ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.5.0.0

Líder da indústria de Prevenção Contra Perda de Dados (DLP)

Solução de segurança de nível empresarial para qualquer setor

DLP para Windows, macOS e Linux

Protegendo a rede inteira

ENDPOINT PROTECTOR | by CoSoSys

Solução avançada de Prevenção Contra Perda de Dados (DLP) que põe fim a vazamentos e roubo de dados enquanto oferece controle de dispositivos de armazenamento portáteis e garantindo conformidade com os regulações de proteção de dados.

Ele foi projetado para proteger dados confidenciais contra ameaças internas, mantendo a produtividade e tornando o trabalho mais conveniente, seguro e agradável.

O Endpoint Protector é um software DLP de nível corporativo para computadores Windows, macOS e Linux, Thin Clients e soluções de Desktop como Serviço (DaaS). A solução é a escolha ideal para empresas que operam em redes com vários sistemas operacionais e possui um formato modular que lhes permite combinar as ferramentas certas para atender a necessidades específicas

Ao implantá-lo, as organizações podem proteger as informações pessoais e atender aos requisitos de conformidade para regulamentos como o LGPD, GDPR, HIPAA, CCPA, PCI DSS, etc. Endpoint Protector também oferece proteção para a propriedade intelectual e segredos comerciais da empresa.

Controle de Dispositivos

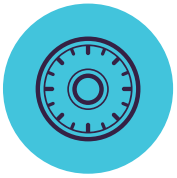
Bloqueie, controle e monitore as portas USB e periféricos para impedir roubo e perda de dados. Defina direitos por dispositivo, usuário, computador, grupo ou globalmente.

Windows / macOS / Linux

Proteção de Conteúdo

Monitore e controle dados em movimento, decidindo quais arquivos confidenciais podem (ou não) deixar a empresa. Filtros podem ser definidos por tipo de arquivo, aplicação, conteúdo pré-definido, conteúdo personalizado, Regex e muito mais.

Windows / macOS / Linux



Criptografia Forçada

Proteja automaticamente dados copiados em dispositivos de armazenamento USB com criptografia AES de 256 bits. Multiplataforma, baseado em senha, fácil de usar e muito eficiente.

Windows / macOS

eDiscovery

Analise os dados em repouso nos endpoints da rede e aplique ações de correção, como criptografar ou excluir, caso de dados confidenciais que sejam identificados em computadores não autorizados.

Windows / macOS / Linux

Principais Benefícios

Fácil de instalar e gerenciar

O Endpoint Protector pode estar em funcionamento em 30 minutos. É fácil de operar tanto por pessoal técnico como não técnico.

Perfis de conformidade pré-definidos

Com as políticas de proteção de dados pré-definidas, é fácil encontrar dados regulamentados e garantir os requisitos de conformidade da LGPD, GDPR, CCPA, HIPAA, PCI DSS e muito mais.

Proteção multiplataformas

A solução oferece os mesmos recursos de segurança e nível de proteção para um computador executando o sistema operacional Windows, macOS ou Linux.

Relatórios detalhados de atividadedo usuário

Com o Endpoint Protector, é possível rastrear, relatar e obter informações valiosas sobre quais dados confidenciais estão sendo transferidos para onde e por quem.

Opções flexíveis de implantação

O Endpoint Protector pode ser implantado de várias maneiras, dependendo das necessidades e da infraestrutura existente na empresa.

Políticas granulares

Direitos de acesso granular para dispositivos removíveis e portas periféricas, bem como políticas de segurança para usuários, computadores e grupos, podem ser facilmente definidos.

DLP para Ambiente Corporativo

Na era da transformação digital e plataformas de colaboração de fluxo de trabalho (Ex.: Teams, Slack etc), abordar os riscos de perda de dados e o a adequação às leis é uma obrigação para as empresas, pois as consequências das violações de dados incluem não apenas multas pesadas, mas também problemas legais e danos à reputação. O Endpoint Protector Enterprise traz a solução de segurança de dados mais eficaz do mercado, permitindo às empresas identificar, monitorar e controlar continuamente os dados que eles precisam proteger, onde quer que estejam.

Remediação pelo Usuário

A opção de Endpoint Protector Enterprise adiciona mais flexibilidade às políticas de segurança. Por meio do recurso de remediação pelo usuário, os usuários finais podem se autocorrigir, o que significa que, após justificar sua atividade, a transferência de informações confidenciais específicas é permitida por um determinado período de tempo.

Console de gerenciamento central

As políticas de prevenção de perda de dados podem ser facilmente definidas para toda a rede a partir do painel centralizado do Endpoint Protector, que oferece uma experiência de usuário aprimorada.

