ENDPOINT PROTECTOR | by CoSoSys

fc BRASIL

Proteja seus dados com a solução DLP Endpoint Protector

DLP | Device Control | Content Aware Protection | Encryption | **MDM**

Cososys: historia

Fundada en 2004

Reconhecida em 2017 Gartner Magic Quadrant for **Enterprise Data Loss Prevention**

Incluída na lista 50 Companhias de Tecnologia de mais rápido crescimento por Deloitte Technology FAST 50 Central Europe em 2011

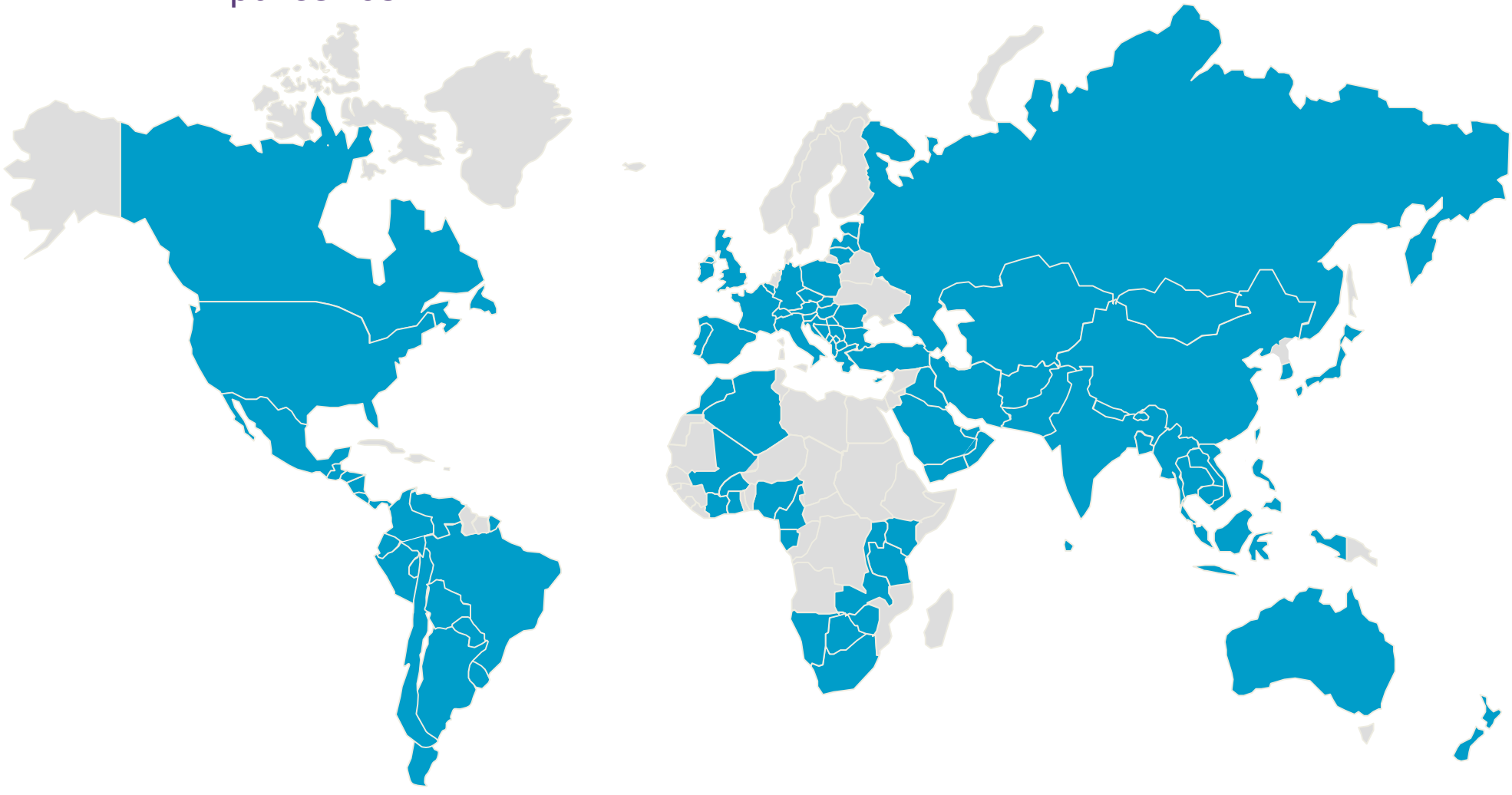
Ganhadora na categoria Data Leakage Prevention em Cybersecurity Excellence Awards nos anos de 2017 & 2016

Revendas em mais de 90 países

Forte crescimento

Capacidade de inovação

Países onde o Endpoint Protector está representado por parceiros:



Firewall e antivirus não são suficientes!

