KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert

February 13, 2020

ESET Enterprise Inspector

Enterprise Inspector is ESET's Endpoint Detection & Response (EDR) solution. It currently runs on Windows and MacOS. ESET Enterprise Inspector collects and analyzes information to help security analysts determine if malicious activities have occurred. The solution also allows for pre-configured remediation actions to be executed when certain conditions are met.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

Endpoint Detection & Response (EDR) solutions have become increasingly popular in just the last few years as a means to help security analysts determine if other security mechanisms have failed, if their systems have been attacked and compromised, and if valuable data has been exfiltrated. Surveys show that 11% of cybersecurity breaches are targeted attacks, and 13% are acts of corporate espionage, designed to steal state or trade secrets. Malware and account takeovers are involved in 48% and 14% of attacks respectively. Almost every industry and every level of government agency are under attack. Organizations are justified in looking for additional security tools to discover and thwart such attempts. A main goal of EDR is often reducing the Mean Time To Respond (MTTR), given that many reports show that attackers can spend months inside organizations before being detected.

EDR solutions look for evidence and effects of malware or other malicious activities that may have slipped past Endpoint Protection (EPP) products and other security tools, such as email/web gateways. Security professionals refer to such data points as Indicators of Compromise (IOCs). Examples of IOC types include:

- MD5 file hashes
- Known bad IPs and URLs
- File/process name mismatches
- Unusual application and network port usage
- Unusual process injections
- Module load point modifications
- Registry changes

EDR solutions log activities centrally, allow administrators to examine endpoints remotely, and generate reports often complete with attribution theories and confidence levels. Key features of endpoint protection products include:

- Host-based agents for detecting malware infection, command and control (C2) traffic, reconnaissance and lateral movement of bad actors, and data exfiltration attempts. Additionally, as part of the detection process, EDR tools can also perform evaluation of threat intelligence information, event correlation, interactive querying, live memory analysis, and activity recording and playback. Using Machine Learning (ML) and Deep Learning (DL) algorithms can help produce normal baselines and reduce false positives.
- Management console for collecting and analyzing information from deployed agents, producing alerts, and facilitating incident response, threat hunting, and forensic investigations.

- Automatic responses can be configured on consoles and executed by agents. Responses can include actions such as termination of processes, file removal, quarantine, memory analysis, forensic evidence collection, and full endpoint restoration.
- Interface to Security Intelligence systems such as SIEM.

EDR solutions can provide additional insights into possible nefarious activities in your enterprise and can serve as a complement to other security tools. EDR is not a substitute for EPP, but rather a component of many modern security architectures, alongside EPP, email/web gateways, Network Threat Detection & Response (NTDR), and even Distributed Threat Deception tools.

EDR solutions require a special set of skills to not only implement and run but also from which to derive value. The inclusion of ML technology does not obviate the need for trained security analysts. Most organizations that successfully deploy EDR have a well-defined IT security organization and one or more SOCs (Security Operations Centers), staffed by knowledgeable security analysts. Such organizations would be categorized as at least Level 1 or 2 in the Hunting Maturity Model.

ESET is headquartered in Bratislava, Slovakia, with many offices and customers around the globe. The company formed more than 30 years ago, and currently serves 110 million users in 200 countries. ESET also publishes industry-leading cybersecurity research and was the first anti-malware vendor to discover LoJax and remediate UEFI malware in 2016. The company has won many awards from independent testers over the years.

2 Product Description

Enterprise Inspector is ESET's EDR product. Agents are available for Windows 10, 8, 7; Windows Server 2019, 2016, 2012, 2008R2; and MacOS X. Linux support is on their roadmap. All nodes in a customer organization can be managed via their browser-accessible enterprise console which can be deployed on customer premises or in IaaS. The product is licensed by node, with monthly or annual subscriptions available.

All Enterprise Inspector agents in a given organization send logs to on-premises repositories, where events are analyzed and stored for one month by default.
Enterprise Inspector can continue working when client machines are not connected to the internet, but the detection rate is generally improved and false positives are reduced when agents can access ESET's cloud-based reputation system LiveGrid®.

ESET Endpoint security agent uses multiple Machine Learning (ML) techniques and pre-configured rules to detect anomalous behavior aiding in creating more aggressive detection rulesets of ESET Enterprise Inspector. EEI relies on powerful sensors on endpoints which provides administrators with deep information on what is happening on the endpoints (even if the activity is supposed to be hidden).

