

HUMAN-CENTRIC SECURITY

Implementação da segurança centrada em pessoas no espaço de trabalho digital moderno

Como a plataforma de proteção abrangente e multicamada da Proofpoint viabiliza a segurança centrada em pessoas na era da transformação digital

proofpoint®



Resumo executivo

O espaço de trabalho digital moderno mudou fundamentalmente a forma como o trabalho é realizado. Organizações adotaram a nuvem e funcionários agora colaboram em uma combinação complexa de ambientes. Estes incluem e-mail, ferramentas de colaboração e mensagens, plataformas de redes sociais, aplicativos de software como serviço (SaaS), grandes modelos de linguagem (LLMs) e serviços de compartilhamento de arquivos.

Essa mudança viabilizou inovações mais rápidas e mais flexibilidade. Contudo, ela também introduziu muitas novas superfícies de risco para perpetradores de ameaças explorarem. Os trabalhadores do conhecimento atualmente geram, armazenam e acessam dados de maneiras que as estratégias de segurança tradicionais, com foco em proteção de redes e endpoints, não conseguem mais acompanhar. Essas mudanças exigem uma arquitetura moderna, alinhada com a forma como organizações e indivíduos trabalham. Uma arquitetura que leva em consideração a realidade de que os usuários — e não a infraestrutura — são os principais alvos das ameaças cibernéticas.

Este white paper aborda como a Proofpoint foi a primeira a oferecer uma plataforma abrangente de Human-Centric Security compatível com essas novas realidades colocando as pessoas no centro da estratégia de defesa moderna.

Este paper:

- ✓ **Explica por que a proteção de pessoas importa** mais do que nunca no atual espaço de trabalho digital
- ✓ **Descreve os problemas centrados em pessoas** que a plataforma da Proofpoint foi criada para resolver
- ✓ **Examina as tecnologias essenciais** por trás de uma arquitetura que detecta ameaças proativamente, orienta e protege os usuários em tempo real e simplifica a investigação e a resposta

As pessoas são o novo perímetro: por que a segurança centrada em pessoas é fundamental

O centro do atual desafio da cibersegurança é o indivíduo. As ameaças centradas em pessoas, o que inclui phishing, sequestro de contas, risco interno e vazamento de dados, já constituem a maioria das violações. A maioria dos ataques modernos não exploram vulnerabilidades técnicas — eles exploram pessoas. Enganando, distraíndo ou manipulando, os perpetradores de ameaças visam usuários em espaços de trabalho digitais cada vez mais complexos.

O foco dos modelos de segurança tradicionais estava na proteção de redes e endpoints. As ameaças modernas, por outro lado, visam vulnerabilidades humanas. Com a plataforma de cibersegurança da Proofpoint, as organizações podem proteger pessoas e defender dados adotando uma abordagem centrada em pessoas. Nossa plataforma oferece as melhores soluções disponíveis para lidar com quatro preocupações críticas: deter ameaças, proteger informações, orientar usuários e fortalecer a postura de segurança de dados e SaaS.

