NET PROTECTOR
Endpoint Security

Endpoint Security (EPS)

More Secure and More Advanced

Easy and complete Endpoint Security solution for Desktops ,Servers, Laptops and mobile devices. Endpoint security forms part of a broader cyber security program that is essential for all businesses, regardless of size. It has emerged from traditional and secure NPAV antivirus software for comprehensive enterprise-grade prevention, detection, response, and threat hunting with the more advanced technology tools and solutions.

Why is Endpoint Security Important?

Due to new emering cyberthreats, cyberattacks, the drastic change in digitalisation and usage of the internet and buisnesses leaning towards remote operations for these The traditional way of protection and enpoint security in not sufficiant.

Every device that employees use to connect to business networks represents a potential risk that cyber criminals can exploit to steal corporate data. These devices, or endpoints, are rapidly increasing and making the task of securing them more difficult. It is therefore vital for businesses to deploy tools and solutions that protect their cybersecurity front line.

NPAV Endpoint protection offers a centralized management console to which organizations can connect their network. The console allows administrators to monitor, manage, investigate and respond to potential cyber threats. This can either be achieved through an on-premise, cloud, or hybrid approach:

On-premise

An on-premise or on-location approach involves a locally-hosted data center that acts as a hub for the management console. This will reach out to the endpoints via an agent to provide security.

