5 Common File Security Mistakes

vaultize

vaultize

5 Most Common File Security Mistakes

With the rise in workforce mobility, rapid advance of consumerization and BYOD trends and the increasing need to satisfy regulatory, privacy and confidentiality requirements, companies are realizing the need for investing in file security.
Many IT managers/CIO/CISO think that just deploying enterprise digital rights management (DRM aka Information Rights Management or IRM), Data Loss Prevention (DLP), Mobile Device Management (MDM) or Data Protection solutions are enough and their responsibility ends there. Although standalone DRM, DLP and MDM have been of immense value, they just remain as check-boxes on paper - without widespread corporate adoption and acceptance. A well-thought approach to file security makes a big difference in the way that organizations do business, meet compliance requirements, ensure privacy, and protect the digital assets of the company – and, in the era of consumerization, allow end-users to be more productive and efficient.

Mistake 1

Perimeter-based Security is Enough and, Information Systems Security means Information Security

Over a period of time, companies have heavily invested into security products including firewalls, anti-malware, anti-spam and intrusion prevention/detection that protect the corporate network (call it, corporate perimeter) and the systems inside it. This approach to information security is not enough in today's world where data is being increasingly used from devices and systems that are outside the corporate perimeter. Hence, the practice of protecting corporate data through systems security and perimeter-based security measures is now being seen as ineffective in the light of security breaches and corporate data leaks in the recent past. As covered in thinking beyond traditional perimeter-based security, the information needs to be protected by-itself such that the security travels along with the information as it moves across endpoints, across systems, across networks and across users (including people outside the organization). This effectively means that a file always travels within a security envelope that can only be opened by authorized users, from authorized devices and from authorized locations based on access rights defined by the corporate IT and the owner of the file. This is information centric (aka data-centric or content-centric) approach that emphasizes the security of the information itself rather than the security of networks, systems, applications or devices.

Mistake 2

MDM is the Only Solution for BYOD and Enterprise Mobility

With the increase in demand for Bring-Your-Own-Device (BYOD) from employees, many organizations hurriedly implemented MDM. There have been instances where MDM badly failed to meet enterprise IT as well as end-user expectations, thus making implementation of successful MDM for BYOD a challenge. End-users typically do not like IT controlling and monitoring the devices they own and the applications they run. As we covered earlier, the wiser alternative is to secure corporate data (or content) and not the device. Instead of controlling and managing employee-owned devices, the idea should be to deliver and keep the content secure on end-user devices and control its use (within a secure container) to comply with corporate policies like sharing, copy/paste and printing.

5 Most Common File Security Mistakes

Mistake 3

Standalone Rights Management is Enough

Many traditional Digital Rights Management (DRM) vendors only provide tools to convert files into DRM-encrypted versions before sharing them using traditional methods like FTP and email. But, the world has changed. End-users are now getting used to consumer file sharing solutions like Dropbox, OneDrive and Google Drive, which are easy to use and always available.

Security can never be left to end-users. Without having a seamlessly integrated rights management and file sharing solution will have two significant disadvantages: one, end-users will bypass rights management and second, they will resort to consumer solutions – resulting in security, data loss and compliance risks. Hence it is important that you consider a Dropbox alternative with DRM integrated into it.

Mistake 4

DLP and DRM are Two Separate Solutions

Data Loss Prevention (DLP) traditionally started as a way to identify sensitive data (whether in motion, in use or at rest) and perform remediation/enforcement (allow, block or quarantine) based on content classification. Remediation in terms of allowing the data, but with some kind of controls wrapped around the contents, never found a place in DLP vendors' agenda (which is nothing but rights management). On the other hand, enterprise DRM solutions available from various vendors, tried to focus only on DRM-encryption and relied on end-users to apply the protection, without weighing the criticality (or sensitivity) of data and automatically DRM-encrypting only that data.

DRM and DLP are in fact two sides of the same coin. Integration of DRM with content-aware data classification (offered by most DLP vendors including Symantec, McAfee and Websense) is core to a successful IT implementation as it ensures that the information that requires highest security is locked down automatically, while information that does not need securing is not touched.

Mistake 5

Protecting Endpoints through Backup and Encryption completes File Security

People often confuse data protection with security. In fact both are equally important for organizations as they are pro-active measures to ensure that the digital asset of the company are safe all the time. Data protection is more about ensuring that you maintain copies of files (backup) so that you can restore the data following any loss due to inadvertent deletion, disk crash or device loss. Data protection also includes encrypting the on-disk data such that no body other than the owner has access to the data (and data can be remotely wiped) following a device loss. But data protection does not deals with corporate data while it is being accessed, used and shared within as well as outside the organization to ensure that it does not fall into wrong hands resulting in a compliance risk (penalty), loss of reputation and eventual loss to business.

vaultize

sales@vaultize.com