PROTEÇÃO CONTRA AMEAÇAS

Detenha as ameaças que visam o seu pessoal

CONSCIENTIZAÇÃO QUANTO À SEGURANÇA

Ofereça orientação contínua aos funcionários

SEGURANÇA E GOVERNANÇA DE DADOS

Evite a perda de dados e controle as comunicações

POSTURA DE SEGURANÇA DE DADOS E SAAS

Corrija exposições de dados e SaaS

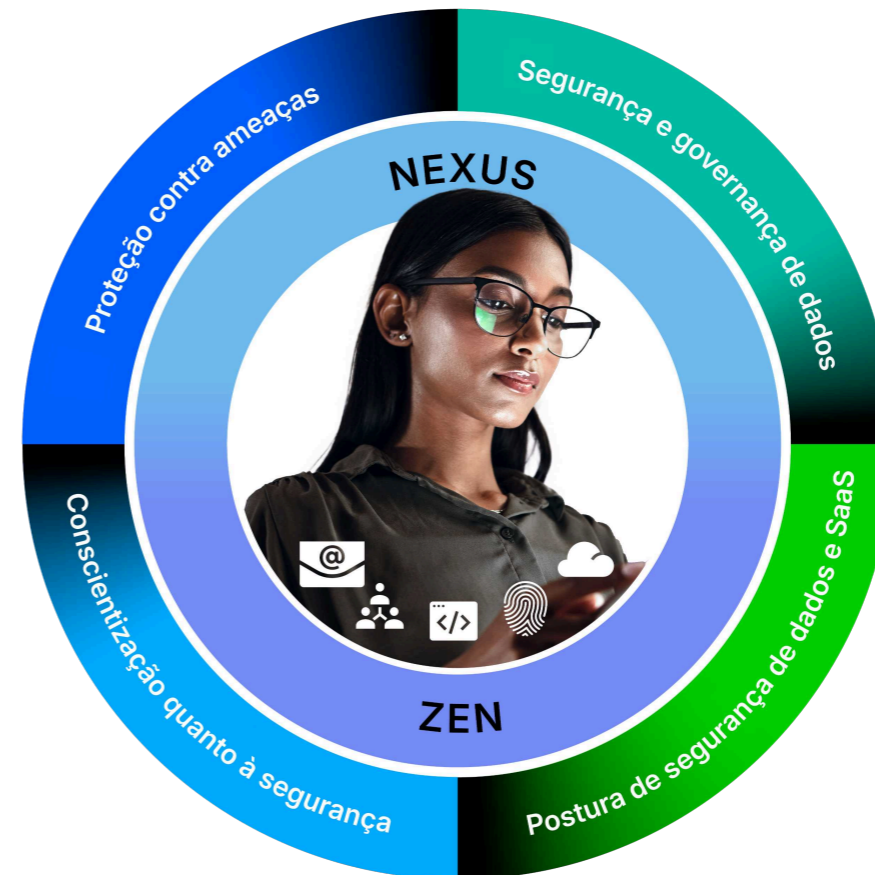


Figura 1. A plataforma de segurança centrada em pessoas da Proofpoint oferece as melhores soluções disponíveis em quatro áreas principais.

Uma plataforma de proteção abrangente e multicamada

A plataforma abrangente da Proofpoint baseia-se em uma arquitetura multicamada que:

- **Detecta ameaças proativamente** em todo o espaço de trabalho digital utilizando capacidades como inteligência artificial avançada, autoaprendizagem e inteligência sobre ameaças em tempo real
- **Oferece um amplo conjunto de pontos de controle do usuário final** que protegem pessoas e dados, não importando onde o trabalho aconteça
- **Alerta, orienta e capacita os usuários** a serem resilientes contra ataques direcionados contra pessoas
- **Simplifica a investigação e a resposta às ameaças**

Essas capacidades são impulsionadas por três tecnologias fundamentais: Proofpoint Nexus, Proofpoint Zen e Proofpoint Threat Protection Workbench. As seções seguintes abordam essas tecnologias.

IMPLEMENTAÇÃO DA SEGURANÇA CENTRADA EM PESSOAS NO ESPAÇO DE TRABALHO DIGITAL MODERNO



Proofpoint Nexus

Detecção respaldada por inteligência artificial e inteligência sobre ameaças

Proofpoint Nexus® é a camada de detecção da arquitetura da Proofpoint. Trata-se de uma plataforma de detecção unificada que conta com inteligência artificial, autoaprendizagem e inteligência sobre ameaças em tempo real.

O Proofpoint Nexus integra vários tipos de modelos de inteligência artificial. Cada um destes foi desenvolvido para analisar indícios de risco específicos em todas as formas como as pessoas trabalham. Isso inclui e-mail, aplicativos de nuvem, ferramentas de colaboração e navegadores.

Principais componentes da estrutura de detecção do Proofpoint Nexus

O **Nexus Threat Intelligence (TI)** assimila continuamente indícios de infraestruturas, campanhas e perpetradores de ameaças conhecidos e desconhecidos para proporcionar aos produtos da Proofpoint detecções com mais contexto e a capacidade de evitar técnicas de ameaças em evolução.

