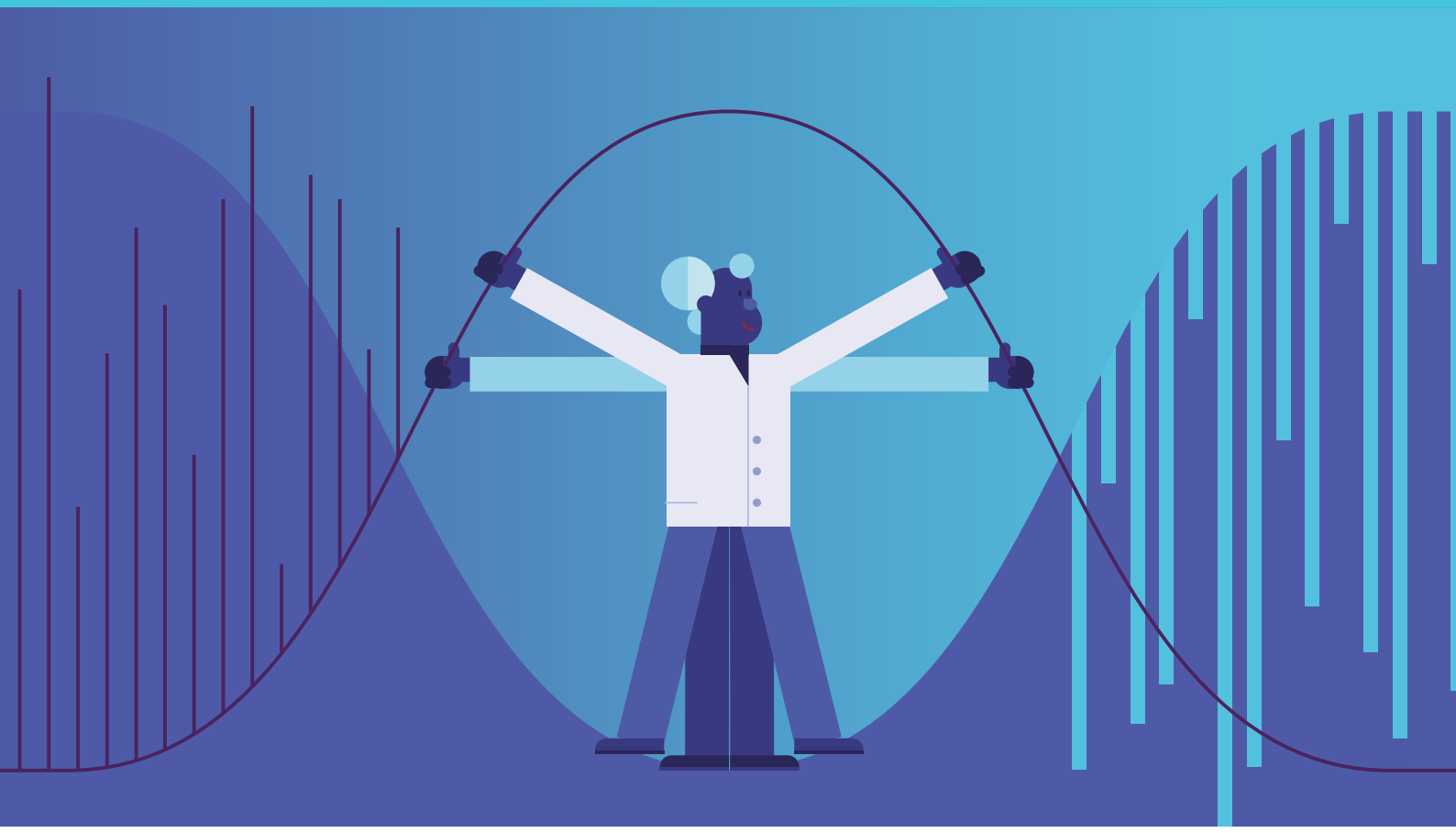
Data Loss Prevention (DLP) **for Healthcare Institutions** Whitepaper



ENDPOINT PROTECTOR | by CoSoSys

Protecting your entire network

Objective

This whitepaper presents the importance of Data Loss Prevention (DLP) solutions for healthcare institutions. As the healthcare sector is among the most affected by data breaches on a global level, it is essential for organizations operating within this sector to ensure the safe handling of data. A proper DLP solution will help address legal requirements and reduce inherent risks related to data security.

