ESET Consumer Security for Windows Product Bulletin

FOR RESELLERS

Document Version 1.0
June, 2023
Author: Matej Kristofik

FOR RESELLERS

Content

Disclaimers

- Dates are subject to change. Final dates will be confirmed.
- Screenshots may not reflect the state of the final version.

FOR RESELLERS

Product changelog

BUILD V16.1

- Installer: Dropped support for Windows 8.1, Windows 8, Windows 7, WHS 2011
- GUI: Added Live Tiles on Overview page
    - Features state indicated inside of tiles on Overview page
    - Added progress animation inside of tiles
- GUI: Added new Light / Dark mode switch to GUI
- GUI: More tools submenu merged with Tools
    - Network Inspector remains placed on Tools page
- GUI: SysRescue removed from GUI
- Banking & Payment Protection: Green frame changes (already released by module)
    - Advanced setup setting hides badge and green frame completely
    - Closing of badge by "X" leads to closing of frame as well
- Banking & Payment Protection - Isolated browser
    - Browser started from desktop icon or product will run in isolated mode - unified behavior between redirection and SAB (module release)
- Removed Anti-Stealth setting from advanced setup (redundant setting)
- Updater: Updater message dialog replaced with alert window
- Bug-fixing, improvements
    - Fixed customization logo incorrectly displayed in GUI
    - Fixed incorrectly displayed Machine Learning advanced setup settings incorrectly displayed
    - Additional network details displayed under Network adapters in GUI

BUILD V16.2

- New onboarding wizard replaces post installation wizard
- Advanced setup: New Protections section in advanced setup
- Protections moved under this new section
- Network traffic scanner (former protocol filtering) moved under detection engine
- Web and email section split into more logical part
- Wording changes and improvements, …
- Firewall: Redesigned and reworked firewall in GUI and advanced settup

- Completely redesigned rule editor
- New layout of firewall settings in advanced setup (new rule editor,
- New layout of Setup page network section
- Redesigned network troubleshooting wizard
- Running processes new sidebar introduced
- Other changes e.g. known network changed to network profiles with activators, …
- Advanced setup: New connectivity section includes proxy settings
- GUI: unified colors communication for pausing, disabling of core and regular features
- Core features: Real-time file system protection, Web access protection, Anti-Phishing protection, Firewall, IDS, Botnet
- New uninstall survey opens during uninstallation
- Other small improvements
    - Updated tooltips
    - Added info about user who started scan
    - By whom was the scan interrupted (user / system)
    - Accessibility: fixed bugs: reading out elements in notifications like paths, headers, links, …
    - Added option to hide unprotected Wi-Fi notification
    - Reworded license statuses in product
- Bug-fixing

BUILD V17.0

- NEW : Identity Protection
- NEW : VPN
- NEW : Browser Privacy & Security

FOR RESELLERS

About Consumer security for Windows

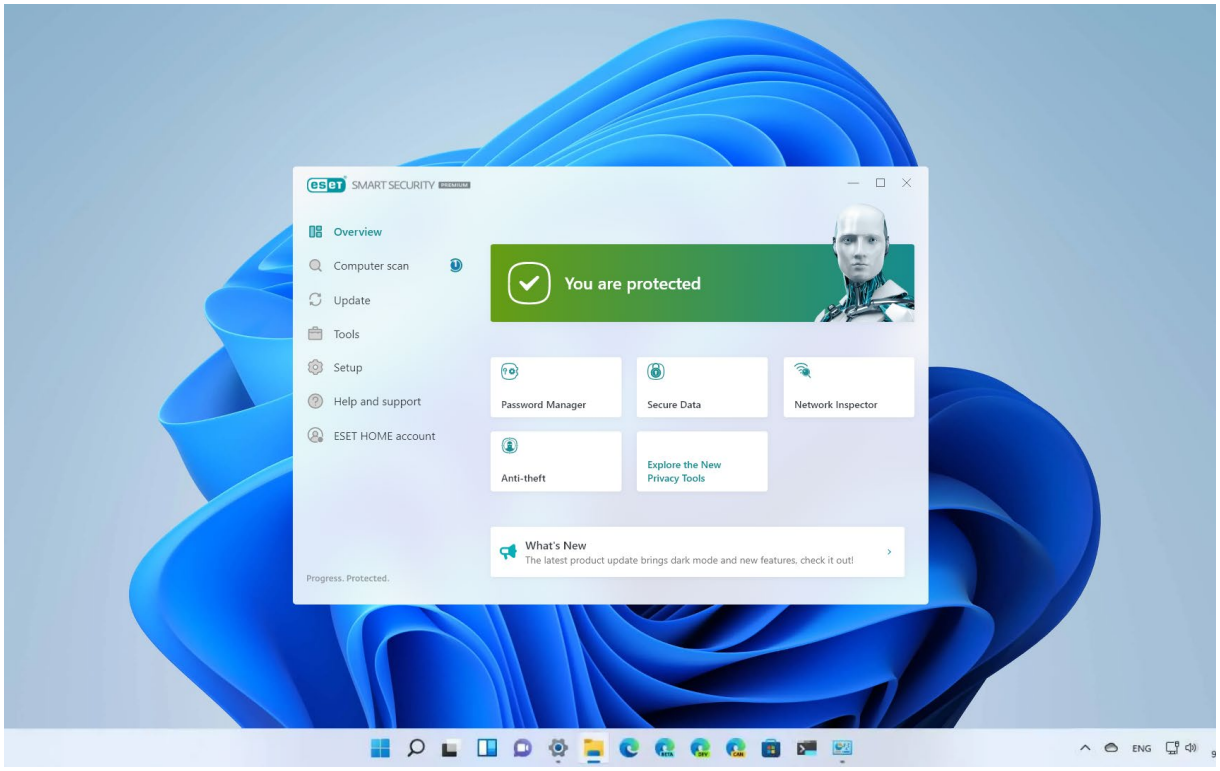
Consumer security for Windows consists of 4 products – **ESET NOD32 Antivirus**, **ESET Internet Security, ESET Smart Security Premium** and **ESET Security Ultimate** each providing a specific level of protection and focused on specific users. All consumer security products are available as the modules within the subscription tiers (ESET HOME Security Essential, ESET HOME Security Premium and ESET HOME Security Ultimate) of the Gemini offering while ESET NOD32 Antivirus is also available as the standalone device protection.