Um enfoque em camadas

Outras soluções de segurança (SIEM, IAM, etc.)
Proteção contra Ameaças Avançadas e Ransonware
DLP - Contra vazamento e perda de dados
Antivirus - baseado em assinaturas
Firewall - Proteção de perímetro via regras de acesso

Problemas para Gerentes IT /CEOs/CISOs:

Vazamento de dados / Perda de dados / Roubo de dados

Uso não controlado de dispositivos

Gestão de dispositivos móveis

Não cumprimento das normas

Produtividade baixa

Solução:

ENDPOINT PROTECTOR | 4

Endpoint Protector Family

fc BRASIL

ENDPOINT PROTECTOR | 4

- Arquitetura Cliente-Servidor
- Disponível como Hardware ou Virtual Appliance ou AWS
- Device Control e Content-Aware DLP
- MDM e MAM para iOS & Android

Enterprises, Government, SMB

MY | ENDPOINT PROTECTOR

- Arquitetura Cliente-Servidor
- Solução baseada na nuvem
- Device Control e Content-Aware DLP
- MDM e MAM para iOS & Android

Enterprises, SMB, SoHo

ENDPOINT PROTECTOR | BASIC

- Solução independente
- USB Lockdown for any Notebook, PC or Netbook
- Controle de dispositivos em alguns segundos

Uso doméstico, SoHo, SMB

EasyLock

- Solução independente
- Criptografia USB
- Criptografia na nuvem
- Criptografia de pasta local
- Criptografia de CDs & DVDs
- Criptografia forzada para dispositivos USB

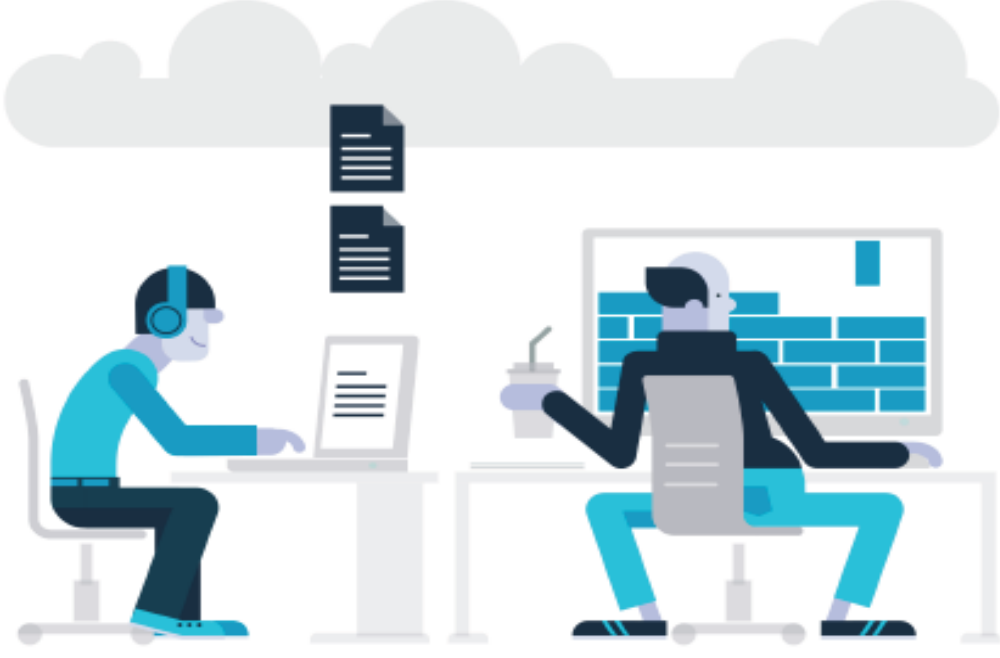
Enterprises, Government, SMB, SoHo

Legenda: MDM - Mobile Device Management / MAM - Mobile Application Management

O que é a prevenção contra perda de dados (DLP)?

A solução de Prevenção contra Perda de Dados é um sistema projetado para detetar possível fuga de dados / perda de dados e evitar estes incidentes através de monitoração, deteção e bloqueio de dados sensíveis. Nos incidentes de vazamento de dados a informação confidencial se faz conhecer a pessoas não autorizadas, seja de forma intencional ou por erro involuntário.

Enquanto você está ocupado na proteção da rede e na configuração do Firewall para controlar as ameaças externas, os empregados podem copiar facilmente informação para dispositivos de armazenamento ou subir arquivos para a nuvem



ENDPOINT PROTECTOR 4

Ajuda muito colocar foco na primeira ameaça do século 21, controlar dados confidenciais que podem sair da empresa, definir o que se pode transferir.

Diga não à espionagem industrial!

Por que você necessita de DLP?

Segundo o IBM 2015 CyberSecurity Intelligence Index, 55% dos incidentes de Segurança foram produzidos dentro da própria empresa. Estes se dividem em atos maliciosos e erros dos usuários. Os empregados propositalmente são responsáveis por 31,5% dos ataques cibernéticos e os 23,5% restantes são usuários descuidados.

