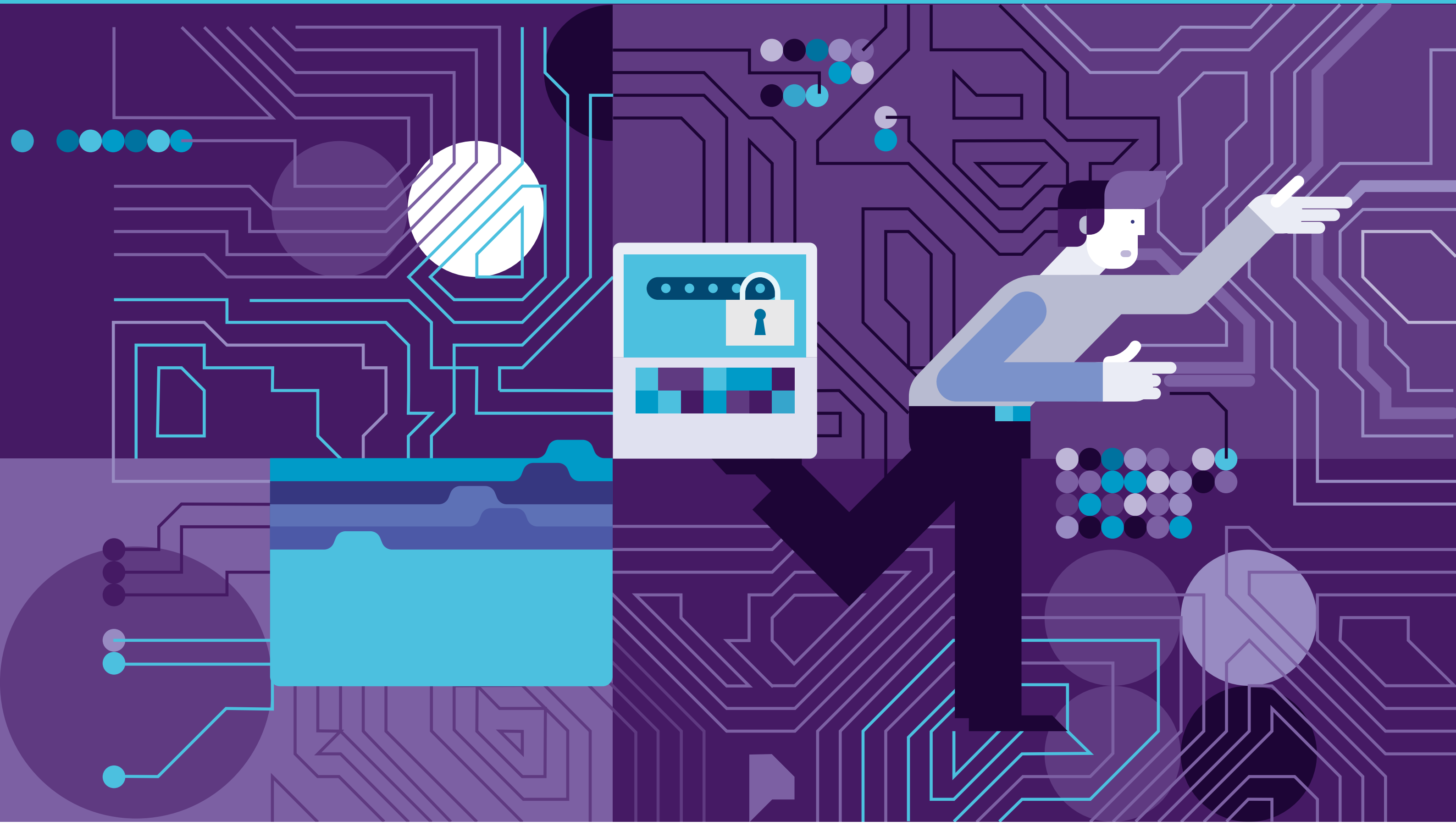
Data Loss Prevention (DLP) **for Technology Companies**

Whitepaper



ENDPOINT PROTECTOR | by CoSoSys

Protecting your entire network

Objective

This whitepaper presents the importance of Data Loss Prevention (DLP) solutions for companies operating within the technology sector. These businesses often store various types of valuable data and are ground zero for cyber-attacks. A proper DLP solution reduces the risk of a data breach, addresses regulatory compliance, and helps mitigating insider threats.

