IBM MaaS360 Secure Mobile Browser

Desbloqueie os dados da sua empresa e reduza a vulnerabilidade dos sites arriscados

Benefícios principais

- Implemente um navegador web robusto que proteja os dados corporativos e aumente a produtividade para iOS, Android e dispositivos Windows Phone
- Use uma plataforma de gerenciamento centralizada que ofereça aos seus funcionários acesso protegido para sites de intranet corporativos e redes sem VPN requerido
- Controle a experiência de internet móvel através de políticas de segurança granulares
- Evite ataques e malware de sites maliciosos
- Supere os seus desafios web móveis que cobrem uma ampla gama de necessidades de negócio

Controle o acesso para web em dispositivos móveis

O IBM® MaaS360® Secure Mobile Browser dá aos seus funcionários acesso protegido para sites de intranet corporativa e redes sem VPN requerido.

Você também pode reduzir a vulnerabilidade que os seus dispositivos móveis têm para sites arriscados que podem conter malware, violem as políticas de Recursos Humanos (RH) ou simplesmente desperdicem o precioso tempo dos seus usuários.

Com o MaaS360 Secure Mobile Browser, as organizações podem especificar categorias de conteúdo que querem evitar que usuários acessem, incluindo sites de redes sociais, sites de download e sites explícitos. Ele tem mais de 60 categorias de critérios de filtragem, com milhões de URLs categorizadas.

Específicas URLs podem ser definidas para filtrar acesso a sites apropriados. Através de políticas e listas negras do IBM® MaaS360® Device Management, navegadores nativos e de terceiros podem ser desabilitados.

O MaaS360 Secure Mobile Browser pode enviar e-mails para os administradores em tempo quase real, alertando-os de tentativas de acessar esses sites.

Com o MaaS360 Secure Mobile Browser você tem:

- Uma plataforma de gerenciamento baseada na nuvem e centralizada
- Uma criação de política fácil de usar e atribuição remota sobre o ar (OTA)
- Acesso protegido a sites de intranet corporativos e rede sem VPN de dispositivo
- Mobilização de SharePoint, JIRA, internal wikis, sistemas ERP legados e muito mais
- Proteção contínua através de interceptação de tráfego de navegador
- Restrição de URLs por categoria e permissão de acesso a URLs específicas
- Bloqueio de malware conhecido e sites maliciosos usando um moto de varredura e banco de dados de reputação
- Desabilitação de cookies, impressão, downloads de arquivos e copiar e colar
- Bloqueio personalizável, notificação em tempo quase real, exceção e opções de relatórios

Figura 1: Exemplo do MaaS360 Secure Mobile Browser em vários dispositivos móveis

Controle a experiência de internet móvel

O MaaS360 Secure Mobile Browser é um navegador web robusto para smartphones e tablets. Ele tem uma interface de usuário intuitiva que inclui navegação por abas, bookmarks, busca, compartilhamento e recursos de histórico. Há muitas formas de implementar o MaaS360 Secure Mobile Browser na sua organização para reduzir a vulnerabilidade dos dispositivos móveis dos seus usuários, evitar violações a políticas de RH ou focar a atenção do usuário.

- **Dispositivos de provedor de tratamento de saúde compartilhados:** Salvaguarde os registros de pacientes e otimize a utilização de dispositivos compartilhados pelos seus trabalhadores da área de saúde focando na referência médica e nos sites de ponto de tratamento, e oferecendo acesso a sites de intranet sem precisar de uma conexão VPN de dispositivo.
- **Dispositivos de ponto de venda (POS) de varejo dedicados:** Melhore a produtividade da sua equipe de varejo e proteja os dados no dispositivo bloqueando os seus dispositivos POS para sites específicos para verificação, busca de inventário ou disponibilidade de armazenamento na web.
- **Dispositivos de ensino compartilhado:** Foque a atenção do estudante restringindo o acesso a sites explícitos para dispositivos de aprendizagem compartilhados na sala de aula, uma prioridade para instituições educacionais para estar em conformidade com as regulações da Lei de Proteção da Internet das Crianças (CIPA).
- **Dispositivos de recepção de hospitalidade:** Aumente a eficiência da sua equipe de hospitalidade limitando os dispositivos para check-in e check-out, vendo amenidades de instalações e acessando o clima ou o tráfego locais.
- **Dispositivos de demonstração de evento:** Potencialize a utilidade da sua equipe de demonstração permitindo acesso a apenas alguns sites selecionados no seu quiosque.

