



NET PROTECTOR

Endpoint Security



Endpoint Security (EPS) Enterprise

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 advanced technology tools and solutions.





Why is Endpoint Security Important?

Due to new emerging cyber threats, cyberattacks, the drastic change in digitalization and usage of the internet, and businesses leaning towards remote operations for these, the traditional way of protection and endpoint security is not sufficient.

Every device that employees use to connect to business networks represents a potential risk that cybercriminals 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.



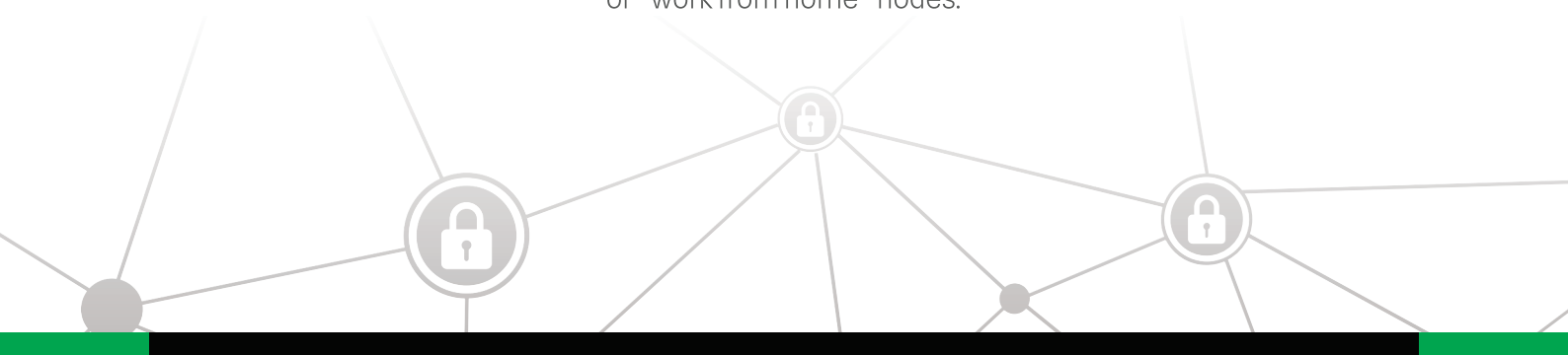
Cloud

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



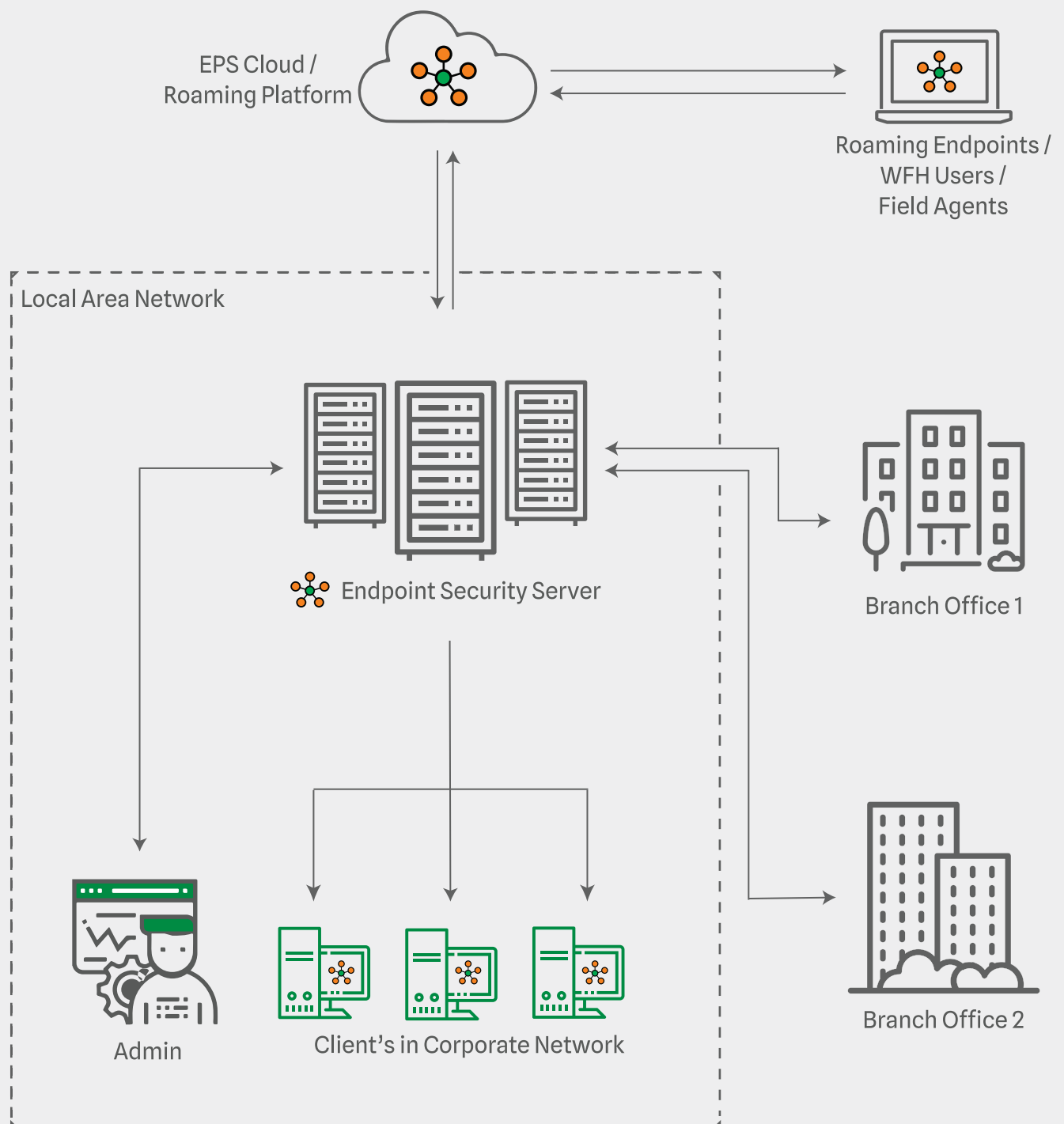
Hybrid

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 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, and malware. Anti-Ransomware Shield to protect from ransomware attacks, Web protection shield for 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

The IDS/IPS actively detects and blocks malicious network activities that exploit application vulnerabilities on managed endpoints. It monitors both inbound and outbound traffic based on predefined rules and provides real-time alerts for potential threats, such as port scanning and Distributed Denial of Service (DDOS) attacks, ensuring enhanced network security.



Advanced Device Control

Advanced Device Control provides comprehensive access control and monitoring for multiple device types, including workstations, USBs, Bluetooth, and other portable devices. It supports offline enforcement and forensics, allowing device usage tracking even without network connectivity. The system offers device authentication and media encryption to enforce strict policies on the use of storage devices, ensuring only whitelisted devices are permitted in the corporate network. This helps protect sensitive data by restricting unauthorized device access.



