NP AV

Net Protector - Endpoint Security

Endpoint Detection & Response (EDR)

BLOCKS ADVANCED SECURITY THREATS

www.adminconsole.net

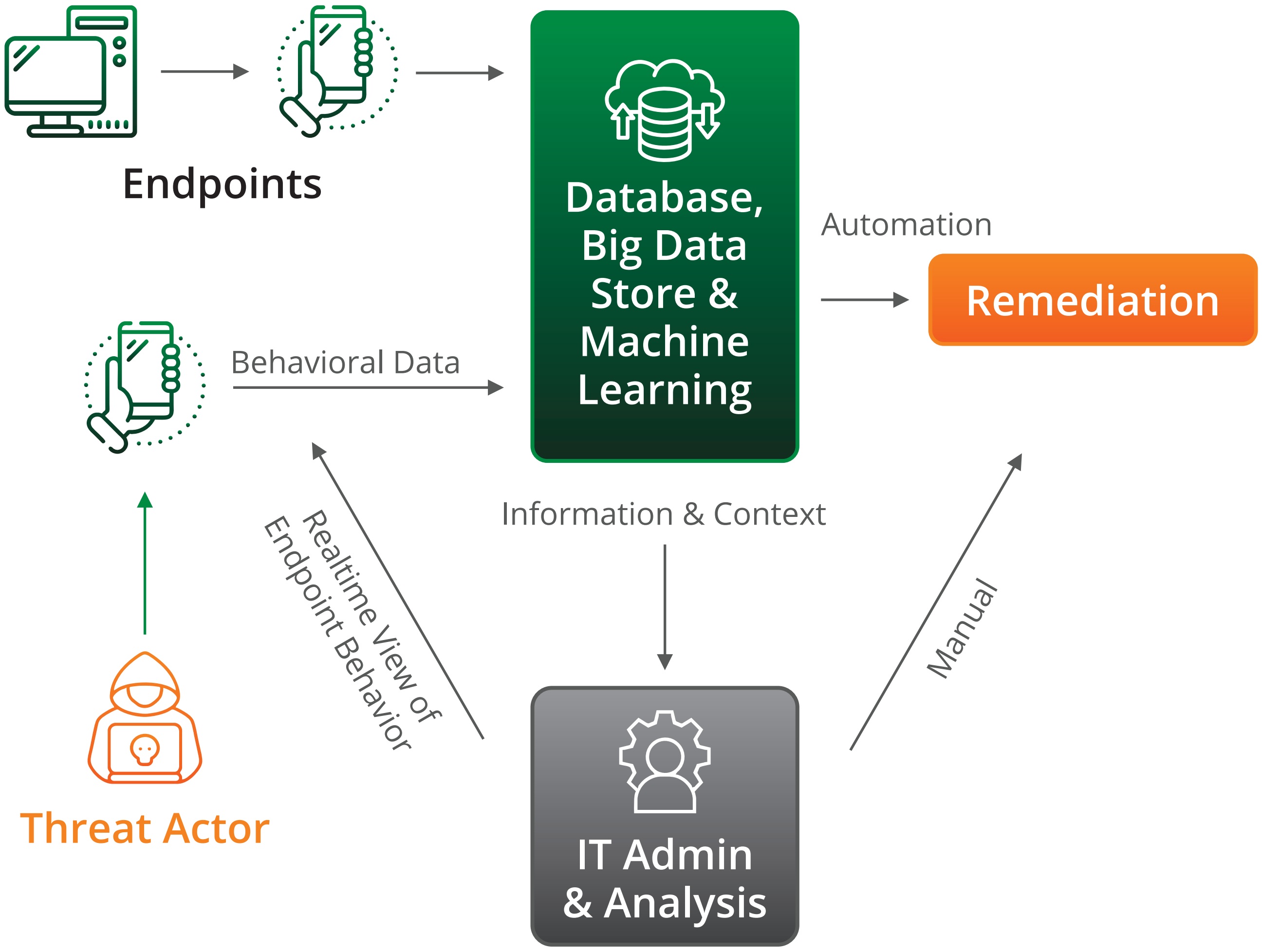
What is NPAV Endpoint Detection & Response (EDR)?

NPAV EDR solution designed to safeguard computer endpoints, such as workstations, servers, laptops, and mobile devices, from a wide range of threats, including malware, ransomware, advanced persistent threats (APTs), and other cyber attacks.

EDR solutions are an essential component of modern cyber security strategies and are used to enhance an organization's ability to detect, respond to, and mitigate security incidents.

EDR platforms help security teams find suspicious endpoint activity to eliminate threats before it can spread and minimize the impact of an attack. It is a part of an endpoint protection platform (EPP), which includes advanced antivirus and anti-malware protection.

How works NPAV Endpoint Detection & Response (EDR)



Key Features of Endpoint Detection & Response (EDR)

Real-Time and Historical Visibility

NPAV EDR provides both real-time and historical visibility into the activities happening on endpoints. Real-time visibility allows organizations to monitor and respond to security events as they occur, while historical visibility enables them to review past incidents and actions for analysis and investigation.