Why do technology companies need a DLP solution?

For companies in the technology sector, intellectual property is often their most valuable asset. Data can also be at the core of what a technology company owns. Besides, these companies are witnessing an explosion in the amount of data they need to protect.

While new technology can be a key enabler, it can also be a key source of vulnerability. With stricter compliance requirements under data protection laws and consumers becoming more aware of how companies use their data, it is essential to ensure that sensitive information is protected.

Sensitive data types for companies in the technology sector

- intellectual property (IP) such as copyrights (source code, designs, arts, databases) and trade secrets (formulas, patterns, processes)
- personally identifiable information (PII), user credentials
- other valuable data such as product roadmaps and employee information

Data Loss Prevention software can protect sensitive data types directly, help with legal requirements and reduce the risk of data loss, data leak, and data theft.

Source code protection

Source code protection is an essential security consideration for technology companies. If it is leaked or stolen, it may give competitors a leading edge in developing new products. Furthermore, malicious outsiders can use it to exploit vulnerabilities within the product. If the company's core value lies in source code or other IP, securing it is paramount to ensure the success, health, and ultimately the future of the business.

Insider threat management

Managing insider threats is also essential for modern technology companies, where collaboration can be central to innovation. Collaboration happens both throughout the organization and with outside partners and vendors. This means an increased number of users with access to sensitive data. Insider threats pose serious business risks to technology companies, whether a result of malicious, negligent, or compromised users.

Compliance with data protection regulations

Many tech firms must comply with different data protection regulations, such as the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Compliance gaps can lead to major penalties and brand damage.

Data security tips for technology companies

Prevent the spread of Shadow IT

Shadow IT or employees using unsanctioned, unofficial apps to get their work done is a problem in normal working conditions. When employees work from home or in hybrid work arrangements it is an even more serious threat to data security. The reason is fairly simple: employees will face new challenges in performing their tasks while working remotely, and they will improvise solutions on the fly, in most cases by using unauthorized apps and software.

Technology companies can prevent the spread of shadow IT by offering a list of approved solutions, especially when employees work remotely. The most widely needed applications are communication-related: video conferencing tools, instant messaging apps, document sharing services, and virtual co-working spaces. By anticipating employees' needs, tech companies can ensure that sensitive data is not uploaded to or processed through potentially dangerous solutions.

Monitor sensitive data at all times

Many companies use DLP tools to protect and monitor sensitive information. However, with more permanent hybrid work arrangements, devices with sensitive data stored on them leave office premises and rely on Virtual Private Networks (VPNs) to connect to company networks. In this way, locally stored data may suddenly become vulnerable.

Companies must check that data protection policies are applied at the endpoint level to ensure that sensitive data is continually protected, whether a device is connected to the internet or not.

Protect all operating systems

Many tech companies run a cross-platform mixed environment not only because of personal preferences but also because they develop applications and solutions that need to run on multiple operating systems.

This means companies must ensure that devices running on all operating systems are connected and protected, primarily when employees work remotely. From VPNs to DLP solutions and videoconferencing tools, they must all function across all operating systems or risk leaving essential personnel outside the company network, with a vulnerable system just waiting to be exploited.

Be vigilant of scams

Companies must remind employees of best security practices and discourage them from clicking on email links from unknown senders or downloading suspicious files. They should also always verify the source of official emails requesting sensitive information and never reveal passwords and login details online.

How does Endpoint Protector help?

Cross-platform protection

Endpoint Protector has been a cross-platform solution from its very inception. It is considered the most trusted DLP solution for macOS on the market, a member of the Linux Foundation, and the only product of its kind to offer and deliver feature parity between Windows, macOS, and Linux. Endpoint Protector can easily be deployed on all operating systems and managed by administrators from a single dashboard, eliminating the need for multiple accounts or control panels.

