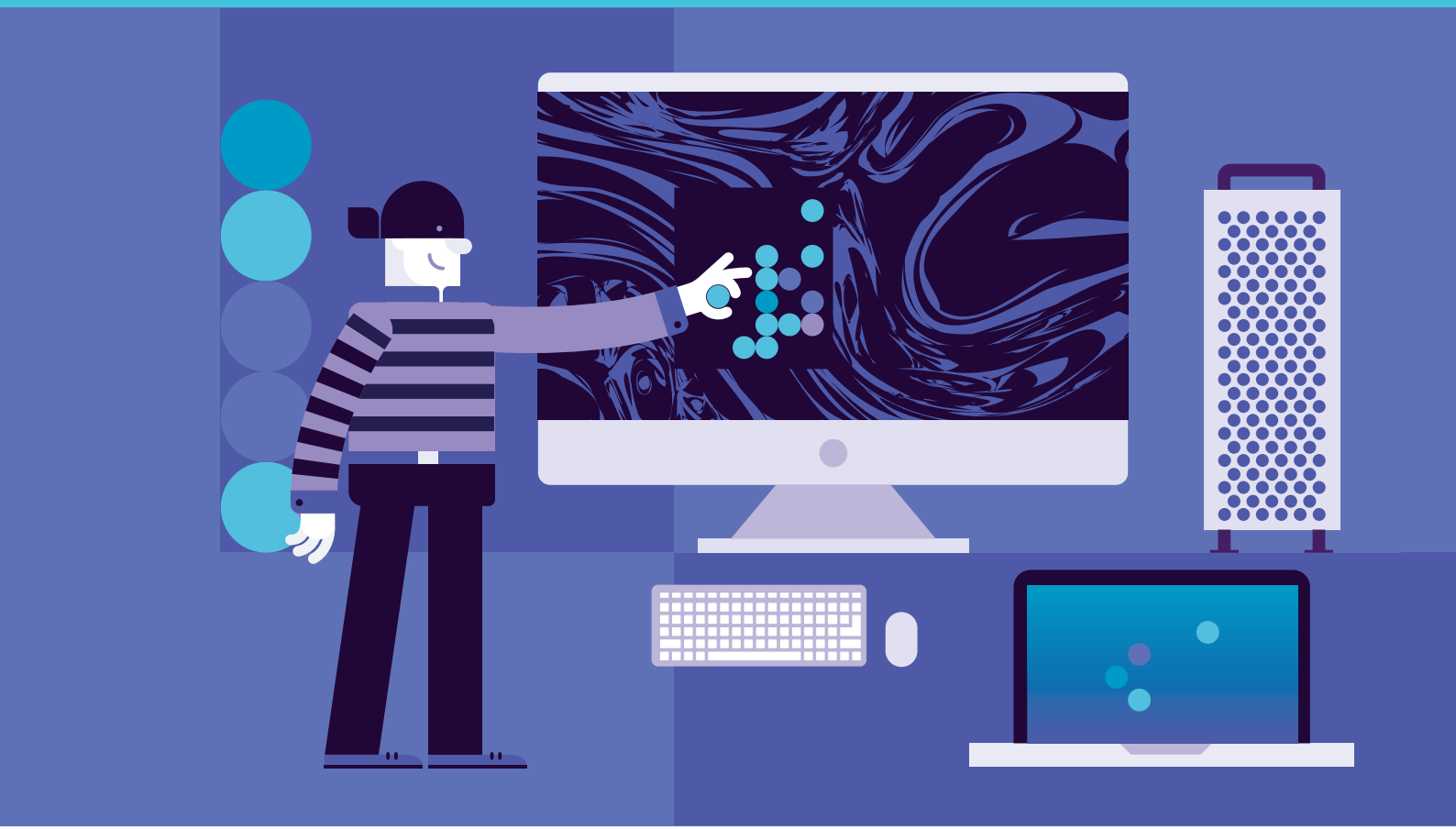
Data Loss Prevention (DLP) for macOS

Whitepaper



ENDPOINT PROTECTOR | by CoSoSys

Protecting your entire network

Objective

In the last two decades, Macs gradually entered the workplace, first as a specialized tool for creatives and, increasingly, as a device of choice in the enterprise. Its rise owes much to the introduction of policies that allowed employees to use their own devices in the workplace or to choose their work technology. Macs are gaining more popularity in the enterprise world and deploying a Data Loss Prevention (DLP) solution on these devices is becoming a pressing question.
This whitepaper outlines the importance of Data Loss Prevention for macOS.