Incident Detection

The solution is designed to identify and catch security incidents that may have evaded prevention measures. This is crucial because no security solution is 100% foolproof, and threats can sometimes bypass initial prevention mechanisms.

Real-Time Recorder

NPAV EDR includes a real-time recorder on the endpoint. This recorder captures and logs activities in real-time, which is essential for detecting and responding to security incidents as they happen.

Complete Visibility

NPAV EDR offers customers complete visibility into each activity occurring on their endpoints from a security perspective. This means that organizations can closely monitor what is happening on their systems and networks to identify suspicious or malicious behavior.

Command Terminal

Security teams can access command terminals with command line prompts and Power shell on endpoints, enabling fast response and manual intervention when needed.

Monitoring Security Events

→ **New process creation**

Detecting when new programs or processes are initiated on an endpoint with details of parent process and child processes.

→ **New file creation**

Keeping an eye on the creation of new files, which can be an indicator of malicious activity.

→ **Unknown running processes and loaded drivers**

Identifying processes and drivers that are not recognized or authorized, potentially indicating a security threat.

→ **Integrity monitoring**

Ensuring that critical system files and configurations remain unchanged, as any unauthorized changes could signify an attack.

→ **Memory access**

Tracking memory access patterns to detect anomalies or suspicious activities.

→ **Network connections**

Monitoring network traffic and connections to identify potentially malicious or unauthorized network activities. Real time and detailed summary of process level network activity including DNS requests, connections, and open ports.

→ **Windows vulnerabilities**

Windows vulnerabilities refer to security weaknesses or flaws in the Microsoft Windows operating system or related software components that can be exploited by malicious actors to compromise the security of a computer or network. These vulnerabilities can vary in severity and impact and at the time of threat elimination patching or updating vulnerabilities improves the system security.

EDR Menu

Easy interaction with endpoints for running processes, executed processes, File explorer, Services, drivers network activity, Hardware inventory, installed softwares, startup apps, scheduled tasks on endpoints.

Accelerates Investigations

NPAV endpoint detection and response is able to accelerate the speed of investigation and because of real time hostorical events and related data.
This keeps track of all the relational events data on endpoint using a massive, powerful graph database,which provides details and context rapidly and at scale, for both historical and real-time data.
This enables security teams to quickly investigate incidents.This enables security teams to effectively track even the most sophisticated attacks and promptly uncover incidents

Attack surfaces Reduction

Attack surfaces are all the places where your organization is vulnerable to cyberthreats and attacks. Endpoint includes several capabilities to help reduce your attack surfaces.
ASR rules help mitigate the risk of common malware infection vectors by restricting the behavior of certain applications and process.

Threat Detection And Response

Blocking for Virus in network for safety.
Detecting threats, blocking risky URLs in network.
Blocking suspicious and vulnerable applications in the network.

Network Service and Process Management

Manage all the services and running processing in the network.

Notification Alerts on

- → Newly Launched applications history on endpoints with detailed information.
- → Detailed information about created files on endpoints with time stamp.
- → Process information which interacting with internet.
- → Unknown installed windows task information
- → All security events from endpoints
- → Integrity monitoring
- → Windows Vulnerabilities

Command execution history

NPAV EDR solution records and reports all executed commands and scripts from various sources, including Windows Command Prompt, Power shell, VBScript, and JScript. This helps in tracking and analyzing user actions on endpoints.

Realtime IoC Hash and Url Blocking

Search for the Malicious files and ulrs using the hashes and blocking of them on endpoints.
Also Reporting the search and block reports to EDR server.

Network Security Statistics

Real time Windows Event Log,Network Connection Logs,Enpoints Firewall Status,
Status of and reports of Attack Surface Reduction (ASR) protection.

System Requirements

EDR Server

Component	Minimum Requirement
Operating System	Any Windows Operating System for EPS Server Configuration.
Processor	~ 500Mhz or Faster
RAM	~ 4 GB
Hard Disk	~ 256 GB
Browser	Chrome, Internet Explorer, Firefox, Opera, Edge and Safari with latest updates
Internet Connection	For EDR Server System only

EDR Client

Component	Minimum Requirement
Operating System	Any Windows Operating System
Processor	~ 500Mhz or Faster
RAM	~ 2 GB
Hard Disk	~ 256 GB
Browser	Chrome, Internet Explorer, Firefox, Opera, Edge and Safari with latest updates

Certifications

OPSWAT. Access Control Notification Anti-Malware GOLD

NATIONAL COMPUTRADE NEWS NCN Innovative Products Award
"Most Popular Antivirus"

WEST COAST LABS CHECKMARK Checkmark Internationally Tested & Certified

For free demo visit: www.adminconsole.net

NP AV

Net Protector AntiVirus

eps@npav.net | 9595306452 | sales@npav.net | 9272707050