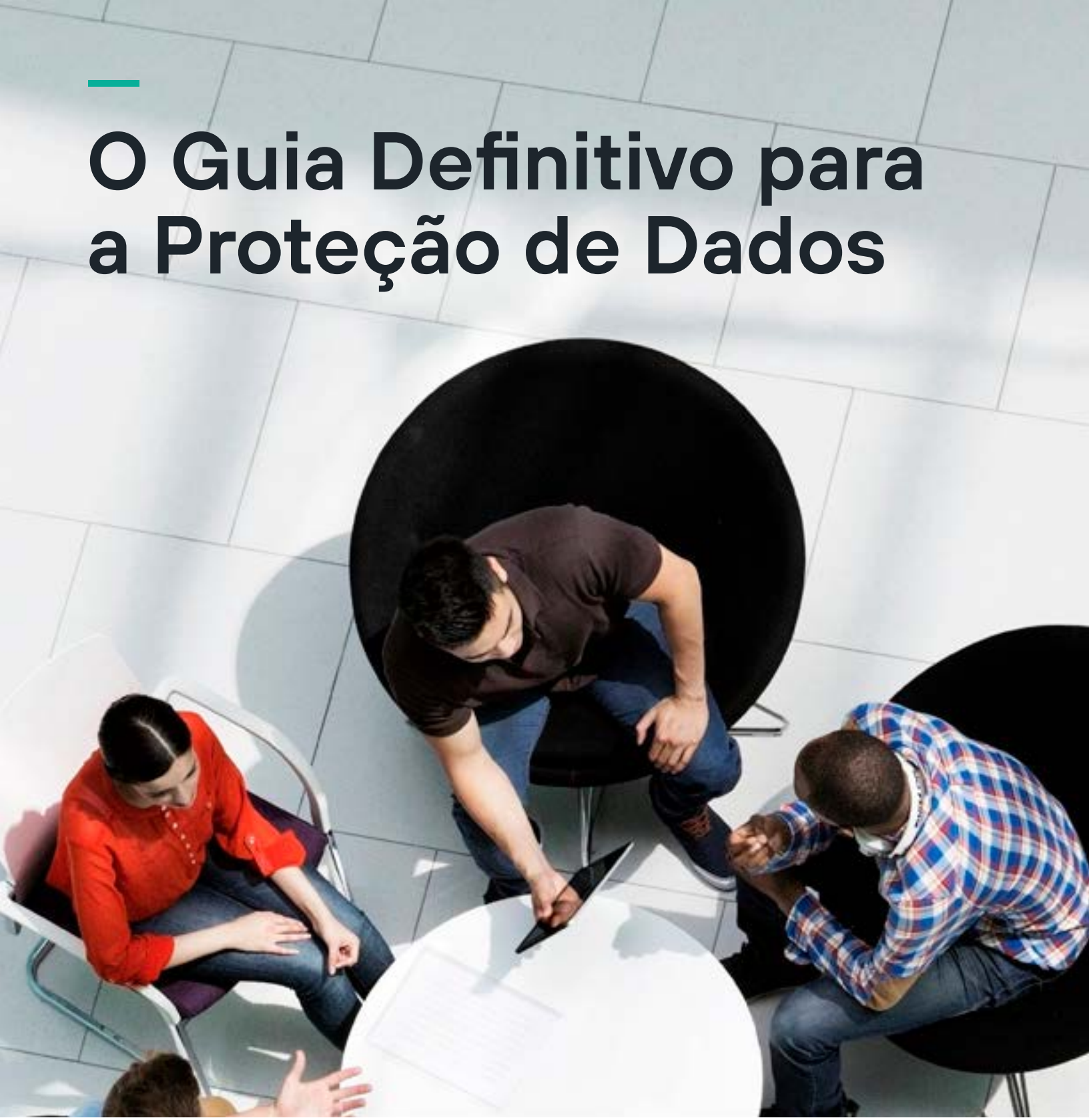
O Guia Definitivo para a Proteção de Dados



Forcepoint

Folheto

Visão Geral do Cenário

De certa forma, a relação entre segurança de dados e desempenho empresarial é uma narrativa tão antiga como os negócios. Afinal, a forma mais simples de vantagem competitiva é a capacidade de uma empresa para esconder sua "receita secreta"—não importa se é um processo proprietário, propriedade intelectual crítica ou mesmo, literalmente, uma receita.

