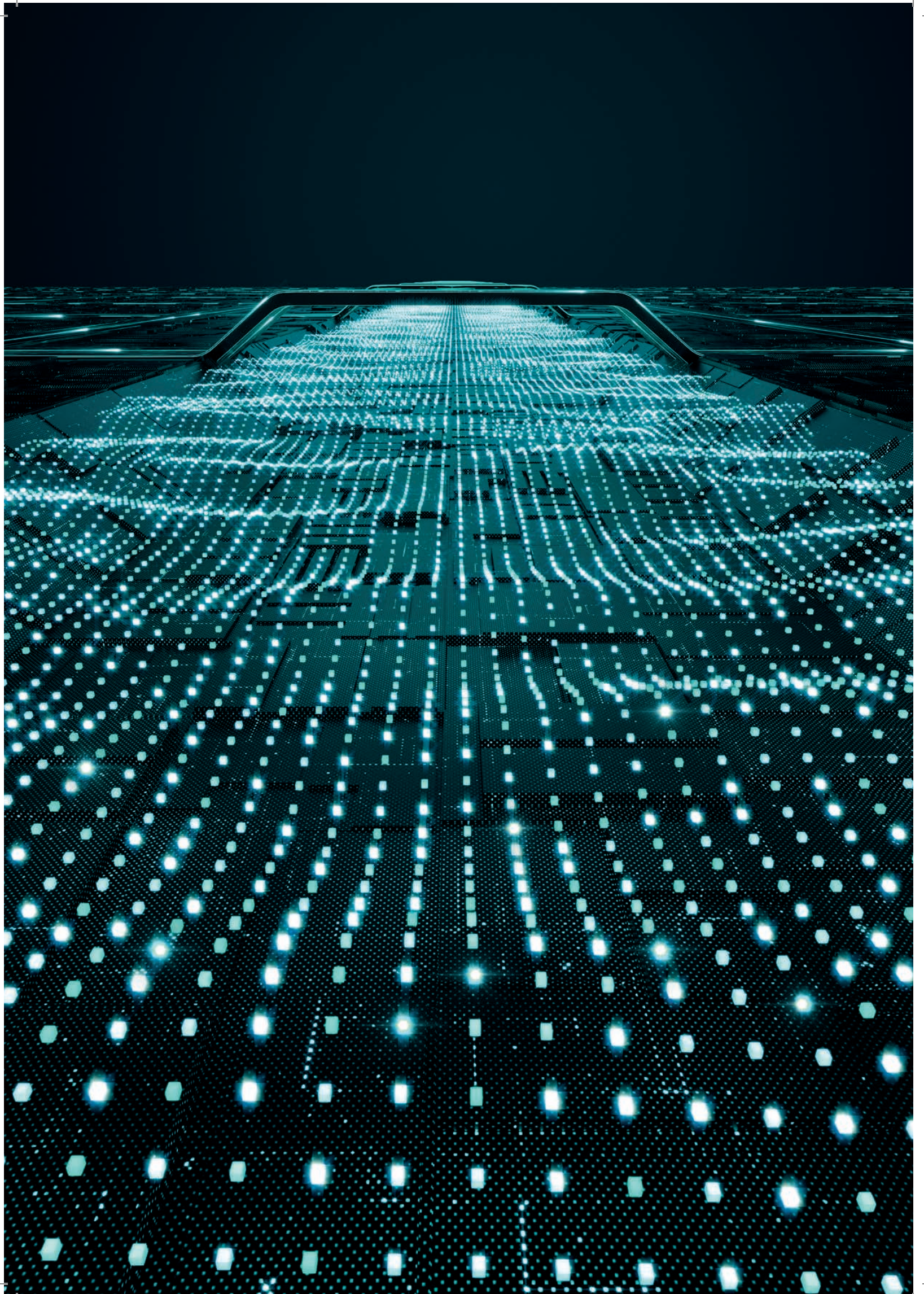




INSPECT

The XDR-enabling component of the
ESET PROTECT platform, delivering
breach prevention, enhanced visibility
and remediation

Progress. Protected.



What is an **Extended Detection & Response (XDR) solution?**

ESET Inspect, the XDR-enabling component of the ESET PROTECT platform, is a tool for identification of anomalous behaviour and breaches, risk assessment, incident response, investigations and remediation.

It enables incident responders to monitor and evaluate all activities in the network and on connected devices. If needed, it also helps automate immediate remedial actions.

ESET's 800+ (and counting) detection rules also enable comprehensive threat hunting.

Why Extended Detection & Response?

