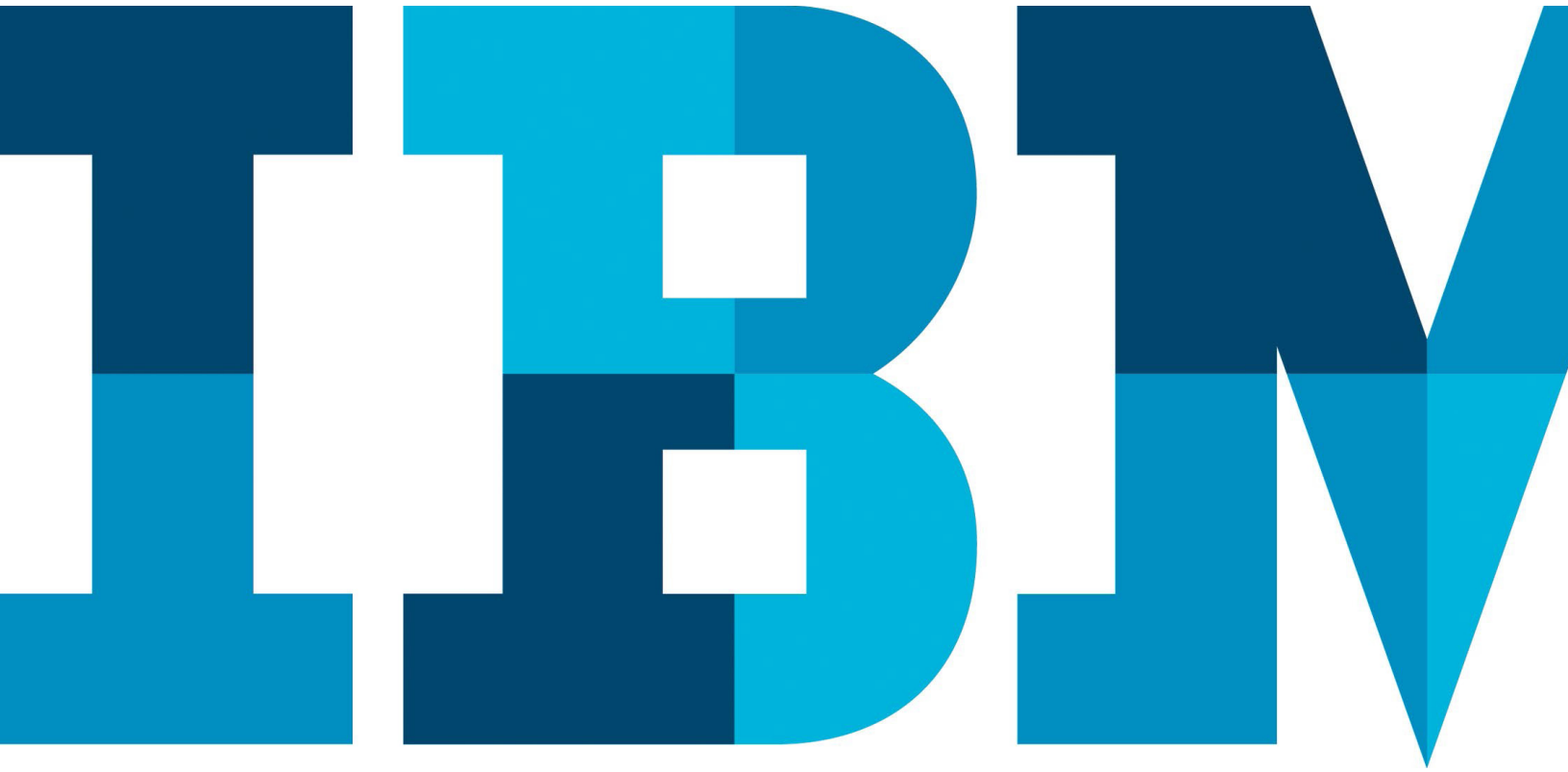
Segurança
Thought Leadership White Paper

Julho de 2015

Plataforma de gerenciamento de endpoint para organizações de todos os tamanhos

O IBM BigFix oferece insight e controle necessários para localizar ameaças, reparar vulnerabilidades e proteger dispositivos. De maneira rápida.