Mas atualmente a questão é infinitamente mais complexa. Estima-se que 90% dos dados do mundo foram criados em apenas dois anos.[1] E, para ampliar esse efeito, a proliferação de dispositivos móveis, relações distantes entre clientes e contratados, funcionários remotos e em roaming, e mais, significa que os dados são armazenados e acessados em mais lugares, por mais pessoas—em qualquer ocasião.

Na esteira dessa mudança na função dos dados no local de trabalho, violações de dados de alta visibilidade ajudaram a criar um novo caso de negócios para a segurança de dados. O impacto financeiro é um fator, é claro: o custo médio de uma violação de dados é US$ 3,26 milhões.[2] Contudo, em termos mais simples, os incidentes de segurança de dados podem causar danos críticos à marca de uma empresa e à confiança de seus clientes.

Setores altamente regulados, como saúde e serviços financeiros, há muito têm uma obrigação legal de proteger dados confidenciais. Mais recentemente, contudo, o aumento da vigilância e conscientização do público sobre segurança de dados ajudou a estimular novas leis que regem como as empresas podem coletar, processar e armazenar dados. Lei de Proteção de Dados Pessoais da Malásia, Regulamento Geral de Proteção de Dados da UE, Princípios de Privacidade da Austrália, Lei de Privacidade do Consumidor da Califórnia—a lista é longa. E é suficiente para fazer qualquer organização—não importa se está ou não sujeita às regulamentações atuais—pensar criticamente sobre proteção de dados.

US$ 3,26 Milhões

Custo médio de uma violação de dados[2]

2.600-10.000

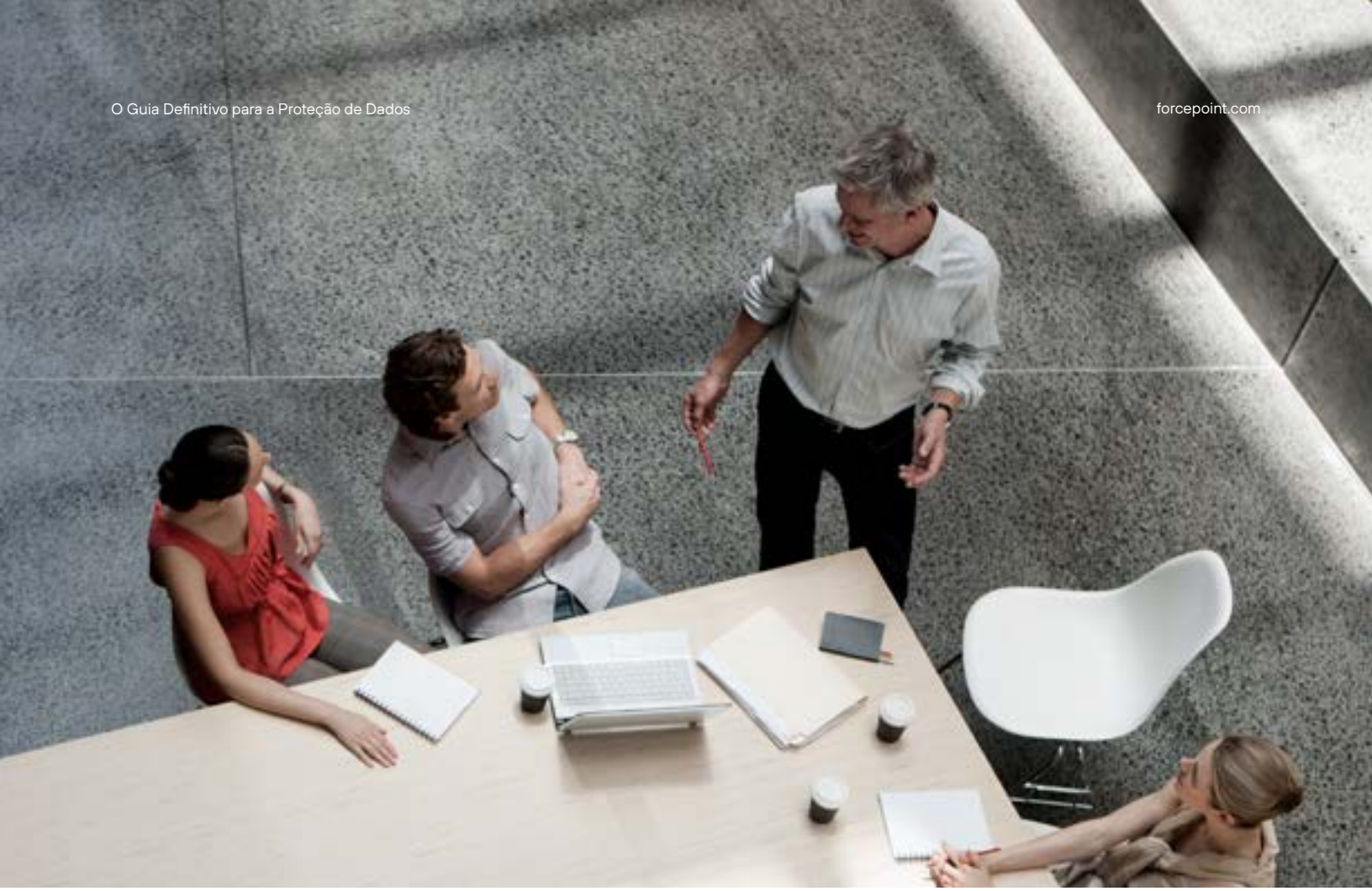
Número de registros confidenciais em uma violação média[2]