GEMINI OFFERING/ACTIVATION MATRIX

All-in-One Protection/Subsciption tiers	**Included products in Subscription tiers**
ESET HOME Security Essential	**ESET Internet Security, ESET NOD32 Antivirus**, ESET Cyber Security, ESET Mobile Security, ESET Parental Control, ESET Smart TV Security
ESET HOME Security Premium	**ESET Smart Security Premium, ESET Internet Security, ESET NOD32 Antivirus**, ESET Cyber Security, ESET Mobile Security, ESET Parental Control, ESET Smart TV Security, **ESET Password Manager**
ESET HOME Security Ultimate	**ESET Security Ultimate, ESET Smart Security Premium, ESET Internet Security**, **ESET NOD32 Antivirus**, ESET Cyber Security, ESET Mobile Security, ESET Parental Control, ESET Smart TV Security, **ESET Password Manager, VPN, Identity Protection**

Device protection (standalone)
ESET NOD32 Antivirus, ESET Mobile Security, ESET Parental Control, ESET Smart TV Security

Each consumer security product for Windows includes multiple layers of real-time protection as well as additional tools/features that further enhance user's ability to protect against various threat vectors e.g. Network Inspector focuses on router and connected devices security while Safe Banking & Browsing provides process protection for users browser. All products aim to maximize protection on device level. For reactive users – it aims to provide "peace of mind" and ensure theirs're protected 24/7 while enabling pro-active users to customize protection into reasonable granularity.



Story

The history began with NOD32 product. The acronym NOD stands for Nemocnica na Okraji Disku ("Hospital at the end of the disk"), a pun related to the Czechoslovak medical drama series Nemocnice na kraji města (Hospital at the End of the City). The first version of NOD32 - called NOD-ICE - was a DOS-based program. It was created in 1987 by Miroslav Trnka and Peter Paško at the time when computer viruses started to become increasingly prevalent on PCs running DOS. Due to the limitations of the OS (lack of multitasking among others) it didn't feature any on-demand/on-access protection nor most of the other features of the current versions. Besides the virus scanning and cleaning functionality it only featured heuristic analysis. With the increasing popularity of the Windows environment, advent of 32-bit CPUs, a shift in the PC market and increasing popularity of the Internet came the need for a completely different antivirus approach as well. Thus the original program was re-written and christened "NOD32" to emphasize both the radical shift from the previous version and its Win32 system compatibility.

Later, ESET Smart Security was introduced adding Firewall and Anti-theft as main differentiator features compared to NOD32 Antivirus. Offering further evolved and new tiers were introduced in 2015 with ESET Internet Security replacing Smart Security and ESET Smart Security Premium to act as premium proposition for users who want it all.

Today, we provide almost complete set of protection not only for Windows OS but also for Android, Apple macOS and iOS connected by ESET HOME platform ecosystem.

ESET's consumer portfolio has evolved to include a brand-unified global offering, thus entering the Consumer Digital Life Protection industry category. ESET aims to position itself as a **Digital Life Protection vendor** in the B2C segment and is introducing two new market categories: **All-in-one protection** and **Device protection**. This decision was made based on various analyses of the market, industry trends and competition.

This new generation of our B2C offering centers the customer, solving their daily digital security challenges and protecting their progress.

There are three main pillars where ESET stands firm and deeply rooted: **security, smart home protection,** and **privacy and identity protection**. These pillars are supported through **ESET HOME—a complete security management platform**—and are enabled via ESET's unique approach to technology: **multilayered security technology, live Cloud protection, Artificial Intelligence,** and **human expertise**. Finally, they are represented via award-winning, easy-to-use solutions with minimal impact on device resources, and enriched by quality of service, local support and social responsibility.

The introduction of a new innovative and simplified consumer offering in October 2023 brings new subscription tiers—ESET HOME Security Essential, ESET HOME Security Premium and ESET HOME Security Ultimate. Enhanced security for our customers' digital life goes hand in hand with new technological functionalities including VPN, Identity Protection, Browser Privacy & Security extension and other improvements in the background of the service.

Our internal analytics and research show that most users are passive when it comes to interaction with our products. They trust our products will provide ultimate protection for their device(s). At the same time, they want to have enough control to do certain tasks pro-actively or set it. Therefore, our ambition is to provide products our users can rely on – with minimal interaction needed to set the product and have it running and protecting. On top, to provide meaningful options and functionality where pro-active users can control and customize it to meet their basic needs.

FOR RESELLERS

Consumer security products for Windows within the New Consumer Offering

Digital Security
Progress. Protected.

