IBM Security
Documento técnico – Liderança de ideias

Mobilize o conteúdo e os aplicativos da sua empresa

Permita a colaboração simples e protegida em dispositivos móveis na empresa

IBM

Estratégia de mobilidade para uma nova era

P: Você tem uma estratégia de virtualização robusta?

R: Estratégia de mobilidade? Você quer saber se os nossos funcionários podem acessar o e-mail nos dispositivos móveis deles? Claro, nós temos isso.

Se a sua resposta é essa, você não está sozinho. Muitas empresas ainda contam com e-mail como o "aplicativo de escolha" para os funcionários se comunicarem fora do escritório. E isso foi uma enorme vitória até mesmo poucos anos atrás. Mas vamos encarar os fatos, checar o e-mail e responder fora do escritório não é exatamente "trabalhar" como remover alguns obstáculos, mover as coisas e manter as aparências. No mundo de hoje, a colaboração móvel tem muito mais potencial para destravar a verdadeira produtividade e facilitar o trabalho real em tempo quase real, mas muitas empresas apenas arranham a superfície e ainda precisam abraçar, planejar e implementar uma estratégia de mobilidade robusta que aproveite o potencial da mobilidade com acesso simples e seguro aos recursos da empresa.

Neste documento discutiremos como o monitoramento contínuo pode ser aplicado a laptops, computadores e outros dispositivos de endpoint.

Neste documento técnico, você aprenderá a:

- Viabilizar o acesso móvel protegido aos dados corporativos sem uma VPN no dispositivo
- Mobilizar o SharePoint, o Windows File Share e todos os seus sites de intranet
- Proteger dados corporativos sigilosos com políticas de segurança robustas e controles DLP
- Fornecer acesso móvel sem exigir alterações na sua rede ou na configuração de segurança de firewall
- Permitir que os usuários colaborem de qualquer lugar usando os dispositivos pessoais deles

Leia para saber mais sobre como é possível fornecer aos funcionários acesso aos recursos por trás do firewall, protegendo os dados com políticas de autorização, criptografia e conteinerização.

Acesso simples com segurança

Aqui está um desafio simples: construir uma casa perfeitamente segura capaz de proteger todos os seus objetos de valor inestimável. Como você faria isso? Você poderia construir uma casa sem janelas e portas, sem nenhum ponto de entrada e saída. Ela provavelmente seria perfeitamente segura, mas pouco útil para a vida real. Ou poderia construí-la com janelas e portas que tenham sistemas de segurança e fechaduras de alta tecnologia para protegê-la e, efetivamente, ter o mesmo nível de segurança, mas ainda assim ser capaz de entrar, sair, receber visitantes e respirar um pouco de ar puro sem arriscar perder seus pertences preciosos.

Sua estratégia de mobilidade pode ser exatamente como uma casa sem janelas ou portas. Ou pode ser como uma casa com janelas e portas que nunca se trancam. Você está encarregado de proteger o conteúdo corporativo, mas também deve torná-lo disponível para os usuários para que eles possam ser produtivos. De listas de contatos de clientes a dados de pacientes, de informações financeiras a arquivos de Recursos Humanos, de aplicativos corporativos a atas de reuniões, as informações que seus funcionários desejam acessar aumentam diariamente, e bloquear o acesso não é mais uma opção viável. Você precisa de algumas portas e janelas, e de um sistema de segurança capaz de garantir que somente as pessoas autorizadas possam passar por elas e entrar.

O que acontece se um usuário leva um smartphone ou tablet pessoal para o trabalho e baixa os contatos de vendas para o dispositivo? E se eles enviarem os relatórios financeiros para o endereço eletrônico pessoal deles para trabalhar de noite em casa depois de colocar as crianças para dormir? E os fornecedores? Você quer compartilhar seu conteúdo e aplicativos para poderem colaborar com mais eficiência, mas o que acontecerá quando o projeto terminar?

Esses cenários acontecem todos os dias. As pessoas encontrarão formas de obter as informações de que precisam, colocando as informações corporativas em risco, a menos que você facilite uma forma mais segura, confiável e simples para elas conseguirem o que desejam.

