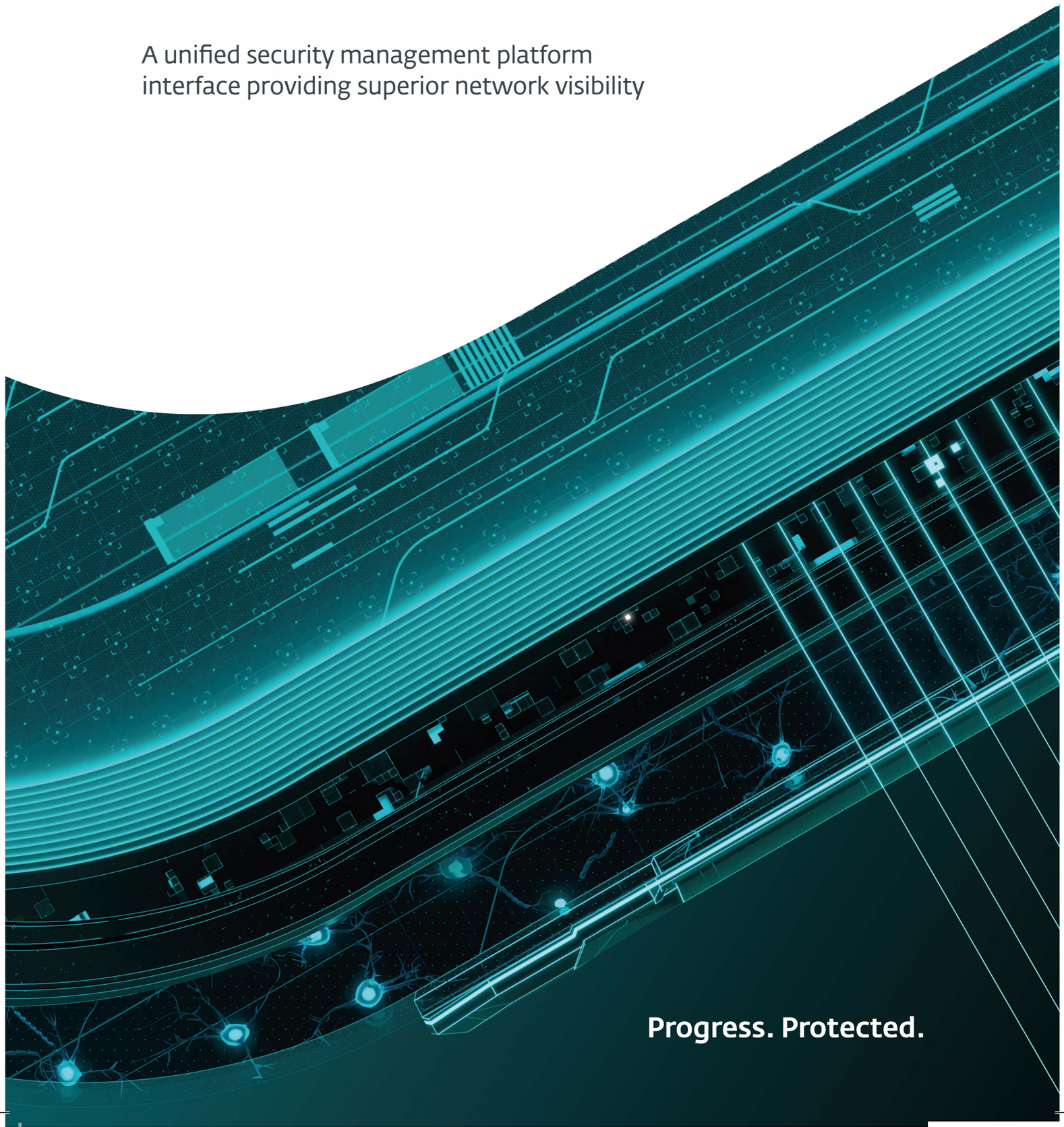
OVERVIEW

PROTECT

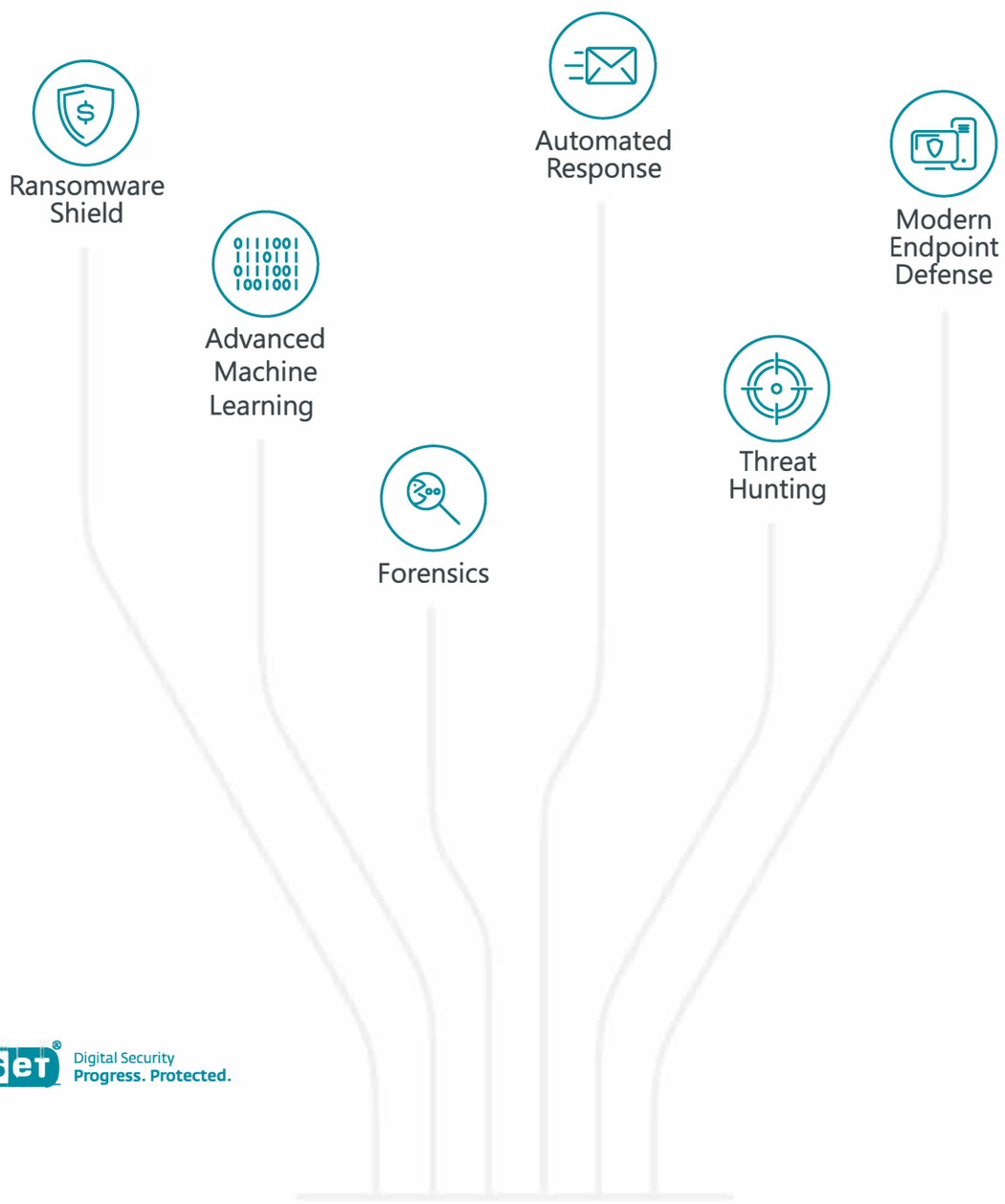
A unified security management platform
interface providing superior network visibility



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

ESET PROTECT is a versatile UEM (Unified Endpoint Management) console that provides access to the powerful ESET PROTECT Platform. It is deployable on-premise or via the cloud, and ensures real-time visibility for on-premise and off-premise endpoints, as well as full reporting and security management for all operating systems.

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



eset Digital Security
Progress. Protected.

ABSITechnology

The ESET Difference

PREVENTION TO RESPONSE

Within a single console, ESET PROTECT combines the management of multiple ESET security solutions. From threat prevention to detection and response, it covers your entire organisation in a multilayered fashion for the best level of protection.

SINGLE-CLICK INCIDENT REMEDIATIONS

From the main dashboard, an IT admin can quickly assess the situation and respond to issues. Actions such as creating an exclusion, submitting files for further analysis, or initiating a scan are available within a single click. Exclusions can be made by threat name, URL, hash or combination.

ADVANCED RBAC

Starting with MFA-protected access, the console is equipped with an advanced Role-Based Access Control (RBAC) system. Assign admins and console users to specific network branches, groups of objects, and specify permission sets with a high degree of granularity.

