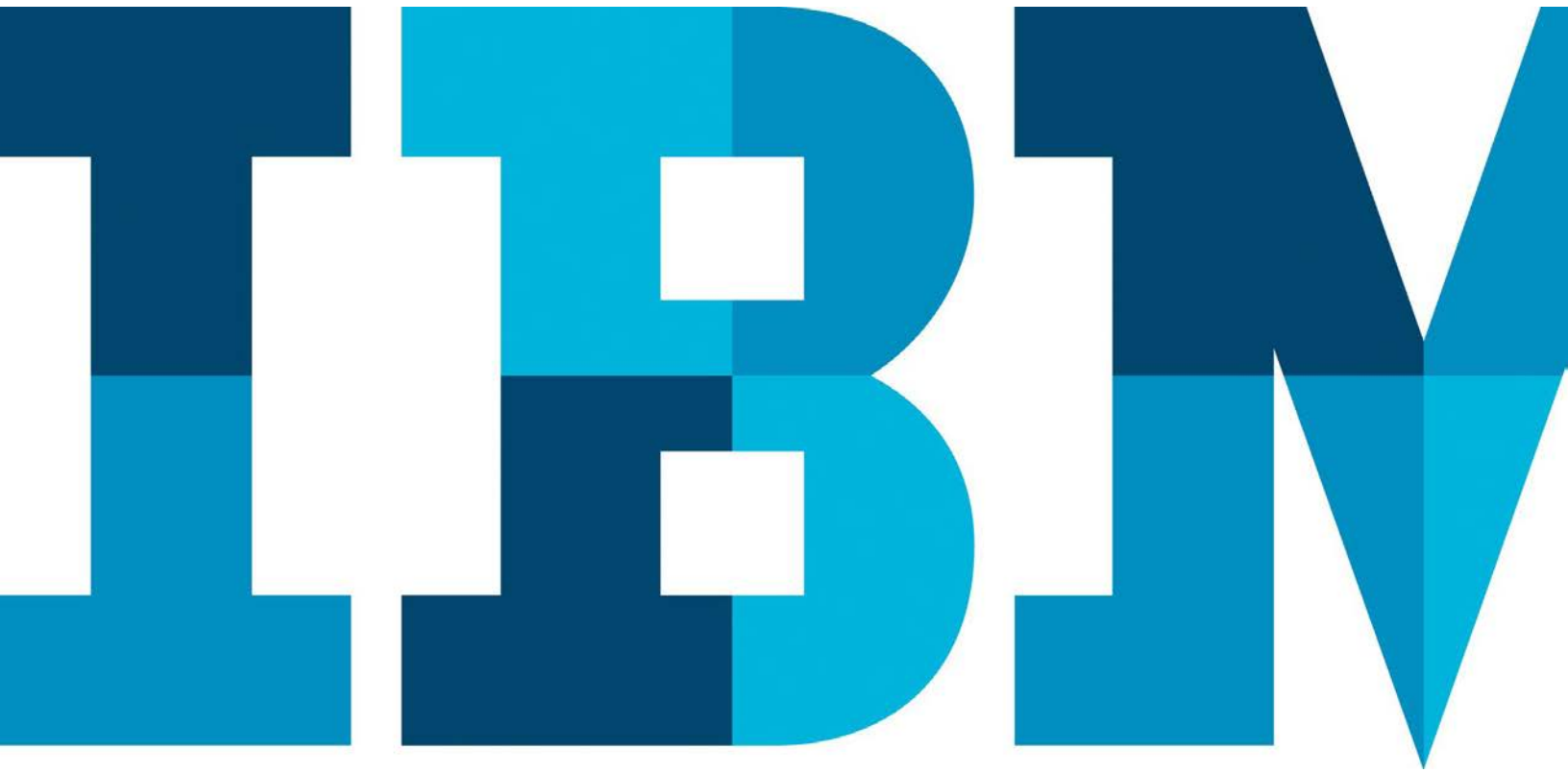
Fevereiro de 2017

Transformando a segurança do endpoint: Caminhando muito além da detecção de ataques

