



Benefícios principais

- Suporta seguramente dispositivos BYOD e a propriedade corporativa
 - Gerencia proativamente ameaças móveis em tempo quase real
 - Reduz o risco de vazamento de dados sensíveis de informações corporativas e pessoais
 - Executa ações automatizadas para remediar os riscos de segurança móvel
-

IBM MaaS360 Mobile Threat Management

Detém o malware móvel no iOS e em dispositivos Android

Malware móvel – a próxima grande ameaça de segurança

As organizações estão sendo transformadas em um ritmo sem precedentes com a mobilidade. A tendência Traga o Seu Próprio Dispositivo (BYOD) continua se espalhando na empresa. Os aplicativos móveis estão criando novos e eficientes fluxos de trabalho para os funcionários. O acesso perfeito para dados de trabalho, e-mails e conteúdo está crescendo em paralelo, melhorando os ganhos de produtividade resultantes dessas tendências.

Como resultado da popularidade e da velocidade na qual os dispositivos móveis se tornam uma grande tendência na empresa, os hackers e os ladrões estão preparando dispositivos móveis com malware e criando a próxima grande ameaça de segurança. Dados corporativos são especialmente vulneráveis a aplicativos mal-intencionados e sites maliciosos.

- 138 bilhões de aplicativos foram baixados em 2014.¹
- O malware móvel está crescendo. O código malicioso está infectando mais que 11,6 milhões de dispositivos móveis em qualquer momento.²
- Recentes ataques WireLurker e Masque ameaçam os dispositivos iOS.^{3,4}
- O dano à marca da empresa é composto por perda financeira, com o custo de uma única violação sendo estimado em mais de US\$ 11 milhões.⁵

Os líderes de TI e de segurança precisam de uma solução de segurança moderna e robusta para proativamente detectar, analisar e remediar malware móvel.

Detenha as ameaças móveis na sua empresa

O IBM® MaaS360® Mobile Threat Management oferece um sistema de ponta para proteção contra malware nos dispositivos iOS e Android. Você pode detectar riscos e gerenciar ameaças, antes que comprometam os dados da sua empresa.



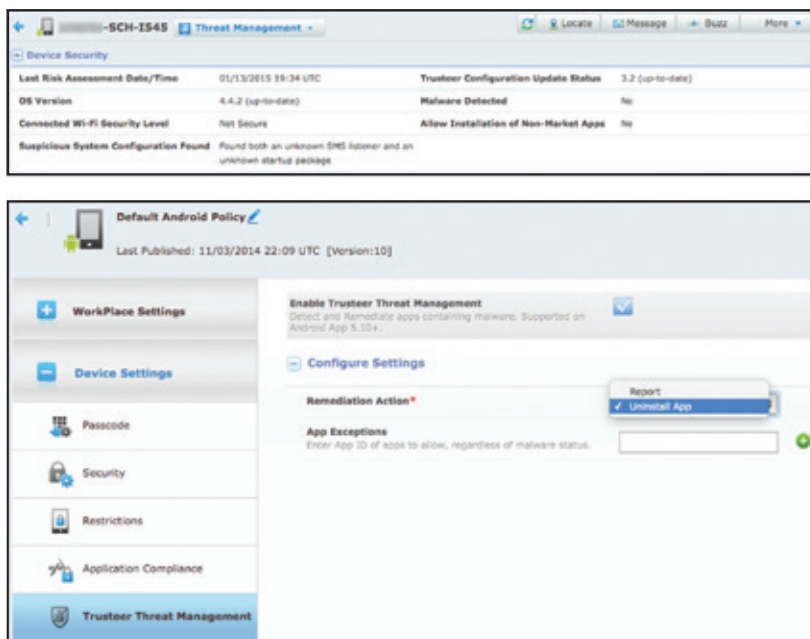


Figura 1: exemplos de dados relatados sobre um dispositivo protegido e as configurações da política no MaaS360 Mobile Threat Management

Através de integração com IBM Trusteer®, usado por centenas de milhões de usuários para se protegerem contra fraude e quebras de dados, o MaaS360 oferece uma nova camada de segurança para o Gerenciamento de Mobilidade Corporativa (EMM).

