Forcepoint Data Loss Prevention (DLP)

Proteção de dados em um mundo com perímetro zero

Forcepoint

Folheto

Forcepoint DLP

Segurança impulsionada pelo ponto humano

A segurança de dados é um desafio infinito. Por um lado, as organizações de TI devem cumprir as regulamentações e proteger a propriedade intelectual contra ataques direcionados e exposição acidental. Por outro, devem se adaptar a macromudanças na TI, como adoção de aplicativos em nuvem, ambientes de nuvem híbridos e tendências de "traga seu próprio dispositivo" (BYOD), que aumentam as formas como os dados podem sair de sua organização.

Essa superfície de ataque em expansão apresenta o desafio mais significativo para a proteção de dados críticos. As equipes de segurança de dados adotam a abordagem aparentemente lógica de correr atrás dos dados: encontrá-los, catalogá-los e controlá-los. No entanto, essa abordagem tradicional para a prevenção contra perda de dados deixou de ser eficaz, porque ignora a maior variável em segurança de dados—as pessoas.

Em vez de se concentrar exclusivamente nos dados, a segurança deveria começar e terminar com as pessoas. A chave é obter visibilidade sobre as interações dos usuários com dados e aplicativos. Depois que isso for alcançado, você pode aplicar um nível de controle com base no risco do usuário específico, e na confidencialidade ou no valor dos dados.

O programa de proteção de dados de uma organização deve considerar o ponto humano—a interseção de usuários, dados e redes. Além disso, a empresa deve manter a vigilância sobre os dados que percorrem a empresa e destacar as pessoas que criam, tocam e movimentam dados.

O Forcepoint DLP aborda o risco centrado nas pessoas com visibilidade e controle em todos os lugares onde as pessoas trabalham e em todos os lugares onde os seus dados residem. As equipes de segurança aplicam pontuação de riscos de usuários para ter foco nos eventos mais importantes e acelerar a conformidade com as regulamentações de dados globais.

A proteção de dados deve:

- **Proteger dados regulados** com um ponto de controle único para todos os aplicativos que as suas pessoas usam para criar, armazenar e movimentar dados.
- **Proteger a propriedade intelectual** com DLP avançado que analisa como as pessoas usam dados, orienta as pessoas para que tomem boas decisões com dados, e prioriza incidentes por risco.

Visibilidade e controle em todos os lugares onde as pessoas trabalham e os dados residem

- **Cloud Applications**
- **Endpoint**
- **Network**
- **Discovery**

Acelerar a conformidade

O ambiente de TI moderno apresenta um desafio intimidador para as empresas que procuram cumprir dúzias de regulamentações de segurança de dados mundiais, especialmente à medida que migram para aplicativos de nuvem e forças de trabalho móveis. Muitas soluções de segurança oferecem alguma forma de DLP integrado, como o tipo encontrado em aplicativos de nuvem.

Contudo, as equipes de segurança enfrentam complexidade indesejada e custos adicionais ao implementar e administrar políticas separadas e inconsistentes entre endpoints, aplicativos de nuvem e redes. O Forcepoint DLP acelera os seus esforços de conformidade, combinando cobertura em pacotes predefinidos para as regulamentações globais com controle central em todo o seu ambiente de TI. O Forcepoint DLP protege com eficiência as informações confidenciais de clientes e os dados regulados, para que você possa comprovar com confiança a conformidade constante.

- → **Cobertura regulatória** para cumprir e manter rapidamente a conformidade com mais de 370 políticas aplicáveis às demandas regulatórias de 83 países.
- → **Localizar e corrigir** dados regulados com descoberta de rede, nuvem e endpoints.
- → **Controle central** e políticas consistentes em todo o ambiente de TI.

Habilitar as pessoas para proteger os dados

O DLP que só contém controles preventivos frustra os usuários, que vão contorná-los com a intenção exclusiva de concluir uma tarefa. Contornar a segurança resulta em risco desnecessário e exposição de dados involuntária.

O Forcepoint DLP reconhece as pessoas como as vanguardas das ameaças digitais atuais.

