Digital Security
Progress. Protected.

POSITION PAPER

DIGITAL SOVEREIGNTY

is only possible with strong IT security

DIGITAL SOVEREIGNTY is only possible with strong IT security

Credits

ORIGINAL AUTHORS:

Thorsten Urbanski
Ildiko Bruhns

CONTRIBUTING EDITORS:

Márk Szabó
James Shepperd

eset® Digital Security
Progress. Protected.

eset Digital Security
Progress. Protected.

The digital autonomy of the European Union as a block is a necessity for economic, social and political self-determination. While it sounds self-evident, it is by no means simple in the present day. Above all, in the digital realm repeated failures in the area of IT security ensure that the much-invoked theme of digital sovereignty falls into question.

Ever since the conflict in Ukraine began, it became clear that Europe is in anything but good shape when it comes to digital sovereignty. The countless attacks on Ukraine's critical infrastructure, and other nation-aligned attacks on Europe's key industries and state-connected sectors have revealed enormous need for early action.

It became apparent that companies, institutions, and public authorities had grown too dependent on digital imports from non-EU countries - or countries whose aligned values are in jeopardy - instead of relying on regional expertise. The effects are noticeable: Supply bottlenecks, missing components, and both products and solutions that do not comply with European standards are among the current challenges placing companies and institutions at risk of faltering. All of this combined endangers Europe's digital sovereignty and could contribute in the long term, to its economic, social and political strengths failing by the wayside.

Among these concerns exists a lack of mature IT security capacity, concepts and technologies in many areas, as the increased and often successful attacks on public authorities, hospitals and governments have shown. It has long been clear that digital sovereignty is not feasible without strong IT security, and in today's digital construct is a key component to European sovereignty.

IT SECURITY AS A BASIC PREREQUISITE FOR ECONOMIC AND POLITICAL SELF-DETERMINATION

According to ENISA's 2024 estimates, companies invested around 9% of their IT investments into information security, representing a meager rise of 1.9% compared to the previous year. However, despite this spending, employee allocations have decreased, all the while ENISA expects a profound upswing in the number of staff needed to prepare company compliance with the NIS2 Directive, DORA and the EU's Cyber Resilience Act, among others. Yet, a large part of the impacted businesses won't be able to ask for additional budgets, especially SME's, of which 34% indicate difficulties in that regard. Meanwhile, 90% of entities expect an increase in cyberattacks in 2025. This all paints a picture of unpreparedness and a misunderstanding of the importance of resilience in the face of the evolving threat landscape.

Cybersecurity plays a crucial role for a digitally sovereign Europe. First and foremost, digital sovereignty means creating a secure data infrastructure for Europe with protected cyberspaces for citizens. This can only be achieved by following the regulations and laws in force in Europe and with participants from the regions own ranks. After all, the primary goal of digital sovereignty is to reliably prevent the destruction, manipulation, unauthorized access and forwarding of data.

Technology and software from Europe must therefore be clearly positioned along with a reliable IT security concept. This is the only way to drive competitiveness forward, especially with Industry 4.0 in mind, but also for the operation of critical infrastructure (CRITIS). The increased pressure on European autonomy as well as prevailing trends on the cyber threat landscape clearly demonstrates that there is an immediate need to catch up and take action, particularly in the area of IT security.

TIME IS OF THE ESSENCE

Cybercriminals are increasingly targeting companies, institutions and even governments. These include APT groups such as MirrorFace, MoustachedBouncer or FishMonger indiscriminately target high-value institutions, agencies or companies. Whether through espionage, supply chain or ransomware attacks, the financial and functional damage can be immense.

That's not where the story ends though. Despite the crackdown on ransomware groups such as LockBit or BlackCat, others like RansomHub or Embargo have picked up their mantle and created something much worse – affiliate networks leveraging ransomware-as-a-service (RaaS) program tools including new EDR killers, a special type of malware designed to terminate, blind, or crash the security product installed on a victim's system. This is problematic, as it can lead to an increase in successful ransomware attacks, especially if they have specific targeting in mind. This could spell particular trouble for those organizations that are either not protected appropriately, or they put preventive measures to the wayside, opting for security that doesn't correspond to their size, scope or needs.

