ENDPOINT PROTECTOR | by CoSoSys

DATENBLATT 5.7.0.0

Branchenführende Data Loss Prevention (DLP)

Geeignet für alle Netzwerkgrößen und Unternehmen

DLP für Windows, macOS und Linux

Schutz für das gesamte Netzwerk

ENDPOINT PROTECTOR | by CoSoSys

Unsere fortschrittliche Data Loss Prevention (DLP)-Lösung macht Schluss mit Datenlecks und Datendiebstahl, während sie gleichzeitig die Kontrolle über tragbare Speichergeräte bietet und die Einhaltung von Datenschutzbestimmungen gewährleistet.

Sie wurde entwickelt, um die sensible, geheime oder personenbezogene Daten vor Insider-Bedrohungen zu schützen und gleichzeitig die Produktivität aufrechtzuerhalten und die Arbeit bequemer, sicherer und angenehmer zu gestalten.

Endpoint Protector ist eine DLP-Software der Enterprise-Klasse für Windows-, MacOS- und Linux-Computer, Thin Clients und Desktop-as-a-Service (DaaS)-Lösungen. Die Lösung ist die ideale Wahl für Unternehmen, die in Multi-OS-Netzwerken arbeiten, und verfügt über ein modulares Format, das es ihnen ermöglicht, die richtigen Module für spezifische Anforderungen zu kombinieren und anzupassen.

Durch den Einsatz der Lösung können Unternehmen personenbezogene Daten schützen und Compliance-Anforderungen für Vorschriften wie DSGVO, HIPAA, CCPA, PCI DSS usw. erfüllen. Endpoint Protector bietet auch Schutz für das geistige Eigentum und die Geschäftsgeheimnisse des Unternehmens.

Device Control

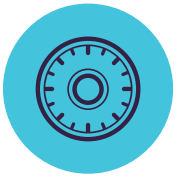
Sperren, steuern und überwachen Sie USB- und Peripherieanschlüsse, um Datendiebstahl und Datenverlust zu verhindern. Legen Sie Rechte pro Gerät, Benutzer, Computer, Gruppe oder global fest.

Windows / macOS / Linux

Content Aware Protection

Überwachen und kontrollieren Sie Daten in Bewegung und entscheiden Sie, welche vertraulichen Dateien das Unternehmen verlassen können und welche nicht. Filter können pro Dateityp, Anwendung, vordefiniertem und benutzerdefiniertem Inhalt, Regex und mehr gesetzt werden.

Windows / macOS / Linux



Enforced Encryption

Sichern Sie auf USB-Speichergeräte kopierte Daten automatisch mit AES-256-Bit-Verschlüsselung. Plattformübergreifend, kennwortbasiert, einfach zu bedienen und sehr effizient.

Windows / macOS

eDiscovery

Scannen Sie die auf den Endpunkten des Netzwerks ruhenden Daten und wenden Sie Abhilfemaßnahmen wie Verschlüsselung oder Löschen an, falls vertrauliche Daten auf nicht autorisierten Computern identifiziert werden.

Windows / macOS / Linux

Wesentliche Vorteile

Leicht zu installieren und zu verwalten

Endpoint Protector kann innerhalb von 30 Minuten einsatzbereit sein. Es ist sowohl von technischem als auch von nicht-technischem Personal leicht zu bedienen.

Vordefinierte Profile zur Erfüllung gesetzlicher Anforderungen

Mit den vordefinierten Datenschutzrichtlinien ist es einfach, zu regulierende Daten zu erfassen und die Einhaltung der Anforderungen von DSGVO , CCPA, HIPAA, PCI DSS und anderen zu gewährleisten.

Plattformübergreifender Schutz

Die Lösung bietet dieselben Sicherheitsmerkmale und dasselbe Schutzniveau für einen Computer mit Windows-, MacOS- oder Linux-Betriebssystem. Sie unterstützt auch Apple Geräte mit Arm-basierten M1 Prozessoren.

Detaillierte Berichte über Benutzeraktivitäten

Mit Endpoint Protector ist es möglich, zu verfolgen, zu berichten und wertvolle Erkenntnisse darüber zu erhalten, welche sensiblen Daten wohin und von wem übertragen werden.

Flexible Bereitstellungsoptionen

Endpoint Protector kann je nach Bedarf und vorhandener Infrastruktur des Unternehmens auf verschiedene Weise eingesetzt werden.

Granulare Richtlinien

Granulare Zugriffsrechte für Wechseldatenträger und Peripherieanschlüsse sowie Sicherheitsrichtlinien für Benutzer, Computer und Gruppen können leicht definiert werden.