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.



Easily Manage & Control Network Protection

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



Data Backup

The Data Backup feature enables secure management of client data from the server, protecting it against ransomware attacks and ensuring data integrity. It offers reliable backup, data recovery, and rollback options, keeping backups free from corruption and ensuring quick restoration of files when needed. This ensures business continuity and protection from data loss.



Traffic monitoring

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



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 diskcheck.



Session Activity

Session activity records details of log-in, log-out, remote desktop, start, and shut down activity with a single setting from the EPS admin console to managed clients.



User Activity Monitor

Monitor user activity using user browsing content.



Web Protection

Web Protection blocks access to unwanted websites, videos, MP3s, and torrents to enhance endpoint productivity. It offers robust malware protection through blended threat detection, leveraging Host Intrusion Prevention Systems (HIPS) and behavioral analytics. The system detects and removes malware over both HTTP and HTTPS traffic, automatically filtering malicious content. Additional features include web filtering, scanning suspicious email attachments, and enhanced remediation capabilities to ensure comprehensive security against online threats.



Vulnerability Scanner

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



File Activity Monitoring

File Activity Monitoring tracks and logs all file activities on managed endpoints, including copying, renaming, deleting, and modifying important files. It provides deep inspection of shared files, recording details such as user names, file names, and client IP addresses. This feature ensures full visibility into file access and activity, enhancing data security and accountability across the network.