Definições de configuração de navegador

- Configure como o navegador padrão
- Aplique as políticas de segurança de contêiner do MaaS360
- Desabilite cookies e downloads de arquivos
- Restrinja a cópia, colagem e impressão
- Habilite o modo de quiosque do navegador
- Defina uma página inicial padrão e personalize bookmarks

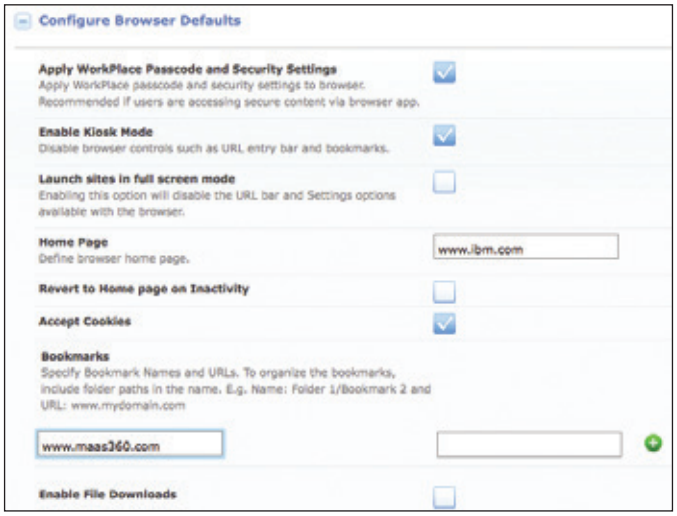

Figura 2: Exemplo de configurações de navegador no console MaaS360

Configurações de filtro de site

- Selecione categorias de URL para permitir, bloquear e rastrear
- Escolha a partir de mais de 60 categorias com milhões de URLs
- Permita exceções baseadas no nome do domínio ou URL
- Sites específicos de lista negra

Figura 3: Exemplo de configurações de filtro de categoria de site no portal

Configurações de notificação de usuário e administração

- Envie texto personalizado ou notificações de HTML para usuários quando tentarem acessar uma URL proibida bloqueada
- Redirecione os usuários a uma URL específica quando políticas forem violadas
- Envie uma notificação para a sua administração quando um usuário for bloqueado
- Defina quantas vezes um usuário pode ser bloqueado antes que a notificação da administração seja enviada

Figura 4: Exemplo de uma notificação de usuário no navegador quando um site está bloqueado

Relatórios de empresa e específicos de dispositivo

- Veja sumário, relatórios gráficos de categoria e domínio bloqueados e histórico rastreado
- Acesse relatórios detalhados de bloqueio de dispositivo específico e histórico de domínio rastreado

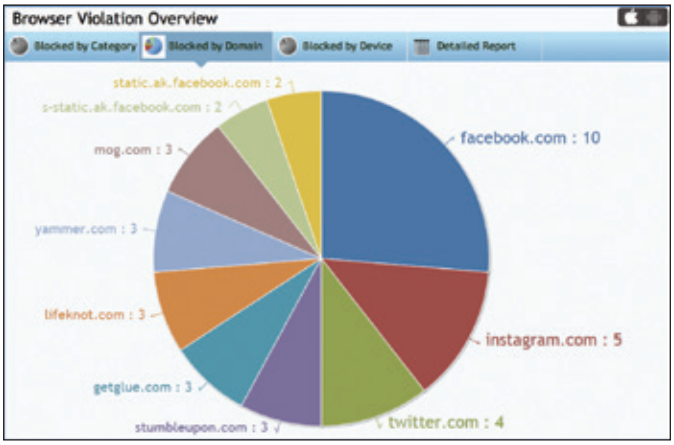

Figura 5: Exemplo de relatório de violações de navegador de dispositivo

Segurança web proativa

O MaaS360 Secure Mobile Browser protege os dados e aumenta a produtividade controlando o acesso aos sites públicos e aos sites de intranet corporativos para dispositivos iOS e Android.

Ele restringe ou permite que os usuários acessem sites baseado nas categorias que você especificar, incluindo:

- Propagandas e popups
- Anonimizadores
- Botnets
- Bate-papo
- Atividade criminal
- Encontros e pessoais
- Sites de downloads
- Entretenimento
- Explícito
- Fóruns e newsgroups
- Apostas
- Jogos
- Hacking
- Compartilhamento de imagens
- Mensagens instantâneas
- Malware
- Notícias
- Par a par
- Phishing e fraude
- Compras
- Redes sociais
- Esportes
- Mídia de transmissão e downloads
- E mais

Desfrute da facilidade de gerenciamento:

- Estrutura de criação de política flexível
- Atribuição de política personalizável
- Integração com o MaaS360 Mobile Device Management para controle otimizado (opcional)

Para saber mais sobre o IBM MaaS360 e começar um teste grátis de 30 dias, acesse www.ibm.com/maas360

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
Fevereiro de 2016

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.

Por favor, recicle

WGD03064-BRPT-01