

Data Loss Prevention Best Practices Whitepaper



**ENDPOINT
PROTECTOR** | by CoSoSys

Protecting your entire network



Objective

Data Loss Prevention (DLP) tools have become an essential part of data protection strategies. Highly flexible and adaptable to any company size, DLP solutions can be tailored to different needs and support compliance efforts with new data protection regulations.

This whitepaper outlines the best practices companies should adopt when implementing DLP tools.

Background & Importance of Data Loss Prevention

There are few companies nowadays that do not keep digital records. Everything from accounting to marketing and basic communication happens on a computer and over the internet. This also means that every company, no matter its size, collects digital data including sensitive categories such as personal information regarding employees, customers, or partners that are protected by law.

With a growing number of security breaches and different cybercrimes, with data being mined, monetized, and resold, not only are customers getting more irritated and upset, but these incidents are also causing reputational, financial, and legal damages to companies that mishandle sensitive data.

Therefore in today's world, data security is a vital factor and a major challenge for every organization, underlined by stricter regulations and severe consequences in the case of data loss.

Data Loss Prevention solutions have become a core component of a company's cybersecurity strategy as they help to ensure that sensitive or critical business information does not get outside the corporate network or to a user without access. With DLP software, companies can defend against data theft, loss, and exfiltration as well as make a difference in the process of data protection. By implementing one, it becomes possible to better identify, manage, and protect valuable business information and assets.

A DLP solution comes with several benefits and helps companies to:

Mitigate insider threats

Protect Intellectual Property (IP)

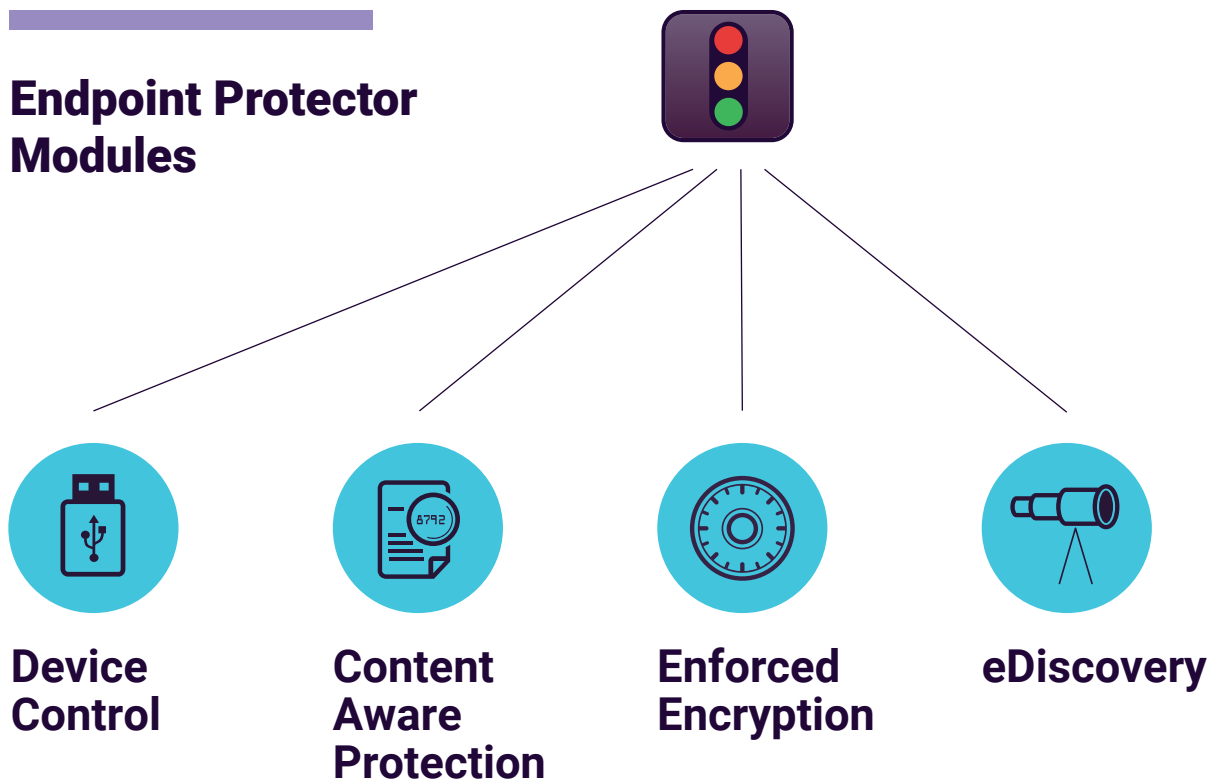
Safeguard customer data

Ensure regulatory compliance

Why Endpoint Protector DLP?

Endpoint Protector by CoSoSys, an award-winning DLP solution, has the objective of helping companies to protect their sensitive data, stopping data leaks and data theft, minimizing insider threats while maintaining productivity, and making work more convenient, secure, and enjoyable.