Data Loss Prevention

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



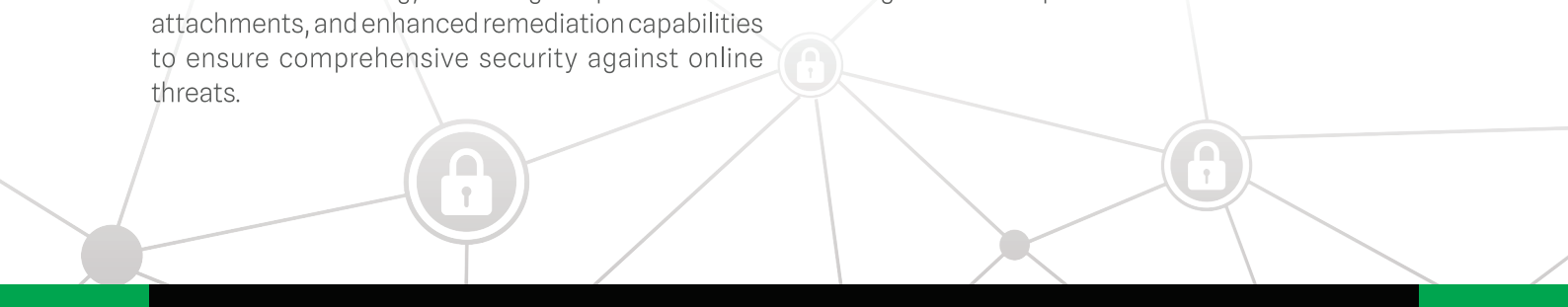
Patch Management

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



Application Control

Application Control allows administrators to view and manage running processes across client systems. It enables easy software transfer, installation, and patch management. With a single setting, administrators can kill, block, or unblock processes, providing granular control over application behavior. Additionally, it supports application blacklisting, preventing unauthorized or harmful applications from running on client endpoints.





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 a large count of PCs.



Remote Data Wiper

It deletes data in selected folders and repeatedly overwrites stored data to prevent recovery using recovery software or forensic image, meaning that it is no longer of any use to anyone. For securely shredding files and folders on the computer using multiple shredding algorithms up to 7 passes.



Global Threat Intelligence

Expertise and analysis concerning worldwide cyber security threats, Advanced Persistent Threats (APTs) encompassing insights into emerging risks, advanced attack vectors, and strategic defense measures.



Advanced ML and AI interaction

Antivirus software leverages advanced machine learning and artificial intelligence algorithms to dynamically analyze file behavior, identify patterns indicative of malware, and proactively defend against evolving threats. This intelligent interaction enables real-time threat detection, rapid response to zero-day attacks, and continuous adaptation to emerging cyber security challenges, ensuring robust protection against sophisticated malware and cyber threats.



SIEM Integration

SIEM integration enables the aggregation of security data from diverse sources such as firewalls, IDS/IPS, antivirus systems, and logs into a central SIEM platform. This allows for real-time monitoring, threat detection, and incident response, providing organizations with a unified view of their security posture and enabling proactive defense against cyber threats through advanced analytics and correlation of security events.



Totally Offline Installation & activation of Server and all Clients

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



Update manager

Supports multiple update servers to ensure continuous and reliable delivery of security updates and patches. This configuration enhances the resilience and efficiency of your endpoint protection strategy.



Advanced protection against file attachments

There are several layers of security measures to detect and mitigate data theft and threats associated with Data Leakage Prevention and malicious files that are uploaded to browsers, network share, Web mail, POP3/SMTP and USB drives.



Endpoint forensic

Cyber security involves investigating and analyzing digital evidence on individual devices (endpoints) to understand and respond to security incidents or breaches. It includes techniques such as data collection, analysis, and interpretation to identify the cause, scope, and impact of security incidents on specific endpoints. This process helps in remediation, threat hunting, and improving overall cyber security posture by uncovering vulnerabilities and mitigating future risks at the device level.



Disk Encryption

NPAV Disk encryption Feature includes file level, folder level, volumes level, and full disk Encryption. If an encrypted disk is lost, stolen, or placed into another computer, the encrypted state of the drive remains unchanged, and only an authorized user can access its contents using the password. NPAV Disk Encryption is an amazing and reliable Feature that helps you fully secure your data.



Asset Management

The Asset Management feature allows organizations to collect comprehensive system information related to endpoints, including both software and hardware details. It tracks changes such as applications installed or uninstalled, as well as any hardware modifications. Additionally, it provides insights into system activity by capturing the system turn-on and shutdown times, helping to ensure accurate monitoring of endpoint usage and changes over time.



Advanced Memory Protection

This feature provides robust memory protection, offering multilayered defense against all types of viruses. It detects and blocks ransomware using heuristic analysis, ensuring advanced protection against fileless attack methods that exploit system memory, safeguarding endpoints from sophisticated threats.