Key benefits

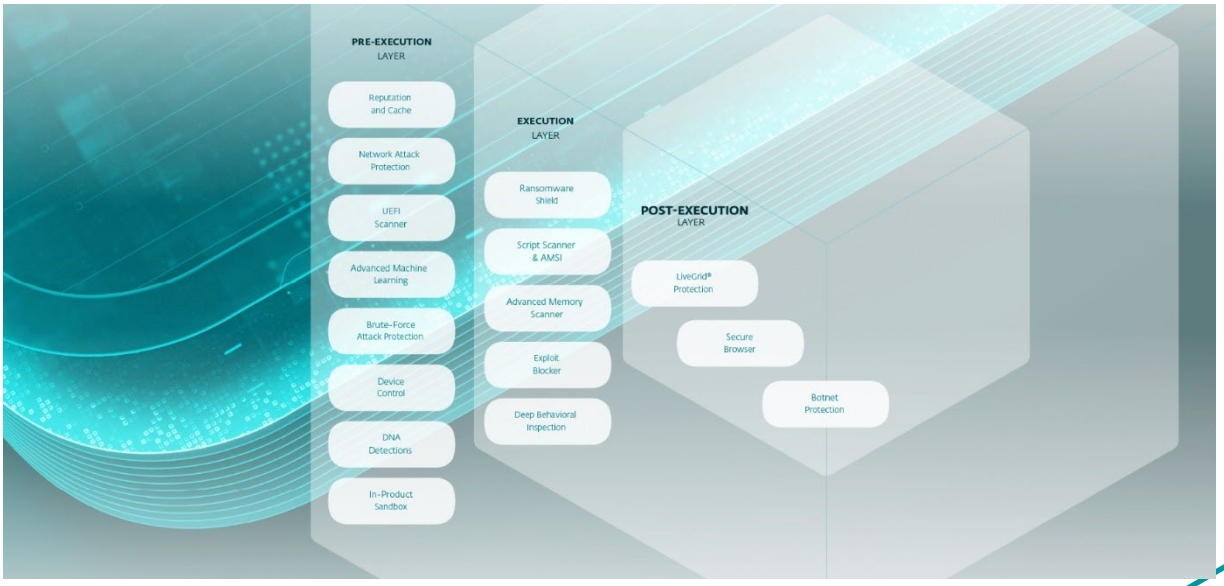
In this chapter we describe key benefits the features and other aspects of ESET consumer security for Windows bring for our customers.

High-performance and low system impact

Products always aim to mix best performance and lowest OS and device load confirmed by independent lab tests. This is achieved by employing optimized techniques to fight new types of threats emerging on the internet

Technologically advanced product

ESET uses multi-layered technologies that go far beyond the capabilities of basic antivirus.



FOR RESELLERS

Technical requirements and compatibility

Product	Compatible operating systems, browsers, and product versions	Other requirements
ESET NOD32 Antivirus **ESET Internet Security** **ESET Smart Security Premium** **ESET Security Ultimate**	• Microsoft Windows 11, 10 with latest updates installed	Internet connection is required to activate or upgrade the product
ESET NOD32 Antivirus ARM **ESET Internet Security ARM** **ESET Smart Security Premium ARM**	• Microsoft Windows 11, 10 on ARM	Device must run ARM compatible chipset such as Qualcomm or Microsoft Internet connection is required to activate or upgrade the product
ESET Password Manager – part of ESET Smart Security Premium	• Android 5.0 or newer • iOS 11 or later	
Safe Banking & Browsing – part of ESET Internet Security and ESET Smart Security Premium	• All browsers except Safari	
VPN	See VPN bulletin	Available for ESET HOME Security Ultimate only
Identity Protection	See Identity Protection bulletin	Available for ESET HOME Security Ultimate only
Browser Privacy & Security (browser extension)	See Key Features section	Feature set differs depending on Offering activated

FOR RESELLERS

Localizations

Documentation – User Guide, Quick Start Guide, Application help, Knowledge base, Product pages.
Languages – Arabic, Bulgarian, Chinese Simplified, Chinese Traditional, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French Canadian, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese Brazilian, Romanian, Russian, Serbian Latin, Slovak, Slovenian, Spanish, Spanish Latin America, Swedish, Thai, Turkish, Ukrainian, Vietnamese, Indonesian

* **ESET Secure Data** will not support right-to-left languages

ESET Consumer security for Windows

It consists of 4 separate Windows OS apps. In this chapter we look into the specifics of each of these apps.

Distribution

Applications are available via ESET global website, ESET HOME, Microsoft Windows app store or via 3rd party web-locations or physical media.

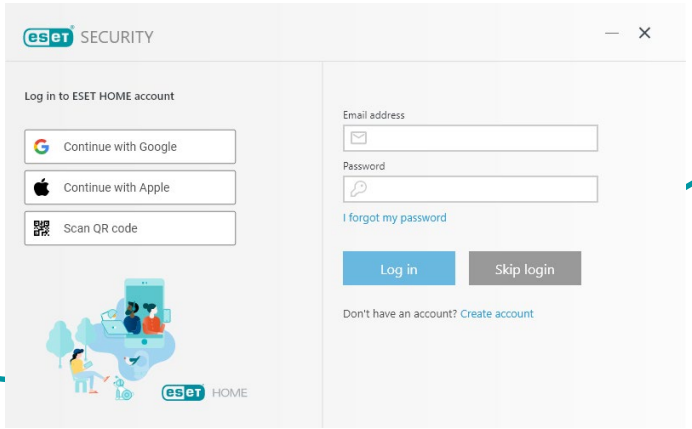
Installation and onboarding

You can always refer to the online help for your respective product current screens and flow.

Primary flow via ESET HOME:

To create this ecosystem we needed to add an optional login/connect feature into our products as that is how users' devices are added to their ESET HOME accounts. A device connected to a ESET HOME account sends updates about its security status and other information to ESET HOME when they happen. Users get the biggest benefit when they connect all their protected devices as they will have an easy access to all security information in one place. They will also be notified about changes in their security anywhere they are thanks to the mobile app. More information about device overview and notifications is in the chapters Devices and Notifications.