Não deixe que o malware atrapalhe a transformação móvel da sua organização. Equilibre as iniciativas de produtividade da sua empresa com a segurança oferecida pelo MaaS360.

Detecção de malware móvel e remediação

- Detecta e analisa o iOS e os aplicativos Android com assinaturas de malware e o comportamento malicioso de um banco de dados atualizado continuamente
- Adiciona exceções do aplicativo para personalizar o uso aceitável do aplicativo
- Define controles de política granulares para executar ações apropriadas
- Usa um motor de regras de conformidade quase em tempo real para automatizar a remediação
- Alerta o usuário e as partes responsáveis quando malware for detectado
- Veja os dispositivos comprometidos no Meu Centro de Alertas e eventos de detecção nos painéis Meu Feed de Atividades
- Desinstala aplicativos com malware automaticamente (para dispositivos Android selecionados, tal como Samsung SAFE™)
- Bloqueia o acesso de dispositivos de exclusão de forma seletiva ou completa
- Restringe o uso de soluções do contêiner MaaS360
- Coleta e exhibe os atributos de ameaça ao dispositivo, inclusive:
 - Malware detectado
 - Configurações suspeitas de sistema encontradas, tais como pacote de inicialização ou auditoria de SMS desconhecido
 - Conexão para um ponto de acesso de Wi-Fi inseguro
 - Instalação de aplicativos que não estão no mercado permitida
 - Versão do sistema operacional
- Revise o histórico de auditoria de eventos de detecção de malware

Detecção de desbloqueados e enraizados suplementares

- Detecta dispositivos móveis comprometidos ou vulneráveis
- Protege contra iOS desbloqueado e dispositivos Android enraizados que podem oferecer aos atacantes privilégios adicionais sobre os sistemas operacionais
- Descobre usuários ocultos e ativa técnicas de ocultação que tentam mascarar a detecção de dispositivos desbloqueados e enraizados
- Usa a lógica de detecção atualizada no ar sem que as atualizações de aplicativo sejam mais responsivas para hackers que se movem rápido
- Define políticas de segurança e regras de conformidade para automatizar a remediação
- Bloqueia o acesso de dispositivos de exclusão de forma seletiva ou completa

Motor de Risco Móvel IBM Security Trusteer

- Oferece camadas de proteção e inteligência de cibercrime para prevenção adaptativa de malware
- Detecta rapidamente e se adapta aos comportamentos do último ataque de tal forma que o malware não tenha virtualmente nenhuma oportunidade de cometer fraude
- Executa uma avaliação de risco móvel em tempo quase real baseada em fatores de risco do aplicativo e dispositivo
- Atualiza-se continuamente para oferecer as últimas verificações de malware, fuga e raiz

Para saber mais sobre as soluções de prevenção de fraude da IBM Security, contate o seu representante da IBM ou Parceiro de Negócio da IBM, ou acesse o seguinte site: ibm.com/security.