Feche o ciclo através de integração da prevenção, detecção, investigação e resposta



IBM

Introdução

Enquanto os ataques cibernéticos parecem ter êxito à vontade, os endpoints continuam sendo o vetor de ataque mais vulnerável e favorável, categorizado como a barreira mais fraca para a entrada de cibercriminosos. Os endpoints exigem uma abordagem contínua e multifacetada para serem protegidos, tanto de forma proativa, para reduzir sua superfície de ataque, quanto reativa, para conter e corrigir ataques detectados.

A indústria da segurança respondeu oferecendo soluções destinadas a identificar e reagir ao malware e ao comportamento malicioso. No entanto, não importa quão boas sejam essas ferramentas, elas sofrem de diversas fraquezas cruciais. As abordagens que se concentram, principalmente na detecção, normalmente abordam apenas parte de um problema maior enfrentado por qualquer empresa. A segurança aprofundada exige que uma organização não só detecte ameaças, mas também avance além da detecção, para entender a postura de segurança total da empresa e, assim, agir de forma decisiva para desfazer o dano de um ataque e evitar que ataques semelhantes ocorram em toda a empresa.

O mito do dia zero

Enquanto muitas organizações se concentram na preparação para um ataque de dia zero, de acordo com um relatório recente da National Security Administration (NSA – Agência de Segurança Nacional), nenhum ataque de dia zero esteve envolvido em uma violação de cibersegurança de alto perfil no período de 24 meses, que terminou em setembro de 2016.[1] Como explicado por Curtis Dukes, vice-gerente nacional de sistemas de segurança da NSA: “O problema fundamental que enfrentamos em cada um desses incidentes foi a falta de higiene cibernética.”.[1]

A maioria dos incidentes foi resultado de técnicas de ataque relativamente simples: métodos comuns como "spear-phishing", "water-holing" e infecção por drive USB. Eles simplesmente se aproveitaram de vulnerabilidades bem conhecidas, que continuam frequentemente presentes devido à falta de reparação, ao monitoramento e ao gerenciamento precário de endpoints. Por que os ataques de dia zero são raramente empregados? Eles são muito difíceis de serem desenvolvidos, tornando-os relativamente caros de se usar, principalmente porque a janela de oportunidade de uma exploração é pequena e, uma vez descoberta, não pode ser usada sem alterações.

Em que falham as soluções convencionais

Falta de visibilidade

A visibilidade incompleta do status do endpoint fornece pouco contexto para a detecção

Complexidade das investigações

Dados e habilidades limitados inibem a investigação precisa e a tomada de decisão

Correção ineficaz

Diferentes ferramentas e equipes reduzem sua habilidade para defender e responder com eficácia

Quando as soluções são inadequadas, as organizações não apenas permitem a entrada de agressores, mas também falham em detectar ataques no contexto e falham em responder com eficácia.

Em outras palavras, se os métodos mais fáceis funcionam, os criminosos os utilizam. É de responsabilidade das organizações de segurança e de TI bloquear esses métodos mais fáceis, forçando criminosos a utilizarem ataques de dia zero e, além disso, se prepararem para detectar e responder quando eles assim o fizerem.

Os desafios da segurança do endpoint

Poucas empresas têm o orçamento, o pessoal e os conhecimentos necessários para proteger cada centímetro quadrado da organização, incluindo todos os endpoints, o tempo todo. Porém, é exatamente isso que suas equipes de segurança estão encarregadas de fazer. No processo de tentar o que é aparentemente impossível, muitas organizações com uma abordagem exclusivamente de segurança enfrentam desafios importantes:

- **Visibilidade insuficiente:** Quando as soluções geralmente se concentram na detecção e contenção, na maioria das vezes, elas não têm contexto suficiente em relação ao estado atual dos endpoints que protegem. Elas podem ter visibilidade limitada sobre como os endpoints são configurados, qual o software instalado e como ele está sendo usado. Mesmo as organizações com melhor visibilidade sobre os endpoints de outras ferramentas podem ficar sobrecarregadas com os dados que estão coletando, deixando-as incapazes de correlacionar seus dados com as atividades detectadas, potencialmente maliciosas, para formar uma base para a fase de investigação, que é fundamental para o desenvolvimento de um plano de resposta.
- **Complexidade das investigações:** Como a detecção é apenas o início do processo de resposta, é fundamental ter uma imagem histórica tão clara quanto possível sobre o ambiente e a atividade que está acontecendo. Assim, a investigação precisa determinar a veracidade e o alcance do ataque, fazendo perguntas como: Isto é realmente um ataque? Qual é a causa raiz? Quantos dispositivos estão afetados? Quantos dispositivos podem ser afetados? Com base nas respostas que a investigação retorna, é possível decidir sobre as etapas necessárias para conter e, em seguida, corrigir o problema. Com uma equipe de operações de segurança sobrecarregada, muitas vezes pequena, visibilidade limitada sobre o ambiente e tempo insuficiente para absorver todas as últimas informações de inteligência de ameaças, as organizações podem ter dificuldades consideráveis para chegar a conclusões apropriadas.
- **Correção ineficaz:** Embora as equipes de segurança e seus portfólios de ferramentas tenham crescido naturalmente ao longo do tempo, eles não cresceram necessariamente de maneira que se complementassem. O resultado foi o isolamento de equipes e ferramentas. Ao adicionar novas funções e novas ferramentas para atender às necessidades específicas, à medida que elas surgem, as organizações podem encontrar-se pagando, instalando, configurando, gerenciando, corrigindo e atualizando dezenas de soluções não integradas, que oferecem visões limitadas do ambiente. Um cliente IBM estava usando 85 ferramentas de segurança diferentes de 45 fornecedores diferentes. Essas infraestruturas misturadas não são apenas caras, mas diante de investigações complexas, dificultam as investigações e as conclusões precisas de incidentes. Qualquer ferramenta específica nesse todo fornece apenas uma pequena porção da imagem total.

  Como a NSA descobriu, a verificação precária do endpoint, e não o temido ataque de dia zero, foi a principal causa de todos os ataques de alto nível nos últimos dois anos em que ela estudou. Em muitos casos, a organização havia deixado as portas e as janelas abertas, negligenciando a correção de vulnerabilidades, por exemplo, convidando o método mais simples de intrusão. Uma vez dentro de uma rede, os agressores podem permanecer ali durante meses. Na verdade, ataques maliciosos e criminosos geralmente levam até 229 dias para serem identificados.[2]

  E uma pesquisa recente sobre violações de dados revelou que mais de 99,9% das vulnerabilidades exploradas haviam sido comprometidas por mais de um ano depois que a Vulnerabilidade e Exposição Comum (CVE) associada foi publicada.[3] Com diferentes ferramentas, é difícil reforçar de maneira proativa os endpoints contra ameaças potenciais ou investigar toda a empresa para encontrar o malware persistente. Isso requer uma verificação abrangente do endpoint, o que inclui monitoramento de atividades, gerenciamento de correção e configuração, imposição de controles de segurança e detecção avançada de malwares.

Todos esses desafios levam a uma estratégia de defesa fragmentada, que é incapaz de fornecer a visibilidade e a coordenação necessárias para prevenir, detectar e responder efetivamente aos ataques direcionados da atualidade.

Uma nova abordagem para a proteção de endpoint

À medida que cresce a confiança das organizações em TI para gerar valor comercial, também crescem as ameaças à infraestrutura de TI. Na verdade, 387 novas ameaças de malware são identificadas a cada minuto.[4] Para ficar à frente dessas ameaças, é preciso uma nova abordagem em relação à segurança do endpoint: uma solução integrada e adaptável que fecha o ciclo de segurança com as principais melhores práticas e recursos de solução.