Integração perfeita

Nossa solução oferece integração com Active Directory (AD) e tecnologia de gerenciamento de informações e eventos de segurança (SIEM). A integração com o SIEM permite a transferência de eventos de atividade para um servidor SIEM para análise e geração de relatórios. Com o AD, grandes implantações podem ser mais simples.

Controle de dispositivos

para Windows, macOS e Linux

Drives USB / Impressoras / Dispositivos Bluetooth / CD e DVD / HDDs externos / Teensy Board / Câmeras digitais / Webcams / Thunderbolt / WiFi / Compartilhamento de rede / FireWire / iPhones / iPads / iPods Drives ZIP / Leitores de cartões / Smartphones Android / Modems USB / OUTROS

Definir Direitos Granularmente

Direitos do dispositivo podem ser configurados globalmente, por grupo, computador, usuário e dispositivo. Use as configurações padrão ou ajuste conforme necessário.

Tipos de Dispositivos e Dispositivos Específicos

Definir direitos - negar, permitir, somente leitura, etc. Os direitos podem ser aplicados a um tipo de dispositivo ou podem ser específicos do dispositivo (com base no VID, PID e Número de Série).

Classes personalizadas

Aplique direitos de dispositivo com base no ID do Fornecedor e no ID do produto para facilitar o gerenciamento de dispositivos do mesmo fornecedor.

Políticas Fora do Horário de Funcionamento

Políticas de Controle de Dispositivo podem ser definidas para serem aplicadas fora do horário normal de trabalho. O horário comercial de início e término e os dias úteis podem ser definidos.

Políticas de Rede Externas

As políticas de rede externa podem ser definidas para serem aplicadas fora da rede da empresa. A aplicação é baseada nos endereços IP do FQDN e do DNS.

Sincronização do Active Directory

Aproveite o AD para simplificar grandes implantações. Mantenha as entidades atualizadas, refletindo os grupos de rede, computadores e usuários.

Informações sobre usuários e computadores

Obtenha melhor visibilidade com informações como IDs de Funcionários, Equipes, Localização, detalhes de contato precisos e muito mais (IPs, endereços MAC, etc.)

Rastreamento de Arquivo

Grave todas as transferências ou tentativas de arquivo para vários dispositivos de armazenamento USB, fornecendo uma visão clara das ações dos usuários.

Shadowing de Arquivo

Crie cópias de sombra de arquivos transferidos para dispositivos autorizados para auditorias detalhadas.

Senha Temporária Offline

Permitir temporariamente o acesso do dispositivo a computadores desconectados da rede. Garanta segurança e produtividade.

Criar Alertas por E-mail

Receba alertas por e-mail em tempo real para vários eventos relacionados ao uso de mídia removível nos computadores da empresa.

Painel e Gráficos

Para uma rápida visão geral dos principais eventos e estatísticas importantes, gráficos e tabelas estão disponíveis.

Relatórios e Análise

Monitore todas as atividades relacionadas ao uso do dispositivo com uma poderosa ferramenta de relatório e análise. Logs e relatórios também podem ser exportados.

Limite de Transferência

Limite o número de arquivos ou o tamanho do arquivo que pode ser transferido dentro de um intervalo de tempo definido. Inclua ou exclua transferências por meio de dispositivos, aplicativos online e compartilhamentos de rede.

Criptografia Forçada

para Windows e macOS

Criptografia de nível militar AES de 256 bits / Técnicas anti-adulteração / Gerenciamento centralizado de senhas / Enviar mensagens aos usuários / Limpeza remota / Configurações de diretiva de senha / OUTROS

Enforced Encryption USB

Autorize apenas dispositivos USB criptografados e garanta que todos os dados copiados em dispositivos de armazenamento removíveis sejam protegidos automaticamente.

Implantação Automática e Somente Leitura

A implantação automática e manual está disponível. A opção de permitir direitos Somente Leitura até que a criptografia seja necessária também é possível.

Senhas Mestras e de Usuário Complexas

A complexidade da senha pode ser definida conforme necessário. Senha Mestra fornece continuidade em circunstâncias como redefinições de senha dos usuários.

Gerenciamento de Senha e limpeza remota

Altere as senhas do usuário remotamente e limpe os dados criptografados no caso de dispositivos comprometidos.

