

SOLUÇÕES CRYPTZONE

O Grupo Cryptzone reúne as pessoas, processos e tecnologia, com o objetivo de mitigar os riscos de segurança da informação nas áreas de: Política de Compliance, Segurança de conteúdo, Acesso seguro e Endpoint Security.

- Mantenha a conformidade com a regulamentação, incluindo HIPPA, HITECH, SOX, FSA, PCI e DPA
- Proteja as informações pessoais do cliente
- Proporcione acesso seguro instantâneo às aplicações financeiras e de dados, mesmo a partir de dispositivos móveis
- Reduza o risco de crimes cibernéticos
- Melhore a eficiência e reduza os custos.

1) AppGate

O **AppGate Security Server** substitui vários produtos com um único aparelho o que é mais fácil de gerenciar e mais barato de se executar:

- **Forte segurança** que protege contra ameaças internas e externas
- Domínios internos seguros protegendo dados críticos atuando como **firewall**.
- **Acesso remoto baseado em papéis** (funções, regras) a partir de qualquer dispositivo, de qualquer local.
- **Controle central das políticas de segurança** e da administração de usuários.
- **Continuidade de negócios e alta disponibilidade** através de **Clustering**. A tecnologia AppGate é projetada para Clustering tornando mais fácil adicionar mais usuários com a mudança de requisitos. É fácil começar com um pequeno sistema e depois expandi-lo para suportar as necessidades de negócio em evolução. O sistema é escalável quase linearmente: um **AppGate Security Server** adicional dá quase o dobro de performance.

- **Monitoramento integral e elaboração de relatórios** de todos os acessos dos usuários para **compliance**. Todas as atividades do usuário e do administrador são registradas para que o acesso aos recursos da rede possam ser rastreados e monitorados. Reduz as despesas gerais em relatórios de compliance. Diferentes tipos de alarmes podem ser definidos e enviados para os sistemas externos para ação imediata.
- **Suporte** a uma ampla gama de **plataformas móveis**, incluindo Nokia Series 60 (Symbian), Windows Mobile, iPhone e iPad.
- **Criptografia**: Todo o tráfego entre os servidores e os dispositivos endpoint são criptografados usando métodos de criptografia forte, incluindo AES128, AES256, Blowfish, 3DES e RC4.
- **Impressão local segura**. Impressão segura pode ser um problema se o usuário estiver em uma rede diferente da que hospeda o aplicativo. **AppGate** módulo de impressão local segura permite ao usuário imprimir em sua impressora local onde ele está trabalhando agindo como um servidor de impressão. A solicitação do usuário de impressão é enviada para o servidor de segurança. O cliente **AppGate** inclui um buffer de impressão local que recolhe os trabalhos de impressão do servidor quando o usuário se loga. Estes podem então ser impressos para a impressora local do usuário garantindo que a informação permaneça segura.

O **AppGate Security Server** - Appliance para o controle de acesso baseado em papéis (funções).

- AppGate para dispositivos móveis - Acesso seguro para iPhone iPad, e Android
- AppGate Satélites - rede virtual segura
- Dispositivo AppGate Firewall - firewall para proteção ponta-a-ponta
- Cryptzone OTP - Um módulo de senha para mobile
- MindTerm - implementação Java do cliente SSH2

2) Secured eControl

- **Secured eControl** - Política de aplicação e de detecção de dados
- **Secured eControl** garante que se tenha conhecimento dos metadados, dados ocultos e informações proprietárias antes de compartilhar conteúdo com outras pessoas e fornece a opção de obter as informações com criptografia de arquivos ou criptografia de e-mail.

Permite Impor o uso de criptografia de e-mail sobre informações sigilosas



Secured eControl tem a capacidade de acionar o uso de criptografia de e-mail se o usuário tentar enviar informações confidenciais como números de cartão de crédito, números de segurança social ou registros de clientes. A informação seria, então, criptografada antes ou completamente bloqueada. Políticas e ações para isso são controladas a partir de uma localização central.

Descoberta de dados confidenciais e Remoção

Quando apoiados com o Workshare Policy Manager, alertas de detecção de conteúdo notificam quando informações confidenciais ou de propriedade intelectual, tais como dados financeiros ou senhas estão dentro de e-mail ou documentos do Microsoft Office e fornecem as ferramentas para remover ou reter a informação. A Descoberta de dados identifica até mesmo textos redigidos indevidamente.

Email Protection

Recebimento de um alerta antes do e-mail ser enviado sempre que um e-mail ou arquivo possam violar uma política de segurança. Para evitar que se envie acidentalmente um e-mail com informações confidenciais, esse recurso pode bloquear ou pedir para remover dados sensíveis. As políticas de segurança são facilmente customizadas e incluem a capacidade de especificar ações diferentes quando um documento é enviado internamente ou externamente, como aplicar a criptografia de e-mail.

