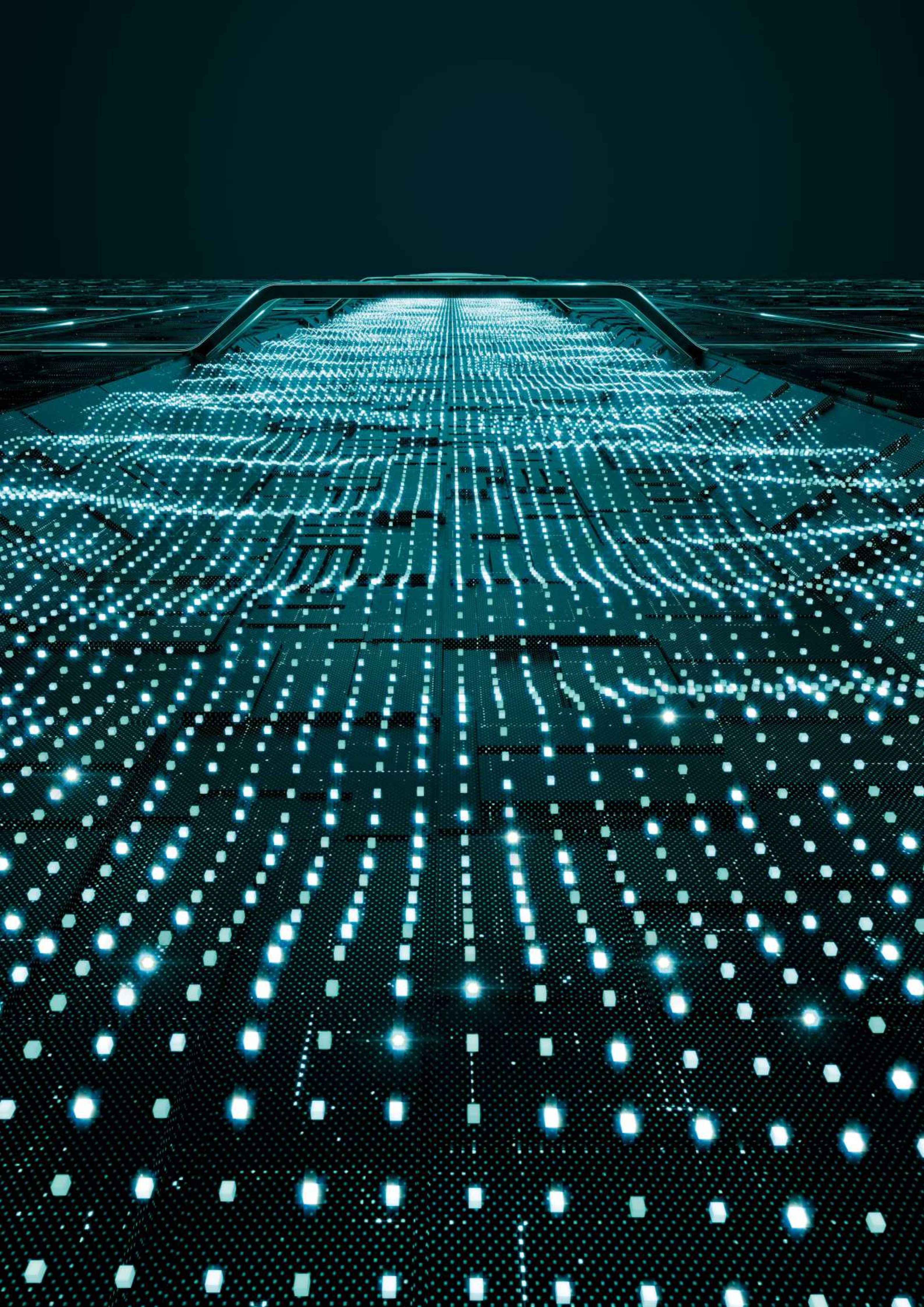
SOLUTION OVERVIEW

ENTERPRISE INSPECTOR

Ensure outstanding visibility and synchronized remediation with ESET EDR

CYBERSECURITY
EXPERTS ON YOUR SIDE



What is an **Endpoint Detection & Response solution?**

ESET Enterprise Inspector is a sophisticated EDR tool for identification of anomalous behavior and breaches, risk assessment, incident response, investigations and remediation.