Why Do Healthcare Institutions Need a DLP Solution?

Health information is among the most sensitive categories of data. Collected in high volume and often stored on vulnerable systems, health data has become an attractive target for malicious outsiders. The rise in attacks has led to a string of high-profile data breaches worldwide, with healthcare companies bearing the reputational, legal, and financial consequences in their aftermath. Besides outsider threats, healthcare data is also predisposed to insider threats, such as human error, carelessness, and disgruntled employees.

Considered both highly sensitive and very valuable, healthcare information has been heavily regulated for years through specialized laws such as the Health Insurance Portability and Accountability Act (HIPAA). Despite this, healthcare has been incurring the highest average data breach costs for ten years in a row, reaching $7.13 million/breach in 2020, according to the Cost of a Data Breach report 2020 released by IBM and the Ponemon Institute.

Sensitive data types that need to be protected

- Personal Health Information (PHI)
- Patient Financial Information including Payment Card Industry (PCI) data
- Patient Care Data
- Personally Identifiable Information (PII)
- Intellectual Property (IP)
- Claims & Cost Data
- Unstructured Data such as Clinical Data and Patient Behavior Data

Data Security Concerns for Healthcare Institutions

Careless Employees & Human Error

One of the biggest contributors to data breaches in the healthcare sector are employees themselves. Whether it's carelessness on their part as they work with sensitive data or their susceptibility to phishing or social engineering attacks, insiders often pose the highest risk to personal information. Therefore, it is essential that employees receive adequate training that educates them on the best practices of handling sensitive data and the importance, both regulatory and reputational, of following them.

However, when it comes to human error, training is less effective as it implies an unconscious mistake made by an employee. This means it can happen to anyone, regardless of how well-informed they are on the dangers of data breaches. Employees feeling the pressure of a deadline or simply feeling tired or unwell can easily send an email to the wrong person or publicly share a document.

Data Protection Legislation

Specialized legislation such as the HIPAA in the US and the GDPR in the EU makes the protection of health information mandatory by law and puts the burden of responsibility squarely on organizations' shoulders. As non-compliance comes with significant fines, meeting the requirements of data protection laws is a key concern for many healthcare companies. They must research which legislation applies to them and the requirements that they are obligated to follow.

Depending on the geographical location, some of the most important regulations that affect healthcare organizations are:

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- General Data Protection Regulation (GDPR)

Third-Party Security Practices

Many healthcare companies work with contractors and while they might have strong data protection strategies in place, these third parties may not. Legislation like HIPAA and GDPR restrict how personal information can be shared with third parties, with organizations collecting the data still liable in the face of the law in case a data breach occurs. This means that, should a vendor suffer a data breach, fines would be issued not only to the party responsible for it but also to the data controller who had an obligation to protect the data it collected.

Data Protection Best Practices for Healthcare Institutions

Knowing where sensitive data is, who is using it and how

Many healthcare institutions put all their efforts into protecting their networks against outside interference. Still, while this is an essential part of data protection strategies, it is crucial to focus on the sensitive information that attracts these attacks.

By protecting sensitive data directly, organizations guard not only against outside threats, but also malicious insiders and employee carelessness. First, however, healthcare institutions must know where their data is and who has access to it. Data transparency and tools that help healthcare providers closely monitor sensitive data wherever it is found are critical for an effective cybersecurity framework.

Checking third parties' security practices

Healthcare organizations must request that vendors prove that they meet best security practices in line with their own cybersecurity frameworks to ensure that an adequate level of security is in place to protect any data that may be transferred to these third parties for data processing or as part of outsourced services.

