Forcepoint

Resumo da Solução

# Forcepoint Data Loss Prevention for Cloud Email

Proteja e controle o seu e-mail, alavancando a tecnologia de DLP mais confiável do setor

## Desafio

- Dados confidenciais estão saindo das organizações em quantidades crescentes por meio de vários canais.
- O e-mail é mencionado como o vetor de ameaças mais popular para os ataques.
- Proteger dados sem sufocar a produtividade dos negócios nunca foi tão importante ou complexo.

## Solução

- A Forcepoint estende a solução de DLP mais confiável do setor para o canal de e-mail.
- Monitore com precisão e previna a perda de dados confidenciais por e-mail.
- Alavanque uma solução de nuvem totalmente administrada para dimensionar a proteção de e-mail de saída e atender às demandas de sua empresa.

## Resultado

- Ganhe eficiência reduzindo drasticamente o número de incidentes falso-positivos por e-mail
- Aumente a conformidade com 3x mais políticas predefinidas do que qualquer outro fornecedor de DLP.
- Migre seu DLP para Forcepoint em menos de 6 semanas, aproveitando a experiência da Forcepoint, políticas prontas para uso e transferência de conhecimentos de primeira linha.

**A segurança de dados continua a crescer como um dos principais focos para as organizações no mundo inteiro. Não importa se os funcionários estão trabalhando dentro dos limites tradicionais de um escritório, ou com a nova norma de trabalho híbrido ou remoto: manter os dados seguros em vários canais é cada vez mais complexo. O e-mail é um canal crítico para as organizações obterem visibilidade e controle para impedir a exfiltração de dados indesejados de arquivos, propriedade intelectual e dados valiosos. Alguns exemplos comuns de perda de dados por e-mail incluem:**

→ **Enviar arquivos ou dados de uma organização para contas** de e-mail privadas pelo e-mail da empresa.

→ **Dados confidenciais** que saem da organização por negligência do usuário ou contas comprometidas.

→ **Uma pessoa interna maliciosa que envia dados e arquivos confidenciais** para concorrentes externos, meios de comunicação e sites de Internet. Com frequência, a intenção é cometer fraudes, sabotar a organização ou roubar dados proprietários.

→ **Como resultado de ataques de phishing e malware, ou adware e spam,** usuários internos bem-intencionados cooperam involuntariamente com agentes mal-intencionados para exfiltrar dados críticos e propriedade intelectual.

**"O e-mail é o vetor de ameaças mais popular para os atacantes usarem para colocar malware em uma organização. O e-mail também é uma linha direta de contato entre usuários e criminosos cibernéticos, levando a bilhões de dólares em fraudes e comprometimento de e-mails comerciais todos os anos."**

IDC, WORLDWIDE MESSAGING SECURITY MARKET SHARES, 2021: HYBRID WORK DRIVES NEED FOR THREAT INVESTIGATION INTEGRATION, DOC # US49144522, JUNE 2022 IDC, PARTICIPAÇÕES NO MERCADO MUNDIAL DE SEGURANÇA DE MENSAGENS, 2021: TRABALHO HÍBRIDO IMPULSIONA A NECESSIDADE DE INTEGRAÇÃO DA INVESTIGAÇÃO DE AMEAÇAS, DOC N.º US49144522, JUNHO DE 2022

**É imperativo que as organizações tenham forte visibilidade e controle de seus e-mails de saída para proteger a propriedade intelectual contra os ataques direcionados, e também contra exposição acidental. A tecnologia que concretiza isso é a Proteção contra Perda de Dados (DLP, Data Loss Protection). De acordo com o IDC, "Nos últimos 24 meses, ocorreu um renascimento no mercado de tecnologias contra perda de dados. Técnicas de classificação manuais e misteriosas estão sendo substituídas por aprendizado de máquina e automatização. O contexto tornou-se o maior habilitador. A eficácia e a eficiência das soluções melhoraram."[1] A segurança de e-mail, combinada com todos os novos avanços em DLP que descobre, protege e controla informações confidenciais, é essencial para controlar o importante vetor de e-mail. Sem recursos fortes de DLP, as violações de segurança de e-mail podem prejudicar gravemente os negócios e a reputação da sua organização.**

## A vantagem do Forcepoint DLP for Cloud Email

Como líder em soluções de segurança de dados, o Forcepoint DLP for Cloud Email oferece visibilidade e controle sem precedentes para e-mails enviados. Em combinação com o DLP for Endpoints, Cloud, Web and Network, o DLP for Cloud Email oferece uma solução multifacetada e potente para proteger os dados da organização. O Forcepoint DLP foi projetado para evitar a perda de dados em todos os lugares onde seu pessoal trabalha e onde quer que seus dados residam.

