Forcepoint Data Loss Prevention

Proteção de dados em um mundo com perímetro zero

Forcepoint

Folheto

forcepoint.com/pt-br

Forcepoint Data Loss Protection (DLP)

Segurança de dados onde as suas pessoas trabalham e os dados residem

A segurança de dados é um problema importante para as organizações de todos os tipos e tamanhos atualmente. Por um lado, as organizações de TI têm obrigação de cumprir regulamentações e proteger informações de identificação pessoal (PII), informações de saúde protegidas (PHI) e outros tipos de informações regulamentadas contra ataques maliciosos direcionados, e também contra perda de dados 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 da organização.

Essa superfície de ataque em expansão é o desafio mais significativo para a proteção de dados críticos. As equipes de segurança de dados devem considerar a explosão da movimentação de dados de "dentro" da organização para todos os locais e canais onde os dados agora residem ou percorrem. É necessário obter visibilidade para todos os dados na nuvem e no local. As equipes de segurança de dados também devem ter visibilidade e controle em todos os canais (endpoint, tráfego da web, rede, e-mail, aplicativos em nuvem e aplicativos privados) com um ponto de administração único.

O Forcepoint DLP é a solução mais confiável do setor e oferece ferramentas para administrar facilmente políticas globais em todos os principais canais: endpoints, rede, nuvem, web, aplicativos privados ou e-mail. Nós podemos simplificar o seu trabalho com os modelos, as políticas e os classificadores mais predefinidos disponíveis, superando qualquer outro provedor de DLP do setor. Isso pode otimizar drasticamente o gerenciamento de incidentes, para que você possa se concentrar no que é mais importante, eliminando riscos para que seu pessoal seja cada vez mais produtivo. O Forcepoint DLP aborda o risco, fornecendo visibilidade e controle em todos os lugares onde suas pessoas trabalham e os seus dados residem.

A proteção de dados deve:

- **Proteger dados regulados** com um ponto de controle unico para todos os aplicativos que as suas pessoas usam para criar, armazenar e movimentar dados.
- **Proteja dados sensíveis a** com DLP avançado que analisa como as pessoas usam os dados, orienta a equipe para que tomem boas decisões com os dados e prioriza os incidentes de acordo com o risco.

Canais importantes protegidos

- **Aplicativos personalizados**
- **Cloud Applications**
- **Aplicativos privados**
- **Endpoint**
- **Network**
- **Discovery**
- **Web**
- **Email**

Acelerar a Conformidade

Habilitar as pessoas para proteger os dados

Detecção e Controle Avançados

Responder ao Risco e Corrigi-lo

Acelerar a conformidade

O ambiente de TI moderno apresenta um desafio intimidador para as empresas que procuram cumprir duzias de regulamentacoes de seguranca de dados mundiais, especialmente a medida que migram para aplicativos de nuvem e forcas de trabalho moveis. Muitas solucoes de seguranca oferecem alguma forma de DLP integrado, como o tipo encontrado em aplicativos de nuvem.

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 esforços de compliance, fornecendo mais de 1.600 classificadores, políticas e modelos predefinidos. Isso acelera a implementação inicial do DLP e simplifica a sua administração contínua. 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.

- → **Regule a cobertura** para atender e manter facilmente a conformidade com mais de 1.600 modelos, políticas e classificadores predefinidos aplicáveis às demandas regulatórias de 83 países e mais de 150 regiões.
- → **Localizar e corrigir** dados regulados com descoberta de rede, nuvem e endpoints.
- → **Central control** and consistent policies across all channels including cloud, endpoint, network, web and email.

Habilitar as pessoas para proteger os dados

O DLP que so contem controles preventivos frustra os usuarios, que vao contorna-los com a intencao exclusiva de concluir uma tarefa. Contornar a seguranca resulta em risco desnecessario e exposicao de dados involuntaria.

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

- → **Descobrir e controlar os dados** eem todos os lugares onde residem, seja na nuvem ou na rede, por e-mail e no endpoint.
- → **Orientar os funcionários** tpara que tomem decisoes inteligentes, usando mensagens que orientam acoes dos usuarios, informam os funcionarios sobre as politicas e validam a intencao do usuario ao interagir com dados criticos.
- → **Colaborar com segurança** com parceiros confiaveis usando criptografia automatica e baseada em politicas, que protege os dados movimentados fora de sua organizacao.
- → **Automatize o etiquetamento e a classificação de dados,** mediante integração com Forcepoint Data Classification e Microsoft Purview Information Protection.

