

Chapter 1 : Azure Information Protection for Office

** Customers purchasing Windows Server CAL agreements, System Center Configuration Manager, System Center Endpoint Protection, Microsoft Active Directory Rights Management Services CALs via the Microsoft Enterprise Volume Licensing agreements may purchase the Enterprise Mobility + Security Add-on offer.*

The solution automatically discovers sensitive data and applies policy-based usage restrictions, allowing only authorized information to leave your organization. Data breaches attributed to third parties are on the rise, but you can combat this information loss with McAfee Data Protection Suite for Rights Management. It merges McAfee data loss prevention technologies with Adobe LiveCycle ES2 Rights Management to provide comprehensive protection for your digital assets in a single solution. Data sent to customers, suppliers, or partners can often end up in the wrong hands. For example, what happens to proprietary company information included in a RFP, after the bidding process is over? How do insurers safeguard sensitive patient data inadvertently sent to the wrong recipient? It boosts control over your data even after it leaves your network, helping to avoid costly and damaging data loss, and keep you compliant. The solution automatically discovers sensitive data on your local drives, without requiring any user interaction, eliminating inefficiencies inherent with manual process-based data protection solutions. It then instantly applies policy-based usage restrictions by accessing the Adobe LiveCycle server to implement access rules that are based on your information security policies. Digital rights management protects files against unauthorized access, regardless of where the file resides or how it is distributed. User access rights are defined by individual, job title, job function, and other parameters. The solution works with Adobe Reader and Microsoft Office. Native support for PDF documents gives you instant support for hundreds of millions of users globally. And since hundreds of document types can be converted into PDF files, you get nearly ubiquitous file protection that works anytime and anywhere. It covers data distributed via email, the web, and USB drives, so you can safely exchange information with partners, suppliers, and customers, without worrying about data loss. With powerful and flexible policy controls, you can keep tabs on all of your data in the field and modify rights as needed. For example, revoke a service manual that is outdated or instantly change rights to eliminate user access to a file. Rest assured that unsecured data cannot leave your network, since all files must have a rights management policy. With simplified data management, robust digital asset protection, and flexible policy controls, you can confidently exchange information with third parties outside the enterprise—without worrying about the security of your most sensitive data. Protect sensitive data automatically Discover sensitive data without any user interaction and eliminate inefficiencies inherent with manual process-based data protection solutions. Instantly scan local user drives to find sensitive data that needs to be protected and immediately assign a rights management RM rule based on your information security policies. Share information with confidence Collaborate with third parties without worrying about data breaches. McAfee Data Protection Suite for Rights Management helps avoid costly and damaging data loss, and supports regulatory compliance. Safeguard data sent to third parties Protect data sent via email, the web, and removable hard drives. Encrypted files can only be accessed by authorized users and the RM protection travels with the document, regardless of the device used to access the file. Secure data throughout the entire lifecycle Audit, revoke, change, or update user privileges to maintain control over data even after it leaves the organization. You can restrict access to data for a specific period of time, rescind a document, and alter authorized users or groups. Protection remains in place regardless of where users are located or the length of time they have the data. Get instant support for hundreds of millions of users Support a broad user base. Adobe Reader includes native support for rights management, giving you instant coverage for hundreds of millions of users. Microsoft Office documents are supported via a simple plug-in. Automated processes eliminate error-prone manual data discovery, lowering administrative overhead. Protection for unsecured data Stop data that does not have a RM applied from leaving your organization via email, web, or removable media device. Deploy, monitor, and generate actionable reports to boost security and support compliance. The McAfee ePO platform pushes data policies out to every corporate endpoint to ensure that all sensitive data is discovered. From a single console, easily manage security

deployment and track, audit, and report on sensitive data access to meet compliance requirements. The following are minimum system requirements only. Actual requirements will vary depending on the nature of your environment.

Chapter 2 : Enterprise Mobility + Security Overview | Microsoft

Easily enforce policies to improve data security. Both Azure Information Protection for Office and Office Message Encryption are policy based and designed to work with the Exchange transport rule engine.

Resources Protect information from unauthorized access—internal and external Azure Information Protection for Office provides a comprehensive policy-based enterprise solution to help protect your valuable information, no matter whom you share it with. Easily enforce policies to improve data security Both Azure Information Protection for Office and Office Message Encryption are policy based and designed to work with the Exchange transport rule engine. That means Azure Information Protection for Office allows you to set up complex policy restrictions easily, with just a single action. Simple and convenient communication management Azure Information Protection for Office is built to work across multiple workloads such as Exchange, SharePoint, and Office documents, and it makes it easier to set restrictions and provide permissions. Office Message Encryption comes with a modern user interface that makes it easy to use. Azure Information Protection for Office includes: Help protect emails against unauthorized access by applying different AIP options to your email messages. Apply custom templates based on your business needs in addition to using default protection templates. Office Message Encryption Easily share protected emails with anybody—inside or outside your organization Provide strong, automated encryption with a cost-effective infrastructure. Easily manage sensitive data using single-action Exchange transport rules. Decrypt and read encrypted email with confidence, without installing client software. Send encrypted and rights protected messages to people inside and outside your organization including users of Office , non-Office email applications, and web-based email services such as Gmail. Azure Information Protection for Office is a cloud-based solution designed to deliver similar protection to customers using Office It can also be purchased as a standalone with these plans: Are there any prerequisites for using Office Message Encryption? The requirements for using Office Message Encryption are as follows: What does this packaging mean to me? If you already have a subscription for Azure Information Protection for Office , you will get encryption service by default, because Office Message Encryption is included with Azure Information Protection for Office For more information, please visit www.microsoft.com. Related products Active Directory Rights Management Services For customers that wish to deploy an on-premises solution.

