Segurança IBM
Thought Leadership White Paper

Julho de 2015

Resposta proativa à ameaças persistentes avançadas atuais

IBM BigFix: Estratégias abrangentes para minimizar risco

Conteúdos

Introdução

Não há nada à prova de falhas no mundo digital de hoje. Incidentes ocorrerão, sejam não intencionais ou maliciosos. Para minimizar dano e impacto organizacional, a organização ágil responderá rapidamente. Para minimizar riscos antes que o dano ocorra, uma organização pode manter um alto e contínuo nível segurança , assegurando que todos os endpoints estejam em conformidade, permitindo automatizar ações para diminuir tempo de resposta e promulgar medidas para controlar infecções em quarentena até que a correção seja concluída.

Atingir esse nível de agilidade, no entanto, requer visibilidade em tempo real e controle sobre todos os endpoints, não só para identificar desvios de políticas, mas também para retornar rapidamente o ambiente para a estabilidade. Um sistema de resposta efetivo também deve gerenciar dispositivos remotos dentro ou fora da rede executando sistemas operacionais heterogêneos. Ele deve ser escalável para atender às crescentes demandas de rede. Deve combinar velocidade, detecção precisa e técnicas de correção de alta qualidade em face de ameaças que são mais rápidas, mais sofisticadas e mais difíceis de evitar.

O IBM ajuda as organizações a manterem a conformidade contínua para evitar ameaças e inclui recursos adicionais para rapidamente responder a incidentes de segurança e minimizar o seu impacto. Desenvolvido com uma arquitetura de agente inteligente, o BigFix entrega visibilidade em tempo real e controle para garantir a proteção operações de TI com proteção próximo a zero-day em ambientes heterogêneos e onde quer que os laptops estejam. Ele inclui os melhores recursos analíticos que fornecem insights para fortalecer a infraestrutura com relação a ataques à rede, servidores e endpoints.

Respondendo a ameaças de forma rápida e efetiva

No mundo interconectado, instrumentado e inteligente de hoje, onde as organizações são distribuídas de forma global, complexa e móvel, tanto a importância de segurança quanto os desafios de proteção de endpoint estão constantemente aumentando. Com as ameaças persistentes avançadas crescendo mais dinâmicas e mais prejudiciais, a necessidade de uma resposta efetiva através de um sistema de alta performance nunca foi tão importante. Ao mesmo tempo, o atraso entre a descoberta de uma vulnerabilidade e a liberação do código de exploit foi medido em meses. Em seguida, ele caiu para semanas e depois, dias. Hoje, a capacidade de direcionar vulnerabilidades anteriormente desconhecidas ou desencadear novas maneiras de explorar vulnerabilidades conhecidas (conhecidas como ataques de pode ser tão breve como algumas horas. Em muitos casos, os criminosos cibernéticos já não precisam descobrir vulnerabilidades de sistema e de aplicativos por conta própria. Eles simplesmente esperam até que as informações de vulnerabilidade tornam-se públicas por pesquisadores de segurança e fornecedores de software. As informações são então usadas para desenvolver código para explorar a vulnerabilidade com mais agilidade do que as organizações podem responder.

Um ataque e uma infecção na infraestrutura de tecnologia da organização especialmente um ataque rápido, inesperado de zero-day pode levar a perdas significativas em renda, produtividade de usuário, relacionamentos com cliente e reputação no mercado. A resposta a esse perigo reside na manutenção de um estado alto e contínuo de segurança para evitar ataques, quando possível, e um sistema de alto desempenho de resposta a incidente, que corresponda à velocidade desses ataques crescentes e atacantes cada vez mais sofisticados.

O BigFix pode fornecer essa conformidade contínua e resposta rápida. O agente inteligente do BigFix continuadamente avalia a conformidade com políticas, automatiza correção e notifica imediatamente o console de gerenciamento centralizado sobre uma mudança de status. Essa abordagem dá às organizações visibilidade de endpoint atualizado e controle, e rapidamente identifica e corrige exposições e riscos à segurança do terminal. Os seus recursos de análise de dados fornecem insight e relatório para atender aos regulamentos de conformidade e objetivos de segurança de TI.