DLP für Enterprise und Mittelstand

Im Zeitalter der digitalen Transformation und der Workstream-Collaboration-Plattformen (WSC) sind Risiken von Datenverlusten und Nichteinhaltung von Compliance Vorschriften ein wesentlicher Aspekt für Unternehmen. Die Folge von Datenschutzverletzungen sind nicht nur hohe Geldstrafen, sondern auch rechtliche Probleme und Reputationsschäden. Endpoint Protector Enterprise ist eine der effektivsten Datenschutzlösungen auf dem Markt. Sie ermöglicht es Unternehmen, die Daten, die sie schützen müssen, kontinuierlich zu identifizieren, zu überwachen und zu kontrollieren, egal wo sie sind.

User remediation

Die Endpoint Protector Enterprise-Variante bietet mehr Flexibilität für Sicherheitsrichtlinien. Durch die Funktion User Remediation können Endbenutzer selbst DLP Richtlinien sicher außer Kraft setzen, sodass sie ihre Aktivitäten rechtfertigen können und sensible Datentransfers für eine bestimmte Zeitspanne erlaubt sind.

Management-Konsole

Im zentralisierten Dashboard von Endpoint Protector, welches eine verbesserte Benutzeroberfläche bietet, können leicht DLP Richtlinien für das gesamte Netzwerk erstellt werden.

Nahtlose Integration

Unsere Lösung bietet Active Directory (AD)-Integration, und Security Information & Event Management (SIEM) Technologie Integration. Mit SIEM können die Übertragung von Aktivitätsereignissen an einen SIEM Server zur Analyse zu übertragen. Mit AD können große Deployments vereinfacht werden.

Device Control

für Windows, macOS und Linux

USB-Laufwerke / Drucker / Bluetooth-Geräte / MP3 Player / Externe HDD / Teensy Board / Digitalkameras / Webcams / Thunderbolt / PDAs / Network Share / Fire Wire / iPhones / iPads / iPods / ZIP-Laufwerke / Serielle Ports / PCMCIA Speichergeräte / Biometrische Geräte / UND VIELE MEHR

Individuelle Rechte vergeben

Geräteberechtigungen können global, per Gruppe, Computer, Benutzer und Gerät konfiguriert werden.

Gerätetypen und spezifische Geräte

Erstellen Sie Geräteberechtigungen – Blockieren, Erlauben, Nur Lesen, etc. – für Gerätetypen oder existierende Geräte (anhand VID, PID und Seriennummer).

Benutzerdefinierte Geräteklassen

Für Produkte eines bestimmten Herstellers lassen sich die Zugriffsrechte mit einer eigenen Geräteklasse anlegen.

Außerhalb Geschäftszeiten Richtlinien

Richtlinien für die Gerätekontrolle können so eingestellt werden, dass sie außerhalb der normalen Arbeitszeiten gelten. Die Start- und Endzeit sowie Arbeitstage können festgelegt werden.

Außerhalb des Netzwerks

Außerhalb des Netzwerk-Richtlinien gelten, wenn der Computer sich außerhalb des Unternehmensnetzwerks befindet. Die Durchsetzung ist basierend auf Domain Name und DNS-IP-Adressen.

Active Directory Synchronisierung

Nutzen Sie die Vorteile von AD, um große Verteilungen zu vereinfachen. Halten Sie die einzelnen Objekte wie Benutzergruppen, Computer und Benutzer jederzeit aktuell.

Informationen zu Benutzer und Computer

Erhalten Sie eine bessere Übersicht mit Informationen zu Mitarbeiter-IDs, Teams, Standort,genauen Kontaktdaten und mehr (IP-/MAC-Adressen, etc.).

Datenprotokollierung

Protokolliert alle Datentransfers oder -versuche auf ausgewählte Online-Anwendungen und Cloud-Services und gibt einen Überblick über Nutzeraktivitäten.

Datenmitschnitt

Speichert eine gespiegelte Kopie einer Datei ab, die auf ein kontrolliertes Gerät transferiert wurde. Kann für Auditzwecke verwendet werden.

Offline Temporäres Passwort

Datentransfers auf vom Netzwerk getrennte Computer können vorübergehend erlaubt werden, damit Sicherheit und Produktivität gleichsam gewahrt bleiben.

E-Mail-Benachrichtigungen

Vor- und benutzerkonfigurierte Benachrichtigungen können per e-mail zugestellt werden, um über die wichtigsten Ereignisse bei Datentransfers informiert zu sein.