Considerações sobre o conteúdo

O conteúdo da empresa fica armazenado em redes corporativas, em lugares como compartilhamentos de arquivos do Windows, SharePoint, sites de intranet e aplicativos da Web. As informações de que as pessoas precisam para colaborar com colegas, parceiros e clientes e realizar seus trabalhos estão presas em unidades internas e repositórios de dados, bases de conhecimento, wikis internos, ERP, SCM, HRM, CRM e outros sistemas de gerenciamento ou processos.

Então a pergunta passa a ser: como oferecer tudo isso para o funcionário móvel moderno que precisa de acesso em qualquer lugar, várias vezes por dia, em dispositivos que não são da sua empresa?

À medida que você protege seus dados e as redes internas, os compartilhamentos de arquivos e outros sistemas que os abrigam, convém pensar sobre as seguintes considerações como parte da sua estratégia de mobilidade. Algumas podem parecer óbvias, mas merecem sua atenção.

1. O conteúdo deve estar acessível para os usuários sob demanda por meio de uma abordagem de envio ou recepção
2. Cada usuário deve ter acesso apenas ao conteúdo necessário, com base no contexto e na identidade
3. Os dados devem ser atualizáveis e sincronizados entre os dispositivos ao longo do tempo
4. O processo de acesso aos dados não deve ser oneroso para o usuário
5. Manter a segurança não deve ser dispendioso, embora seja um grande investimento
6. Manter a segurança não deve exigir muito tempo da TI
7. Os dados em movimento devem ser criptografados e protegidos
8. Os dados não devem ser autorizados a sair da organização sem autorização
9. Os dados criados e armazenados em aplicativos devem ser preservados
10. Como os dispositivos pessoais não são de propriedade da organização, há um limite para o que você pode controlar

Um dos objetivos mais importantes de toda legislação de segurança cibernética federal deve ser o de permitir que os invadidos ajam rapidamente para proteger seus sistemas, como os fazem os invasores.

Tecnologias atuais

Vamos dar uma olhada nas tecnologias que estão sendo usadas hoje e em alguns dos problemas inerentes à habilitação da segurança e da produtividade.

E-mail

E-mail é o aplicativo de escolha para a colaboração, mas é apenas uma ferramenta entre muitas.

Ele não foi projetado para colaboração. O e-mail dá suporte a comunicações um-para-um ou um-para-muitos, mas não a interações muitos-para-muitos, que é o que os usuários precisam para ser realmente produtivos. Ele estimula o desenvolvimento de silos entre os grupos que deveriam estar trabalhando em conjunto.

As informações trocadas por e-mail podem ficar obsoletas rapidamente: as pessoas recebem uma planilha e continuam trabalhando nela sem perceber que ela já foi substituída por outra mais atual.

O maior problema é que os dados podem ser cortados, colados e encaminhados para lugares que você não quer que eles vão.

VPN

Fazer logon com uma VPN é uma escolha comum para prover acesso por trás de um firewall.

Infelizmente, forçar o login para ter acesso degrada a experiência do usuário. Entre um conteúdo novo, mas difícil de acessar, e um conteúdo obsoleto fácil de encontrar no anexo de um e-mail antigo, as pessoas podem optar pelo caminho mais fácil.

VPNs requerem licenças por dispositivo, ou seja, os custos podem aumentar ao longo do tempo. Além disso, há evidências de que o uso de uma VPN pode descarregar a bateria do dispositivo mais rapidamente.

Como os dispositivos móveis usam a tecnologia sem fio para se conectar, convém exigir criptografia. No entanto, há a questão do acesso em roaming. Em geral, as soluções que dependem de criptografia de nível mais elevado têm o potencial de falhar quando os usuários transitam entre pontos de acesso. Felizmente, existem algumas soluções que resolvem isso.

Virtualização da área de trabalho

Alguns aplicativos permitem que você exiba uma área de trabalho em dispositivos móveis. Todos os itens acessíveis no computador também estariam disponíveis no smartphone ou tablet. No entanto, isso geralmente é caro, e a experiência do usuário pode ser precária. Com essa abordagem, disponibilidade e desempenho estão fortemente dependentes da conectividade de rede. Além disso, problemas de resolução e de tamanho de tela representam outro desafio, especialmente em smartphones que possuem telas pequenas e espaços de trabalho reduzidos. Os aplicativos otimizados para um ambiente de área de trabalho podem ser acessados em um dispositivo móvel pela virtualização da área de trabalho, mas isso não significa que eles serão necessariamente úteis.