O BigFix ajuda as organizações a responderem rapidamente às ameaças de hoje com:

- **Velocidade impressionante:** Seja aplicando uma correção para corrigir uma vulnerabilidade recém-descoberta em centenas de milhares de endpoints ou mudando a configuração de um sistema de modo que ele esteja em conformidade com padrões, o BigFix pode afetar a mudança em toda a organização dentro de minutos. Com o BigFix, avaliação e análise são realizados no próprio endpoint o que aumenta a velocidade de descoberta, a entrega de software e a validação. Menos comunicação é necessária entre o servidor de gerenciamento e o endpoint, aumentando a velocidade e reduzindo a necessidade de banda larga da rede consumida.
- **Precisão excepcional:** O BigFix pode interrogar com precisão qualquer aspecto de um endpoint e fornecer uma visualização completa em tempo real dos problemas que existem no ambiente. Ao fazer isso, ele permite que as organizações descubram problemas de forma rápida e ele fornece uma camada adicional de defesa quando as defesas de segurança tradicionais falham completamente ou fornecem correções muito tarde para evitar um incidente. O console de gerenciamento centralizado da solução fornece uma visualização única, granular para visibilidade e controle abrangentes ao longo das redes globais distribuídas. Os operadores podem executar ações corretivas em minutos e receber validação imediata de que a ação foi concluída com sucesso.
- **Qualidade de controle:** Conforme vírus, worms e botnets fazem mudanças na configuração em um computador, essas muitas vezes passam despercebidas por abordagens tradicionais de segurança, como antivírus e anti-spyware. Mas com a visibilidade granular em propriedades de endpoint, o BigFix possibilita que as organizações vejam essas mudanças e automatizem medidas corretivas para manterem a conformidade. De forma semelhante, o BigFix pode descobrir aplicativos instalados em sua infraestrutura. Quando uma parte de código malicioso tenta instalar aplicativos não autorizados, o BigFix tem a capacidade de identificar esse comportamento em tempo real e de corrigi-lo automaticamente.
- **Proteção baseada em nuvem:** O BigFix pode fornecer segurança para endpoints fixos, conectados à rede e móveis, endpoints conectados à Internet mais rápidos do que esperar a distribuição em massa de arquivos de assinatura de um fornecedor. O BigFix faz referência cruzada de informações de ameaça com relação a um banco de dados grande, baseado em nuvem, para avaliar o potencial arquivo malicioso e URLs em tempo real e entrega proteção anti-malware a endpoints, conforme necessário. Um laptop usado em um aeroporto, por exemplo, pode receber em qualquer lugar, a qualquer hora, proteção baseada em nuvem das ameaças escondidas em websites que ele visita ou em arquivos que ele recebe.

- **Auto-quarentena de rede:** O BigFix pode avaliar automaticamente endpoints com relação a configurações de conformidade necessárias e se um endpoint for descoberto como fora de conformidade, a solução pode configurar o endpoint de modo que ele seja colocado em quarentena de rede até que a conformidade seja atingida. O BigFix retém o acesso de gerenciamento para o endpoint, mas todos os outros acessos são desativados.

Colocar um ataque de vírus sob controle rapidamente

Um ano depois de sofrer um ataque grave a partir de um worm baseado na Internet, que precisou de quatro horas por sistema para reparo, a um custo total de US$ 1,6 milhões, uma grande universidade implementou o BigFix como uma defesa melhor contra o próximo ataque.

Quando o próximo conjunto de worms afetou a universidade, somente cerca de dois por cento de mais de 12.000 computadores que executavam o BigFix foram comprometidos. Esses sistemas infectados foram rapidamente e automaticamente reparados com inconveniência mínima para os seus proprietários. Dos outros 8.000 computadores que não estavam executando o BigFix, mais de 15 por cento ficaram infectados e exigiram uma grande quantidade de trabalho para reparar.