However, it's not only APT's and cybercriminals that can cause large scale disruptions. In the second half of 2024, a faulty security update of a widely used cyber vendor from the United States caused a global Blue Screen of Death (BSOD) wave, impacting major organizations and institutions employing the security solution of this vendor. Impacts to Europe? Major airports in Czechia, Hungary, Slovakia, the Netherlands, Spain and Germany had their operations affected. Financial institutions such as banks, or state services were also impacted, including critical sectors such as transportation and shipping, healthcare services, retail and more all having halted some or all their operations. This unprecedented disruption showcased how all it takes is a single break in a chain to wreak complete havoc.

" It is imperative that European countries develop a common ground for enhanced resilience in the face of the ever-growing specter of globally sourced cyber security attacks. Now, more than ever, cross-sectoral initiatives with the backing of security experts can show how top security doesn't mean having to go outside one's comfort zone. With respect to European regulations and needs, it is easier to establish powerful prevention than before."

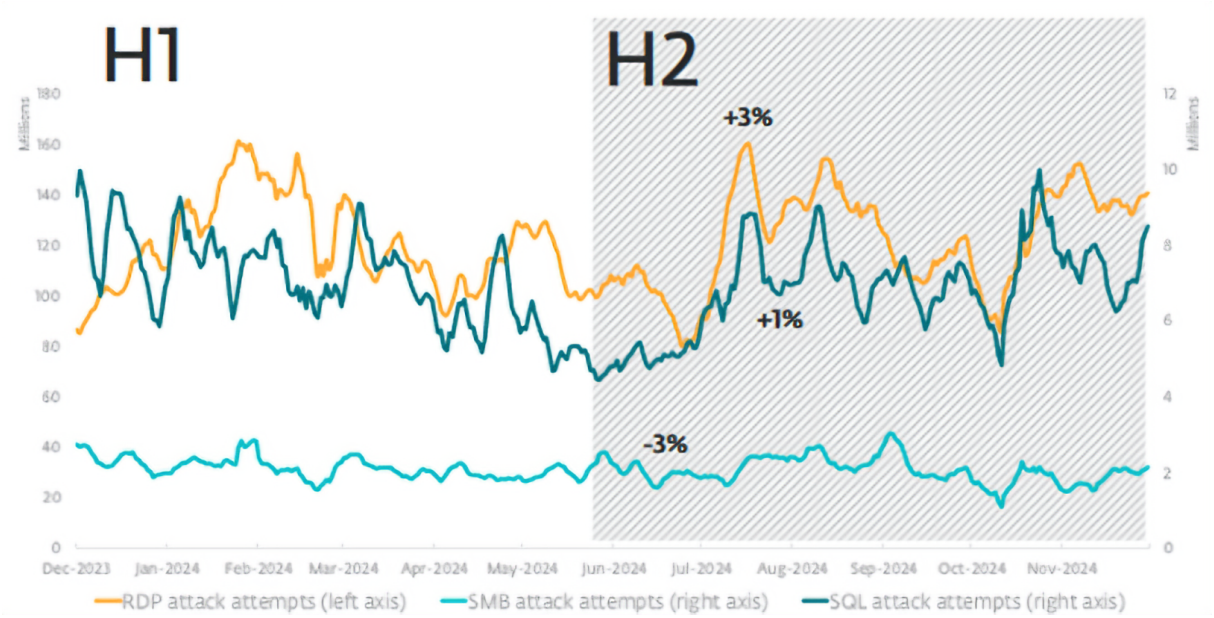
Andy Garth, ESET Government Affairs Lead

At the same time, many technologies that enable hybrid work regimes have also opened up numerous backdoors for hackers; for example, through the emote Desktop Protocol and corporate VPNs keep being abused by malicious actors.

