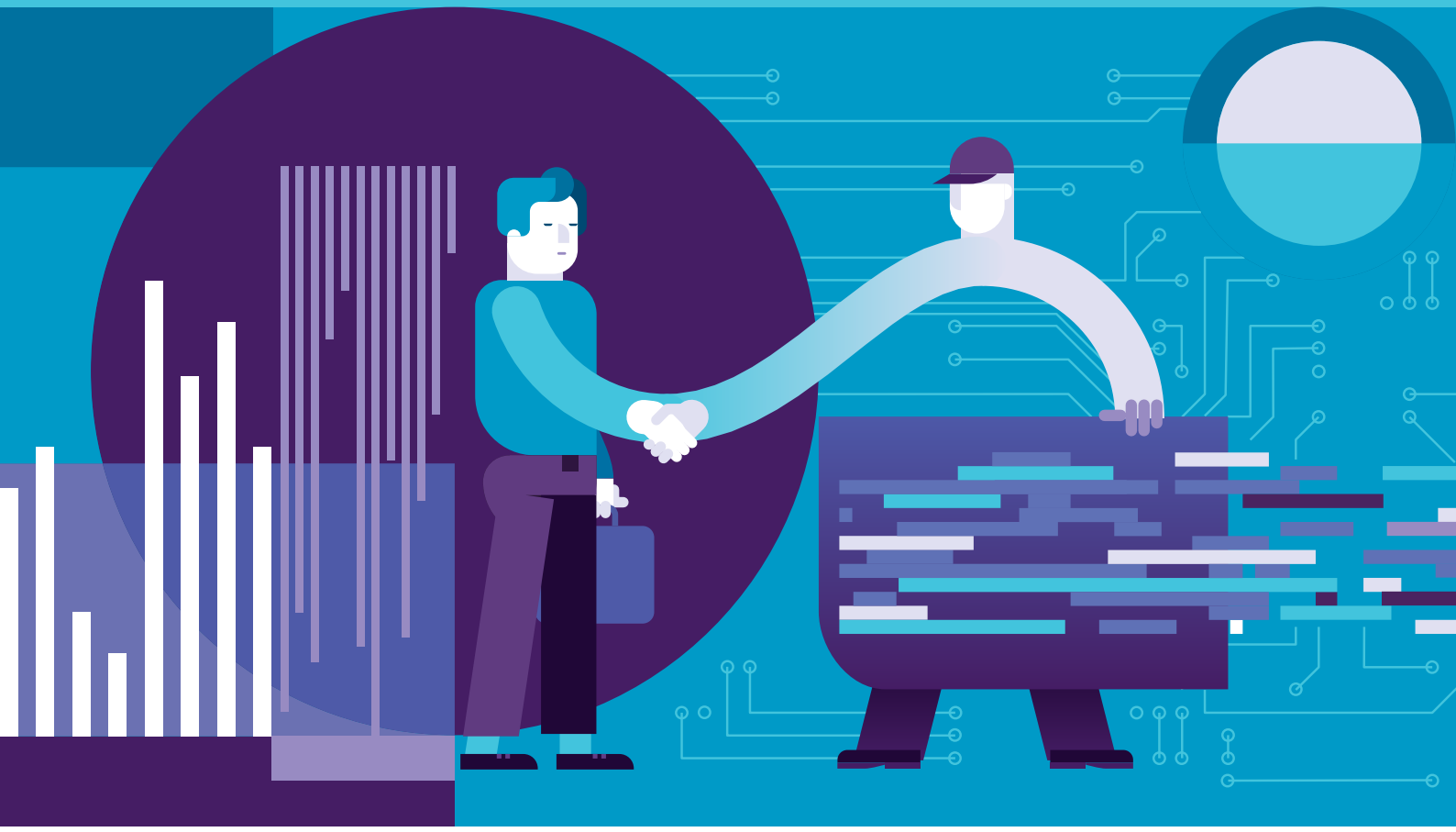
Data Loss Prevention Best Practices

Whitepaper



ENDPOINT PROTECTOR | by CoSoSys

Schützen Sie Ihr gesamtes Netzwerk

Ziele

Data Loss Prevention (DLP)-Tools sind zu einem wesentlichen Bestandteil von Datenschutzstrategien geworden. Hochflexibel und anpassungsfähig an jede Unternehmensgröße, DLP-Lösungen können auf unterschiedliche Bedürfnisse zugeschnitten werden und die Bemühungen um die Einhaltung der neuen Datenschutzbestimmungen und Vorschriften unterstützen.
Dieses Whitepaper skizziert die besten Praktiken, wie Unternehmen bei der Implementierung von DLP-Tools vorgehen.

