Data Loss Prevention (DLP) **for Insurance Companies** Whitepaper

ENDPOINT PROTECTOR | by CoSoSys

Protecting your entire network

Objective

This whitepaper intends to highlight the main reasons why insurance companies need to consider deploying a Data Loss Prevention (DLP) solution, provide data protection best practices, and present the most important features of Endpoint Protector to safeguard sensitive data.

Why Do Insurance Companies Need Data Loss Prevention?

Insurance providers work with sensitive data, which makes them desirable cyber targets. To ensure the safety of customers' personal information and other sensitive data, insurance companies have to follow strict data protection requirements. These requirements oblige companies to implement the best cybersecurity practices or face considerable fines for non-compliance.

Data breaches can be especially damaging to an insurance company's reputation and bottom line. Trust is an essential part of every successful insurance business and, if it is compromised, customers are likely to turn to other companies with better standing.

Human Error

A leading cause of business data loss, human error can take multiple forms such as inappropriate data access, careless data handling, or not adhering to security procedures. Employees can send an email to the wrong person or attach the wrong file to the email; thus, sensitive customer data ending up inadvertently in the wrong hands. They can also have access to data for which they have no need, or in an attempt to complete work quicker, may cut corners and compromise data security.

Data Protection Regulations

Due to the sensitive nature of the data they collect, insurance companies are subject to strict data protection regulations, often more so than other businesses. Under the EU's General Data Protection Regulation (GDPR), a significant chunk of the customer data they need to collect for insurance purposes is part of its special category data. In the US, a lot of insurance data falls under the scope of specialized laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Graham-Leach-Bliley Act (GLBA), or the Sarbanes-Oxley Act (SOX). These regulations bring with them considerable fines in case of non-compliance.

Social Engineering

Beyond regulatory requirements, the insurance industry is one of the most attractive targets for cybercriminals, not only because of the amount of data it collects but also because it opens the door to insurance fraud. These kinds of attacks do not always exploit vulnerabilities within a system but increasingly target careless employees through phishing and social engineering.

Data Protection Tips for Insurance Companies

Protect data on the endpoint

Insurance companies tend to have a very mobile workforce. From insurance inspectors making field visits to sales representatives doing on-site presentations or evaluations, many employees venture outside of the office on business. In today's digitized work environment, when they do, they take their work computers with them and access them remotely. Leaving the security of the company network can spell disaster for data: many data protection tools are applied at the network level and therefore leave devices vulnerable once they are outside it.

The solution is fairly easy: companies must protect data directly on the endpoint. This means that software is installed directly on a computer and ensures security continues wherever a device is physically located. In this way, whether employees connect to a public wireless computer on the go or leave their devices open where third parties have access to them, data protection policies will ensure that sensitive data stays secure.

Protect data on portable devices

Another frequent blind spot of data protection strategies is portable devices. Many data protection strategies focus on internet-based threats and neglect the easy way in which data can be simply copied onto a USB stick, a laptop can be stolen from an employee on his way to a business meeting or a phone can be forgotten in a car or coffee shop.

The best way to protect against this kind of data theft or loss is encryption. By ensuring data on portable devices is always automatically encrypted, that hard drives are encrypted, and that remote wipe and encryption are activated on mobile phones, companies can help mitigate the threat. For portable devices, device control policies can also help block their connection or regulate which devices are allowed to connect to a computer.

Use compliance profiles

Compliance with data protection legislation is a key concern across all sectors these days. This increased need for compliance has prompted the development of data protection policy profiles that make it easier for companies to use tools such as DLP solutions in their compliance efforts. This essentially means that these tools come with tailor-made profiles for specific laws such as GDPR, HIPAA, etc. which allow companies to make the best of their DLP tools without having to go through the process of using legal requirements to build their own policies.