For H2 2024, ESET registered around 160 million RDP attack attempts, a 3% increase compared to the previous semester. Likewise, there's been an increase in SQL attack attempts, which goes hand in hand with other network intrusion attacks.

As for VPNs, there's been multiple cases of major vulnerability exploitations by threat actors, with the Volt Typhoon APT group successfully breaching the Dutch Ministry of Defense in 2023.

Thus, the threat landscape is littered with landmines ready to explode in the face of company or government security, and it is essential for these entities to handle this responsibility in accordance with both EU and country specific regulations. It is also critical that these entities enact measures that decrease the amount of time it takes to detect and respond to any incident. Time is of the essence, and for Europe, it's time it took its security seriously.



H1 2024 – H2 2024: Trends of RDP, SMB and SQL attack attempts, seven-day moving average

Source: ESET Threat Report H2 2024, p. 32

IT SECURITY MADE IN EUROPE

Attacks on critical sectors by APTs or large-scale security failures are not isolated incidents. This was demonstrated, for instance, by the security vulnerability found in Citrix software that paralyzed the University Hospital in Düsseldorf in September 2020. Likewise, the many disruptive attacks on critical infrastructure in Ukraine, such as those targeting its energy sector have showcased the devastating consequences of digital attacks in the real world.

Experts assume that attacks on health, manufacturing, energy, or government, will continue, as processes become gradually more connected and digitalized. Thus, governments and public authorities must ensure that they become more independent in the area of information security, so that they will not be defenseless against such threats in the future.

For this reason, the European Cyber Security Organization (ECSO) launched their "Cybersecurity Made in Europe" label, highlighting the quality and values of European security vendors that meet the criteria.

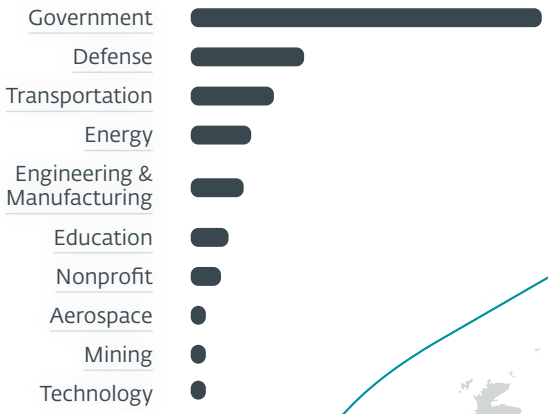
To be awarded this badge, companies must demonstrate that:

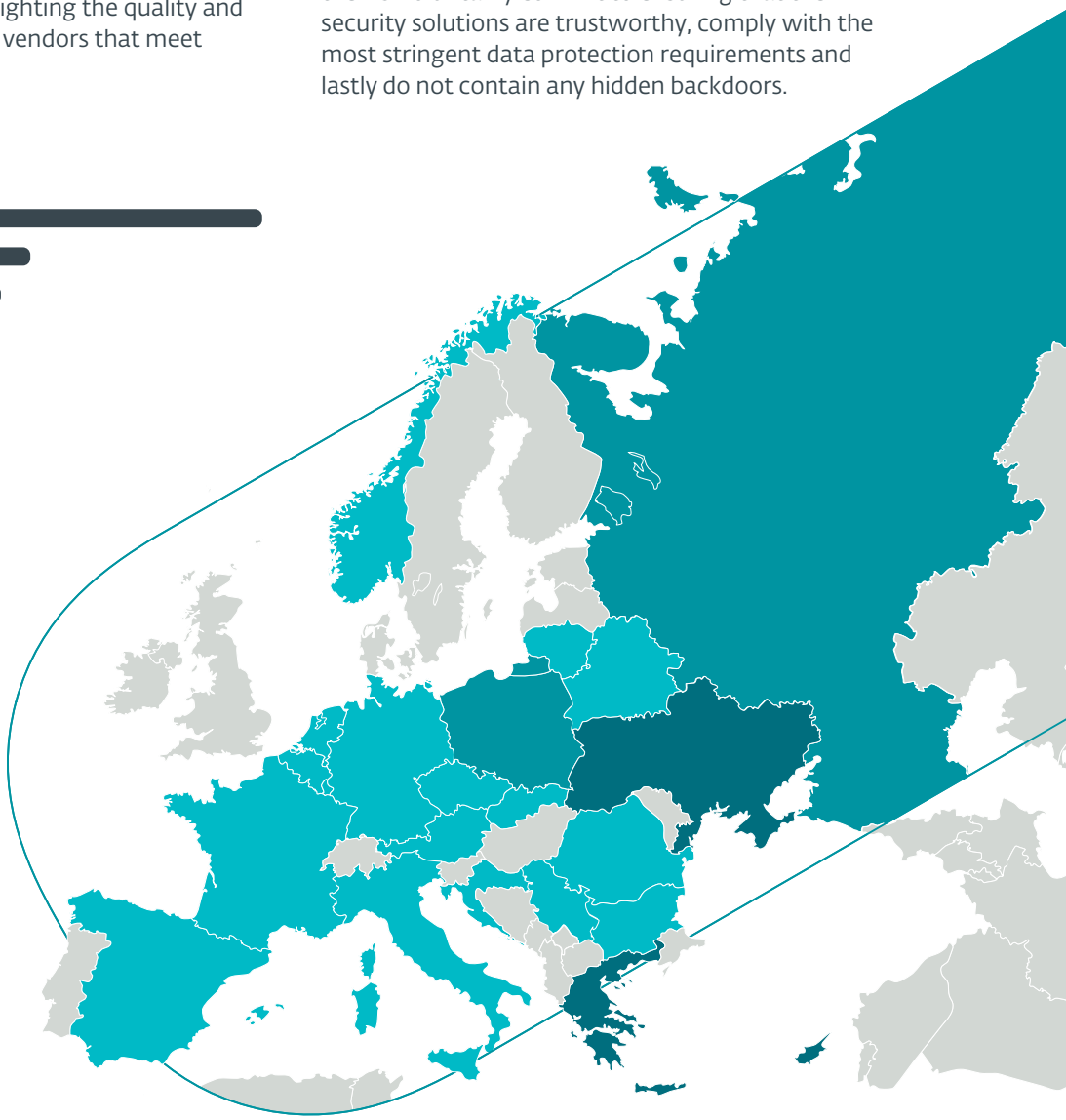
1. The head office of the company is located in Europe.
2. The majority of the employees are employed in Europe.
3. The core market is Europe.
4. Respect the 10 baseline security requirements specified by ENISA.

The latter baseline requirements are essential for products and services in information and communication technology, as to comply implies strong security.

Organizations and users thus ensure that they are able to trust the performance and reliability of the technologies and solutions so labeled, as well as their unconditional compliance with the law.

With this label, creators with their headquarters in the EU voluntarily commit to ensuring that their security solutions are trustworthy, comply with the most stringent data protection requirements and lastly do not contain any hidden backdoors.





ESET telemetry shows that in Europe, the most targeted sector is government, closely followed by defense and transportation.

ESET: THE EUROPEAN RESPONSE TO CYBERCRIME

ESET was one of the first companies to be awarded this label. By signing the voluntary declaration of conformity, ESET has confirmed its commitment to EU data protection and trusted IT protection solutions. In addition, in is role as specialized security entity, ESET launched several research collaborations in 2020 and 2021, including with the European Organization for Nuclear Research (CERN), Europol and the French National Agency for the Security of Information Systems (ANSSI). Continued exchange with transnational cybersecurity organizations are forthcoming.

Thinking and acting with foresight is also exactly what organizations desperately need in the fight against cybercriminals. In cases demonstrating the most sophisticated types of attack, many public authorities and companies would have been spared had they been using endpoint detection and response solutions. This technology continuously searches within a system for security vulnerabilities, suspicious behavior and unusual events. However, forming a proper defense with just endpoint security is no longer enough to ward off the most insidious types of malware, or targeted attacks.

