



Forcepoint Insider Threat Data Protection

**OBTENHA VISIBILIDADE INCOMPARÁVEL DO COMPORTAMENTO
DOS USUÁRIOS E SEUS DADOS**



Forcepoint Insider Threat Data Protection

VISIBILIDADE INCOMPARÁVEL DO COMPORTAMENTO DOS USUÁRIOS E DA MOVIMENTAÇÃO DE DADOS PARA PROTEÇÃO LÍDER DO SETOR

ABORDAGEM "DE DENTRO PARA FORA" DA FORCEPOINT

A inovadora abordagem "de dentro para fora" da Forcepoint em cibersegurança irá revolucionar a forma como você protege os seus dados críticos. Insider Threat Data Protection fornece visibilidade profunda para ameaças internas, vinculando a movimentação de dados ao comportamento de seus usuários, não importa onde estejam.

UM SISTEMA DE ALERTA ANTECIPADO PARA AMEAÇAS INTERNAS

A visibilidade precoce do comportamento dos usuários fornece alerta para ameaças aos seus dados com origem interna. Impeça que os dados críticos saiam da organização e identifique usuários maliciosos e negligentes para minimizar os riscos de ameaças.



Por que você deve se preocupar

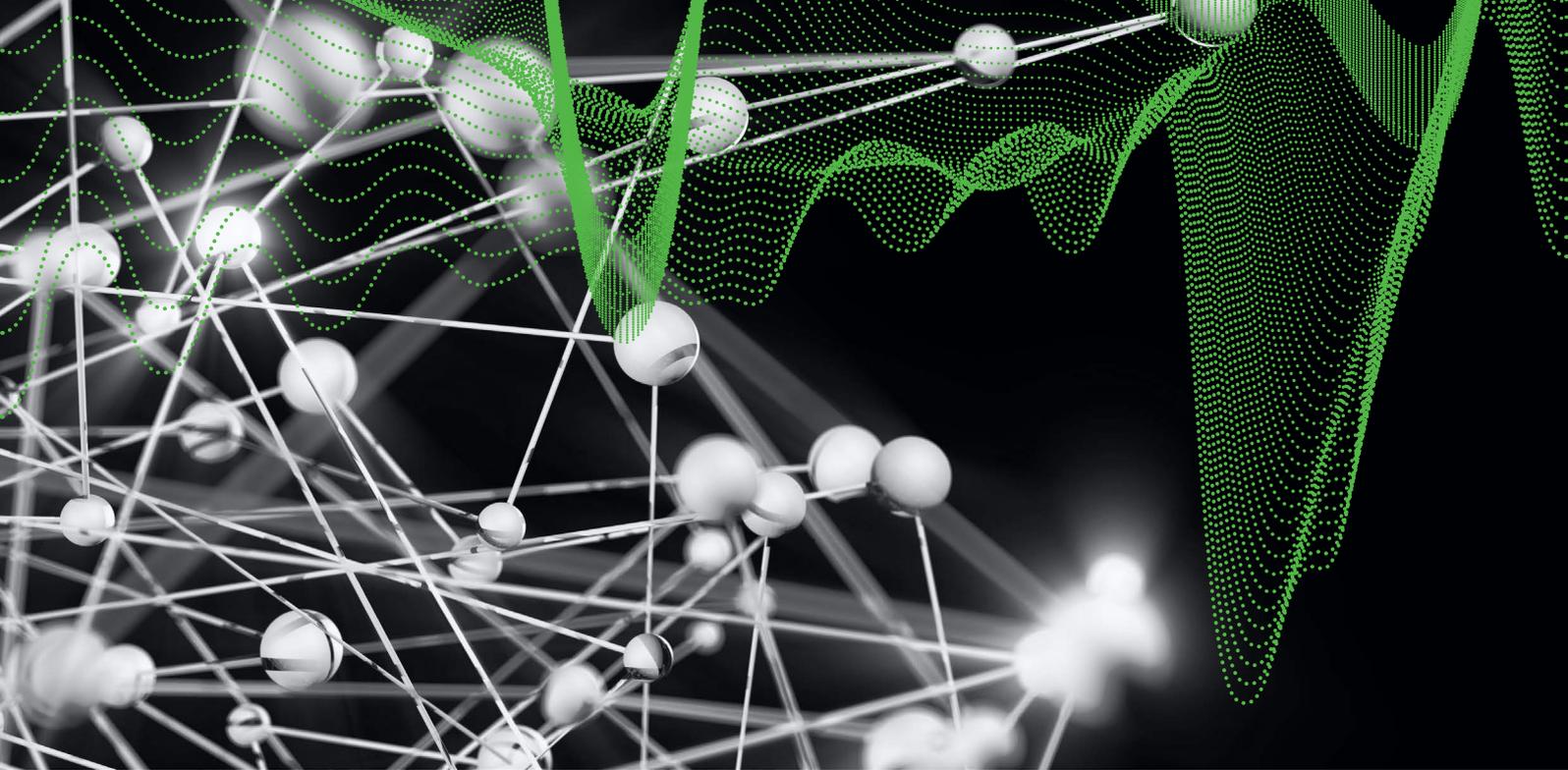


Em 2015, os três principais tipos de dados violados foram informações de identificação pessoal (PII), credenciais de autenticação e propriedade intelectual (PI). E 37% dessas violações, os resultados indicaram comportamento de pessoas internas - deliberado ou não intencional.¹

Portanto, como você pode habilitar melhor as suas equipes para acessar os dados de que precisam e mantê-los seguros?

A Forcepoint oferece o único sistema de alerta antecipado para defesa contra comportamentos de risco originados por ameaças internas.

¹ Forrester: Visão Geral do Mercado - Prevenção contra Perda de Dados, maio de 2016



Desafios para solucionar o problema

AMEAÇAS COM ORIGEM INTERNA



88%