Hintergrund & Bedeutung von Datenverlust Prävention

Es gibt heutzutage nur noch wenige Unternehmen, die keine digitalen Aufzeichnungen haben. Alles, von der Buchhaltung bis zu Marketing und grundlegender Kommunikation geschieht auf einem Computer und über das Internet. Dies bedeutet auch, dass jedes Unternehmen, unabhängig von seiner Größe digitale Daten sammelt, einschließlich sensibler Inhalte wie persönliche Informationen über Mitarbeiter, Kunden oder Partner, die gesetzlich geschützt sind. Mit einer wachsenden Zahl von Sicherheitsverletzungen und unterschiedlicher Cyberkriminalität, wobei Daten nicht nur abgerufen, monetarisiert und weiterverkauft werden, werden die Kunden immer sensibler und verärgerter. Diese Vorfälle verursachen Reputations-, finanzielle und rechtliche Schäden für Unternehmen, die mit sensiblen Daten unsachgemäß umgehen. Daher ist die Datensicherheit in der heutigen Welt ein entscheidender Faktor und eine wichtige Herausforderung für jede Organisation, unterstützt durch strenge Vorschriften und schwerwiegende Folgen im Falle eines Datenverlusts. Data Loss Prevention-Lösungen sind zu einem Kernbestandteil für die Cyber-Sicherheitsstrategie der Unternehmen geworden, da sie dazu beitragen, dass sensible oder kritische Geschäftsinformationen nicht aus dem Unternehmensnetzwerk gelangen oder an einen nicht berechtigten Benutzer.

Mit DLP-Software können sich Unternehmen auch gegen Datendiebstahl, -verlust und -exfiltration schützen und heben sich dadurch von anderen Unternehmen im Prozess des Datenschutzes ab.

Durch die Implementierung eines solchen Systems wird es möglich, wertvolle Geschäftsinformationen und Vermögenswerte besser zu identifizieren, zu verwalten und zu schützen.

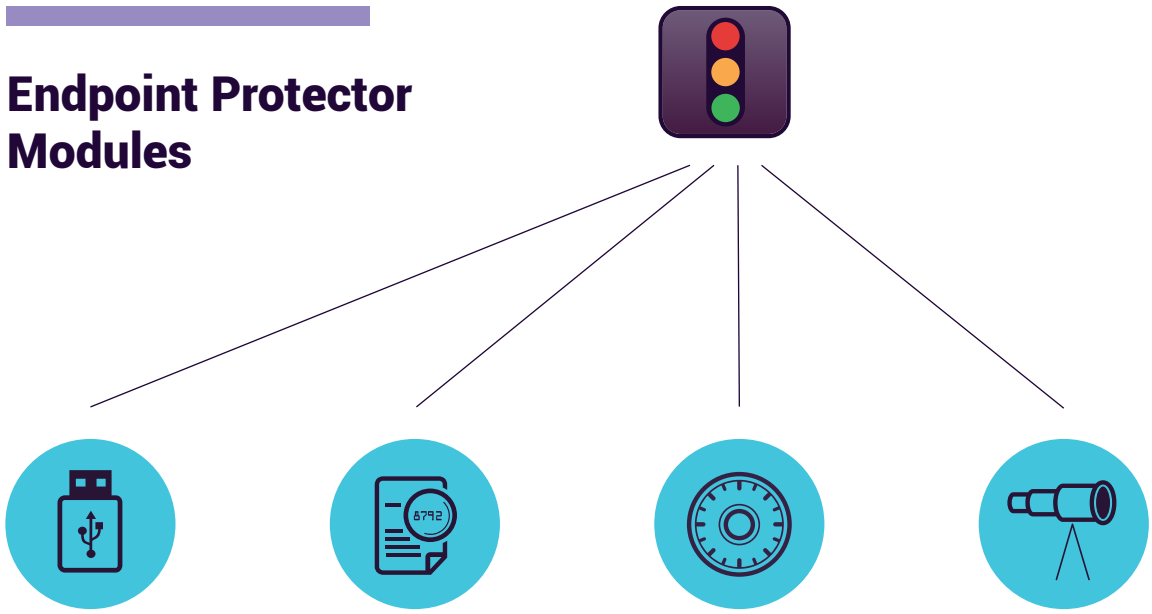
Eine DLP-Lösung hat viele Vorteile und hilft Unternehmen dabei:

- **Insider-Bedrohungen eindämmen**
- **Geistiges Eigentum schützen**
- **Kundendaten schützen**
- **gesetzliche Vorschriften einhalten**

Warum Endpoint Protector DLP?