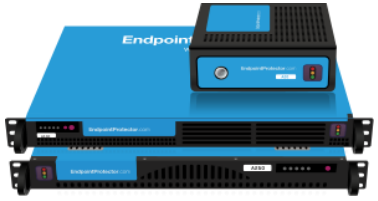
"Somente 45 % dos ataques cibernéticos provém do exterior."

IBM 2015 Cyber Security Intelligence Index

23,5 % são Erros de usuários

Apresentação do Produto

Flexibilidade de implementação



Hardware Appliance

- Out-of-the-box solution
- Implementação em minutos
- Modelos disponíveis para todo tipo de redes de 20 a 4000+ endpoints

Virtual Appliance

- Formatos: .ovf, .ova, .vmx, .vhd, .pvm, .xva
- Implementação em menos de 1 hora
- Compatívelcom VMware, VirtualBox, Parallels e Microsoft Hyper-V

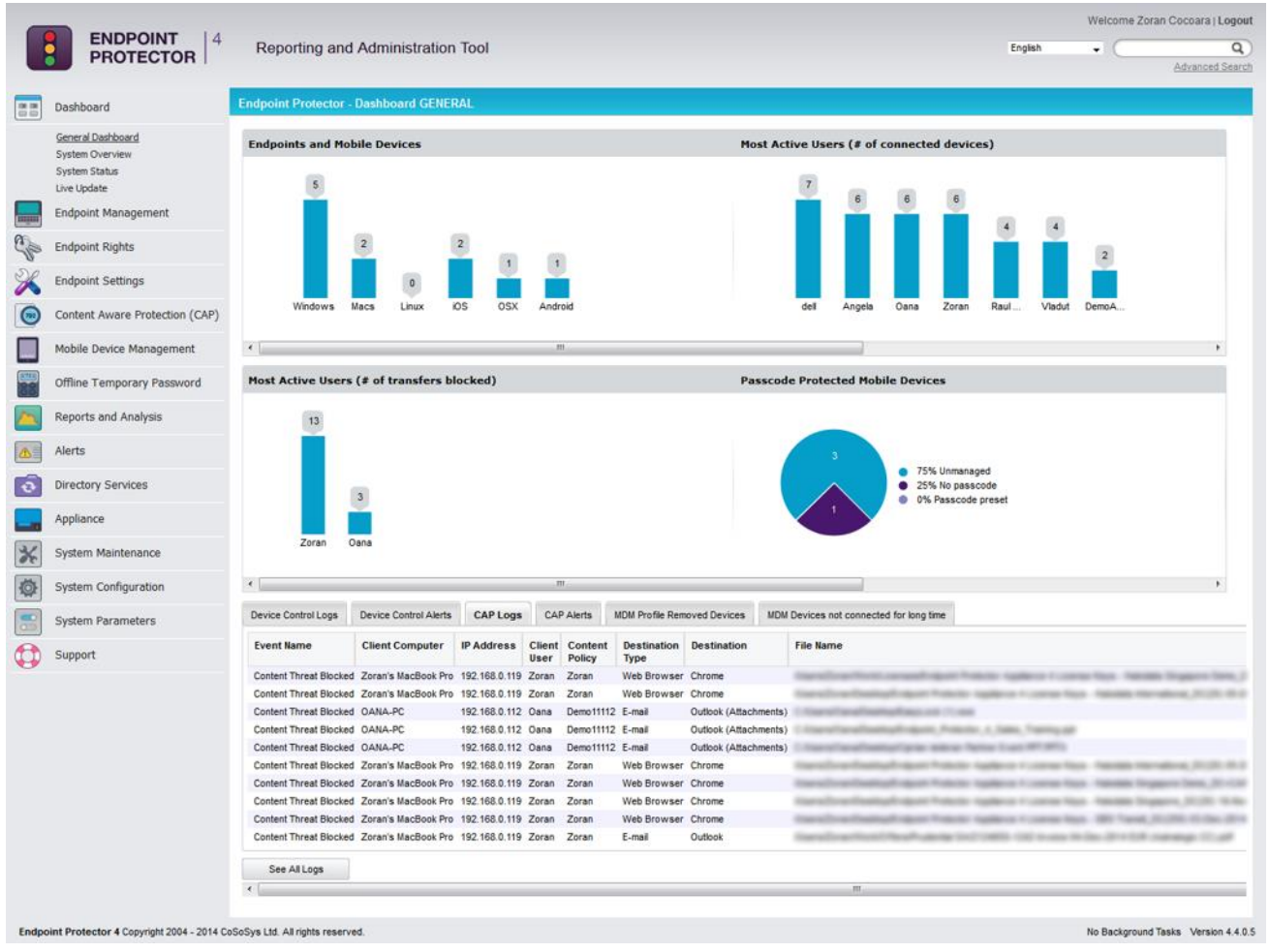
Cloud-based

- Baixo custo operacional
- Acesso fácil para administrar e criar relatórios
- Escalabillidade e disponibilidade