### Identificação de dados extrema

O Forcepoint DLP fornece mais de 1.500 classificadores e modelos predefinidos que permitem implementação e identificação de dados confidenciais com rapidez. Também alavanca tecnologias avançadas, utilizando análise de linguagem natural, aprendizado de máquina e uma das tecnologias de impressão digital mais fortes do setor, para identificar com precisão dados armazenados, em trânsito e em uso. Para a segurança dos dados, a visibilidade é fundamental e o DLP Discover da Forcepoint permite uma forte visibilidade seguida pela identificação formal dos dados para que todas as formas de dados possam receber o controle adequado. Isso é importante por vários motivos:

- → **Conformidade.** O Forcepoint DLP abrange regulamentações críticas como GDPR, HIPA e muitas outras em 83 países para garantir que as organizações cumpram constantemente os padrões de conformidade.
- → **Simplicidade.** Criar e implementar classificadores que atendam às necessidades de uma organização e requisitos de negócios consome uma enorme quantidade de tempo e recursos para uma implementação de DLP. Com os modelos e classificadores predefinidos da Forcepoint, as organizações podem implementar rapidamente classificadores específicos para uma variedade de setores e tipos de dados, simplificando drasticamente o DLP.
- → **Eficiência.** Com a tecnologia abrangente de identificação de dados da Forcepoint, o Forcepoint DLP reduz drasticamente o número de falsos positivos, enquanto classifica e prioriza incidentes críticos para investigação.

### Controle unificado de políticas

Uma estratégia de DLP forte deve se estender por todos os canais principais, como endpoint, nuvem, web e e-mail. Muitas vezes, as organizações tratam cada um desses canais de forma isolada, com produtos de DLP diferentes que se concentram em um canal único, como nuvem ou e-mail. Com Forcepoint, você pode proteger todos esses canais com a mesma solução e administrá-los a partir de uma única política. Configurar uma vez e implementar várias vezes traz controle inigualável sobre os dados em sua organização, oferecendo um único painel de controle em todos os canais críticos onde ocorre perda de dados. O uso de políticas por meio do DLP for Cloud Email também pode permitir visibilidade sobre dispositivos adicionais, como tablets e telefones, que normalmente não são cobertos por soluções comuns de endpoint.

### Escalabilidade sem precedentes

O Forcepoint DLP for Cloud Email tem a vantagem de ser um serviço totalmente gerenciado na nuvem, entregando a elasticidade de recursos comuns em implementações em nuvem. Se, por exemplo, houver uma intensificação de e-mails de saída a qualquer momento, o DLP for Cloud Email permite expansão rápida e, em seguida, redução de recursos para atender efetivamente às demandas da intensificação. Também habilita o serviço de DLP contínuo para atender às crescentes demandas de sua organização sem precisar implementar e configurar hardware adicional para atender a essas demandas.

### Proteção adaptável ao risco

A Forcepoint é o primeiro fornecedor do setor a fornecer DLP adaptável ao risco. Por meio do monitoramento contínuo da atividade do usuário, a solução permite que seu pessoal fique livre para fazer mais e intervir apenas quando identificar atividades de alto risco ou padrões de comportamento arriscado. A automação permite a fiscalização quase em tempo real; em outras palavras, pode prever e interromper uma invasão antes que ela aconteça.