Endpoint Protector von CoSoSys, eine preisgekrönte DLP-Lösung, hat das Ziel, Unternehmen beim Schutz ihrer sensiblen Daten zu unterstützen, Datenlecks und Datendiebstahl zu verhindern, Insider-Bedrohungen bei gleichzeitiger Aufrechterhaltung der Produktivität zu minimieren und die Arbeit bequemer, sicherer und angenehmer zu gestalten.

Endpoint Protector Modules



Device Control

USB- und Peripherie-Anschluss-Steuerung

Geräte sperren, überwachen und verwalten. Granulare Steuerung auf der Grundlage von Anbieter-ID, Produkt-ID, Seriennummer und mehr.

Content Aware Protection

Scannen von Daten in Bewegung

Überwachen, steuern und blockieren von Dateiübertragungen. Detaillierte Kontrolle durch Inhalts- und Kontextkontrolle.

Enforced Encryption

Automatische USB Verschlüsslung

Verschlüsseln, verwalten und sichern von USB-Speichergeräten durch Schutz der Daten während der Übertragung. Passwortbasiert, einfach zu bedienen und sehr effizient.

eDiscovery

Scannen von ruhenden Daten

Sensible Daten erkennen, verschlüsseln und löschen. Detaillierte Inhalts- und Kontextprüfung durch manuelle oder automatische Scans.

Endpoint Protector Enterprise

Endpoint Protector Enterprise adressiert die komplexen Herausforderungen der Datenschutzstrategie, mit denen Unternehmen konfrontiert sind. Durch die Wahl unserer Lösung können Unternehmen sensible Datenkategorien wie personenbezogene Daten (PII) oder geistiges Eigentum (IP) schützen, Insider-Bedrohungen vermeiden und die Anforderungen von Datenschutzbestimmungen wie der Datenschutz Grundverordnung (DSGVO), dem BSI Grundschutz, dem Informationssicherheitsgesetz (ISO27001), dem VDA Anforderungskatalog, oder dem Payment Card Industry Data Security Standard (PCI DSS) erfüllen. Endpoint Protector Enterprise vereint Sicherheit und Flexibilität und trägt dazu bei, die aktuellen Anforderungen an den Datenschutz in großem Maßstab zu erfüllen. Es bietet:

Verbesserte Skalierbarkeit und Flexibilität

Gewährleistet den Schutz von zehntausend oder mehr Endpunkten ohne Beeinträchtigung der Produktivität. Durch die granularen und flexiblen Richtlinien des Produkts können die besonderen Anforderungen jeder Abteilung erfüllt werden, ohne dass unternehmensweit die gleichen Richtlinien angewendet werden müssen.

Betriebssystemübergreifend

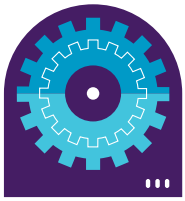
Mit Endpoint Protector Enterprise können Sicherheitsrichtlinien in physischen und virtuellen Umgebungen gleichermaßen durchgesetzt werden. Unsere Multi-Betriebssystem-Lösung bietet Schutz für Windows-, MacOS- und Linux-Endpunkte, Thin Clients und Desktop-as-a-Service (DaaS)-Plattformen.

Nahtlose Integration

Endpoint Protector Enterprise lässt sich leicht in das Ökosystem eines Unternehmens integrieren und erleichtert verteilte Implementierungen. Die Lösung gewährleistet die Integration sowohl mit Active Directory (AD) als auch mit der SIEM-Technologie.

Zero-Day-Support für MacOS

Kunden erhalten bei jedem Upgrade auf die neueste MacOS-Version sofortige Unterstützung für neue Endpoint Protector-Funktionen, ohne Verzögerungen oder Auswirkungen auf kritische Arbeitsabläufe.