Previously, users of Windows consumer products needed ESET HOME account only to turn on Anti-Theft. We needed to change this as now this connection is not limited to Anti-Theft but it applies to the whole product and its features. Now, users of ESET NOD32, ESET Internet Security and ESET Smart Security Premium can optionally connect their devices to ESET HOME from the product's home screen. Login is also offered at the beginning of the installation process in Live Installer but users can skip this step. Those who don't have a ESET HOME account can create one at home.eset.com. The account does not need to have a verified email address (via verification link sent in an email) to finish the installation or connection/login process. Login is still required when trying to turn on Anti-Theft. If user decides to use Change license feature (to use a different license for product activation) and the device is connected to their ESET HOME they will be able to simply choose one of their licenses available in their account.



Installation and product onboarding consists of 1 main steps (bellow).

1. **Product consents** – user is asked to provide consent for EULA, ESET LiveGrid® feedback system, Potentially unwanted applications, Customer Experience Improvement Program

- Activation is automatic as installer already includes all license information provided by ESET HOME

Note: Installation requires Admin privileges and Windows OS will show the Windows “UAC dialog” before installation start. User must allow it to start.

Secondary flow via direct download

Installation and product onboarding consists of 2 main steps (bellow). Installation requires Admin privileges and Windows OS will show the Windows “UAC dialog” before installation start. User must allow it to start.

1. **Product consents** – user is asked to provide consent for EULA, ESET LiveGrid® feedback system, Potentially unwanted applications, Customer Experience Improvement Program

2. **Activation** options – TRIAL license, Use a purchased license key, Use ESET HOME account (separate step as well as activation option depending on specific user-flow) , Purchase license

Other installation flows & options

- **Silent installation** – installation can be completely silent if admin provides parameters via CMD line. List of Endpoint parameters can be found here

- **Custom installation** – we offer a possibility to customize installer and add various parameters to the installer itself such as country / deal / partner ID / custom log or splash screen. Such installer needs to be created via ESET Back-office or via Dexter directly.

- **BETA** – for access to Beta program, request your access from peter.randziak@eset.com

FOR RESELLERS

Features availability comparison

Feature	ESET **NOD32 Antivirus**	ESET **Internet Security**	ESET **Smart Security Premium**	ESET **Security Ultimate**
Antivirus	•	•	•	•
Antispyware	•	•	•	•
Anti-Phishing	•	•	•	•
Exploit Blocker	•	•	•	•
Ransomware Shield	•	•	•	•
Script-Based Attacks Protection	•	•	•	•
Host-based Intrusion Prevention System (HIPS)	•	•	•	•
UEFI Scanner	•	•	•	•
Advanced Machine Learning	•	•	•	•
Intel Threat Defense Technology	•	•	•	•
Firewall IMPROVED		•	•	•
Brute Force Attack Protection		•	•	•
Antispam		•	•	•
Network Attack Protection		•	•	•
Botnet Protection		•	•	•
Safe Banking & Browsing		•	•	•

FOR RESELLERS

Feature	ESET **NOD32 Antivirus**	ESET **Internet Security**	ESET **Smart Security Premium**	ESET **Security Ultimate**
Browser Privacy & Security NEW		•	•	•
Webcam Protection		•	•	•
Network Inspector		•	•	•
Anti-Theft		•	•	•
Password Manager IMPROVED			•	•
Secure Data			•	•
LiveGuard			•	•
VPN NEW				•
*Identity Protection NEW				•

NOTE: Exploit Blocker, HIPS Behavior Detection, Advanced Machine Learning, Secure Data and Banking & Payment protection is not available for ARM products

***Identity Protection scope differs based on country. See Identity Protection bulletin for more details**

FOR RESELLERS

Key Technologies

ESET LiveGrid

ESET LiveGrid® (built on the ESET ThreatSense.Net advanced early warning system) utilizes data that ESET users have submitted worldwide and sends it to the ESET Research Lab. By providing suspicious samples and metadata from the wild, ESET LiveGrid® enables us to react immediately to the needs of our customers and keep ESET responsive to the latest threats.

ESET malware researchers use the information to build an accurate snapshot of the nature and scope of global threats, which helps us focus on the right targets. ESET LiveGrid® data plays an important role in setting priorities in our automated processing.

Additionally, it implements a reputation system that helps to improve the overall efficiency of our anti-malware solutions. A user can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid®. When an executable file or archive is being inspected on a user's system, its hashtag is first compared against a database of white- and blacklisted items. If it is found on the whitelist, the inspected file is considered clean and flagged to be excluded from future scans. If it is on the blacklist, appropriate actions are taken based on the nature of the threat. If no match is found, the file is scanned thoroughly. Based on the results of this scan, files are categorized as threats or non-threats. This approach has a significant positive impact on scanning performance. This reputation system enables effective detection of malware samples even before their signatures are delivered to the user's computer via an updated virus database (which happens several times a day).

In addition to the ESET LiveGrid® reputation system, ESET LiveGrid® feedback system collects information about your computer related to newly detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer's operating system.

Host-based Intrusion Prevention System (HIPS)

It protects users system from malware and unwanted activity attempting to negatively affect computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys. HIPS is separate from Real-time file system protection and is not a firewall; it only monitors processes running within the operating system.

ESET LiveGuard

Cloud-based sandbox for ESET Smart Security Premium, developed to detect new, never-before-seen types of threats. It utilizes different machine learning models once a file is submitted. After this process, the sample is run through a full sandbox which simulates user behavior to trick evasive techniques.

