Forcepoint DLP

IMPEÇA PERDA E FURTO DE DADOS, DEMONSTRE CONFORMIDADE E PROTEJA MARCAS, REPUTAÇÃO E PROPRIEDADE INTELECTUAL

FORCEPOINT
POWERED BY Raytheon

Forcepoint DLP

IMPEÇA PERDA E FURTO DE DADOS, DEMONSTRE CONFORMIDADE E PROTEJA MARCAS, REPUTAÇÃO E PROPRIEDADE INTELECTUAL

Desde danos a reputações até multas e penalidades de agências reguladoras, uma violação de dados pode ter consequências devastadoras. Forcepoint DLP habilita você a descobrir e proteger dados confidenciais não importa onde estejam – em pontos de extremidade, na nuvem ou no local. Amplie os negócios e impulsione a inovação, adotando com segurança serviços de colaboração na nuvem como Microsoft Office 365 e Box. Proteja ativos críticos de informação em computadores portáteis Mac OS X e Microsoft Windows. Proteja dados pessoais e propriedade intelectual, e cumpra casos de uso de conformidade rapidamente, com uma biblioteca abrangente de políticas out-of-the-box, usando os recursos de DLP exclusivos do Forcepoint para impedir furto de dados.

Forcepoint DLP habilita os seus negócios

- Reduza o risco de furto de dados ao adotar serviços em nuvem como Microsoft Office 365 e Box com aumento da visibilidade de dados.
- Implemente controles de segurança eficaz que você pode auditar facilmente para cumprir requisitos de conformidade e regulatórios.
- Identifique dados confidenciais em imagens, como dados digitalizados e capturas de tela.
- Identifique e impeça ameaças internas com análises comportamentais.
- Localize facilmente e proteja arquivos armazenados em dispositivos Mac, Microsoft Windows e Linux.
- Unifique suas soluções de segurança, coordene as políticas para defesas, compartilhe inteligência em vários pontos e aproveite a gestão centralizada de sua segurança de dados.
- A central de gestão de incidentes e o fluxo de trabalho de emails habilitam as pessoas certas a revisar e responder a incidentes de perda de dados.

Principais recursos

- Reconheça os dados confidenciais ocultos em imagens, documentos digitalizados e capturas de tela.
- Implemente com segurança os serviços na nuvem, como Microsoft Office 365 e Box, mantendo visibilidade e controle sobre dados confidenciais.
- O Drip DLP considera a transmissão cumulativa de dados para identificar pequenas quantidades de vazamentos de dados.
- Identifique funcionários de alto risco, identificando atividades que indicam furto de dados.
- Detecte dados com impressões digitais em dispositivos de ponto de extremidade dentro e fora da rede corporativa.
- Suporte para dispositivos de ponto de extremidade Mac OS X e Microsoft Windows.
- Detecte envio de dados confidenciais para fora da empresa por email, uploads na web, mensagens instantâneas e clientes de serviços em nuvem. Inclui descriptografia SSL quando usado com Forcepoint Web Security.

"O TRITON Architecture foi a solução mais forte que encontramos para proteger e prevenir contra vazamentos de dados"

—Amir Shahar, Gerente de Segurança da Informação, Cellcom Israel Ltd.

Recursos Forcepoint DLP

ADOTE A INOVAÇÃO COM CONFIANÇA

Atender as necessidades dos clientes e manter a competitividade requer inovar e habilitar sua força de trabalho para adotar novas tecnologias. Forcepoint DLP permite alavancar com segurança serviços potentes na nuvem, como Microsoft Office 365, Box e SalesForce. com, habilitando a sua empresa a continuar a crescer e inovar. Forcepoint DLP habilita sua força de trabalho em roaming, protegendo seus dados confidenciais e sua propriedade intelectual dentro e fora da rede.

CUMPRA E DEMONSTRE A CONFORMIDADE

Uma biblioteca abrangente de políticas outof- the-box torna fácil para seu pessoal de TI implementar rapidamente os controles para cumprir os requisitos regulatórios e proteger a propriedade intelectual. Você pode escolher as políticas apropriadas para cumprir seus requisitos de conformidade, e também as políticas necessárias para sua propriedade intelectual. Forcepoint fornece um conjunto de recursos de detecção de PI avançados, flexível o suficiente para cumprir as necessidades de proteção de dados com uma interface do usuário fácil de usar, que permite selecionar as políticas para proteger a sua propriedade intelectual e seus dados confidenciais em um único modelo. Forcepoint também ajuda a satisfazer auditores com relatórios personalizados, e habilita você a personalizar relatórios, conforme necessário.

