

APX Módulos DLP

OBTENHA VISIBILIDADE, CONTROLE E SEGURANÇA PARA DADOS CONFIDENCIAIS RECEBIDOS E ENVIADOS, APLIANDO OS RECURSOS DE DLP CORPORATIVO PARA SEUS CANAIS DE WEB E EMAIL

Desde danos a reputações até multas e penalidades de agências reguladoras, uma violação de dados pode ter consequências devastadoras para a sua empresa. Além disso, à medida que as forças de trabalho ficam mais móveis, é essencial obter visibilidade sobre os dados confidenciais que entram e saem da rede.

Para impedir os furtos de dados, demonstrar conformidade e proteger sua marca e propriedade intelectual, as defesas de TI devem funcionar fora da sua empresa. Você deve proteger os seus dados sensíveis em canais de Web e Email para sua força de trabalho móvel que trabalha fora da rede. Ampliar os recursos de DLP corporativos completos para suas defesas habilita você a implementá-los para canais de Web e Email e muito, muito mais.

POR QUE OS MÓDULOS FORCEPOINT™ WEB DLP E FORCEPOINT EMAIL DLP?

Os módulos Forcepoint Web DLP e Forcepoint Email DLP alavancam tecnologia altamente precisa e líder do setor para cumprir com rapidez e facilidade os requisitos de conformidade e regulatórios, ampliando os recursos de DLP completos de classe empresarial para os canais de Web e Email. Fornecem visibilidade em tempo real e histórica para a transmissão de dados confidenciais em todas as ocasiões. Com recursos exclusivos, incluindo OCR (reconhecimento óptico de caracteres) e identificação de criptografias personalizadas, Forcepoint leva o DLP de classe empresarial para um novo nível.

- Uma biblioteca abrangente de modelos out-of-the-box habilita configurar e implementar rapidamente políticas para identificar e impedir o furto de dados críticos.
- Com um assistente fácil de usar, implementar os módulos de DLP para Web e Email com seu pessoal existente nunca foi tão fácil.
- Obtenha visibilidade para dados recebidos e enviados em sua rede com canais de Web e Email
- Evite "drip-DLP," o furto lento de dados de números de cartões de crédito ou outros registros, um ou dois de cada vez.
- Impeça Ameaças Internas com análises comportamentais que identificam e sinalizam as que apresentam risco para sua empresa.
- O OCR (reconhecimento óptico de caracteres) expõe texto em uma imagem para impedir que os dados saiam ocultos em capturas de tela, fotos e outras imagens.
- Com AP-EMAIL, aplique políticas de DLP a tráfego do Microsoft Office 365 para proteger dados confidenciais enquanto adota novas tecnologias.
- Remedie dados confidenciais, com recursos para auditar, bloquear, permitir, alertar, notificar, colocar em quarentena* ou criptografar*, quando encontrados. (* somente para o módulo Email DLP)



SOLUÇÃO COM IMPLEMENTAÇÃO RÁPIDA QUE IMPEDE QUE MEUS DADOS CRÍTICOS SAIAM DA REDE POR CANAIS DE WEB E EMAIL

Com uma biblioteca abrangente de modelos e políticas out-of-the-box, o Forcepoint habilita você a começar rapidamente a proteger os seus dados confidenciais

PRECISO ADMINISTRAR COM EQUIPE EXISTENTE

A arquitetura Forcepoint TRITON® é totalmente integrada, que combina relatórios, gestão de dados e políticas em uma única interface de usuário para suas soluções de Web, Email, Dados, Nuvem e Móveis.

IDENTIFIQUE E EDUQUE USUÁRIOS DE ALTO RISCO

As análises comportamentais identificam e sinalizam os usuários que podem apresentar um risco para empresa devido a maus hábitos ou até insatisfação.

NÃO SEI QUAIS DADOS ESTÃO SAINDO DA MINHA REDE OU COMO

Obtenha visibilidade sobre os dados confidenciais que entram e saem de seus canais de Web e Email, com Forcepoint Web DLP e Forcepoint Email DLP.

VISIBILIDADE PARA OS DADOS CONFIDENCIAIS LOCALIZADOS EM IMAGENS DE ARQUIVOS LEGADOS DIGITALIZADOS

Forcepoint Optical Character Recognition (OCR) pode ver texto em imagens e aplicar políticas para impedir que dados confidenciais em imagens digitalizadas saiam da rede.

PRECISO GARANTIR QUE OS DADOS REGULADOS NÃO VAZEM DE MINHA REDE EM PEQUENOS LOTES

Interrompa o vazamento de dados lento com Forcepoint Drip DLP. Ao analisar os eventos cumulativos ao longo do tempo, detecta o furto "drip" de um registro ou número de cartão de crédito de cada vez.



A DIFERENÇA FORCEPOINT:

ACE (Advanced Classification Engine)

Forcepoint ACE fornece defesas contextuais em linha e em tempo real para segurança Web, Email, de Dados e Móvel, usando pontuação de riscos composta e análises preditivas para fornecer a segurança mais eficaz disponível. Também fornece contenção ao analisar o tráfego de entrada e saída com defesas com reconhecimento de dados para proteção líder do setor contra furto de dados. Classificadores para análise de segurança, dados e conteúdo em tempo real, resultantes de anos de pesquisa e desenvolvimento, habilitam o ACE a detectar mais ameaças do que os mecanismos antivírus tradicionais todos os dias (a comprovação é atualizada diariamente em <http://securitylabs.forcepoint.com>). O ACE é a defesa primária por trás de todas as soluções Forcepoint TRITON e é apoiado pelo Forcepoint ThreatSeeker Intelligence Cloud.

CONTATO

www.forcepoint.com/contact

SOBRE FORCEPOINT

Forcepoint™ é uma marca comercial da Forcepoint, LLC. SureView®, ThreatSeeker® e TRITON® são marcas comerciais registradas da Forcepoint, LLC. é uma marca comercial registrada da Raytheon Company. Todas as outras marcas comerciais e registradas pertencem aos respectivos proprietários.

[DATASHEET_MODULE_DLP_PT]-100007PT.011416

FORCEPOINT
TRITON® APX

www.forcepoint.com