Chapter 3 : Security @ Adobe | Announcing the McAfee Data Protection Suite for Rights Management

Foxit PDF Security Suite can be purchased through volume licensing for as little as \$10 per user. A variety of licensing, service and support options are available through Foxit's worldwide.

ConnectedPDF Security - grant and revoke document access. ConnectedPDF Document Management - Track to see who opens your document and what they do and notify readers of new updates. ConnectedPDF Collaboration - Elevate your teamwork with connected reviews or send requests to others to get a file. Documents evolve over time and need to be updated. Paragraph edit and have text flow across multiple paragraphs, columns, and pages. Change the document layout by moving text boxes, changing their size, or how text is justified. Professionalize documents by adding stamps, watermarks, headers, footers, bates number, etc. Often we create new documents from pages of existing documents. Drag and drop pages within a document or from one document to another. Crop, delete, add, swap, flatten, and rotate PDF pages When teams collaborate and share information, they work at their best. Integrate with leading Content Management Systems. Utilize popular storage sharing products. Initiate shared reviews and provide and manage comments. The connected world shares documents in the PDF format. Foxit is the first vendor to deliver PDF 2. Many workflows require information within PDF documents be shared in other file formats. Interfaces with your scanner to scan and convert to PDF. Will convert existing scans i. OCRs image based content into selectable and searchable text. OCR option to make text editable, which is really valuable when updating documents when you only have the hardcopy. Many documents contain confidential information. ConnectedPDF Powered - grant and revoke document access. Permanently remove redact visible text and images from PDF to protect sensitive information. JAWS Job Access With Speech compatibility allowing blind and visually impaired users to read the screen either with a text-to-speech output or by a refreshable Braille. Checks accessibility of PDF files to verify if the document complies with Section technology standards. Identifies and provides fixes for accessibility checker failed results to make the PDF file comply with Section technology standards. PDF editor capabilities available through a web browser, so you have access everywhere, all the time. Bundled with PhantomPDF subscriptions. Bundled with PhantomPDF 1-time purchases for one year and customers who are current on maintenance.

Chapter 4 : Licensing & Pricing “ Enterprise Mobility + Security | Microsoft

When looking for a software that is going to maximize efficiency while minimizing liabilities, one must make sure that the software is capable of managing users, maintaining data records, maintaining security groups, and running security rights reports.

Multi-factor authentication, including biometric scanning for datacenter access. Internal datacenter network is segregated from the external network. Role separation renders location of specific customer data unintelligible to the personnel that have physical access. Faulty drives and hardware are demagnetized and destroyed. Logical security Lockbox processes for a strictly supervised escalation process greatly limit human access to your data. Learn how to activate Lockbox. Servers run only processes that are whitelisted, minimizing risk from malicious code. Dedicated threat management teams proactively anticipate, prevent, and mitigate malicious access. Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access. Data security Encryption at rest protects your data on our servers. Exchange Online Protection provides advanced security and reliability against spam and malware to help protect your information and access to email. User controls Office Message Encryption allows users to send encrypted email to anyone, whatever email service recipients may use. Azure Rights Management prevents file-level access without the right user credentials. Admin controls Multi-factor authentication protects access to the service with a second factor such as phone. Data loss prevention prevents sensitive data from leaking either inside or outside the organization while providing user education and empowerment. Built-in mobile device management capabilities allow you to manage access to corporate data. Mobile application management within Office mobile apps powered by Intune provides granular controls to secure data contained in these apps. Built in antivirus and antispam protection along with advanced threat protection safeguard against external threats. British Airways secures data across mobile devices and operating systems We wanted a safe, secure solution that was cost-effective and ran out-of-the-box on multiple mobile devices and operating systems. Read the paper Top 10 security and privacy features Review the top security and privacy considerations to help you determine the security and trustworthiness of cloud service providers and their services. Find out how this solution helps them detect sensitive data sharing and proactively manage information security risks.

Chapter 5 : Free PDF Editor Download. Edit PDF Files Quickly | Foxit Software

Foxit PDF Security Suite - Overview An important file format for sharing confidential documents that require rights management protection is PDF. It is far more effective for Enterprises to deploy a single rights management solution which supports their most used file formats - typically the Microsoft Office and PDF file formats.

Chapter 6 : Best Digital Rights Management Software | Reviews of the Most Popular Systems

Microsoft Azure AD Premium and Azure Rights Management can help protect your corporate assets: Deliver information protection in the cloud or in a hybrid model with.

Chapter 7 : Pricing - Information Protection | Microsoft Azure

Office is a security-hardened service, designed following the Microsoft Security Development calendrierdelascience.com bring together the best practices from two decades of building enterprise software and managing online services to give you an integrated software-as-a-service solution.

Chapter 8 : Azure Security Center | Cloud Security | Microsoft Azure

DOWNLOAD PDF SECURITY SUITE RIGHTS MANAGEMENT FOR COST

Learn more about Azure Security Center's latest capabilities announced at the RSA conference Understand security state across on-premises and cloud workloads Get a unified view of security across all of your on-premises and cloud workloads.

Chapter 9 : McAfee Data Protection Suite for Rights Management Content Aware and DLP

Get the latest on today's cyberthreats. Register for the Microsoft Security Intelligence Report Volume 23 webcast to gain insights into security trends and find the top ways to protect your organization from destructive cyberattacks.