DAS ORGANIZAÇÕES RECONHECEM QUE AS AMEAÇAS INTERNAS SÃO **MOTIVO DE ALARME**



69%

DAS ORGANIZAÇÕES NÃO TÊM **INFORMAÇÕES CONTEXTUAIS** SUFICIENTES



56%

DAS FERRAMENTAS GERAM **EXCESSO DE FALSOS POSITIVOS**



MUITAS DEPENDEM DE DLP E SIEM – FERRAMENTAS TRADICIONAIS, COM FOCO EM AMEAÇAS EXTERNAS

VISIBILIDADE



42%

não confiam que têm visibilidade em toda a empresa para acesso de usuários privilegiados



16%

têm muita confiança de que têm essa visibilidade

ORÇAMENTO



88%

reconhecem o orçamento como uma **prioridade principal**

Menos de 40%

têm um orçamento dedicado para proteção contra ameaças internas

72%

declararam que usam ferramentas de autenticação e gestão de identidades para administrar o abuso de usuários privilegiados – a maioria usa ferramentas de cibersegurança existentes que não foram elaboradas para combater ameaças internas





Obtenha visibilidade incomparável do comportamento dos usuários e dos dados

Nossa solução – Forcepoint Insider Threat Data Protection

Insider Threat Data Protection da Forcepoint é a primeira solução da indústria que fornece um alerta antecipado para uma ameaça interna e impede a exfiltração de propriedade intelectual e dados regulamentados. Fornece visibilidade de seus usuários e dados, e proteção completa de suas informações, vinculando a movimentação de dados ao comportamento do usuário. A Forcepoint protege a sua organização contra sistemas sequestrados, credenciais roubadas, funcionários maliciosos e perda de dados acidental. Insider Threat Data Protection é altamente escalável e as organizações mais sensíveis do planeta confiam em sua proteção. Fornece a visibilidade necessária de seus dados - no escritório, no percurso ou na Nuvem, com o contexto sobre como seus funcionários estão usando seus dados confidenciais.



