Forcepoint

9 Passos para o Sucesso em Proteção de Dados

Proteção de dados é entender os riscos potenciais para os seus dados e saber como agir se ocorrerem.

Mas como você pode equilibrar o que a sua organização precisa para trabalhar com o que precisa para manter os dados seguros?

Estes nove passos orientarão você em como implementar controles de proteção de dados que sejam tanto mensuravelmente eficazes como viáveis para o seu dia a dia, e identificar oportunidades para fortificar a sua solução com proteção de dados adaptável a riscos.

1

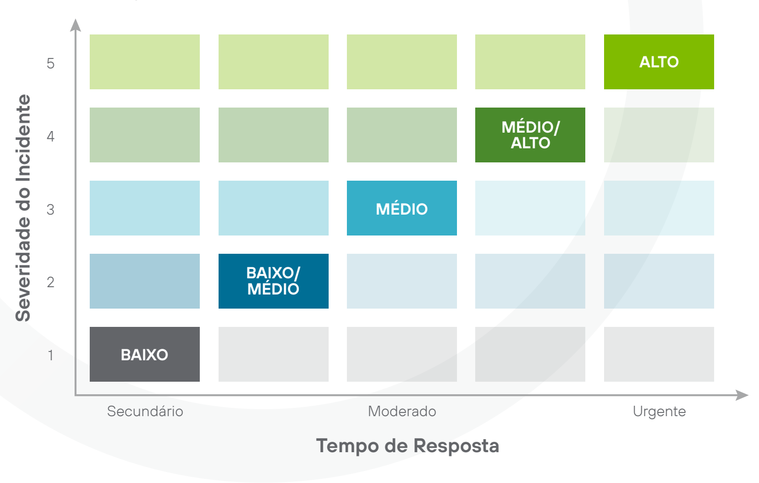
Crie um Perfil de Riscos da Informação

Um perfil de riscos ajuda a entender o que você precisa obter de sua solução de proteção de dados. Primeiro, identifique os riscos que quer mitigar e relacione os tipos de dados a que se referem, agrupando por tipo de dados, conforme necessário. Depois, defina redes, endpoints e canais de nuvem onde os dados poderiam potencialmente ser perdidos, junto com os controles que você usa atualmente para protegê-los.

2

Criar um Gráfico de Severidade e Resposta para Incidentes de Dados

Mapear cada tipo de dados com seu impacto empresarial permitirá que você priorize as respostas e mantenha os recursos de segurança focados onde são mais eficazes. Para algumas organizações, isso pode ser um exercício desafiador. Para começar, reúna-se com os proprietários dos dados para discutir quais tipos devem ser protegidos e qual é o risco se forem comprometidos. Em seguida, classifique em uma escala de 1-5 (1=baixo impacto, 5=alto impacto) e defina um tempo de resposta aceitável para cada um, de acordo com a severidade do risco—recomendamos proteger os tipos de dados de alto risco primeiro.



A Diferença Adaptável a Riscos:
A proteção de dados adaptável a riscos foi elaborada para priorizar atividades de alto risco, aplicar controles de forma autônoma com base em risco e reduzir o tempo necessário para investigar um incidente.

3

Determine uma Resposta a Incidente de Dados por Canal e Severidade

Ficar um passo à frente em proteção de dados significa saber como responder a incidentes antes que ocorram. Relacione todos os canais em sua rede, endpoints e nuvem onde há fluxo de dados. Em seguida, determine uma resposta apropriada para incidentes de baixo a alto impacto, com base nas necessidades do canal.

A Diferença Adaptável a Riscos:
Uma solução adaptável a riscos considera o nível de risco de cada pessoa que toca em seus dados, habilitando você a ajustar as respostas a incidentes com base em risco individual. Por exemplo, adaptar a resposta para somente auditoria para usuários de baixo risco e só bloquear para usuários de alto risco garante que cada membro de sua equipe possa trabalhar sem comprometer dados ou impactar a produtividade dos usuários.

Canais	Nível 1 Baixo	Nível 2* Baixo-Médio	Nível 3 Médio	Nível 4* Médio-Alto	Nível 5* Alto	Observações
E-mail	Criptografar	Eliminar Anexos de E-mail	Quarentena	Quarentena	Bloquear	Criptografar
Web	Auditar	Auditar/Notificar	Bloquear/Notificar	Bloquear/ Notificar		Proxy a Bloquear
Web Segura						Inspeção SSL
FTP						Proxy a Bloquear
Impressora de Rede						Instalar Agente de Impressora DLP
Personalizado						
Aplicativos de Nuvem			Quarentena com Anotação	Quarentena		