It handles a wide range of file types, including documents, scripts, installers and executable files. Suspicious file are run in a safe, sandboxed environment within the ESET HQ Cloud combining:

- Static analysis of code
- Deep inspection of the sample
- Machine learning
- In-memory analysis
- AI for behavior-based detection

Advanced Machine Learning

What was the main driver behind developing Advanced ML?

We have started to develop the ESET Advanced Machine Learning engine as yet another cutting-edge protective layer focused on ESET's endpoint products. This is in addition to our cloud-focused machine learning effort that already provides protection for our end-users.

What are the main benefits and expectations from this technology?

Advanced Machine Learning's main goal was to improve our detection capabilities, making our detection engine more efficient in everyday detection as well as in cases of never-seen-before or zero-day cyberthreats. More information and research use cases about Advanced Machine Learning can be found here and here.

How does it compare with the competition?

The main advantage of ESET's Advanced Machine Learning is its high detection rate with balanced FP rate based on multiple approaches, namely static and dynamic analysis as well as sandboxing of a suspicious sample. This allows the engine to properly extract features of the sample and correctly classify it as clean, malicious or potentially unwanted. Another distinctive advantage of ESET's Advanced Machine Learning is its resilience against adversarial attacks, as it utilizes a wide variety of machine learning algorithms, including decision trees, LSTM and deep learning.

UEFI Scanner

The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. For a basic user, it represents a type of a device firmware that replaces a computer's BIOS in "modern" devices. Compared to BIOS, it's more generic and can be found on systems which are not in the 'IBM PC compatible' class. Like BIOS, it runs during device start-up (when the device is restarted or turned-on).

The very advanced capabilities that make UEFI such an attractive platform also open a way to new vulnerabilities that didn't exist in the age of the more rigid BIOS. For example, the ability to run custom executable modules makes it possible to create malware that would be launched by UEFI before any anti-malware solution – or the OS itself – had a chance to start. The complex architecture of UEFI inevitably contains vulnerabilities, which can potentially enable cybercriminals to introduce malware that would persist on the system even after complete OS reinstallation. For example, vulnerabilities which can allow the attacker with local access to bypass firmware, write protections and re-flash the firmware.

By exploiting these vulnerabilities, the perpetrators will become able to launch both indiscriminate and targeted attacks, allowing them to:

- Intercept data input and output, safely ex-filtrate stolen data
- Create reliably hidden areas in the computer's flash memory
- Compromise electronic signatures
- Establish hidden channels of communications with remote command and control servers
- Load external OSs using UEFI's networking interfaces

Ransomware Shield

ESET Ransomware Shield is an additional layer protecting users from ransomware. This technology monitors and evaluates all executed applications based on their behavior and reputation. It is designed to detect and block processes that resemble the behavior of ransomware. The technology is activated by default. If ESET Ransomware Shield is triggered by a suspicious action, then the user will be prompted to approve or deny a blocking action. This feature is fine-tuned to offer the highest possible level of ransomware protection together with other ESET technologies including Cloud Malware Protection System, Network Attack Protection and DNA Detections.

It delivers enhanced behavior-based detection techniques to protect against malware that tries to damage devices by encrypting as many files as it can locate on local and network drives and demand ransom.

Network Attack Protection

Network Attack Protection is an extension of firewall technology and improves detection of known vulnerabilities on the network level. It constitutes another important layer of protection against spreading malware, network-conducted attacks and exploitation of vulnerabilities for which a patch has not yet been released or deployed.

Anti-phishing

The term phishing defines a criminal activity that uses social engineering (the manipulation of users to obtain confidential information). Phishing is often used to gain access to sensitive data such as bank account numbers, PIN numbers and more.

ESET Smart Security, ESET Smart Security Premium, ESET Internet Security, and ESET NOD32 Antivirus provide Anti-Phishing protection to block web pages known to distribute phishing content - Protects your privacy and assets against attempts by fake websites to acquire sensitive information such as usernames, passwords, or banking details.

Anti-Phishing protection improvements are based around protection against homoglyph attacks in which an attacker tries to fool the end-user by replacing characters in addresses with different but similar-looking characters.

Arial	http://www.google.com
Times New Roman	http://www.google.com
Georgia	http://www.google.com
Cambria	http://www.google.com
Calibri	http://www.google.com
Veranda	http://www.google.com
Lucida Consol e	ht t p: / / www. googl e. com

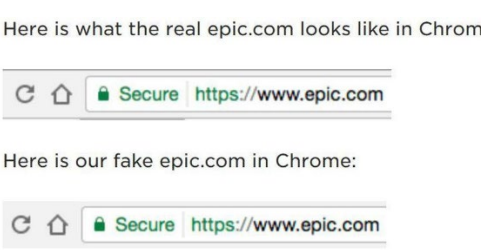


Image shows how attacker can trick users with homoglyph by replacing known site name (google) with attackers site masked. On right side, you can see result of URL link in Chrome browser.

As well as sites like banks, PayPal and Apple, we now also protect trusted media sites, to prevent fake news from gaining undeserved prominence.

WMI and System Registry Scanner

WMI is short for **Windows Management Instrumentation**. As the name implies, it is a set of tools that manage devices and applications in a Windows environment. These include (remotely) changing system settings, properties and permissions. WMI also offers many tools to gather information about a system or a network. WMI Scanner is built to detect malware that can use WMI to move laterally, harvest credentials and search for useful information within the Windows environment.

Windows System Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry.

Like so many other administrative tools and processes, the Windows registry can be used as intended, or for nefarious purposes. Since it is so ingrained into the operating system, it's a prime target for attacks and allows

them to get around standard security controls.