DATA BREACHES

Not only do companies need to identify that a data breach has occurred, they also need to contain and remediate it. All of this needs to be done with the utmost precision and without any disruption to business continuity. Most businesses are not prepared to perform this type of full-fledged investigation, and instead hire an outside vendor to assist. Today, organisations need increased visibility into their computers to ensure that emerging threats, risky employee behaviour and unwanted applications are not putting company profits and reputation at risk.

The top industries for data breaches are traditionally ones that have valuable data such as financial, retail, healthcare and the public sector. However, that does not mean that other industries are safe – just that hackers typically weigh effort versus the payoff.

ADVANCED PERSISTENT THREATS (APT) AND TARGETED ATTACKS

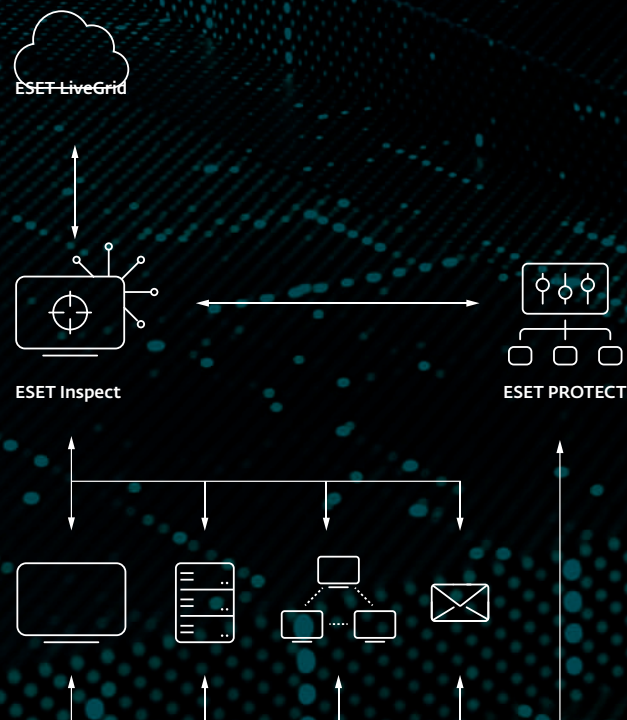
XDR systems are commonly utilised to: identify APTs or targeted attacks via Threat Hunting; reduce incident response time; and proactively prevent future attacks. Uncovering APTs in particular is important for enterprises as most businesses today don't feel prepared for the newest attacks that can be undetected in the network for days or even months.


Provides a **unique behaviour and reputation-based detection** that is fully transparent to security teams and gives them real-time feedback gathered from over 100 million endpoints in our LiveGrid.

INCREASED ORGANISATION VISIBILITY

Insider threats and phishing attacks are major problems for enterprise businesses. Phishing attacks are commonly used against enterprises because of the large number of employees to target. The odds are good that a single employee will take the bait and end up compromising the entire business. Insider attacks are another threat for enterprises, again because the large number of workers increases the odds that one of them may be working against the company's best interests.

XDR systems provide the increased visibility necessary for organisations to see, understand, block and remediate any issues across all their devices. ESET Inspect can for example quickly identify and stop malicious scripts that masquerade themselves as parts of benign documents, such as Word files.





Today, organisations need increased visibility into their computers to ensure that **emerging threats**, **risky employee behaviour** and **unwanted applications** are not putting company profits and reputation at risk.



The ESET Difference

COMPLETE PREVENTION, DETECTION AND RESPONSE

Enables quick analysis and remediation of any security issue in your network. ESET's underlying multilayered security, in which every single layer sends data to ESET Inspect, analyses vast amounts of data in real time so that no threat goes undetected.

SOLUTION FROM A SECURITY-FIRST VENDOR

ESET has been fighting cyber threats for more than 30 years. As a science-based company it has long been at the leading edge of developments like machine learning, cloud technology and now XDR.

PREVENTION IS BETTER THAN CURE

ESET's approach to XDR is tightly connected to its multi-award-winning prevention products. Thanks to its commitment to developing high-quality detection technology, ESET prevention technology is world-leading.

DETAILED NETWORK VISIBILITY

With transparent detection rules (ESET has 800+ and counting), advanced indicators of compromise (IoC) and search capability, an In-Depth Executable Review of your network will allow you to identify anything suspicious.

READY TO START WORK NOW

ESET's solution works out-of-the-box, but is powerful enough to allow granular modification by experienced threat hunters.

FLEXIBILITY OF DEPLOYMENT

We let you decide how to deploy your security solution: ESET Inspect can run via your own servers on-prem, or via a cloud-based installation, allowing you to tune your setup according to your TCO targets and hardware capacity.

