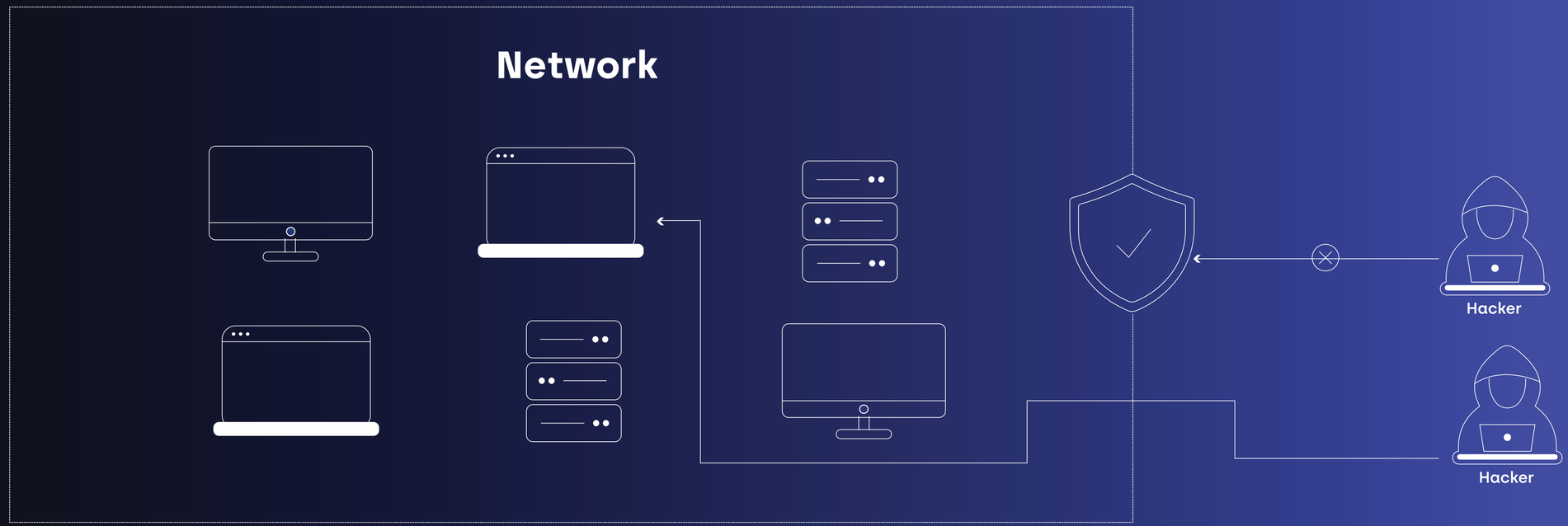
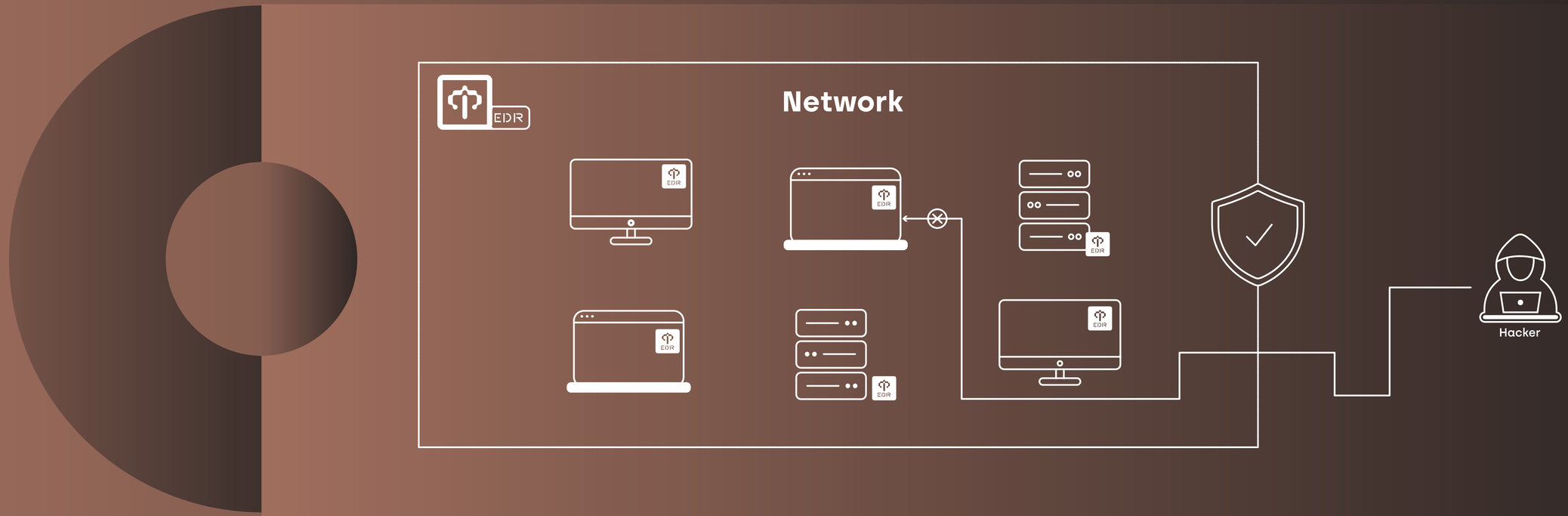