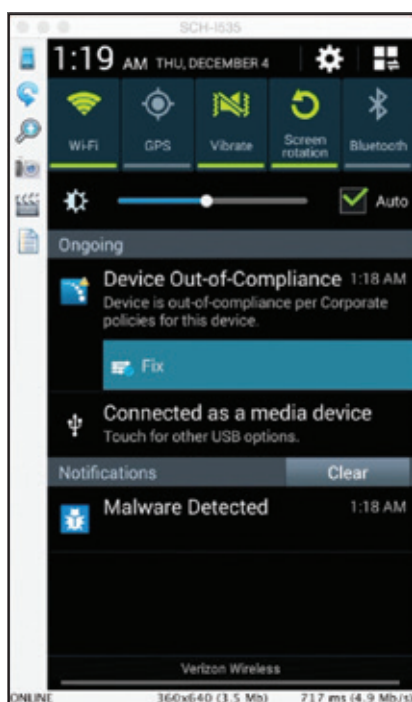


Figura 2: exemplo de notificação de malware em dispositivo



© Copyright IBM Corporation 2016

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
Janeiro de 2016

IBM, o logotipo IBM, ibm.com e X-Force são marcas comerciais da International Business Machines Corp., registradas em muitas jurisdições do mundo. BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® e dispositivo, MaaS360 PRO™, MCM360™, MDM360™, MI360®, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360® e We do IT in the Cloud.™ e dispositivo são marcas comerciais ou marcas comerciais registradas da Fiberlink Communications Corporation, uma empresa da IBM. Os nomes de outros produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atualizada das marcas registradas da IBM está disponível na web em “Informações de direitos autorais e marcas comerciais” em ibm.com/legal/copytrade.shtml

Apple, iPhone, iPad, iPod touch e iOS são marcas comerciais registradas ou marcas comerciais da Apple Inc., nos Estados Unidos e em outros países.

Este documento é atual na data inicial de publicação e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países nos quais a IBM opera.

Os dados de desempenho e os exemplos de clientes citados estão presentes apenas para propósitos ilustrativos. Os resultados reais de desempenho podem variar dependendo das configurações específicas e das condições operacionais. É de responsabilidade do usuário avaliar e verificar a operação de qualquer outro produto ou programa com o produto ou programas da IBM.

AS INFORMAÇÕES NESTE DOCUMENTO SÃO FORNECIDAS “COMO ESTÃO”, SEM QUALQUER GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUSIVE SEM QUALQUER GARANTIA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM PROPÓSITO PARTICULAR E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO VIOLAÇÃO. Produtos da IBM têm garantia de acordo com os termos e condições dos acordos sob os quais são fornecidos.

O cliente é responsável por garantir a conformidade para com as leis e regulamentos a ele aplicáveis. A IBM não fornece nenhum aconselhamento jurídico ou representa ou garante que seus serviços ou produtos garantirão que o cliente esteja em conformidade com qualquer lei ou regulamento.

As declarações referentes às futuras direções e intenções da IBM estão sujeitas a alteração ou retratação sem notificação e representam apenas metas e objetivos.

Declaração de boas práticas de segurança: A segurança de sistema de TI envolve proteger sistemas e informações através da prevenção, detecção e resposta a acesso indevido de dentro e fora da sua empresa. O acesso indevido pode resultar em informações sendo alteradas, destruídas ou desapropriadas ou pode resultar em dano ou uso indevido dos seus sistemas, inclusive ataque aos outros. Nenhum sistema ou produto de TI deveria ser considerado completamente seguro e nenhum único produto ou medida de segurança pode ser completamente efetivo para evitar o acesso indevido. Os sistemas e produtos da IBM são projetados para fazerem parte de uma abordagem de segurança abrangente, que necessariamente envolverão procedimentos operacionais adicionais, e podem exigir outros sistemas, produtos ou serviços para ser mais efetivo. A IBM não garante que os sistemas e produtos sejam imunes contra conduta maliciosa ou ilegal de nenhuma parte.

- 1 Relatório anual da Arxan: “*State of Mobile App Security Reveals an Increase in App Hacks for Top 100 Mobile Apps*”, Novembro de 2014, Arxan Technologies, Inc., <https://www.arxan.com/2014/11/17/arxans-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/>
- 2 Kindsight Security Labs Malware Report – Q4 2013, Alcatel-Lucent, <http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf>
- 3 Xiao, Claud, WireLurker: A New Era in OS X and iOS Malware, Blog post on Palo Alto Networks; 5 de novembro de 2014, <http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/>
- 4 Zue, Hui, Wei, Tao and Zhang, Yulong; Masque Attack: All Your iOS Apps Belong to Us, 10 de novembro de 2014, <https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html>
- 5 2013 Cost of Cyber Crime Study: United States, Sponsored by HP Enterprise Security, Ponemon Institute, October 2014, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf



Por favor, recicle