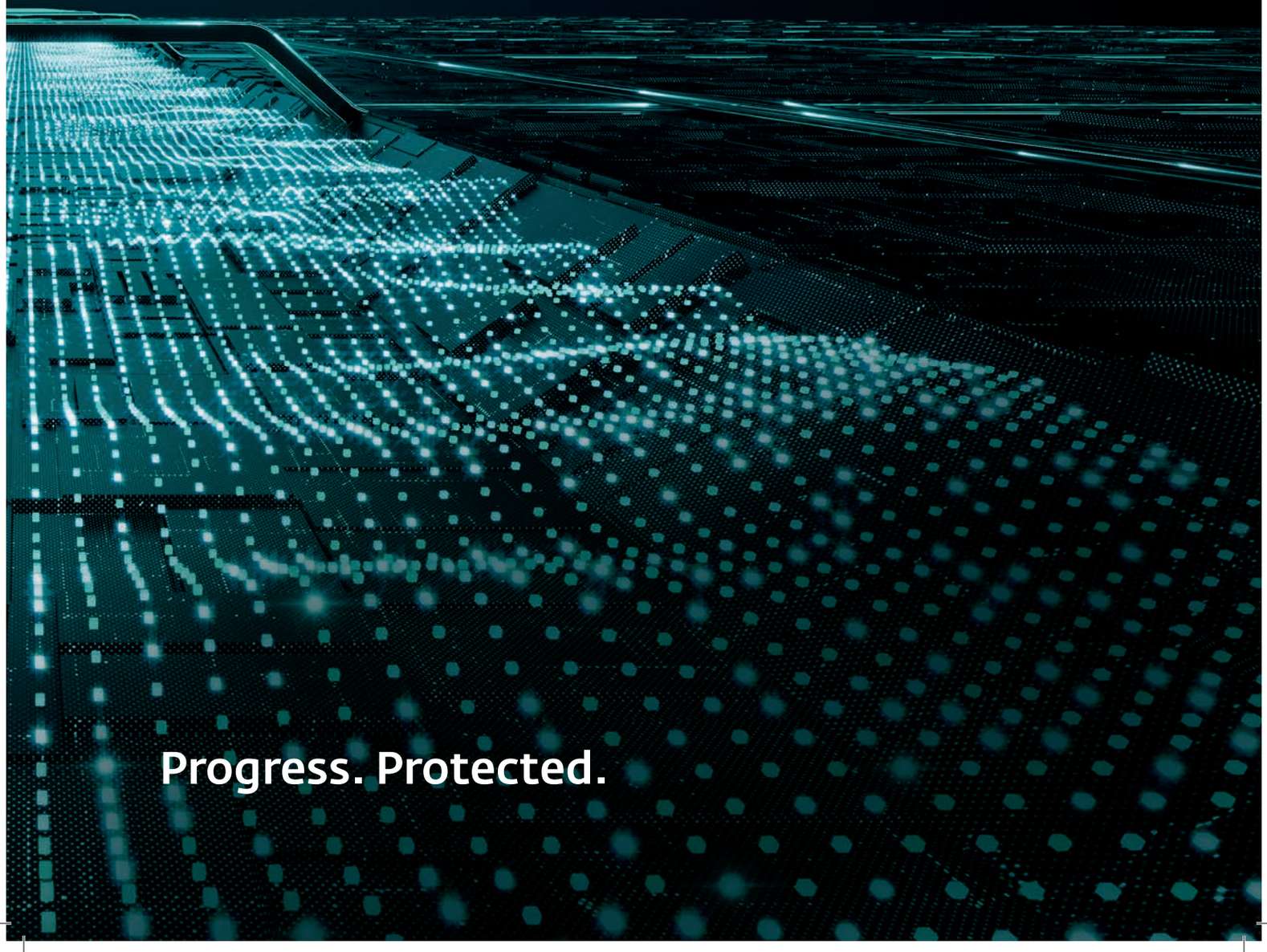
SOLUTION OVERVIEW

PROTECT

Unified security management platform
providing superior network visibility.