It can, for example, be affected by Windows malware that maintains an infection on machines and steals data without installing files. The malware resides in the computer registry only and is therefore not easy to detect. Its code reaches another machine through a malicious Microsoft Word document before creating a hidden, encoded auto-start registry key.

Exploit blocker

This is designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and MS Office components. It monitors the behavior of processes for suspicious activity that might indicate an exploit.

When Exploit Blocker identifies a suspicious process, it can stop the process immediately and record data about the threat, which is then sent to the ESET LiveGrid® cloud system. This data is processed by the ESET Research Lab and used to better protect all users from unknown threats and zero-day attacks (newly released malware for which there is no pre-configured remedy).

The technology was equipped with an additional detection method focusing on stealing system tokens, while the current version has been enhanced to cover more malicious attacks.

Intel Threat Defense Technology

New HW based security that will Boost in ransomware protection by integrating Intel's hardware-based ransomware detection technology can deliver. Tapping into telemetry at the CPU level is an effective step we can take to enable improved tracking of malicious encryption. Basically, for ESET this means exposing ransomware as it attempts to avoid detection in memory. For ESET and its customers, the value proposition of this collaboration lies in the parallel benefits of using Intel® TDT machine learning models to assist with the detection of ransomware and simultaneously off-loading these processing demands to the Intel integrated graphics controller (GPU), keeping overall system performance high.

Brute Force Attack Protection

Brute-force attack protection blocks password-guessing attacks for Remote-desktop protocol. A brute-force attack is a method of discovering a targeted password by systematically trying all combinations of letters, numbers, and symbols.

Key Features

ESET HOME

ESET HOME is the complete security management platform . Connect user's device to the ESET HOME to view and manage all his activated ESET licenses and devices. He / She can renew, upgrade, or extend owned license and view important license details. In the ESET HOME management portal or mobile app, user can edit Anti-Theft settings, add different licenses, download customized products installers to his devices, check the product security status, or share licenses through email.

Parental Control

The Parental control module allows user to configure parental control settings, which provide parents with automated tools to help protect their children and set restrictions for devices and services. The goal is to prevent children and young adults from accessing pages with inappropriate or harmful content.

Parental control lets user block webpages that may contain potentially offensive material. In addition, parents can prohibit access to more than 40 pre-defined website categories and over 140 subcategories.

Device Control

Functionality provides automatic device (CD/DVD/USB/...) control including **Web-cam protection**. This module allows user to block or adjust extended filters/permissions and define a user's ability to access and work with a given device. This may be useful if the computer administrator wants to prevent the use of devices containing unsolicited content.

Gamer Mode

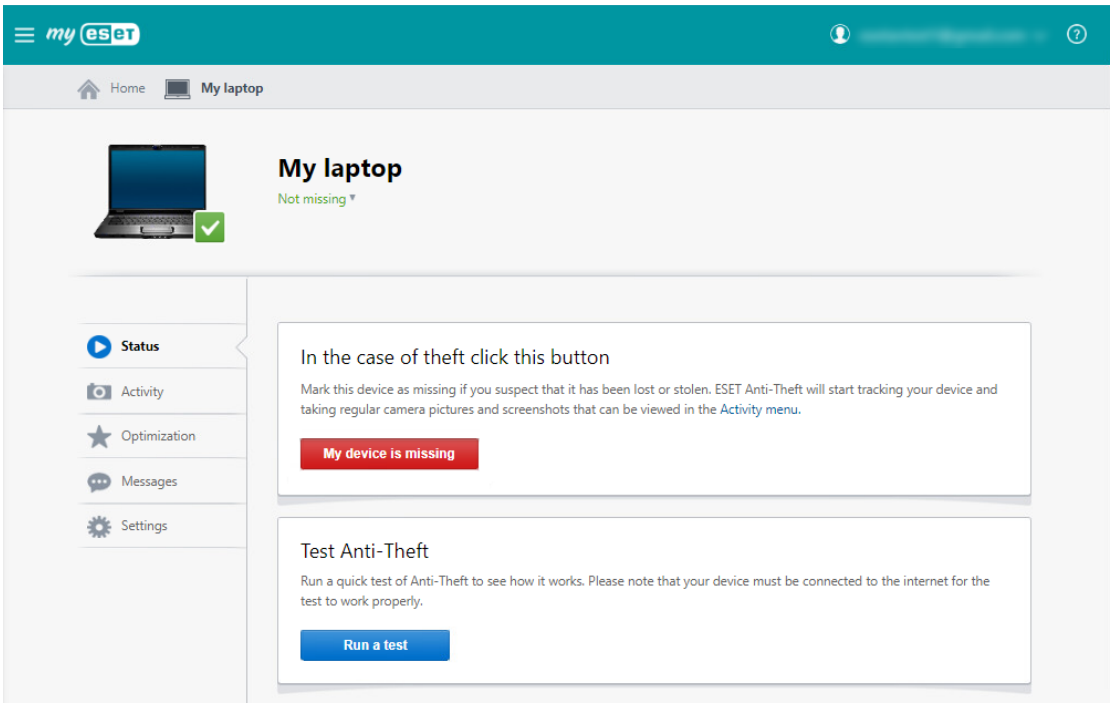
Feature for users that demand uninterrupted usage of their software, do not want to be disturbed by pop-up windows, and want to minimize CPU usage. Gamer mode can also be used during presentations that cannot be interrupted by antivirus activity. By enabling this feature, all pop-up windows are disabled, and the activity of the scheduler will be stopped completely. System protection still runs in the background but does not demand any user interaction.