Introdução

Cada endpoint conectado ao seu sistema é um ponto de vulnerabilidade uma pequena porta que, se deixada aberta, pode expor toda a rede ao desastre. Ataques cada vez mais agressivos e sofisticados não podem mais ser evitados por mecanismos de segurança tradicionais, explorando fraquezas na vasta gama de endpoints conectados ao seu sistema. Com o cenário mudando a cada segundo, cada endpoint deve ser continuamente descoberto e monitorado para que ameaças possam ser eliminadas imediatamente em tempo real antes que elas afundem o navio inteiro. Para proteger a rede, cada endpoint deve ser gerenciado com segurança antes, durante e depois de potenciais ataques cibernéticos.

Com as ameaças de criminosos cibernéticos crescendo exponencialmente, como a sua organização pode evitar ser a próxima manchete por ter sofrido violação grave na segurança de dados? Como é possível identificar e corrigir vulnerabilidades em tempo real, enquanto se assegura que o sistema de gerenciamento de segurança, sem esforço, se integra e está em conformidade com políticas internas, padrões de segurança e regulamentos governamentais? Enxergue ameaças para todos os endpoints para que seja possível localizar e corrigi-las

Não é possível consertar o que você não pode ver.

O primeiro e mais básico requisito para assegurar a segurança é ter uma visualização completa em tempo real de cada endpoint conectado ao seu sistema ao longo de redes globais dinâmicas. Quando você é capaz de identificar potenciais vulnerabilidades e ameaças, é possível tomar ação imediatamente para evitar ataques que podem danificar a reputação da sua organização e causar graves perdas financeiras.

O IBM ajuda a proteger todos os seus endpoints a partir de terminais móveis como um laptop em uma cafeteria até dispositivos de ponto de vendas (POS) que se conectem por meio de sites de parceiros. Ele permite que você monitore continuamente cada terminal para potenciais ameaças e esteja em conformidade com políticas de segurança, operacionais e regulamentações

O BigFix funciona até mesmo em locais remotos com banda estreita ou nenhuma banda. E tem mais, um estudo recente descobriu que fornecer à equipe de segurança uma ferramenta de resposta a incidente efetiva como o BigFix pode ser o único responsável pela diminuição decusto por uma violação de dados mais do que técnicas de criptografia e treinamento de funcionários, além de ser necessário chamar terceiros para ajudar, o que pode aumentar ainda mais o custo de uma violação.

"...uma equipe de resposta a incidente pode reduzir o custo de uma violação de dados em US$ 12,60, de US$ 154 para US$ 141,40."

— Instituto Ponemon[1]

O BigFix inclui uma ampla faixa de verificações integradas, prontas para uso, de conformidade nativa para requisitos de segurança e regulamentações. Depois que o BigFix te avisa sobre uma ameaça, os seus recursos de correção automática permitem que você responda com incrível velocidade, parando potenciais ataques. O recurso de gerenciamento de correção automatizada do BigFix torna simples implementar rapidamente correções, mudanças na configuração e atualizações de política. Com o BigFix, você tem um alto nível de confiança de que endpoints são corrigidos e protegidos com êxito na primeira ameaça para que você possa ter certeza de que toda a rede esteja segura e em conformidade. A implementação de correção automatizada também reduz o tempo que a equipe de segurança e operacional escassa e valiosa deve gastar em tarefas manuais, liberando-a para projetos de valor mais alto.

Proteção contra ataque antes, durante e depois de um evento

O BigFix fornece monitoramento de endpoint contínuo, dinâmico, granular, proteção contra ameaças, resposta a incidente e controle de conformidade em todo o ciclo de vida da ameaça.