KEXTless-Agent und Apple-zertifizierte Kernel-Erweiterungen

Endpoint Protector ist ein DLP-Pionier auf dem Markt, der einen KEXTless-Agenten anbietet und volle Unterstützung für zukünftige MacOS-Versionen erhält. Darüber hinaus werden alle anderen macOS Client-Versionen von Endpoint Protector unter Apples speziellen Anforderungen zertifiziert.

Best Practices zur Erhaltung der Datensicherheit

DLP-Lösungen sind zu einem wesentlichen Bestandteil von Datenschutzstrategien geworden. Sie sind hochflexibel und an jede Unternehmensgröße anpassbar, können auf unterschiedliche Bedürfnisse zugeschnitten werden und unterstützen die Einhaltung neuer Datenschutzbestimmungen wie DSGVO oder CCPA.

Wir haben eine Liste bewährter Verfahren zusammengestellt, die Unternehmen im DLP-Auswahlprozess helfen und eine effiziente Datenschutzstrategie gewährleisten.

Sensible Daten identifizieren und überwachen

Unternehmen müssen erkennen, welche Art sensibler Daten sie sammeln, wo sie gespeichert werden und wie sie von den Mitarbeitern genutzt werden. DLP-Tools werden mit vordefinierten Profilen für sensible Daten geliefert, während sie es den Unternehmen gleichzeitig ermöglichen, neu Profile nach ihren eigenen Bedürfnissen einzurichten. Indem sie die Datenlogging Funktion einschalten, können Unternehmen herausfinden, wie Daten innerhalb und außerhalb ihres Netzwerks fließen. Es kann ihnen helfen, Schwachstellen im Umgang mit Daten und schlechte Sicherheitspraktiken Ihrer Mitarbeiter zu erkennen.

Implementierung einer plattformübergreifenden DLP-Lösung

macOS und Linux holen langsam zu Windows auf und Organisationen sollten sie bei der Auswahl ihrer DLP-Tools nicht ignorieren. Plattformübergreifende DLP-Lösungen wie Endpoint Protector bieten eine Funktionsparität zwischen Windows, MacOS und Linux, was bedeutet, dass vertrauliche Daten unabhängig vom Betriebssystem, auf dem ein Computer läuft, gleichwertig geschützt sind. Darüber hinaus können alle Endpunkte im Unternehmensnetzwerk über dasselbe Dashboard gesteuert werden.

Richtlinien erstellen und testen

Um die sensiblen Daten, die sie identifizieren, zu kontrollieren, bieten DLP-Tools Unternehmen eine breite Palette von vorkonfigurierten Regeln und Richtlinien, die im gesamten Unternehmensnetzwerk durchgesetzt werden können. Diese können verhindern, dass sensible Daten über potenziell unsichere Kanäle wie Messaging-Anwendungen, die gemeinsame Nutzung von Filesharing- und Cloud-Diensten übertragen werden. Sie können auch einschränken, an wen sensible Daten per E-Mail gesendet werden. Wenn es um ruhende Daten geht, können Unternehmen mit DLP-Lösungen sensible Daten löschen oder verschlüsseln, wenn sie auf nicht autorisierten Computern gefunden werden.

Kontrollieren, was über die Schnittstellen eines Endpunkts verbunden werden kann

Daten können nicht nur über das Internet, sondern auch durch den Einsatz von Wechseldatenträgern verloren gehen. Unternehmen können DLP-Lösungen verwenden, um USB- und Peripherieanschlüsse an Geräten zu blockieren oder nur den Anschluss von bestimmten Geräten auf der Whitelist zuzulassen. Eine erzwungene Verschlüsselung kann auch ein Weg sein, um sicherzustellen, dass bei Verwendung eines USB-Geräts alle an dieses Gerät übertragenen Daten automatisch verschlüsselt werden und somit für jedermann ohne Passwort unzugänglich sind.

Verschiedene Berechtigung vergeben

Der Zugang zu sensiblen Daten und deren Verwendung sollte je nach den Aufgaben eines Mitarbeiters und der Gruppe, der er angehört, eingeschränkt werden. DLP-Tools ermöglichen es Administratoren, verschiedene Berechtigungsebenen für Benutzer in einem Unternehmensnetzwerk einzurichten, die auf einzelnen Benutzern, Geräten, Gruppen oder Abteilungen basieren. Auf diese Weise können Unternehmen sicherstellen, dass Mitarbeiter, die normalerweise nicht mit sensiblen Daten arbeiten, nur begrenzten oder gar keinen Zugang zu diesen Daten haben, während sie gleichzeitig die Arbeit der Personen, die täglich mit diesen Daten zu tun haben, nicht behindern.