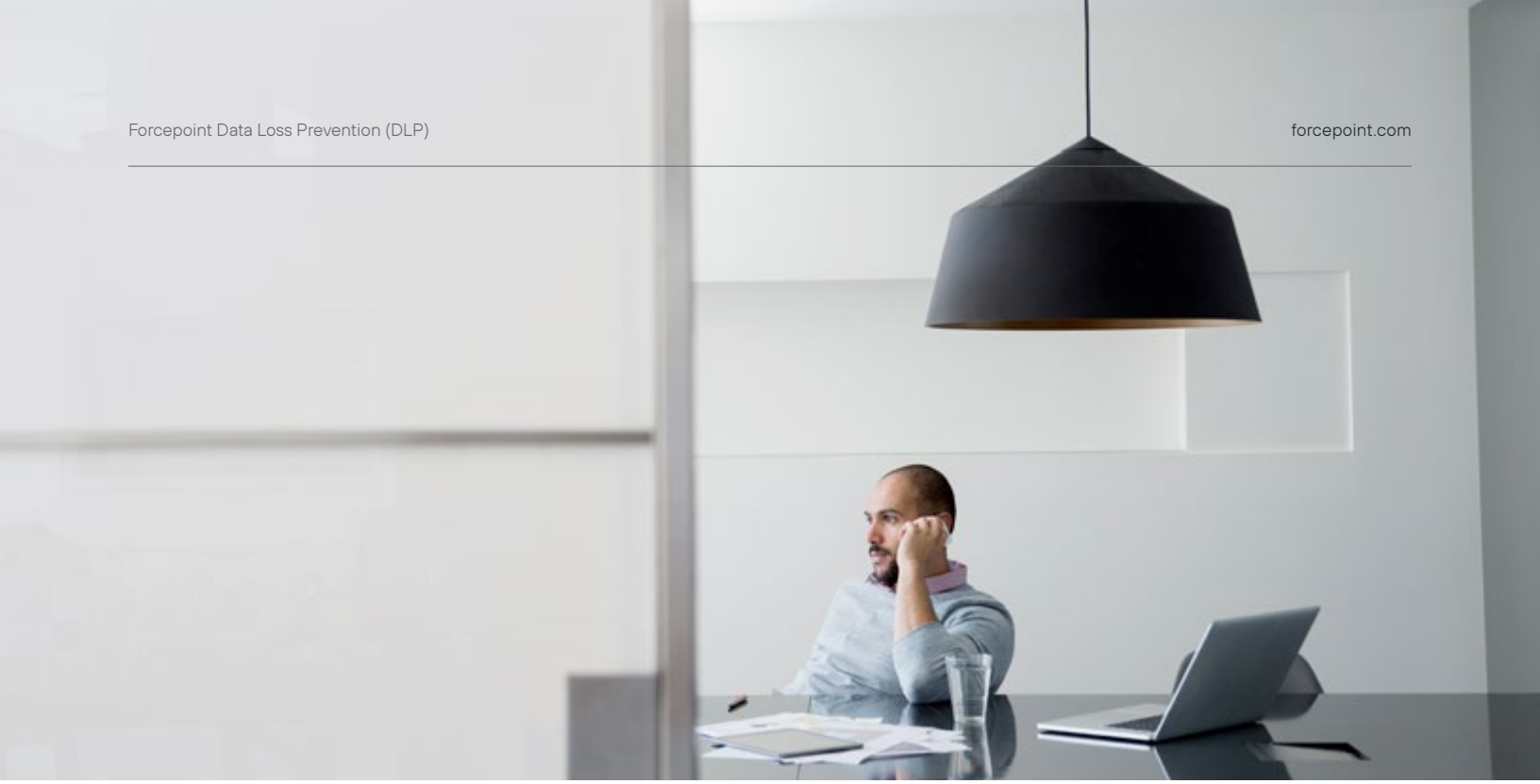
- → **Descobrir e controlar os dados** em todos os lugares onde residem, seja na nuvem ou na rede, por e-mail e no endpoint.
- → **Orientar os funcionários** para que tomem decisões inteligentes, usando mensagens que orientam ações dos usuários, informam os funcionários sobre as políticas e validam a intenção do usuário ao interagir com dados críticos.
- → **Colaborar com segurança** com parceiros confiáveis usando criptografia automática e baseada em políticas, que protege os dados movimentados fora de sua organização.
- → **Automatizar etiquetamento e classificação de dados**, interagindo com as principais soluções de classificação de dados de terceiros (por exemplo, Microsoft Azure Information Protection, Titus, Boldon James).

Detecção avançada e controles que seguem os dados

As violações de dados maliciosas e acidentais são incidentes complexos, não são eventos únicos. O Forcepoint DLP é uma solução comprovada que empresas de análises (incluindo Gartner, Radicati e outras) reconhecem como líder no setor. As ofertas de DLP da Forcepoint estão disponíveis em duas versões: DLP for Compliance e DLP for Intellectual Property (IP) Protection.

O Forcepoint DLP for Compliance and IP Protection fornece recursos críticos que abordam a conformidade com opções como:

- → **Reconhecimento óptico de caracteres (OCR)** identifica dados incorporados em imagens quando armazenados ou em trânsito.
- → **Identificação robusta** para Informações de Identificação Pessoal (PII) oferece verificações de validação de dados, detecção de nome verdadeiro, análise de proximidade e identificadores de contexto.
- → **Identificação de criptografia personalizada** expõe dados ocultos contra descoberta e controles aplicáveis.
- → **Análise cumulativa** para detecção com Drip DLP (ou seja, dados que saem lentamente ao longo do tempo).
- → **Integração com Microsoft Azure Information Protection** analisa arquivos criptografados e aplica controles de DLP apropriados aos dados.