MITRE ATT&CK™

ESET Inspect references its detections to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework, which – with just one click – provides you with comprehensive information about even the most complex threats.

REPUTATION SYSTEM

Extensive filtering enables security engineers to identify every known-good application, using ESET's robust reputation system. The ESET system contains a database of hundreds of millions of benign files to ensure security teams spend their time on unknown, and potentially malicious files, not on false positives.

AUTOMATION AND CUSTOMISATION

Easily tune ESET Inspect to the level of detail and automation you need. Choose your level of desired interaction, and the type and amount of data to be stored, during the initial setup and with the help of preset user profiles, and then let Learning Mode map your organisation's environment and suggest exclusions to false positives. where needed.

Use Cases

In-Depth Threat Detection – Ransomware

Nowadays, ransomware tries to be unnoticed in the network, silently spreading among as many network endpoints as possible. It penetrates into machine backups to ensure even rollback to previous images will not prevent the immediate execution of the ransomware.

ESET Inspect agent extends the functionality of ESET endpoint security solutions and allows you to proactively detect ransomware that already may exist on your network. In a typical ransomware scenario, a user receives an email with a document attached. The user then proceeds to open the word document and is asked to run macros. Once the user runs macros, an executable is dropped on the system and begins encrypting everything it can, including mapped drives.

ESET Inspect allows your security team to see alerts on this kind of behaviour, and in a few clicks you can see what was affected, where and when a specific executable, script or action was performed, and analyse the cause of it “back to the root.”

USE CASE

A business wants additional tools to proactively detect ransomware in addition to being notified promptly if ransomware-like behaviour was seen in the network.

SOLUTION

- ✓ Input rules to detect applications when executing from temporary folders.
- ✓ Input rules to detect Office files (Word, Excel, PowerPoint) when they execute additional scripts or executables.
- ✓ Alert if any of the most common ransomware extensions are seen on a device.
- ✓ View Ransomware Shield alerts from ESET Endpoint Security Solutions in the same console.

The screenshot displays the ESET Protect & Inspect Cloud interface. On the left is a navigation sidebar with options like Dashboard, Computers, Detections, Search, Incidents, Executables, Scripts, and Admin. The main area shows a detailed view of a blocked process:

- Blocked by Anti-Phishing blacklist:** Detected by ESET Endpoint Security product. Occurred 6 days ago on Jan 25, 2022, at 5:00:52 PM.
- Accessing process:** Medium: chrome.exe
- Command Line:** --type=utility --field-trial-handle=159215044013251570943637622333554436646995.131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mgo-platform-channel-handle=1824/prefetch.B
- Username:** hb-c-ep07john
- User Role:** Enduser
- SHA-1:** 87C41FD0654083FBASC93A...
- Signature type:** Trusted
- Signer Name:** Google LLC
- Seen on:** 1 computer
- First Seen:** 6 days ago - Jan 25, 2022, 4:58:29 PM
- Last Executed:** 6 days ago - Jan 25, 2022, 6:24:18 PM

Below this, there's a section for ESET LiveGrid® showing reputation and popularity metrics. To the right, a process tree diagram shows the execution flow from user\nt.exe (5008) to explorer.exe (5068), then to 7zg.exe (7524), 7zg.exe (2964), and 7zg.exe (5080), which then runs chrome.exe (8092). A text box on the right states: "Process tree and detailed information about malicious code behaviour".

Behaviour Detection and Repeat Offenders

The weakest point in security is often a person sitting by the keyboard, even without any bad intentions.

ESET Inspect easily identifies these potentially weak elements by sorting the computers by number of unique alarms triggered. If a user triggers multiple alarms, it is a clear indicator their the activity should be validated.

USE CASE

In your network, you have users that are repeat offenders when it comes to malware. The same users continue to get infected time after time. Is it due to risky behaviour? Or are they being targeted more often than other users?

SOLUTION

- ✓ Easily view problem users and devices.
- ✓ Quickly complete a root cause analysis to find the source of infections.
- ✓ Remediate found infection vectors such as email, web or USB devices.

Threat Hunting and Blocking

The distinctive strength of ESET Inspect lies in its threat hunting ability to “find a needle in a haystack”.

By applying filters to data that sort based on file popularity or reputation, digital signature, behaviour and contextual information, any malicious activity can be easily identified and investigated. Setting up multiple filters allows automated threat-hunting tasks and can adjust the detection threshold to a company-specific environment.

Any malicious activity can be easily identified and investigated.

USE CASE

Your early warning system or security operations center (SOC) delivers a new threat warning. What are your next steps?