Amazon Web Services

Interface de Administração

- Interface de usuário baseada em Web
  - Multilíngua
    - Português
    - Espanhol
    - Francês
    - outros
- Intuitiva
- Gestão centralizada
- Active Directory
- Curva de aprendizagem curta



Descrição Geral do Produto

Control de Dispositivos
Para Windows, Mac OS X e Linux

Mobile Device Management
Para iOS e Android

Content Aware Protection
Para Windows, Mac OS X e Linux

Mobile Application Management
Para iOS e Android

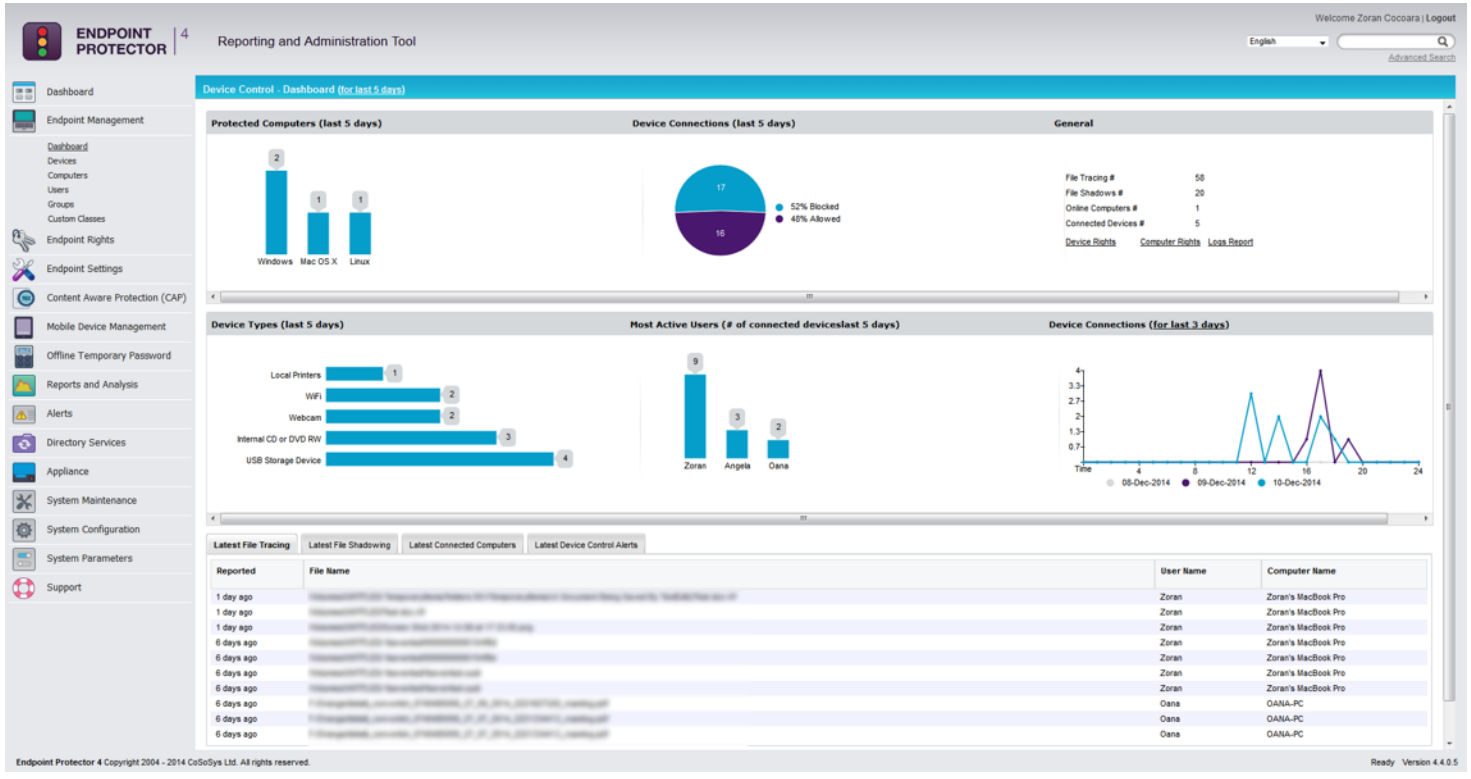
Enforced Encryption
Para Windows e Mac OS X

E-Discovery
Para Windows, Mac OS X e Linux

Controle de Dispositivos

Device Control

A solução mais granular do mercado, permitindo o controle dos dispositivos USB e de outros dispositivos de armazenamento.



Estabelecer Permissões: Por Dispositivo | Usuário | Máquina | Grupo | Globais

Estabelecer Aceso: Permitir Acesso| Negar Acesso| Acesso de somente leitura| etc.

Estabelecer Alertas: Conectado | Desconectado | etc.