Protegendo a organização distribuída e complexa de hoje

Como muitas organizações agora são globais, suas infraestruturas de rede muitas vezes lutam para se manterem. Muitas infraestruturas são executadas sobre largura da banda baixa, redes de alta latência. Visibilidade insatisfatória e longos tempos de atraso se traduzem em curso insatisfatório de dados e risco aumentado. TI não sabe o estado dos dispositivos, se ele foi explorado ou, após a entrega do software, se uma correção foi implementada em um endpoint. Além disso, os criminosos cibernéticos aprenderam a tirar vantagem da reliance corporativa em e-mail e as ações simples da web como a abertura de um anexo do e-mail ou clicar em um link da web podem resultar em dados confidenciais perdidos, infraestrutura danificada ou em uma reputação arruinada.

Além disso, muitas organizações possuem um grande número de sistemas legados e devem gerenciar ativos que são executados em uma variedade de plataformas. Enquanto alguns podem considerar uma infraestrutura heterogênea como uma boa estratégia de segurança defensiva, isso complica a capacidade de efetivamente gerenciar e proteger endpoints. E, conforme as infraestruturas se expandem, o desafio de gerenciar e proteger um número crescente de endpoints aumenta proporcionalmente.

O BigFix é projetado para dar às organizações os recursos que eles precisam para gerenciar e proteger ambientes complexos e heterogêneos:

- **Gerenciamento otimizado de dispositivos remotos e móveis:** A arquitetura distribuída de agente inteligente do BigFix permite a descoberta contínua e a avaliação de laptops aonde quer que estejam. Qualquer sistema que esteja executando o agente da solução pode agir como uma retransmissão um ponto de comunicação para políticas e correção e qualquer retransmissão roteável publicamente pode avaliar e assegurar a conformidade da configuração em endpoints que estejam conectados à Internet. Como cada agente tem uma cópia local da política, a retransmissão pode enviar qualquer mudança de política diretamente para o endpoint, desde que a retransmissão esteja conectada à Internet.

- **Conformidade contínua:** O BigFix vem com listas de verificação de melhor prática que podem ser usadas para avaliar a conformidade. O agente inteligente fornece a aplicação de política contínua e proteção de endpoint, quer o endpoint esteja ou não conectado à rede corporativa. Assim que uma configuração de endpoint é modificada, o agente pode detectar se esse comportamento está fora de conformidade e pode executar automaticamente as tarefas necessárias para trazer o endpoint de volta em um estado de conformidade. Em seguida, ele notifica o servidor de gerenciamento sobre essa atividade. O resultado é a proteção constante contra exploits, independentemente de onde um endpoint está.
- **Suporte de multiplataforma:** O suporte de multiplataforma do BigFix simplifica a administração de ambientes heterogêneos incluindo aqueles com sistemas legados e aplicativos. A solução do BigFix suporta ambientes que executam várias gerações do Microsoft Windows bem como sistemas operacionais UNIX, Linux e Mac incluindo ambientes virtualizados.
- **Minimizando vulnerabilidades antes de um exploit:** O BigFix tem a capacidade de executar touch em qualquer chave de registro, arquivo, serviço ou componente que esteja no endpoint. Ele também pode gerenciar qualquer aplicativo ou serviço que esteja no endpoint. Se a equipe de TI precisa saber o que está dentro de uma chave de registro, eles podem usar o BigFix para consultar o ambiente e obter uma resposta precisa em minutos. Um endpoint que estiver off-line quando a consulta for enviada irá responder à política uma vez que o endpoint é roteável na Internet.
- **Informações de segurança e integração de gerenciamento de eventos:** Informações sobre a vulnerabilidade do BigFix enriquecem o banco de dados de vulnerabilidade do IBM Security QRadar, resultando em correlação mais precisa entre riscos e ofensa e em relatórios de conformidade melhorados. As soluções do QRadar e BigFix juntas fornecem monitoramento contínuo, cumprimento de conformidade, correção e relatório; endpoint, rede, evento de segurança e correlação de vulnerabilidade avançados; e identificação de dispositivo e correção.
- **Suporte de prevenção de perda de dados (DLP):** O BigFix ajuda a melhorar recursos de proteção de dados enquanto controla custos operacionais. Políticas de DLP podem ser criadas e aplicadas para limitar ou evitar a transmissão de ativos digitais por meio de canais de transmissão comuns, como e-mail e ajudam a proteger dados em dispositivos que deixam as instalações. O BigFix regula o acesso a dispositivos externos de armazenamento e recursos de rede para ajudar a evitar perda de dados, o que, combinado com a varredura de arquivos, ajuda a proteger contra riscos de segurança. Modelos predefinidos podem ser usados para identificar, monitorar e, opcionalmente, bloquear a transmissão de dados sensíveis como números de cartão de crédito.
- **Tempo rápido para proteção:** O BigFix pode gerenciar até 250.000 endpoints sobre infraestruturas altamente distribuídas, de rede altamente complexa, a partir de um servidor de gerenciamento único. E como os próprios endpoints executam a avaliação e aplicação de política, a organização não precisa investir em e gerenciar uma imensa infraestrutura do servidor de gerenciamento de endpoint. Independentemente de tamanho ou complexidade de rede, o BigFix pode ser implementado rapidamente, normalmente em questão de horas.