Network Inspector

ESET Network Inspector is a feature included in ESET Smart Security Premium and ESET Internet Security. This feature was introduced as Home Network Protection in version 10.
This diagnostic tool provides information about the security of your router. It also displays a list of devices connected to user's network. It may be necessary to consult support resources for router or contact internet service provider to resolve certain issues within user's home network.

Anti-Theft

In case Anti-Theft is activated on at least one of user's devices and it gets lost or stolen user can come to ESET HOME to try to find it. When user marks a device as missing it will automatically start taking photos and screenshots and tracking location. Photos, screenshots and detected locations displayed on a map can be found in Activity tab. One-way messaging lets user contact the finder with a customized message that will appear on the missing device's screen. After the device is found and user marks device as recovered all automatic actions will be stopped. Optimization of settings aims to help users achieve the best Anti-Theft functionality.



Safe Banking& Browsing

Banking & Payment Protection is an additional layer of protection designed to protect financial data during online transactions. With “Secure all browsers” mode it designed to start all supported web browsers in a secure mode.

From technical perspective – it provides protection of the browser process itself against any malicious changes or intervention.

Secure Data

Secure Data by ESET allows user to encrypt data on Windows OS device and USB drives to prevent the misuse of private, confidential information.

Password Manager

The application itself is browser extension-based and supported by all major browsers. In addition, it will be available as a native application on Android and iOS devices.

It delivers a set of standard PWM features:

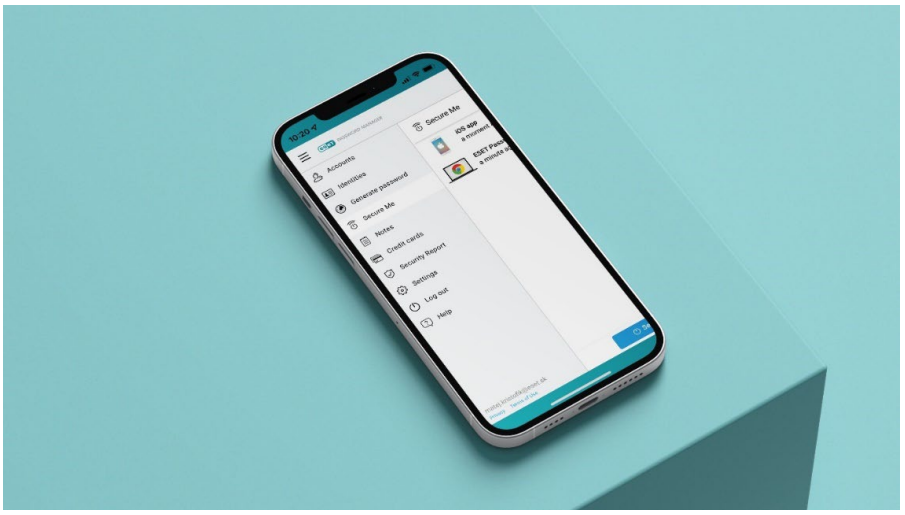
- Automatic synchronization and backup, password generator, secure notes, identity and address management, account recovery key, amount of stored accounts, two-factor authentication, credit cards management, offline access and data export

Includes new functionalities compared to the previous version:

- Remote logout from websites, security report + ‘Have I been pwned?’ feature, remotely clear browsing history, remotely close open browser tabs

In late 2020 we added management of password stores to ESET HOME as it came as a necessity for our new version of ESET Password Manager. Users that want to use it and share its benefits with others need a verified ESET premium license added to their Licenses in ESET HOME. With such license user can assign available

password stores to any email address – their own for their personal use or to somebody else's if they want them to use ESET Password Manager. ESET HOME users also can remove any password store in case they want to free them, or they can move them to other premium license in case they have a new one.



Browser Privacy & Security extension

Browser extension is part of Safe Banking & Browsing (former Banking & Payment Protection). It aims to provide an additional layer of privacy and security when user online.

The extension will work only with our Windows product not as a standalone extension. This way it will be able to have some functionalities on top of other extensions as it uses our module – for example Metadata cleanup is a feature that is a competitive advantage.

Extension application availability per platform

Windows	macOS	Android	iOS
Yes **Requires ESET product**	**No**	**No**	**No**
ESET Internet Security, ESET Smart Security Premium **ESET Security Ultimate**	-	-	-

Chrome	Firefox	Edge	Safari
Yes	**Yes**	**Yes**	**No**

Quantity per subscription

Not applicable – extension can be installed supported browser with consumer endpoint product installed (except ESET NOD32 Antivirus)

Browser tech. requirements

- **Browsers with latest updates installed**

Localizations

- **Shares the same language as the used browser**

Features

Secure Search – mark google search results as safe once scanned by our product

Browser Cleanup – removes browser private data using on-demand removal or scheduled periodic cleanup

***Website Settings Review –** review or block allowed website notifications that can interact with system even if website is closed.