MSP READY

If you're a Managed Service Provider (MSP) taking care of your clients' networks, you'll appreciate the full multi-tenancy capabilities of ESET PROTECT. MSP licences are automatically detected and synced with the licencing server, and the console lets you do advanced actions such as install/ remove any 3rd party application, run scripts and remote commands, list running processes, HW configurations, etc.

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 scrutinised and validated by third-party testers who show how effective our approach is at stopping the latest threats.

DYNAMIC AND CUSTOM REPORTING

ESET PROTECT provides over 170 built-in reports and allows you to create custom reports from over 1000 data points. This allows organisations 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

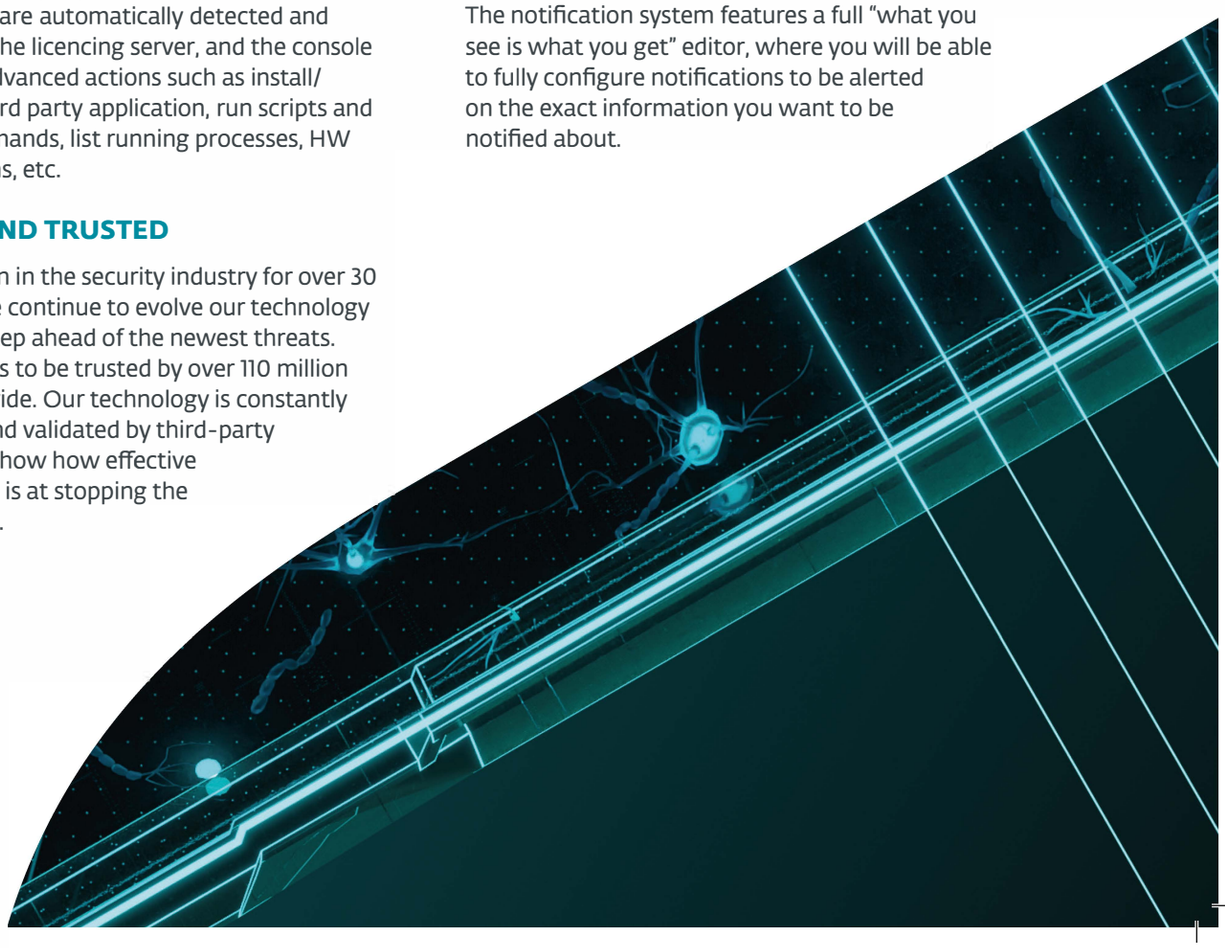
Dynamic groups can sort computers based on current device status or defined inclusion criteria. Tasks can then be set up to trigger actions such as scans, policy changes or software installs / uninstalls based off dynamic group membership changes.