Dashboard und Grafiken

Mit den Grafiken und Charts erhalten Sie jederzeit einen schnellen Überblick über die wichtigsten Ereignisse und Statistiken.

Reporte und Analysen

Kontrolle der Aktivitäten bei Datentransfers mit einem leistungsstarken Reporte- und Analyse-Werkzeug. Logs und Reporte können exportiert werden.

Transfer Limit

Begrenzen Sie die Anzahl von Dateien oder die Größe von Dateien, die innerhalb eines festgelegten Zeitintervalls übertragen werden. Beziehen Sie Übertragungen über Geräte, online Anwendungen und Netzwerkfreigaben ein oder schließen diese aus.

Enforced Encryption

für Windows und macOS

256-Bit-AES-Government-zugelassene Verschlüsselung / Anti-Manipulationstechniken / Anwendungsintegrität / Nachrichten an Benutzer senden / Zurücksetzen auf Werkseinstellungen / Passwortrichtlinien einstellen / UND VIELE MEHR

USB erzwungene Verschlüsselung

Erlaubt ausschließlich verschlüsselte USB-Geräte und stellt sicher, dass kopierte Daten darauf automatisch geschützt werden.

Automatisch bereitgestellt und schreibgeschützt

Die Bereitstellung kann sowohl manuell also auch automatisch erfolgen. Bietet zudem die Option, schreibgeschützte Rechte zuzulassen, bis eine Verschlüsselung erforderlich ist.

Komplexe Master- und Benutzerpasswörter

Die Kennwortkomplexität kann nach Bedarf festgelegt werden. Das Master-Passwort bietet Kontinuität wie z.B. im Falle des Zurücksetzens eines Benutzerpassworts.

Passwortverwaltung und Fernlöschung

Benutzerkennwörter ferngesteuert ändern und löschen verschlüsselte Daten im Falle von kompromittierten Geräten.

Content Aware Protection

für Windows, macOS und Linux

Email Clients: Outlook / Thunderbird / Lotus Notes / Webbrowser: Internet Explorer / Firefox / Chrome / Safari / Instant Messaging: Skype / Slack / WhatsApp / Cloud-Services & File Sharing: Dropbox / iCloud / OneDrive / BitTorrent / AirDrop / Andere Anwendungen: iTunes / FileZilla / SFTP / Total Commander / Team Viewer / UND VIELE MEHR

Austrittspunkte Denylist

Filter können basierend auf einer Liste festgelegter, überwachter Anwendungen angelegt werden. USB-Speichergeräte, Netzwerkfreigaben und andere Austrittspunkte werden inhaltlich überwacht.

Dateityp Denylist

Blockt bestimmte Dokumente abhängig vom Dateityp, auch wenn die Dateiendung manuell vom Benutzer verändert wurde.

Optische Zeichenerkennung

Prüfen Sie Inhalte von Fotos und Bildern und erkennen Sie vertrauliche Informationen aus gescannten Dokumenten und ähnlichen Dateien.

Individuelle Inhalte Denylist

Filter können auch auf Grundlage eigener Inhalte, wie z.B. Schlüsselwörtern, angelegt und verschiedene Wörterbücher denylistbasiert erstellt werden.

Dateinamen Denylist

Filter basierend auf Dateinamen können anhand von Dateiname und -Endung sowie definiert werden, ebenso nur durch Dateiname oder -Endung.

Speicherort Denylist und Allowlist

Filter basierend auf dem Speicherort der Dateien auf der lokalen Festplatte. Diese können individuell definiert werden, um enthaltene Unterordner ein- oder auszuschließen.

Regular Expressions Denylist

Erweiterte benutzerdefinierte Filter können erstellt werden, um Wiederholungen bei Datentransfers berücksichtigen zu können.

Außerhalb der Geschäftszeiten und Außerhalb des Netzwerk

Definieren und Festlegen von Schutzmaßnahmen, die außerhalb der Geschäftszeiten oder außerhalb des Netzwerks gelten.

Domain & URL Allowlist

Erlaubt allowlistbasiert Firmenportale oder Emailadressen, damit Mitarbeiter bei der Arbeit flexibel bleiben und zugleich die Unternehmen-srichtlinien umgesetzt werden können.

Überwachung Screenshots und Zwischenablage

Sperrt Screenshot-Funktionen und verhindert die Abwanderung sensibler Daten durch Kopieren & Einfügen / Ausschneiden & Einfügen, um die Einhaltung der Datensicherheitsrichtlinie zu verbessern.

