HUMAN-CENTRIC SECURITY

# O multiplicador de forças em uma arquitetura de cibersegurança moderna

Por que a segurança centrada em pessoas é um elemento fundamental em uma estratégia de defesa moderna, adaptando, conectando e maximizando os seus investimentos atuais em cibersegurança

proofpoint.

# Resumo executivo

Uma responsabilidade crucial do CISO moderno é determinar os investimentos estratégicos críticos a serem feitos na arquitetura de cibersegurança da empresa. Há alguns pilares de segurança bem reconhecidos — como borda de serviço de acesso seguro (SASE), detecção e resposta estendidas (XDR) e identidade — que precisam estar no núcleo da estratégia de defesa da organização. Esses pilares não podem funcionar independentemente. Eles precisam atuar conjuntamente para assegurar que a arquitetura enfrente as ameaças atuais e prepare a organização para as ameaças futuras. Contudo, embora cada um desses pilares seja um componente fundamental, nenhum deles leva em consideração a maior ameaça de todas — as pessoas e o que elas fazem.

A segurança centrada em pessoas fecha o cerco: da caixa de entrada ao endpoint, da identidade às ameaças internas. Porque por trás de cada violação há um ser humano: comprometido, descuidado ou malicioso.

Este white paper explora como a segurança centrada em pessoas é o elemento crítico — e transformador — em uma arquitetura de cibersegurança moderna.

**Este paper:**

- **Explica como a segurança centrada em pessoas desempenha um papel crucial** na sua arquitetura como um todo, eliminando pontos cegos na sua proteção existente e detectando riscos causados por seres humanos no atual espaço de trabalho digital.
- **Apresenta a plataforma de segurança centrada em pessoas da Proofpoint.** Este paper descreve como a Proofpoint atua como um plano de controle estratégico, amplificando os seus investimentos existentes em segurança e protegendo a sua organização contra ameaças centradas em pessoas.

# Além de perímetros e produtos isolados: o que não funciona

Muitos CISOs ainda combatem ameaças modernas com modelos ultrapassados. Isso significa controles compartimentados, insights fragmentados e ferramentas que não se adaptam com a rapidez necessária. A superfície de ataque mudou — e a sua reação também precisa mudar.

Esta é a nova realidade: os atacantes de hoje visam pessoas, e não portas. Com a expansão dos espaços de trabalho digitais, os adversários estão visando seres humanos no e-mail e em vários outros canais digitais. Isso inclui ferramentas de colaboração e mensagens, plataformas de redes sociais, aplicativos de nuvem, grandes modelos de linguagem (LLMs) e serviços de compartilhamento de arquivos. Os atacantes também podem sequestrar comunicações empresariais confiáveis e interromper relacionamentos com fornecedores e clientes.

Ao mesmo tempo, os dados não se perdem sozinhos. Por trás de cada incidente de perda de dados estão ações humanas. Usuários descuidados negligenciam o tratamento de dados críticos ou confidenciais. Usuários maliciosos vão embora com os dados. Malfeitores comprometem contas de usuário para roubar dados. Usuários fora de conformidade fazem uso indevido dos dados.

Escolher as melhores ferramentas disponíveis continua sendo importante. Porém, os CISOs de hoje em dia também precisam se concentrar na construção de uma arquitetura inteligente e coesa — que evolua com o cenário de ameaças e que assegure que essas ferramentas trabalhem juntas para proporcionar os resultados de defesa esperados.

**Na Proofpoint, nós criamos algo único no setor:** uma plataforma abrangente de Human-Centric Security que atua como um multiplicador de forças — amplificando os seus investimentos em segurança para e-mail, identidades, dados e acessos.

Nós não nos limitamos a fechar lacunas de segurança. Por meio de integrações profundas com parceiros como CrowdStrike, Okta, Zscaler, Microsoft, Palo Alto Networks e outros, nós minimizamos o tempo de permanência, neutralizamos ataques com antecedência e devolvemos tempo para a sua equipe de segurança.