Device Control

Controlar os tipos de dispositivos e portas mais comuns:

- USB Devices
- Digital Cameras
- Smartphones / PDAs
- FireWire Devices
- MP3 Player / Media Player Devices
- Biometric Devices
- Bluetooth Devices
- ZIP Drives
- ExpressCards (SSD)
- Wireless USB
- Serial Port
- Teensy Board
- PCMCIA Storage Devices
- Local and Network Printers
- Network drives
- and more…

Device Control

Administrar USB e dispositivos externos

- Criar permissões por tipo de dispositivo
- Criar permissões com alta granularidade
- Criar permissões a base de VID, PID, SN
- Criar Classes personalizadas

File Tracing e File Shadowing

- Visão dos dados transferidos de e para USB
- File Tracing - Informe sobre arquivos
- File Shadowing - Guarda uma cópia
- Tracing de arquivos apagados

Offline Temporary Password (OTP)

- Manter produtividade mesmo que os equipamentos estejam sem conexão
- Acesso a relatório e a análise uma vez conectados
- OTP Timeframe: de 30 minutos a 30 dias

Criptografia Forçada

- Os dados transferidos são criptografados automaticamente
- Administrar os dispositivos de forma remota(change passwords, wipe etc.)

Device Control

Proteção para Thin Clients

- Device Control para Thin Clients
- Device Control para Terminal Servers

Alertas

- Alertas de Sistema e usuários
- Eventos

Relatórios e Análises

- Gráficos, relatórios
- Opção de exportação

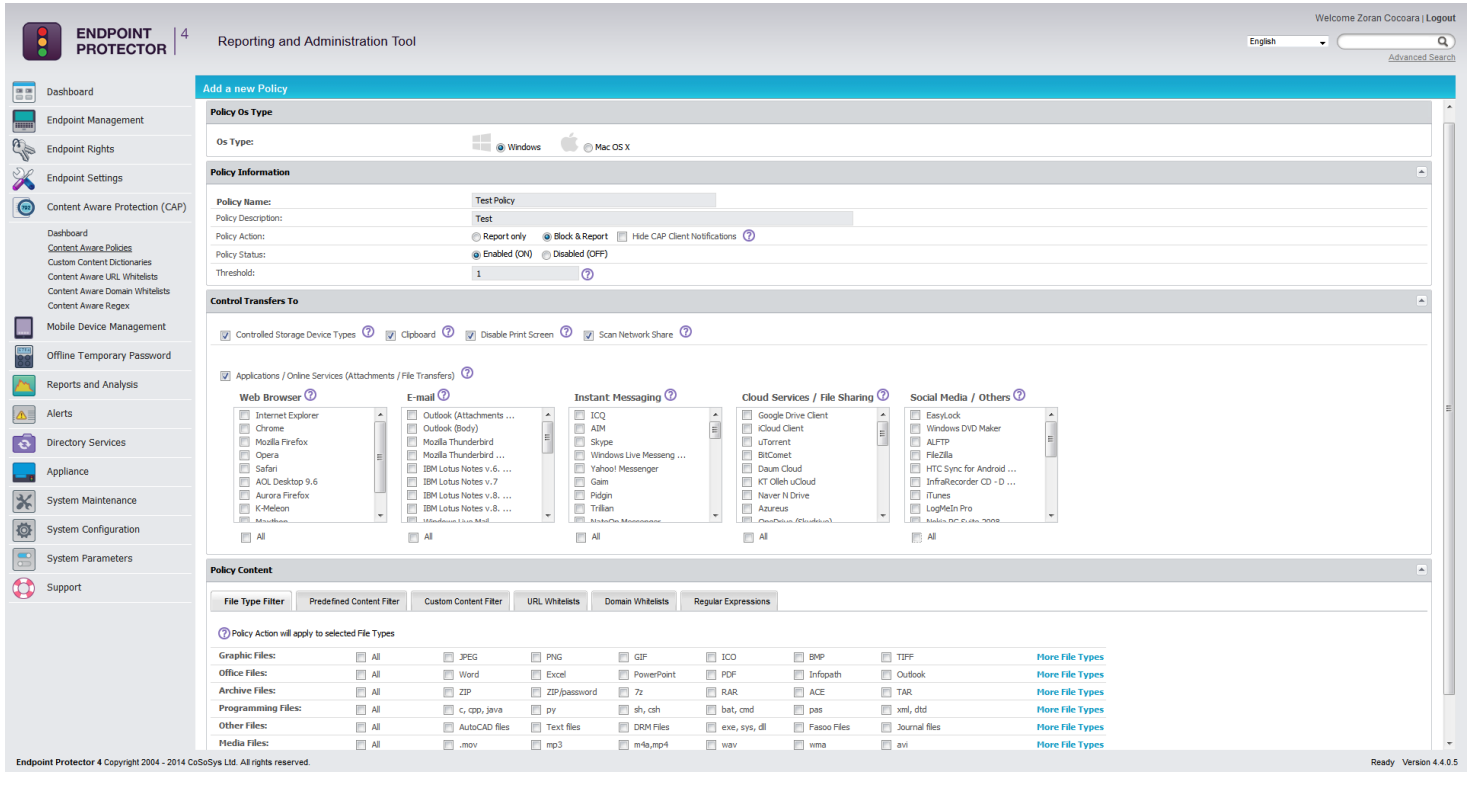
Integração SIEM

- Enviar Logs a SEM/SIEM server
- Ver todos os eventos de Segurança em um mesmo local

Content Aware Protection

Content Aware Protection

Controle os dados confidenciais que saem de sua rede através de vários pontos de saída: e-mail, armazenamento na nuvem, mensagem instantânea, redes sociais e outras aplicações online.



