



# SECURITY MANAGEMENT CENTER

**Enterprise-grade security management solution** providing  
visibility, management and reporting across all OSes

CYBERSECURITY  
EXPERTS ON YOUR SIDE



# What is an **endpoint security management console?**

**ESET Security Management Center utilizes a web console to provide real-time visibility for on-premise and off-premise endpoints as well as full reporting and security management for all OSes.**

It is a single pane of glass over all ESET security solutions deployed in the network and controls endpoint prevention, detection & response layers across all platforms – covering desktops, servers, agentless virtual machines and even managed mobile devices.

# Why endpoint security management?

## VISIBILITY

Zero-days, advanced persistent threats, targeted attacks and botnets are all concerns for industries across the world. Having visibility into these threats in real time is extremely important to allow IT staff to respond promptly and mitigate any risk that may have developed. Due to a continued emphasis of companies to add a mobile workforce, visibility is not just needed on-premise but off-premise as well.

ESET Security Management Center provides up-to-date information to provide IT staff with the status of all computers whether they are on-premise or off-premise. It also provides visibility into all OSes that a company might have, not just a limited few. In most instances, visibility is also enhanced to show device-level information such as hardware or software inventories.

## MANAGEMENT

Today's cybersecurity landscape is constantly evolving with new attack methods and never-before-seen threats. When an attack or data breach occurs, organizations are typically surprised that their defenses were compromised or are completely unaware that the attack even happened. After the attack is discovered, organizations may then want to execute specific tasks across devices such as scans. In addition, this may lead organizations to completely change their configuration policies to better protect against a future attack.

ESET Security Management Center allows organizations to adjust the policies or configurations of endpoint security products at any point in time. In addition, tasks can be executed remotely and automatically on devices to save IT admins the time from manually having to execute tasks on each individual computer.

## REPORTING

Most organizations nowadays, if they do not need to meet any compliance, have internal requirements related to reporting. No matter the organization, there will be reports that need to be generated at scheduled intervals and provided to relevant parties, or stored for a future date.

ESET Security Management Center allows organizations to set up reports to be generated at scheduled intervals and saved to specific folders, or emailed directly to someone who requested it. Reports can be customized to provide the requestor the reports exactly how they might want them. This process is paramount to saving IT admins time in the busy work associated with on-going reporting.

*“The major advantage of ESET is that you have all users from one console and can manage and properly review their security status.”*

— Jos Savelkoul, Team Leader ICT-Department;  
Zuyderland Hospital, Netherlands; 10.000+ seats

Reports can be customized to provide the requestor the reports exactly how they want them.

Having visibility into security incidents in real time is extremely important to allow IT staff to respond promptly and mitigate any risk that may have developed.

No matter the organization, there will be reports that need to be generated on scheduled intervals and provided to relevant parties, or stored for a future date.





The ESET Security Management Center provides over 170 built-in reports and allows you to create custom reports from over 1000 data points.

Dynamic groups can sort and filter computers based on current device status, which changes over time.

# The ESET difference

## PREVENTION TO RESPONSE

ESET combines the management of our Endpoint products with our Endpoint Detection and Response solution, ESET Enterprise Inspector and our sophisticated online sandbox ESET Dynamic Threat Defense into a single easy-to-use management console.

## SINGLE-CLICK INCIDENT REMEDIATIONS

From the threats tab, an IT admin can create an exclusion, submit files for further analysis or initiate a scan from a single click. Exclusions can be made by threat name, URL, hash or combination.

## FULLY CUSTOMIZABLE NOTIFICATION SYSTEM

The notification system features a full "what you see is what you get" editor, where you will be able to fully configure notifications to be alerted on the exact information you want to be notified about.

## DYNAMIC AND CUSTOM REPORTING

The ESET Security Management Center provides over 170 built-in reports and allows you to create custom reports from over 1000 data points. This allows organizations to create reports to look and feel exactly as they might want. Once created, reports can be set up to be generated and emailed at scheduled intervals.