68%

Porcentagem de violações de dados que não são percebidas durante meses[2]

Nesse contexto, uma coisa ficou clara: Habilitar empresas e funcionários a ter bom desempenho no ambiente de negócios atual requer uma mudança em como pensamos sobre segurança de dados. No estado de mudança constante que se tornou a nova normalidade, políticas reativas não são mais suficientes para manter a nossa segurança. Vamos explorar como adotar uma abordagem proativa em proteção de dados—e por que é uma escolha segura para as empresas atualmente.

Estima-se que 90% dos dados do mundo foram criados em apenas dois anos.[1]



Elevando a Função de Segurança de Dados

Para muitas equipes de segurança de dados, os dias consistem em ciclos de receber um alerta, investigar e corrigir os danos. Enxágue e repita. O problema? Políticas inflexíveis com frequência marcam atividades de baixo risco, o que resulta em alertas "falsos positivos". Investigá-los gera uma carga de trabalho imensa para as equipes de segurança de dados que já têm mais tarefas e responsabilidades para cumprir do que conseguiriam.

Uma tecnologia de proteção de dados que consiga ler o contexto da atividade digital pode reduzir essa carga para as equipes de segurança de dados, ajudando-as a concentrar suas investigações em incidentes que sejam realmente ameaçadores e filtrar os que não representam um risco real para a empresa. E priorizar melhor o tempo permite que a equipe de segurança evolua sua função em uma organização, de simplesmente aplicar regras para liderar proativamente a empresa para um futuro mais seguro e eficiente.

Habilitando o Crescimento Profissional

Os especialistas em segurança de dados que não estão sobrecarregados com alertas falsos podem orientar outros funcionários, contribuindo para seu desenvolvimento profissional e trajetória de carreira.

Habilitando o Crescimento da Empresa

Os profissionais de segurança que encontram eficiências em suas próprias cargas de trabalho podem ajudar a identificar oportunidades para que a empresa cresça com uso mais inteligente dos dados. (Ou identificar riscos de comportamentos de dados que possam impedir o crescimento da empresa.)

Habilitando a Transformação Digital

Dinamizar as investigações com base no entendimento contextual dos incidentes de dados permite que as equipes tenham tempo para otimizar suas políticas e procedimentos para adequação a uma cultura de dados habilitada pela nuvem—o que permite uma transformação digital mais rápida e vantagem competitiva para a empresa.