Organizations are increasingly being targeted by criminals for:

- Technical inadequacy due to the quick switch to hybrid work regimes., increasing the attack surface without corresponding security measures, budgets or staff capacity.
- Untrained employees unintentionally become security vulnerabilities.
- The rise of cybercriminals as professional hacker groups, including motivated nation-aligned attacks
- Increased use of sophisticated malware like EDR killers

In order for these organizations to identify the majority of external attacks, employee misconduct and unwanted applications must be addressed as quickly as possible, and need to be fully informed about what is happening on their networks, building resilience with prevention in mind.

ASPECTS THAT BUILD TRUST

- Company headquarters must be in the EU.
- The company must offer trustworthy IT security solutions.
- The products on offer must not contain any hidden access (no backdoors).
- The company's IT security research and development must take place in the European Union.
- The company must undertake to comply with the requirements of the EU's General Data Protection Regulation, and NIS2 for those in a critical sector.

STAYING AHEAD OF THREATS: PREVENTION FIRST AS A STRATEGY

To bring about digital sovereignty there is no doubt that public authorities and companies must rise to the challenge of digitalization. If IT managers want to be proactive, they should adopt a consistent prevention-first approach within their organization because conventional protection solutions, consisting of malware and spam filters as well as firewalls, are no longer sufficient to prevent cyberattacks. Professional APT attacks are increasingly circumventing these mechanisms by infiltrating systems stealthily, unnoticed and in multiple stages.

For this reason, ESET has adapted its solutions to the requirements of different organization sizes. The idea is to achieve a security posture that handles threats before they create incidents, stopping them before they could even touch an endpoint, minimizing the time security teams have to invest on incident response and remediation.

ESET's "Prevention-first approach" consists of four pillars, each tackling a different aspect of preventive cybersecurity. These pillars are:

- Minimize the attack surface
- Reduce complexity
- Boost your cyber hygiene
- Stay ahead of compliance

Let's discuss in detail what each pillar represents.

MINIMIZE THE ATTACK SURFACE

First and foremost, to prevent easy access to company networks, they should actively look for ways to shrink their attack surface. As the age of digitalization marches on, an increasing number of resources will be placed on connected services such as the cloud, as well as across multiple endpoint devices like computers, phones, tablets, or IoTs. This requires robust protection, stacking up multiple layers of proactive protection capable of resisting attacks at the size and scale warranted by an organization's environment.

Approaches like Zero-Trust link to prevention here, restricting unauthorized access by demanding constant and extensive verification any time data access is requested.

ESET answers these needs with its robust ESET PROTECT Platform, which thanks to its numerous modules and functionalities effectively protects against software vulnerabilities, sophisticated attacks such as fileless malware or ransomware, network intrusion, and phishing.

REDUCE COMPLEXITY

As the fight against sophisticated threats requires multiple stacks of security solutions working in tandem, some organizations might find themselves overwhelmed by the number of tasks stemming from this area. Managing multiple solutions requiring separate sign-ins or operating in swivel chair environments hopping from one screen to another constantly can result in visibility gaps, alert fatigue, and ultimately a complete loss of control.

At ESET, we design our solutions with simplicity in mind, delivering comprehensive capabilities unified into a single pane of glass. In addition, we integrate with multiple other solutions such as Microsoft Sentinel, IBM QRadar, Stellar Cyber, Elastic or Mindflow, helping security operations consolidate their cyber defense in a cost-efficient way.

Alternatively, we can free up an organization's IT teams through our ESET MDR services, enabling enterprise-grade security for all, effectively leveling the playing field for all organizations looking to make a headway in their security efforts.

BOOST YOUR CYBER HYGIENE

Keeping up with all things security, such as regular security updates, patch management, applying novel security policies and incident response playbooks can be difficult. What's more, as one of the chief culprits behind many incidents is human error, it is critical that security is understood as a baseline daily operational requirement.

As security is essential, ESET continuously tries to disseminate security awareness content, including its awarded content by ESET Research, to help improve one's chances against the onslaught of malicious behavior. This is also strengthened by the commitment to paid and free training services such as the ESET Cyber Security Awareness Training, which enables a gamified way to learn security terminology and best practices.