Uma abordagem eficaz sobre a segurança do endpoint dá suporte à visibilidade clara da infraestrutura e das atividades, à completa compreensão e resposta necessárias aos ataques, bem como às ações precisas para conter e corrigir ataques. Ela permite que uma organização:

- Corrija continuamente as vulnerabilidades que podem ser usadas para estabelecer uma base em seu ambiente, reduzindo a superfície de ataque efetiva.
- Analise e registre continuamente a atividade do endpoint para ajudar a detectar atividades relacionadas a qualquer tipo de ataque (incluindo exploração de vulnerabilidade conhecida, ataques de dia zero ou intrusão não relacionada a malware).
- Reduza tanto o tempo necessário para detectar uma violação quanto o "tempo de permanência" que um invasor pode permanecer na infraestrutura depois de ganhar acesso.
- Aprimore ferramentas de detecção de endpoint baseadas em assinaturas, com sistemas baseados em comportamento que usam heurísticas para correlacionar múltiplos eventos que são indicativos de comportamento evasivo.
- Utilize um agente de modo de kernel para proporcionar visibilidade completa sobre a atividade do endpoint, em vez de um agente de modo de usuário, que pode não detectar um malware mais sofisticado e evasivo.
- Dê suporte a recursos inteligentes de investigação e resposta, com ferramentas para avaliar o alcance de um ataque, priorizar a ameaça e fornecer a capacidade de corrigir imediatamente.
- Melhore e automatize os esforços de conformidade, mapeando a imposição contínua de políticas e controles de endpoint diretamente a uma ampla gama de padrões e regulamentos do setor, facilitando a preparação para auditoria como parte de um ambiente geral de segurança.
- Forneça visibilidade contínua e completa em todos os endpoints que possam ser compartilhados por várias equipes, facilitando a colaboração entre operações de TI e operações de segurança.
- Permita a implantação rápida e forneça valor tangível em algumas horas ou dias, e não semanas ou meses.

Proteção inteligente de endpoint

O IBM® BigFix® representa uma nova categoria de proteção inteligente de endpoint, permitindo uma estratégia de segurança de endpoint abrangente que implementa respostas diretas e medidas de segurança proativas por meio da mesma plataforma.

A adição do módulo IBM BigFix Detect é uma resposta à realidade do horizonte de ameaça atual, em que intrusos podem obter acesso a praticamente qualquer empresa, seja por meio de um ataque de um intruso mal-intencionado ou do erro inocente de um usuário autorizado. Aos recursos proativos estabelecidos da plataforma BigFix, com sua visibilidade sobre a configuração e as atividades do endpoint, que ajudam a organização a gerenciar a prontidão, antes que um ataque ocorra, o BigFix Detect adiciona recursos de resposta: a capacidade de lidar com ataques e malwares depois que eles ocorrem.

O BigFix Detect fornece três recursos principais projetados para fechar o ciclo da segurança do endpoint. A proteção contínua, a detecção inteligente e a resposta orientada são combinadas com a visibilidade em tempo real sobre a atividade e o status de segurança do endpoint, para que as empresas possam ver claramente, entender completamente e atuar com precisão para enfrentar as ameaças.