Protegendo os Dados Onde o Trabalho Ocorre

A prevenção contra perda de dados tradicional protege os dados em três pontos de acesso: em sua rede, nos endpoints e, cada vez mais, na nuvem. E isso poderia ser suficiente—se as pessoas que acessam os dados permanecessem dentro desses perímetros. Mas, cada vez mais, não permanecem e, assim que o perímetro é ultrapassado, suas políticas de proteção de dados desabam. Isso significa que não é mais suficiente colorir dentro das linhas. Vamos examinar o que pode ser feito para superar isso.

Implicações da Transformação da Nuvem

A migração para a nuvem não é uma questão de "se". É uma questão de "quando". As demandas de funcionários, clientes e parceiros estratégicos remotos só aceleram a linha do tempo, pressionando por uma adoção mais rápida da nuvem. Um exemplo? Das empresas atuais, 87% dependem de acesso a aplicativos de negócios móveis pelos funcionários em smartphones pessoais[3] —isso é chamado de "traga seu próprio dispositivo", ou BYOD (Bring Your Own Device). Além disso, quase um terço dos millennials dizem que fazem download de arquivos da empresa para esses dispositivos e instalam aplicativos de nuvem de outros fornecedores (Bring Your Own Cloud ou BYOC) sem notificar a TI ou a liderança executiva. Esses comportamentos criam o que é conhecido como Shadow ITe demonstram que a empresa nem sempre está no controle de quando e como migrará para a nuvem. Contudo, não importa qual seja o ritmo, as políticas de segurança implementadas se esforçam para correr atrás na adaptação às novas demandas.

Um motivo é que os fornecedores de aplicativos de nuvem tendem a priorizar portabilidade, acessibilidade e facilidade de uso—não necessariamente a segurança dos dados que ficaram portáteis, acessíveis ou fáceis de usar. Têm foco em um modelo de responsabilidade compartilhada em que protegem a infraestrutura, mas deixam a proteção dos dados compartilhados na infraestrutura para o cliente. Isso significa que, considerando a natureza transicional e móvel do trabalho atualmente, você é que precisa criar proteção de dados que acompanhe as suas pessoas.

As Pessoas São o Novo Perímetro

Como você pode manter os dados seguros quando as pessoas que os usam atravessam as suas linhas de defesa? É necessário um novo perímetro: as pessoas.

A proteção de dados centrada nas pessoas permite que os dados sejam mantidos em um ambiente seguro, que as pessoas possam acessar não importa onde trabalhem. Além disso, vincular a segurança de dados à identidade de uma pessoa habilita políticas que levam em conta o risco pessoal, fornecendo insight sobre a intenção—por exemplo, um incidente envolvendo um funcionário antigo pode preocupar muito menos do que um incidente com um fornecedor questionável ou ex-funcionário insatisfeito. Por fim, monitorar a segurança de dados no nível das pessoas fornece visibilidade sobre como usam os dados em diferentes dispositivos e aplicações, fornecendo contexto que pode ajudar as equipes de segurança a identificar melhor as ameaças e aprender com elas.

Apresentando o Caso de Negócios para Proteção de Dados

A proteção de dados centrada nas pessoas é muito adequada para a realidade dinâmica das empresas atualmente—mas quanto vale para a sua? Para responder, vamos derrubar o mito que atrapalha as equipes de segurança de dados em todos os lugares: de que a proteção é inimiga da produtividade. Com as ferramentas e processos certos, uma pode habilitar a outra.

Respostas Específicas

As táticas tradicionais de prevenção contra perda de dados podem simplesmente bloquear ações arriscadas—por exemplo, salvar um arquivo confidencial da empresa em um pen drive pessoal. E se essa ação for realizada por um ex-funcionário insatisfeito ou prestador de serviços ocasional, essa resposta faz sentido. Com frequência, porém, não é o caso: pode ser um executivo da empresa simplesmente tentando fazer backup de um arquivo importante ou transferir para outro computador. Mas as políticas tradicionais de segurança de dados não identificam a diferença e, como rotina, bloqueiam totalmente atividades digitais inocentes—impedindo a produtividade da empresa em consequência.