User Remediation

Ermöglicht es Benutzern, eine DLP-Richtlinie sicher außer Kraft zu setzen und bietet Optionen zur Rechtfertigung von Datenübertragungen. Erhöht die Verantwortlichkeit der Endbenutzer und das Bewusstsein für sensible Datentranfers in der Organisation.

SIEM Integration

Reichern Sie Ihre SIEM-Plattform mit externen Log-Daten an und stellen Sie ganzheitliche Sicherheitsinformationen über alle Werkzeuge sicher.

Schwellenwerte für Filter

Erweiterte Regeln für die Erkennung von Inhalten. Definieren Sie komplexe Bedingungen für die Überprüfung von Inhalten, indem Sie mehrere Kriterien (PIIs, Wörterbuchwörter, reguläre Ausdrücke usw.) mit logischen Operatoren (UND/ODER) benutzen.

Transfer Limit

Legt ein Übertragungslimit innerhalb eines bestimmten Zeitintervalls fest. Dieser kann entweder auf der Anzahl der Dateien oder der Dateigröße basieren. E-Mail-Benachrichtigungen bei Erreichen des Limits sind individuell einstellbar.

Kontextuelles Scannen von Inhalten

Aktiviert einen erweiterten Prüfmechanismus für eine genauere Erkennung von sensiblen Inhalten wie z.B. personenbezogene Daten. Kontextanpassung ist verfügbar.

Offline Temporäres Passwort

Datentransfers auf vom Netzwerk getrennte Computer können vorübergehend erlaubt werden, damit Sicherheit und Produktivität gleichsam gewahrt bleiben.

Dashboards, Reporte und Analysen

Kontrolle der Aktivitäten bei Datentransfers mit einem leistungsstarken Reporte- und Analyse-Werkzeug. Logs und Reporte können auch in SIEM-Lösungen exportiert werden.

Compliance (DSGVO, HIPAA usw.)

Stellt die Einhaltung der gesetzlichen Regelungen und Vorschriften wie PCI DSS, DSGVO, HIPAA etc. sicher. Vermeiden Sie Bußgelder und andere Strafen.

DLP für Drucker

Richtlinienerstellung für lokale und Netzwerkdrucker, damit vertrauliche Dokumente nicht ausgedruckt werden können.

DLP für Thin Clients

Schützt Daten auf Terminal Servern und verhindert Datenverluste in Thin Client-Umgebungen genauso wie in jedem anderem Netzwerktyp.

eDiscovery

für Windows, macOS und Linux

Dateityp: Grafikdateien / Office Dateien / Archivdateien / Quellcodedateien / Mediendateien / Vordefinierte Inhalte: Kreditkarten / Personenbezogene Informationen / Adressen / Sozialversicherungsnummern / ID / Ausweis / Telefonnummern / Steuer-ID / Krankenversicherungsnummern / Individuelle Inhalte: Dateinamen / Reguläre Ausdrücke / Schlagworte / UND VIELE MEHR

Daten verschlüsseln und entschlüsseln

Ruhende Daten mit vertraulichen Informationen können verschlüsselt werden, um unbefugten Benutzerzugriff zu verhindern. Entschlüsselungsaktionen sind ebenfalls verfügbar.

Daten löschen

Treten klare Verstöße gegen interne Richtlinien auf, können vertrauliche Informationen auf nicht autorisierten Endpunkten erkannt und direkt gelöscht werden.

Speicherort-Scan Denylist

Filter können anhand vordefinierter Speicherorte erstellt werden. Vermeiden Sie redundantes Scannen von ruhenden Daten (data at rest) mit gezielten Inhaltskontrollen.

Automatische Scans

Zusätzlich zu initialen und inkrementellen Scans können Scanvorgänge auch zeitlich geplant werden – entweder einmalig oder wiederkehrend (wöchentlich oder monatlich).

Reporte und Analysen

Kontrolle der Aktivitäten bei Datentransfers mit einem leistungsstarken Reporte- und Analyse-Werkzeug. Logs und Reporte können auch in SIEM-Lösungen exportiert werden.

Scannen-Status

Überprüfen Sie einfach den aktuellen Status Ihres Scans. Der Scan-Status wird im Format 0-100% angezeigt.

Schwellenwerte für Filter

Legt die maximale Anzahl von Regelverstößen fest, bis zu denen Datentransfers noch erlaubt sind. Dies kann für jeden einzelnen Inhalt oder als Summe aller Inhalte definiert werden.

Compliance (DSGVO, HIPAA usw.)

Stellt die Einhaltung der gesetzlichen Regelungen und Vorschriften wie PCI DSS, DSGVO, HIPAA etc. sicher. Vermeiden Sie Bußgelder und andere Strafen.