Outra questão que a TI precisa considerar é que os recursos do servidor e da rede devem ser capazes de dar suporte a vários dispositivos conectados na sua rede ao mesmo tempo.

Compartilhamentos de arquivos de terceiros

Compartilhamentos de arquivos de terceiros permitem manter material na nuvem. Um dos grandes problemas aqui é que você não tem controle. O conteúdo pode ser enviado para qualquer pessoa, acessado por qualquer pessoa, e você pode ter problemas de controle de versão.

Existe um problema de experiência do usuário também. Os usuários não gostam de ser forçados a aprender a usar um novo software só para ter acesso ao conteúdo de que eles precisam, e você deverá levar em consideração o tempo que eles precisarão para aprender.

Os compartilhamentos de arquivos de terceiros também podem sair caros: conforme adiciona usuários, você precisa adicionar licenças, além disso, pode não ser possível usar os investimentos existentes, como lojas de aplicativos e conteúdo.

Aplicativos de terceiros e personalizados

Se você procurar um desenvolvedor terceirizado para os seus aplicativos, ficará dependente do seu fornecedor. A prevenção de vazamento de dados (DLP) pode não vir integrada no aplicativo.

Você pode tentar desenvolver seus próprios aplicativos, mas, em seguida, precisará de uma equipe para dar suporte a eles e a todas as alterações que serão necessárias para novos tipos de dispositivos, atualizações de sistema operacional etc.

Muitos especialistas em segurança, altos funcionários de segurança cibernética do governo federal e líderes do Congresso estão pressionando por uma maior ênfase no monitoramento contínuo, em ferramentas de monitoramento automatizado e na reação rápida a ataques contra sistemas de tecnologia da informação do governo.

A importância das políticas

Se você pretende permitir que os usuários acessem os recursos corporativos em seus dispositivos pessoais, precisará criar políticas para regular a forma como seus dados são acessados e usados.

Você pode exigir que o usuário digite uma senha antes de acessar dados importantes.

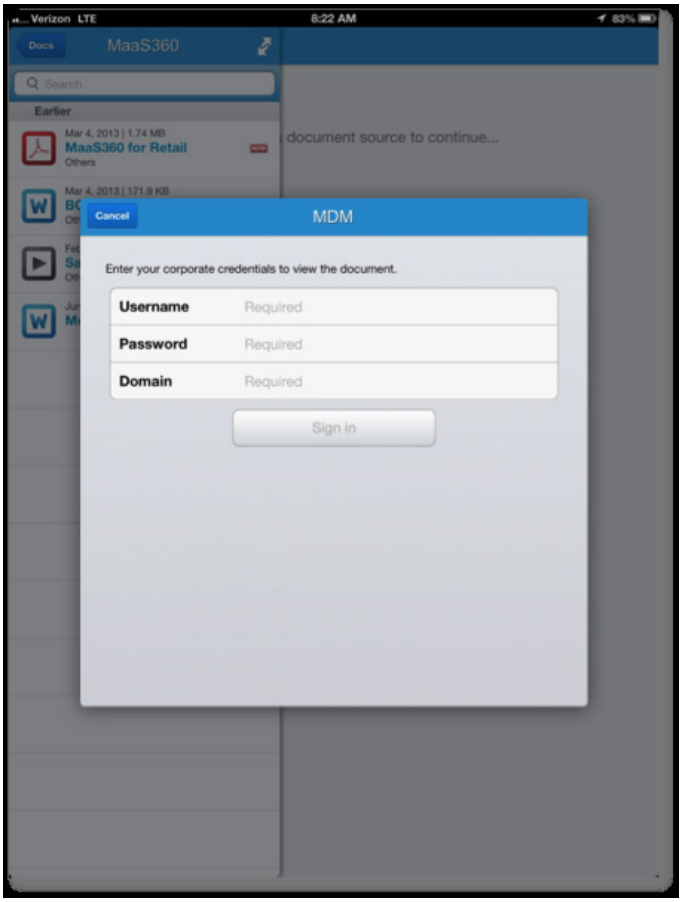

Figura 1: Um pedido de autenticação

Você também pode restringir o recurso de cortar e colar texto de um documento.