Putting together and testing a data breach response plan

Healthcare institutions are being actively targeted, and the bigger the amount of data they collect, the more tempting a target they make for cyberattacks. And while a strong cybersecurity framework based on standards like the CIS Controls can prevent up to 97% of all data breaches, the sad reality is that there is no foolproof plan to prevent all data breaches. Sometimes an employee bypasses security measures out of frustration or someone with high-level access falls for a social engineering attack or a newly discovered vulnerability in software or hardware is exploited before it can be patched. These are unexpected situations that can compromise the most airtight data protection strategy.

Because there is no way of guaranteeing a healthcare organization will not be hit by a data breach, it's important for them to have a data breach response plan in place and test it beforehand to ensure its effectiveness. In this way, employees are prepared for a security incident and know what is expected from them when one occurs.

Reasons Why a DLP is Necessary for Healthcare Institutions

Saving money

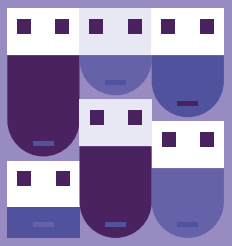
The average total cost of a data breach in the healthcare industry is higher than the cross-industry average according to the *Cost of a Data Breach 2020* report. This essentially means that, besides the loss of patient trust and the damage to a company's public image, there is also a substantial financial price to be paid.
Therefore, it is less costly for healthcare institutions to invest in data protection measures and ensure breaches are avoided than to risk an incident and have to pay the considerable bill associated with it.

Protecting reputation

When an organization fails to live up to the requirements they are legally obligated to follow, it causes a loss of trust in existing patients and generates reluctance in new ones. Individuals are likely to avoid institutions with a proven track record of data breaches.
By applying data protection strategies, healthcare organizations can reassure patients that they take data protection seriously and stay compliant with regulations adopted to protect their personal information.

Offering data visibility

While traditional data protection solutions like antiviruses and firewalls are designed to keep intruders out and are an essential part of any data protection strategy, they do not directly address the need to protect personal information but serve a more general role of protecting an institution's network and all its data. DLP tools are designed to protect special categories of data through predefined or customized policies, finding sensitive data on an institution's network, and monitoring it. In this way, healthcare institutions can have a clear picture of where sensitive patient data is stored and how it is being transferred and used by their employees.



Controlling portable devices

Another blind spot of traditional data protection strategies is related to portable devices, often used as a loophole by both insiders and malicious outsiders. Files can easily be copied onto USBs, for example, and then taken outside of the work environment where they, and the data on them, are extremely vulnerable. External drives, with their high storage spaces, are even more problematic, although more conspicuous than USBs.
DLP tools can block removable devices from being connected to endpoints or permit connection and transfer of files only onto trusted devices such as those issued by healthcare institutions to their staff.

How Endpoint Protector Helps Healthcare Institutions to Secure Their Data?

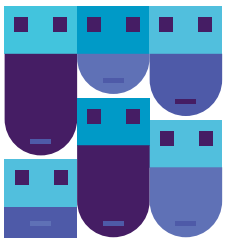
Meeting compliance requirements

Endpoint Protector DLP comes with predefined compliance profiles that address common regulatory use cases, including HIPAA and GDPR. It also offers healthcare organizations the option to build their own policies based on their needs to better protect medical data or intellectual property. The flexible and customizable policies allow healthcare organizations to control and monitor sensitive data within and outside the work environment.

Blocking unauthorized health data transfers

Using powerful contextual scanning and content inspection tools and predefined policies, Endpoint Protector DLP identifies health data in files and in the body of emails before they are sent, blocking their transfer through unauthorized channels.

Most health data is forbidden from leaving an organization's premises without being encrypted or transmitted to secure, authorized channels. This ties into the need to limit data access to a need-to-know basis. Employees, particularly when working from home, may be tempted to use third-party unauthorized apps and services to perform their duties efficiently. They might use popular instant messaging applications, personal emails, cloud storage services, or one-time web transfer services. With the security of these services not tested by healthcare organizations' IT departments, there is a high risk of data leaks.