## AUTOMATION FRAMEWORK

Dynamic groups can sort computers based on current device status or defined inclusion criteria. Tasks can then be set up to trigger actions such as scans, policy changes or software installs/uninstalls based off dynamic group membership changes.

## FULLY AUTOMATED VDI SUPPORT

A comprehensive hardware detection algorithm is used to determine the identity of the machine based on its hardware. This allows automated re-imaging and cloning of non-persistent hardware environments. Therefore, ESET's VDI support requires no manual interaction and is fully automated.

## PROVEN AND TRUSTED

ESET has been in the security industry for over 30 years, and we continue to evolve our technology to stay one step ahead of the newest threats. This has led us to be trusted by over 110 million users worldwide. Our technology is constantly scrutinized and validated by third-party testers who show how effective our approach is at stopping the latest threats.

*"Outstanding company, superb technical support, provides strong threat protection and central management."*

— Dave, Manager of IT; Deer Valley Unified School District, USA;  
15,500+ seats

# Use cases

## Ransomware

A user opens a malicious email containing a new form of ransomware.

### SOLUTION

- ✓ IT department receives a notification via email and their SIEM that a new threat was detected on a certain computer.
- ✓ A scan is initiated with a single click on the infected computer.
- ✓ The file is submitted to ESET Dynamic Threat Defense by another click.
- ✓ After confirming the threat has been contained, warnings in ESET Security Management Center are cleared automatically.

## Code developers

Programmers who work with code on their work computer can tend to create false positives due to compiling software.

### SOLUTION

- ✓ IT department receives a notification via email and its SIEM that a new threat was found.
- ✓ The notification shows the threat came from a developer's computer.
- ✓ With one click, the file is submitted to ESET Dynamic Threat Defense to confirm the file is not malicious.
- ✓ IT department, with one click, puts an exclusion in place to prevent future false positives from being displayed on this folder.





# VDI deployments

Non-persistent hardware environments typically require manual interaction from an IT department or create reporting and visibility nightmares.

## SOLUTION

- ✓ After deploying a master image to computers already present in ESET Security Management Center, computers will continue reporting to the previous instance despite a complete re-image of the system.

---

- ✓ Machines that after the end of a work shift return back to their initial state will not cause duplicate machines and instead will be matched into one record.

---

- ✓ On deployment of non-persistent images, you can create an image that includes the agent, then whenever a new machine is created with another hardware fingerprint, it automatically will create new records in ESET Security Management Center.

---

# Hardware and software inventory

Organizations need to know what software is installed on each computer, as well as how old each computer is.

## SOLUTION

- ✓ View every installed piece of software, including version number, in the computer record.

---

- ✓ View every computer's hardware details, such as device, manufacturer, model, serial number, processor, RAM, HD space and more.

---

- ✓ Run reports to view a more holistic view of an organization to make budgetary decisions on hardware upgrades in future years based off current make and models.

---

# Software remediation

Organizations need to know when an unapproved software has been installed, then are required to remediate the software afterwards.

## SOLUTION

- ✓ Set up a dynamic group within ESET Security Management Center to look for a specific unwanted piece of software.

---

- ✓ Create a notification to alert the IT department when a computer meets this criterion.

---

- ✓ Set up a software uninstall task in the ESET Security Management Center to execute automatically when a computer meets the dynamic group criteria.

---

- ✓ Set up a user notification that automatically pops up on the user's screen indicating that they committed a software installation violation by installing the above software.

---

ESET Security Management Center can be installed on Windows, Linux or deployed as Virtual Appliance.

Multi-tenancy support and 2FA secured logins allow full streamlining of responsibilities across large enterprise teams.

*“Centrally managed security on all endpoints, servers and mobile devices was a key benefit for us.”*

— IT Manager; Diamantis Masoutis S.A., Greece;  
6.000+ seats

# ESET Security Management Center technical features

## FLEXIBLE INSTALL

ESET Security Management Center can be installed on Windows, Linux or via Virtual Appliance. After install, all management is done via a web-console, allowing easy access and management from any device or operating system.

