NP AV

Net Protector - Endpoint Security

Endpoint Detection & Response (EDR)

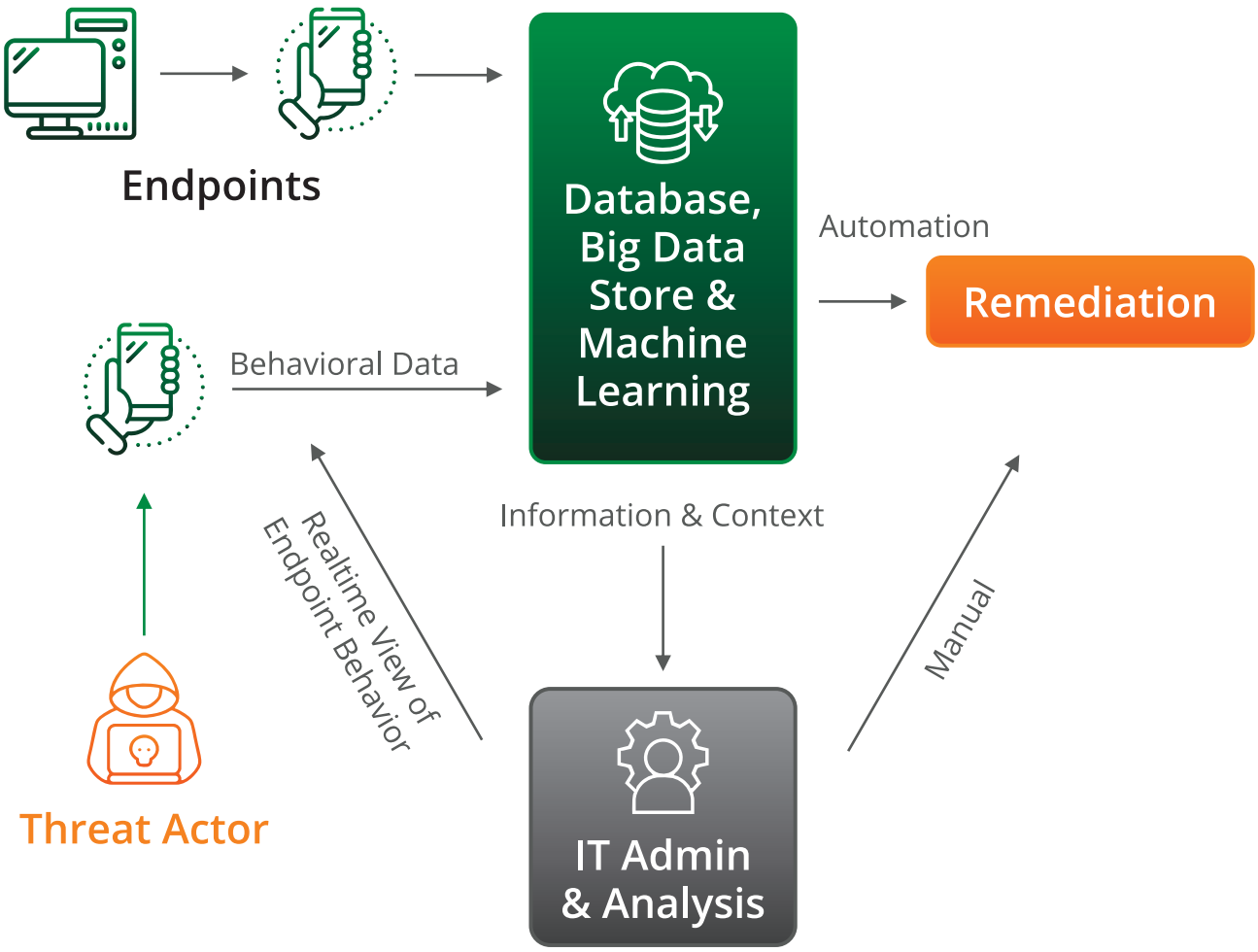
BLOCKS ADVANCED SECURITY THREATS

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)

Threat Intelligence

Threat Hunting

Proactively uncover hidden threats, advanced attacks, and suspicious activities across your enterprise before they escalate into critical security incidents.

Network Connection Logs

Gain complete visibility into every inbound and outbound endpoint connection to quickly detect lateral movement, command-and-control communication, and data exfiltration attempts.

DNS Query Analysis

Continuously analyze DNS traffic to identify malicious domains, DNS tunneling, command-and-control activity, and sophisticated attacker reconnaissance techniques.

Attack Surface Reduction (ASR)

Reduce your organization's attack surface by preventing risky application behavior, malicious scripts, unauthorized macros, and abuse of legitimate administrative tools.

MITRE ATT&CK Mapping

Correlate every security event with the MITRE ATT&CK framework to understand attacker techniques, accelerate investigations, and strengthen threat detection coverage.

