



Forcepoint Insider Threat

**VISIBILIDADE INCOMPARÁVEL DO COMPORTAMENTO DOS USUÁRIOS PARA
PROTEGER A PROPRIEDADE INTELECTUAL E DETECTAR AMEAÇAS INTERNAS**



Forcepoint Insider Threat

A VISIBILIDADE INCOMPARÁVEL DA ATIVIDADE PRECOCE NOS COMPUTADORES DOS USUÁRIOS PREVINE O ROUBO E A PERDA DE DADOS POR SISTEMAS SEQUESTRADOS, INSIDERS MALICIOSOS OU USUÁRIOS FINAIS NEGLIGENTES.

INTRODUÇÃO

O Forcepoint Insider Threat tem identificado e bloqueado ameaças internas para governos e empresas listadas na Fortune 100 há mais de 15 anos. Com mais de 1 milhão de endpoints implementados, a solução comprovada Forcepoint Insider Threat protege algumas das organizações mais sensíveis do planeta. Um cliente de varejo da Fortune 100 obteve 60% de retorno do investimento no primeiro ano da implementação.

15

BLOQUEANDO AMEAÇAS INTERNAS HÁ MAIS DE 15 ANOS

1.000.000

MAIS DE 1 MILHÃO DE ENDPOINTS PROTEGIDOS



**Retorno do
investimento: 60%**



**Reprodução:
<16 meses**

O Forcepoint Insider Threat fornece visibilidade incomparável da atividade precoce nos computadores dos usuários, ajudando a impedir o roubo e a perda de dados, ao:

DETECTAR

Detectar atividade suspeita, seja a acidental ou intencional.

IMPEDIR

Impedir um sistema sequestrado, um insider malicioso ou mesmo um erro de usuário, garantindo que sua propriedade intelectual não seja comprometida.

ESTABELECEER

Estabelecer a linha de base do comportamento normal, indicando os primeiros indícios de riscos potenciais quando um usuário se desvia da atividade padrão.

FORNECER CONTEXTO

Fornecer contexto sobre o comportamento de um usuário, ajudando em sua investigação.

IDENTIFICAR

Identificar automaticamente os usuários de maior risco. Uma visão por sobre o ombro permite que você acrescente contexto ao comportamento de risco. Isso permite avaliar se o sistema foi sequestrado, se a ação do funcionário foi maliciosa ou se foi um ato acidental.

Forcepoint Insider Threat capacita a sua organização

Forcepoint Insider Threat economiza tempo e esforço, pontuando e priorizando automaticamente os usuários de maior risco, o que reduz a necessidade de analisar milhares de alertas. Isso libera a sua equipe para se concentrar em tarefas de alta prioridade e melhora a eficiência. Forcepoint Insider Threat também fornece o contexto e as evidências forenses necessárias para atribuição inegável e cadeia de custódia – simplificando investigações, acusações e conformidade.

BENEFÍCIOS DO FORCEPOINT INSIDER THREAT:

Não há outro fornecedor que associa todas estas vantagens para defender seus dados contra as ameaças internas em um único produto.

- ▶ Somente o Forcepoint Insider Threat oferece captura de vídeo digital e reprodução em endpoints com Windows e Mac OS.
- ▶ Nossa Central de Comandos fornece uma forma altamente intuitiva de identificar os usuários de maior risco e ver rapidamente padrões que podem revelar riscos mais abrangentes
- ▶ Forcepoint Insider Threat fornece controle granular sobre quando coletar dados e o que coletar especificamente para proteger a privacidade dos usuários.
- ▶ Somente o Forcepoint Insider Threat integra-se ao Forcepoint DLP para ajudar você a tomar decisões de reparação mais inteligentes e com mais agilidade depois que o comportamento de risco é detectado.

PRINCIPAIS RECURSOS:

Forcepoint é o único fornecedor a disponibilizar estes recursos de defesa contra ameaças internas essenciais em um único produto.