Security Engineers (SEs) thus have access not only to the data that ESET's EEI evaluated as relevant to the case, but to all event data from the organizations' endpoints. Data acquired on an endpoint is stored on the server, so even if the endpoint is encrypted or destroyed during the attack, SEs have full visibility into what was happening during the attack until the point of destruction. SEs can also request additional data from a computer suspected of compromise, where a snapshot of relevant security configuration data is compiled and sent to the server. The data received from endpoints is automatically enriched with the data from ESET's global LiveGrid® (cloud-based reputation system) adding information about reputation, popularity, age of the file, etc. There is also similar data available computed specifically just for the current enterprise, so filters such as "seen on just one computer in the enterprise" or "first seen today in the enterprise" are easily applicable. ESET pulls this information from its own data stores as well as 3rd-parties such as Opswat, PhishLabs, Virus Total, etc. ESET publishes its threat intelligence discoveries for the benefit of the community using standard protocols including STIX and TAXII. ESET Enterprise Inspector looks for a variety of different high-level activities to detect directed attacks, lateral movement by APT-type actors, address spoofing, privilege escalation, abnormal process execution and injection, abnormal DLL usage, abnormal file access, client agent tampering, registry changes, remote PowerShell script execution, remote network connections with attempts to execute code, and data exfiltration attempts.

Enterprise Inspector can also generate attribution theories with confidence levels. Customers have flexibility in creating rules for detection thresholds and alerting. Customers can also filter out certain conditions that may occur so as to reduce false positives. Customers can design rules for assignment of attributes and also edit event attributes during investigations.

ESET offers customers guidance on putting together playbooks. Automated response actions can include network isolation of suspect nodes, process termination, moving/deleting files, and running scripts. An example of a default automatic response is that when malware is detected on a node, that node is blocked from communicating with any node other than the security console. Enterprise Inspector does not perform automatic rollback to last known good state.

Nearly 1,700 preconfigured reports are available in the ESET Security Management Center (ESMC), and customer admins can customize additional reports. ESET also has an enterprise dashboard for customers which shows process trees and other relevant information, including cyber threat intelligence related to the event in question.

Many organizations are using EDR solutions for threat hunting. Interactive live querying across multiple nodes in an organization, inventory collection, and live memory analysis are available to administrative users of ESMC. Natural language querying is not supported due to the perceived inaccuracies in results. Full file, process, and network correlation analysis can be performed from the console in an investigation. ESET SysInspector takes periodic snapshots capturing key registry entries, system configuration, and hardware/software inventories for ongoing comparisons. SysInspector can be triggered remotely from ESMC. ESET Enterprise Inspector performs system file integrity monitoring. ESET can coordinate with desktop configuration tools such as Microsoft SCCM or RedHat Satellite to allow approved updates of system files without setting off false alarms.

Event recording/playback functions are possible to assist in forensic investigations. Customers can use Enterprise Inspector to look at the Master File Tables (MFTs) on devices, and ESET is the only vendor that supports UEFI scanning.

ESET can interoperate with 3rd-party SIEM solutions via connectors for IBM QRadar and Splunk, and it can send data as syslog. Interoperation with SOAR products is possible over APIs. ESET does not currently interoperate with other vendor's Unified Endpoint Management, IT Ticketing, or change management solutions.

ESET EEI supports 2FA for administrators. Customers could also protect the console with Microsoft AD credentials and associated authentication methods. Federated access using SAML is not supported. ESET agents require local administrative accounts to install and run but can work in conjunction with Privileged Access Management (PAM) solutions.

ESET's Enterprise Inspector works in conjunction with their EPP product, Endpoint Security ESET instantiates EDR and EPP into two distinct agents.

ESET is part of the App Defense Alliance, along with Google, Lookout, and Zimperium. The App Defense Alliance works to secure mobile apps on Google Play store. ESET is a contributor to and has published research on MITRE ATT&CK™, and includes analysis in accordance with MITRE ATT&CK™ within their enterprise administrative consoles.

3 Strengths and Challenges

ESET Enterprise Inspector contains nearly all the features that customers are looking for in an EDR solution. ESET makes good use of multiple sophisticated ML algorithms to discover evidence of malicious behavior across all nodes in an enterprise. The ability to perform live querying is a benefit to threat hunters. Their support for UEFI and MFT scanning is a competitive differentiator in this market. Activity recording/playback is also a feature that ESET has that not all EDR products support yet.

Enterprise Inspector allows for all the most common playbook actions to be automatically executed. Automatic quarantining for malware-infected systems can help prevent the spread of malware, especially ransomware. ESET also offers guidance to their customers when setting up their playbooks.

ESET has a global support organization. ESET's products are continually enhanced by information from their threat intelligence and research teams around the globe.
We recommend adding support for SAML federation for administrative users of the cloud-based enterprise console.

Strengths

- Scoring system for behavioral rules & detailed auditing functionality for admins
- Excellent implementation of multiple, advanced ML algorithms for discovering malicious activity patterns
- Support for most commonly used and requested automatic response options
- UEFI and MFT scanning helps find rootkits that other solutions may miss (ESET Endpoint Security)
- Integration with PAM tools

Challenges

- No interoperability with IT Ticketing, Change Management, or Unified Endpoint Management solutions
- Does not support SAML for admin access to management console
- More advanced MFA for console coming in 2020

4 Related Research

Leadership Brief: The Differences Between Endpoint Protection (EPP) and Endpoint Detection (EDR) - 80186
Leadership Brief: Do I Need Endpoint Detection & Response (EDR) - 80187
Leadership Compass: Enterprise Endpoint Security: Anti-Malware Solutions - 71172

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.