SOLUTION

- ✓ Leverage the early warning system to retrieve data on upcoming or new threats.
- ✓ Search all computers for existence of the new threat.
- ✓ Search all computers for indicators of compromise that the threat existed prior to warning.
- ✓ Block the threat from being able to infiltrate a network or execute within an organization.

Network Visibility

ESET Inspect is an open architecture solution, which means that a security team can adjust detection rules describing attack techniques to the specific environment of the organisation.

Open architecture also gives flexibility to configure ESET Inspect to detect violations of organisation policies about using specific software like torrent applications, cloud storages, Tor browsing, starting own servers and other unwanted software.

USE CASE

Some businesses are worried about applications users are running on systems. Not only do you need to worry about traditionally installed applications but also portable applications that do not actually install. How can you stay in control of them?

SOLUTION

- ✓ Easily view and filter all installed applications across devices.
- ✓ View and filter all scripts across devices.
- ✓ Easily block unauthorized scripts or applications from running.
- ✓ Remediate by notifying users about unauthorised applications and automatically uninstall.

Not only do you need to worry about traditionally installed applications, but also portable applications that do not actually install. How can you stay in control of them?

Security teams can **adjust detection rules** describing attack techniques to the specific environment of their organisation.



Context Aware Investigation and Remediation

The “maliciousness” of an activity depends on the context.

Activities performed on computers of network administrators are very different from the ones in the finance department. With proper grouping of computers, security teams can easily identify if this user is entitled to perform a specific activity on this machine. Synchronisation of ESET PROTECT endpoint groups and ESET Inspect rules provide outstanding results of contextual information.

USE CASE

Data is only as good as the context behind it. For proper decisions, you need to know what the alerts are, on what devices they are occurring and which users are triggering them.

SOLUTION

- ✓ Identify and sort all computers according to Active Directory, automatic groupings or manual groupings.
- ✓ Allow or block applications or scripts based on computer grouping.
- ✓ Allow or block applications or scripts based on user.
- ✓ Only receive notifications for certain groups.

Easy Setup and Easy Response – No Security Team Required

Even if a company has dedicated security teams, it's often difficult to quickly prioritise and decide the next steps among all the triggered alarms.

Therefore, for each triggered alarm there are proposed next steps to be performed for remediation. When ESET Inspect identifies a threat, it provides a quick response functionality. Specific files can be blocked by hash, processes can be killed and quarantined, and selected machines can be isolated or turned off remotely.

USE CASE

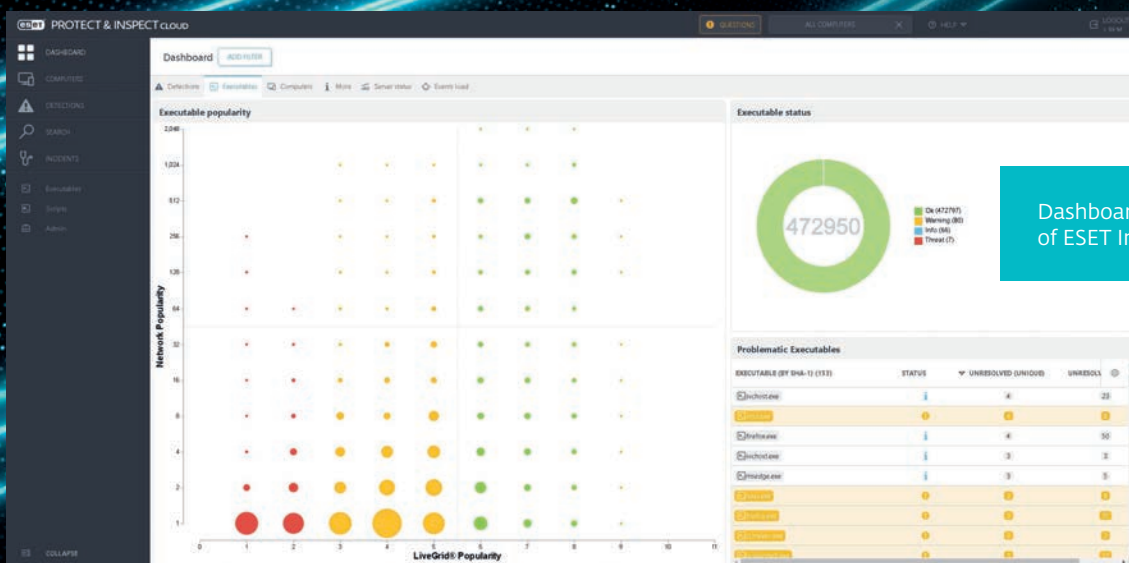
Not all businesses have dedicated security teams, and inputting and implementing advanced detection rules can be a struggle.