- ▶ Coleta e agregação de metadados para criar uma linha de base para comportamentos de usuários e grupos, habilitando você a detectar automaticamente quando um usuário adota um comportamento fora do padrão.
- ▶ Integração com Forcepoint DLP, fornecendo os recursos forenses de que você precisa para tomar decisões de reparação mais inteligentes e com mais agilidade depois que o comportamento de risco é detectado.
- ▶ Agregação de alertas para identificar rapidamente os usuários de maior risco.
- ▶ A coleta e a reprodução de vídeos ajudam a acelerar a investigação, permitindo a atribuição e mostrando a intenção dos funcionários, sendo admissíveis nos Tribunais de Justiça.



Visibilidade incomparável do comportamento dos usuários

Recursos do Forcepoint Insider Threat

Desenvolvido como uma solução para ameaças internas, o Forcepoint Insider Threat não é uma solução existente adaptada para o problema – é uma ferramenta de segurança única e incomparável, projetada especificamente para proteger os seus dados contra ameaças maliciosas ou acidentais. O desenvolvimento do Forcepoint Insider Threat foi liderado por uma equipe de especialistas em segurança de domínio, que dedicaram suas carreiras à proteção das informações.

Forcepoint Insider Threat fornece estes recursos de proteção de dados incomparáveis:

- ▶ **Protege** contra ameaças internas não intencionais e comportamento interno malicioso.
- ▶ **Reprodução de vídeo** fornece contexto comportamental completo para diferenciar rapidamente ações maliciosas e involuntárias, facilmente analisado e compreendido por pessoal não técnico – e tudo isso respeitando as diretrizes de privacidade dos funcionários com políticas personalizáveis e orientadas aos negócios.

- ▶ **Análises** priorizam os usuários com comportamento anômalo e fornecem visibilidade profunda de suas ações, incluindo comportamentos anteriores.
- ▶ **Integrado ao sistema de em toda a empresa**, – não é necessário comprar ou manter um número de aplicações de softwares independentes.
- ▶ A arquitetura **distribuída** evita impacto na performance.
- ▶ Agente estável, leve e **comprovado**.
- ▶ **Coleta de dados** de múltiplas fontes, incluindo Forcepoint DLP.
- ▶ **Detecta** o comportamento de risco mesmo quando os usuários estão fora da rede corporativa.



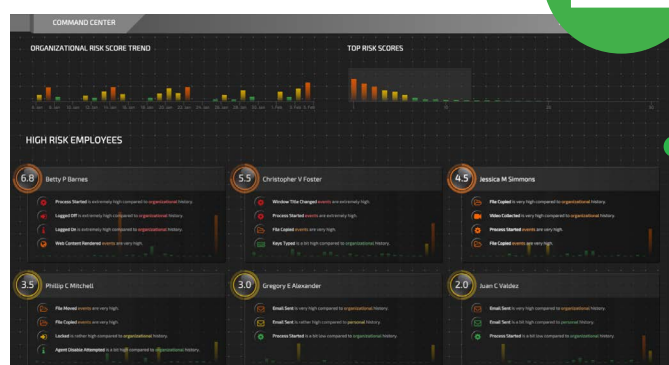
Componentes do Forcepoint Insider Threat

MECANISMO ANALÍTICO DE PONTUAÇÃO DE RISCOS DO COMPORTAMENTO DOS USUÁRIOS

- Forcepoint fornece a visibilidade necessária para ter sinais de alertas precoces de usuários com dados sequestrados, de ações maliciosas ou apenas cometendo erros – antes que dados confidenciais sejam vazados ou roubados.
- Forcepoint Insider Threat economiza tempo e esforço, pontuando e priorizando automaticamente os usuários de maior risco, o que reduz a necessidade de analisar milhares de alertas.
- A Central de Comandos do Forcepoint Insider Threat fornece uma forma altamente intuitiva de identificar os usuários de maior risco e ver rapidamente padrões que podem revelar riscos mais abrangentes.
- O recurso de captura e reprodução de vídeo do Forcepoint Insider Threat fornece visibilidade sem paralelos sobre comportamentos suspeitos antes que se tornem problemas (por exemplo, criação de back doors, armazenamento de dados).

COMO O FORCEPOINT INSIDER THREAT PROTEGE CONTRA AMEAÇAS INTERNAS

- Cria linhas de base do comportamento individual e organizacional entre canais para entender qual comportamento é normal e esperado.
- Procura anomalias no comportamento individual para detectar ameaças internas potenciais (intencionais e não intencionais).
- Fornece uma pontuação de riscos consolidada para cada usuário em cada dia, e destaca rapidamente as tendências de riscos para 30 dias.
- Simplifica o processo de investigação priorizando os usuários de riscos.