Background & Importance of DLP for macOS

Over the last few years, macOS has gained an increasingly important role in enterprises. Bring-your-own-device (BYOD) and corporate-owned personally-enabled (COPE) policies have made it possible for employees to choose macOS as their preferred operating system. With its solid Unix-based architecture and native encryption options, macOS running devices have long been considered more secure than their Windows running counterparts. And while this makes cyberattacks more difficult, it does not make them impossible. Macs might be more secure against outside threats such as brute force attacks and viruses but are still vulnerable to data loss and data theft by insiders.

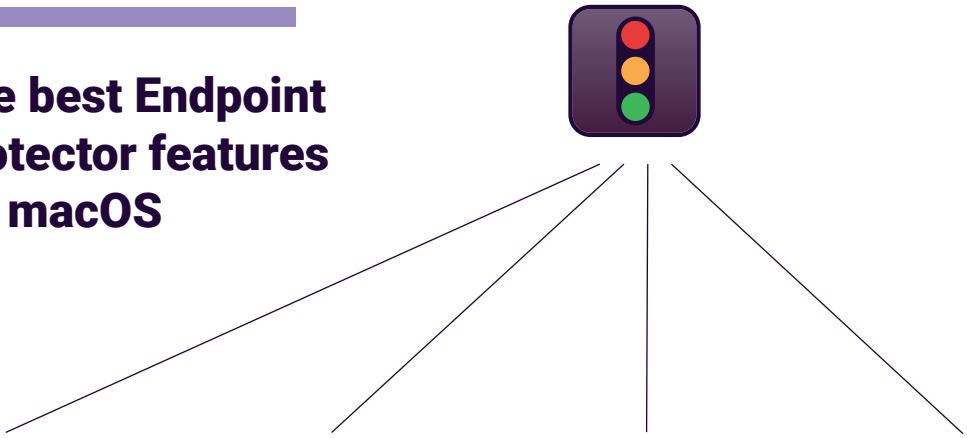
Human error is the third most common cause for data breaches, accounting for 23% of all data breaches.
2020 Cost of a Data Breach Report by Ponemon Institute and IBM Security

Data Loss Prevention (DLP) tools are an essential part of organizations' data protection strategies. Highly flexible and adaptable to any company size, DLP solutions can be tailored to different needs and support compliance efforts with data protection regulations. They help organizations to protect sensitive data such as Personally Identifiable Information (PII) or Intellectual Property (IP) from leaks and theft as well as minimize the risk of insider threats.

The objective of the Endpoint Protector DLP for macOS

When it comes to macOS, few DLP products on the market have shown their commitment to macOS as Endpoint Protector has. A truly cross-platform solution from the very beginning, Endpoint Protector's development team has strived to build a powerful, easy-to-use tool that helps companies protect their data regardless of the operating systems their devices run on. As one of the first DLP tools for macOS on the market, Endpoint Protector quickly became the solution of choice for companies running multi-operating-system networks. It has shown its tireless commitment to macOS over the years by offering zero-day support ahead of the release of all the operating system's major new updates.

The best Endpoint Protector features for macOS



Device Control

Endpoint Protector offers device control options that allow companies to limit, block, and monitor the use of USB ports and connected storage devices. These policies are extremely granular meaning they can be applied to particular computers, users, groups, or entire departments. They also include whitelists and blacklists for increased flexibility and the possibility of defining trusted devices.

USB Enforced Encryption

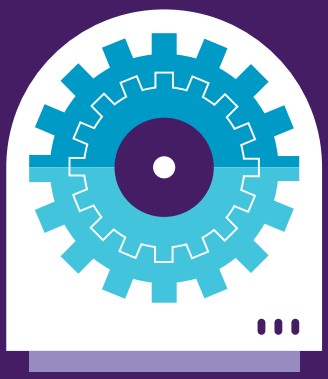
The solution offers the possibility to enforce encryption on USBs connected to a company computer. This means that an encryption solution can be deployed automatically to any trusted USB storage device connected to an endpoint. Once installed, files copied onto USBs will be encrypted with government-approved 256bit AES CBC-mode encryption.