O **Nexus Language Model (LM)** aproveita o poder dos avançados modelos de linguagem de inteligência artificial para avaliar o tom, a urgência e a estrutura linguística das mensagens utilizadas em ataques de engenharia social como, por exemplo, comprometimento de e-mail corporativo (BEC).

O **Nexus Relationship Graph (RG)** correlaciona as atividades do usuário, o histórico comportamental e a importância do cargo para determinar a probabilidade de comportamentos arriscados ou de ataques direcionados contra indivíduos de alto risco.

O **Nexus Machine Learning (ML)** detecta comportamentos incomuns dos usuários em ferramentas de comunicação e colaboração, identificando indícios sutis, mas impactantes, de contas comprometidas ou de mau uso por parte de elementos internos.

O **Nexus Computer Vision (CV)** reconhece táticas de fraude visual e falsificação de marcas analisando o layout, o posicionamento do logotipo e imitações do design. Por meio de tecnologia avançada de visão computacional, ele detecta ameaças ocultas em elementos visuais, como sites de phishing, códigos QR, anexos maliciosos e e-mails falsificados.

O Proofpoint Nexus detecta ataques avançados de phishing, roubo de credenciais, tentativas de impostura e campanhas de ransomware. Em um caso da vida real, o Proofpoint Nexus identificou um comprometimento de fornecedor que resultou em uma fraude de faturamento contra um departamento financeiro. O Proofpoint Nexus bloqueou o ataque antes da execução identificando o uso de linguagem incomum e discrepâncias visuais e aplicando a inteligência sobre ameaças existente, obtida de seu conjunto de dados global.

O Proofpoint Nexus também é excelente na proteção de dados. Em um outro caso da vida real, quando um funcionário colocou dados de clientes em uma ferramenta de inteligência artificial generativa não autorizada, o Proofpoint Nexus detectou o padrão de dados confidenciais, elevou a pontuação de risco e bloqueou a ação.

O Proofpoint Nexus analisa mais de **2,6 bilhões de e-mails por dia, inspeciona mais de 450 milhões de URLs diariamente** e correlaciona indícios de centenas de perpetradores de ameaças. Essa escala imensa aumenta tanto a precisão quanto a responsividade em todo o cenário de ameaças.



Proofpoint Zen

Pontos de controle e orientação contextual para o usuário

O Proofpoint Zen™ é a camada de imposição e de orientação do usuário na arquitetura da Proofpoint. Ele impõe as políticas de segurança precisamente onde os usuários trabalham. Os pontos de controle no pacote Proofpoint Zen convertem inteligência em orientação conforme as políticas e proteção em tempo real. Isso ajuda os usuários a tomar decisões mais seguras sem perda de tempo.

Principais componentes do pacote Proofpoint Zen

O **Proofpoint Zen for Outlook** capacita os usuários a atuar como defensores de linha de frente ao incorporar ferramentas de segurança em seus fluxos de trabalho de e-mail. Com inteligência sobre ameaças em tempo real do Proofpoint Nexus, ele mostra alertas contextuais aos usuários quando estes recebem e-mails suspeitos, além de facilitar denúncias. Ele dá incentivos inteligentes para evitar comportamentos arriscados e alerta sobre dados confidenciais nos e-mails enviados.

O **Proofpoint ZenWeb** é uma extensão leve para navegadores baseados no Chromium que protege atividades de Web em SaaS, compartilhamento de arquivos e ferramentas de inteligência artificial generativa e protege os usuários contra sites de phishing. Ao utilizar detecções ao vivo por meio dos modelos de ameaças do Proofpoint Nexus, ele oferece detecção e prevenção de ameaças em tempo real, sem afetar a produtividade dos usuários.

O **Proofpoint Zen Endpoint DLP/Insider Threat Management** oferece proteção em nível de dispositivo contra perda de dados e ameaças internas monitorando o comportamento do usuário no endpoint. Ele monitora uso de USB, atividades na área de transferência, operações de sincronização de arquivos e comportamentos de aplicativos. Ele captura imagens de tela de ações suspeitas dos usuários e a cronologia das atividades dos usuários.