Likewise, ESET's solutions such as its ESET PROTECT dashboard centralizes and automates multiple IT management tasks, including vulnerability and patch management, providing full visibility into all endpoints. What's more, thanks to ESET Secure Authentication and ESET Full Disk Encryption, businesses can remain secure that their sensitive data and access to it won't get compromised, respecting regulations such as the GDPR or NIS2.

STAY AHEAD OF COMPLIANCE

With a correctly implemented prevention-first approach, organizations can get ahead of compliance and cyber insurance requirements,

Modern requirements typically ask for state-of-the-art security, which in Europe often means a requirement to protect sensitive information such as personal data or financial details to the maximum degree. As soon as an adversary gains access to these, an organization becomes liable to face legal repercussions.

Thus, products like ESET Inspect, the XDR-enabling solution of the ESET PROTECT Platform offer key capabilities that are proven to neutralize ransomware and zero-day threats utilizing AI for better detection. Moreover, in concert with other modules such as our authentication solution, encryption, and vulnerability and patch management, customers can keep compliant with industry regulations, and effectively lower their cyber insurance premiums.

PROUDLY EUROPEAN

As ESET solutions come from the heart of Europe, the necessary legal requirements are always kept front and center in research and development, keeping a secure-by-design approach, which we can then effectively share with our clients. This is a win-win situation, as the more secure and compliant our product is, the better for its end-users.

ESET develops all its technology in-house and in its own research labs. This also includes multi-factor authentication and data encryption – across all popular operating systems, whether cloud-based or on-premises. As a result, ESET security solutions are uniform and based upon a commitment to prevention. This is a great example of what future-proof IT security solutions must look like if they are to become a reliable anchor for companies, institutions and public authorities in their capacities ensuring digital sovereignty, and thus represent the needed investment in Europe's future.