Detectar riscos em nível das pessoas torna possível considerar o contexto e a intenção por trás de uma ação, habilitando respostas de segurança específicas—e não genéricas. Isso não apenas reduz as interrupções nos fluxos de trabalho dos funcionários, mas também diminui as atividades de investigação das equipes de segurança, permitindo que ajudem o progresso em vez de bloqueá-lo.

Redução da Vulnerabilidade

Mesmo um funcionário sem má intenção pode se frustrar com as políticas de segurança padrão que bloqueiam seu trabalho. Portanto (ainda sem má intenção) pode tentar encontrar um atalho, ignorando as regras ligeiramente, para passar pelo bloqueio de segurança. Nesse último exemplo, talvez divida o arquivo em segmentos menores e envie por e-mail para um computador pessoal, para poder salvar no pen drive.

Isso cria dois problemas. Primeiro, essa sequência de ações pode motivar um alarme ainda mais urgente do que uma tentativa de salvar um arquivo em pen drive, porque indica que uma pessoa está tentando contornar medidas de segurança. Provavelmente será necessário investigar, o que requer tempo e recursos. Mas talvez o que motive mais preocupação é que atalhos como esses, embora pareçam inocentes, podem introduzir novas vulnerabilidades que enfraquecem as políticas de segurança que os motivaram. A proteção de dados centrada nas pessoas permitirá políticas mais flexíveis e apropriadas, impedindo essa espiral de solapamento antes que comece.

Abordagem Proativa

Como qualquer professor, proprietário de animal de estimação ou profissional de segurança de dados pode testemunhar, prevenir que uma "bagunça" ocorra é muito mais eficiente do que limpá-la depois.

Com as dicas contextuais e os insights comportamentais que os dados centrados nas pessoas fornecem, é possível bloquear ameaças reais antes que inflijam danos, sem impedir que as empresas tenham desempenho no mais alto nível. Os funcionários podem trabalhar sem tropeçar em políticas de segurança inflexíveis. As equipes de segurança de dados atarefadas podem triar alertas com precisão e se concentrar em incidentes que realmente gerem risco. É segurança de dados—sem comprometimento.

O Novo Padrão para Proteção de Dados

A natureza das ameaças de segurança em constante evolução significa que precisamos ajustar a nossa mentalidade para manter a segurança dos dados—e isso inclui aceitar que a mudança é, e sempre será, constante. É por isso que os nossos princípios essenciais para proteção de dados são criados tendo em mente as necessidades do futuro:

1. Uma cultura de segurança de dados preventiva e não punitiva

A função das equipes de segurança de dados evoluirá de aplicar políticas de segurança de forma retroativa para liderar as organizações e os funcionários em comportamentos mais seguros para uso de dados.

2. Avaliação de riscos centrada em pessoas

O uso de dados móveis e dinâmicos requer segurança que considere a única constante: o usuário. Isso habilita segurança flexível, que se adapta à medida que o comportamento e o nível de risco da pessoa mudam.

3. Visão holística dos dados

Manter visibilidade completa sobre os dados em trânsito fora de sua rede, entre endpoints ou na nuvem fornece dicas contextuais sobre intenção, ajudando a informar respostas de segurança adequadas.

4. Políticas consistentes, não importa qual seja o ambiente

Definir o seu perímetro de segurança no nível das pessoas garante que os dados sejam protegidos não importa onde estiverem armazenados ou forem acessados.

Está pronto para o futuro na jornada para a proteção de dados proativa?

› **Confira o nosso infográfico,** 9 Passos para o Sucesso em Proteção de Dados.

1. IBM Marketing Cloud, "10 Key Marketing Trends for 2017"
2. Ponemon Institute, "U.S. Cost of a Data Breach Study", 2017
3. Syntonic, "BYOD Usage in the Enterprise", 2016

Forcepoint

forcepoint.com/contact

Sobre a Forcepoint

A Forcepoint é líder em cibersegurança para proteção de usuários e dados, com a missão de proteger as organizações ao impulsionar transformação digital e crescimento. As soluções da Forcepoint adaptam-se em tempo real a como as pessoas interagem com dados, fornecendo acesso seguro e habilitando os funcionários a criar valor. Com sede em Austin, Texas, a Forcepoint cria ambientes seguros e confiáveis para milhares de clientes no mundo inteiro.