Migração de fornecedor de antivírus no Hospital Concord

Migrações de fornecedor de antivírus podem, muitas vezes, deixar uma organização exposta durante a transição. Utilizando os recursos de automação no BigFix, o Hospital Concord pôde migrar sem interrupção ou exposição, atingindo desempenho melhorado ao mesmo tempo.

A remoção e instalação teve uma média de cinco a dez minutos por máquina, com varreduras completas levando entre 30 e 60 minutos. A implementação foi quase invisível emdash nenhum usuário fez chamadas ao help desk durante a fase de lançamento. Após o lançamento, as pontuações de usabilidade da estação de trabalho aumentaram de um a sete numa escala de 10 pontos. A dispersão de atualizações de definição e varreduras manuais completas que anteriormente paralisavam muitas estações de trabalho podem agora ser implementadas tão rapidamente que elas passam praticamente despercebidas.

Assegurando resposta rápida a incidente

Mesmo nos ambientes mais seguramente gerenciados, incidentes acontecerão. Além de fornecer os recursos para ajudar as organizações a manterem um alto nível contínuo de segurança e de se preparar efetivamente para um incidente, o BigFix oferece funcionalidade de correção específica para minimizar dano e retornar endpoints para a estabilidade o mais rápido possível quando um incidente ocorre.

Visibilidade histórica sobre o estado de conformidade pode ser uma ferramenta especialmente poderosa para descobrir um status passado que levou a um problema. Uma organização que foi vítima de um ciber-ataque, por exemplo, pode examinar o seu status de conformidade no momento do ataque para descobrir onde existia vulnerabilidades. Essa capacidade de drill down em detalhes específicos de endpoints em conformidade e fora de conformidade pode ajudar a identificar diferenças críticas e fornecer insights que podem ser usados para trazer endpoints em conformidade e fortalecer a postura geral de segurança da organização.

Os exemplos a seguir mostram como o BigFix pode ser usado para resposta a incidente:

- **Desativando controles ActiveX ou DLLs que estão sendo explorados:** O BigFix pode implementar rapidamente políticas que encerram um controle explorado ou uma biblioteca de vínculo dinâmico (DLL) assim que uma vulnerabilidade for identificada limitando o dano a partir de um ataque potencial mesmo antes que uma correção do fornecedor esteja disponível. Quando um exploit de zero-day é descoberto, a solução pode executar políticas que transformam etapas de correção manuais fornecidas pelo fornecedor em políticas automatizadas, para ajudar a identificar se endpoints são potencialmente vulneráveis e, em seguida, minimizar os problemas.
- **Migrando de um controle técnico para outro:** Substituindo uma solução antivírus em virtude do alto custo ou a ineficácia pode, muitas vezes, ser um desafio. Além disso, há o risco potencial de que endpoints serão expostos durante a migração. O BigFix permite que uma organização remova facilmente e com segurança uma solução em apenas um dia. Ele também ajuda a instalar produtos a partir de um novo fornecedor. Em qualquer operação, a velocidade da solução ajuda a reduzir a janela de vulnerabilidade a ataque.