Proteção contínua

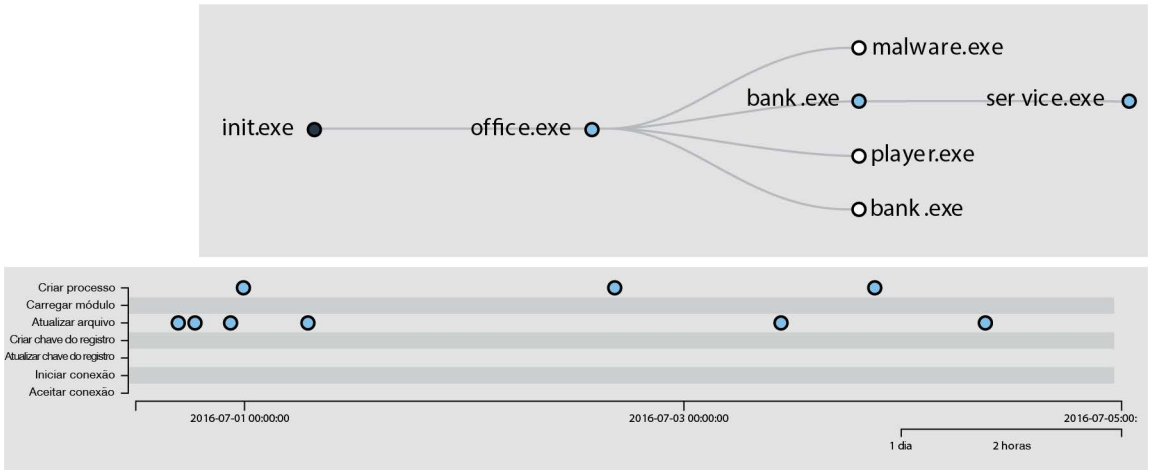
A proteção contínua permite que as organizações evitem ameaças conhecidas e emergentes. A proteção contínua, começando pela detecção de anomalias, é equivalente a manter as portas e as janelas trancadas, forçando os invasores a trabalharem mais para conseguir entrar, como com o uso de ataques de dia zero, que são mais complicados e caros. A proteção contínua permite às empresas:

- Monitorar os controles de segurança continuamente.
- Manter linhas de base padronizadas que sejam relevantes para segurança, conformidade, configuração e correção.
- Lançar as atualizações pré-verificadas de aplicativo do sistema operacional em minutos ou horas e não em dias ou semanas.
- Implantar, monitorar e impor agentes de segurança de terceiros.
- Facilitar a colaboração no gerenciamento de correção e de configuração entre operações de TI e operações de segurança.

Detecção inteligente

A detecção inteligente emprega um agente de modo de kernel que permite que todas as atividades críticas do endpoint sejam coletadas, ao contrário de agentes de modo de usuário, menos eficazes. Em seguida, ela aplica a inteligência de ameaça e padrões comportamentais para detectar ataques, em vez de métodos ineficazes de detecção de malware baseados em assinatura. A detecção inteligente aproveita a inteligência obtida de milhões de endpoints ativos na plataforma BigFix para correlacionar eventos, reconhecer comportamentos maliciosos e analisar a causa raiz, ajudando a acelerar a correção.

Detecção inteligente



A detecção inteligente correlaciona eventos, reconhece comportamento malicioso e analisa a causa raiz, ajudando a acelerar a correção.

Resposta orientada

A resposta orientada com base em contexto de uma ferramenta de consultor confiável baseada em software ajuda a iniciar a investigação de um ataque fundamentada na atividade detectada, incluindo a definição da veracidade, da exposição e do escopo do incidente e, em seguida, fornece sugestões de correção. A resposta orientada aproveita uma enorme biblioteca de sistemas operacionais pré-validados de diversos fornecedores e pacotes de instalação de conteúdo de aplicativos para fornecer opções de correção relevantes em minutos, seja para um endpoint individual, um grupo de endpoints ou para toda a empresa.

Em seguida, a resposta orientada permite uma correção rápida ao criar mensagens IBM Fixlet®, que são as mensagens do BigFix que fornecem instruções aos agentes para realizar uma ação. As mensagens Fixlet podem ser lançadas logo após a determinação da ação corretiva adequada. Suas ações incluem correções, reconfigurações ou colocação dos endpoints afetados em quarentena, ou até mesmo a restauração remota da imagem deles.