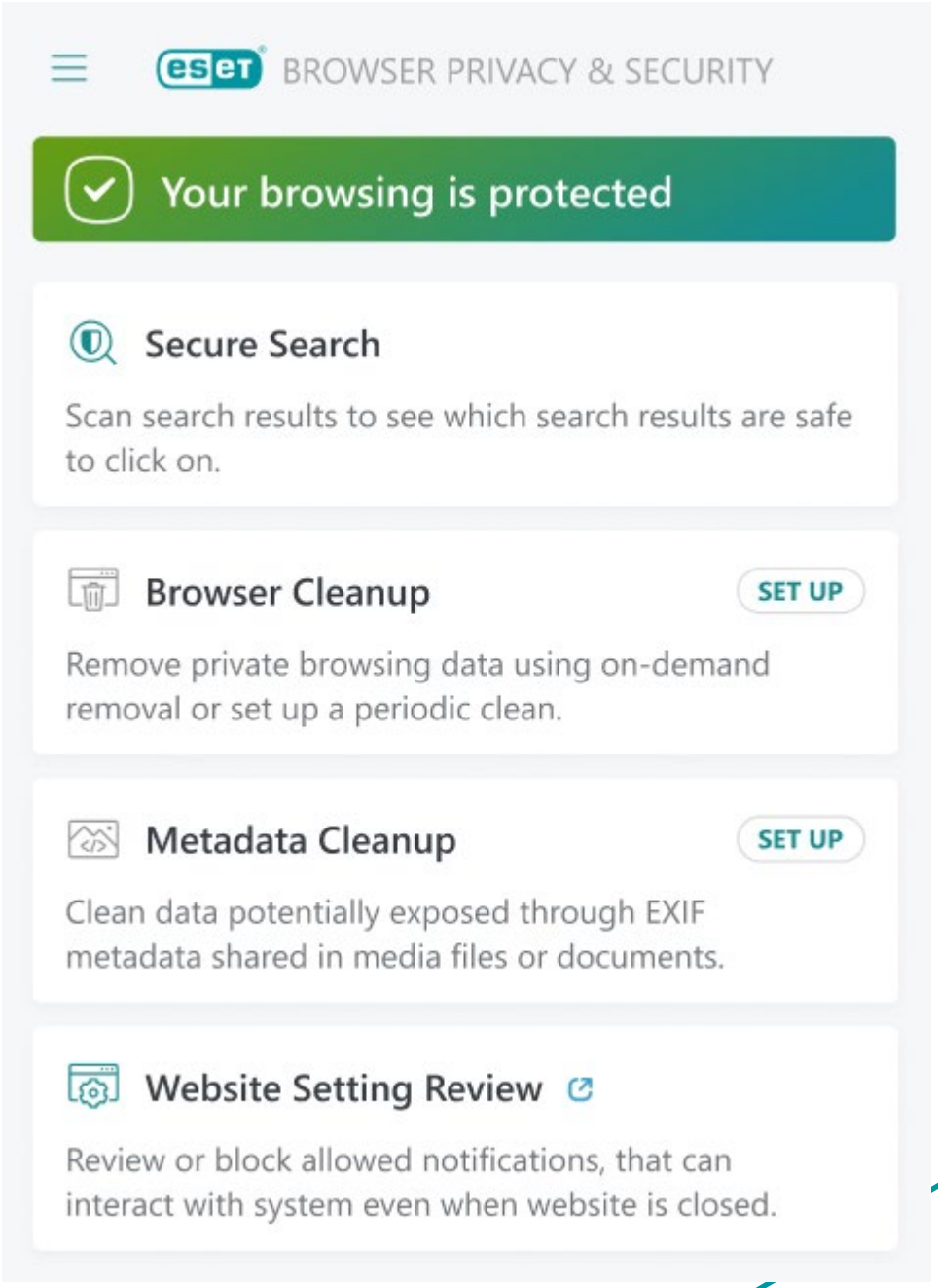
***Metadata Cleanup** – protects your privacy by removing metadata from media such as photo exif (location, camera type, time/date of photo taken)

**Available with Ultimate line only*

Activation flow

No need to go to extension store. Extension will be downloaded and added to browser during product installation

Visuals


BROWSER PRIVACY & SECURITY
Your browsing is protected
Secure Search
Scan search results to see which search results are safe to click on.
Browser Cleanup
SET UP
Remove private browsing data using on-demand removal or set up a periodic clean.
Metadata Cleanup
SET UP
Clean data potentially exposed through EXIF metadata shared in media files or documents.
Website Setting Review
Review or block allowed notifications, that can interact with system even when website is closed.

FOR RESELLERS

VPN

VPN stands for **"Virtual Private Network"** and describes the functionality to establish a private network connection when using public as well as private networks. Once user connects to a location in VPN application, his device is assigned a new IP address and his online traffic is now secured and encrypted. This makes it more difficult for third parties to track users' activities online and steal data. The encryption takes place in real time.

Internal note:

VPN feature will be provided by 3rd party vendor. VPN application will be white-labeled and customized for ESET customers.

VPN feature consists of VPN infrastructure (datacenters, servers, etc.), VPN services (provision of functional service – establishment of protected network connection), VPN application and integration with ESET HOME ecosystem by vendor (development of APIs by vendor and possibility to call them) and by ESET (billing events setup, logic behind calling the APIs, etc.). ESET will use vendor's infrastructure, services, customized application, and APIs to provide VPN feature to their customers

Please see VPN bulletin for more information

FOR RESELLERS

Identity Protection

USA	Global
Credit & Credit score monitoring Services notify you of changes made to credit reports so user can act against potential misuse of your personal information **Social Security Tracking** **Dark Web Monitoring** **Social Media Monitoring** **…**	**Dark Web Monitoring** Searching for and monitoring personal information such as email account, passwords, IDs found on the dark web
2 adults + unlimited children under 18	Individual
Includes insurance up to 1 Mil USD	No insurance
Includes identity restoration service	Includes identity restoration service
eset.identityforce.com	ESET HOME

Please see Identity Protection bulletin for more information

FOR RESELLERS

Product upgrades & End of life policy

Products have built in capability to upgrade to the latest version whenever available. This applies to module updates as well to new builds available. In minor cases, product will require user to provide updated EULA consent otherwise most updates happen in background. User may be asked to restart his device. On top, the current version and update status is available in the “Update” product tab.

End-of-life policy and currently supported products are available at on the official ESET end of life policy page. In short – only latest major version is fully supported until new major version comes out (happens in one-year cycles)