O **Proofpoint Zen Cloud API Connectors** estende a segurança a plataformas de SaaS baseadas em nuvem, como Microsoft 365, Google Drive, Slack e Box. Ele monitora uploads de arquivos e detecta comportamentos incomuns, como compartilhamento excessivo. Ele também viabiliza fluxos de trabalho personalizados em ferramentas de coordenação, automação e resposta (SOAR) e Okta.

O **Zen Communications Connectors** captura comunicações em plataformas regulamentadas, como Microsoft Teams, Zoom e Slack, para fins de arquivamento e supervisão. Ele assimila mensagens de vários canais em um formato de arquivamento unificado e se integra com ferramentas de supervisão para fluxos de trabalho jurídicos e de recursos humanos.

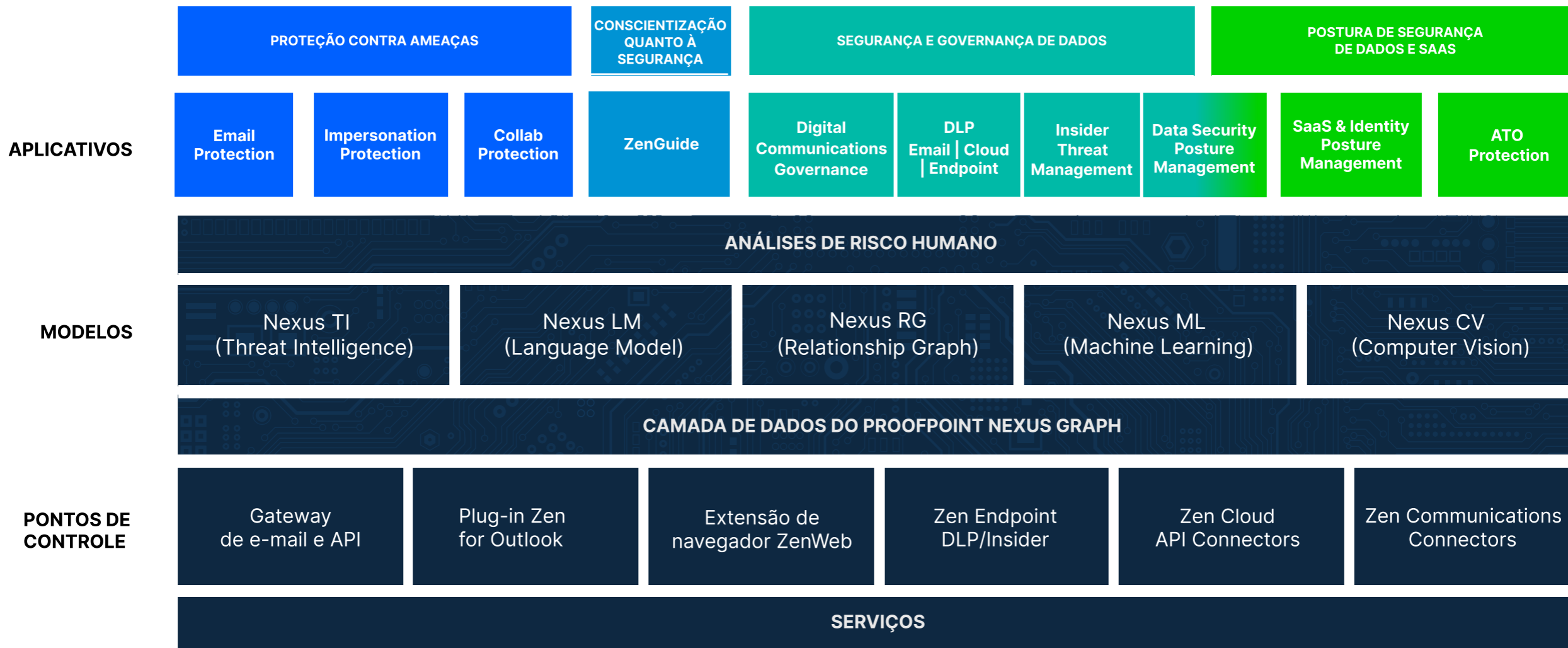


Figura 2. A plataforma de segurança centrada em pessoas da Proofpoint é construída com base em uma arquitetura multicamada. Os produtos da Proofpoint (em nossas áreas fundamentais de soluções de Proteção contra ameaças, Conscientização quanto à segurança, Segurança e governança de dados e Postura de segurança de dados e SaaS) utilizam diretamente as capacidades de nossas tecnologias essenciais Nexus e Zen.

