Net Protector NP AV 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

Browser 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.

Email Protection

» Restricted Email Access

Ensures sensitive content or attachments are only sent to permitted email addresses (e.g., Outlook), preventing unauthorized distribution.

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.

Notification Alerts

» Interactive Alerts

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

Screenshot Facility

» Image Capture

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

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.

Folder Lock Protection

» Customizable Security

Offers flexible security options to lock and protect files and folders based on organizational requirements.

Device Control

» Peripheral Control

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

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.

Certifications

Net Protector NP AV Cyber Security

Endpoint Security Cloud