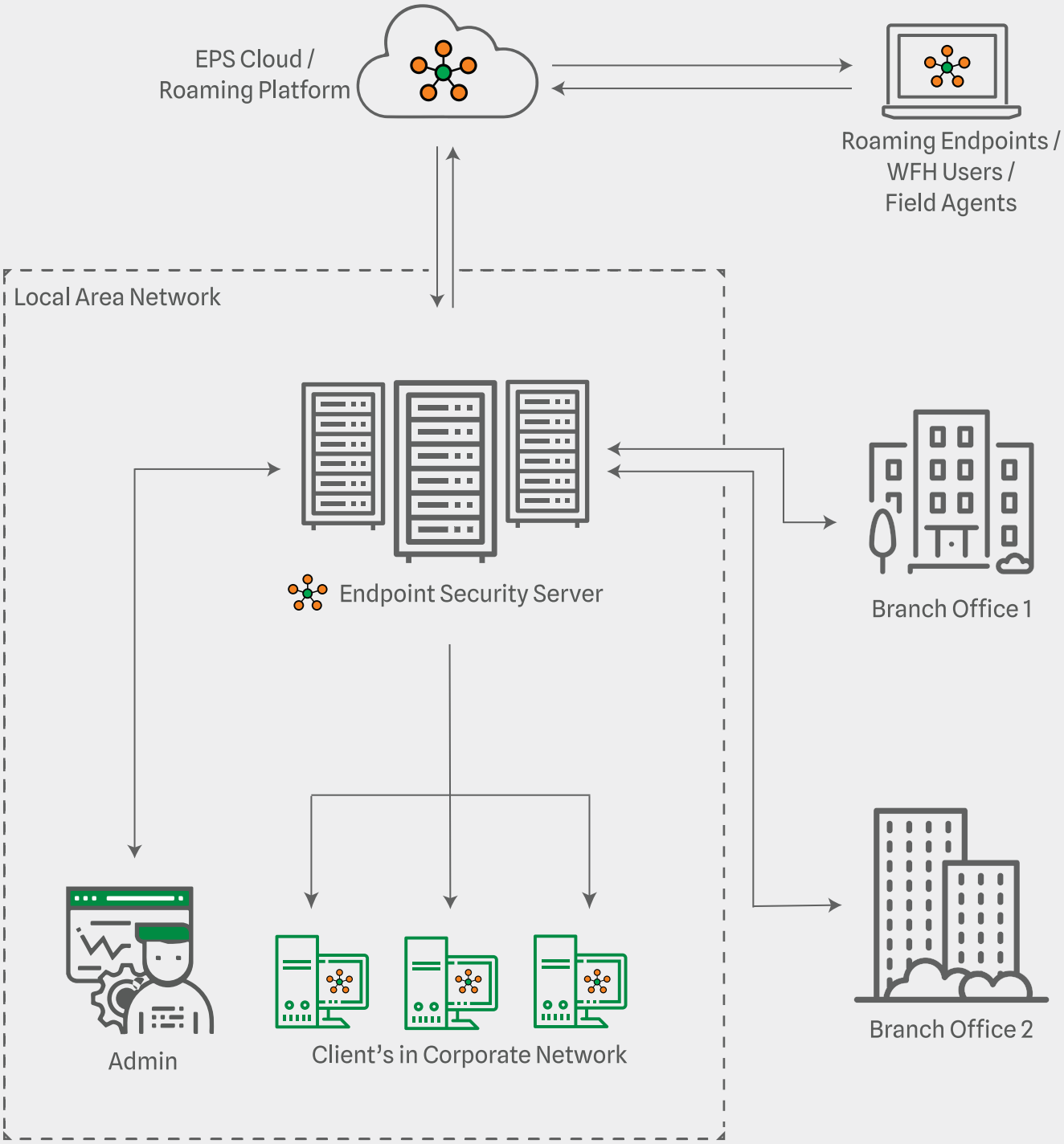
Cloud

This approach enables administrators to monitor and manage endpoints through a centralized management console in the cloud, which devices connect to remotely. Cloud solutions use the advantages of the cloud to ensure security behind the traditional perimeter, so its better to manage the roaming endpoint laptops or Work from home nodes.

Hybrid

A hybrid approach mixes both on-premise and cloud solutions. This approach has increased in prevalence since the pandemic has led to increased remote working.

Endpoint Security (EPS) Network Flow Diagram



Key Features of Endpoint Security (EPS)

Cloud Based Endpoint Security Console

Ease of access increased exponentially as you can now manage the admin console from anywhere. Secure and reliable device independent access which allows the admin to access the console from any internet enabled PC/Mobile/Tablet.

Centralized and Real-time Administration

Web-based console with graphical dashboard for Network Endpoints Statistics , Security health status, Endpoints vulnerability, Statistics of Clients, Update and Threat status etc.

Multilayered Protection

protection against all types of viruses , malware . Anti-Ransomware Shield to protect from ransomware attacks , Web protection shield for the phishing and malicious and blocking unwanted sites , Advertise blocking shield for Adware & saves internet bandwidth, CPU, Memory etc.

Anti-Phishing

Blocks fraudulent bank look-alike pages & login credential stealing links.

IDS/IPS

Detects malicious network activities which exploit application vulnerabilities and blocks intruder attempts on the managed endpoints.

Live Chat and Remote Desktop Viewer

System Admin can view desktop of client PC remotely by single click. Live chat with clients. Also can send the important announcement to client by the type of notification admin wants to send.

Advanced Device Control

Enforcing policies regarding the use of storage devices, mobile and portable devices USB, WPD ,MTP ,PTP devices, CD/DVD etc. Easy to Restrict devices can also Allow only white listed devices in corporate network.

Application Control

View and Manage running processes. Transfer ,Install software or run application and patches on clients easily. Kill,Block Unblock Processes of clients on single setting.

Data Backup

Manage client data backup from the server. Data backup will protect the client's data from all kinds of ransomware attacks. The backup will be secured and will remain to be corruption free. Monitoring and managing functionalities will be enabled for the admin.

Easily Manage & Control Network Protection

View Protected and Unprotected Client PCs in the network. Launch scanning and updates from the centralized management console.

Firewall

Monitors inbound and outbound network traffic administrator can easily add and manage rules for the network traffic based on the connecting ports , IP, Application etc.

Password Management

We secure and automate the process for managing local administrative passwords on endpoints, admin can set the endpoint's password from anywhere on one click. Easy to view previous password history.