- **Atualizando rapidamente controles de proteção de endpoint:** O BigFix pode assegurar que clientes de segurança do terminal estejam sempre em execução e que assinaturas de vírus estejam atualizadas. Verificação de ciclo fechado assegura que as atualizações e outras alterações estejam concluídas, incluindo a verificação de Internet para endpoints desconectados a partir da rede. Uma organização também pode usar o BigFix para desativar os serviços por exemplo, fechar portas Telnet abertas que expõem o sistema a vulnerabilidades.
- **Migrando para um novo navegador em massa:** Um exploit de navegador pode expor a organização a risco permitindo que atacantes remotos executem código arbitrário quando os usuários acessarem determinados websites. Com o BigFix, as organizações têm a flexibilidade para mudar para outro navegador e até mesmo grandes infraestruturas podem realizar a migração no dia.
- **Descobrindo e limpando malware que não pode ser removido:** Para combater um ataque de malware, o BigFix pode levantar regras de firewall IPSec para colocar em quarentena sistemas infectados a partir do resto da rede. Permitir comunicações de saída somente para um servidor de correção permite que a equipe de TI construa definições de política que identifiquem qual impacto o vírus está tendo. A equipe de TI também pode examinar outros endpoints para ver se eles demonstram esse comportamento e colocar em quarentena aqueles que o fazem. Assim que uma correção estiver disponível, o BigFix pode assegurar que endpoints estejam desinfetados e permaneçam atualizados.

Componentes chave de solução

Soluções de resposta a incidente de alto desempenho no portfólio do BigFix são:

- Conformidade do IBM BigFix: Fornece contínua aplicação de configuração de segurança de TI e correção, com os melhores recursos de análise de dados para coletar e arquivar resultados de verificação de segurança automatizados. Fornece uma variedade de visualizações sobre o status de conformidade e risco à segurança, a partir de visualizações de rolagem de agregação de alto nível até a identificação de pontos de acesso, para drill-downs obtendo informações detalhadas.
- Proteção do IBM BigFix: Detecta e remove malware antes que ele possa explorar vulnerabilidade. Informações de referências cruzadas com um banco de dados grande, baseado em nuvem e continuamente atualizado. Verifica arquivos e URLs com relação a esse banco de dados para potencial malicioso em tempo real e entrega proteção anti-malware a endpoints do Mac e Windows, conforme necessário.

Conclusão

O IBM BigFix ajuda as organizações a manterem a conformidade contínua para evitar ameaças, assim como recursos de análise de dados para fortalecer a infraestrutura com relação a ataques. A sua tecnologia de agente inteligente fornece várias camadas de segurança e ajuda a descobrir comportamento anômalo em tempo real. Os administradores podem direcionar esses sistemas que são afetados com ações específicas customizadas para um tipo exato de configuração de endpoint ou tipo de usuário. O BigFix traz visibilidade penetrante, em tempo real, correção automatizada e escalabilidade global para o processo de resposta a incidente. Isso permite que as organizações protejam endpoints não importa onde eles estejam localizados, como eles estão conectados ou se eles estão ligados ou desligados da rede, enquanto minimiza o impacto de exploits à rede, a endpoints e a usuários finais.

Para obter mais informações

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

Declaração de Práticas de Boa Segurança: A segurança do sistema de TI envolve sistemas de proteção e informações através de prevenção, detecção e resposta a acesso incorreto de dentro ou de fora de sua empresa. Acesso incorreto pode resultar em informações sendo alteradas, destruídas, desapropriadas ou de uso impróprio ou pode resultar em dano ou uso impróprio de seus sistemas, incluindo para uso em ataques em outros. Nenhum sistema de TI ou produto deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança pode ser completamente efetivo na prevenção de uso impróprio ou acesso. Sistemas, produtos e serviços IBM são projetados para serem parte de uma abordagem de segurança abrangente, legal, que envolverá necessariamente procedimentos operacionais adicionais e podem requerer que outros sistemas, produtos ou serviços sejam mais efetivos. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS SEJAM IMUNES, OU TORNARÃO A SUA EMPRESA IMUNE DE, A CONDUTA MALICIOSA OU ILEGAL DE QUALQUER PARTE.

IBM Security
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América em
Julho de 2015

WGW03131-BRPT-00