It monitors and evaluates all the activities happening in the network (for example user, file, process, registry, memory and network events) in real time and allows you to take immediate action if needed.

Why **Endpoint 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, organizations need increased visibility into their computers to ensure that emerging threats, risky employee behavior 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

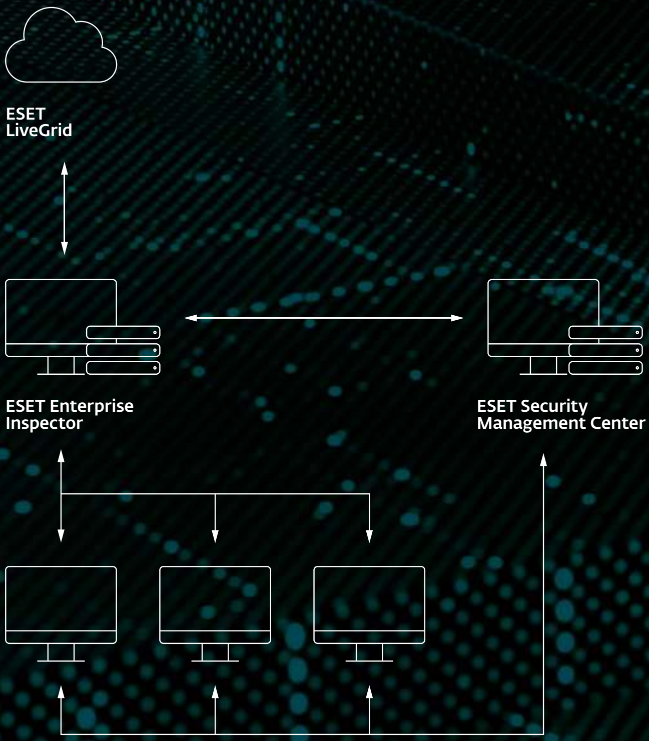
EDR systems are commonly utilized to: identify APTs or targeted attacks via Threat Hunting; reduce incident response time; and proactively prevent future attacks. Uncovering APTs in particular is important for enterprises as most businesses today don't feel prepared for the newest attacks that can be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

Provides a **unique behavior 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 ORGANIZATION 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.

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



ESET's Endpoint Protection Platform
Multilayered endpoint security where every single layer sends data to ESET Enterprise Inspector.