Progress. Protected.

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

ESET PROTECT is a versatile UEM console, deployable on-premise or via the cloud, that 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.

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 the IT staff to respond promptly and mitigate any risk that may have developed. Due to a continued emphasis on companies to add a mobile workforce, visibility is not just needed on-premise but off-premise as well.

ESET PROTECT provides up-to-date information to inform IT staff about the status of all endpoints 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 to ensure complete situational awareness.

MANAGEMENT

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

ESET PROTECT comes with powerful and smart predefined policies but allows organisations to fine-tune the policies or configurations of endpoint security products at any time. In addition, tasks can be automated to save IT admins the time from manually having to execute them on each individual computer.

REPORTING

On top of having to meet data compliance regulations, most organizations have their internal requirements related to reporting. No matter the organisation, there will be reports that need to be generated at scheduled intervals and provided to relevant parties or stored for future use.

ESET PROTECT can generate reports at scheduled intervals and saved to specific folders or emailed directly to someone who requested it. There are dozens of useful report templates, and these can be used right away or customised to provide the requestor with what they need. 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 on one console and can manage and properly review their security status."

— Jos Savelkoul, Team Leader ICT-Department;
Zuyderland Hospital, Netherlands, 10,000+ seats

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.

No matter the organisation, there will be reports that need to be generated at scheduled intervals and provided to relevant parties or stored for future use.

The ESET difference

PREVENTION TO RESPONSE

Within a single console, ESET PROTECT combines the management of multiple ESET's security solutions. From threat prevention to detection and response, they cover 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 create an exclusion, submit files for further analysis or initiate 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.

FULLY CUSTOMISABLE 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

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.

PROVEN AND TRUSTED

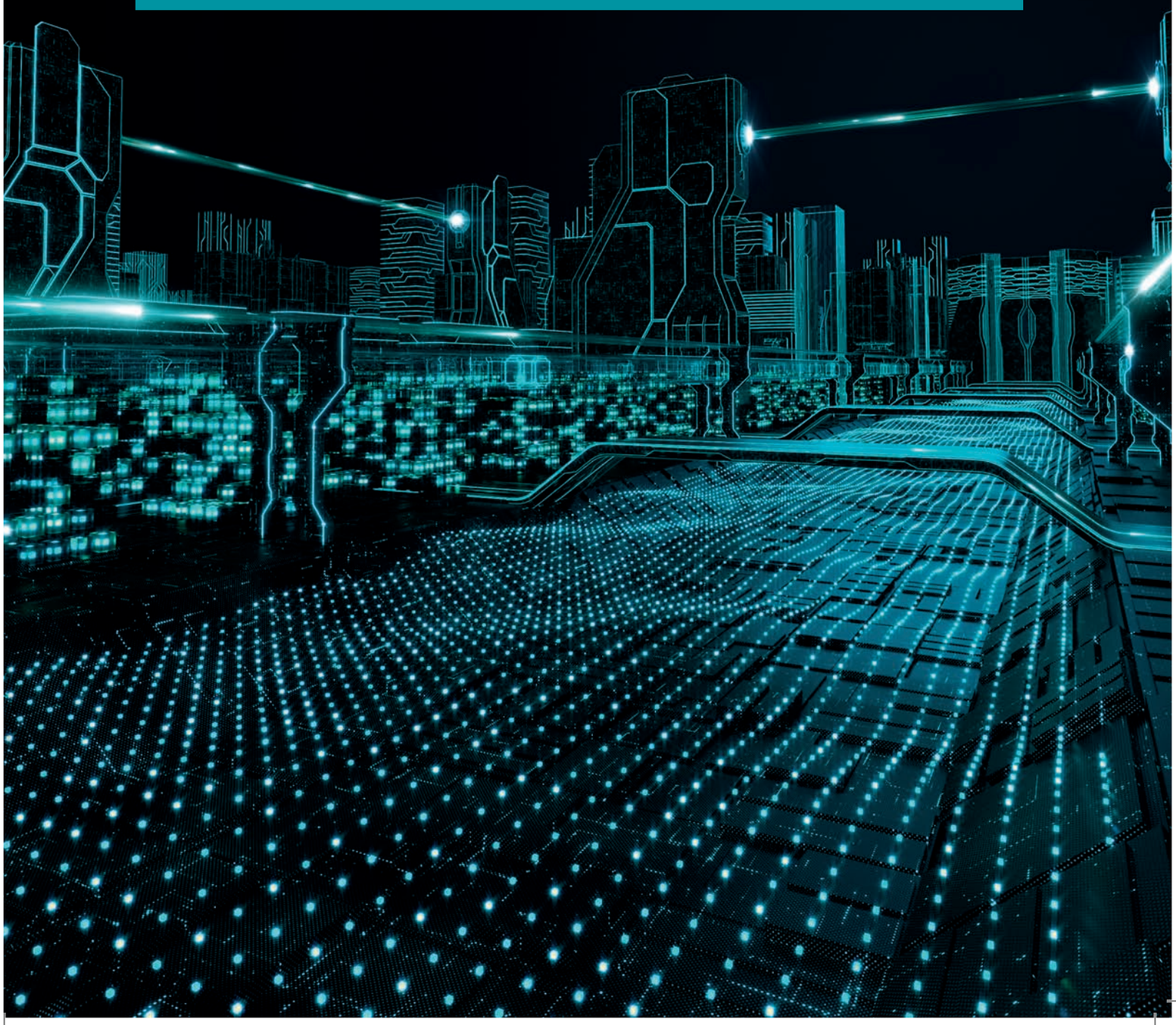
ESET has been in the security industry for over 30 years, and we continue to evolve our technology to stay one step ahead of the newest threats. This has led us to be trusted by over 110 million users worldwide. Our technology is constantly scrutinised and validated by third-party testers who show how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