1 IDC, Worldwide Digital Loss Technologies Market Shares, 2020: DLP IS Dead, Long Live DLP, nº de doc US48261521, outubro de 2021

## Soluções Forcepoint DLP for Cloud Email

### DLP for Cloud Email - proteção de dados de saída

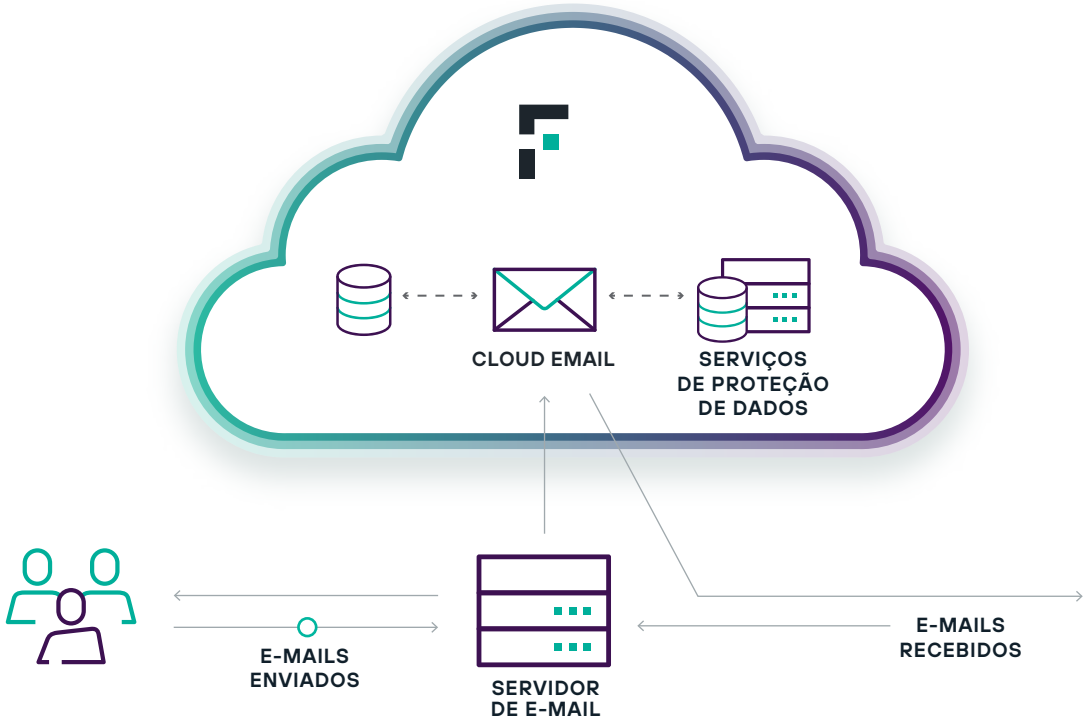
A Forcepoint simplifica a implementação do DLP for Cloud Email trabalhando em linha com seu fornecedor de segurança de e-mail atual para verificar e-mails de saída. Utilizando conectores universais do DLP for Cloud Email, a Forcepoint integra produtos populares de outros fornecedores, como Google e Microsoft, para encaminhar alguns ou todos os e-mails de saída para a Forcepoint Cloud. Ali, o Forcepoint DLP examina de acordo com as políticas de DLP e age em conformidade com o seu plano de DLP predefinido. Os e-mails podem ser permitidos, colocados em quarentena ou criptografados (com o módulo de criptografia separado) antes do envio. Notificações são enviadas sobre e-mails em quarentena, que podem ser configurados para retenção por até 30 dias, a menos que sejam liberados por um administrador autorizado. Para manter a reputação de uma organização, todos os e-mails de saída também são verificados quanto a spam, vírus e malware.

**Recursos padrão:**

- → **Interface de políticas simples** que oferece proteção contra vírus, malware e spam
- → **Painéis de controle, registros e relatórios de apresentação**
- → **Assinatura de e-mail pessoal**

**Suplementos:**

- → **Forcepoint Cloud Email Extended Reporting History** (opções para 6, 12 e 18 meses)
- → **Forcepoint Email Security Encryption Module**
- → **Forcepoint Email Security Image Analysis Module**




**forcepoint.com/contact**

© 2023 Forcepoint. Forcepoint e o logotipo da FORCEPOINT são marcas comerciais da Forcepoint. Todas as outras marcas registradas usadas neste documento pertencem às respectivas empresas
[FP-DLP For Cloud Email-Solution Brief-PT] 24Jul2023