Efficient source code protection

While many DLP tools struggle to accurately identify programming languages due to the complex libraries needed for it, Endpoint Protector has revolutionized source code detection by implementing N-gram-based text categorization. Thus it identifies programming languages with an accuracy rate as high as 98%. Once you can accurately identify the source code, DLP policies can be efficiently applied to monitor and protect it.

Real-time alerts and reports

A robust DLP solution provides real-time alerts of the protected data and generates reports of policy violations. With incident notifications, companies can ensure real-time control over data flow. Prevention and mitigation of security incidents also become easier.

Reports can be particularly useful for auditing and compliance purposes. They can help tech companies prove that they have functional data protection policies in place that ensure that sensitive information is being kept secure. With Endpoint Protector, it is possible to track, report, and get valuable insights about what sensitive data is being transferred where and by whom.

Protection against client uninstall

The security of the solution itself and the anti-tampering measures are also key features that make a DLP tool complete and effective. Our solution is equipped with different protection mechanisms and security features to ensure continuous data protection, including client uninstall protection and client integrity check.

With these measures, the uninstallation of the Endpoint Protector client by a user can be prevented, even if the user is an administrator for the computer. Furthermore, the client sends an alert to the Endpoint Protector server and notifies the Endpoint Protector administrator about the action.

Granular policies

One of Endpoint Protector’s most attractive features is the dynamic and granular way its policies can be deployed. Admins can set access rights not only on a global level but also based on groups, users, endpoints, or even device type. Settings can also be customized depending on needs, with some computers having different or more rigorous policies enabled.

This high level of flexibility is ideal for networks that require stricter enforcement of DLP policies on certain endpoints, such as computers used for data processing or editing of copyrighted material.

Collaboration security

While collaboration tools are easy to use and can boost productivity, they usually lack the necessary security controls and visibility needed to fulfill an organization's risk management goals.

With Endpoint Protector, companies can better control the movement of sensitive data across popular collaboration software like Microsoft Teams, Slack, Zoom, and Skype. The solution identifies sensitive data across collaboration tools and companies can take action immediately.

Small footprint client

One of the main fears concerning the adoption of DLP tools company-wide is the impact they will have on both the speed of devices they are monitoring and employees’ productivity. Endpoint Protector has a lightweight agent with no performance impact on the protected computers.

Predefined and customizable policies

Endpoint Protector comes with predefined protection policies for the most common sensitive data, such as customer data, and offers companies the possibility to define their custom categories based on their needs. Tech companies can then easily scan a wide variety of file types for the sensitive data they want to protect and ensure that its transfer is monitored and controlled.

Seamless integration

It is important for companies operating within the tech sector to have a seamless experience across security products. Our solution offers Active Directory (AD) and Security Information and Event Management (SIEM) integration.

Endpoint Protector by CoSoSys User Ratings

4.6

Product Capabilities

4.3

Integration & Deployment

86%

would recommend Endpoint Protector

reviewed in the last 12 months

4.6

Evaluation & Contracting

4.8

Service & Support

Gartner peerinsights™

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

Conclusion

Technology companies worldwide trust Endpoint Protector to secure their confidential information while allowing data sharing and supporting innovation. Endpoint Protector safeguards protection for sensitive data such as intellectual property and customer information. It also reduces the risk of insider threats and data loss from malicious, negligent, and compromised users.

About Endpoint Protector

Endpoint Protector by CoSoSys is an advanced all-in-one DLP solution for Windows, macOS, and Linux computers, Thin Clients, and Desktop-as-a-Service (DaaS) platforms. The solution puts an end to unintentional data leaks, protects from malicious data theft, and offers seamless control of portable storage devices. Its content filtering capabilities for data at rest and in motion range from predefined content based on dictionaries, regular expressions to profiles for data protection regulations such as PCI DSS, GDPR, CCPA, HIPAA, etc.

To learn more about the solution, visit our website **EndpointProtector**.com

EndpointProtector.com

COSOSYS

HQ (Romania)

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

Germany

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

North America

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

South Korea

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