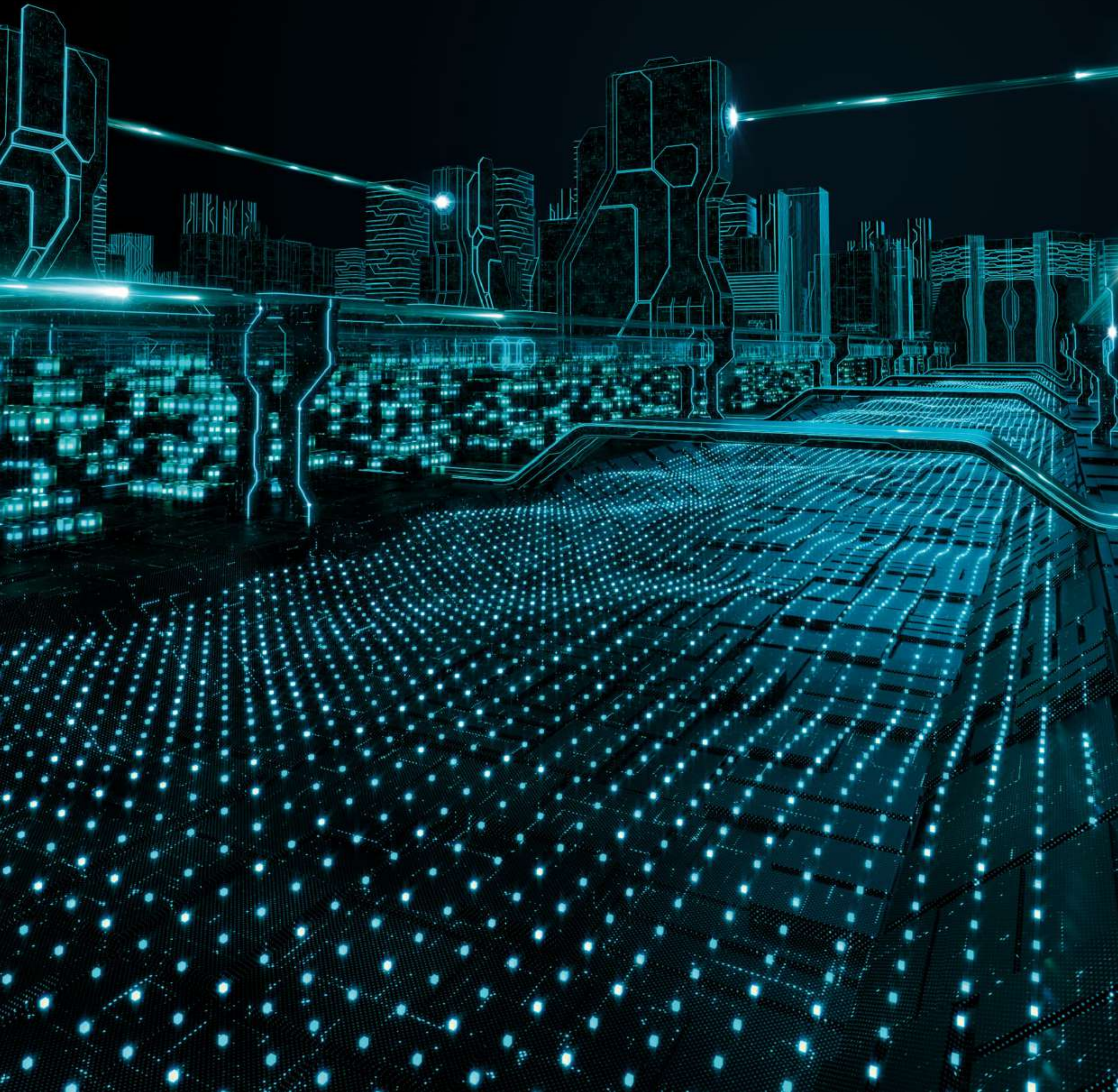
+

ESET Enterprise Inspector
Sophisticated EDR tool that analyzes vast amounts of data in real time so no threat goes undetected.

=

Complete prevention, detection and response solution that allows quick analysis and remediation of any security issue in the network.

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



Key benefits

SYNCHRONIZED RESPONSE

Built on top of existing ESET endpoint security offering, it creates a consistent ecosystem that allows cross-linking of all relevant objects and synchronized remediation of incidents. Security teams can kill processes, download the file that triggered a detection, or simply initiate a computer reboot, shutdown, scan, or isolate the device from the network directly from the console.

OPEN ARCHITECTURE

Provides a unique behavior and reputation-based detection that is fully transparent to security teams. All rules are written in a common XML format and can be easily customized and created to match the needs of specific enterprise environments, including SIEM integrations.

REMOTE ACCESS

ESET Enterprise Inspector features remote PowerShell capabilities that allow Security Engineers to remotely inspect and configure their organization's computers, so a sophisticated response can be achieved without breaking the user's workflow.

MULTIPLATFORM

ESET Enterprise Inspector supports Windows and MacOS, which makes it a perfect choice for multiplatform environments.

PUBLIC API

ESET Enterprise Inspector features an API that enables accessing and exporting of detections, and their remediation to allow effective integration with tools such as SIEM, SOAR, ticketing tools and many others.

ADJUSTABLE SENSITIVITY

Easily suppress detections by adjusting the sensitivity of rules for different computer groups or users. Combine criteria such as file name, path, hash, command line, signer, to fine-tune the trigger conditions.

MITRE ATT&CK™

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

REPUTATION SYSTEM

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

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 Enterprise Inspector 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.