Remoção de dados escondidos no Word, Excel, PowerPoint

Remoção de dados localizados em células escondidas em planilhas do Excel, limpeza de informações confidenciais armazenadas em notas do PowerPoint e asseguramento de que as modificações ou supressões em documentos do Word registrados pelo modo 'controlar alterações' não podem ser lidos por terceiros. Pode personalizar 25 opções de limpeza de metadados com diferentes opções para os destinatários da organização e de ambientes externos.

Limpeza de Batch Metadata

Possibilita selecionar um número de arquivos e executar a limpeza de lotes de metadados para remover os metadados de todos os arquivos.

Classificação de Documentos

Pode-se restringir facilmente o acesso a documentos sensíveis do negócio, definindo as classificações do documento. A classificação controla a distribuição de documentos por e-mail e irá alertar sobre a natureza potencialmente sensível do documento que se está tentando enviar por e-mail e pode impedir que documentos sejam enviados para específicos usuários internos ou externos.

Auto Zip Attachments

Compressão (zip) automática de anexos quando o arquivo exceder um limite específico.

Preview dos anexos que foram limpos

Ao limpar os anexos de e-mail pode-se visualizar o anexo limpo antes de enviar o e-mail.

Document Inspector do Office 2007

Aprimoramento do Inspetor de Documento do Office 2007 e fornecimento de políticas configuráveis que vão proteger os dados confidenciais, incluindo a aplicação de política de propriedades documento.

Apague Informação Sensível

Possibilita deletar (black out) o conteúdo selecionado em documentos no Microsoft Word (DOC e DOCX) para que ele não seja mais disponibilizado. As ferramentas de redação de texto deletam informações confidenciais e apagam permanentemente o conteúdo do documento.

Múltiplas Opções de Remoção de Metadados

Remoção de metadados ocultos com esta opção de remoção de metadados, ou uma organização pode definir uma política automatizada para fazer a remoção automática de metadados de forma transparente ao usuário.

Descoberta de Metadados em Documentos protegidos

Recebimento de alertas de documentos protegidos por senha, documentos compactados e documentos com direitos de edição limitados que contêm metadados.

3) NETconsent

- NETconsent Suite Política de segurança - sistema de gestão da Política de segurança
- NETconsent Policy Manager - Módulo Gestão de Políticas para criar provas legalmente válidas de que os empregados viram, entenderam e concordaram com as políticas
- NETconsent Examiner - Compreensão do Módulo de Política de Gestão para testar, monitorar e reportar aos funcionários as políticas do ambiente de trabalho

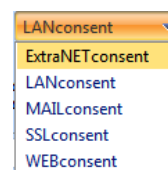
- Netconsent Informer - Política de Módulo de Gestão para disseminar anúncios eletrônicos que todos precisam conhecer
- Netconsent Assessor - Módulo Política de Gestão para a comunicação de negócios automatizados, opiniões através de votação, realização de avaliações e análise de feedback dos funcionários e atitudes
- NETconsent Reporter - Módulo Política de Gestão para analisar, acompanhar, presenciar, gerir a política e gestão de riscos de informação
- Aplicação Whitelisting SE46 - controle de aplicativos por meio de whitelisting

NETconsent Dashboards:

- Dashboard disponível no Centro de Gerenciamento de Políticas ou na Intranet
- Gráficos com o cumprimento da política por toda a organização e tabela por áreas
- Apresentação de documentos em vários idiomas
- Relatórios de fácil compreensão e altamente flexíveis
- Resumo de relatórios para a gerência sênior e Relatórios de exceção para os gestores de linha
- Relatórios direcionados através de "Listas de Distribuição"

Gerenciamento de Política Automatizada (Automated Policy Management)

- Repositório centralizado de Políticas
- Único ponto de revisão de documentos
- Distribuição automatizada
- Garante que Políticas relevantes sejam distribuídas para Pessoas Relevantes
- Abordagem orientada
- Política de Utilização Aceitável pela TI
- Prioriza com base no risco
- Aplica sempre que necessário: de forma consultiva, voluntária ou forçada
- Testa a compreensão do usuário
- Impacto mínimo na infraestrutura de TI



NETconsent facilidades:

- Entrega de Informações Gerenciais
- Oferece Informações: Auditável e Probatória
- Permite melhor compreensão, Revisão regular da política, Programa de Formação Centrada e Risco Reduzido
- Integração permanente com as novas tecnologias
- + 175.000 usuários do Reino Unido e +25.000 no mundo
- Virtualização suportada
- Programa de testes de carga
- Resolução de problemas
- Totalmente baseado na web
- Capacidades de integração com múltiplos diretórios

4) Secured eMail

- **Secured E-mail** - criptografia de e-mail através de Política de controle

Leis e regulamentos mandam as empresas protegerem informações sensíveis através de criptografia. Com **Secured eMail**, informações confidenciais em um e-mail podem ser criptografadas com o toque de um botão. Não importa se o destinatário é um colega de trabalho ou um parceiro externo - ele pode abrir as informações criptografadas de qualquer computador ou dispositivo inteligente e enviar de volta uma resposta criptografada.