These profiles do not ensure compliance by themselves but significantly contribute to it. Complex cybersecurity frameworks that combine data monitoring, DLP tools, and antivirus software, among others, are needed to reach full compliance, but these profiles make data loss prevention easier to implement as part of data protection strategies.

How Endpoint Protector Safeguards Sensitive Data?

Ensure compliance

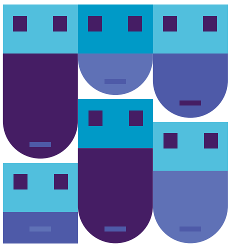
By deploying Endpoint Protector, insurance companies can reach easier the compliance requirements of different data protection regulations such as the GDPR, HIPAA, GLBA, SOX, etc. The solution can discover, monitor, and control sensitive customer data, as well as help to ensure that employees cannot transfer, copy, or upload data classified as personal information under data protection laws.

Predefined policies

With the predefined data protection policies, it is easy to find regulated data and to ensure compliance requirements. Insurance companies also have the possibility of defining their own policies based on data that they specifically collect or is considered sensitive.

Protect customer information

With Endpoint Protector DLP, it is possible to discover, monitor, and remediate a wide variety of sensitive data types, including PII.



Monitor and control peripheral devices

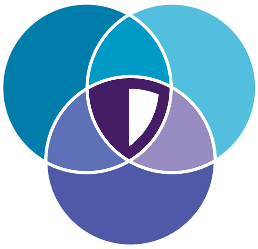
Endpoint Protector DLP comes equipped with a powerful and granular Device Control module that allows insurance companies to limit or block the use of USB and peripheral ports. The solution supports a wide range of device types, including digital cameras, memory cards, smartphones, printers, and many more. By applying policies, only trusted company-issued devices can connect to a computer. Thus not only accidental or intentional data leaks can be prevented, but the risks of USB malware and BadUSB attacks are also minimized.

Discover sensitive information on users computers

The eDiscovery module of Endpoint Protector can discover and identify customer data stored on endpoints, providing data visibility and securing organizations' most valuable data. After identifying customer data, administrators can take remediation actions, including deleting or encrypting files found on unauthorized users' computers.

Protect users in WFH

Endpoint Protector ensures that data protection policies remain in place even when employees work remotely, as it is installed directly on the devices. In this way, policies will stay active no matter where the devices are located.



Cross-platform protection

The solution offers the same security features and level of protection for a computer running on Windows, macOS, or Linux operating systems. All endpoints, no matter their OS, can also be monitored from a single dashboard, making the management of policies a breeze.

Protection in offline mode

Endpoint Protector policies remain active whether a company computer is online or offline, which means sensitive data is controlled and monitored at all times, and logging continues as normal. The data is stored locally, and when a connection is reestablished, logs are automatically sent back to the server.

SIEM integration

Endpoint Protector offers integration with Security Information & Event Management (SIEM) technology, allowing clients to transfer activity events to a SIEM server for analysis and reporting.

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

Working closely with personal data makes companies in the insurance industry vulnerable to both insider and outsider attacks and puts insurers' businesses in jeopardy in case of data leaks, loss, or theft. To ensure the security of customer data and other sensitive information, insurers must comply with various data protection requirements including those imposed by HIPAA, GDPR, SOX, GLBA, and other acts, regulations, and standards. Following such a wide range of requirements can be challenging for insurance providers. A DLP solution can help significantly reduce data protection risks.

With Endpoint Protector DLP, insurance companies can safeguard sensitive customer data directly, meet compliance requirements and ensure that confidential information does not end up in unauthorized hands. The solution efficiently monitors and controls USB and peripheral ports and offers USB encryption options.

About Endpoint Protector

Endpoint Protector by CoSoSys is an advanced enterprise-grade DLP solution for Windows, macOS, and Linux computers, Thin Clients, and Desktop-as-a-Service (DaaS) platforms. The solution efficiently stops unintentional data leaks, protects from malicious data theft, and offers seamless control of portable storage devices. Its 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 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