Net Protector NPAV Cyber Security | Endpoint Security Cloud

NPAV Endpoint
Data Loss Prevention

NPAV Endpoint Data Loss Prevention (DLP) is an advanced security solution designed to safeguard sensitive data by monitoring, detecting, and preventing unauthorized access, sharing, or transfer of information. By providing real-time tracking and robust control mechanisms, NPAV Endpoint DLP ensures that data remains protected across various environments, including endpoint devices, cloud-based locations, and on-premises systems.

Key Features of NPAV Endpoint DLP

Upload Monitoring

» **Real-Time Monitoring**

Tracks user interactions within web applications, including downloads, uploads, and data transfers.

» **Upload Restrictions**

Enforces policies to block and report the unauthorized upload of sensitive data to restricted websites.

» **Activity Logging**

Logs all actions involving sensitive data, such as downloads, uploads, and access attempts, for auditing and compliance.

» **Browser Compatibility**

Supports Chrome, Microsoft Edge, Firefox, Opera, Tor, Aurora Firefox, and Maxthon.

» **Screenshot Capture**

Takes automatic screen shots of suspicious activity, particularly when sharing files through browsers.

» **Remote Tool Compatibility**

Supports Anydesk, Teamviewer, RealVNC, Windows Remote, TightVNC, Ultraviewer etc.

» **Bluetooth**

Monitor and control Bluetooth activities. It detect and block file transfers over Bluetooth2.

Email Protection

» **Restricted Email Access**

Ensures sensitive content or attachments are only sent to permitted email addresses.

» **Attachment Scanning**

Scans attachments for malware, ransomware, and other malicious software.

» **Phishing Protection**

Identifies and blocks phishing links.

» **User Specified Attachment**

Selected type of attachment Allowed/Blocked for sending through mail.

AI Tool / Application Monitoring

» Enables Data Leak Prevention (DLP) monitoring for selected AI applications and platforms. The feature inspects user interactions, file uploads, clipboard activities, and data transfers to AI tools to detect, monitor, and prevent unauthorized sharing of sensitive or confidential information.

Screenshot Facility

» Image Capture

Captures and logs screenshots when sensitive data is being uploaded, providing visual evidence of suspicious activity.

Sensitive Data Scanning

» Data Protection

Scans for sensitive information, such as credit card details, personal identifiers, and financial data, ensuring protection against unauthorized access and breaches.

Protected Folder

» The Protected Folder Feature secures data by applying protection policies to specified folders. It prevents unauthorized actions such as copy/paste (Clipboard Protection), printing, exporting, and using "Save As" to relocate files, ensuring controlled access and preventing data leakage.

Data Discovery & Classification

» Identify and locate sensitive data across endpoints and cloud with Data Discovery. Classify information as Public, Confidential, or Restricted with Data Classification to meet compliance (GDPR, DPDP) and apply proper security controls like encryption, access management, and monitoring.

Download Monitoring

» File Control

Tracks and restricts the downloading of specific file types, such as executables, compressed files, and sensitive documents, to prevent unauthorized data exposure.

Device Control

» Peripheral Control

Monitors and controls access to peripheral devices, such as USBs and printers, to prevent data leaks.

Drive Encryption

» Drive encryption is like locking your data in a super-secure box. Even if someone steals your computer or hard drive, they can't see or use your files without the special key (password). It protects your information so only you can access it.

Drive Monitoring

» Comprehensive Tracking

Monitors and controls data stored and transferred across local drives, removable devices, and network drives.

» File Type Monitoring

Monitors a wide range of file types, including Office files, graphic files, programming files, and other confidential data.

File Classification

» File Classification identifies, categorizes, and labels files based on their content, sensitivity, or regulatory requirements. By classifying files automatically or manually, organizations can enforce appropriate security policies, manage access controls, and ensure compliance with data protection standards.

» Automatic Classification: Uses content analysis, keywords, or metadata to categorize files.

Manual Tagging: Allows users or administrators to assign classifications to files as needed.

Print-Screen Blocking

» Print-screen blocking prevents users from capturing screenshots of sensitive information. This feature restricts the use of the print-screen function to protect confidential data.

» The print-screen action is blocked to prevent unauthorized screenshot capture.

Printer Activity

» Monitors and logs all printer-related actions to prevent unauthorized printing of sensitive data.

» Tracks all printing activities for enhanced data security.

» Logs printer usage to detect and prevent data leakage through printed documents.

Bluetooth File Transfer

» Monitors and restricts Bluetooth file transfer to prevent unauthorized data sharing.

» Prevents unauthorized data exchange through Bluetooth connectivity.

Notification Alerts

» Interactive Alerts

Sends real-time notifications and warnings to users regarding unauthorized data access or transfer, allowing immediate action.

Certifications

Net Protector NP AV Cyber Security | Endpoint Security Cloud

help@npav.net
9325102020

sales@npav.net
9272707050