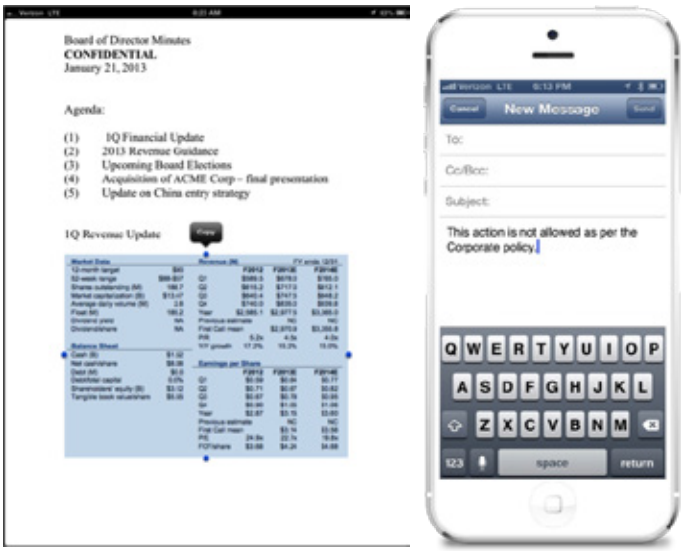

Figura 2: Controles de prevenção de vazamento de dados, como restrições de copiar e colar

IBM® MaaS360® Productivity Suite

O MaaS360 Productivity Suite ajuda a superar os desafios apresentados pelas tecnologias atuais e foi concebido com múltiplas formas de permitir o acesso seguro e a proteção dos seus dados em repouso:

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

O MaaS360 usa um contêiner para uma abordagem dual persona: dados, aplicativos e conteúdo específicos da empresa ficam em uma área protegida no dispositivo. Você determina os controles aplicados a essa área protegida, assim e-mail, contatos, calendários, aplicativos (e os dados dentro deles), documentos e o acesso a páginas da Web podem ser protegidos.

Figura 3: MaaS360 Productivity Suite e MaaS360 Content Suite

O MaaS360 Productivity Suite usa políticas de persona para especificar a segurança em todos os dispositivos de um usuário. Essas políticas são criadas no portal do MaaS360 e implantadas nos dispositivos inscritos remotamente, portanto a TI não precisa tocar nos dispositivos.

Quando o dispositivo sai de conformidade ou o projeto termina e o fornecedor vai embora, você simplesmente remove o contêiner remotamente, e os dados e aplicativos desaparecem.

O contêiner tem segurança integrada. Ele conta com criptografia AES-256 em conformidade com FIPS 140-2. Você pode exigir que os usuários insiram um código de acesso ao acessá-lo. Você também poderá usar essas definições de política para remover o contêiner completamente se os dispositivos estiverem com jailbreak ou rooting, ou se não tiverem sido verificados em um período de tempo especificado.

Você também pode impedir que arquivos sejam movidos, copiados ou impressos do contêiner, e pode impedir que arquivos sejam importados para ele.

IBM® MaaS360® Content Suite

O MaaS360 Content Suite oferece um contêiner criptografado e ferramentas de produtividade para distribuir, exibir, editar e compartilhar documentos em dispositivos móveis, dando às organizações o controle que de precisam e aos funcionários o acesso que exigem:

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® Mobile Document Sync

O MaaS360 Mobile Content Management oferece um contêiner de documentos móveis para colaboração em conteúdo com um conjunto robusto de recursos de gerenciamento do ciclo de vida para distribuir, atualizar, gerenciar e proteger documentos. Os administradores de TI podem forçar recursos de autenticação, copiar e colar e restrições só de visualização. Os usuários podem acessar o conteúdo distribuído pela empresa e repositórios de arquivos como SharePoint, Box e Google Drive.

O MaaS360 Mobile Document Editor foi projetado para impedir vazamentos de dados corporativos e, ainda assim, permitir aos usuários criar, editar e salvar. Os usuários podem colaborar no Word, Excel, PowerPoint e em arquivos de texto em dispositivos móveis de qualquer lugar.