Insider Data Protection da Forcepoint é a combinação de nossa solução de DLP Corporativo líder do setor, que fornece visibilidade e controle sobre a movimentação de dados, com a nossa incomparável solução Forcepoint Insider Threat, que aplica análise comportamental e forense para identificar comportamentos arriscados de usuários. Esta combinação potente bloqueia mais ameaças internas do que qualquer outra solução no mercado.

A solução mais estável e escalável da indústria, que cresce com a sua organização



Movimentação de Dados



Comportamento do Usuário



Proteção de Dados Completa

Vantagens do DLP da Forcepoint (Forcepoint DLP e Forcepoint DLP Endpoint)

O RECURSO MAIS AVANÇADO DE IMPRESSÃO DIGITAL DA INDÚSTRIA

- ▶ **PreciseID Fingerprinting** detecta até fragmentos de dados não estruturados e estruturados, no escritório, no percurso ou na Nuvem.
- ▶ **agentes de endpoint da categoria fornecem visibilidade e controle sem paralelos sobre dados confidenciais em notebooks com Windows e Mac OS** - dentro e fora da rede corporativa.

TECNOLOGIAS AVANÇADAS PARA PROTEGER DADOS CONFIDENCIAIS

- ▶ **O Reconhecimento Óptico de Caracteres (OCR) identifica textos ocultos em imagens.** Proteja dados ocultos em documentos digitalizados legados, .jpegs, projetos em CAD, MRIs e capturas de tela.
- ▶ **O Aprendizado de Máquina da Forcepoint** reduz a barreira de entrada para aprendizado de máquina ao não exigir um falso positivo durante a configuração.
- ▶ **O Drip DLP** combate o ataque lento e discreto, quando os dados são extraídos em pequenos volumes para evitar serem detectados.
- ▶ **Configuração de políticas e implementação em uma única vez** para estender os controles de DLP corporativo a canais comuns de exfiltração, como web e e-mail.

Vantagens do Forcepoint Insider Threat

VINCULE A MOVIMENTAÇÃO DE DADOS AO COMPORTAMENTO DO USUÁRIO

- ▶ **Deteção precoce bem antes de se tornar um Incidente de DLP;** por exemplo, um funcionário fazendo stockpiling de dados ou criando backdoors.
- ▶ **Implemente com rapidez decisões de reparação mais inteligentes** depois que um comportamento de risco de usuário for detectado