Endpoint Protector Modules



USB & peripheral port control

Lockdown, monitor and manage devices. Granular control based on vendor ID, product ID, serial number and more.



Scanning data in motion

Monitor, control and block file transfers. Detailed control through both content and context inspection.



Automatic USB encryption

Encrypt, manage and secure USB storage devices by safeguarding data in transit. Password-based, easy to use and very efficient.



Scanning data at rest

Discover, encrypt and delete sensitive data. Detailed content and context inspection through manual or automatic scans.



Endpoint Protector Enterprise

Endpoint Protector Enterprise addresses the complex data protection strategy challenges that enterprises face. By choosing our solution, enterprises can protect sensitive categories of data such as Personally Identifiable Information (PII) or Intellectual Property (IP), mitigate insider threats, and meet the requirements of data protection regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Payment Card Industry Data Security Standard (PCI DSS). Endpoint Protector Enterprise blends security and flexibility, helping to meet the current requirements of data protection at scale. It provides:



Enhanced scalability and flexibility

Ensures protection for ten thousand or more endpoints without impacting productivity. Through the product's granular and flexible policies, the particular needs of every department can be met without having to apply the same policies company-wide.



Cross-platform protection

With Endpoint Protector Enterprise, security policies can be enforced equally in physical and virtual environments. Our multi-OS solution offers protection for Windows, macOS, and Linux endpoints, Thin Clients, and Desktop-as-a-Service (DaaS) platforms.



Seamless integration

Endpoint Protector Enterprise can be easily integrated into the ecosystem of an enterprise and facilitates distributed deployments. The package ensures integration with Active Directory (AD) as well as with SIEM technology.



Zero-day support for macOS

Clients get instant support for new Endpoint Protector features, without any delays or impact on critical workflows, whenever they upgrade to the latest macOS version.



KEXTless agent and Apple-notarized kernel extensions

Endpoint Protector is a pioneer DLP vendor on the market to feature a KEXTless agent and get full support for future macOS versions. More than that, all the other macOS Client versions of Endpoint Protector are notarized under Apple's notarization requirements.



Best Practices to Ensure Data Security

DLP solutions have become an essential part of data protection strategies. Highly flexible and adaptable to any company size, they can be tailored to different needs and support compliance efforts with new data protection regulations such as the GDPR or the CCPA.

We have compiled a list of best practices that will help companies in the DLP selection process and will ensure an efficient data protection strategy.

Identify and monitor sensitive data

Enterprises must identify the type of sensitive data they collect, where it is being stored, and how it is being used by employees. DLP tools come with predefined profiles for sensitive data while also allowing companies to define new profiles based on their own needs. By turning on data monitoring, companies can find out how data flows within and outside their network. It can help them discover vulnerabilities in data handling and bad security practices among their employees.

Implement a cross-platform DLP solution

macOS and Linux are slowly catching up with Windows and organizations should not ignore them when choosing their DLP tools. Cross-platform DLP solutions like Endpoint Protector offer feature parity between Windows, macOS, and Linux which means that sensitive data will have the same level of protection regardless of the operating system a computer is running on. It also allows for all endpoints on the company network to be controlled from the same dashboard.

Set up policies and test them

To control the sensitive data they identify, DLP tools offer companies a wide array of pre-configured-rules and policies that can be enforced across the company network. These can block sensitive data from being transferred via potentially unsecure channels such as messaging apps, file sharing, and cloud services. It can also limit who sensitive data is sent to by email. When it comes to data at rest, DLP solutions allow companies to delete or encrypt sensitive data when it is found on unauthorized computers.



Control what can connect to a company endpoint

Data can be lost not only via the internet but also through the use of removable devices. Companies can use DLP solutions to block USB and peripheral ports on devices or allow only whitelisted devices to connect to them. Enforced encryption can also be a way to ensure that, if a USB is being used, all files transferred to it are automatically encrypted and thus inaccessible to anyone without a password.