O Forcepoint DLP for IP Protection inclui as opções acima, e também aplica a detecção e controle mais avançados de perda de dados potenciais, com recursos como:

- → **Aprendizado de máquina** permite que os usuários treinem o sistema para identificar dados relevantes e nunca vistos antes. Os usuários fornecem ao mecanismo exemplos positivos e negativos para marcar documentos empresariais similares, código-fonte e mais.
- → **Impressão digital** de dados estruturados (como bancos de dados) e não estruturados (como documentos) permite que os proprietários dos dados definam tipos de dados e identifiquem correspondências completas e parciais entre documentos de negócios, planos de design e bancos de dados, e depois apliquem o controle ou a política certos, de acordo com os dados.
- → **Análises** identificam mudanças no comportamento do usuário em relação à interação de dados, como aumento do uso de e-mail pessoal. Com Dynamic Data Protection (DDP), o Forcepoint DLP torna-se ainda mais eficaz, porque alavanca análises comportamentais para entender o risco de usuários, o que em seguida é usado para implementar políticas adaptadas aos riscos. Isso permite que as equipes de segurança implementem políticas dinâmicas e individualizadas, em vez de políticas globais estáticas.

Identificar, administrar e corrigir o risco de proteção de dados

As abordagens tradicionais para DLP sobrecarregam os usuários com falsos positivos e deixam de identificar dados em risco. Além de reduzir a eficácia das equipes de segurança, isso frustra os funcionários ou os usuários finais, porque eles consideram as soluções de segurança como um obstáculo à sua produtividade nos negócios. Com as análises, o Forcepoint DLP reduz os falsos positivos, o que ajuda nas operações de segurança. Para aumentar a conscientização de segurança dos funcionários, o DLP disponibiliza orientação de funcionários e integração com soluções de classificação de dados.

- → **Concentrar as equipes de resposta** no maior risco, com incidentes priorizados que destacam as pessoas responsáveis pelo risco, os dados críticos em risco e padrões comuns de comportamento entre usuários.
- → **Aumentar a conscientização dos funcionários** para tratamento de dados confidenciais e informações proprietárias com orientação dos funcionários em Windows e macOS, além de habilitar os funcionários com integração de soluções de classificação como Boldon James e Microsoft Azure Information Protection.
- → **Aplicar recursos de identificação de dados com DLP avançado**, como impressão digital, em endpoints de trabalho remoto e aplicativos de nuvem empresariais.
- → **Habilitar os proprietários de dados e gerentes de negócios** com fluxo de trabalho de incidentes distribuído por e-mail para revisar incidentes de DLP e responder.
- → **Proteger a privacidade dos usuários** com opções de anonimização e controles de acesso.
- → **Adicionar o contexto dos dados** nas análises de usuário mais abrangentes, em integrações profundas com Forcepoint Insider Threat e Forcepoint Behavioral Analytics.

Visibilidade em todos os lugares onde as pessoas trabalham, controle em todos os lugares onde os seus dados residem

Atualmente, as empresas enfrentam os desafios de ambientes complicados, em que os dados estão em todos os lugares, e precisam de proteção de dados em lugares que não são administrados ou de propiedade da empresa. O Forcepoint DLP for Cloud Applications amplia as análises e as políticas de DLP para aplicativos de nuvem críticos, de forma que seus dados sejam protegidos, não importa onde residam.

- → **Concentrar as equipes de resposta para identificar e proteger** dados em aplicativos de nuvem, armazenamentos de dados em rede, bancos de dados e endpoints administrados.
- → **Identificar e prevenir automaticamente** o compartilhamento de dados confidenciais para usuários externos ou usuários internos não autorizados.
- → **Proteger os dados** em tempo real para uploads e downloads de aplicativos de nuvem críticos, incluindo Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack e muitos outros.
- → **Unificar a aplicação de políticas** com console único para definir e aplicar políticas para dados em trânsito e descoberta de dados em todos os canais—nuvem, rede e endpoints.
- → **Implementar uma solução hospedada pela Forcepoint** que amplia os recursos de políticas de DLP, incluindo impressão digital e aprendizado de máquina, para os aplicativos de nuvem, com a opção de manter osincidentes e dados forenses em seu datacenter.

O Forcepoint DLP inclui análises avançadas e modelos de política regulatória com um único ponto de controle em todas as implementações. As empresas escolhem as opções de implementação adequadas a seu ambiente de TI.