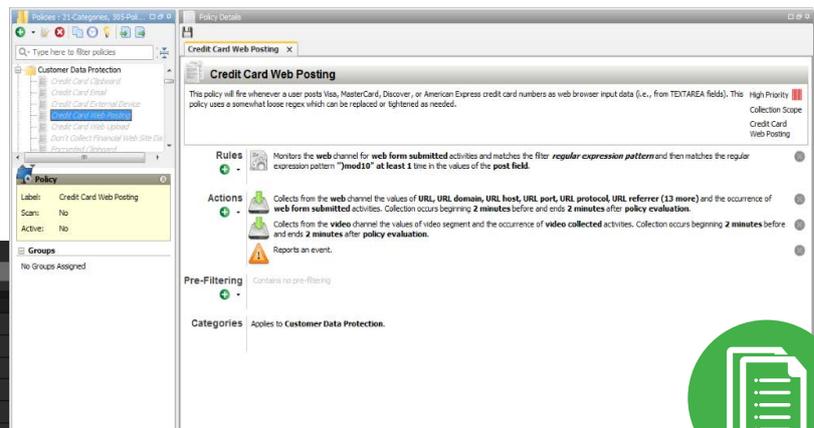
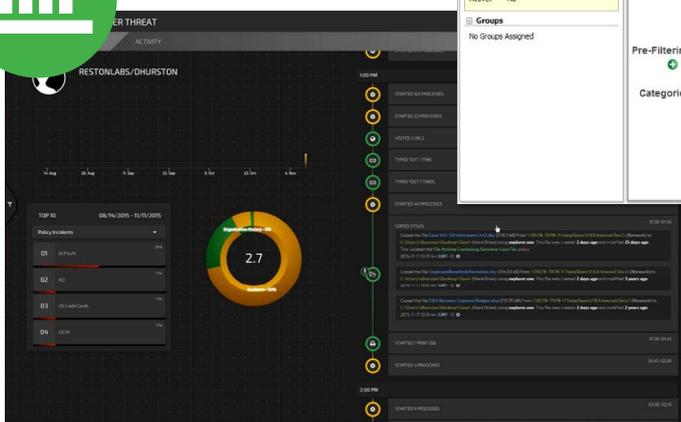
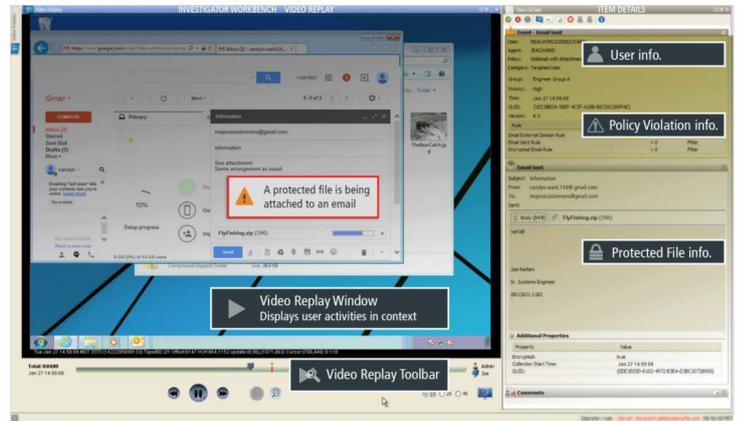
MECANISMO ANALÍTICO DE PONTUAÇÃO DE RISCOS DO COMPORTAMENTO DOS USUÁRIOS

- ▶ A Forcepoint fornece os sinais de alertas antecipados de um sistema sequestrado, credenciais roubadas, funcionário malicioso ou apenas cometendo erros – antes que dados confidenciais sejam vazados ou roubados.
- ▶ Economiza tempo e esforço, pontuando e priorizando automaticamente os usuários de maior risco, o que reduz a necessidade de analisar milhares de alertas.
- ▶ Cria linhas de base do comportamento individual e das normas organizacionais entre canais para identificar comportamentos de risco.
- ▶ Fornece uma pontuação de riscos de usuários consolidada para cada usuário em cada dia, e destaca rapidamente as tendências de riscos para 30 dias.