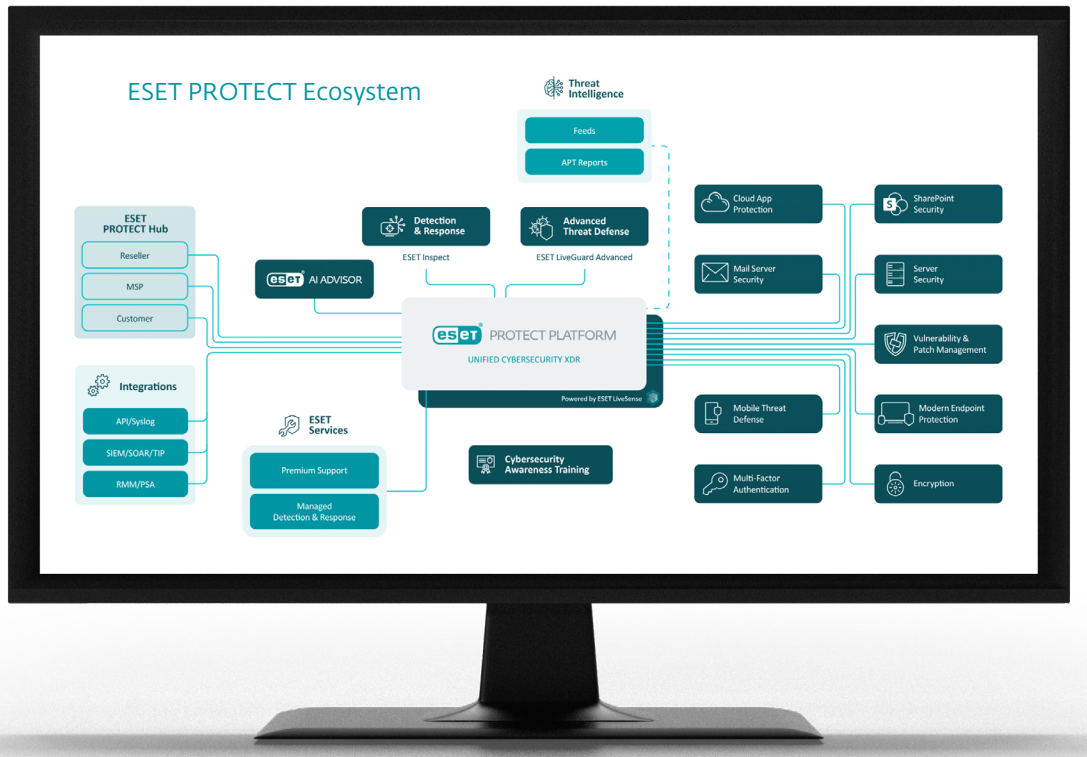
Prevention-first approach

Minimize the attack surface

The best strategy for countering the ever-evolving attacks starts with shrinking the attack surface. It requires robust protection across email, endpoints, cloud applications, mobile devices and entire networks.

ESET PROTECT Platform:

- **Stacks up multiple layers** of proactive protection, so that IT teams can mitigate the risks, and resist the attacks.
- Effectively protects **against phishing, insider threats, malware**, compromised credentials and vulnerabilities.
- Delivers **powerful AI-native prevention**, detection and response, enriched with world-class threat intelligence.



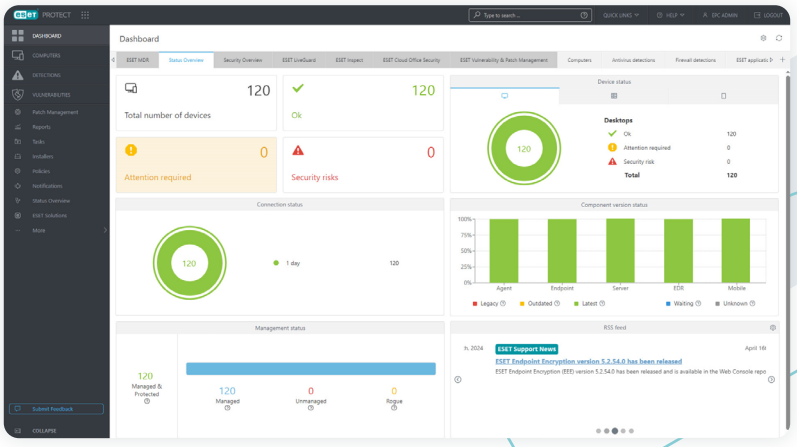
Digital Security
Progress. Protected.

Reduce complexity

Managing multiple solutions requiring separate sign-ins, especially as the threat landscape constantly evolves, becomes more complex. This can lead to gaps in visibility and alert fatigue, resulting in loss of control.

ESET PROTECT Platform:

- Delivers comprehensive range of capabilities unified into a **single pane of glass**.
- Consolidates your cyber defense **in a cost-efficient way**.
- **Frees up your in-house IT teams** when combined with ESET Managed Detection and Response Services (MDR).

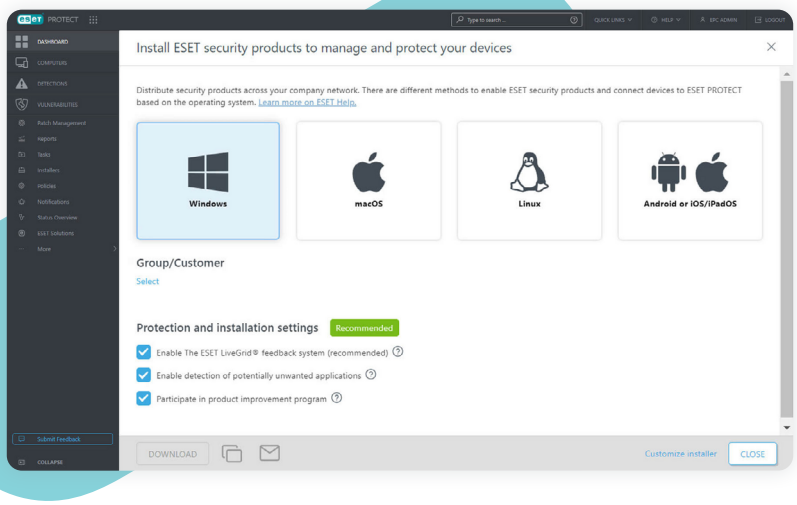


Boost your cyber hygiene

Keeping up with all the best practices, such as regular updates, patch management, encryption and applying security policies can be overwhelming. IT professionals should rely on automated solutions that simplify the routines for them.