O MaaS360 Mobile Document Sync permite aos usuários sincronizar facilmente o conteúdo entre dispositivos móveis gerenciados para continuar a criar ou editar seus arquivos sem interrupção. A TI pode aplicar políticas ao conteúdo, como restringir o recurso de copiar e colar ou bloquear a abertura ou o compartilhamento em aplicativos não gerenciados. Esses controles podem ser aplicados a todos os documentos, a um grupo de documentos ou a documentos individuais, oferendo a flexibilidade necessária para proteger os preciosos dados corporativos.

Os casos de uso de compartilhamento de conteúdo protegido são numerosos em praticamente todas as organizações, seja em vendas, marketing, operações ou finanças:

- Veja e compartilhe mudanças de última hora a uma apresentação de vendas em qualquer lugar, logo antes da reunião com o cliente
- Colabore com os últimos dados financeiros em uma planilha antes de embarcar em um avião

- Faça brainstorm de mensagens de marketing e compartilhe com colegas enquanto está em um café
- Distribua documentos trimestrais financeiros para a diretoria, e defina que o documento expire após a reunião
- Compartilhe materiais de produtos em tempo quase real com as equipes de vendas para que elas não precisem ter dificuldades para encontrar a última folha de dados ou informações competitivas
- Certifique-se de que os tablets em lojas de varejo tenham as informações de produtos e inventário mais atualizadas

IBM® MaaS360® Gateway Suite

O MaaS360 Gateway Suite é um componente essencial para ajudar a tornar tudo isso possível. Ele protege dados em movimento, fornecendo acesso contínuo e protegido ao seu conteúdo corporativo e intranet usando dispositivos móveis:

- Ofereça acesso simples e protegido aos dados em dispositivos móveis sem VPN no dispositivo; não é preciso passar pela VPN sempre que quiser acessar as informações
- Mobilize SharePoint, Windows File Shares, sites da intranet e aplicativos da Web
- Proteja dados com políticas de segurança robustas e controles DLP
- Não há necessidade de alterações na rede ou nas configurações de segurança do firewall

Figura 4: Fluxos de dados com o MaaS360 Gateway

Você pode configurar opções de política para gerenciar como o MaaS360 Productivity Suite interage com os dispositivos dos usuários. Por exemplo, você pode especificar URLs para wikis corporativos, sistemas de rastreamento de bugs etc., ou pastas corporativas acessíveis pelo MaaS360 Gateway, e eles aparecerão como favoritos no MaaS360 Secure Mobile Browser. Você também pode especificar se a autenticação é necessária para acessar esses locais.

O MaaS360 Gateway determina o que os usuários dos recursos corporativos verão quando acessarem o contêiner de dados nos dispositivos deles.

Experimente antes de comprar

É rápido e fácil experimentar o MaaS360. Além disso, o tempo investido na configuração do MaaS360 para as suas necessidades vale a pena. Após decidir que o MaaS360 é a solução certa para a sua organização, seu ambiente de teste se tornará seu ambiente real!

Para experimentar o MaaS360 sem custo, clique aqui. Comece agora mesmo! Não existem processos de configuração complicados, e você não precisa alterar sua infraestrutura. Experimente o MaaS360 hoje!

Figura 5: Produtos MaaS360

Sobre o IBM MaaS360

O IBM MaaS360 é a plataforma de gerenciamento de mobilidade corporativa que garante produtividade e proteção de dados da forma como as pessoas trabalham. Milhares de organizações confiam no MaaS360 como a base para suas iniciativas de mobilidade. O MaaS360 oferece um abrangente gerenciamento com fortes controles de segurança entre usuários, dispositivos, aplicativos e conteúdo para dar suporte a qualquer implantação de mobilidade. Para saber mais sobre o IBM MaaS360 e começar um teste grátis de 30 dias, acesse www.ibm.com/maas360

Sobre o IBM Security

A plataforma de segurança da IBM fornece inteligência de segurança para ajudar as organizações a proteger de forma holística funcionários, dados, aplicativos e infraestrutura. A IBM oferece soluções de gerenciamento de identidades e acessos, gerenciamento de informações de segurança e eventos, segurança de banco de dados, desenvolvimento de aplicativos, gestão de riscos, gerenciamento de endpoint, proteção contra invasões de última geração e muito mais. A IBM opera uma das organizações mais abrangentes de P&D em segurança. Para mais informações, acesse www.ibm.com/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
Março de 2016

Por favor, recicle

WGW03111-BRPT-01