## SINGLE PANE OF GLASS

All ESET endpoint products despite the OS can be managed from a single ESET Security Management Center instance. In addition, ESET Security Management Center supports full Mobile Device Management (MDM) of Android and iOS devices.

## COMPLETELY MULTI-TENANT

Multiple users and permission groups can be created to allow access to a limited portion of the ESET Security Management Center instance. This allows full streamlining of responsibilities across large enterprise teams.

## HARDWARE/SOFTWARE INVENTORY

Not only does ESET Security Management Center report on all installed software applications across an organization, it also reports on installed hardware. This allows you to do more from a single location by dynamically grouping computers based off make, model, OS, processor, RAM, HD space and many more items.

## GRANULAR POLICY CONTROL

Organizations can set up multiple policies for the same computer or group and can nest policies for inherited permissions. In addition, organizations can configure policy settings as user-configurable, so you can lock down any number of settings from the end users.

## SIEM SUPPORT

ESET Security Management Center fully supports SIEM tools and can output all log information in the widely accepted JSON or LEEF format.



Dashboard of ESET Security Management Center

# About ESET

**ESET—a global player in information security—has been named as the only Challenger in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms.\***

For more than 30 years, ESET® has been developing industry-leading IT security software and services, delivering instant,

comprehensive protection against evolving cybersecurity threats for businesses and consumers worldwide.

ESET is privately owned. With no debts and no loans, we have the freedom to do what needs to be done for the ultimate protection of all our customers.

## ESET IN NUMBERS

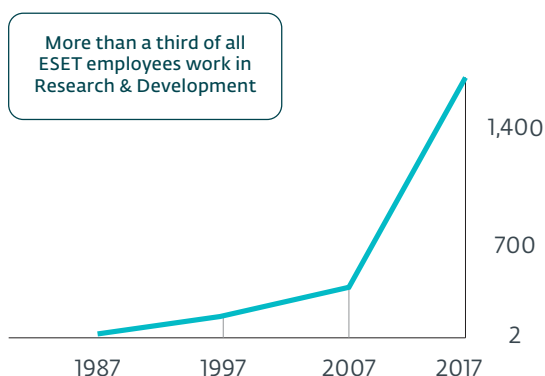
**110m+**  
users  
worldwide

**400k+**  
business  
customers

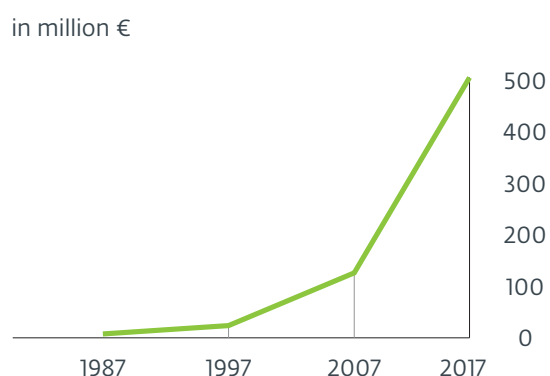
**200+**  
countries &  
territories

**13**  
global R&D  
centers

## ESET EMPLOYEES



## ESET REVENUE



\*Gartner does not endorse any vendor, product or service depicted in its research publications. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

---

SOME OF OUR CUSTOMERS

---

**HONDA**

protected by ESET since 2011  
license prolonged 3x, enlarged 2x

**Canon**

Canon Marketing Japan Group

protected by ESET since 2016  
more than 14.000 endpoints

**Allianz**   
Suisse

protected by ESET since 2016  
more than 4,000 mailboxes

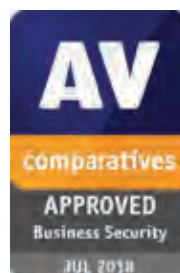


ISP security partner since 2008  
2 million customer base

---

SOME OF OUR TOP AWARDS

---



*“Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the shortlist for consideration in enterprise RFPs for anti-malware solutions.”*

KuppingerCole Leadership Compass

Enterprise Endpoint Security: Anti-Malware Solutions, 2018