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 reconhecido por Forrester, Gartner, Radicati Group e Frost & Sullivan como líder do setor em soluções de DLP. Uma das principais características do Forcepoint DLP é a capacidade de identificar dados armazenados, em trânsito e em uso. Destaques em identificação de dados:

- → **Reconhecimento óptico de caracteres (OCR)** identifica dados incorporados em imagens quando armazenados ou em transito.
- → **Identificação robusta** para Informacoes de Identificacao Pessoal (PII) oferece verificacoes de validacao de dados, deteccao de nome verdadeiro, analise de proximidade e identificadores de contexto.
- → **Identificação de criptografia personalizada** expoe dados ocultos contra descoberta e controles aplicaveis.
- → **Análise cumulativa** para deteccao com Drip DLP (ou seja, dados que saem lentamente ao longo do tempo).
- → **Integração com Forcepoint Data Classification,** utilizando modelos de IA/AM altamente treinados para fornecer classificação muito precisa dos dados em uso.

- → **Aprendizado de máquina** permite que os usuarios treinem o sistema para identificar dados relevantes e nunca vistos antes. Os usuarios fornecem ao mecanismo exemplos positivos e negativos para marcar documentos empresariais similares, codigo-fonte e mais.
- → **Impressão digital** de dados estruturados (como bancos de dados) e nao estruturados (como documentos) permite que os proprietarios dos dados definam tipos de dados e identifiquem correspondencias completas e parciais entre documentos de negocios, planos de design e bancos de dados, e depois apliquem o controle ou a politica certos, de acordo com os dados.
- → **Análises** identificam mudancas no comportamento do usuario em relacao a interacao 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 analises comportamentais para entender o risco de usuarios, o que em seguida e usado para implementar politicas adaptadas aos riscos. Isso permite que as equipes de seguranca implementem politicas dinamicas e individualizadas, em vez de politicas globais estaticas.

Identificar, administrar e corrigir o risco de proteção de dados

MAs abordagens tradicionais para DLP sobrecarregam os usuarios com falsos positivos e deixam de identificar dados em risco. Alem de reduzir a eficacia das equipes de seguranca, isso frustra os funcionarios ou os usuarios finais, porque eles consideram as solucoes de seguranca como um obstaculo a sua produtividade nos negocios. Com as analises, o Forcepoint DLP reduz os falsos positivos, o que ajuda nas operacoes de seguranca. Para aumentar a conscientizacao de seguranca dos funcionarios, o DLP disponibiliza orientacao de funcionarios e integracao com solucoes de classificacao de dados.

- → **Concentrar as equipes de respostae** no maior risco, com incidentes priorizados que destacam as pessoas responsaveis pelo risco, os dados criticos em risco e padroes comuns de comportamento entre usuarios.
- → **Aumente a conscientização dos funcionários** fsobre como lidar com dados confidenciais e informações proprietárias, com treinamento de funcionários nas plataformas Windows e macOS, além de possibilitar aos funcionários a integração de soluções de classificação como Forcepoint Data Classification e Microsoft Purview Information Protection.
- → **Aplicar recursos de identificação de dados com DLP avançado,** como impressao digital, em endpoints de trabalho remoto e aplicativos de nuvem empresariais.
- → **EHabilitar os proprietários de dados e gerentes de negócios** com fluxo de trabalho de incidentes distribuido por e-mail para revisar incidentes de DLP e responder.
- → **Proteger a privacidade dos usuários** com opcoes de anonimizacao e controles de acesso.
- → **Adicionar o contexto dos dados** nas analises de usuario mais abrangentes, em integracoes 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

As empresas atuais enfrentam os desafios de ambientes complicados, nos quais os dados estão em toda parte e precisam de proteção em lugares que não são administrados ou não são de propriedade da empresa. O Forcepoint ONE CASB, SWG e ZTNA ampliam as análises e as políticas de DLP para aplicativos críticos de nuvem, tráfego da web e aplicativos privados baseados na web, para que seus dados fiquem protegidos, onde quer que se encontrem. As APIs REST, como a API do Forcepoint DLP APP Data Security, trazem visibilidade e aplicação de DLP para aplicativos internos desenvolvidos de forma personalizada.