Proteção de Conteúdo

para Windows, macOS e Linux

Clientes de email: Outlook / Thunderbird / Apple Mail / Navegadores da Web: Internet Explorer / Firefox / Chrome / Safari / Mensagens instantâneas: Skype / Slack / WhatsApp / Serviços em nuvem e compartilhamento de arquivos: Dropbox / iCloud / OneDrive / BitTorrent / AirDrop / Outros aplicativos: iTunes / FileZilla / SFTP / Total Commander / TeamViewer / OUTROS

Bloqueios por Pontos de Saída
Os filtros podem ser configurados com base em uma grande lista de aplicativos monitorados. Dispositivos de armazenamento USB, compartilhamentos de rede e outros pontos de saída podem ser monitorados.

Bloqueios por Tipos de Arquivos
Filtros de Tipo de Arquivo podem ser usados para bloquear documentos com base no tipo real do arquivo, mesmo que os usuários alterem a extensão.

Reconhecimento Óptico de Caracteres
Inspecione o conteúdo de fotos e imagens, detectando informações confidenciais de documentos digitalizados e outros arquivos similares.

Lista de Bloqueios de conteúdo predefinido e personalizado
Os filtros podem ser criados com base em conteúdo predefinido, como números de cartão de crédito ou números de CPF e conteúdo personalizado como palavras-chave ou expressões.

Bloqueios por Nome de Arquivo
Filtros com base nos nomes dos arquivos podem ser criados. Eles podem ser configurados com base no nome e na extensão do arquivo, apenas no nome ou na extensão

Localização de Arquivos Negados e Permitidos
Filtros baseados na localização dos arquivos no Disco Rígido local. Estes podem ser definidos para incluir ou excluir subpastas.

Bloqueios por Expressões Regulares
Uma ferramenta poderosa para identificar uma sequência de caracteres que definem um padrão de pesquisa.

Fora do Horário e Fora da Rede
Defina e ajusta políticas de fallback que serão aplicadas fora do horário comercial ou fora da rede.

Permissões de Domínio e URL
Aplique as políticas da empresa, mas permita aos funcionários a flexibilidade necessária para realizar seu trabalho. Habilite o recurso DPI e portais ou endereços de e-mail da empresa na lista de permissões.

Monitoramento da Captura de Tela e da Área de Transferência
Revogar os recursos de captura de tela. Elimine vazamentos de dados de conteúdo confidencial por meio de Copiar e Colar / Recortar e Colar, aprimorando a política de segurança de dados.

Remediação pelo Usuário
Capacita os usuários a sobrepor com segurança uma política DLP e oferece opções para justificar as transferências de dados. Ajuda a aumentar a responsabilidade e ciência do usuário final em relação às transferências de dados sensíveis na empresa.

Integração SIEM
Aproveite os produtos de Informações de Segurança e Gerenciamento de Eventos externalizando logs. Garanta uma experiência perfeita nos produtos de segurança.

Limite para Filtros
As Regras Avançadas de Detecção de Conteúdo permitem a definição de condições complexas para varredura de conteúdo combinando vários critérios (PIIs, palavras de dicionário, expressões regulares, etc.) usando operadores lógicos (AND/OR).

Limite de Transferência
Defina um limite de transferência dentro de um intervalo de tempo específico. Pode ser baseado no número de arquivos ou no tamanho do arquivo. Alertas por e-mail quando o limite é atingido estão disponíveis.

Verificação de Conteúdo Contextual
Habilite um mecanismo de inspeção avançado para detecção mais precisa de conteúdo sensível, como PIIs. A personalização de contexto está disponível.

Senha Temporária offline
Permitir temporariamente transferências de arquivos em computadores desconectados da rede. Garanta segurança e produtividade.

Dashboards, Relatórios e Análises
Monitore a atividade relacionada à transferência de arquivos com uma poderosa ferramenta de relatório e análise. Obtenha relatórios gráficos para executivos de nível C.

Conformidade (LGPD, GDPR, HIPAA, etc.)
Torne-se compatível com as regras e regulamentos do setor, como PCI DSS, LGPD, GDPR, HIPAA, etc. Evite multas e outros preconceitos.

DLP para Impressoras
Políticas para impressoras locais e de rede para bloquear a impressão de documentos confidenciais e evitar perda de dados e roubo de dados.

DLP para Thin Clients
Proteja dados em servidores de terminal e evite perda de dados em ambientes Thin Client, assim como em qualquer outro tipo de rede.

Recursos adicionais estão disponíveis. Saiba mais solicitando uma demonstração em EndpointProtector.com

eDiscovery

para Windows, macOS e Linux

Tipo de Arquivo: Arquivos Gráficos / Arquivos Office / Arquivos de Compactação / Arquivos de Programação / Arquivos de Mídia / etc. / Conteúdo Pré-definido: Cartões de Crédito / Informações Pessoalmente Identificáveis /Endereços / SSNs / IDs / Passaportes / números de telefone / IDs Fiscais / Números de Planos de Saúde / etc. / Conteúdo Personalizado / Nome do Arquivo / Expressão Regular / HIPAA / OUTROS

Criptografar e Descriptografar Dados

Os dados em repouso que contêm informações confidenciais podem ser criptografados para impedir o acesso de funcionários não autorizados. Ações de descriptografia também estão disponíveis.