File Tracing and File Shadowing

File Tracing allows companies to monitor data traffic between protected computers and removable devices. It logs transfers and actions taken on files such as renaming, deletion, access, modification, and more. The File Shadowing feature saves a copy of all files that were flagged as violating security policies on the server for additional review.

Protecting Source Code

Endpoint Protector has revolutionized source code detection by implementing N-gram-based text categorization to identify programming languages with an accuracy rate as high as 98%. Once the source code can be accurately identified, DLP policies can be efficiently applied to monitor and protect it.



KEXTless agent and Apple-notarized kernel extensions

When it comes to choosing solutions for Macs, companies must take extra care. Any tools they choose must use the new macOS system extensions as Apple has started deprecating kernel extensions (KEXTs) with the release of macOS Big Sur. The latest version of Endpoint Protector comes with a KEXTless agent built on Apple's new Endpoint Security Framework, making Endpoint Protector a pioneer DLP vendor to release an agent that doesn't use a KEXT. Endpoint Protector's legacy client continues to work on older macOS versions (from macOS 10.8 to macOS 10.15). The legacy macOS client version of Endpoint Protector is notarized under the Apple notarization requirement, which gives users more confidence that the software they download and run has been checked for known security issues.

Zero-day support for macOS

Zero-day support guarantees that a solution will be tested for compatibility with a new macOS version prior to its public release. With Apple rolling out one major macOS upgrade every year and updates on an almost monthly basis, zero-day support is essential for any company using Mac endpoints in the workplace.

Without zero-day support, companies risk not only errors and the dreaded Kernel panics, but a lapse in their data loss prevention strategy. This not only puts their data at risk, but if DLP tools are used as an active part of compliance policies with data protection regulations such as HIPAA, GDPR, PCI DSS etc., it can also lead to noncompliance and steep fines. With Endpoint Protector, companies can confidently allow employees to deploy the latest macOS versions as the solution will already be compatible with them and thus data protection will continue as normal without its security being compromised.

Endpoint Protector Enterprise

Endpoint Protector Enterprise is a DLP package that focuses on the needs of enterprise customers and comes as a response to the requirements and challenges of data protection. The package is an ideal blend of security and flexibility that helps to prevent data loss and data theft in both physical and virtual environments. By opting for this package, enterprises can easily and efficiently identify, monitor, and control sensitive data. They can also consistently govern sensitive data transfers between internal, outsourced workforces, third-party collaborators, and system administrators.

User remediation

Adds more flexibility and security to policies

Seamless integration

With Active Directory (AD) and Security Information & Event Management (SIEM) technology

Management console

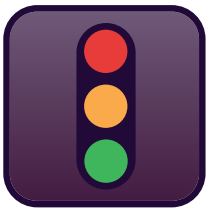
For easier scaling and more flexibility

Conclusion

Endpoint Protector has become the most trusted DLP solution for macOS on the market due to its commitment to evolving its products at the same level across all operating systems it supports. And, through its dedicated macOS team, it ensures compatibility at all times, continually protecting data every time there is an upgrade or new developments in Apple's operating system.

"We have tried many security products, but **Endpoint Protector** is the best of the breed of data loss prevention (DLP) that easily integrates into Apple, Mac and mixed multi-OS environments."

Brian Bloom
CTO, Multipoint Network



About Endpoint Protector

Endpoint Protector by CoSoSys is an advanced Data Loss Prevention (DLP) solution that puts an end to data leaks and data theft while offering control of portable storage devices and ensuring compliance with data protection regulations. It is designed to protect confidential data against insider threats while maintaining productivity and making work more convenient, secure, and enjoyable. An enterprise-grade DLP software, Endpoint Protector is an ideal choice for companies running on multi-OS networks. By deploying it, organizations can safeguard information required by regulations such as the GDPR, HIPAA, CCPA, or PCI DSS.

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