Einrichten einer Richtlinie für DLP

Viele Organisationen investieren stark in die Sicherheit von Firmennetzwerken, die, sobald ein Computer außerhalb des Netzwerks z. B. im Homeoffice genutzt wird, die darauf gespeicherten sensiblen Daten anfällig für Verletzungen machen können. Es ist sehr wichtig, Richtlinien für die Arbeit aus dem Home-Office einzurichten, die DLP-Tools umfasst, die außerhalb des Unternehmensnetzwerks funktionieren und unabhängig davon, ob ein Gerät online oder offline ist. Auf diese Weise können sie sicherstellen, dass die Daten kontinuierlich geschützt sind, unabhängig davon, wohin ein Firmencomputer mitgenommen wird.

Mitarbeiter für DLP und Datensicherheit sensibilisieren

Es ist von entscheidender Bedeutung, dass die Mitarbeiter den Bedarf an DLP-Tools, die besten Sicherheitspraktiken und die Folgen eines Datenverstoßes verstehen. Unternehmen können die Ergebnisse der DLP-Datenüberwachung nutzen, um das Bewusstsein für Achtsamkeit im Umgang mit sensiblen Daten zu schärfen und die Mitarbeiter bei deren Korrektur zu unterstützen. Ein Verständnis für die Bedeutung von DLP kann auch verhindern, dass Mitarbeiter versuchen, Richtlinien zu umgehen, und stattdessen alle Probleme, auf die sie stoßen könnten, an Admins melden, die dann die DLP-Richtlinien für einen besseren Gesamtschutz optimieren können.

Endpoint Protector by CoSoSys Benutzer Bewertung

4.6

Funktionalität

4.5

Integration und Installation

90%

würden Endpoint Protector empfehlen

Rückblickend auf die letzten 12 Monate

4.6

Beratung & Verträge

4.3

Sevice & Support

Gartner peerinsights™

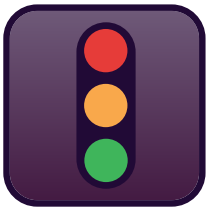
Highly-rated in **Gartner Peer Insights** for enterprise data loss prevention solutions.

Fazit

Die Zahl der Cyberangriffe nimmt von Jahr zu Jahr zu und mit der zunehmenden Flut von Vorschriften ist der Datenschutz ein obligatorischer Bestandteil der Sicherheitsstrategie jedes Unternehmens. Datenschutzverletzungen können katastrophale Folgen haben und ziehen oft hohe Geldstrafen, Reputationsschäden und den Verlust des Kundenvertrauens nach sich.

DLP-Lösungen erfreuen sich immer größerer Beliebtheit, da Organisationen nach Möglichkeiten suchen, die Risiken im Zusammenhang mit sensiblen Daten - einschließlich Verlust, Diebstahl und Missbrauch - zu verringern. Für die Einhaltung von Vorschriften wie DSGVO, IT Grundschutz etc. zur Minderung von Insider-Bedrohungen, zum Schutz von geistigem Eigentum und den Schutz der Kundendaten sollte eine optimale DLP-Lösung implementiert werden.

Durch die Nutzung bewährter Verfahren können Unternehmen nach einer Lösung zur Vermeidung von Datenverlusten suchen, die ihren speziellen Anforderungen am besten gerecht wird und einen besseren Schutz ihrer wertvollen Vermögenswerte bietet.



Über Endpoint Protector

Endpoint Protector von CoSoSys, ist eine fortschrittliche All-in-One DLP-Lösung für Windows, MacOS und Linux sowie Thin Clients, die unbeabsichtigten Datenlecks ein Ende setzt, vor böswilligem Datendiebstahl schützt und eine nahtlose Kontrolle über tragbare Speichergeräte bietet. Die Filterung reicht von Inhalten, die auf Wörterbüchern und regulären Ausdrücken basieren, bis hin zur Filterung nach Datenschutzbestimmungen wie DSGVO, CCPA, PCI DSS, HIPAA usw.

EndpointProtector.de

EndpointProtector.de

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