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.

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.



Technical features

SINGLE PANE OF GLASS

All ESET endpoint products can be managed from a single ESET PROTECT console. This includes workstations, mobiles, servers, and virtual machines and the following OSes: Windows, macOS, Linux, and Android.

SUPPORT FOR XDR

To further improve situational awareness and provide visibility across your network, ESET PROTECT works together with ESET Inspect, the XDR-enabling component of the ESET PROTECT platform. ESET Inspect is multiplatform (Windows, macOS and Linux), enables advanced threat-hunting and remediation, and can seamlessly integrate with your Security Operations Center.

FULL DISK ENCRYPTON (FDE)

Full Disk Encryption is native to ESET PROTECT, managing the encryption of data on both Windows and Mac (FileVault) endpoints, improving data security and helping organisations solve the problem of data regulation compliance.

ADVANCED THREAT DEFENSE

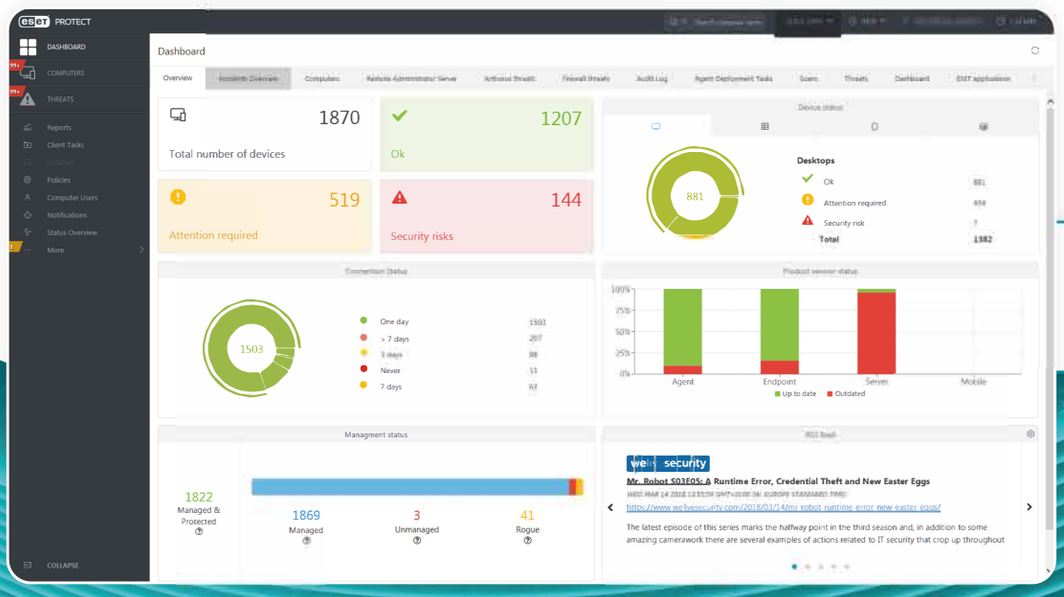
The support for advanced threat defense greatly improves detection of zero-day threats such as ransomware by quickly analysing suspicious files in ESET's powerful cloud sandbox. In addition, it runs a battery of highly comprehensive malware scans, including cloud detonation.

HARDWARE/SOFTWARE INVENTORY

Not only does ESET PROTECT report on all installed software applications across an organisation, it also reports on installed hardware.

COMPLETELY MULTITENANT

Multiple users and permission groups can be created to allow access to a limited portion of the ESET PROTECT console. This allows full streamlining of responsibilities across large enterprise teams. This allows you to do more from a single location by dynamically grouping computers based on make, model, OS, processor, RAM, HD space and many more items.



Dashboard of ESET PROTECT

eset Digital Security. Progress. Protected.

ABSI Technology

GRANULAR POLICY CONTROL

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

SIEM AND SOC SUPPORT

ESET PROTECT fully supports SIEM tools and can output all log information in the widely accepted JSON or LEEF format, allowing for integration with Security Operations Centers (SOC).

ESET VULNERABILITY & PATCH MANAGEMENT

Actively tracks vulnerabilities in operating systems and common applications, and enables automated patching across all endpoints managed through ESET PROTECT.

