA) developed by ESET for endpoints running Windows or macOS operating systems. Your mobile devices can thus be conveniently managed via our central management console - ESET PROTECT. ESET Full Disk Encryption not only protects businesses from data loss, but also helps you comply with data protection regulations such as the GDPR. With just one click, the solution easily encrypts system disks or partitions remotely, protecting the dormant data on your devices in case of theft or loss.

SECURE AUTHENTICATION

Multi-factor authentication (MFA), often known as two-factor authentication (2FA), is a powerful authentication method that requires users to identify themselves with more than one element. By combining a static password with a second, dynamic factor, the risk of data loss is significantly reduced. ESET Secure Authentication (ESA) serves as a basis for organizations to meet compliance requirements and acts preventively to avoid access control incidents. With ESA, organizations of all sizes easily implement MFA for shared systems (Windows & Server logins, Microsoft Cloud services such as Microsoft 365 or OWA, SAML, FIDO, ADFS 3.0, VPNs and RADIUS-based services).

Note: ESET Full Disk Encryption is available exclusively as an upgrade for endpoint licenses or available in individual bundles.



Application example for hardened endpoints and mailboxes via cloud sandboxing

eSET DYNAMIC THREAT DEFENSE

With ESET Dynamic Threat Defence (EDTD), you have a cloud-based sandbox analysis that significantly raises the level of protection for Exchange Server and endpoints, virtually eliminating threats such as zero-day attacks, APTs, attachment phishing, ransomware, or any other malware distributed via USB or download (web, Microsoft 365, SharePoint). Potentially dangerous and unknown binary code found by the ESET Endpoint solution is sent to the cloud sandbox for analysis. You can define the criteria for submitting the samples in detail via policies. In the cloud, the sample is run in physical and virtual environments and analyzed using AI and various machine learning algorithms. The result of the scan is then made available to all endpoints in your organization (even outside your corporate network).

THE MOST IMPORTANT FEATURES IN A NUTSHELL:

- Optimized protection thanks to cloud-based sandbox analysis using AI and machine learning algorithms
- Submitted samples are analyzed in an ESET-owned cloud in Europe
- Analysis results are immediately made available to all endpoints in your organization
- Detailed analysis report after an average of two to five minutes
- Detailed customization of the rules on which files to submit
- Easy rollout by adding the EDTD license to ESET PROTECT

Note: ESET Dynamic Threat Defence is only available as an upgrade for endpoint licenses or in individual bundles.

Cloud sandboxing eliminates the threat even before it reaches the user.



Level 2: Proactive Inspection (Inside View)

Detect anomalies in real time and maintain control over your environment

eSET ENTERPRISE INSPECTOR

ESET Enterprise Inspector (EEI) is an endpoint detection and response (EDR) solution to prevent, detect and remediate security incidents in your organization. It enables you to sustainably secure your corporate network and detect emerging threats in real time. Thanks to extensive analysis capabilities, ESET Enterprise Inspector provides forensic insights into current as well as past incidents and helps you prevent future attacks. Alerts can be ranked, prioritized, and tracked based on their threat potential using flexible predefined scoring capabilities, providing IT admins with immediate notification of malicious activities and processes. When alerts are received, ESET Enterprise Inspector also provides suggestions for possible countermeasures.

Organizations today need to be fully aware of what's happening on their network to promptly identify external attacks, employee misconduct and unwanted applications.

Endpoint + EDR = Endpoint Protection & Response (EPR)

ESET's Endpoint Solutions
Every single layer of our endpoint solution delivers data to ESET Enterprise Inspector.

A comprehensive EPR solution
to defend against threats to your network, including prevention, detection and remediation measures.

ESET Enterprise Inspector
Sophisticated EDR tool that lets you analyze large amounts of data in real time to detect any threat early.

Level 3: Anticipatory Intelligence (External View)

Preventive protection through perfect situational awareness

eset THREAT INTELLIGENCE

ESET Threat Intelligence (ETI) adds the knowledge of the World Wide Web to the protection level of your corporate network and informs you early on about targeted attacks, APTs, zero-day threats and botnets. The ESET security solution thus supports IT managers in identifying threats to the corporate network at an early stage.

ETI bridges the gap between information from our own network and data collected by ESET from the digital world. It uses information collected from more than 110 million sensors worldwide via ESET LiveGrid®, which is transmitted to our cloud-based security system and processed in our research and development centres around the globe. Thus, ESET is able to provide its customers with vast and special knowledge to better understand the risks and effectively respond to threats.