* Granularidade adicional disponível com Proteção de Dados adaptável a riscos

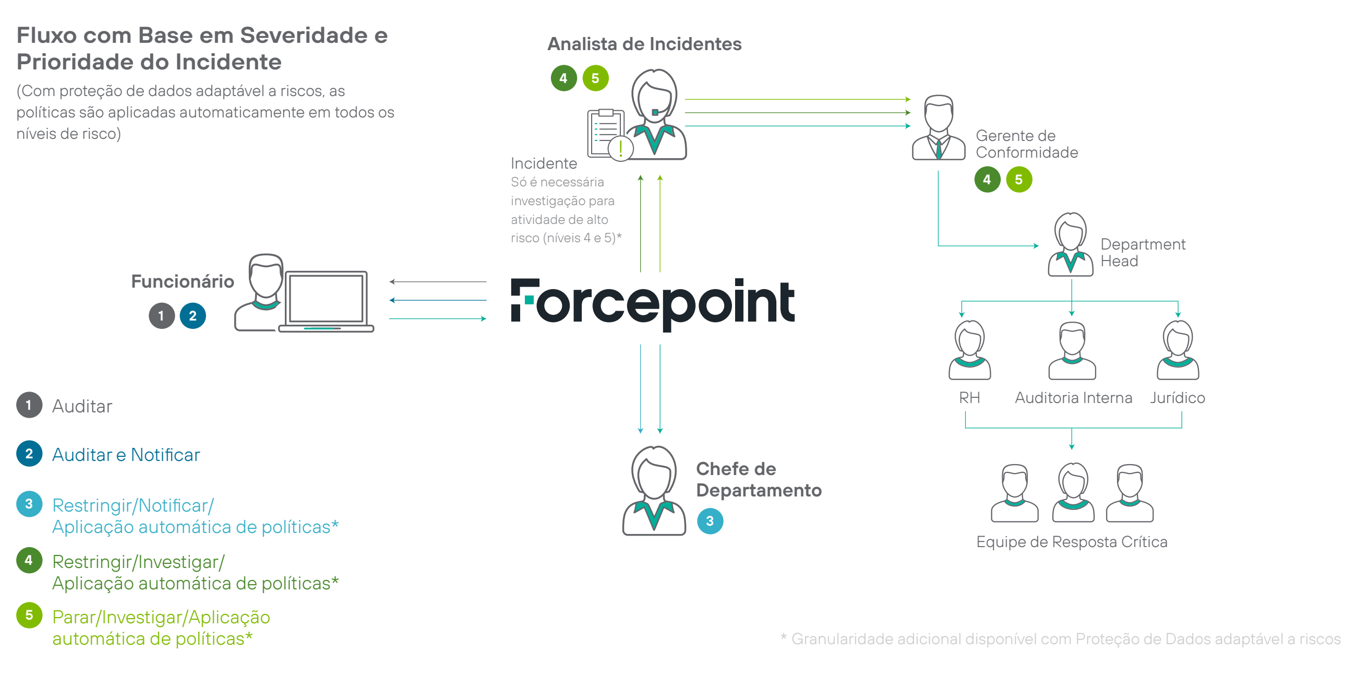
4

Estabelecer um Fluxo de Trabalho de Incidentes

Garanta que as suas equipes de segurança possam agir no momento em que um incidente é detectado, definindo claramente o fluxo de trabalho de resposta para incidentes de baixo a alto impactos. Para incidentes com impacto mais baixo, automatize sempre que possível. Isso vai liberar banda de rede para remediação prática de incidentes com impacto mais alto.

A Diferença Adaptável a Riscos:
Uma solução adaptável a riscos permite analisar incidentes com base em nível de risco individual, sem precisar envolver um analista de incidentes para determinar a melhor ação a adotar. Os incidentes vinculados a pessoas de baixo risco podem não apresentar uma ameaça à sua empresa; portanto, permitir que continuem (com salvaguardas adicionais como criptografia para transferência de arquivos por USB ou exclusão automática de anexos de e-mail) pode manter as rodas da produtividade girando.

Os administradores podem adotar a mesma abordagem proativa com pessoas e incidentes de alto risco, bloqueando ou restringindo automaticamente ações específicas até que um analista de incidentes possa investigar.


Fluxo com Base em Severidade e Prioridade do Incidente
(Com proteção de dados adaptável a riscos, as políticas são aplicadas automaticamente em todos os níveis de risco)

* Granularidade adicional disponível com Proteção de Dados adaptável a riscos

5

Atribuir Papéis e Responsabilidades

Aumentar a estabilidade, a escalabilidade e a eficiência operacional do programa de proteção de dados, definindo quem é quem em sua equipe. Atribuir papéis principais, como administradores técnicos, analistas de incidentes, investigadores forenses e auditores, e atribuir direitos e acessos apropriados para cada um deles.