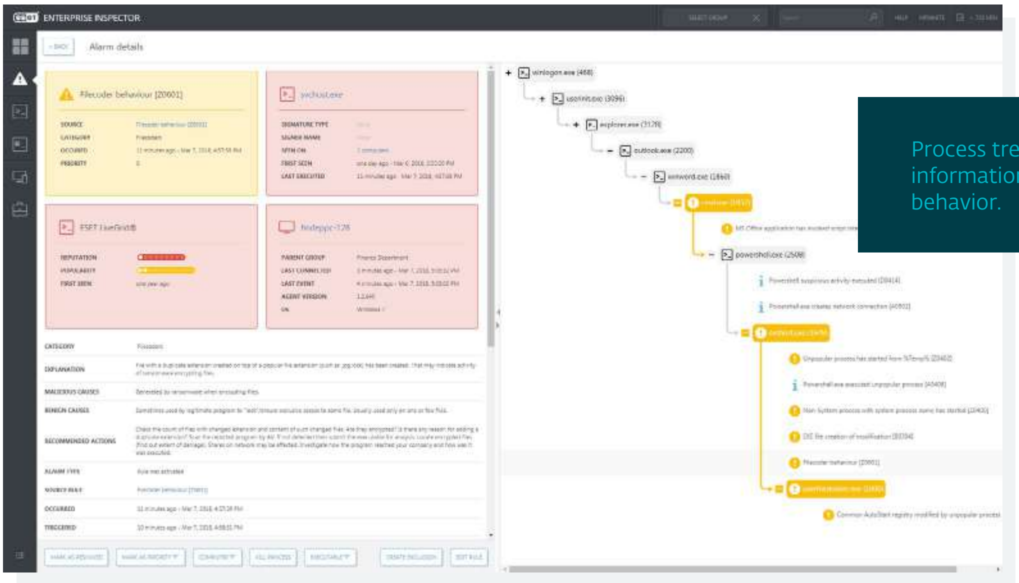
ESET Enterprise Inspector allows your security team to see alerts on this kind of behavior, and in a few clicks you can see what was affected, where and when a specific executable, script or action was performed, and analyze the cause of it "back to the root."

USE CASE

A business wants additional tools to proactively detect ransomware in addition to being notified promptly if ransomware-like behavior 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.



Process tree and detailed information of a Filecoder behavior.

Behavior Detection and Repeat Offenders

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

ESET Enterprise Inspector 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 behavior? 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 Enterprise Inspector is in threat hunting by a “finding a needle in a haystack” approach.

By applying filters to data that sort based on file popularity or reputation, digital signature, behavior 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 Enterprise Inspector is an open architecture solution, which means that a security team can adjust detection rules describing attack techniques to the specific environment of the organization.

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

USE CASE

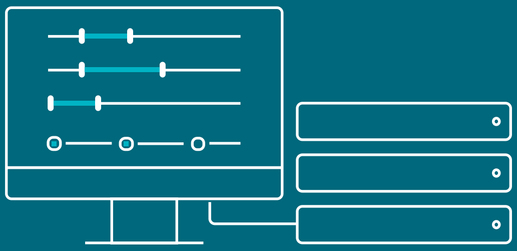
Some businesses are worried about applications users are running on systems. Not only do you need to worry about traditionally installed applications but also portable applications that do not actually install. How can you stay in control of them?

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 unauthorized 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 organization.



Context Aware Investigation and Remediation

"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. Synchronization of ESET Security Management Center endpoint groups and ESET Enterprise Inspector 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 prioritize 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 Enterprise Inspector 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

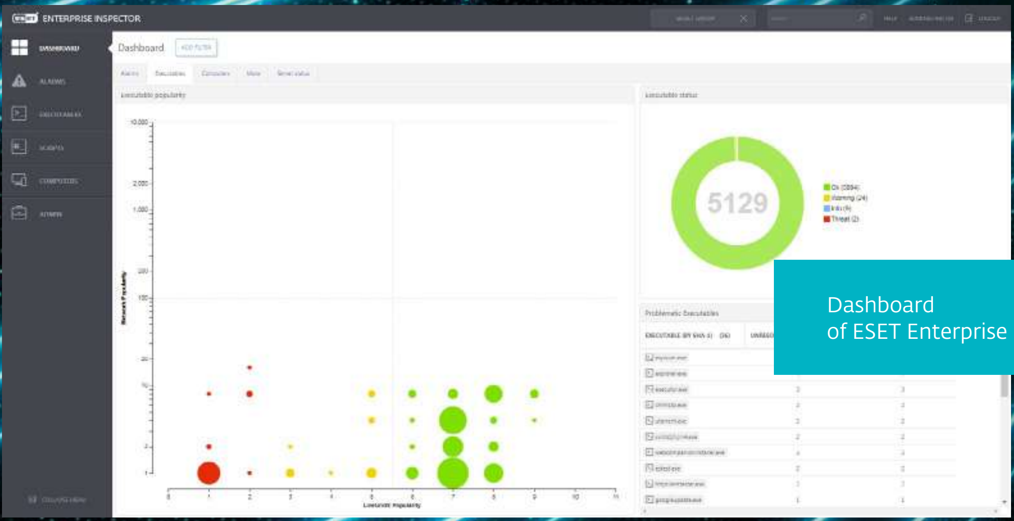
Not all businesses have dedicated security teams, and inputting and implementing advanced detection rules can be a struggle.