ENDPOINT DETECTION & RESPONSE
EDR

Endpoint Detection and Response 
system, abbreviated as **EDR**, is a system that uses machine learning and activity monitoring to identify attacks and behaviors that lead to threats.

Ransomware attacks and new attacks known as APT have transformed the cyber security perspective of organizations. However, an organization’s most critical and sensitive data and systems are stored on servers and are well-guarded inside data centers using security tools like firewalls, etc. According to the American company “IDC”, nearly 70% of successful security penetrations that resulted in information leakage or disruption started from endpoints. In recent years, remote work has increased significantly with the development of Internet communication infrastructure, especially after the Corona pandemic. All this has caused the boundary of organizations’ computer networks to go beyond a building or a city geographically. For this reason, endpoint security has become more complicated and, at the same time, more critical than in the past. On the other hand, older defense tools such as antiviruses and other EPP products that use signature-based detection and prevention methods cannot prevent these attacks by themselves. These tools are necessary for any organization and prevent a high percentage of attacks. Still, in the face of APT attacks, Fileless attacks, advanced ransomware, and phishing attacks, they do not have the required efficiency.

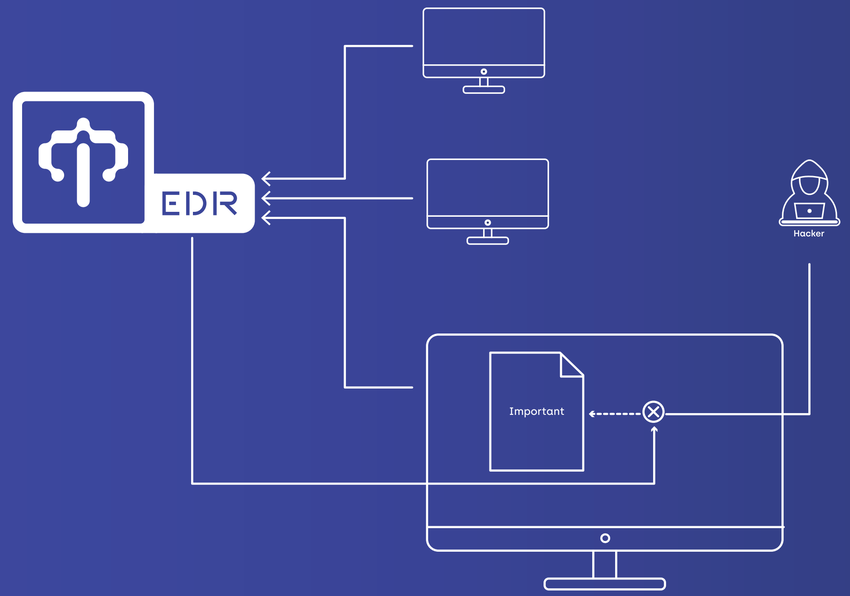
The EDR system collects and deeply investigates system events using data analysis techniques. In addition to providing a comprehensive view of network events to the organization’s security managers, by using behavioral analysis methods, it detects and reports malicious behaviors and is significantly effective in reducing the time to discover, investigate and respond to attacks.