Proofpoint Threat Protection Workbench

Investigação rápida e
remediação automatizada

Quando uma ameaça é detectada ou uma violação de política é sinalizada, rapidez e clareza tornam-se essenciais. Para as equipes de centros de operações de segurança (SOCs), múltiplos consoles, excesso de cliques e dependência de outras equipes aumentam o tempo de resposta e conseqüentemente aumenta o risco de ataques bem-sucedidos.

O Proofpoint Threat Protection Workbench é a camada de investigação e automação da arquitetura da Proofpoint. Ao oferecer um console intuitivo e centralizado, ele simplifica as investigações de ameaças e a remediação. Ele permite que as equipes de segurança façam triagem, analisem e respondam a ameaças sem os atrasos causados pela alternância entre ferramentas ou por dados fragmentados.

As equipes de segurança utilizam o Proofpoint Threat Protection Workbench para processar envios à caixa de correio para denúncia de abuso, escalar indícios de usuários de alto risco e investigar campanhas de ameaças. Ao correlacionar a inteligência sobre ameaças do Proofpoint Nexus com o comportamento do usuário e com os limites determinados pela política, o Proofpoint Threat Protection Workbench oferece alertas de alta fidelidade em vez de ruído indesejado.

Exemplos de casos de uso do Proofpoint Threat Protection Workbench

- Respostas automatizadas para investigações de sequestro de contas
- Visualizações de caminhos de cliques de usuários visados
- Resumo de ameaças complexas em múltiplos canais

Todas essas capacidades reduzem a carga de trabalho do analista e o tempo de permanência das ameaças. Para responder às ameaças, os analistas podem acionar roteiros diretamente ou utilizar APIs para escalá-las para outros componentes integrados em suas estruturas de segurança mais amplas.

Conclusão

Uma arquitetura criada especificamente para segurança centrada em pessoas

A natureza do risco cibernético mudou. As ameaças não visam apenas sistemas — elas visam pessoas. A complexidade do espaço de trabalho digital superou as defesas criadas para sua proteção. Conforme os usuários se movimentam livremente entre e-mail, navegadores, ferramentas de colaboração e aplicativos de nuvem, o modelo de segurança tradicional — criado com base em perímetros estáticos e controles padronizados — não consegue mais acompanhar as mudanças.

A plataforma da Proofpoint resolve esse desafio alinhando a arquitetura de segurança com a maneira como as pessoas trabalham. Por meio do Proofpoint Nexus, as organizações obtêm visibilidade orientada por inteligência artificial sobre ameaças centradas em pessoas, com base em inteligência sobre ameaças e análise comportamental inigualáveis. Com o Proofpoint Zen, nossa plataforma protege e orienta os usuários no momento certo, sem atrito. Com o Proofpoint Workbench, as equipes de segurança respondem mais rapidamente, com insights mais claros e com menos sobrecarga operacional.

Isso não é teoria. Nossa plataforma é uma arquitetura comprovada em escala de produção que reduz o risco e acumula resiliência a longo prazo. As organizações podem proteger os fluxos de trabalho de hoje e se prepararem para a próxima evolução do risco humano.

Ao combinar detecção de padrão internacional, controles comportamentais integrados e uma resposta rápida e integrada, podemos ajudar a sua organização a reduzir o risco onde mais importa: na interseção de pessoas, dados e ameaças.



proofpoint®

A Proofpoint, Inc. é uma empresa líder em cibersegurança e conformidade que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo 85% das empresas da Fortune 100, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em www.proofpoint.com/br.

Conecte-se com a Proofpoint: [LinkedIn](#)

Proofpoint é uma marca registrada ou marca comercial da Proofpoint, Inc. nos Estados Unidos e/ou em outros países. Todas as demais marcas comerciais aqui mencionadas são propriedade de seus respectivos donos.

DESCUBRA A PLATAFORMA DA PROOFPOINT →

0303-002-07-01