IBM MaaS360 Secure Mobile Mail

Controle os dispositivos móveis e de e-mail da empresa

Benefícios principais

- Apoie BYOD de forma segura
- Separar os dados pessoais dos corporativos
- Reduza o risco de vazamento de dados sensíveis
- Use o cadastro único para autenticação
- Possibilite verificações de conformidade online e offline
- Apague o contêiner de e-mails, perfis corporativos, ou todo o dispositivo
- Ofereça uma interface de usuário simples e intuitiva que não retardará os seus funcionários
- O MaaS360 não tem acesso a dados de e-mail confidenciais
- Não está alinhado com dados de e-mail sem riscos de desempenho ou interrupção

Forneça acesso protegido ao e-mail corporativo

O IBM® MaaS360® Secure Mobile Mail oferece um aplicativo de produtividade de escritório protegido com e-mail, calendário e contatos para permitir que os funcionários colaborem de forma segura com colegas enquanto preserva a experiência móvel nos seus dispositivos pessoais.

Como um componente fundamental do IBM® MaaS360® Productivity Suite, ele trata de preocupações principais de riscos de perda de dados.

Através da autenticação e autorização, apenas os usuários aprovados e válidos podem acessar e-mails e dados sensíveis. Com políticas para controlar o fluxo de dados, você pode restringir o compartilhamento por usuários, encaminhamento de anexos e cópia e colagem. Dispositivos que forem perdidos, roubados ou comprometidos podem ser seletivamente apagados para remover o contêiner de e-mail protegido, todos os anexos e perfis.

Escolha a abordagem certa para salvaguardar o e-mail

Outras soluções protegem o e-mail interceptando o fluxo de e-mail, removendo anexo e carregando-os num aplicativo separado. Isso normalmente leva a experiências de usuário deslocadas entre o cliente de e-mail nativo e os aplicativos independentes que podem apenas fornecer a visualização de documentos.

O MaaS360 Secure Mobile Mail funciona perfeitamente dentro do MaaS360 Productivity Suite para gerenciar todos os e-mails, calendários, contatos, aplicativos, documentos e a web de um local de trabalho isolado nos seus dispositivos móveis.

Os usuários podem permanecer produtivos com uma experiência de usuário consistente desde o tratamento de e-mails até a visualização, edição e compartilhamento de documentos.

Aplicativo Gerente Robusto de Informações Pessoais (PIM)

- Salvaguarde e-mail, calendário e contatos
- Forneça autenticação e bloqueie acesso de e-mail não autorizado
- Controle e-mails e anexos no contêiner
- Veja anexos diretamente no aplicativo
- Não apenas veja, mas crie, edite, salve e compartilhe conteúdo de forma segura no IBM® MaaS360® Content Suite
- Trabalhe com tipos de arquivos comuns, inclusive Word, Excel, PowerPoint, formatos de texto e PDF

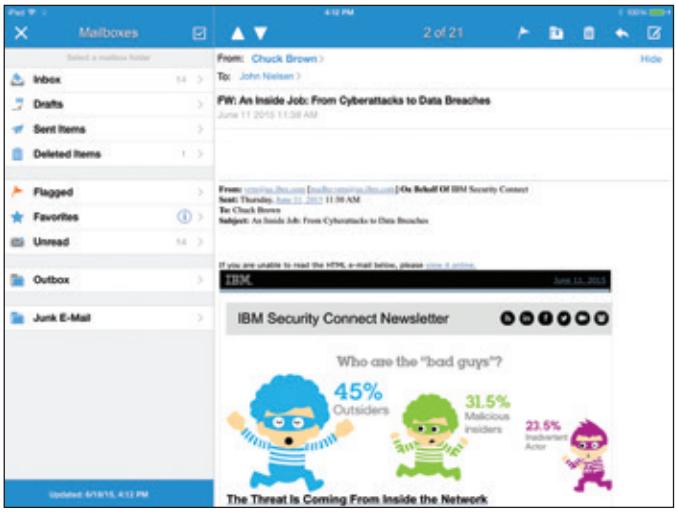

Figura 1: Exemplo de contêiner, caixa de entrada e um e-mail, conforme podem aparecer em um dispositivo

Forte prevenção de perda de dados

- Controle onde os arquivos podem ser copiados ou movidos
- Restrinja o encaminhamento e o movimento para outros aplicativos
- Desabilite a cópia, colagem e captura de tela
- Proteja não apenas os anexos do e-mail, mas o texto do e-mail também
- Force as verificações de conformidade de dispositivos
- Apague seletivamente o contêiner e os anexos, mesmo fora do e-mail

