Data Loss Prevention (DLP) for **Finance & Banking Institutions**

Whitepaper

ENDPOINT PROTECTOR | by CoSoSys

Protecting your entire network

Objective

This whitepaper presents the importance of Data Loss Prevention (DLP) solutions for financial institutions, including a broad range of companies managing financial assets and financial records.

The financial services and technology sector requires reliable security tools to protect sensitive data, such as personally identifiable information (PII) and financial data.

Banks
Credit Card Companies
Insurance Companies
Credit Unions
Investment Funds
Stock Brokerages
Accounting Companies
Consumer Finance Companies
Real Estate Funds
Government related enterprises and others.

Why Do Finance & Banking Institutions Need a DLP Solution?

Banking and financial services collect and process vast amounts of sensitive data daily, making them prime targets for cybercrime and data loss. Besides external threats, financial organizations are also extremely predisposed to internal threats.

Consequently, they are also some of the most heavily regulated organizations when it comes to data protection. International standards and national laws legislate the way financial information is collected, stored, and processed. Companies in this sector must adhere to rigid sets of requirements, otherwise risking monetary and legal penalties, as well as a loss of reputation that can severely impact their bottom lines.

A good DLP solution can protect the data from being leaked, lost, or stolen. For financial institutions, it is an efficient tool in preventing data breaches and avoiding fines, legal problems, and reputational damage. With a comprehensive DLP solution, insider threats are minimized, and compliance with different data protection regulations is easier to achieve.

Compliance with Data Protection Regulations

The importance and sensitivity of the information that financial institutions collect, whether they are banks, insurance companies, or organizations that offer other financial services, has been acknowledged even before the advent of digital records. A push for accountability and transparency has brought about the appearance of laws that regulate how financial information is stored and processed.

The most commonly known rules and regulations that apply to financial institutions:

General Data Protection Regulation (GDPR)
Payment Card Industry Data Security Standard (PCI-DSS)
Gramm-Leach-Bliley Act (GLBA)
Sarbanes–Oxley Act (SOX)

Mitigating Insider Threats

Whether it's falling for a phishing attack, sending confidential data via insecure channels, or bypassing security measures to facilitate their work, employees are at the heart of some of the world's most notorious data breaches.

Top 5 internal data security threats

Social engineering
Data sharing outside the company
Shadow IT
Use of unauthorized devices
Physical theft of company devices

Securing Data in the Age of Work From Home (WFH)

Remote work makes data protection more challenging for organizations, especially for highly regulated industries such as the financial and banking sector. In 2020, the sudden transition from office to home had presented several difficulties to both employees and security, IT, and compliance leaders.

When working remotely, employees aren't at their regular work stations and likely don't have the same equipment. They also have other responsibilities and distractions like childcare and roommates, especially if they work from home.

That's why it's so important that security and IT teams equip employees with the solutions they need to work securely, wherever they are. Financial institutions have previously been reluctant to adopt WFH strategies due to the risk they pose to compliance efforts, but during the extraordinary circumstances caused by the outbreak of the COVID-19 pandemic, they have been forced to reconsider these.

Data Protection Best Practices for Financial Institutions

Safeguard data on the move

Whether it's employees working remotely or third-party vendors that provide essential aspects for financial services organizations, nowadays, sensitive data is often on the move. This is a frequent blind spot in data security strategies, with cybersecurity frameworks focusing on securing data on the company network while overlooking what happens once that data has left office premises.

Therefore, it is important that financial services firms implement data protection solutions that work even if a computer is not connected to the company network. This usually means that they need to be applied at the endpoint level rather than at the network level.

When it comes to third parties, companies must ensure that their vendors have adequate cybersecurity policies in place that will offer the same level of data protection for sensitive data they do. This can be done by making data protection frameworks a mandatory requirement for all vendors.

Don't ignore internal threats

With the biggest threat to sensitive data being considered malicious outsiders, insiders can often be overlooked as sources of risk, although they are among the major causes for data breaches.

An efficient way of mitigating the risk of internal threats is a combination of training and Data Loss Prevention (DLP) tools. Companies need to raise awareness about the dangers of data leaks and their financial and reputational consequences. They also need to educate their employees about the best data protection practices and how they can stay clear of social engineering tactics.

DLP solutions can be used to leverage training efforts by applying effective data protection policies, ensuring sensitive data is not transferred through insecure channels or to unwanted third parties.

Have a response plan

When it comes to cybersecurity, unfortunately, there is no 100% foolproof strategy for ensuring data breaches do not happen. This is why companies must always be prepared in the eventuality, no matter how small, that a data breach might happen to them.

