McAfee™

McAfee Data Loss Prevention Endpoint

Don't be the next data loss statistic

Are you losing data without even knowing it? Your customer information, intellectual property, financial data, and personnel files may be leaving your corporate borders right now. And the perpetrators are not only hackers—they can also be your own employees. Accidental and malicious data loss can occur through common channels such as email, web posting, USB drives, and uploading to the cloud—potentially costing you millions. Every day, companies fall victim to massive data loss through malicious and unintentional leakage of information. What if you could easily and effectively stop data loss? What if you could meet industry and government compliance and protect intellectual property at the same time? Now you can—with the comprehensive McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint).

Device-to-Cloud DLP

McAfee DLP Endpoint is integrated with MVISION Cloud DLP. On-premise DLP policies can be easily extended to the Cloud with a single click and as fast as under one minute.[1] On-premises DLP classification tags is shared with cloud DLP policies to ensure consistent data loss detection.

Advanced Protection Capabilities

McAfee DLP Endpoint provides comprehensive protection for all possible leaking channels, including removable storage devices, the cloud, email, instant messaging, web, printing, clipboard, screen capture, file-sharing applications, and more.

Key Advantages

- **Device-to-cloud DLP:** Easily extend on-premises DLP policies to the cloud for consistent data loss detection.
- **Advanced protection capabilities:** Leverage fingerprinting, classification, and file tagging to secure sensitive, unstructured data, such as intellectual property and trade secrets.
- **Centralized management:** Native integration with McAfee® MVISION ePolicy Orchestrator® (MVISION ePO™) helps streamline policy and incident management.[2]
- **Compliance enforcement:** Ensure compliance by addressing day-to-day user actions, such as emailing, cloud posting, downloading to removable media devices, and more.
- **User education:** Real-time feedback via an educational popup helps shape corporate security awareness and culture.

Connect With Us

McAfee DLP Endpoint key features include:

- Capability to set Microsoft Azure Information Protection (AIP) labels for data in motion and to recognize AIP labeled files.[3]

- Integration with third-party user behavioral analytics (UEBA) tackles insider threat. It conducts security analytics to detect unusual and highly risky user and entity behavior.

- Manual classification empowers users to manually classify documents, increases employee data protection awareness, and reduces administrative burden.

- User-initiated scan and remediation allows users to run endpoint discovery scans and perform self-remediation actions.

- Classification is flexible and includes dictionaries, regular expressions and validation algorithms, registered documents, and support for third-party user classification solutions

- Unique tagging technology identifies documents according to their origin helps prevent sensitive information from web applications, network applications, and network shares from being duplicated, renamed, or leaving the corporate premises.

- Enhanced virtualization support protects remote desktops and virtual desktop infrastructure (VDI) solutions.

Centralized Management

- Managed by a Cloud-native management console—MVISION ePO—for streamlined policy and incident management.[4]

- It shares the same policy and classification engines, and incident workflows with McAfee® MVISION Cloud (CASB) and McAfee® Network DLP.

- Multiple policies and reusable rule sets offer you the ability to define multiple DLP policies across the organization and help you create policies according to office, department, regulation, and more.

- Enhanced granularities in incident management can query/filter/view by any incident property (for example, device serial number, evidence file name, and groups).

- Centralized event monitoring and auditing capabilities.

- Improved role-based access control (also known as separation of duties) for policy management, as well as incident review.

- Easy-to-access help desk interface.

Supported Platforms

- Windows 10 (32-bit and 64-bit)
- Windows 8 or 8.1 (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows Server 2019
- Windows 2016 (64-bit)
- Windows 2012 (64-bit) and Windows 2012 R2 (64-bit)
- Windows 2008 (32-bit and 64-bit) and Windows 2008 R2 (32-bit and 64-bit)
- macOS Catalina 10.15 or later
- macOS Mojave 10.14 or later
- macOS High Sierra 10.13 or later
- macOS Sierra 10.12 or later
- OS X El Capitan 10.11 or later
- OS X Yosemite 10.10 or later
- OS X Mavericks 10.9.0 or later

Supported Browsers

- Internet Explorer version 11 or higher
- Mozilla Firefox 48 or higher
- Google Chrome 65 or higher

Compliance Enforcement and User Education

With the corporate perimeter disappearing, it is getting more challenging for corporations to enforce compliance. McAfee DLP Endpoint can not only help you monitor day-to-day user behaviors, but also can ensure compliance by providing user education. With a click of a button, McAfee DLP Endpoint offers detailed reports to prove to auditors, senior management, and other stakeholders that internal and regulatory compliance measures are in place. It offers templated policies for regulations and use cases, making it easy for you to stay compliant. Your users also get real-time feedback via enforcement popups based on your corporate policy, and these bite-sized educational opportunities help you build a stronger corporate security culture.

Supported McAfee ePO Software

- McAfee ePO 5.9.1 and 5.10 for DLP 11.1 or higher

Support for McAfee MVISION ePO (SaaS)

- For DLP 11.5 or higher, no software or DLP extension installation is required. A username and password are required for authentication to access MVISION ePO.

For a full list of supported platforms, browsers, and software, please refer to McAfee Knowledge Base.

Learn More

For more information, visit www.mcafee.com/dlp-endpoint.

1. Based on consistent McAfee internal lab testing.
2. McAfee DLP Endpoint version 11.5 or higher.
3. Ibid.
4. Ibid.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com