SOLUTION

- ✓ Over 300+ built-in preconfigured rules.
- ✓ Easily respond by simply clicking a single button to block, kill or quarantine devices.
- ✓ Proposed remediation and next steps are built into alarms.
- ✓ Rules are editable via XML language to allow easy fine-tuning or creation of new rules.

The “maliciousness” of an activity depends on the **context**. Synchronisation of ESET PROTECT endpoint groups and ESET Inspect rules provide outstanding results of contextual information.

For each triggered alarm, there are proposed next steps to be performed for remediation.



Dashboard of ESET Inspect

Solution capabilities

INCIDENT MANAGEMENT SYSTEM

Group objects such as detections, computers, executables or processes into logical units to view potential malicious events on a timeline, with related user actions. ESET Inspect automatically suggests to the incident responder all related events and objects that can greatly help in an incident's triage, investigation, and resolution stages.

LIVE RESPONSE OPTIONS

ESET Inspect comes packed with easily accessible one-click response actions such as rebooting and shutting down an endpoint, isolating endpoints from the rest of the network, running an on-demand scan, killing any running process, and blocking any application based on its hash value. Additionally, thanks to ESET Inspect's live response option, called Terminal, security professionals can benefit from the full suite of investigation and remediation options in PowerShell.

ROOT CAUSE ANALYSIS

Easily view the root cause analysis, and full process tree, of any potentially malicious chain of events, drill down to the desired level of detail and make informed decisions based on the rich provided context and explanations for both benign and malicious causes, written by our malware experts.

PUBLIC API

ESET Inspect features a Public REST API that enables the accessing and exporting of detections and their remediation to allow effective integration with tools such as SIEM, SOAR, ticketing tools and many others.

THREAT HUNTING

Use the powerful query-based IOC search and apply filters to raw data for sorting based on file popularity, reputation, digital signature, behaviour, or other contextual information. Setting up multiple filters allows automated, easy threat hunting and incident response, including the ability to detect and stop APTs and targeted attacks.

SAFE AND SMOOTH REMOTE ACCESS

Incident response and security services are only as smooth as the ease with which they are accessed – both in terms of the incident responder's connection to the console, and the connection with the endpoints. The connection works at close to real-time speed with maximum security measures applied, all without the need for third-party tools.

ONE-CLICK ISOLATION

Define network access policies to quickly stop lateral movement by malware. Isolate a compromised device from the network with just one click in the ESET Inspect interface. Also, easily remove devices from the containment state.

ANOMALY AND BEHAVIOUR DETECTION

Check actions carried out by an executable and utilize ESET's LiveGrid® Reputation system to quickly assess if executed processes are safe or suspicious. Monitoring anomalous user-related incidents is possible due to specific rules written to be triggered by behaviour, not simple malware, or signature detections. Grouping of computers by user or department allows security teams to identify if the user is entitled to perform a specific action or not.

TAGGING

Assign and unassign tags for fast filtering of objects such as computers, alarms, exclusions, tasks, executables, processes, and scripts. Tags are shared among users, and once created, can be assigned within seconds.

MULTIPLE INDICATORS OF COMPROMISE

View and block modules based on over 30 different indicators, including hash, registry modifications, file modifications and network connections.

OPEN ARCHITECTURE AND INTEGRATIONS

ESET Inspect provides unique behaviour- and reputation-based detection that is fully transparent to security teams. All rules are easily editable via XML to allow fine-tuning or easily created to match the needs of specific enterprise environments, including SIEM integrations.

COMPANY POLICY VIOLATION DETECTION

Block malicious modules from being executed on any computer in your organisation's network. ESET Inspect's open architecture offers the flexibility to detect violations of policies that apply to the use of specific software like torrent applications, cloud storage, Tor browsing or other unwanted software.

SOPHISTICATED SCORING

Prioritize the severity of alarms with a scoring functionality that attributes a severity value to incidents and allows admins to quickly identify computers with a higher probability for potential incidents.

LOCAL DATA COLLECTION

View comprehensive data about a newly executed module, including time of execution, the user who executed it, dwell time and the devices attacked. All data is stored locally to prevent sensitive data leakage.

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



protected by ESET
since 2017 more than
9,000 endpoints



protected by ESET
since 2016 more than
4,000 mailboxes



Canon Marketing Japan Group

protected by ESET
since 2016 more than
32,000 endpoints



ISP security partner
since 2008 2 million
customer base

COMMITTED TO THE HIGHEST INDUSTRY STANDARDS



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



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



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.



eset[®] Digital Security
Progress. Protected.