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 licensing server, and the console lets you do advanced actions such as install/remove any 3rd party application, run scripts, remote commands, list running processes, HW configurations, etc.

"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

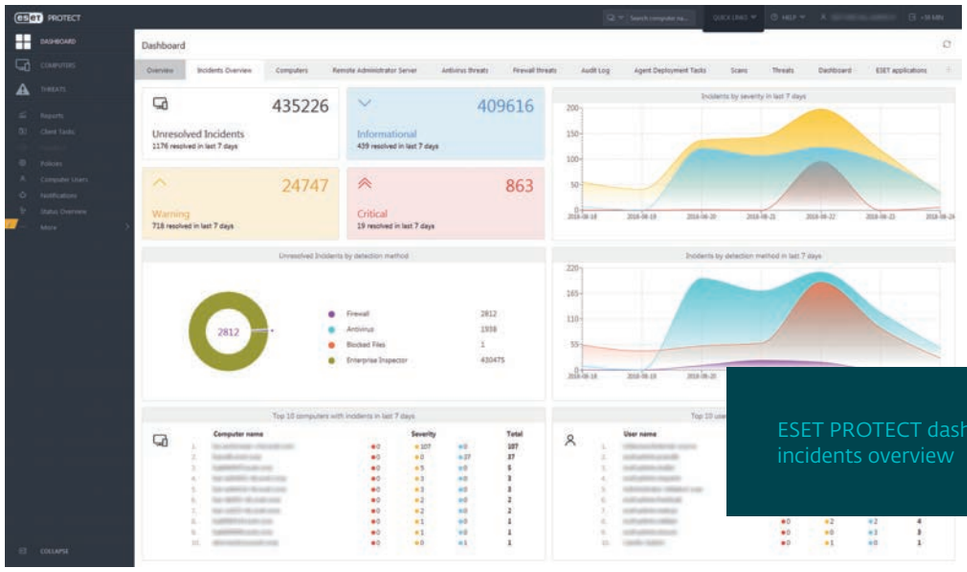
- ✓ IT department receives a notification via email and their SIEM that a new threat was detected on a certain computer.
- ✓ A scan is initiated with a single click on the infected computer.
- ✓ The file is submitted to ESET LiveGuard Advanced with another click.
- ✓ After confirming the threat has been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

Code developers

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.