Secured eMail oferece poderosa criptografia ponta-a-ponta, fácil de usar. **Secured eMail** integra Microsoft Outlook e Lotus Notes. Para enviar um e-mail criptografado, o usuário simplesmente aperta o botão Enviar Secured. Destinatários de e-mails protegidos não precisam comprar uma licença para ler o e-mail ou responder de forma segura.

5) Secured eFile

- **Secured eFile**— segurança de arquivo e criptografia controlados centralmente

Proteção da propriedade intelectual e de informações confidenciais é uma preocupação de segurança máxima para qualquer negócio hoje em dia. Profissionais precisam compartilhar documentos e arquivos com colegas de trabalho, clientes e parceiros em uma base diária e, freqüentemente, esses itens contêm informações confidenciais. A criptografia de arquivos ajuda na segurança da informação, minimizando o risco dela ser acessada por usuários não autorizados. Cryptzone **Secured eFile** cria uma plataforma segura para a colaboração no ambiente de trabalho.

Secured eFile permite que as pessoas possam compartilhar arquivos e pastas de forma segura com indivíduos e grupos dentro e fora da organização.

Fácil de usar, a ferramenta de criptografia de arquivos permite que usuários possam proteger as informações e especificar exatamente quem na organização mais precisa de acesso. A console de gerenciamento central permite aos administradores implantar políticas de segurança em toda a organização, enquanto a tecnologia embutida cuida de gestão dos direitos de acesso, autenticação de usuário e chaves de criptografia. Com **Secured eFile** os usuários, clientes e parceiros têm acesso à informação de que necessitam.

6) Secured eCollaboration

- **Secured eCollaboration** - Add on para o Microsoft SharePoint[®] criptografia de arquivos

Uma organização que utiliza o Microsoft SharePoint[®], pode usar o **Secured eCollaboration**. Microsoft SharePoint é uma poderosa ferramenta para colaboração e gerenciamento de conteúdo, mas o SharePoint não vem pré-equipado com ferramentas para criptografia forte ou eficiente de gestão de propriedades do usuário. Os usuários geralmente armazenam informações confidenciais na forma de dados financeiros, informações de clientes, planos de projetos, contratos - dados que devem ser protegidos, na plataforma de colaboração. Como usar o poder do SharePoint, mas também garantir que informações sensíveis só sejam acessíveis aos usuários autorizados?

Secured eCollaboration é a primeira solução no mercado projetada especificamente para SharePoint criptografia e segurança. **Secured eCollaboration** integra com o SharePoint e fornece toda a criptografia e ferramentas de gerenciamento de acesso e direitos necessários para que co-trabalhadores possam compartilhar informações de forma segura. Administradores controlam políticas de segurança de forma centralizada, os usuários gerenciam documentos usando criptografia SharePoint e

atribuem direitos de acesso em linha com as políticas e fortes recursos de segurança garantem a conformidade de Compliance.

- Criptografia SharePoint rápida e fácil - ferramentas intuitivas são integradas à interface de usuário do SharePoint.
- Integração com o Microsoft Active Directory® torna o gerenciamento de direitos de acesso do usuário para criptografia do SharePoint uma tarefa fácil
- Console de gerenciamento central que permite a TI implantar e gerenciar políticas de criptografia SharePoint.
- Autenticação de usuário, chaves de criptografia e senhas SharePoint gerenciados automaticamente.
- "Check-in/check-out" nativos do SharePoint e versões de documentos são totalmente suportados na solução de criptografia do SharePoint, garantindo que cada versão seja criptografada e segura.

7) Secured eUSB

- **Secured eUSB** - gerenciamento centralizado de ferramenta de implementação de criptografia USB

Assumindo o controle de segurança USB

O uso de grande propagação de drives flash USB é uma questão importante para os líderes empresariais. Como proteger dados sensíveis quando é tão fácil de copiar para um dispositivo USB?