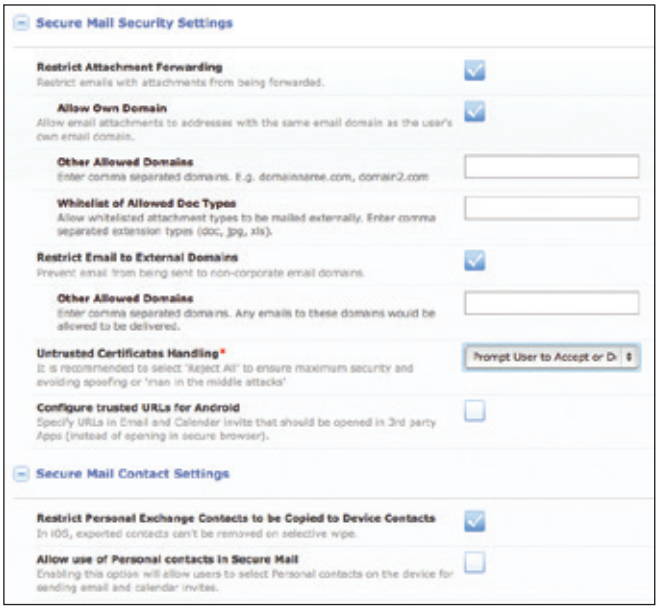

Figura 2: Exemplo de configurações de segurança para o MaaS360 Secure Mobile Mail

Fácil integração com a sua infraestrutura

- Baseado na infraestrutura Exchange ActiveSync existente
- Use o Diretório Ativo para simplificar a autenticação e autorização
- Suporte para e-mail na nuvem, como Office 365 e Gmail
- Integre uma segurança de e-mail robusta no nível de dispositivo que não esteja alinhado com dados do e-mail
- O MaaS360 não tem acesso a dados de e-mail confidenciais
- Sem riscos adicionais de desempenho ou interrupção

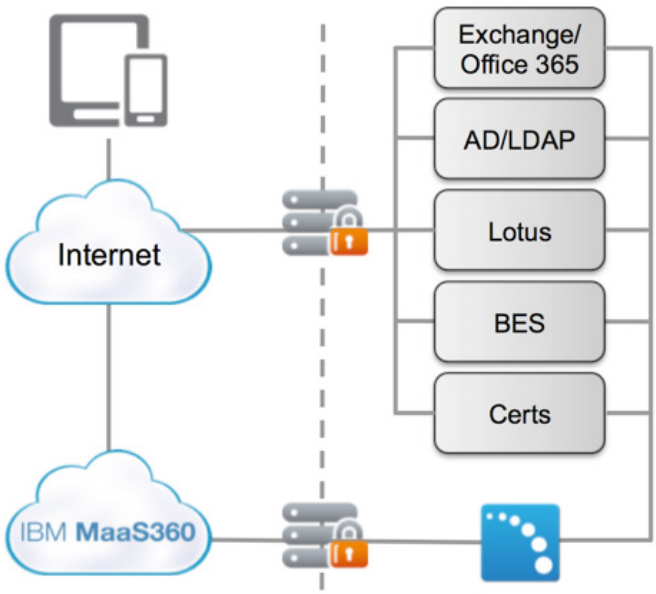

Figura 3: Visão geral simples de integração do MaaS360 com sistemas de TI

Contínuos alertas e relatórios de segurança

- Configure ações de execução de conformidade automatizadas
- Receba alertas automáticos de violações de conformidade
- Tome ação direta através de intervenção de automação ou manual
- Veja relatórios gráficos do histórico de segurança e conformidade

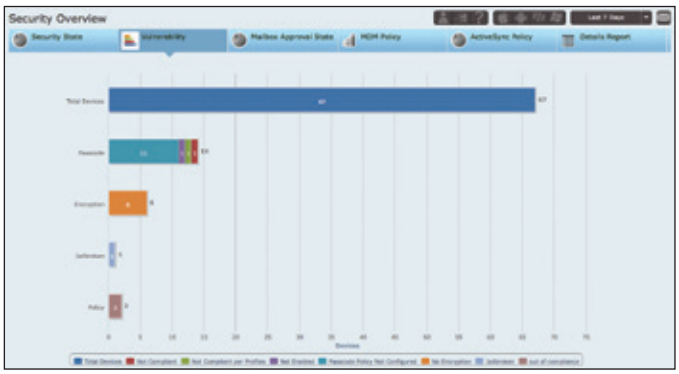

Figura 4: Exemplo de relatórios de segurança do MaaS360

Contenha o e-mail corporativo

O e-mail ainda é um dos aplicativos mais importantes em smartphones e tablets, mas pode se tornar um desafio para a segurança móvel da sua organização e para as políticas de conformidade também.

O MaaS360 Secure Mobile Mail salvaguarda o e-mail de negócio e os anexos para evitar que dados corporativos vazem, enquanto mantém os funcionários produtivos e em ação.

Principais recursos

- Proteja e-mails (tanto textos quanto anexos), calendários e contatos no seu contêiner
- Possibilite autenticação e bloqueie o acesso de e-mail não autorizado
- Conduza verificações de conformidade online e offline antes de acessar o e-mail
- Use a conformidade FIPS 140-2, criptografia AES-256 tanto para iOS quanto Android
- Veja anexos diretamente no aplicativo
- Controle onde os arquivos podem ser copiados ou movidos
- Restrinja o encaminhamento, movimento para outros aplicativos, colar e captura de tela
- Apague seletivamente os anexos, mesmo fora do e-mail
- Trabalhe no MaaS360 Content Suite para armazenar, ver, editar e compartilhar conteúdo

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

WGD03062-BRPT-01