

Data Loss Prevention

Overview

Provides Data Loss Prevention for your organization - regardless of where your employees or your critical information reside. It can scan every file on every PC in your organization to uncover where confidential Data At Rest resides as well as prevent confidential Data In Motion from leaking out (via email / attachments, USB devices, web postings, etc.). In today's increasingly mobile world, where employees and contractors alike demand instant access to corporate assets and confidential information from remote locations, protecting that information can be extremely difficult. Traditional network-based solutions have porous perimeters. Removable media? Webmail? Instant Messaging? All these escape the control of many of our competitors. Thus, they offer only limited "data loss prevention".

Data Loss Prevention is superior because it can identify and protect sensitive information no matter where it's being accessed. It operates preemptively to keep your organization continuously ahead of today's constantly evolving threat landscape. It is installed at the desktop level and reports back over encrypted HTTPS protocols, instead of over the network. This is crucial since it streamlines the process of detecting and blocking any unauthorized attempts to move data outside the organization. Simply put it builds a protective circumference around each computer in your organization, rather than just network traffic. This is more effective and comprehensive in securing your confidential data than network-based solutions.

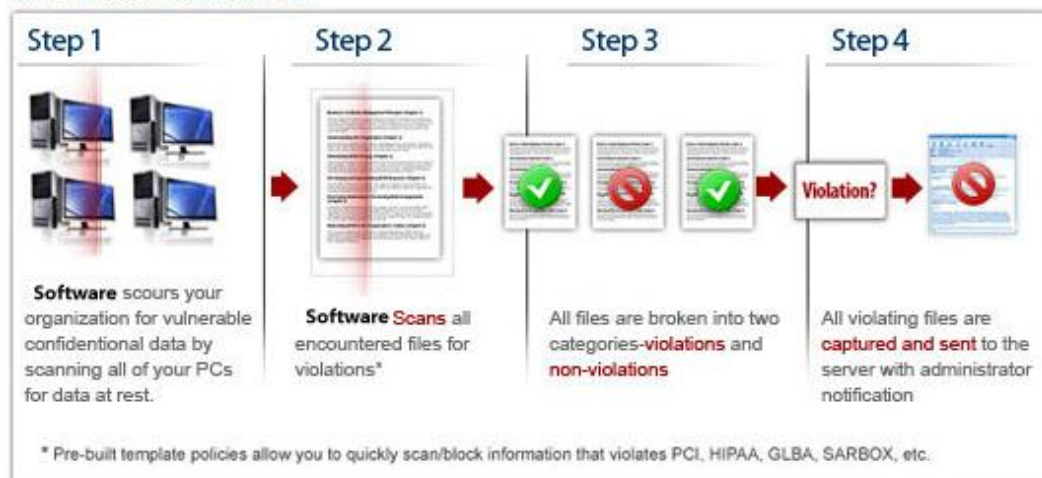
Uncovers your risks by scanning all of the PCs in your organization to show you where confidential information resides (Data At Rest).

Prevents confidential Data In Motion from leaking out of your organization via webmail, attachments, web postings or USB devices.

How Data Loss Prevention Works



How Data at Rest Works



Single Agent Architecture

Single Agent architecture allow you to identify, track, and control who accesses your data, what data they access, and what they can and cannot do with that data. Most importantly, all of this is done with an application that can be deployed and configured in a matter of minutes with a minimum of allocated resources. Other DLP solutions? They can take weeks or months to install, require training courses for policy creation and create significant strains (financial and operational) on the organization.

Confidential data is often lost through errors and oversights, rather than malicious intent. For example, the wrong recipient is mistakenly added to a group email containing sensitive company financial data or customer credit card information. not only blocks the email from getting into the wrong hands, it is also configured to “coach and educate” employees to adopt due care and best practices, as set by your company. It lets users and administrators choose the appropriate tradeoff between a high detection rate on one hand and a low level of false positives on the other.

Removable Media Monitoring & Control

Integrated Removable Media Monitoring and Control strikes the ideal balance between protection of a business’s assets and the efficiency of day-to-day operations. blocks the copying of any file to removable media (USB drive, iPod, external hard drive) based on the file's content, and the employee’s job function. So, an employee’s computer or user profile can be set, using , to allow copying of email, attachments and attempts to write to removable media, but not spreadsheets with confidential company financials. This is much more targeted and so more effective than competitive solutions, which frequently employ an “all or nothing” approach when it comes to removable media.

Easy to Use and Install

Software architecture runs on computers across the organization, even those computers that never connect to the corporate network. can be installed in minutes, without the need for dedicated hardware, and managed centrally from any web browser. It is flexible and scalable. It can operate as on-demand Software as Service, or behind your company’s firewall. makes real-time security decisions to detect and prevent threats to the confidential data inside your organization.