Antes: Monitoramento contínuo

A melhor proteção contra ameaças é descobrir vulnerabilidades e protegê-las antes que um exploit possa causar estragos em todo o seu ambiente de dados e de rede. O BigFix cumpre a conformidade de configuração contínua com políticas de segurança e regulamentação em cada endpoint para eliminar desvio de configuração que possa abrir janelas de oportunidade para potenciais ataques. Um agente inteligente único em cada endpoint monitora, gerencia e relata sobre o status de todos os endpoints em tempo real, independentemente do tipo de sistema operacional. Se uma correção ou configuração for alterada, o BigFix automática e autonomamente reaplica a política, ajudando a assegurar que a ação do usuário ou o malware não possa comprometer o endpoint.

Durante: Proteção contra ameaças

Equipes de segurança podem ser sobrecarregadas por um mar de vulnerabilidades sem os dados contextuais para ajudá-las a concentrarem os seus esforços nas fraquezas que são mais propensas a serem exploradas. Não é incomum por várias semanas ou mesmo meses passar entre a descoberta de uma vulnerabilidade conhecida e a correção conhecida que está sendo aplicada. Ao mesmo tempo, as equipes de segurança podem não ter uma visão abrangente do status do endpoint, o que limita a sua compreensão do cenário de ameaças.

O BigFix analisa dados de todos os endpoints e prioriza e exibe informações de status do endpoint no painel, enquanto alimenta essa inteligência de endpoint para o IBM Security. O QRadar avalia vulnerabilidades de acordo com o nível de ameaça, indo pelo ruído de milhões de eventos de segurança para dar a você a análise em minutos com uma priorização de risco dos endpoints mais vulneráveis que devem ser protegidos para evitar ou interromper um ataque em potencial.

O BigFix, junto com o IBM Security Trusteer, fornece proteção contra malware avançado durante ameaças, assegurando que o seu endpoint seja protegido enquanto espera que a correção apropriada seja liberada pelo fornecedor do aplicativo.

Depois: Resposta a incidente

Após uma ameaça ter sido descoberta, a equipe de segurança precisa tomar ação de correção rapidamente em todos os endpoints dentro e fora da rede.

O BigFix inclui ações de quarentena customizáveis e automáticas, de modo que endpoints que não estejam em conformidade ou comprometidos sejam colocados em quarentena até a correção estar concluída. Processos automatizados, em tempo real podem reduzir janelas de correção de dias ou semanas para apenas horas ou minutos ajudando a desinfetar rapidamente endpoints e assegurar a conformidade constante com políticas de segurança e outras.

"Agora podemos rapidamente, facilmente e com precisão produzir relatórios de auditoria... Isso nos ajudou a obter uma soma considerável de dólares em incentivo ao uso da solução. "

—Eddy Stephens, Chief Information Officer, Infirmary Health System

---

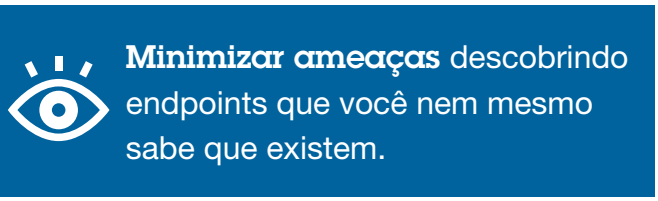
Visibilidade e controle compartilhados entre as operações de segurança e de TI

O BigFix fornece uma abordagem unificada para conformidade permitindo que ambas as equipes de segurança e operacionais vejam o estado atual de todos os endpoints em uma visão rápida. Com a visualização dinâmica da solução do estado de configuração, ambas as equipes podem ver imediatamente cada endpoint dento ou fora da rede e independentemente do local e se esses endpoints estão ou não em conformidade.

A plataforma BigFix integra e automatiza avaliação e correção, permitindo que as equipes de segurança e de operações operem simultaneamente para corrigir e direcionar risco, trazer sua organização para a conformidade contínua, enquanto reduz custos. Ativando proteção de endpoint, o BigFix oferece cinco recursos que são indispensáveis visibilidade, escalabilidade, confiança, conformidade e velocidade.

Agora que sabemos o que implementamos e onde, estamos melhor posicionados para localizar qualquer furo não corrigido em nossos sistemas e manter os nossos dados corporativos protegidos.