Use Cases

VDI deployments

PROBLEM

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

SOLUTION

- ✓ After deploying a master image to computers already present in ESET PROTECT, computers will continue reporting to the previous instance despite a complete re-imaging of the system.
- ✓ Machines returning to their initial state at the end of a work shift will not cause duplicate machines and instead will be matched into one record.
- ✓ Upon deployment of non-persistent images, you can create an image that includes the agent, so whenever a new machine is created with another hardware fingerprint, it automatically creates new records in ESET PROTECT.

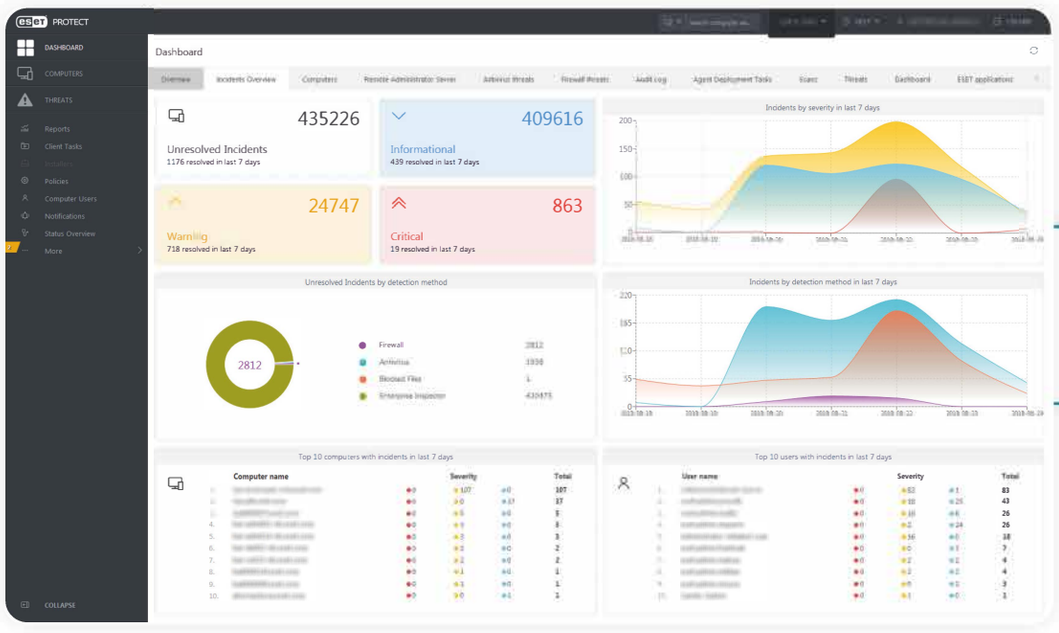
Software remediation

PROBLEM

Organisations need to know when unapproved software has been installed, and to remediate the software afterwards.

SOLUTION

- ✓ Set up a dynamic group within ESET PROTECT 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 PROTECT console 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 have committed a software installation violation by installing the software in question.



ESET PROTECT dashboard—incidents overview

Digital Security
Progress. Protected.

ABSI Technology

Ransomware

PROBLEM

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 LiveGuard Advanced with another click.
- ✓ After confirming the threat has been contained, warnings in the ESET PROTECT console are cleared automatically.

Code developers

PROBLEM

Programmers who work with code on their work computers might 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 LiveGuard Advanced 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.

Hardware and software inventory

PROBLEM

Organisations 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 organisation in order to make budgetary decisions on hardware upgrades in future years based on current makes and models.

HOW TO BUY:

Simply purchase any of the solutions
for busin
de

START YOUR 30-DAY TRIAL NOW

Unlock your 30-day free trial to test out the fully functional solution, including protection for endpoints.

eset Digital Security
Progress. Protected.

About ESET

WHEN TECHNOLOGY ENABLES PROGRESS, ESET® IS HERE TO PROTECT IT.

ESET brings over 30 years of technology-driven innovation and provides the most advanced cybersecurity solutions on the market. Our modern endpoint protection is powered by unique ESET LiveSense® multilayered security technologies, combined with the continuous use of machine learning and cloud computing. Backed by the world's best threat intelligence and research, ESET products offer the perfect balance of prevention, detection and response capabilities. With high usability and unparalleled speed, we are dedicated to protecting the progress of our customers, ensuring maximum protection.

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

195
countries and territories

13
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 2022

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in December 2022.

Leader
SPRING
2023

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

The Radicati Group, Inc.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET has been recognised asa 'Top Player' for the fourth year in a row in Radicati's 2023 Advanced Persistent Threat Market Quadrant.