Excluir Dados

Se ocorrerem violações claras da política interna, exclua as informações confidenciais assim que forem detectadas nos pontos de extremidade não autorizados.

Lista de Bloqueios por Localização de Digitalização

Os filtros podem ser criados com base em locais predefinidos. Evite a varredura redundante de dados em repouso com inspeções de conteúdo direcionadas.

Varreduras Automáticas

Além das varreduras limpas e incrementais, as varreduras automáticas podem ser agendadas - uma vez ou recorrentemente (semanalmente ou mensalmente).

Resultados da Varredura

Monitore os logs para a varredura de dados em repouso e tome as ações de correção conforme necessário. Logs e relatórios também podem ser exportados para soluções SIEM.

Status da Varredura

Verifique facilmente o status atual da sua digitalização. O status da digitalização é exibido no formato de 0 a 100%.

Limite para filtros

Defina o número de violações de políticas que um arquivo pode conter para que a política de segurança seja aplicada e o arquivo relatado ao servidor.

Conformidade (LGPD, GDPR, HIPAA, etc.)

Torne-se compatível com as regras e regulamentos do setor, como PCI DSS, LGPD, GDPR, HIPAA, etc. Evite multas e outros preconceitos.

Lista de Bloqueios por Tipo de Arquivo

Filtros de Tipo de Arquivo podem ser usados para descobrir documentos com base no tipo real do arquivo, mesmo que os usuários alterem a extensão.

Lista de Bloqueios por Conteúdo Predefinidas

Filtros podem ser criados com base em conteúdo predefinido, como números de cartão de crédito, números de seguridade social e muito mais.

Lista de Bloqueios por Conteúdo Personalizado

Filtros também podem ser criados com base em conteúdo personalizado, como palavras-chave e expressões. Vários Dicionários da Blacklist podem ser criados.

Bloqueos por Nome de Arquivo

Filtros com base nos nomes dos arquivos podem ser criados. Eles podem ser configurados com base no nome e na extensão do arquivo, apenas no nome ou na extensão.

Lista de Bloqueios por Expressões Regulares

Uma ferramenta poderosa para identificar a sequência de caracteres que define um padrão de pesquisa.

Lista de Permissões por Arquivos Permitidos

Embora todas as outras tentativas de transferência de arquivos sejam bloqueadas, as whitelists podem ser criadas para evitar redundância e aumentar a produtividade.

Lista de Permissões tipo MIME

Evite a varredura redundante em nível global, excluindo a inspeção de conteúdo para determinados tipos MIME.

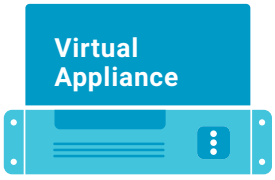
Integração SIEM

Aproveite os Produtos de Informações de Segurança e Gerenciamento de Eventos externalizando logs. Garanta uma experiência perfeita nos produtos de segurança.

100% de Flexibilidade de Implantação

Nossos produtos são de nível empresarial e evoluem continuamente para melhor atender a qualquer tipo de rede e indústria. Com uma arquitetura cliente-servidor, eles são fáceis de implantar e são gerenciados centralmente a partir da interface baseada na web. Além do Dispositivo Virtual, o servidor pode ser hospedado por nós e nas principais infraestruturas de nuvem, como Amazon Web Services, Microsoft Azure ou Google Cloud.

Device Control, Content Aware Protection, Enforced Encryption e eDiscovery estão disponíveis para computadores executando em diferentes versões e distribuições do Windows, macOS e Linux.



Virtual Appliance

Cloud Services

Amazon Web Services
Microsoft Azure
Google Cloud

Cloud-Hosted

Gartner peerinsights™

Altamente classificado no **Gartner Peer Insights** para prevenção de perda de dados corporativos.

Endpoints Protegidos

Windows	Windows 7 / 8 / 10 / 11	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2022	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS (kext and kextless agent)	Apple Silicon M1		●	●	●	●
	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

*Para mais informações sobre versões e distribuições suportadas, consulte EndpointProtector.com/linux

COSOSYS

Matriz (Romênia)

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

Alemanha

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

América do Norte

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

Coreia do Sul

contact@cososys.co.kr
+82 70 4633 0353
+82 20 4633 0354