Solution Brief

Keep Your Data Safe for Office 365

Content-aware protection for your most sensitive data

Organizations of all sizes are adopting cloud-based Microsoft Office 365 as a way to give users greater flexibility and access to core business applications anytime, anywhere, and on virtually any device. While Office 365 includes built-in data loss prevention capabilities, additional protection is needed when it comes to preventing data loss from advanced persistent threats, as well as insiders. McAfee® Data Loss Prevention (McAfee DLP) provides a one-stop, comprehensive protection for your most sensitive data in the cloud and elsewhere. It protects intellectual property and ensures regulatory compliance for these types of data: Payment Card Industry (PCI), personally identifiable information (PII), and protected health information (PHI). McAfee DLP offers expansive, yet flexible, polices and templates that can help address risky employee behavior by protecting sensitive data from day-to-day user actions.

There are many benefits that McAfee DLP offers for Office 365 and beyond:

- Prevent sensitive data leakage via outbound email, whether it is connected to a physical or hosted Microsoft Outlook/Microsoft Exchange Server.
- Protect Outlook Web Application (OWA) with Exchange Online via McAfee SaaS Email and its sophisticated built-in DLP templates.
- Prevent sensitive data being uploaded via either the browser directly or via the desktop cloud sync folder to OneDrive for Business. Any files saved to OneDrive for Business will also be monitored and can be blocked.
- Scan and block sensitive files being uploaded to SharePoint Online, and automatically tag necessary files downloaded from the application. Once the file is tagged, its security attributes are preserved against copying to the clipboard, renaming, saving to removable storage, and more.
- Detect sensitive data being copied to the clipboard.
- Detect sensitive data sent to a local or network printer.
- Detect sensitive data saved to USB or other removable media.
- Detect sensitive data saved or copied to network shares.
- Discover sensitive data on the endpoint file systems.

- Detect and prevent leakage of “partial files” resulting from copy/paste to new files and alternate file formats.
- Detect and prevent sensitive data access from suspicious processes (through integration with McAfee Threat Intelligence Exchange).
- Protect the loss of sensitive data though other communication protocols such as FTP and SSH.
- Detect sensitive data sent through instant messaging platforms such as Google Chat, Yahoo, Snapchat, or any messages sent through web-based applications.
- Require and record justifications for variations from corporate policies, while educating and adapting user behavior.

McAfee DLP and its related solutions continue to improve cloud protection with features that address the ever-changing threat landscape. Please check **www.mcafee.com/o365** for the latest updates.

Learn More

For more information or to start an evaluation of McAfee DLP, contact your McAfee representative or channel partner, or visit **www.mcafee.com/DLP**.

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2015 McAfee, Inc. 61995brf_dlp-for-o365_0615_fnl_ETMG

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com