Traffic monitoring

Administrator can monitor the Internet Traffic over the LAN with help of Advanced graphical charts.

Web Protection

Blocks unwanted sites, videos, MP3s, Torrents & increases the productivity of endpoints.

System Tune-Up

System tune-up utility which digs deep into your computer and fixes trouble areas. It performs several functions, including defragmenting your PC's hard drive, repairing the incredibly problematic Windows Registry, and freeing up disk space by deleting useless and duplicate files. Scheduled tune-up and monthly disk check.

Session Activity

Session activity record details of log in-log out, Remote desktop,Start and shutdown activity with single setting from the EPS admin console to managed clients.

User Activity Monitor

Monitor user activity using user browsing content.

Printer Activity Monitor

EPS comprises of Print Activity feature that efficiently monitors and logs printing tasks done by the managed endpoints with all necessary details such as number of copies, Document Name ,Date Time , IP ,Machine Name etc.

Push Installer (Remote Install)

You can scan for all protected and un-protected PCs in the network and then push the installation to the client PCs. This feature is very useful for managing large count of PCs.

Vulnerability Scanner

Scans & lists exposed areas of all network endpoints as well as roaming devices.

Low disk space email alert

Get Low disk space alerts on WhatsApp and mail provided by admin

File Sharing Activity

EPS comprises of File Sharing & Activity Monitoring feature that efficiently monitors and logs activity of managed endpoints. File monitoring feature with deep inspection monitors and records access to shared files with details as user names, file names, client IP addresses.

Data Loss Prevention

Monitoring confidential and user defined data shared through removable drives, network and browser applications with the snapshots from endpoints while Data breach occurred.

Patch Management

Centralized patch management solution to patch Vulnerabilities of Microsoft and third party applications.

Offline Updates - Weekly

You can download the Net Protector Endpoint Security server and client updates and patches from our website and apply on the server machine. The clients will automatically pull the updates from the server over your LAN without need for internet on server or clients. This feature is very useful for Government or Defense organizations.

Totally Offline Installation & activation of Server and all Clients

The server and clients can be installed without any internet connection.

Product Edition & Feature Comparision

Features	Professional	Advanced	Enterprise
Antivirus & Anti-Malware	✓	✓	✓
Anti-Ransomware Shield	✓	✓	✓
Anti-phishing	✓	✓	✓
Data Backup	✓	✓	✓
Live Chat and Remote Desktop Viewer	✓	✓	✓
Application Control	✓	✓	✓
Firewall Protection	✓	✓	✓
IDS / IPS	✓	✓	✓
Instant Messaging Protection	✓	✓	✓
OS Vulnerability Scanner	✓	✓	✓
System Tunner	✓	✓	✓
Advanced Device Control	✓	✓	✓
Asset Management - Hardware Change Notification	✓	✓	✓
Email Notification	✓	✓	✓
Web Protection	✓	✓	✓
LAN Monitor	✓	✓	✓
Advertise Blocker	✓	✓	✓
Traffic Monitor	✓	✓	✓
Printer Activity Monitor		✓	✓
Patch Management		✓	✓
File Sharing Activity		✓	✓
Session Activity Monitor		✓	✓
Corporate Web Control		✓	✓
IT Ticket System			✓
Security Operation Center			✓
Password Management			✓
Disk Encryption			✓
Data Loss Prevention (DLP)			✓

NPAV Endpoint Security Apk available on Google Play Store for EPS Cloud Assistance

System Requirements

EPS 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
Additional Software	Dot Net Framework
Internet Connection	For EPS Server System only

EPS 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. BRONZE CERTIFIED Anti-Malware

NCN Innovative Products Award "Most Popular Antivirus"

Checkmark Internationally Tested & Certified

For free demo visit: www.adminconsole.net

NP AV Net Protector AntiVirus
eps@npav.net | 9595306452 | sales@npav.net | 9272707050 | www.adminconsole.net