Set different levels of authorization

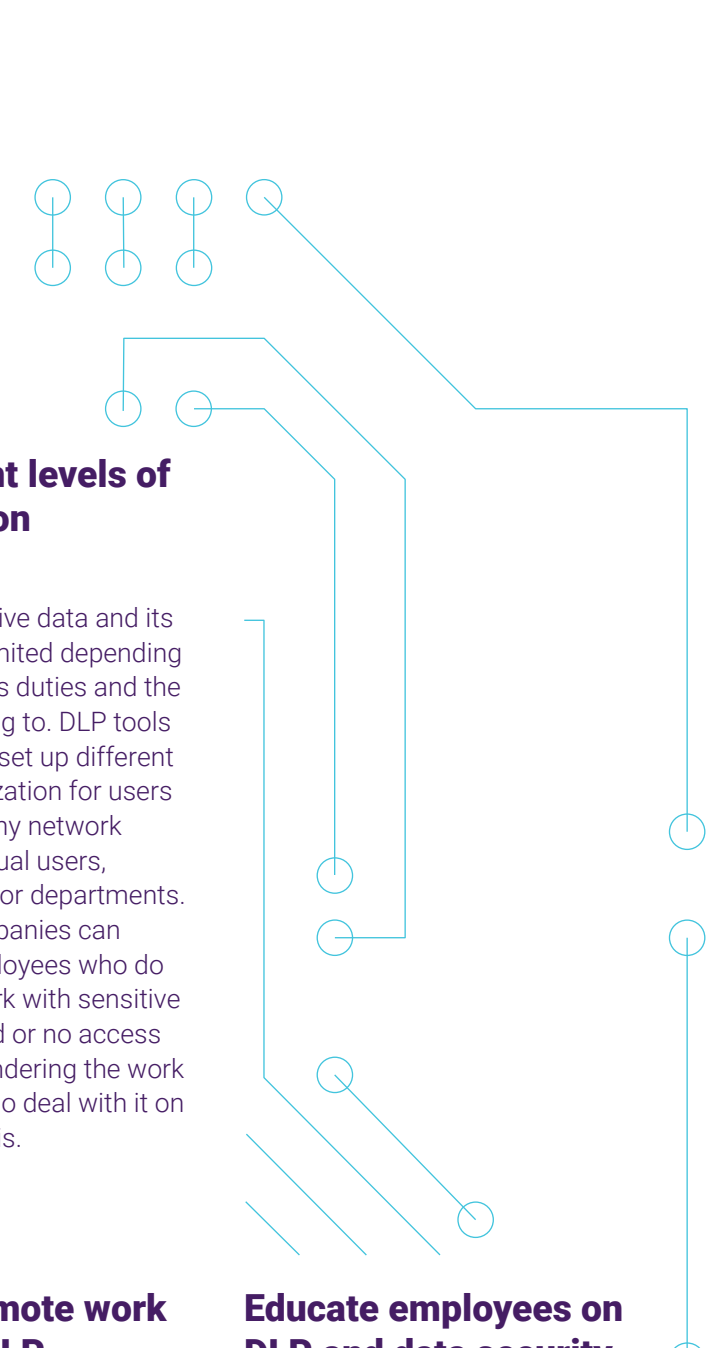
Access to sensitive data and its use should be limited depending on an employee's duties and the group they belong to. DLP tools allow admins to set up different levels of authorization for users across a company network based on individual users, devices, groups, or departments. In this way, companies can ensure that employees who do not normally work with sensitive data have limited or no access to it while not hindering the work of individuals who deal with it on a day to day basis.

Set up a remote work policy for DLP

Many organizations invest heavily in the security of company networks which, once a computer is taken home, can leave the sensitive data stored on it vulnerable to breaches. It is important to set up a remote work policy that includes DLP tools that will work outside the company network and whether a device is online or offline. In this way, they can ensure that data is continually protected, no matter where a company computer travels to.

Educate employees on DLP and data security

It's critical that employees understand the need for DLP tools, the best security practices, and the consequences of a data breach. Enterprises can use the results of DLP data monitoring to raise awareness over bad practices and help employees correct them. An understanding of the importance of DLP can also prevent employees from attempting to circumvent policies and instead report any problems they may be experiencing to admins who can then tweak DLP policies for higher overall efficiency.



Endpoint Protector by CoSoSys User Ratings



Product Capabilities



Integration & Deployment

90%

would recommend
Endpoint Protector

reviewed in the last 12
months



Evaluation & Contracting



Service & Support



Highly-rated in **Gartner Peer Insights** for enterprise data loss prevention solutions.

Conclusion

The number of cyberattacks is increasing every year and with the rising tide of regulations, data protection is a mandatory part of every company's security strategy. Data breaches can be disastrous in themselves and they are often followed by hefty fines, brand damage, and loss of customer trust.

DLP solutions are growing in popularity as organizations are looking for ways to reduce the risks related to sensitive data – including loss, theft, and misuse. For compliance with regulations such as GDPR, CCPA, PCI DSS or HIPAA, mitigation of insider threats, protection of intellectual property and customer data, a best-of-breed DLP solution should be implemented.

By leveraging best practices, companies can seek out a data loss prevention solution that best suits their particular needs and offers greater protection for their valuable assets.



About Endpoint Protector

Endpoint Protector by CoSoSys, is an advanced all-in-one DLP solution for Windows, macOS, and Linux as well as Thin Clients, which puts an end to unintentional data leaks, protects from malicious data theft and offers seamless control of portable storage devices. It's content filtering capabilities for both data at rest and in motion range from predefined content based on dictionaries, regular expressions to profiles for data protection regulations such as GDPR, CCPA, PCI DSS, HIPAA, etc.

EndpointProtector.com

EndpointProtector.com



HQ (Romania)

sales@cososys.com
+40 264 593 110 / ext. 103
+40 264 593 113 / ext. 202

North America

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475

Germany

vertrieb@endpointprotector.de
+49 7541 97826730
+49 7541 97826734 / ext. 202

South Korea

contact@cososys.co.kr
+82 70 4633 0353
+82 20 4633 0354