6

Iniciar Projeto em Modo de Monitoramento

Depois que você tiver sua solução de proteção de dados da rede implementada, um período de monitoramento permitirá que você identifique padrões em sua atividade e defina uma referência para ajudar a reconhecer comportamentos normais de usuários. Depois que esse período estiver concluído, analise o comportamento que observou e apresente seus achados à equipe executiva, com recomendações para mitigar riscos. Em seguida, você pode colocar essas recomendações em ação, monitorar seu sucesso e apresentar aos executivos novamente.

A Diferença Adaptável a Riscos:
Com uma solução adaptável a riscos, analisar incidentes em modo somente auditoria (em oposição a modo de aplicação graduada) destacará a redução de incidentes que requerem investigação—sem comprometer seus dados. Além disso, você vai observar incidentes mais positivos sem desperdiçar recursos para abordar ameaças falsas.

7

Mover para Proteção Proativa

O que você aprendeu em modo de monitoramento fornecerá o nível de confiança de que precisa para transicionar para o modo de bloqueio para eventos de alto risco, ou em conformidade com seu plano de resposta a incidentes. À medida que implementa proteção de dados para endpoints e aplicativos de nuvem aprovados, você vai monitorar, analisar, reportar, otimizar e reportar novamente seus achados para a equipe executiva.

8

Integrar Controles de Proteção de Dados em Toda a Empresa

Ao delegar responsabilidades para líderes de segurança em vários departamentos, pense em "eficiência". Por exemplo, os proprietários de dados já são responsáveis em caso de perda de dados; portanto, denominá-los como gerentes de incidentes ajuda-os a entender como os dados são usados por outras pessoas e avaliar os riscos, eliminando consultas desnecessárias.

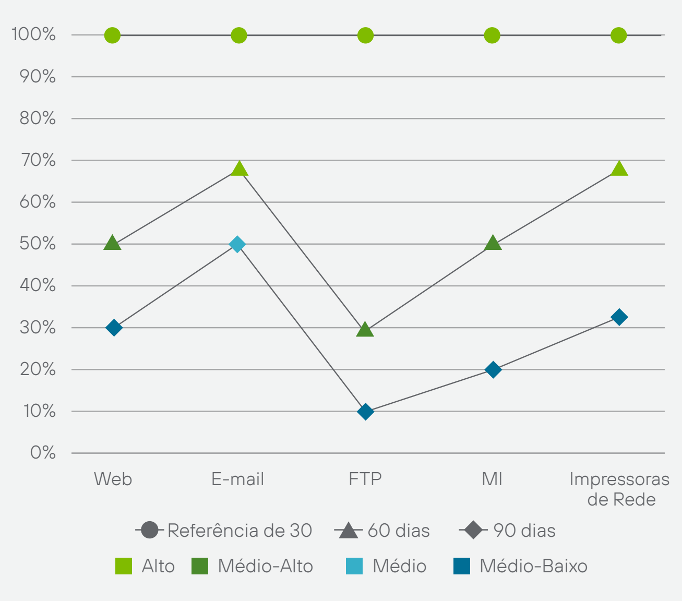
Comece a delegar, solicitando que a equipe de segurança faça uma reunião de início de projeto para apresentar os controles de proteção de dados para as outras pessoas. Em seguida, ofereça treinamento para os novos membros das equipes e defina um período de tempo durante o qual você ajudará com a resposta a incidentes, até que se sintam à vontade com os seus processos. Você também pode considerar oferecer coaching em tempo real para reforçar esses processos.

9

Monitore os Resultados de Redução de Riscos

Você começou a se preparar para isso no Passo 6—veja o que falta: Agrupe incidentes relativos juntos, por critérios como severidade, canal, tipo de dados e regulamentação. Em seguida, defina seus períodos de Monitoramento e Redução de Riscos para que tenham duração igual (experimente duas semanas cada, para começar) a fim de preservar a integridade de seus resultados.

Probabilidade de Perda de Dados



Número de Incidentes acima de 90 dias

Incidentes	E-mail	Web	FTP	MI	Impressora de Rede
Referência de 30 dias	150	200	50	10	45
60 dias	100	100	15	5	30
Redução de risco em 60 dias	33%	50%	70%	50%	33%
90 dias	76	60	5	2	15
Redução de risco em 90 dias	49%	70%	90%	80%	67%

Metas

60 dias
Redução de 25%+

90 dias
Redução de 50%+

A Diferença Adaptável a Riscos:
Com uma abordagem adaptável a riscos, é recomendado que você forneça uma comparação dos incidentes capturados em modo somente auditoria (todos os incidentes) em comparação com incidentes que requerem investigação com aplicação graduada. O resumo deve mostrar o número de incidentes para cada nível de risco 1-5, em contraste com os que requerem investigação (níveis de risco 4-5).

Não importa se você adotar uma abordagem tradicional ou ampliar sua segurança com proteção adaptável a riscos, esta fórmula comprovada ajudará a orientar você para o sucesso.

Quer ver a proteção adaptável a riscos em ação?

Veja Aqui

Forcepoint

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. [23MAR2020]