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

Tools

Remote Command Prompt

Execute secure remote commands from a centralized console to investigate incidents, collect forensic evidence, and remediate compromised endpoints instantly.

FastXQuery

Perform lightning-fast endpoint investigations using powerful SQL-like queries to retrieve real-time system telemetry across thousands of managed devices.

Firewall Management

Centralize firewall policy management and enforce consistent security configurations across all endpoints to strengthen enterprise network protection.

Patch Management

Identify missing patches, prioritize vulnerabilities, and automate update deployment to minimize security risks while maintaining operational continuity.

Comprehensive System Reports

Installed Software

Maintain a comprehensive inventory of installed applications to detect unauthorized software, improve asset visibility, and simplify compliance management.

Startup Applications

Detect unauthorized startup programs and persistence mechanisms commonly exploited by malware to maintain long-term access to compromised systems.

Services Monitoring

Continuously monitor Windows and Linux services to identify unauthorized changes, suspicious activity, and potential indicators of compromise.

Health Status

Monitor endpoint health, system performance, policy compliance, and resource utilization in real time to ensure maximum operational efficiency.

Threat Detection and Response

Virus Cases

Track, investigate, and respond to malware incidents through centralized visibility, automated containment, and detailed forensic analysis.

Network Blocked URL

Monitor blocked malicious URLs and suspicious web destinations to identify compromised endpoints and prevent users from accessing harmful content.

Web Protection

Protect users against phishing websites, malware downloads, exploit kits, and malicious web content with intelligent real-time web security.

Shell Execution Insights

Gain complete visibility into PowerShell, CMD, and script execution activities to detect fileless attacks and suspicious administrative tool abuse.

Shell Execution Response

Automatically detect, block, and contain malicious PowerShell commands and scripting attacks before they compromise critical business systems.

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.

Security Controls & Response

CIS Benchmarks

Continuously assess endpoint configurations against CIS Benchmarks to strengthen security posture and simplify regulatory compliance initiatives.

IT Ticket Management

Accelerate security operations with integrated ticket management that streamlines incident tracking, collaboration, and issue resolution workflows.

IOC Hash Management

Instantly search, identify, and eliminate known malicious files across your enterprise using centralized IOC hash intelligence and automated response.

URL & IP Blocking

Prevent communication with malicious IP addresses and URLs through centralized policy enforcement and real-time threat intelligence integration.

Security Operations and Compliance

PCI DSS

Supports PCI DSS compliance by helping organizations secure systems that process, store, or transmit payment card data.

NIST 800-53

Supports security controls aligned with the NIST 800-53 framework for risk management and regulatory compliance.

Trust Services Criteria (TSC)

Provides visibility and controls that support Security, Availability, Confidentiality, Privacy, and Processing Integrity requirements.

GDPR

Helps organizations protect personal data and support GDPR compliance through monitoring and policy enforcement.

HIPAA

Supports HIPAA compliance by providing security monitoring, audit logging, and protection for sensitive healthcare information.

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.

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.

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

System Requirements

EDR Server

Component	Minimum Requirement
Operating System	**Windows** : Windows Server 2022 / 2019 / 2016 /2012 / 2008 / 2003 **Linux** : Ubuntu 19 and later
Processor	~ 500Mhz or Faster
RAM	~ 4 GB
Hard Disk	~ 256 GB
Browser	Chrome, Internet Explorer, Firefox, Opera, Edge and Safari with latest updates
Additional Software	Dot Net Framework
Internet Connection	For EPS Server System only

EDR Client

Component	Minimum Requirement
Operating System	**Windows** : Windows 11/ 10 / 8.1 / 8 / 7, Vista, & XP **Mac** : macOS 10.12 and later **Linux** : Ubuntu 16.04 and later, RHEL 7.6 and later, Fedora 32 and later, Debian 9 and later, CentOS 7.8 and later, Suse 12.0 and later Boss 7 and later **Android** : Android version 9.0 to 15.0 Mobile Device Management for Android - MDM Mobile, Tablets & Interactive panels
Processor	~ 500Mhz or Faster
RAM	~ 2 GB
Hard Disk	~ 256 GB
Browser	Chrome, Internet Explorer, Firefox, Opera, Edge and Safari with latest updates

EDR Server Sizing Guide

Endpoints	CPU Crores	RAM	Storage	API Servers
100	4 Cores	16 GB	200-300 GB	2
200	6-8 Cores	16-32 GB	400-600 GB	3
500	12-14 Cores	32-48 GB	1-15 TB	4
800	16-20 Cores	32-48 GB	1.5-2 TB	5-6
1000	20-24 Cores	48-64 GB	2.5-4 TB	6-8

Certifications

Net Protector AntiVirus
eps@npav.net | 9595306452 | sales@npav.net | 9272707050