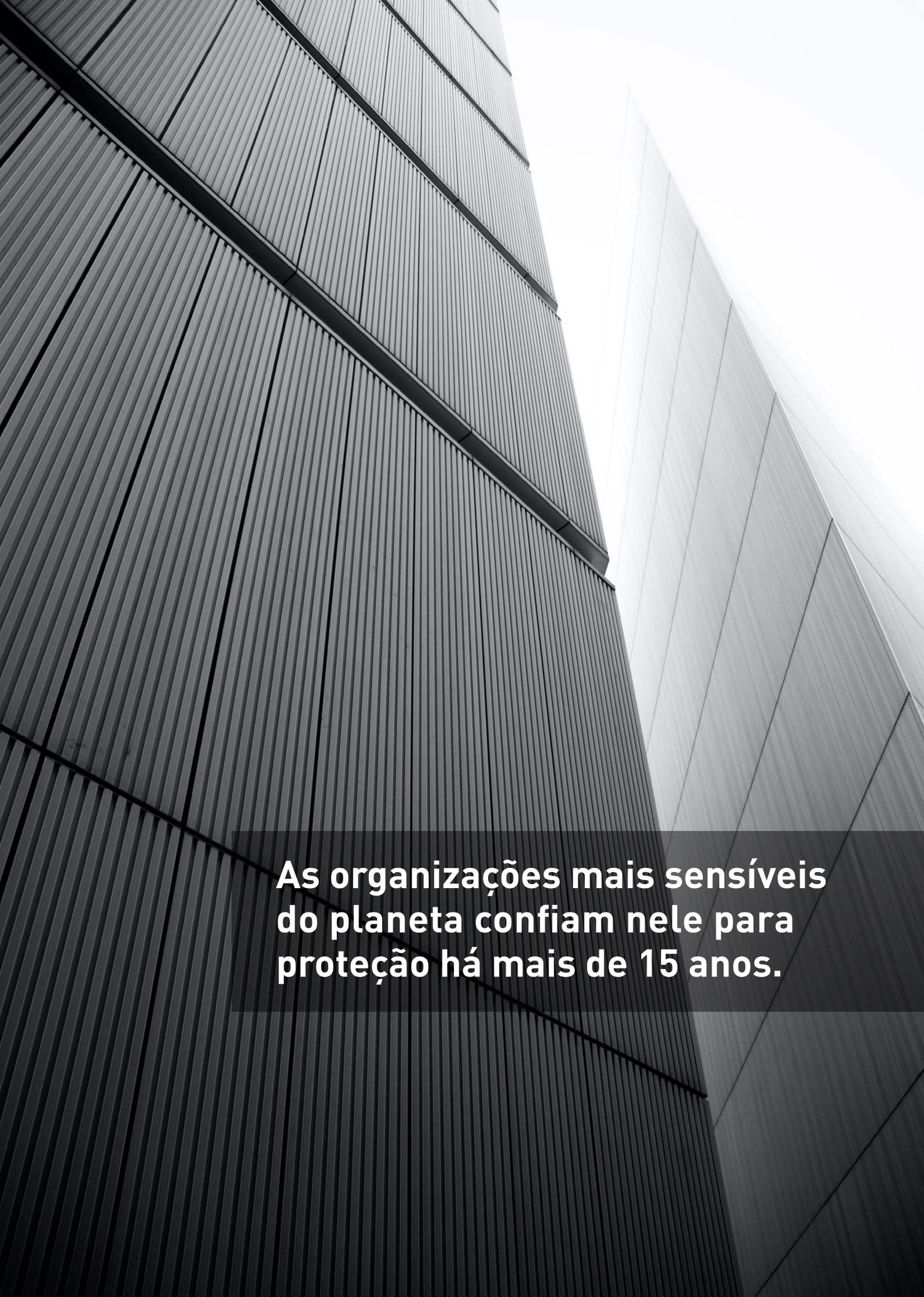


CAPTURA DE VÍDEO E REPRODUÇÃO COM ANÁLISE FORENSE

- ▶ As capturas de tela e sua reprodução fornecem uma visão “por sobre o ombro”, com visibilidade sem paralelos sobre comportamentos suspeitos antes que se tornem problemas.
- ▶ Obtenha evidências para a atribuição e determine se a causa foi um sistema sequestrado, credenciais roubadas, funcionário malicioso ou erros inocentes.
- ▶ Se necessário, os dados forenses do Forcepoint Insider Threat são admissíveis em um tribunal.
- ▶ A Central de Comandos do Forcepoint Insider Threat prioriza automaticamente os seus usuários de maior risco, reduzindo a necessidade de analisar milhares de alertas.
- ▶ Um aprofundamento fácil do comportamento de risco de usuários e uma linha de tempo expansível mostram as atividades que tornam o funcionário um usuário de risco.



A Forcepoint tem mais de 15 anos de experiência em proteção de dados para empresas comerciais ao redor do mundo, e também as organizações governamentais, militares e de inteligência mais altamente seguras.



**As organizações mais sensíveis
do planeta confiam nele para
proteção há mais de 15 anos.**

CONTATO

www.forcepoint.com/contact

© 2017 Forcepoint. Forcepoint e o logotipo FORCEPOINT são marcas comerciais da Forcepoint. Raytheon é uma marca registrada da Raytheon Company. Todas as outras marcas comerciais utilizadas neste documento são de propriedade de seus respectivos proprietários.

[BROCHURE_INSIDER_THREAT_DATA_PROTECTION_PT] 400012.030117