ESET PROTECT dashboard—incidents overview

VDI deployments

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-image 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.
- ✓ On 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.

Hardware and software inventory

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

SOLUTION

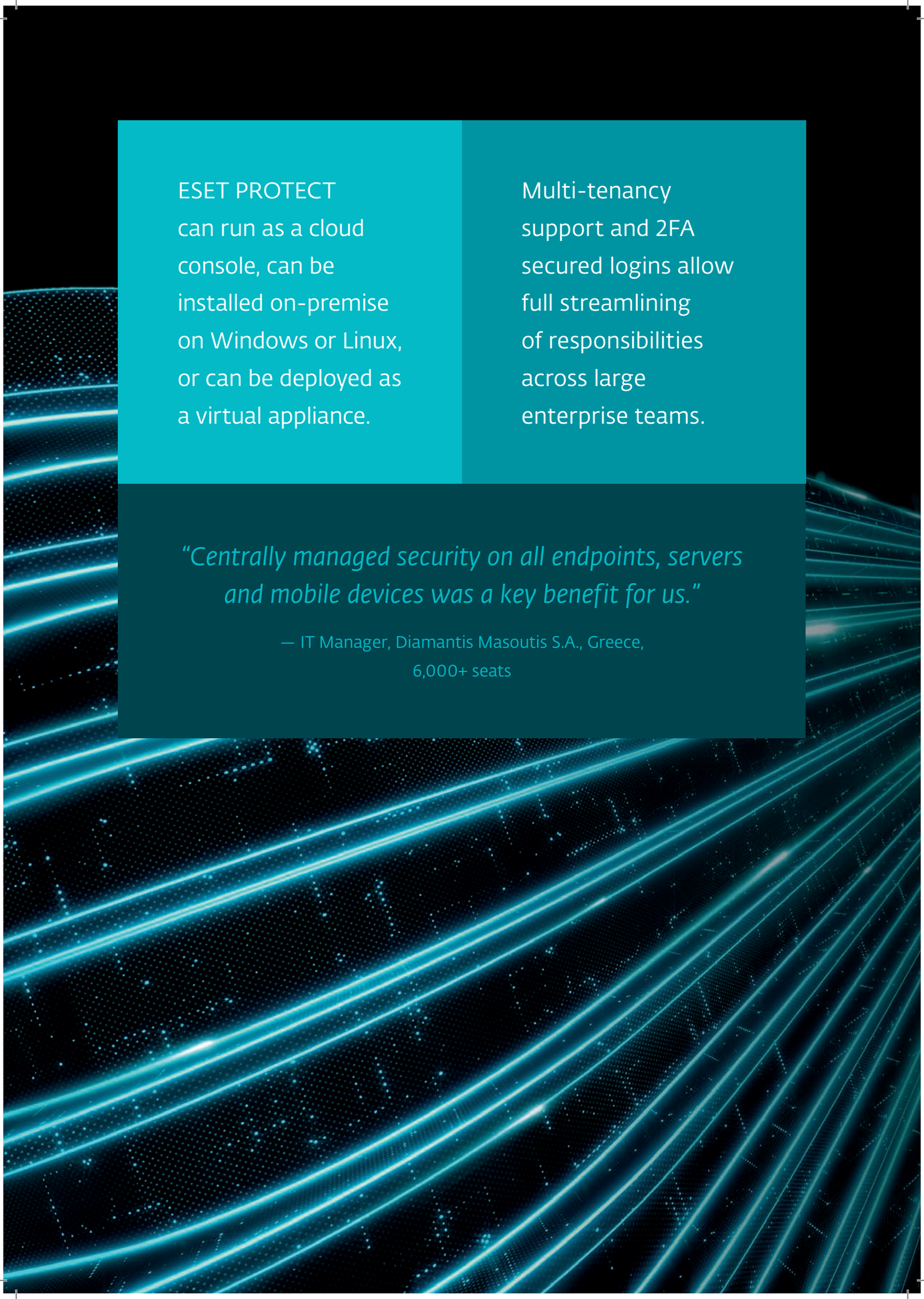
- ✓ View every installed piece of software, including version number, in the computer record.
- ✓ View every computer's hardware details, such as device, manufacturer, model, serial number, processor, RAM, HD space and more.
- ✓ Run reports to view a more holistic view of an organisation in order to make budgetary decisions on hardware upgrades in future years based on current makes and models.