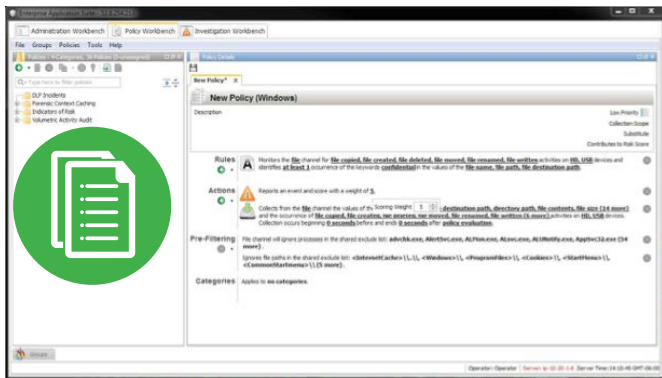


Simplifica o processo de investigação priorizando os usuários de riscos



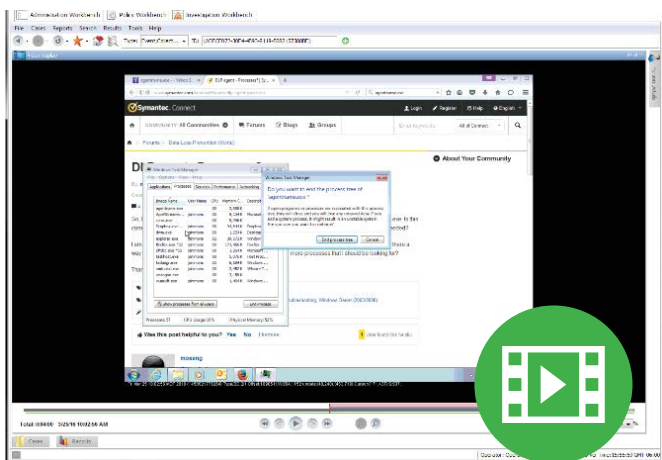
IDENTIFICAÇÃO ORIENTADA POR POLÍTICAS DOS COMPORTAMENTOS DE RISCO

- Os clientes podem definir comportamentos específicos que sabidamente são arriscados, com base em um conjunto ou sequência de atividades.
- Essas políticas permitem a detecção de uma ampla variedade de monitoramento de atividades, desde requisitos de conformidade de PII e HIPAA até proteção de propriedade intelectual e detecção limitada de malware.
- As políticas específicas de clientes influem na pontuação geral de riscos.
- Os clientes podem ajustar manualmente a ponderação dessas políticas para ajustar o nível de contribuição à pontuação geral de riscos.



VISUALIZAÇÃO MOSTRANDO CONTRIBUIDORES DA PONTUAÇÃO DE RISCOS

- Para cada usuário em cada dia, um gráfico intuitivo é gerado, permitindo que um investigador entenda rapidamente quais tipos de atividades resultaram em pontuação de risco elevada.



REPRODUÇÃO DE VÍDEO DA ESTAÇÃO DE TRABALHO

- 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.
- Políticas fornecem o contexto e a evidência necessários para atribuir um incidente a um usuário e determinar se teve seus dados sequestrados, aplicou ações maliciosas ou apenas errou.
- Os investigadores podem exibir facilmente o vídeo da estação de trabalho de usuários de alto risco e ver qualquer atividade suspeita, com facilidade de atribuição que é admissível em tribunais.