EDR
Network
EDR
EDR
EDR
EDR
EDR
Hacker

Endpoint Detection and Response system (EDR)

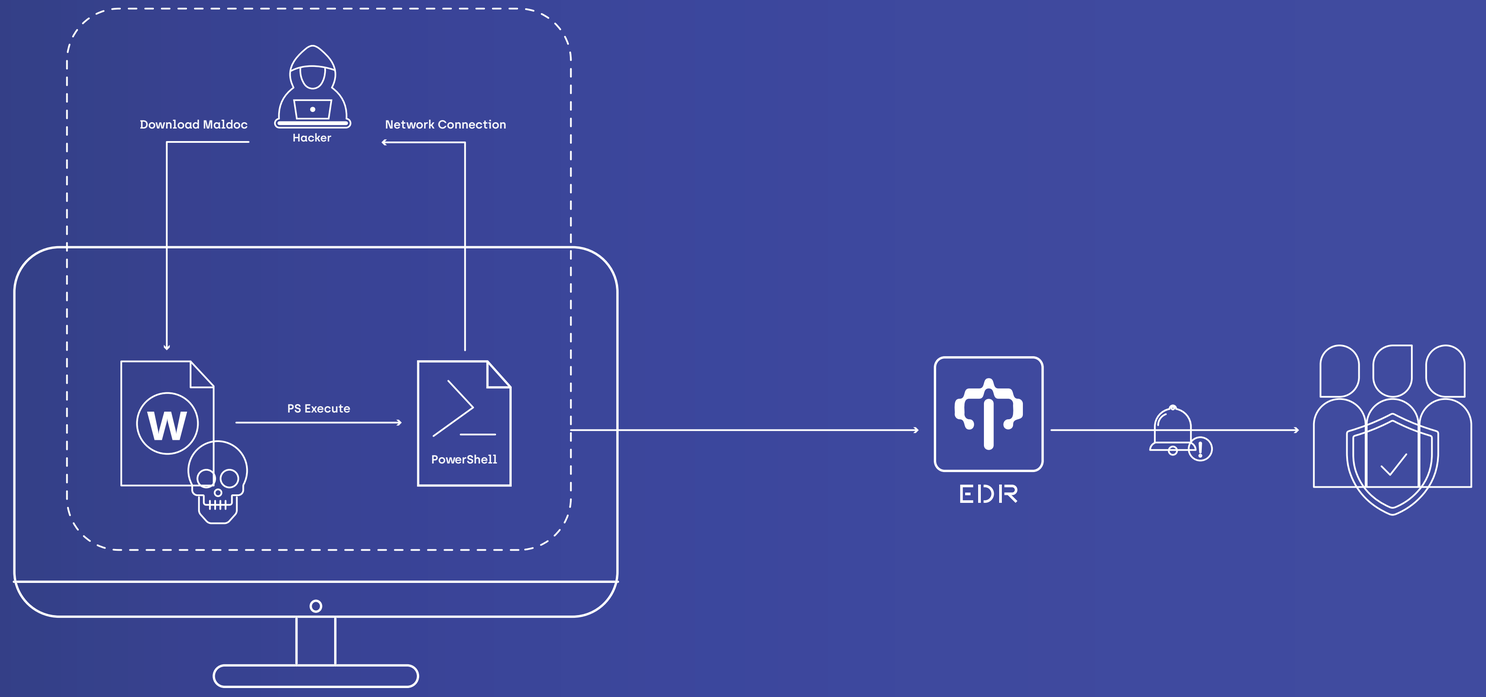
The EDR system collects and analyzes the system behaviors of all network endpoints. In addition to giving the user a comprehensive view of all system events, it looks for malicious and infected processes with data analysis techniques.