Apêndice A: Visão geral dos componentes da solução de DLP

Forcepoint DLP – Endpoint	O Forcepoint DLP – Endpoint protege seus dados críticos em endpoints Windows e Mac, dentro e fora da rede corporativa. Inclui proteção e controle avançados para dados armazenados (descoberta), em trânsito e em uso. Integra-se com Microsoft Azure Information Protection para analisar dados criptografados e aplicar controles de DLP apropriados. Habilita a autocorreção do risco de dados pelos funcionários, com base em orientação de diálogos de orientação de DLP. A solução monitora uploads da web, incluindo HTTPS, e também uploads para serviços na nuvem como Office 365 e Box Enterprise. Integração completa com Outlook, Notes e clientes de e-mail.
Forcepoint DLP – Cloud Applications	Habilitado pelo Forcepoint CASB, o DLP – Cloud Applications estende as análises avançadas e o controle unificado do Forcepoint DLP para aplicativos de nuvem aprovados, incluindo Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack e muitos outros.
Forcepoint DLP – Discovery	O Forcepoint DLP – Discovery identifica e protege dados confidenciais em servidores de arquivos, SharePoint (no local e na nuvem), Exchange (no local e na nuvem), e detecção em bancos de dados como SQL Server e Oracle. Tecnologias avançadas de impressão digital identificam dados regulados e propriedade intelectual armazenados e protegem esses dados, aplicando criptografia e controles apropriados. O Discovery também inclui OCR, que fornece visibilidade sobre dados em imagens.
Forcepoint DLP – Network	O Forcepoint DLP – Network entrega o ponto de aplicação crítico para impedir o roubo de dados em trânsito por canais de e-mail e web. A solução ajuda a identificar e prevenir exfiltração de dados e perda de dados acidental contra ataques externos ou ameaças internas. O OCR reconhece dados em uma imagem. As análises identificam DLP para impedir o roubo de dados em um registro de cada vez, e outros comportamentos de usuário de alto risco.

Apêndice A: Visão geral dos componentes da solução de DLP

	FORCEPOINT DLP – ENDPOINT	FORCEPOINT DLP – CLOUD APPLICATIONS	FORCEPOINT DLP – DISCOVER	FORCEPOINT DLP – NETWORK
Como é implementado?	Forcepoint One Endpoint	Forcepoint Cloud	Discovery Server administrado pela TI	Appliance de rede ou nuvem pública
Qual é a função primária?	Coleta de informações no endpoint do usuário	Descoberta de dados e aplicação de políticas na nuvem ou com aplicativos entregues na nuvem	Descoberta, exame e correção de dados armazenados em datacenters	Visibilidade e controle para dados em trânsito por web e e-mail
Onde os dados são descobertos / protegidos quando armazenados?	Endpoints Windows, Endpoints MacOS	OneDrive, Sharepoint Online, Exchange Online, Google Drive, Box, DropBox, Salesforce, ServiceNow	Servidores de arquivos e armazenamentos de rede no local, servidor Sharepoint, servidor Exchange, bancos de dados como Microsoft SQL Server, Oracle e IBM DB2	
Onde os dados em trânsito são protegidos?	E-mail, Web: HTTP(S), impressoras, mídias removíveis, servidores de arquivos / NAS	Uploads, downloads e compartilhamento para Office 365, Google Apps, Salesforce.com, Box, Dropbox e ServiceNow via API e todos os outros apps principais proxy		E-mail, proxy ActiveSync, Web: HTTP(S) ICAP
Onde os dados em uso são protegidos?	Zoom, Webex, Google Hangouts, mensagens instantâneas, compartilhamentos de arquivos VOIP, aplicativos (clientes de armazenamento de nuvem), área de transferência do SO	Durante atividades de colaboração usando aplicativos de nuvem		
Dynamic Data Protection*	Suplemento			Suplemento
Reconhecimento óptico de caracteres			Incluído	Incluído
Integrações com classificação de dados e etiquetamento	Microsoft Azure Information Protection, Boldon James, Titus			
Onde pode haver impressão digital de dados?*	Dados estruturados (bancos de dados), não estruturados (documentos), binários (arquivos não textuais)			
Administração unificada de políticas	Configuração e aplicação de políticas com console único dos endpoints para aplicativos de nuvem Entre datacenters e na nuvem pública			
Biblioteca robusta de políticas	Descoberta e aplicação a partir de biblioteca de políticas de conformidade abrangente			

Os seres humanos são o novo perímetro.

Forcepoint

forcepoint.com/contact

Sobre a Forcepoint

A Forcepoint é líder em cibersegurança para proteção de usuários e dados, com a missão de proteger as organizações ao impulsionar transformação digital e crescimento. As soluções da Forcepoint adaptam-se em tempo real a como as pessoas interagem com dados, fornecendo acesso seguro e habilitando os funcionários a criar valor. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para milhares de clientes no mundo inteiro.

[DLP-BROCHURE-PT-BR] 3Nov2020