Dateityp Denylist

Blockt bestimmte Dokumente abhängig vom Dateityp, auch wenn die Dateiendung manuell vom Benutzer verändert wurde.

Vordefinierte Inhalte Denylist

Filter können auf Basis vorkonfigurierter Inhalte erstellt werden, z.B. für Kreditkarten- oder Sozialversicherungsnummern und viele weitere.

Benutzerdefnierte Inhalte Denylist

Filter können auch auf Grundlage eigener Inhalte, wie z.B. Schlüsselwörtern, angelegt und verschiedene Wörterbücher denylistbasiert erstellt werden.

Dateinamen Denylist

Erstellen Sie Filter für Dateinamen, die Festlegung kann wahlweise sowohl auf Dateiname und -Endung als auch auf einer der beiden Werte erfolgen.

Regular Expressions Denylist

Erweiterte benutzerdefinierte Filter können erstellt werden, um Wiederholungen bei Datentransfers berücksichtigen zu können.

Datei Allowlist

Während alle anderen Datentransfers blockiert werden, können allowlistbasiert Ausnahmen definiert werden zur Vermeidung von Redundanzen und zur Erhöhung der Produktivität.

MIME Type Allowlists

Vermeiden Sie redundantes Scannen auf globaler Ebene durch Ausschließen bestimmter Dateiendungen bei Inhaltsprüfungen.

SIEM Integration

Reichern Sie Ihre SIEM-Plattform mit externen Log-Daten an und stellen Sie ganzheitliche Sicherheitsinformationen über alle Werkzeuge sicher.

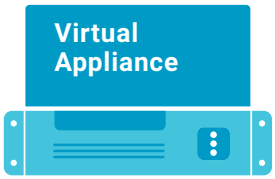
Weitere Funktionen sind verfügbar. Erfahren Sie mehr und fragen Sie eine Demo auf EndpointProtector.de an.

100% Einsatzflexibilität

Unsere Produkte sind für alle Unternehmen geeignet und werden ständig weiterentwickelt, um jede Art von Netzwerk und Branche optimal bedienen zu können. Mit einer Client-Server-Architektur sind sie einfach zu implementieren und werden zentral über die webbasierte Oberfläche verwaltet. Neben einer virtuellen Appliance, kann die Lösung auch bei uns gehostet werden oder in Cloud Infrastrukturen wie Amazon Web Services, Microsoft Azure oder Google-Cloud.

Verschiedene Anmeldeoptionen, einschließlich lokaler Konten, on-premise Active Directory (AD)-Authentifizierung Azure AD und OKTA Single Sign-on (SSO) sind verfügbar und ermöglichen eine einfachere und leichtere Kontrolle für Administratoren. Eine Multi-Faktor-Authentifizierung (MFA) ist ebenfalls möglich.

Device Control, Content Aware Protection, Enforced Encryption und eDiscovery sind für Computer unter verschiedenen Windows-Betriebssystemen, MacOS- und Linux-Versionen und -Distributionen verfügbar.



Virtual Appliance

Cloud Services

Amazon Web Services
Microsoft Azure
Google Cloud

Cloud-Hosted

Gartner peerinsights™

Ausgezeichnet im **Gartner Peer Insights** für Enterprise Data Loss Prevention Lösungen.

Geschützte Endgeräte

Windows	Windows 7 / 8 / 10 / 11	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2019	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS (kext and kextless agent)	Apple Silicon M1		●	●	●	●
	macOS 13.00	Ventura	●	●	●	●
	macOS 12.00	Monterey	●	●	●	●
	macOS 11.00	Big Sur	●	●	●	●
	macOS 10.15	Catalina	●	●	●	●
	macOS 10.14	Mojave	●	●	●	●
	macOS 10.13	High Sierra	●	●	●	●
	macOS 10.12	Sierra	●	●	●	●
	macOS 10.11	El Capitan	●	●	●	●
	macOS 10.10	Yosemite	●	●	●	●
	macOS 10.9	Mavericks	●	●	●	●
	macOS 10.8	Mountain Lion	●	●	●	●
Linux	Ubuntu		●	●	●	n/a
	OpenSUSE / SUSE		●	●	●	n/a
	CentOS / RedHat		●	●	●	n/a
	Fedora		●	●	●	n/a

*Weitere Informationen über unterstützte Versionen und Distributionen finden Sie unter EndpointProtector.de/linux

COSOSYS

Official Partner

North America

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

Germany

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

Romania

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