LOCALIZE E PROTEJA DADOS CONFIDENCIAIS EM IMAGENS

Uma captura de tela maliciosa ou registros legados digitalizados e armazenados como imagens que apresentam pontos cegos para soluções DLP tradicionais, mas não para o Forcepoint DLP. Com o reconhecimento óptico de caracteres (OCR) da Forcepoint, você pode identificar de forma confiável e proteger dados confidenciais em uma imagem. Esse recurso exclusivo permite controlar o fluxo de informações confidenciais em capturas de tela, páginas de fax, fotos de smartphones e impressas, assim como documentos como cheques, recibos e arquivos legados digitalizados, protegendo contra ataques avançados e ameaça interna de furto de dados. Outros recursos exclusivos podem identificar métodos de criptografia personalizada e "Drip DLP" que são usados com frequência para evadir a detecção.

IDENTIFIQUE COMPORTAMENTOS DE USUÁRIO DE 'ALTO RISCO' E EDUQUE OS USUÁRIOS PARA AUMENTAR A CONSCIENTIZAÇÃO

Desde erros de usuários até conteúdo malicioso, os usuários finais com frequência estão no coração dos incidentes de perda de dados. Forcepoint DLP usa dados analíticos comportamentais para identificar proativamente os usuários de alto risco:

- Usuários ingênuos com freqüência geram risco, devido a maus hábitos que podem ser apontados e corrigidos antes que a perda de dados ocorra.
- Funcionários insatisfeitos podem ser identificados no início da atividade maliciosa.

Forcepoint DLP fornece com segurança para os usuários o acesso aos dados de que precisam para ajudar a impulsionar a empresa para a frente, mitigando simultaneamente as ameaças internas.

Componentes do Forcepoint DLP

Há duas opções principais do Forcepoint DLP, que podem ser implementadas juntas ou de forma independente para cumprir suas metas de segurança. Isso fornece flexibilidade para satisfazer as necessidades atuais e capacidade para crescer com a empresa.

FORCEPOINT DLP DISCOVERY	Para proteger dados, você deve ter capacidade para localizá-los onde quer que residam. Forcepoint DLP Discovery habilita você a localizar e proteger dados confidenciais na rede, e também os dados confidenciais armazenados em serviços na nuvem, como Microsoft Office 365 e Box. Com o acréscimo do Forcepoint DLP Endpoint, a potência do Forcepoint DLP Discovery pode ser ampliada para pontos de extremidade Mac OS X e Microsoft Windows dentro e fora da rede.
FORCEPOINT DLP NETWORK	A última chance para impedir o furto de dados é quando estão em movimento nos canais de Email e Web. Forcepoint DLP Network ajuda a identificar e impedir perda de dados maliciosa e acidental contra ataques externos ou da crescente Ameaça Interna. Técnicas contra evasão de ameaças avançadas com OCR potente para reconhecer dados em uma imagem. Use Drip DLP para impedir o furto de dados um registro de cada vez, e para monitoramento de comportamentos e anomalias para identificação de usuários de alto risco.
FORCEPOINT DLP ENDPOINT	Forcepoint DLP Endpoint estende OCR, 'Drip DLP' e outros controles contra perda de dados para os pontos de extremidade Mac OS X e Microsoft Windows, dentro e fora da rede. Forcepoint habilita o compartilhamento seguro de dados armazenados em dispositivos removíveis usando políticas para criptografia de arquivos. Monitoramento de uploads da web, incluindo HTTPS, e também uploads para serviços na nuvem, como Microsoft Office 365 e Box. Integração completa com Outlook, Notes e clientes de email, usando a mesma interface de usuário das soluções Forcepoint Data,Web, Email e Endpoint.
MÓDULO DE ANÁLISE DE IMAGEM	Para cumprir obrigações regulatórias em muitas partes do mundo, ou simplesmente garantir um ambiente sem assédio, o módulo opcional de análise de imagem permite identificar imagens explícitas, como pornografia, armazenadas na rede da empresa ou em movimento por canais de Email ou Web.