Se você conta conosco apenas para proteção de e-mail, estamos apenas começando. Seja bem-vindo à era das plataformas.

proofpoint.

# Os pilares fundamentais de uma arquitetura moderna de cibersegurança

Todo CISO os reconhece. Estes são os pilares fundamentais reconhecidos de uma arquitetura moderna de cibersegurança: **SASE, XDR, identidade e SecOps/automação.** Conforme descrito a seguir, cada um deles é essencial e resolve um conjunto importante de preocupações de risco. Há, porém, um problema: nenhum deles leva em consideração o maior risco no atual cenário de segurança — as pessoas. **Por isso a segurança centrada em pessoas é, atualmente, o pilar mais importante de todos.**

**SecOps e automação** Simplifica detecção, investigação e resposta eliminando o trabalho manual e os fluxos de trabalho compartimentados. Resolve tempos de resposta excessivos, fadiga de alertas e ineficiência operacional. A Proofpoint automatiza a triagem de ameaças e a imposição de políticas com roteiros integrados, insights detalhados de risco humano e APIs flexíveis. Isso permite que equipes de centros de operações de segurança (SOCs) reajam mais rapidamente e com mais precisão.

## SASE

Permite acesso seguro e otimizado a aplicativos e dados, independentemente do dispositivo ou da localização do usuário. Resolve forças de trabalho distribuídas, acesso à nuvem e imposição consistente de políticas em ambientes remotos. Quando informado por sinais de risco centrados em pessoas, o SASE pode priorizar a proteção de comportamentos ou usuários de alto risco.

## Segurança centrada em pessoas

Coloca as pessoas no centro da proteção considerando a realidade de que os usuários — e não a infraestrutura — são os principais alvos das ameaças cibernéticas. A plataforma de Human-centric Security da Proofpoint resolve phishing, perda de dados e comprometimento de contas combinando detecção de ameaças à base de inteligência artificial com orientação de usuários em tempo real. Para reduzir o risco centrado em pessoas, nossas tecnologias Nexus e Zen identificam com exclusividade e precisão exposições, comportamentos e usuários arriscados.