Under most of the new data protection laws, organizations also must notify data protection agencies of any major data breaches, as well as all those affected by the breach. It is therefore essential for companies to put together an incident response plan and test. In this way, if a data breach happens, they can react efficiently, have notification procedures in place, and can quickly recover in its aftermath.

Increase transparency

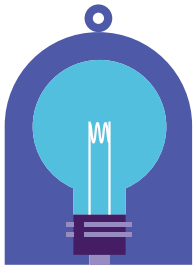
Knowing where your data is and who has access to it is one of the foundations of any successful data protection strategy and an essential part of any compliance efforts. Logging the movements of sensitive data can also offer a significant advantage in the case of auditing or when a company must provide proof of its data protection efforts to regulatory bodies.

DLP and data classification tools can be used to define and identify sensitive data on company networks. Its movements can then be monitored and reported, helping organizations have a better grasp of how sensitive data flows within their systems and where it is most vulnerable.

How Endpoint Protector Helps Financial Institutions to Protect Their Data?

Ensures compliance

Endpoint Protector DLP comes with predefined compliance profiles, addressing common regulatory and IP protection use cases, including international laws and standards such as PCI DSS and local ones such as RBI Cybersecurity Framework.
Banks and financial institutions also have the possibility of defining their own policies based on data that they specifically collect or is considered sensitive in the context of their particular industry.

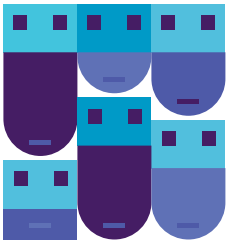


Protects Intellectual Property (IP)

By allowing companies to define what sensitive data means to them and customize policies, Endpoint Protector DLP ensures that security policies can be applied to IP. Once these custom definitions are set up, the solution can search file formats for the defined content, discover intellectual property documents and files, monitor and control their transfer.

Protects customer information

With Endpoint Protector DLP, it is possible to discover, monitor, and remediate over 100 types of sensitive data, including PII and financial data. The solution provides visibility into the entire network and all traffic, including transfers via the internet, to cloud apps and portable storage devices, print screens, and more.
Based on predefined and customizable detection rules, as well as contextual conditions that align with requirements in regulations, Endpoint Protector can automatically discover PII and offer remediation actions to protect it.



Monitors and controls peripheral devices

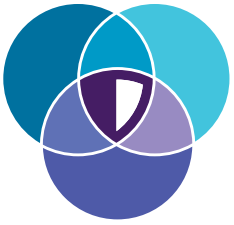
Endpoint Protector DLP comes equipped with a powerful and granular Device Control module that allows companies to limit or block the use of USB and peripheral ports. By applying these policies, only trusted company-issued devices can connect to a computer.
With the Device Control module, banks and financial companies can gain full control of USB devices and peripheral ports. In this way, they can prevent accidental or intentional data leaks and minimize the risks of USB malware and BadUSB attacks. Device security is enforced by granular access rights and easy-to-define policies.

Protects 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.
Policies are applied directly to sensitive data, thus financial companies can easily monitor and control the transfer and use of personal information remotely, ensuring that it is not sent outside the company or uploaded to unauthorized third party services.

Discovers sensitive information

The eDiscovery module of Endpoint Protector can discover and identify regulated data stored on endpoints or hard drives, providing data visibility and securing organizations' most valuable data. After identifying sensitive data such as PII, administrators can take remedietion actions, including deleting or encrypting files found on unauthorized users' computers.



Cross-platform protection

Endpoint Protector has been a cross-platform solution since it was first developed and has earned a reputation as the most trusted DLP solution for macOS on the market. By offering feature parity for Windows, macOS, and Linux, Endpoint Protector ensures that financial organizations get the same level of protection for a computer regardless of the operating system they're running on. All endpoints, no matter their OS, can also be monitored from a single dashboard, making the management of policies a breeze.

Offline protection 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.

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

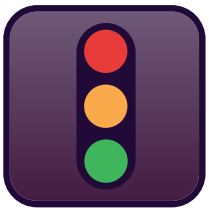
Gartner peerinsights™

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

Conclusion

Security threats for financial services firms can result in significant damages such as fines, legal fees, or lawsuits, as well as in the loss of customer trust. Since the financial sector revolves around trust, a data breach can seriously impact the company's brand and market value.

Major financial services firms, including banking institutions and credit unions, trust Endpoint Protector DLP to safeguard their sensitive data. Endpoint Protector DLP enables financial firms to take full advantage of the performance benefits of mobility, portability, and communications solutions, without compromising security.



About Endpoint Protector

Endpoint Protector by CoSoSys is an enterprise-grade 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 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