“Eu durmo melhor à noite sabendo que os nossos dados estão seguros com a Forcepoint.”

—Ahmet Taskeser, Senior SIMM Leader, Finansbank

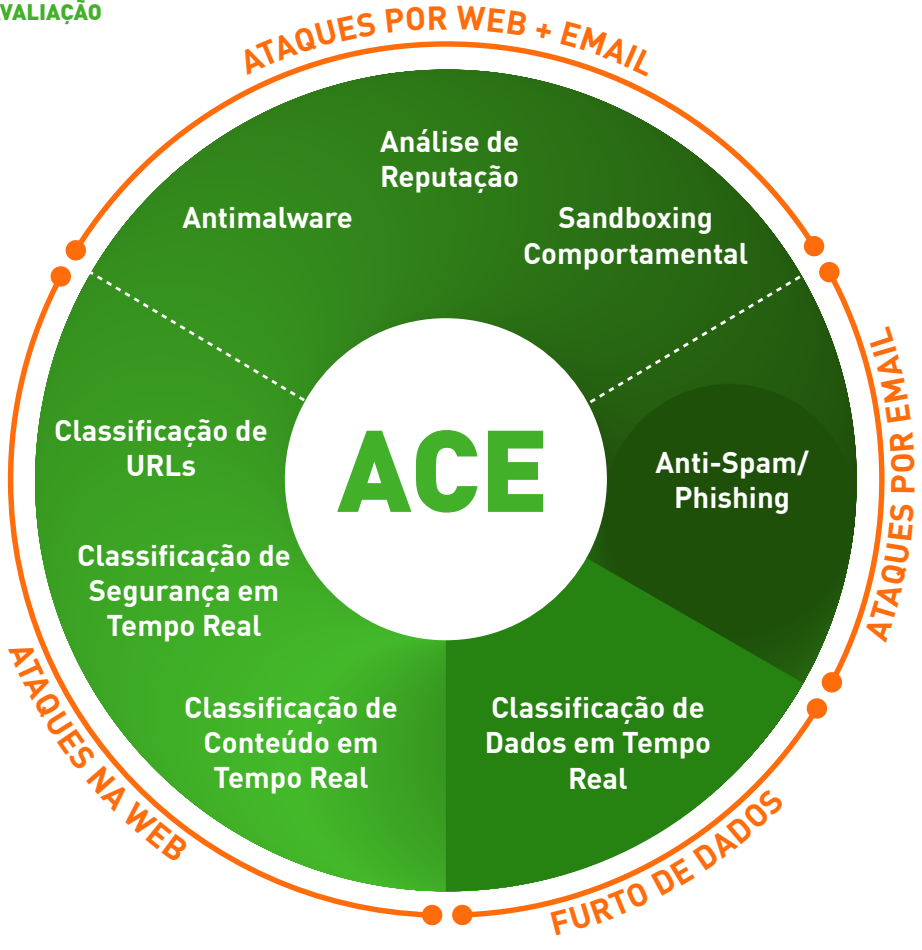
A potência por trás das soluções TRITON Architecture

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 Architecture e é apoiado pelo Forcepoint ThreatSeeker Intelligence.

CONJUNTO INTEGRADO DE RECURSOS DE AVALIAÇÃO DE DEFESAS EM 8 ÁREAS PRINCIPAIS.

- 10.000 dados analíticos disponíveis para apoiar inspeções profundas.
- Mecanismo de segurança preditivo que vê diversos movimentos à frente.
- A operação em linha não apenas monitora, mas **bloqueia** as ameaças.