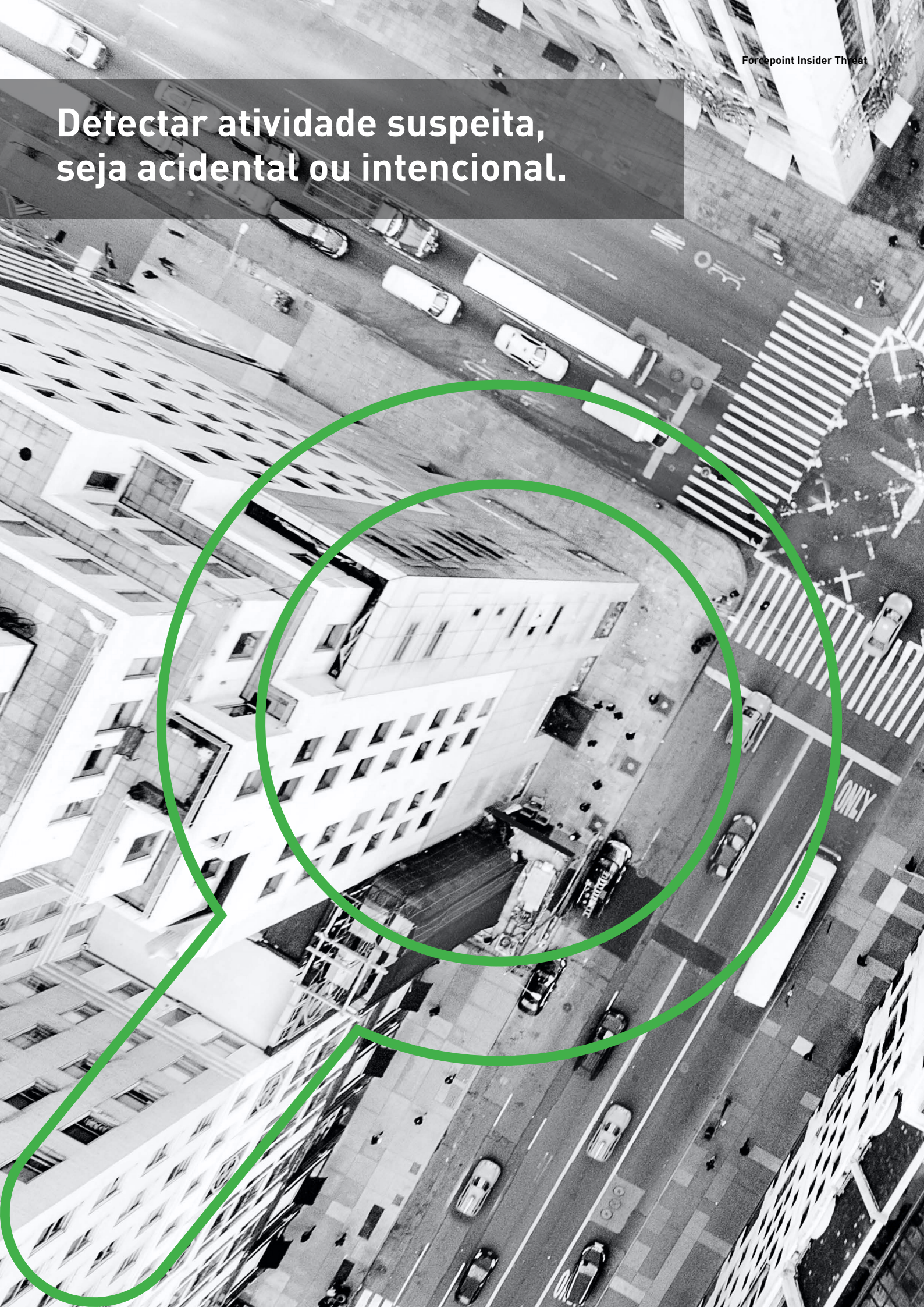
REVISÃO DA ATIVIDADE EM LINHA DE TEMPO E DETALHES FORENSES ADICIONAIS

- A Central de Comandos do Forcepoint Insider Threat economiza tempo e esforço, pontuando e priorizando automaticamente os usuários de maior risco, o que reduz a necessidade de analisar milhares de alertas.
- Um aprofundamento fácil dos usuários de risco e uma linha de tempo expansível, mostrando os atos efetivos do usuário que o tornam um usuário de risco.
- Gravação e reprodução fornecem visibilidade sobre a intenção do usuário e simplificam o processo de investigação.
- Fornece o contexto e o conteúdo das ações dos usuários, auxiliando a atribuição e apoiando a acusação de comportamento malicioso.



Para agendar uma demonstração ou obter mais informações, visite www.forcepoint.com/contact.

**Detectar atividade suspeita,
seja acidental ou intencional.**



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_FORCEPOINT_INSIDER_THREAT_PT] 400011.030117