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.

“Maliciousness” of an activity depends on the context. Synchronization of ESET Security Management Center endpoint groups and ESET Enterprise Inspector rules provide outstanding results of contextual information.

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



Dashboard
of ESET Enterprise Inspector

Solution capabilities

THREAT HUNTING

Apply data filters to sort it based on file popularity, reputation, digital signature, behavior or contextual information. Setting up multiple filters allows automated easy threat hunting, including APTs and targeted attacks which is customizable to each company's environment. By adjusting behavior rules, ESET Enterprise Inspector can be customized also for Historic Threat Hunting and "rescan" the entire events database.

INCIDENT DETECTION (ROOT CAUSE ANALYSIS)

Quickly and easily view all security incidents in the detections section. With a few clicks, security teams can see a full root cause analysis, including what was affected, where, and when the executable script, or action was performed.

INVESTIGATION AND REMEDIATION

Use a built-in set of rules and create your own rules to respond to detected incidents. Each triggered detection features a proposed next step to be performed for remediation. Quick response functionality enables specific files to be blocked by hash, processes to be killed and quarantined, and selected machines to be isolated or turned off remotely. This quick response functionality helps to ensure that any single incident will not fall through the cracks.

ONE-CLICK ISOLATION

Define network access policies to quickly stop malware's lateral movements. Isolate a compromised device from the network by just one click in the EEI interface. Also, easily remove the devices from the containment state.

SCORING

Prioritize the severity of alarms with scoring functionality that attributes a severity value to incidents and allows the admin to easily identify computers with a higher probability of a potential incident.

TAGGING

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

DATA COLLECTION

View comprehensive data about a newly executed process, including time of execution, user who executed it, dwell time and affected devices.

SECURE LOG-IN

Enable two-factor authentication - an extra layer of security for your administrator account to prevent an adversary from logging in, even if they have your password.

INDICATORS OF COMPROMISE DETECTION

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

ANOMALY AND BEHAVIOR DETECTION

Check actions that were 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 are possible due to specific rules written to be triggered by behavior, 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.

COMPANY POLICY VIOLATION DETECTION

Block malicious modules from being executed in your network. Detect violations of policies about using specific software like torrent applications, cloud storages, Tor browsing or other unwanted software.

About ESET

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+	400k+	200+	13
users worldwide	business customers	countries & territories	global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017
more than 14,000 endpoints

Canon
Canon Marketing Japan Group

protected by ESET since 2016
more than 9.000 endpoints

Allianz
Suisse

protected by ESET since 2016
more than 4,000 mailboxes

T · ·

ISP security partner since 2008
2 million customer base

ESET is compliant with ISO/IEC 27001:2013, an internationally recognized and applicable security standard in implementing and managing information security. The certification is granted by the third-party accredited certification body SGS and demonstrates ESET's full compliance with industry-leading best practices.

ESET is a dedicated contributor to MITRE ATT&CK. By being one of the most referenced vendors and active contributors, ESET confirms its commitment to provide the best protection to the community and our customers.

ESET RECOGNITIONS

AV
comparatives
Certified
EPR 2020
Strategic Leader

SE Labs
AAA
JAN-MAR 2021
ENTERPRISE ENDPOINT PROTECTION

AV TEST
av-test.org
04/2021
APPROVED
CORPORATE
ENDPOINT
PROTECTION
WINDOWS
TOP PRODUCT

G2
Leader
SUMMER
2021

Gartner
peerinsights
customers' choice
2019
™

canalys
CYBERSECURITY
CHAMPION
2021

ANALYST VOICES

Gartner

ESET was named the only Challenger in 2019 Gartner Magic Quadrant for Endpoint Protection Platforms, for the second year running.

FORRESTER®

ESET was included in the **Now Tech: Enterprise Detection And Response, Q1 2020 report** - Forrester's overview of 29 enterprise Detection and Response solutions.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET retains its 'Top Player' status in **Radicati's 2021 APT Protection Market Quadrant report**.

Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, August 20, 2019. 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.

Gartner Peer Insights is a free peer review and ratings platform designed for enterprise software and services decision makers. Reviews go through a strict validation and moderation process to ensure information is authentic. Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

CYBERSECURITY
EXPERTS ON YOUR SIDE