Forcepoint

Um dia na vida dos dados sensíveis

Uma funcionária. Uma manhã comum. Uma explosão exponencial do risco de dados. Veja como isso acontece e como impedi-lo.

O Risco Já Está Aqui

53%

DOS INCIDENTES INTERNOS SÃO ACIDENTAIS OU POR NEGLIGÊNCIA

DTEX 2026 Cost of Insider Risks

13%

DOS INCIDENTES SÃO CONTIDOS EM MENOS DE 30 DIAS

DTEX 2026 Cost of Insider Risks

Mais de 200 Dias

TEMPO MÉDIO PARA RESOLVER INCIDENTES INTERNOS (MALICIOSOS E ACIDENTAIS)

IBM 2026
Cost of a Data Breach Report

$19,5 Milhões

CUSTO MÉDIO ANUAL TOTAL DOS INCIDENTES INTERNOS

DTEX 2026
Cost of Insider Risks

Conheça Alice

Alice é uma representante de vendas se preparando para uma reunião de alto impacto com um parceiro. Ela está fazendo seu trabalho. Ela não está tentando causar um incidente de segurança. **Veja o que acontece com os dados sensíveis enquanto ela se prepara.**

Salesforce → Excel

Alice gera um relatório das suas principais contas estratégicas no Salesforce e o baixa como arquivo Excel. Os dados incluem nomes de contas, contatos e valores de receita.

PII regulamentada, PI e dados de contas estratégicas saem de um ambiente CRM

Excel → Nuvem

Ela carrega o arquivo em uma plataforma de colaboração para compartilhar com sua equipe. SharePoint. Box. OneDrive. Não importa qual.

Os dados críticos agora existem em múltiplos locais, acessíveis a qualquer pessoa com permissão.

Excel → IA pública

Alice usa uma ferramenta de IA pública para resumir tendências e criar pontos de discussão. Ela carrega o arquivo Excel diretamente no prompt.

Dados críticos foram carregados em uma Shadow AI com um prompt arriscado.

Saída da IA → Slack

Ela compartilha o resumo gerado pela IA com sua equipe no Slack.

Novo conteúdo que inclui elementos de dados críticos se espalha para um canal de colaboração.

Slack → E-mail externo

Alice envia o resumo por e-mail a um parceiro fora da organização.

Os dados críticos são exportados pelo canal mais arriscado, sem controles de acesso ou auditoria.

O que acabou de acontecer?

PII. Propriedade intelectual. Informações estratégicas. Em um único dia, tudo isso explodiu por plataformas de colaboração, armazenamento em nuvem, ferramentas de IA e limites de confiança externos. Alice não pretendia causar um problema. Ela simplesmente tentava trabalhar de forma mais inteligente e rápida. É isso que torna o risco interno tão difícil de gerenciar: a maior parte não é maliciosa. É humana.

Uma nova abordagem: segurança que segue os dados

Proteger dados sensíveis requer uma abordagem contínua que se adapta em tempo real. Não uma lista de verificação. Não um conjunto de políticas estáticas. Um ciclo. **Forcepoint chama essa abordagem de Data Security Everywhere.**

Descobrir
Estabelecer visibilidade sobre os dados sensíveis onde quer que estejam

Classificar
Identificar o tipo, o uso de negócios e o nível de sensibilidade dos dados

Priorizar
Concentrar a atenção onde o risco é maior

Proteger dados sensíveis não é uma lista de verificação. **É um ciclo contínuo.cycle.**

Proteger
Aplicar políticas de forma consistente em todos os canais para reduzir o risco

Remediar
Tratar vulnerabilidades antes que se tornem violações

Forcepoint Data Security Cloud

As cinco etapas se conectam em uma plataforma unificada: Forcepoint Data Security Cloud. Uma plataforma. Um conjunto de políticas. Visibilidade completa em cada ambiente onde os dados existem, se movem e são utilizados.

Saiba mais

©2026 Forcepoint. Forcepoint e o logotipo FORCEPOINT são marcas comerciais da Forcepoint. Todas as outras marcas comerciais utilizadas neste documento são de propriedade de seus respectivos donos. [FP-A Day in The Life-PT] 24Apr2026