Estabelecer Permissões: Por Usuário | Máquina | Grupo | Globais

Estabelecer Filtros: Por Extensão de Arquivo | Conteúdo Predefinido | Conteúdo Personalizado | Expressões Regulares

Estabelecer Alertas: Reportado | Bloqueado

Content Aware Protection

Aplicações controladas

- E-Mail Clients
  - ✓ Outlook
  - ✓ Lotus Notes
  - ✓ Thunderbird, etc.
- Web Browsers
  - ✓ Internet Explorer
  - ✓ Firefox
  - ✓ Chrome
  - ✓ Safari, etc.
- Instant Messaging
  - ✓ Skype
  - ✓ ICQ
  - ✓ AIM
  - ✓ Microsoft Communicator
  - ✓ Yahoo Messenger, etc.
- Cloud Services/File Sharing
  - ✓ Dropbox, iCloud, SkyDrive
  - ✓ BitTorrent, Kazaa, etc.
- Other Applications
  - ✓ iTunes
  - ✓ Samsung Kies
  - ✓ Windows DVD Maker
  - ✓ Total Commander
  - ✓ FileZilla
  - ✓ Team Viewer
  - ✓ EasyLock,
  - ✓ and more…

Arquivos controlados:

- Graphic Files
  - ✓ .jpeg, .png, .gif, .bmp, .tiff
- Office Files
  - ✓ .docx, .pptx, .xlsx, .pstx, .pdf
- Archive Files
  - ✓ .zip, .rar, .ace, .tar
- Programming Files
  - ✓ .cpp, .java, .py, .sh, .csh, .bat
- Other Files
  - ✓ .exe, .sys, .dll, .dwg, .drm
- Media Files
  - ✓ .mp3, .mp4, .m4a, .avi, .wma
- and more…

Content Aware Protection

Filtro de conteúdo Predefinido

- Informação pessoal, DNI, E-mails, etc.
- Credit Card, Endereços, IBAN, etc.

Filtro de Conteúdo personalizado

- Dicionário Personalizado
- Definir Palavras Chave e Expressões

Expressões Regulares

- Create custom Regex
- Filter recurrent content

Filtro por Tipo de arquivo

- Filtros a base de extensão
- Detecta o código hash

Content Aware Protection

Threshold para filtro predefinido

- Por conteúdo Específico
- A nível global

Desabilitar área de transferência

- Desabilitar Copiar & Colar

Disable Print Screen

- Revogar as capacidades de fazer captura de tela

Offline Temporary Password (OTP)

- Acceso a registros uma vez reconectados à rede
- (OTP) Timeframe: de 30 min a 30 dias

Content Aware Protection

Controle de Impressora

- Escanear os dados transferidos a impressoras locais e em rede

Políticas HIPAA

- Assegurar o cumprimento
- Bloquear a transferência de documentos que contêm informação como medicamentos aprovados de FDA, códigos ICD-9 e léxico de diagnóstico

File Tracing / File Shadowing

- Tracing de todos os datos copiados para e dos dispositivos
- File Tracing registra informação de arquivo
- File Shadowing guarda cópia de arquivo transferido

Lista branca de Domínio & URL

- Evitar escaneamento redundante
- Assegurar que a produtividade não seja afetada

Content Aware Protection

Proteção para Thin Clients

- Content Aware Protection para Thin Clients
- Content Aware Protection para Terminal Servers

Alerts

- Estender alertas do Systema e dos eventos do usuário
- Alertas criados por políticas aplicadas

Relatórios e Análises

- Gráficos, relatórios
- Opção de exportar

Integração SIEM

- Enviar Logs a SEM/SIEM server
- Ver todos os eventos de Segurança em um mesmo local

eDiscovery (Analisando os dados em repouso)

E-Discovery

- Escaneia e identifica dados sensíveis no computador em máquinas Windows, MacOS e Linux.