Visibilidade: insight e controle para cada endpoint, em toda parte



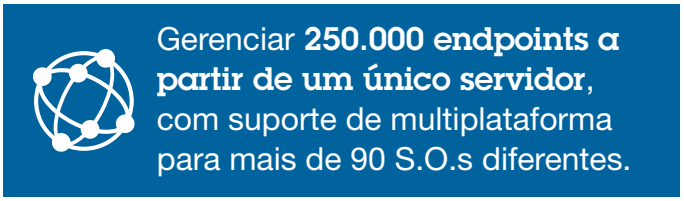
O BigFix entrega visibilidade granular, contínua, em tempo real e controle de cada endpoint conectado à sua rede independentemente do tipo de sistema operacional ou local. Sejam desktops, laptops, caixas automáticos, servidores (ambos: físicos e virtuais), dispositivos de POS ou ainda outros, o BigFix pode descobrir e controlar cada endpoint. Após implementar o BigFix, as organizações normalmente descobriram mais de 35 por cento de endpoints se conectando à sua rede corporativa do que identificados anteriormente.

Um agente do BigFix em cada endpoint verifica continuamente a conformidade com segurança, as políticas operacionais e regulamentações, agrega e analisa os dados e exibe o status de endpoint no painel de gerenciamento do BigFix fornecendo notificações quase instantâneas de vulnerabilidades, como proteção contra vírus desatualizada ou software não licenciado que podem conter malware potencialmente prejudicial.

Agora que sabemos o que implementamos e onde, estamos melhor posicionados para localizar qualquer furo não corrigido em nossos sistemas e manter os nossos dados corporativos protegidos.

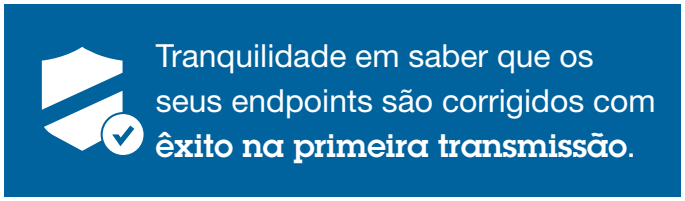
— Allstate

Escalabilidade: Proteção completa através do universo do endpoint



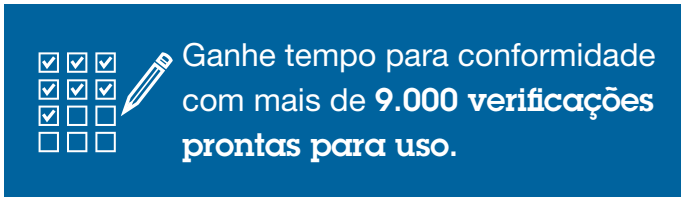
O seu sistema de segurança deve ser capaz de escalar, sem esforço, para proteger um número em constante mudança e cada vez maior de endpoints. O BigFix permite que você gerencie e proteja até 250.000 endpoints, quer estejam dentro ou fora de sua rede, tudo a partir de um único servidor e painel. O BigFix é altamente extensível, suportando mais de 90 tipos e versões de sistemas operacionais para assegurar a cobertura em todas as plataformas. Ao mesmo tempo, o BigFix minimiza o impacto de medidas de segurança no desempenho do dispositivo, ajudando a manter os usuários produtivos e o seu trabalho ininterrupto.

Confiança: Garantia de que a correção é feita de maneira correta na primeira vez



O BigFix funciona na primeira vez com uma notável taxa de sucesso de correção na primeira transmissão e automaticamente propaga atualizações de configuração e de política conforme as necessidades do sistema e de dados. O agente inteligente em cada endpoint relata sobre o status da correção em tempo real, dando a você visibilidade até o aquele momento no status de conformidade de correção de todos os seus endpoints.