Visibilidade em tempo real

A plataforma BigFix fornece visibilidade contínua em tempo real por todo o ciclo de segurança do endpoint, permitindo a descoberta e a auditoria de todos os endpoints, reunindo o inventário de todo o uso e o licenciamento de software e a avaliação contínua da configuração, da segurança, da conformidade e da situação da correção.

Milhares de atributos são coletados continuamente dos endpoints e enviados para um único servidor de gerenciamento por meio de um único agente multiuso. O agente pode ser usado em todos os tipos de endpoints, desde computadores e servidores até caixas eletrônicos e dispositivos de ponto de venda (PDV), incluindo aqueles que executam Microsoft Windows, Microsoft Windows Mobile, UNIX, diferentes distribuições do Linux e o Apple Mac OS, independentemente dos endpoints serem físicos ou virtuais, fixos ou móveis. O agente usa o mínimo de memória, recursos de computação e largura de banda.

Embora a solução ofereça relatórios extensivos de configuração e conformidade, uma ferramenta de consulta ad hoc também permite que os administradores consultem os endpoints e extraiam resultados precisos em segundos.

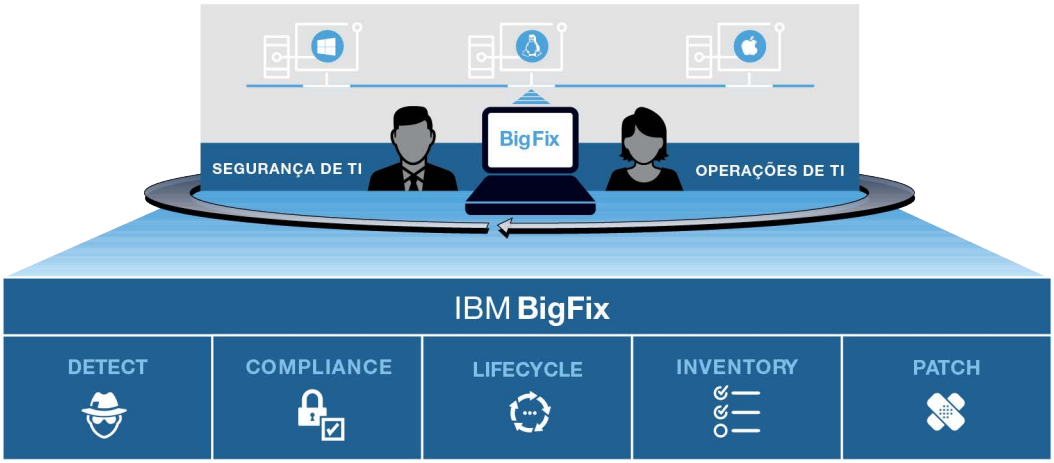
Uma plataforma colaborativa de segurança e gerenciamento de endpoint

Para um setor acostumado a tecnologias múltiplas, fragmentadas e a soluções pontuais, o BigFix oferece uma alternativa atrativa: uma plataforma de console único e agente único que aborda as operações, a segurança e as iniciativas de conformidade em tempo real e em escala global. Um servidor BigFix pode dar suporte a mais de 200 mil endpoints, permitindo que as organizações aproveitem ao máximo seus investimentos em segurança e gerenciamento de sistemas.

A plataforma BigFix é composta de vários componentes integrados:

- **IBM BigFix Detect:** Detecção, investigação baseada em contexto e correção de ameaças ativas focada de maneira precisa, possibilitadas pelo mais novo módulo da plataforma BigFix
- **IBM BigFix Compliance:** Conformidade contínua das políticas de segurança, operacionais e regulatórias
- **IBM BigFix Lifecycle:** Correção, provisionamento e distribuição de software e controle remoto de endpoints
- **IBM BigFix Inventory:** Visibilidade sobre quais softwares estão instalados e como estão sendo usados, ajudando a reduzir custos e a aumentar a conformidade
- **IBM BigFix Patch:** Recursos que compactam os ciclos de correção em minutos ou horas e não mais em dias ou semanas, com uma taxa de sucesso de primeira aplicação de mais de 98%

Plataforma colaborativa de segurança e gerenciamento de endpoint



A plataforma BigFix reúne recursos abrangentes de segurança de endpoint sob uma única cobertura.