Software remediation

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 committed a software installation violation by installing the software in question.



ESET PROTECT can run as a cloud console, can be installed on-premise on Windows or Linux, or can be deployed as a 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

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 encryption of data on both Windows and Mac (FileVault) endpoints, improving data security and helping organizations solving the problem of data regulation compliance.

ADVANCED THREAT DEFENCE

The support for advanced threat defence 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.

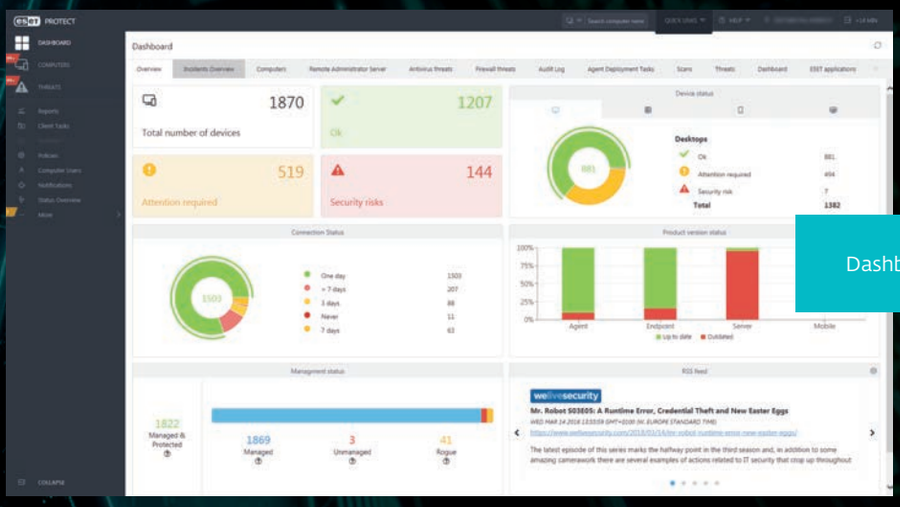
This allows you to do more from a single location by dynamically grouping computers based on make, model, OS, processor, RAM, HD space and many more items.