Secured eUSB permite assumir o controle pois é uma solução abrangente e fácil de usar para segurança de USB que incorpora todas as funcionalidades necessárias para proteger a propriedade intelectual e cumprir com as leis de proteção de dados e regulamentos para a área de Compliance. **Secured eUSB** fornece criptografia forte, controle centralizado das políticas de segurança USB, políticas de senhas e direitos de acesso do usuário, Relatórios de conteúdo de dados automáticos, permitindo a implantação e controle segurança de USB em toda a rede. Com **Secured eUSB** os dados em todas as unidades flash USB na organização estão garantidos e permitem **visibilidade total** do movimento de dados.

- Criptografia USB pode ser implementada rapidamente e facilmente - sem necessidade de infraestrutura complexa.
- Overhead de administração é minimizado pois os usuários são orientados por meio do processo de criptografia USB e Recursos internos fornecem suporte Helpdesk básico.

- Tecnologia avançada garante os mais altos níveis de segurança USB.
- Ferramentas de gerenciamento central permitem implementar e reforçar as políticas de criptografia USB.
- Relatórios de conteúdo de dados automáticos fornecem uma trilha de auditoria completa para garantir a conformidade regulamentar e que a criptografia USB está em uso.
- Sistemas anti-roubo bloqueiam dispositivos USB perdidos ou roubados para evitar perda de dados.

8) Secured eDevice

- **Secured eDevice** - controle de dispositivos e portas

Proteção ativa contra violações de segurança e perda de dados.

Mídia de armazenamento e dispositivos portáteis, tais como DVDs, MP3 players, drives flash USB, telefones celulares e tablets representam uma ameaça de segurança muito real para as organizações. Os funcionários podem facilmente usar um cartão de memória SD ou drive USB para copiar e mover grandes volumes de informações confidenciais, ou inadvertidamente importar um vírus para a rede fazendo o download de dados de um CD-ROM. Proibição do uso de todos os dispositivos periféricos não é a solução. As organizações precisam se proteger contra essas ameaças internas ao mesmo tempo, permitindo que as pessoas usem os recursos de TI de que precisam para ser eficientes e produtivas.

Secured eDevice monitora e reforça o controle de dispositivos e políticas de transferência de dados em todos os computadores na rede. Políticas de controle de dispositivos podem ser definidas para **bloquear** uma grande variedade de **mídias e dispositivos**, **restringir as opções de PrintScreen**, limitar o acesso a arquivos específicos ou ao conteúdo do arquivo e limita as permissões de transferência de arquivo. Console de gerenciamento centralizado fornece atualizações em tempo real sobre o acesso ao dispositivo e movimentação de dados, com destaque para os problemas potenciais de segurança. Poderosas ferramentas de relatórios fornecem relatórios detalhados para o cumprimento regulamentar e de auditoria.

Secured eDevice é usado por grandes empresas ao redor do mundo, incluindo instituições financeiras e agências de segurança do governo, bem como pequenas e médias empresas.

Benefícios de controle de dispositivo:

- Forte Controle de dispositivo I/O protege contra ameaças internas Políticas são aplicadas em todos os computadores, mesmo quando está offline ou conectado via VPN
- Implantação automática de políticas a todos os computadores, servidores e laptops
- Controle granular sobre precisamente quais dispositivos I/O cada usuário tem permissão para acessar
- Fácil de usar com gerenciamento central e controle
- Flexível e escalável para suportar novas necessidades de negócio
- Acompanhamento integral através de relatórios de atividade do usuário para o cumprimento regulamentar e de auditoria

9) Secured eDisk

- **Secured eDisk** - criptografia de disco rígido

Criptografia de disco rígido (HD)

Através do trabalho de colaboração empresarial e móvel, algumas das informações mais sensíveis da organização ficam armazenadas nos discos rígidos e em mídia removível. A perda, roubo ou apropriação indevida de um desses sistemas ou meios de comunicação poderia expor informações corporativas, registros de pessoal, os segredos do governo, ou de propriedade intelectual e produzir efeitos desastrosos para a organização. A solução de segurança permite proteger dados de ameaças e cumprir os regulamentos, sem a necessidade de administração de TI excessiva.

Secured eDisk Protect é um produto de criptografia completa de disco rígido que protege todos os discos rígidos em laptops, estações de trabalho e servidores, bem como mídias removíveis. Usando **Secured eDisk Protect**, as informações confidenciais permanecem seguras e mantêm compliance mesmo se um sistema é perdido, roubado ou eliminado de forma inadequada. A administração centralizada torna a proteção fácil de implantar e gerenciar.

- Criptografia 100% transparente
- Forte, com autenticação pré-boot com suporte para Tokens
- Integração com o Microsoft Active Directory
- Criptografia completa e parcial de disco rígido
- Fácil implantação de uma localização central
- Single sign-on
- Suporte a Hibernação