- → **Concentre as equipes de resposta para identificar e proteger** dados em aplicativos de nuvem, armazenamentos de dados em rede, bancos de dados, e endpoints gerenciados e não gerenciados.
- → **Identificar e prevenir automaticamente** o compartilhamento de dados confidenciais para usuarios externos ou usuarios internos nao autorizados.
- → **Proteger os dados** em tempo real para uploads e downloads de aplicativos de nuvem criticos, incluindo Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack e muitos outros.
- → **Unificar a aplicação de políticas** com console unico para definir e aplicar politicas para dados em transito e descoberta de dados em todos os canais—nuvem, rede e endpoints.
- → **Implementar uma solução hospedada pela Forcepoint** que amplia os recursos de politicas de DLP, incluindo impressao digital e aprendizado de maquina, para os aplicativos de nuvem, com a opcao de manter osincidentes e dados forenses em seu datacenter.
- → **Visualize incidentes e administre ferramentas de terceiros** por meio de APIs REST expostas. Automatize fluxos de trabalho de administração de incidentes e forneça suporte a processos de negócios que dependem de incidentes de DLP por meio de ferramentas de automação e serviço, como ServiceNow, Nagios e Tableau, bem como soluções SIEM/SOAR, como Splunk e XSOAR.

O Forcepoint DLP inclui analises avancadas e modelos de politica regulatoria com um unico ponto de controle em todas as implementacoes. As empresas escolhem as opcoes de implementacao 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 criticos em endpoints Windows e Mac, dentro e fora da rede corporativa. Inclui protecao e controle avancados para dados armazenados (descoberta), em transito e em uso. Integra-se com Microsoft Azure Information Protection para analisar dados criptografados e aplicar controles de DLP apropriados. Habilita a autocorrecao do risco de dados pelos funcionarios, com base em orientacao de dialogos de orientacao de DLP. A solucao monitora uploads da web, incluindo HTTPS, e tambem uploads para servicos na nuvem como Office 365 e Box Enterprise. Integracao completa com Outlook, Notes e clientes de e-mail.
Forcepoint ONE CASB	Com Forcepoint ONE CASB, estenda 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. Obtenha controle contínuo de dados críticos para os negócios, não importa onde os usuários estejam ou qual dispositivo usam.
Forcepoint ONE SWG	O Forcepoint ONE SWG permite acessar qualquer site ou fazer download de qualquer documento com segurança, e mantendo o desempenho de web de alta velocidade de que a sua equipe precisa. Integração com RBI para renderização de contêiner seguro de sites arriscados e Zero Trust CDR para sanitização completa de todos os documentos para download.
Forcepoint ONE ZTNA (lançamento no 2º semestre de 2023)	O Forcepoint ONE ZTNA oferece acesso remoto Zero Trust simples, seguro e escalável para aplicativos de nuvem internos e privados, sem necessidade de VPN, em dispositivos gerenciados e não gerenciados.
Forcepoint DLP —Discover	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 deteccao em bancos de dados como SQL Server e Oracle. Tecnologias avancadas de impressao digital identificam dados regulados e propriedade intelectual armazenados e protegem esses dados, aplicando criptografia e controles apropriados. O Discovery tambem inclui OCR, que fornece visibilidade sobre dados em imagens.
Forcepoint DLP —Network	O Forcepoint DLP – Network entrega o ponto de aplicacao critico para impedir o roubo de dados em transito por canais de e-mail e web. A solucao ajuda a identificar e prevenir exfiltracao de dados e perda de dados acidental contra ataques externos ou ameacas internas. O OCR reconhece dados em uma imagem. As analises identificam DLP para impedir o roubo de dados em um registro de cada vez, e outros comportamentos de usuario de alto risco.
Forcepoint DLP for Cloud Email	O Forcepoint DLP for Cloud Email impede a exfiltração indesejada de seus dados e informações proprietárias por e-mail de saída. Você pode combinar com outras soluções Forcepoint DLP para canais, como Endpoint, Network, Cloud e Web, para simplificar seu gerenciamento de DLP, escrevendo uma política e implementando-a em vários canais. Diferente das soluções fora da nuvem, o Forcepoint DLP for Cloud Email tem imenso potencial para escalabilidade contra aumentos imprevistos de tráfego de e-mail. Também permite que o tráfego de e-mails de saída cresça junto com os seus negócios, sem precisar configurar e administrar recursos de hardware adicionais
Forcepoint DLP App Data Security API	A API de Forcepoint DLP App Data Security facilita para as organizações a proteção de dados em seus aplicativos e serviços personalizados internos. Ela permite a análise de tráfego de arquivos e dados e aplica ações de DLP, como permitir, bloquear, solicitar confirmação com um pop-up personalizado, criptografar, cancelar compartilhamento e quarentena. É uma API REST fácil de entender e simples de usar, sem necessidade de treinamento extenso ou conhecimento de protocolos complexos. Também é neutra em relação à linguagem, permitindo desenvolvimento e consumo em qualquer linguagem de programação ou plataforma.