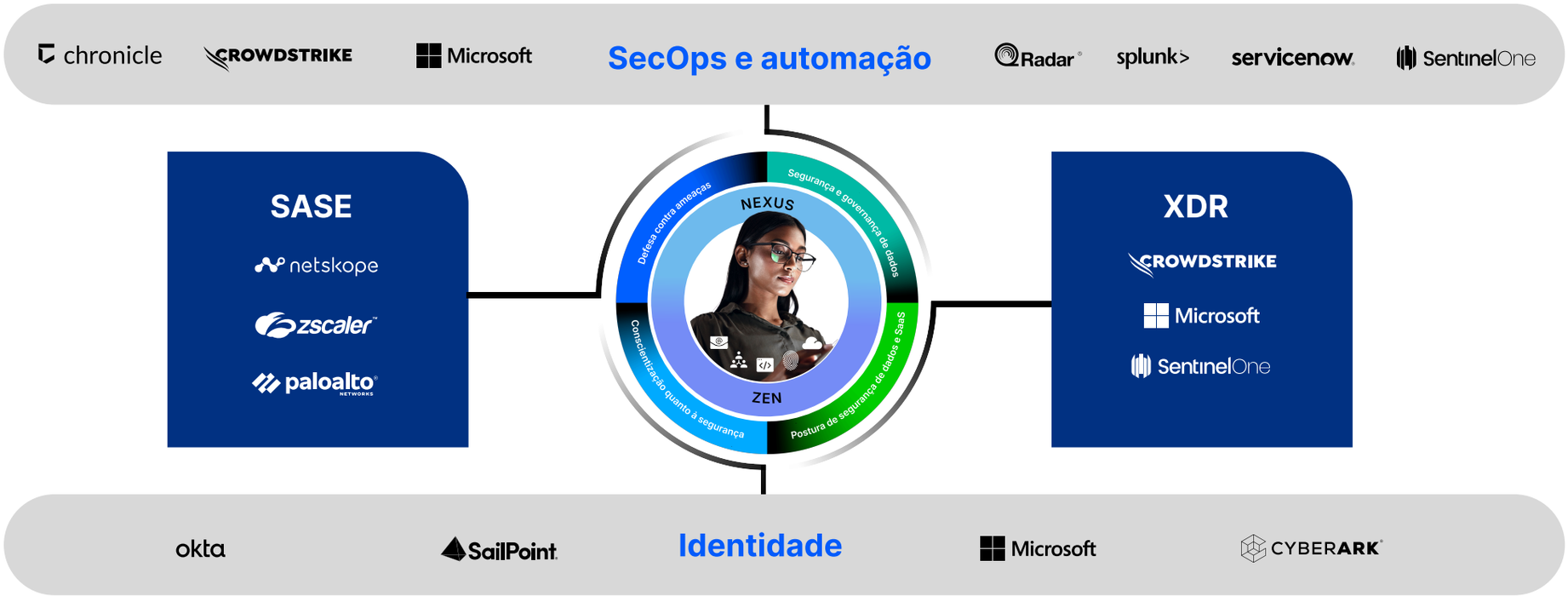
## XDR

Unifica telemetrias de e-mail, endpoints, nuvem e redes, simplificando a detecção, investigação e resposta a ameaças. Resolve silos de visibilidade e respostas lentas. A telemetria centrada em pessoas da Proofpoint — por exemplo, quem está sendo visado e quem apresenta risco — pode melhorar a XDR com um contexto antecipado e decisivo.

**Identidade** Protege acessos e identidades de usuários em ambientes de nuvem e locais detectando sequestros de contas, mau uso de credenciais e configurações indevidas de software como serviço (SaaS). Resolve multiplicidade de identidades e acesso não autorizado monitorando continuamente permissões, comportamentos de login e configurações arriscadas em aplicativos. Com a visibilidade proporcionada pela Proofpoint de quem tem acesso ao quê — e por quê — as equipes de segurança podem evitar movimentação lateral e impor privilégios mínimos.

proofpoint.

# A segurança centrada em pessoas como um multiplicador de forças




**A plataforma de segurança centrada em pessoas da Proofpoint** atua como um plano de controle estratégico na sua arquitetura de cibersegurança. Ela se integra com os seus investimentos atuais em segurança oferecendo sinais de risco centrados em pessoas que transformam sua eficácia.

Nossa plataforma reúne compreensão sobre classificação dos dados, intenção do usuário e contexto da ameaça. Ela utiliza inteligência artificial, autoaprendizagem e inteligência sobre ameaças em tempo real para obter insights e promover decisões automatizadas sobre política.

Veja a seguir algumas das muitas maneiras pelas quais a **plataforma Human-centric Security da Proofpoint** integra-se com os outros pilares da sua arquitetura, transformando a sua proteção como um todo:

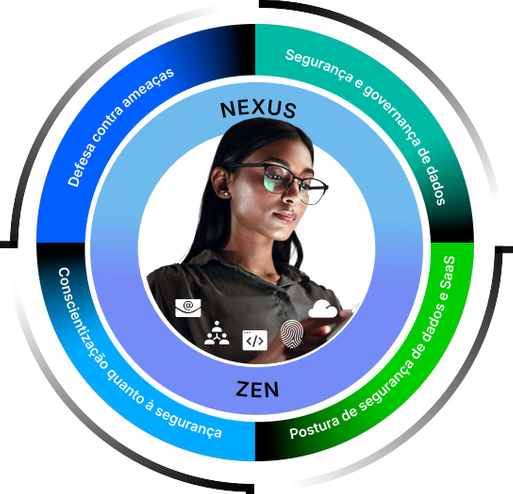
## Resposta acelerada e automatizada

A Proofpoint integra-se com plataformas de gerenciamento de eventos e informações de segurança (SIEM) e de coordenação, automação e resposta de segurança (SOAR) para reduzir o tempo médio necessário para detectar, investigar e responder — oferecendo alertas centrados em pessoas e automatizando ações de resposta. Sinais de risco da Proofpoint desencadeiam roteiros automatizados no Cortex XSOAR ou no Splunk SOAR que colocam usuários em quarentena ou redefinem credenciais. Alertas detalhados no Splunk ou no Microsoft Sentinel reduzem os falsos positivos e aceleram a triagem. Telemetria de comportamentos dos usuários e dados de ameaças da Proofpoint são compartilhados entre sistemas para viabilizar fluxos de trabalho unificados.

## SASE e controle de acessos adaptável

Com parceiros como Zscaler e Palo Alto Networks, a Proofpoint integra inteligência sobre ameaças e comportamental para influenciar políticas de acesso em tempo real. Os usuários visados passam por autenticação adicional ou têm seu acesso bloqueado via Zscaler ou Palo Alto Prisma Access. Atividades maliciosas desencadeiam uma imposição de política imediata.

Isso é SASE informado por pessoas, e não apenas por pacotes.




## A XDR que começa quando os ataques têm início

O phishing ainda é o principal ponto de entrada. Nós fechamos o cerco com CrowdStrike, Microsoft Sentinel e SentinelOne. Um e-mail marcado como suspeito desencadeia o isolamento do endpoint no CrowdStrike ou no SentinelOne em questão de segundos em vez de horas. A pontuação de risco do usuário e o contexto de ameaça direcionada da Proofpoint aumentam o detalhamento dos alertas no Microsoft Sentinel.

A Proofpoint oferece visibilidade sobre o primeiro contato para que a sua XDR não fique alheia ao início do ataque.

## Proteção de identidade e acesso privilegiado

Nós compartilhamos contexto de risco com Okta, CyberArk e SailPoint para moldar dinamicamente o controle de acessos. Nós identificamos os seus usuários mais arriscados e compartilhamos esses insights com nossos parceiros. Comportamento suspeito? Impomos autenticação por múltiplos fatores. Usuário de alto risco? Aplicamos políticas e controles adaptáveis. Conta comprometida? Revogamos o acesso. Juntos, nós transformamos a Zero Trust em realidade por meio de uma imposição adaptável com base na identidade.

proofpoint.