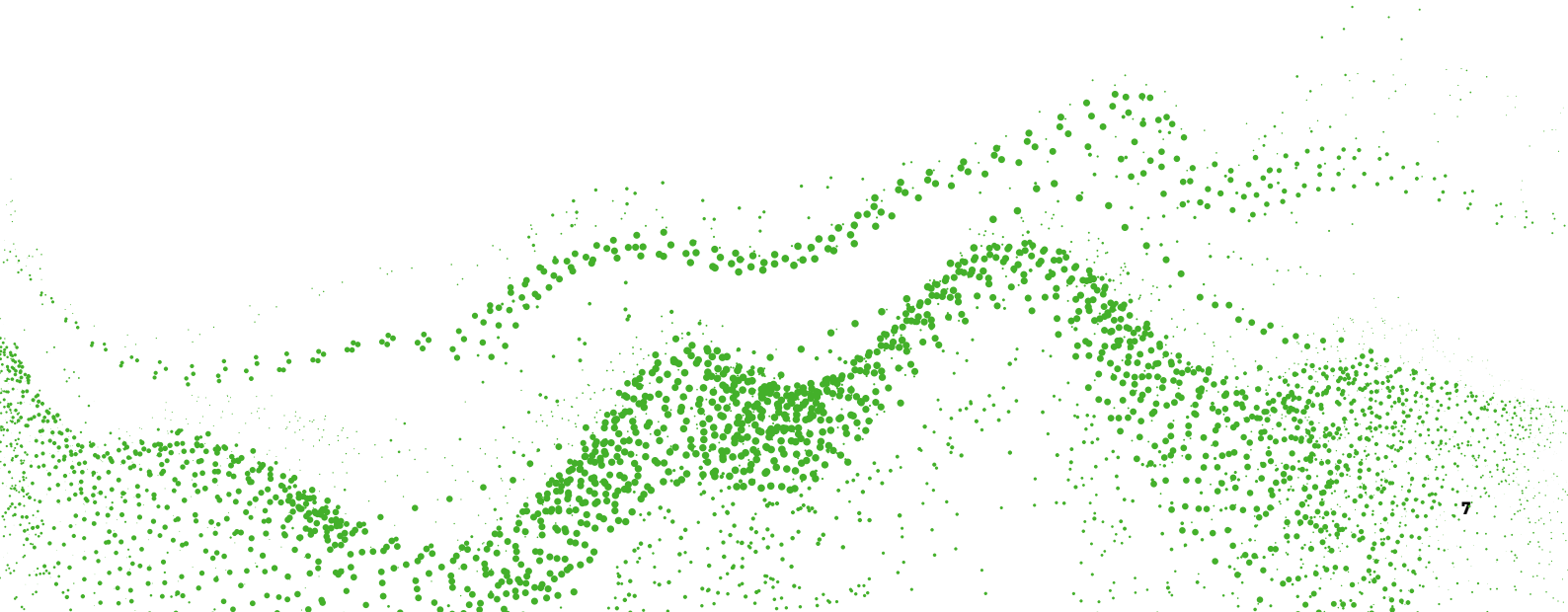


Forcepoint ThreatSeeker Intelligence

O Forcepoint ThreatSeeker Intelligence, administrado pelo Forcepoint Security Labs , fornece a inteligência de segurança coletiva essencial para todos os produtos de segurança Forcepoint. Reúne mais de 900 milhões de pontos de extremidade, incluindo entradas do Facebook e, em conjunto com as defesas de segurança do Forcepoint ACE, analisa até 5 bilhões de solicitações ao dia. Esse reconhecimento abrangente de ameaças de segurança habilita o Forcepoint ThreatSeeker Intelligence a oferecer atualizações de segurança em tempo real que bloqueiam Ameaças Avançadas, malware, ataques de phishing, fraudes e scams, e fornecem as avaliações da Web mais recentes. O Forcepoint ThreatSeeker Intelligence é incomparável em alcance e no uso das defesas em tempo real do ACE para analisar dados coletivos. (Quando você faz upgrade para Forcepoint Web Security, o Forcepoint ThreatSeeker Intelligence ajuda a reduzir a sua exposição a ameaças da web e furto de dados.)

TRITON Architecture

Com segurança melhor da categoria, a arquitetura unificada Forcepoint TRITON Architecture oferece proteção no ponto de clique com defesas em linha e em tempo real do Forcepoint ACE. As defesas em tempo real incomparáveis do ACE são apoiadas pelo Forcepoint ThreatSeeker Intelligence e os conhecimentos dos pesquisadores do Forcepoint Security Labs. O resultado potente é uma arquitetura única, com uma interface de usuário unificada e inteligência de segurança unificada.



CONTACT
www.forcepoint.com/contact

© 2017 Forcepoint. Forcepoint e o logotipo FORCEPOINT são marcas comerciais da Forcepoint. Raytheon é uma marca registrada da Raytheon Company. Todas as outras marcas comerciais utilizadas neste documento são de propriedade de seus respectivos proprietários.

[BROCHURE_FORCEPOINT_DLP_PT]-400004PT.030117

FORCEPOINT
POWERED BY Raytheon