Apêndice B: Visão geral dos componentes da solução de DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD	FORCEPOINT ONE SWG	FORCEPOINT ONE ZTNA: FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (LANÇAMENTO NO 2° SEMESTRE DE 2023)
Qual é a função primária?	Descoberta de dados e aplicação de políticas de proteção de dados no endpoint do usuário por meio de aplicativos, web, impressão, mídias removíveis, por exemplo.	Descoberta de dados e aplicacao de politicas na nuvem ou com aplicativos entregues na nuvem	Descoberta, exame e correção de dados armazenados em datacenters e outros ambientes locais	Visibilidade e controle para dados em trânsito por web e webmail na rede	Visibilidade e controle para dados em trânsito por web e webmail na rede	Visibilidade e controle para dados em trânsito por e-mail externo	Visibilidade e controle de dados em aplicativos e serviços personalizados internos	Visibilidade e aplicação de políticas de proteção de dados para dados em trânsito (uploads e downloads) em um aplicativo privado corporativo
Onde os dados são descobertos / protegidos quando armazenados?	Windows endpoints MacOS endpoints	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 uso são protegidos?	E-mail, Web: HTTP(S), impressoras, midias removiveis, 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 de uso frequente via proxy		E-mail, impressoras, web: HTTP(S) ICAP	Email	HTTP(S)	Aplicativos personalizados internos e serviços personalizados	Uploads e Downloads via ZTNA Connector para aplicativos privados
Onde os dados em uso são protegidos?	Zoom, Webex, Google Hangouts, mensagens instantâneas, compartilhamento de arquivos VOIP, compartilhamento em M365 Teams, aplicativos (clientes de armazenamento de nuvem), área de transferência do sistema operacional	Durante atividades de colaboracao usando aplicativos de nuvem					Aplicativos personalizados internos e serviços personalizados	

Apêndice B: Comparação de recursos de componentes da solução DLP

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD	FORCEPOINT ONE SWG	FORCEPOINT ONE ZTNA: FORCEPOINT DLP APP DATA SECURITY API	FORCEPOINT ONE ZTNA (LANÇAMENTO NO 2º SEMESTRE DE 2023)
Proteção Adaptável ao Risco	Adicionar		Adicionar	Adicionar	Adicionar	Add-on; suporte atualmente com túneis GRE/ IPSec com Forcepoint ONE SWG		
Reconhecimento óptico de caracteres			Incluido	Incluido	Incluido			Suporte a OCR para melhoria do DLP (2º semestre de 2023)
Integrações com classificação de dados e etiquetamento	Forcepoint Data Classification e Microsoft Purview Information Protection.							
Onde pode haver impressão digital de dados?*	Dados estruturados (bancos de dados), não estruturados (documentos), binários (arquivos não textuais)							Disponível no 2º semestre de 2023
Administração unificada de políticas	Configuração e aplicação de políticas com console único dos endpoints para aplicativos de nuvem							Disponível no 2º semestre de 2023
Biblioteca robusta de políticas	Descoberta e aplicação da maior biblioteca de políticas de conformidade do setor							

Forcepoint

forcepoint.com/contact

Sobre a Forcepoint

A Forcepoint simplifica a segurança para empresas e governos globais. A plataforma all-in-one verdadeiramente nativa da nuvem da Forcepoint facilita a adoção de Zero Trust e evita roubo ou perda de dados confidenciais e propriedade intelectual, não importa onde as pessoas estejam trabalhando. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para clientes e seus funcionários em mais de 150 países. Entre em contato com a Forcepoint em www.forcepoint.com, Twitter e LinkedIn.

[FP-DLP-Brochure-PT-BR] 018Aug2023