Conformidade: Adesão contínua e automática aos padrões



Endpoints que não possuem as correções críticas ou que têm erros de configuração deixam os seus dados e a infraestrutura totalmente abertos para ataque. Usando um agente inteligente em cada endpoint, o BigFix monitora, gerencia e cumpre um estado de conformidade contínua para segurança,, regulamentação e operações. Com mais de 9.000 verificações de conformidade nativas prontas para uso para várias políticas, bem como a capacidade de criar rápida e facilmente políticas customizadas, o BigFix é projetado para ganhar tempo para conformidade e diminuir custos operacionais. Políticas podem ser cumpridas com base no tipo ou local do endpoint. Se um endpoint for considerado fora de conformidade, pode ser automaticamente colocado em quarentena até que uma ação de correção seja tomada.

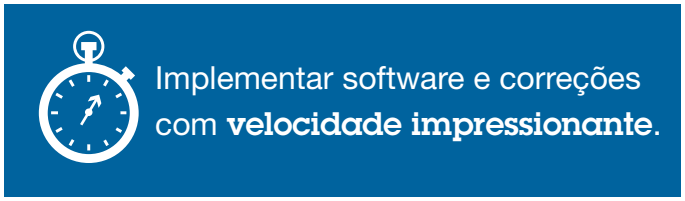
O BigFix reforça a segurança de endpoint no Infirmary Health System

Infirmary Health System, a maior equipe de saúde não-governamental do Alabama, necessitava automatizar e reforçar o gerenciamento de segurança e de endpoint para proteger melhor os dados e atender aos requisitos do Ato de Portabilidade e Prestação de Contas de Seguro de Saúde (HIPAA) federal, bem como requisitos para uso.

Trabalhando com Tecnologia ESM, um Parceiro de Negócios IBM, a organização implementou o IBM BigFix junto com as soluções do IBM Security QRadar, permitindo que a equipe protegesse endpoints e respondesse imediatamente a ameaças da organização. A visibilidade em tempo real em todos os endpoints, com análise e priorização de vulnerabilidades, permitiu que a equipe tomasse medidas corretivas, concentrando-se nos endpoints mais críticos primeiro, antes que todo o sistema pudesse ser comprometido.

Além disso, o BigFix cumpriu a conformidade contínua com segurança e políticas regulamentares. O BigFix também ajudou a reduzir custos aperfeiçoando operações de segurança e de TI através da visibilidade e do controle compartilhados a partir de uma única plataforma. A taxa de sucesso de correções aumentou de 40 por cento para 90 por cento. O tempo de implementação de software foi reduzido de sete semanas para apenas dois dias.

Velocidade: Resposta a ataques com velocidade impressionante



O BigFix permite responder a ataques rapidamente, isolando e minimizando perigo de um único endpoint antes que possa causar danos caros na rede inteira. A implementação

de correções e upgrades pode ser feita com velocidade impressionante, de modo que logo que uma ameaça é descoberta e um procedimento de mitigação é concebido, a proteção pode ser imediatamente aplicada através de redes globais em questão de minutos.

Conclusão

O BigFix pode fortalecer a variação de segurança de sua organização enquanto reduz custos fornecendo visibilidade automatizada, contínua e em tempo real e controle em todos os endpoints conectados à sua rede. Unindo décadas de experiência das da IBM, ás famílias de soluções QRadar e Trusteer, ele é um elemento chave no fornecimento de proteção abrangente contra ameaças para as organizações. O agente único, o painel único, a solução do BigFix de servidor único permite que você veja, altere e cumpra políticas de segurança e conformidade de endpoint em tempo real, em uma escala global. Sua abordagem integrada, de circuito fechado ao gerenciamento de risco e de operações ajuda a reduzir custos e assegurar um estado contínuo de conformidade.

Para obter mais informações

Para saber mais sobre sistemas de proteção de dados IBM, entre em contato com o seu representante IBM ou Parceiro de Negócios IBM ou visite: **ibm.com**/security/bigfix

IBM Security
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
em Julho de 2015

[1] "2015 Estudo de Custo de Violação de Dados: Análise Global," *Instituto Ponemon*, Maio de 2015. http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-preach/

Recicle

WGW03126-BRPT-00