A reliable data basis with an assured reputation as well as an extremely low false positive rate is of enormous importance to operators of a SOC. Only the combination of all the findings provides a perfect picture of the situation.

Reporting + Datafeeds = External Situation Picture

Early Warning System
Monitors your assets in cyberspace using one of the best data foundations in the world.

ESET Threat Intelligence
delivers global data from secured sources in real time, protecting your online presence, certificates and apps and ultimately your reputation

Data feeds
110 million sensors, honey pots, DarkWeb and social media data, and in-house teams of experts ensure quality.



PROTECT

Central management console
Holistic, simple, flexible



Optimized bundles
Broad portfolio of offers



AUTHENTICATION



ENCRYPTION



CLOUD SANDBOXING



ENDPOINT DETECTION &
RESPONSE



ENDPOINTS/SERVER



CLOUD SECURITY



MOBILE DEVICES



THREAT INTELLIGENCE
SERVICES

Complementary solutions

The answer to your needs

CENTRAL MANAGEMENT CONSOLE

- Cloud or on-premises operation
- Optimized for managed service providers
- Automation through dynamic groups
- Hardware and software inventory
- Individual reporting
- Supports all relevant operating systems

OPTIMIZED BUNDLES

- Customized offering from home office to enterprise
- High flexibility: on-premises today, cloud tomorrow
- Attractive and fair conditions
- Expandable and upgradeable
- Broad coverage of legal requirements
- Fair Use Policy - agile management of your licenses



Please **contact us**

Whatever your business size, our scalable and customizable solutions will keep you protected against any threat.

On-premises or cloud-based – the choice is yours!

Contact your ESET partner support or [contact us directly](#) with your needs, requirements and questions. We'll make sure you get the level of protection that's right for your business.

Information Security

for companies of any size

TECHNICAL REQUIREMENTS:

- ESET PROTECT (cloud or on-premises operation)
- Valid ESET license for ESET Endpoint and/or Mail and/or Server Security
- ESET Business Account linked to ESET PROTECT
- Participation in ESET LiveGrid® (cloud-based reputation database)

QUALITY MANAGEMENT - MADE IN EU:

- Available everywhere - fully automated protection of the entire organization
- Full control over your data thanks to transparent (sample) analyses within the EU
- Unique speed in analyzing incoming alerts
- Reliable and secure - easily meet all requirements of data protection regulations (e.g. GDPR)
- Great flexibility in terms of license type, hardware usage and infrastructure requirements

KEY FEATURES IN BRIEF:

- Remote management console (cloud-based or centrally managed)
- Also available as a managed service (MSP)
- Extensibility options:
 - Endpoint Detection and Response
 - Threat Intelligence Services

BENEFITS FOR ENTERPRISES:

- Additional security layer for the IT infrastructure
- Relieve employees and conserve (hardware) resources
- Extend compliance and security standards
- Central management of all ESET security solutions via ESET PROTECT
- License diversity - combine any operating system (Windows, Mac, Linux) and device (mobile, desktop, server) according to your needs

Try it out with confidence - at no cost!

We are happy to provide you with a free trial license for your desired solution. You can test your network requirements and determine the suitability of our products. If you decide to go ahead, you'll benefit from the many years of expertise of our sales partners. From product and price consulting to technical support, you can get everything from a single source.

[Get your free 30-day trial now](#)

About ESET

As a European manufacturer with more than 30 years of experience, ESET offers a broad portfolio of security solutions for any size of business. We protect all endpoints and servers across operating systems with award-winning multi-layered technology, support your data protection with multi-factor authentication and certified encryption products, and keep your network safe from zero-day threats with cloud sandboxing. Our endpoint detection and response solutions and threat intelligence services

complement our offering in terms of forensics as well as targeted protection against cybercrime and APTs. ESET doesn't rely solely on next-gen technologies, but combines insights from the cloud-based reputation database ESET LiveGrid® with machine learning and human expertise to give you the best protection.

SATISFIED CUSTOMERS



**Champion
Partner**

A strong team on the field
and digitally since 2019



Protected by ESET since 2016
More than 4,000 mailboxes



ISP Security Partner since 2008
2 million customers

PROVEN



ESET was awarded the trust seal
"IT Security made in EU"



Our solutions are certified
according to quality standards

ESET IN FIGURES

110+ million

Users
worldwide

400k+

Business
Customers

200+

Countries &
Regions

13

Research &
development
centres worldwide



**welive
security™**
BY **eset**