EDR system behavioral detection engine

New generations of attacks and malware can easily bypass old tools like AV. AV analysis method, which is mainly based on signature analysis, distinguishes between malicious and non-malicious files by finding malicious codes. Before sending the malware to their targets, most organized attackers use several methods to ensure that different antiviruses do not detect it. In addition, newer malware uses the current tools and infrastructure of the operating system, so it is impossible to see whether these files are malicious by detecting the signature.

In the behavioral diagnosis approach, an approach is not necessarily destructive on its own, but the sequence of a set of behaviors is destructive. By modeling the system-level behaviors of all network computers, the EDR system behavior analysis engine first ensures that all model system behaviors are saved. And in the second stage, by modeling the behavior of malware and attackers, it identifies and reports malicious behavior.


Download Maldoc
Hacker
Network Connection
PS Execute
PowerShell
EDR

The difference between EDR and other EPP products like antivirus

EPP products, such as antivirus, have similar goals to EDR systems but cover different needs. By detecting malicious files and actions with signature-based approaches, EPP products prevent malicious behavior and maintain system security by preventing malicious files from executing. On the other hand, EDR systems hunt cyber threats with the behavior analysis approach assuming an attacker's presence in the network. The EDR systems approach is complementary to the EPP products approach. EPPs are the organization's first line of defense against attacks, and EDR is the organization's second layer of protection. EDR's behavioral analysis approach detects attacks that cannot be detected by the previous generation of EPPs, and EDR provides the security analyst with the capabilities to hunt these threats.
An effective defensive security strategy in an organization uses the EPP prevention approach and the EDR detection and hunting approach simultaneously.

Differences between EDR and SIEM

Despite the many similarities between these two products in some aspects, they have two main differences in the place of use and function:

Differences in detecting attacks:

EDR systems focus on endpoint attacks, which are the new targets of organized attacks, in addition to significantly increasing the accuracy of detecting attacks; on the other hand, it reduces the number of false positive alerts and the cost of the organization's cyber security operations. EDR systems' capabilities in endpoint data analysis (such as events related to system processes) are far beyond the capabilities of SIEM systems. And it is considered a more robust defense tool than SIEMs against attacks at the endpoint level.

Differences in attack response capability:

SIEM systems do not inherently have the capabilities to respond to attacks and rely on other products, such as SOAR, to respond. But EDR systems in the first stage prevent the spread of current attacks and reduce the area under the attack with various capabilities to limit the attack. And in the second stage, providing in-depth investigation tools helps the security analyst identify the starting point and root of the attack and supports the organization's security team to prevent the attack from happening again. Ultimately, the optimal strategy is to let EDR identify threats on the endpoint and send the logs of EDR systems to the SIEM for aggregation.

EDR is suitable for which businesses?

Protecting data and preventing intrusion into an organization’s internal network requires more care and monitoring than at the current level. Therefore, EDR service is recommended for all companies, public and private departments, and organizations that are looking for the following:

- Identifying and eliminating access points and attacks to the internal network
- Constant security monitoring at endpoints
- Preventing attacks and possible threats that can lead to data leaks or data loss

Spara’s EDR product has been produced as one of the most important products used in the security industry to increase security at the endpoints. The Spara EDR system is considered a successful domestic example of modern technology. Many government and institutional clients have trusted Spara’s EDR system, and the Spara team has successfully met the needs of these organizations in the field of endpoint security.