ESET PROTECT Platform:

- **Centralizes and automates** multiple IT security and management tasks, including vulnerability and patch management.
- Provides **full visibility** of all endpoints, subscriptions, and vulnerability & patching statuses across your asset inventory; **always up to date**.
- Solves poor password hygiene and **prevents unauthorized access** with easy-to-use multi-factor authentication (MFA).
- Increases your organization's **data security** with a powerful full-disk encryption.

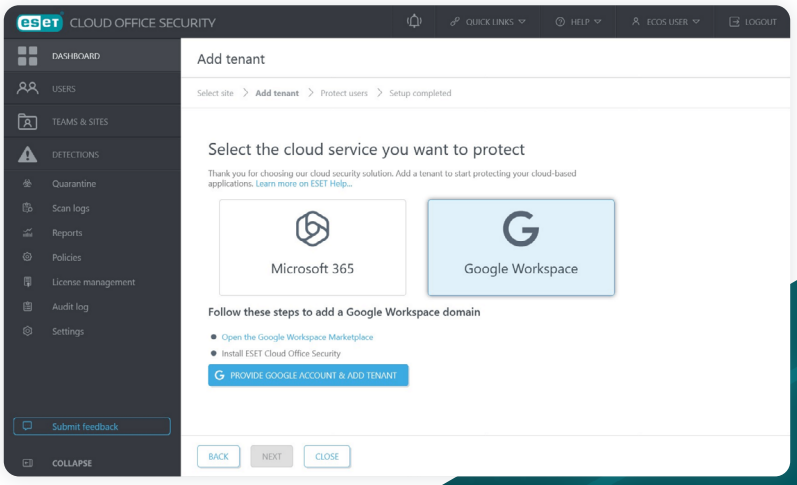


Stay ahead of compliance

With the right, prevention-first approach, you get ahead of the requirements as they are typically built on the latest trends and proven proactive measures.

ESET PROTECT Platform:

- Identifies and **neutralizes ransomware and zero-day threats** utilizing AI and cloud sandbox analysis.
- **Protects your whole business environment**, including advanced protection for Microsoft and Google Workspace apps
- ESET XDR and MDR solutions plus key capabilities, such as MFA, encryption **keep you compliant** with industry regulations, and effectively lower cyber insurance premium.
- ESET Cybersecurity Awareness Training **secures the required education** for your entire workforce.



Digital Security
Progress. Protected.

This is ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats with our AI-Native, prevention-first approach. We combine the power of AI and human expertise to make protection easy and effective.

Experience best-in-class protection thanks to our in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers.

ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat-hunting capabilities with a broad variety of security services, including managed detection and response.

Our highly customizable solutions include local support and have minimal impact on performance, identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

ESET protects your business so you can unlock the full potential of technology.

ESET IN NUMBERS

1bn+
protected internet users

500k+
business customers

178
countries and territories

11
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017
more than 9,000 endpoints

Allianz Suisse

protected by ESET since 2016
more than 4,000 mailboxes

Canon
Canon Marketing Japan Group

protected by ESET since 2016
more than 32,000 endpoints

ISP security partner since 2008
2 million customer base

RECOGNITION

AV comparatives
APPROVED
Business Security
DEC 2024

ESET is a consistent **top-performer in independent tests** by AV-Comparatives and achieves best detection rates with no or minimal false positives.

SPRING 2025
Grid Leader

ESET consistently achieves top rankings on the global G2 user review platform and its solutions are **appreciated by customers worldwide**.

IDC ANALYZE THE FUTURE

ESET has been recognized as a Leader in endpoint security in the IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024 Vendor Assessment.