Por que a IBM?

No mundo em constante evolução da segurança de TI, pode ser difícil confiar que sua organização está fazendo tudo o que é necessário para prevenir, detectar e responder rápida e adequadamente às ameaças. Para ajudar as organizações a alcançarem esse ponto, o IBM BigFix oferece uma plataforma integrada que combina de forma exclusiva a segurança proativa de endpoint com mecanismos de detecção inteligentes e respostas orientadas baseadas em contexto.

Essa coleção abrangente de recursos permite que as organizações melhorem sua condição de segurança em todas as etapas do ciclo de segurança do endpoint, permitindo que elas mudem os resultados potenciais antes, durante e após um ataque:

- **Preparação em vez de infiltração:** Um programa de segurança sólido e bem embasado permite que uma organização se coloque na melhor posição possível em caso de ataque e se mantenha nessa posição continuamente.
- **Prevenção em vez de exploração:** O gerenciamento de endpoint contínuo e priorizado pode impedir a maioria dos ataques que exploram vulnerabilidades conhecidas para conseguir invadir.
- **Detecção em vez de expansão:** A coleta e a correlação abrangentes de atividades do endpoint aceleram a detecção para evitar que os invasores se movam lateralmente pela rede e explorem outras vulnerabilidades uma vez que tenham obtido acesso.
- **Análise em vez de contrabando de dados:** A análise e a resposta baseadas em contexto podem ser usadas para gerar um Fixlet de correção ou para alertar os administradores sobre atividades maliciosas antes que os dados possam ser contrabandeados.
- **Resposta em vez da execução do ataque:** Os administradores podem avaliar e executar várias opções de correção imediatamente.

Para obter mais informações

Para saber mais sobre o IBM BigFix, visite **ibm.com**/security/bigfix para assistir a um vídeo de demonstração do produto em ação ou contate seu representante IBM ou Parceiro de Negócios IBM para organizar uma prova de conceito para o seu ambiente.

Declaração de boas práticas de segurança: A segurança de sistemas de TI envolve a proteção de sistemas e de informações por meio de prevenção, detecção e resposta ao acesso inadequado de dentro e de fora de sua empresa. O acesso inadequado pode resultar em alteração, destruição, emprego indevido ou uso incorreto de informações, ou pode causar danos ou uso indevido de seus sistemas, inclusive para uso em ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança pode ser completamente efetivo na prevenção do uso ou acesso inadequado. Sistemas, produtos e serviços da IBM são projetados para fazer parte de uma abordagem de segurança legal e abrangente, o que implicará necessariamente em procedimentos operacionais adicionais e poderá exigir que outros sistemas, produtos ou serviços sejam mais eficazes. A IBM NÃO GARANTE QUE QUAISQUER SISTEMAS, PRODUTOS OU SERVIÇOS SEJAM IMUNES, OU TORNARÃO SUA EMPRESA IMUNE À CONDUTA MALICIOSA OU ILEGAL DE QUALQUER OUTRA PARTE.

1 Chris Bing, "NSA: no zero days were used in any high profile breaches over last 24 months," *FedScoop*, 15 de setembro de 2016. http://fedscoop.com/nsa-no-zero-days-were-used-in-any-high-profile-breaches-over-last-24-months

2 "2016 Cost of Data Breach Study: Global Analysis," *Ponemon Institute LLC*, junho de 2016. http://www-03.ibm.com/security/data-breach/

3 "2015 Data Breach Investigations Report," *Verizon Enterprise Solutions*, 2015. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

4 "McAfee Labs Threat Report," *McAfee Labs*, fevereiro de 2015. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América em fevereiro de 2017

WGW03269-BRPT-00