GRANULAR POLICY CONTROL

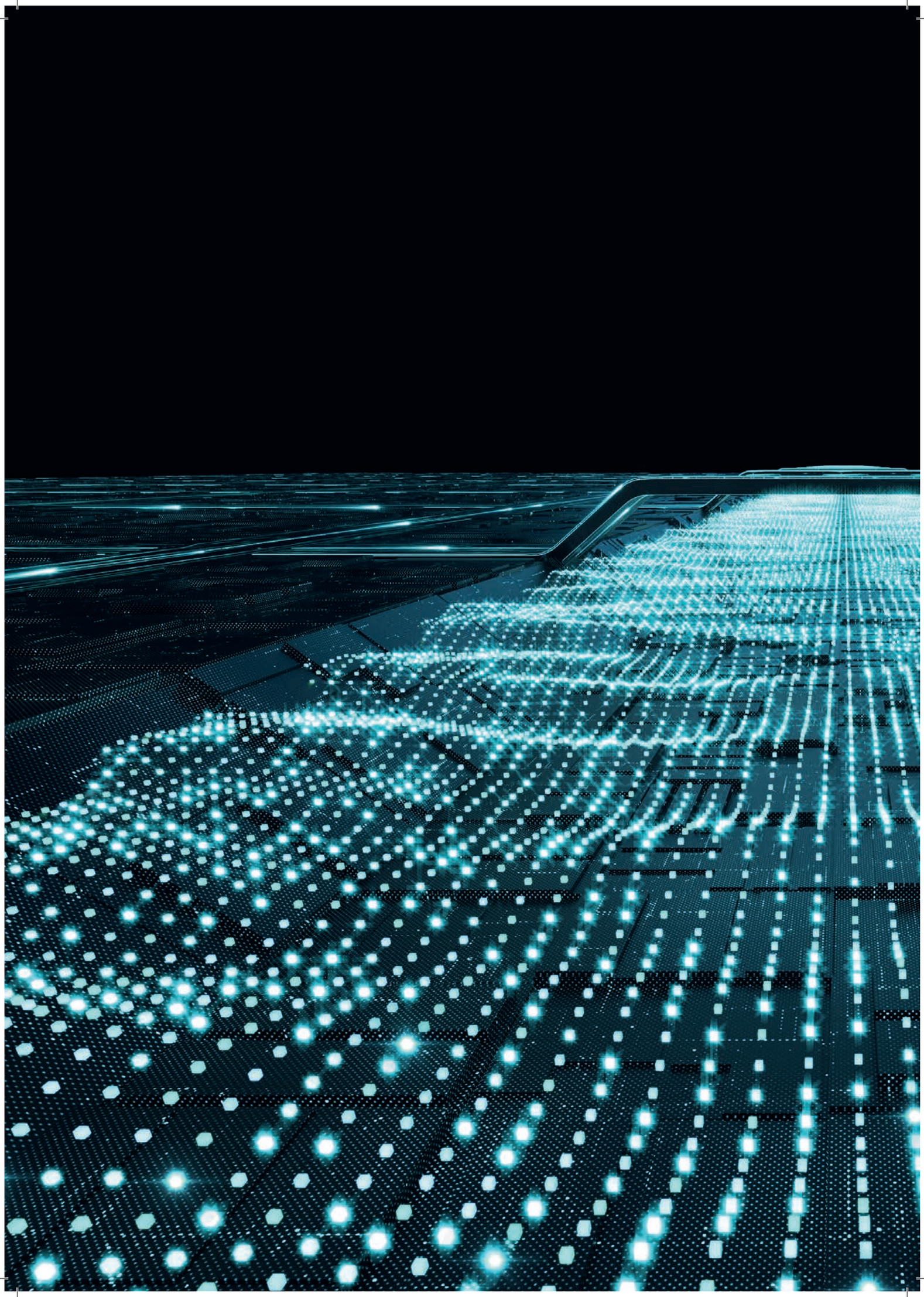
Organisations can set up multiple policies for the same computer or group and can nest policies for inherited permissions. In addition, organisations can configure policy settings as user-configurable, so you can lock down any number of settings from the end users.

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).



Dashboard of ESET PROTECT



Your next steps

How to buy:
Simply purchase any of the solutions for businesses directly from *our dedicated website*.

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

Migration from on-premise ESET console:
Do you currently use ESET's on-prem console? Contact an ESET partner in your area to assist you with migration.
https://www.eset.com/int/business/partner/find/

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

ESET IN NUMBERS

1bn+
internet users protected

400k+
business customers

200+
countries & 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

T

ISP security partner since 2008 2 million customer base

COMMITTED TO THE HIGHEST INDUSTRY STANDARDS

AV comparatives APPROVED Business Security DEC 2021

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in December 2021.

G2 Leader WINTER 2022

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

FORRESTER®

ESET solutions are regularly recognized by leading analyst firms, including in "The Forrester Tech Tide(TM): Zero Trust Threat Detection And Response, Q2 2021" as a sample vendor.

Digital Security
Progress. Protected.