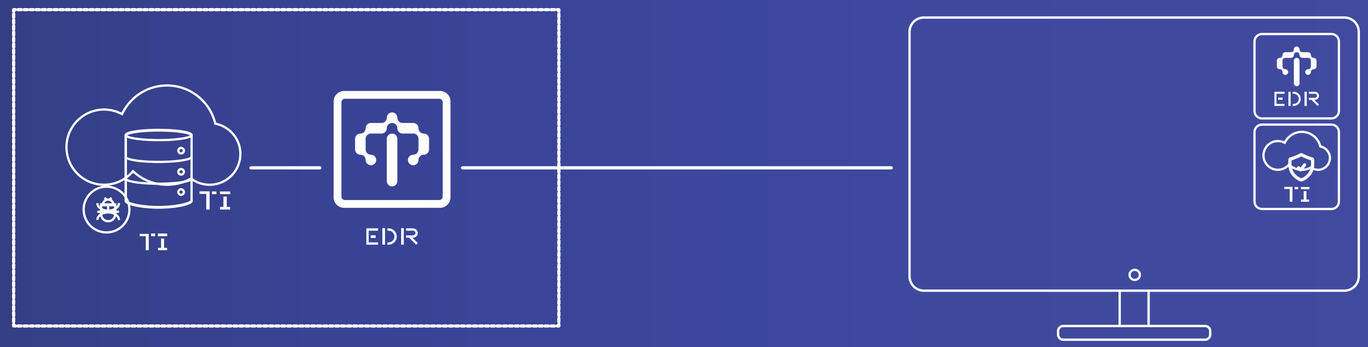
Benefits of Spara’s EDR

One of the specific points of Spara’s EDR product from other similar products is the technical knowledge of the Spara team in implementing penetration tests and simulating attacks which have caused the existing requirements and gaps to be covered with more sensitivity and attention in the design of the EDR system and finally, this system has high accuracy and speed compared to similar products.

- Service installation without reboot and downtime
- High-accuracy threat detection and alert generation with minimum false positive
- Threat detection using behavioral analytics instead of signature-based
- Providing a comprehensive view of all end-points activities
- Increasing the speed of threat analysis
- Using a database of attacks and processed data to prevent attacks
- Increasing the speed of responding to attacks
- Improving threat hunting by providing contextual data on attacks

Threat intelligence system

Threat intelligence systems, also known as “TI”, are cloud-based infrastructures consisting of pre-processed data from recent attacks and current threats worldwide. This data helps the EDR systems to gain knowledge and data about the latest attacks in the world and to have methods to counter them. Using the TI system along with the EDR system doubles the protection capabilities.



Required resources

The EDR system agent currently supports Win7 SP1 and higher operating systems. If the organization wants to use the on-premise version of the product, it must prepare a virtual machine with the following features:
Minimum System Requirements:
CPU: 8 Core
RAM: 32 GB
Storage: 1TB SSD (3 months)
These features are suitable for about 5K EPS (targeted for about 1000 clients).

Recommended System Requirements
CPU: 16 Core
RAM: 128 GB
Storage: 3TB SSD (3 months)
These features are suitable for about 15K EPS (targeted for about 5000 clients).
Naturally, more hardware resources are required for more clients. This amount of resources is a rough estimate, and the exact amount of hardware resources needed is obtained by checking the client's site and evaluating its requirements.

Setup and Installation

1-Server installation

The EDR server is a containerized app that can be set up using docker. Spara has its docker registry in Iran, which does not have the usual restriction (imposed by sanctions) other dockerized apps have. It is also possible to update the server anytime by downloading the latest docker image version. To set up this service in general, you need a domain name to connect. The initial setup, configuration, and turning of the detection engine for the first time are done by the Spara team.

2- Client (Agent) installation on endpoints

To install the EDR agent on all computers, we provide the customer with an MSI installation file. This file can be installed and set up through the network management tools used by the organization. Remote deployment is also possible using the username and password of the destination computer by the Spara support team’s deployment tools.

About Spara

Today cyber risks are a critical threat to all organizations worldwide. In the past, organizations tried to provide their cyber security only by using the security equipment and software available in the market. But today, cyberattacks have a very complex structure, so it is no longer possible to deal with them using traditional methods. Therefore, to deal with advanced cyber threats, organizations need to use advanced detection and prevention systems to identify them in the shortest possible time in case of cyber penetration.

In this regard, “Spara” company and a group of the best cyber security experts in the country have produced new products, diverse services, and comprehensive cyber security solutions. “PAM”, “EMS” and “EDR” are the most important products of Spara. Spara’s security services and solutions also include a wide range of security services such as “Security Operations Center”, “Penetration Test”, “Threat Hunting”, “Red Team”, “Governance, Risk Management, and Compliance”, “Incident Response”, “Consulting” and “Training”.

We have been trusted by:

+98(0)21-22275003

info@spara.ir

www.spara.ir