OVERVIEW

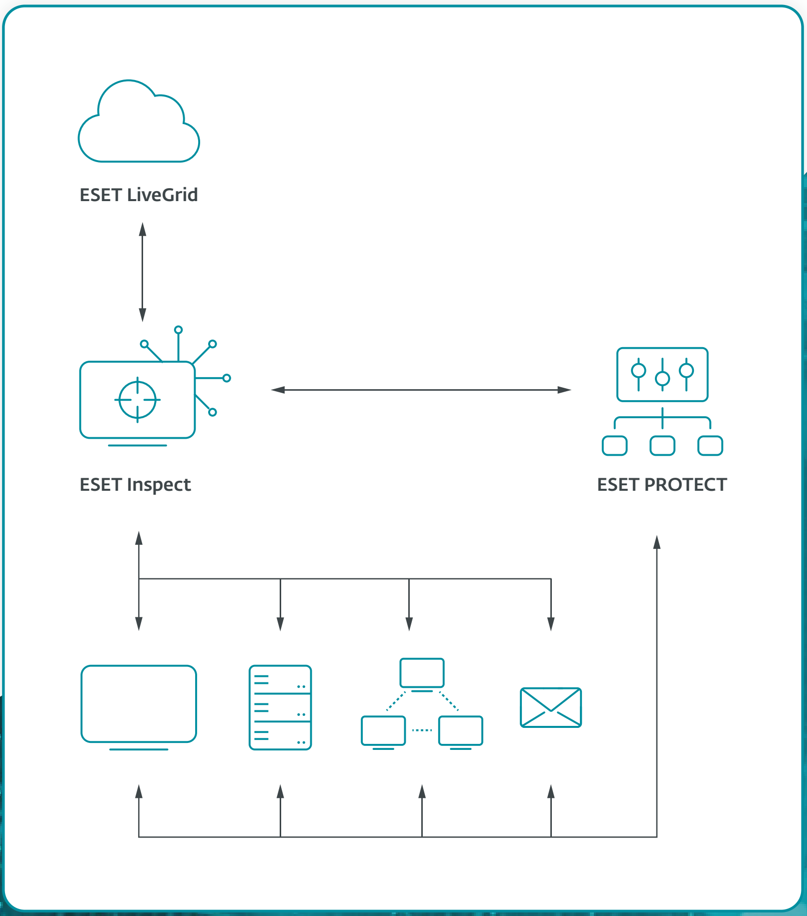
# ESET INSPECT

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

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

**ESET Inspect, the XDR-enabling component of the ESET PROTECT Platform, is a tool for identifying anomalous behavior 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. It also helps automate immediate remedial actions, if needed. ESET's 800+ (and counting) detection rules enable comprehensive threat hunting.



# 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, analyzes 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.

### 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.

### 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.

### 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 CUSTOMIZATION

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 organization's environment and suggest exclusions to false positives, where needed.

# Solution capabilities

## INCIDENT MANAGEMENT SYSTEM

Group objects such as detections, computers, executables or processes into logical units to view potentially 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 processes, 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.

## MULTIPLE INDICATORS OF COMPROMISE

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

## THREAT HUNTING

Use the powerful query-based IoC search and apply filters to raw data for sorting based on file popularity, reputation, digital signature, behavior, 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

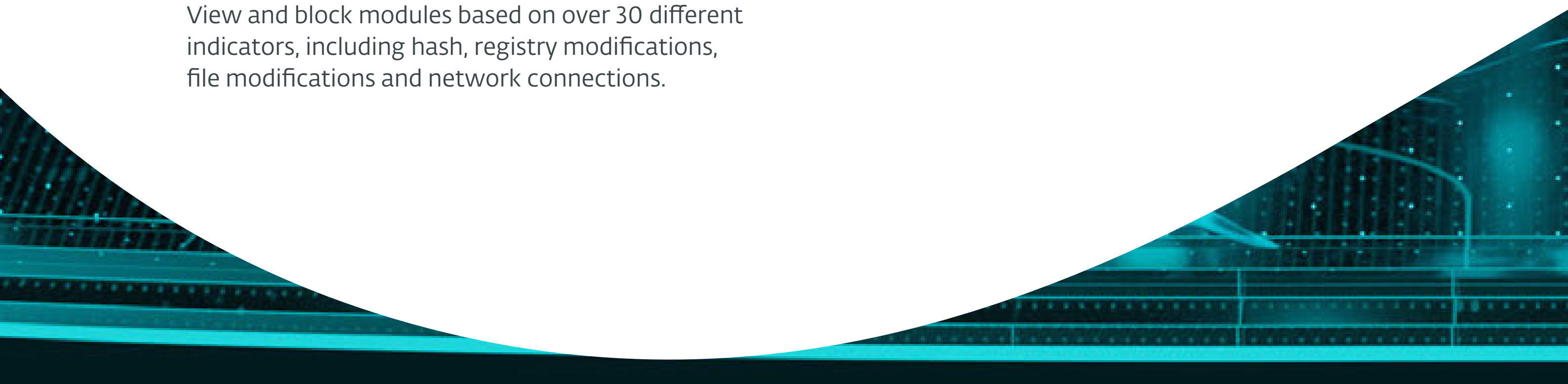
Incident response and security services are only as smooth as the ease with which they are accessed—both in terms of the incident responder's connection to the console, and the connection with the endpoints. The connection works at close to real-time speed with maximum security measures applied, all 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 BEHAVIOR 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 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.



## 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.

## COMPANY POLICY VIOLATION DETECTION

Block malicious modules from being executed on any computer in your organization'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.

## OPEN ARCHITECTURE AND INTEGRATIONS

ESET Inspect provides unique behavior 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.

## 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.

# Use Cases

## Behavior Detection and Repeat Offenders

### PROBLEM

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.

## Easy Setup and Easy Response—No Security Team Required

### PROBLEM

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.

## Threat Hunting and Blocking

### PROBLEM

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

### PROBLEM

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.

# In-Depth Threat Detection—Ransomware

### PROBLEM

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

# Context Aware Investigation and Remediation

### PROBLEM

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.

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+ | 400k+ | 195 | 13 |
|---|---|---|---|
| protected internet users | business customers | countries and territories | 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

MITRE ATT&CK™

ESET is one of the top referenced and engaged vendors directly involved in the refinement and population of the MITRE ATT&CK knowledge base.

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