Controlling removable devices

Endpoint Protector comes with granular device control options which means that organizations can block or limit the use of USB and peripheral ports to authorized company-issued devices. The solution also offers enforced encryption options, ensuring that any data copied onto a USB is automatically encrypted and access to it is restricted to those with a decryption key.

Restricting access to data

One of the many ways health data becomes vulnerable is when it's locally stored on employees' hard drives. Many times these files are used once and forgotten or archived although they should be deleted when no longer needed.

Endpoint Protector DLP can scan data stored locally for healthcare information and when it is identified on unauthorized personnel's computers, remediation actions such as deletion or encryption can be taken. In this way, healthcare organizations can reduce the digital trail of health records and ensure they are only stored where needed.

Monitoring and logging

Endpoint Protector not only controls how health data is transferred and stored but also continually monitors its movements. All attempts to violate a policy are logged. DLP monitoring and logging features allow healthcare organizations to identify weaknesses in their cybersecurity strategies and their employees. By using them, they can save money through more effective training for employees and more cost-effective cybersecurity strategies that address known vulnerabilities.

Health data protection while working remotely

Implemented at the computer level, Endpoint Protector's security policies continue to work whether a computer is connected to a healthcare institution's network or the internet. In this way, healthcare data protection is uninterrupted.

This is especially important now during the COVID-19 pandemic. Although regulations such as HIPAA have been relaxed to allow for remote work, none of their requirements have been waived. It is therefore essential for healthcare organizations to ensure continuous compliance.

Saving time

Endpoint Protector DLP is easy to deploy and manage, offering protection on the endpoint and ensuring that sensitive data is easily monitored and controlled from a single dashboard. Being a cross-platform solution, it guarantees that, whether endpoints are running on Windows, macOS, or Linux, they have the same level of protection.

Remediation actions such as deletion or encryption of sensitive data when it is found on unauthorized users' computers are also available on the dashboard, saving administrators considerable time.

How Endpoint Protector Helps Spectrum of Hope?

Spectrum of HOPE

Spectrum of Hope is a healthcare provider that secures patient and financial data from leakage, loss, and unauthorized transfers with Endpoint Protector by CoSoSys.

“Endpoint Protector adds a strong layer of data security. It is heavily relied upon for keeping our data intact and secure and works well within our current security plan. In addition, CoSoSys customer service is excellent.” says Josh McCown, IT Director at Spectrum of Hope

As a healthcare provider, Spectrum of Hope has to meet strict HIPAA requirements as well compliance with regulations such as the PCI DSS.

"We like its easy management, reporting, and file shadowing features, and how closely it monitors data transfers and simplifies compliance," remarks McCown. “It also has the best reporting system I've seen; it doesn't give extraneous information or random numbers, but understandable timestamps showing who did what and when.“ Endpoint Protector gives McCown the audit capabilities he needs for specific management requests.

”Attachments sent by email, and the potential for files to be shared via external media such as USB, are primary risk vehicles," mentions McCown. "We need to monitor logins, file access, what is done with a file, encrypt documents, protect PCI transactions and keep all data in the network and lock it down."

Why Endpoint Protector?

- Monitors data and file transfers (email, USB, Skype, Outlook, Google Drive, etc.)
- Streamlines compliance
- Blocks unauthorized file transfers
- Intuitive and user-friendly interface

Endpoint Protector by CoSoSys User Ratings

4.6

Product Capabilities

4.3

Integration & Deployment

83%

would recommend Endpoint Protector

reviewed in the last 12 months

4.6

Evaluation & Contracting

4.7

Service & Support

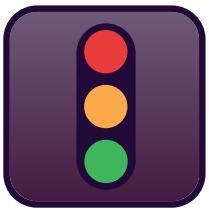
Gartner peerinsights™

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

Conclusion

DLP tools have become an indispensable asset to healthcare institutions that regularly operate large networks full of sensitive data that is often vulnerable to loss or theft due to overworked or careless employees or malicious outsiders.

Being vulnerable to both outsider and insider threats, it is time for healthcare organizations to look beyond minimum compliance requirements and add data security to the top of their priorities list.



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