- Identifica, gerencia e controla quais dados confidenciais estão armazenados nos computadores

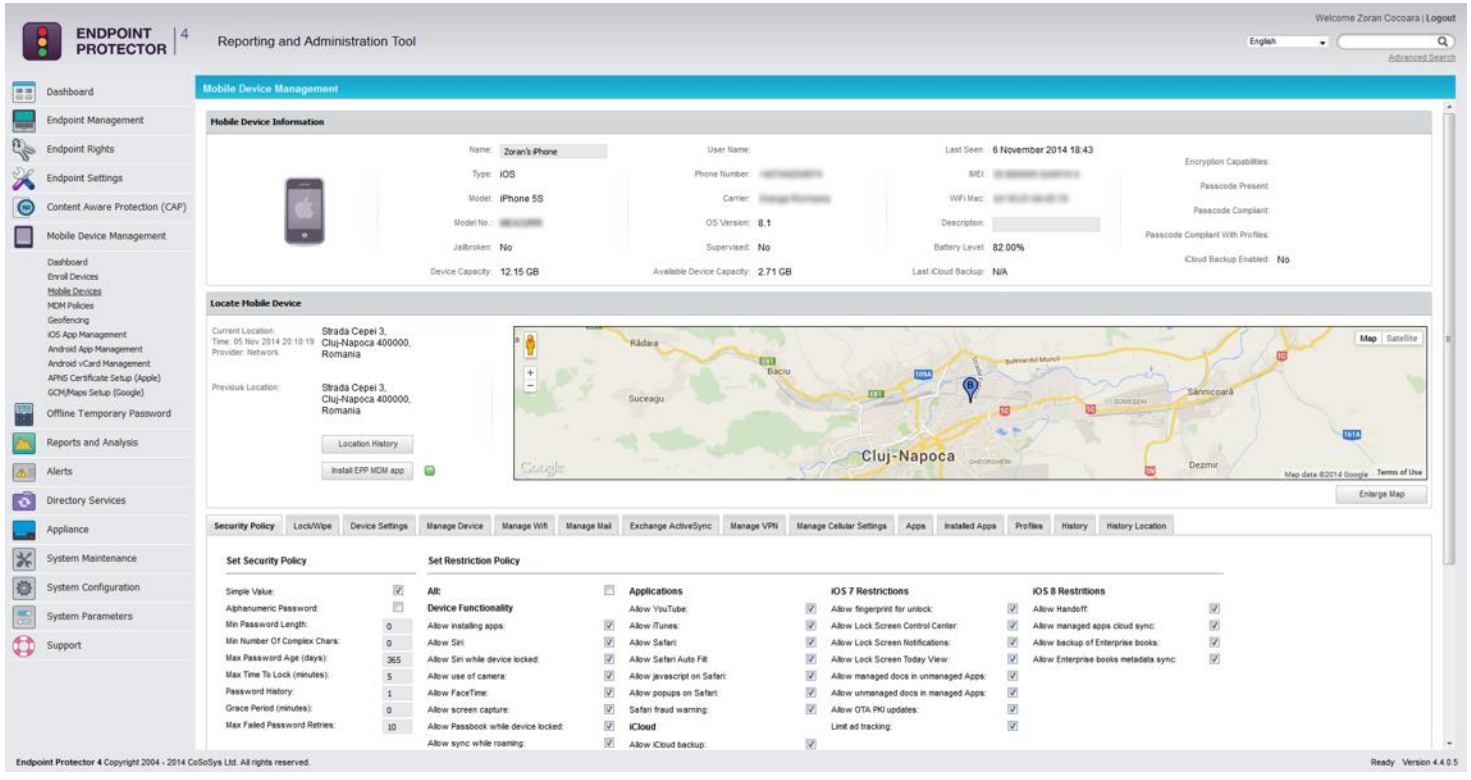
- Propriedade intelectual como segredos de negócios, patentes, direito autoral e projetos industriais devem ser acessados somente por pessoas autorizadas e confiáveis

- O eDiscovery vasculha todos os documentos residentes em desktops, laptops e servidores, identificando e localizando dados confidenciais, além de oferecer medidas de correção para a proteção proativa contra o vazamento de dados.

Mobile Device Management

Mobile Device Management

Gerencie a frota de dispositivos móveis mediante a aplicação da segurança, a gestão de aplicações, implementando a configuração de rede, geofencing e mais. Uma das soluções mais fáceis de usar do mercado.



Aplicação de Segurança: Senha | Criptografia | etc.

Segurança em caso de perda: Tracing | Localização | Bloqueio | Apagar

Gerenciar Aplicações: Identificar | Implementar | Eliminar | etc.

Gerenciar Redes: E-mail | WiFi | VPN | etc.

Mobile Device Management

Inscrição/Provisionamento Sem fio

- Inscrição via SMS, E-mail, Código QR, Enlace direto
- Instalação com 3 cliques
- Aplicação EPP MDM app disponível

Forçar a Criptografia do Dispositivo

- Proteção de Dados habilitando capacidade de criptografia
- Comprimento de senha, etc

Apagamento Remoto

- Evitar o roubo de dados em caso de perda do dispositivo

Seguimento & Localização

- Vigiar os dispositivos móveis
- Saber onde se encontram os dados críticos do negócio

Mobile Device Management

Segurança baseada em senha

- Comprimento mínimo da senha
- Complexidade da Senha & Retentativas
- Tempo de bloqueio de tela

Restrições de funcionalidades no iOS

- Desativar câmera
- Desativar Handoff
- Desativar Apps, Cloud sync, etc

Desabilitar built-in functionalities para Android

- Disable Camera
- Disable Handoff
- Disable Apps Cloud sync, etc.