# Seus próximos passos: estratégicos em vez de táticos

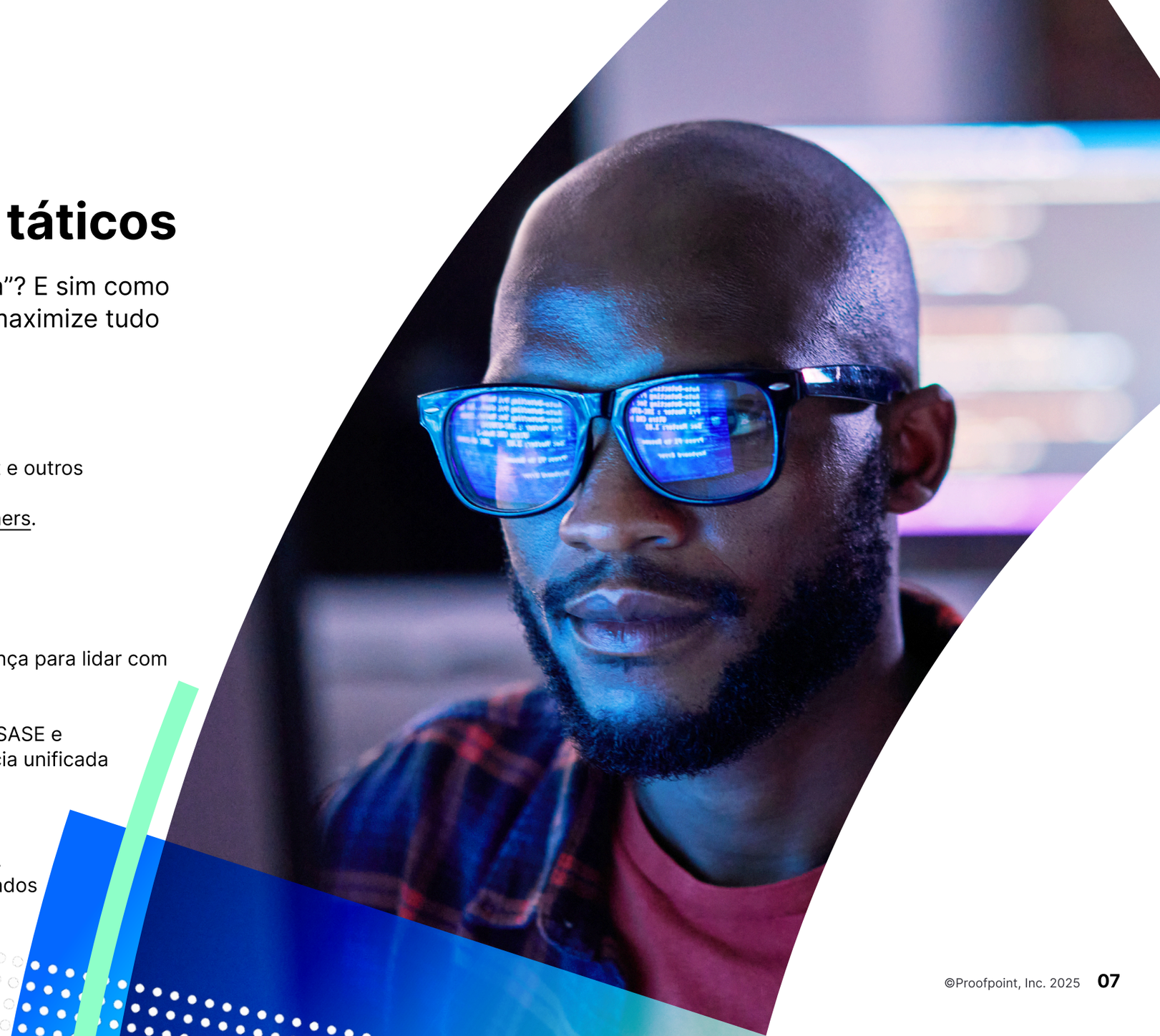
A questão não é “qual será a próxima ferramenta”? E sim como criar uma plataforma que se adapte, conecte e maximize tudo o que você já tem.