Live Chat and Remote Desktop Viewer

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



Password Management

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



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 the number of copies, document name, date time, IP, machine name, etc.



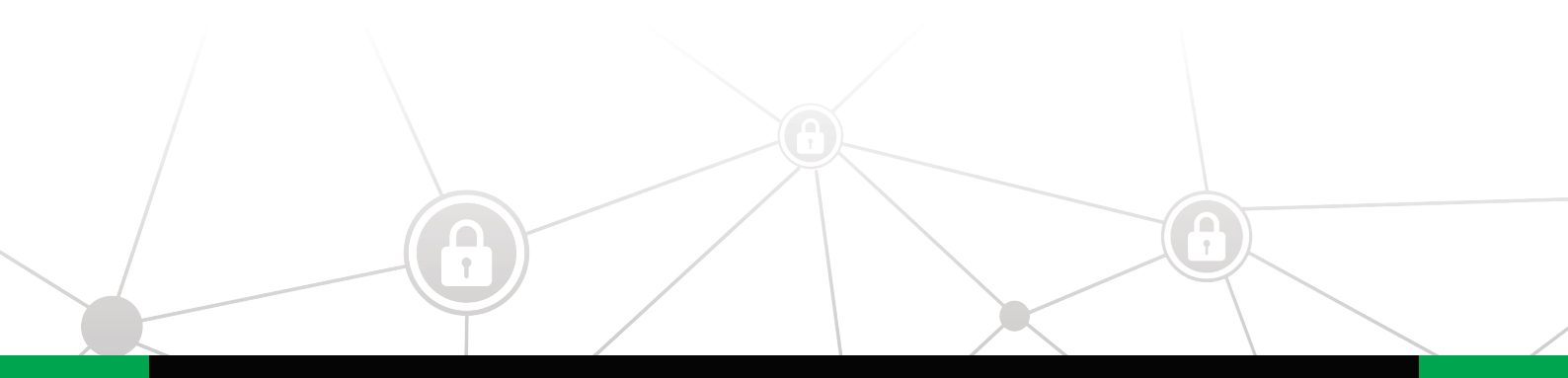
Offline Updates - Weekly

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



Low disk space email alert

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





Endpoint Security (EPS)

Product Edition & Feature Comparision

Features	SME	Business	Total	Enterprise
Antivirus	✓	✓	✓	✓
Anti Ransomware	✓	✓	✓	✓
Email Protection	✓	✓	✓	✓
IDS/IPS Protection	✓	✓	✓	✓
Firewall Protection	✓	✓	✓	✓
Phishing Protection	✓	✓	✓	✓
Browsing Protection	✓	✓	✓	✓
SMS Notification	✓	✓	✓	✓
Vulnerability Scan	✓	✓	✓	✓
Roaming Platform	✓	✓	✓	✓
Artificial Intelligence	✓	✓	✓	✓
Asset Management		✓	✓	✓
Spam Protection		✓	✓	✓
Web Filtering		✓	✓	✓
Advanced Device Control		✓	✓	✓
SIEM Integration		✓	✓	✓
Application Control - Blacklist			✓	✓
Application Control - Safelist			✓	✓
Tuneup			✓	✓
File Activity Monitor			✓	✓
Patch Management			✓	✓
YouTube Access Controller				✓
Google Access Controller				✓
Disk Encryption Management				✓

Add on Features-

- ✦ IT Ticket System
- ✦ Data Loss Prevention (DLP)
- ✦ YouTube Access Manager
- ✦ Google Login Management
- ✦ Realtime IoC Hash and Url Blocking
- ✦ Pre-Attack Surface Reduction
- ✦ Threat Detection and Response
- ✦ Network Access Control
- ✦ Network Service & Process Management

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



System Requirements

EPS Server

Component	Minimum Requirement
Operating System	Windows Server 2022 / 2019 / 2016 / 2012 / 2008 / 2003
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	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
Processor	~ 500Mhz or Faster
RAM	~ 2 GB
Hard Disk	~ 256 GB
Browser	Chrome, Internet Explorer, Firefox, Opera, Edge and Safari with latest updates

Certifications



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



Checkmark
Internationally
Tested & Certified



For free demo visit: www.adminconsole.net



Net Protector AntiVirus

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

© Biz Secure Labs Pvt Ltd. All rights reserved.