Implementar ajustes em iOS e Mac OS X

- E-mail
- VPN
- WiFi

Mobile Device Management

Geofencing

- Políticas baseadas na localização
- E.g. desativar câmera do smartphone somente dentro do perímetro da empresa

Restrições de iOS

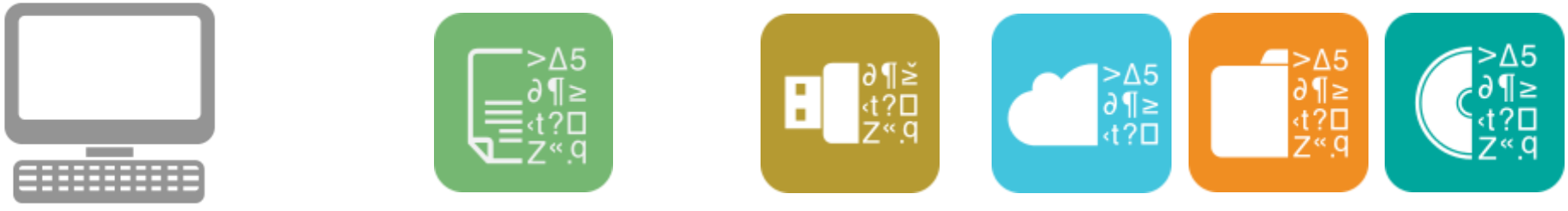
- Block iCloud
- Block Safari
- Block iTunes, etc.

Funcionalidades somente para Android

- Reproduzir som se o dispositivo estiver perdido
- Bloquear WiFi
- Bloquear Bluetooth

Enforced Encryption

Enforced Encryption



EasyLock – Cross-platform Enforced Encryption with Endpoint Protector

- Permite somente o acesso dos dispositivos USB com EasyLock e também obriga a cópia na partição criptografada

EasyLock – Cross-platform Data Encryption

- Criptografia de força militar AES-256 bits
- Intuitivo drag & drop ou copy/paste
- Disponível para USB, Pasta Local, Nuvem, CDs & DVDs

Diferenciadores

“Tudo em um” DLP & MDM

- A vantagem de controlar as estações de trabalho mais importantes dentro da mesma console de administração

Compatível com múltiplas plataformas

- Windows, Mac OS X, Linux, iOS, Android

Fornecido em múltiplos formatos

- Virtual Appliance
- Hardware Appliance
- Solução baseada na nuvem

Modular

- Fácil de ativar novos módulos
- Todos os módulos são preinstalados
- Licenciado de forma separada – pagar somente pelo que precisa

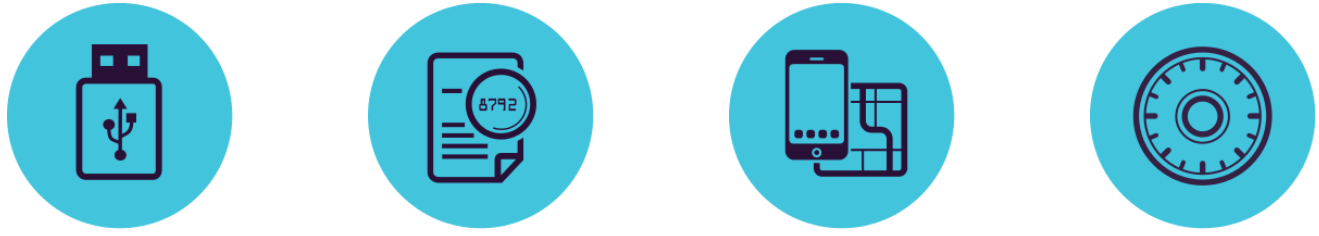
Granular

- Criar políticas e designar permissões em distintos níveis: dispositivo, usuário, máquina, grupo, global
- Ir mais além de simplemente bloquear / permitir dispositivos ou transferências de documentos e crear políticas de somente leitura, somente reportar e baseadas em conteúdo

Conclusão

Proteger seus dados em todas as estações de trabalho da empresa é essencial.

Proteja sua rede e seus dados confidenciais contra as ameaças trazidas por dispositivos portáteis de armazenamento, serviços na nuvem e postos de trabalho móveis.



Demonstração da Console

Dúvidas?

Para mais informação por favor entre em contato!

Web: www.fcbrasil.com.br

E-mail: vendas@fcbrasil.com.br

Telefones: (21) 4063-7703 / (11) 4063-4840

Obrigado por sua presença!