## Saiba mais sobre nossas integrações

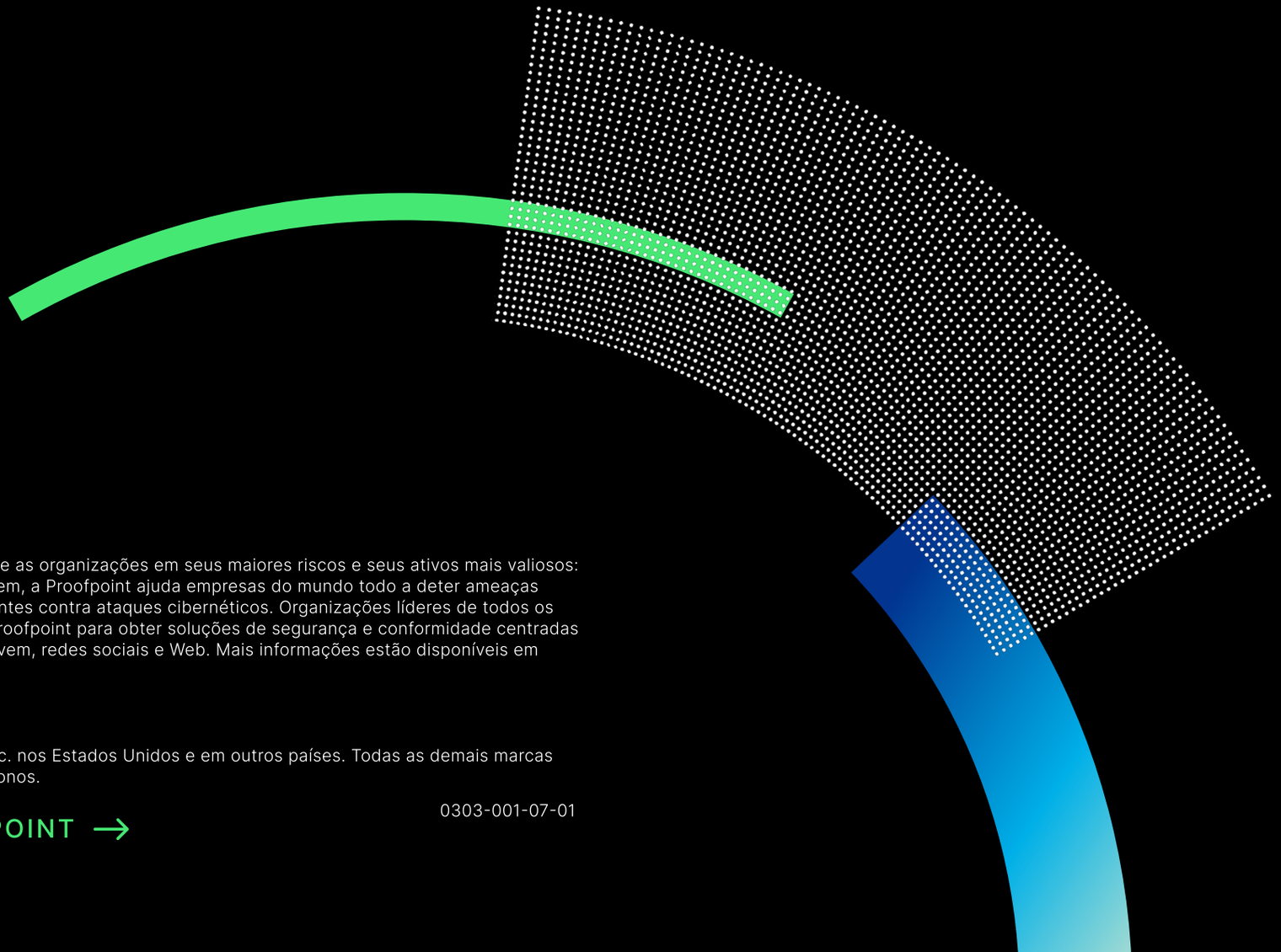
Descubra mais casos de uso de integração entre a Proofpoint e outros componentes da sua arquitetura de cibersegurança.
Visite proofpoint.com/use/partners/technology-alliance-partners.

## Fale hoje mesmo com a Proofpoint

- **Avalie** o nível de preparação da sua arquitetura de segurança para lidar com ameaças centradas em pessoas.
- **Saiba** como os seus investimentos existentes — em XDR, SASE e identidade — podem ser amplificados por nossa inteligência unificada sobre risco humano.
- **Veja** como realmente é uma segurança orientada por plataforma e como dar os primeiros passos para realizá-la. Nós mostraremos a você como transformar insights centrados em pessoas em resultados de segurança transformativos.



proofpoint.



proofpoint®

A Proofpoint, Inc. é uma empresa líder em cibersegurança 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



0303-001-07-01

DESCUBRA A PLATAFORMA DA PROOFPOINT →