IBM Global Technology Services
Thought Leadership White Paper

Novembro de 2012

Desenvolvimento de programas corporativos de mobilidade mais eficazes

Um guia prático com instruções para a criação de programas corporativos mobilidade com a ajuda de parceiros

IBM

A proliferação de dispositivos móveis, juntamente com uma força de trabalho cada vez mais global e remota, que exige o acesso imediato aos recursos corporativos, criou uma enorme necessidade de programas de mobilidade. Estes programas abrangem infraestruturas, tecnologias e políticas que permitem aos funcionários e outros stakeholders implementar aplicativos corporativos e acessar os recursos corporativos em dispositivos móveis – como smartphones e tablets. Embora algumas empresas permitam que os funcionários trabalhem apenas em dispositivos móveis de propriedade da empresa, outras estão cada vez mais implementando programas de "traga seu próprio dispositivo" (BYOD), que permitem que os funcionários selecionem e comprem os seus próprios dispositivos móveis para funções de trabalho.

Programas de mobilidade podem permitir às empresas criar valor significativo para os funcionários, parceiros e clientes. Com acesso permanente aos recursos corporativos, os funcionários podem trabalhar em praticamente qualquer lugar – e as empresas podem aumentar a sua produtividade, eficiência e vantagem competitiva. Mas os programas de mobilidade também podem representar desafios significativos para as organizações. Com algumas das melhores práticas firmemente enraizadas no segmento de mercado – devido ao crescimento rápido e recente das tecnologias móveis – muitas empresas que desejam criar programas de mobilidade não sabem como nem por onde começar. Outras que optam por desenvolver seus programas no local estão descobrindo que esta é uma iniciativa cara, complicada, arriscada e demorada.

Este artigo é um guia prático para traçar estratégias e implementar programas corporativos de mobilidade mais eficazes e detalha os recursos que os parceiros corporativos podem trazer para o desenvolvimento e suporte de seu dispositivo de propriedade da empresa ou de programas corporativos como o BYOD. Ele se concentra em programas corporativos de telefonia móvel para os funcionários, em vez de clientes.

A consumerização da TI

A demanda generalizada de dispositivos móveis no local de trabalho, juntamente com uma força de trabalho cada vez mais dispersa, obrigou as empresas a suportar o uso da tecnologia móvel no local de trabalho. Em uma pesquisa recente da IBM com 675 Chief Information Officers (CIOs) e gerentes de TI de grandes empresas em todo o mundo, 74 por cento dos entrevistados disseram que estão dando maior prioridade ao desenvolvimento de um ambiente de trabalho flexível em comparação com outros investimentos ao longo dos próximos 12 meses.[1] A maioria dos entrevistados também acredita que o trabalho flexível trará ganhos de produtividade, e quase metade acredita que ele irá, potencialmente, aumentar as receitas.[2]

De acordo com uma análise do Gartner, em 2014, 80 por cento dos profissionais móveis usarão pelo menos dois dispositivos móveis para acessar sistemas e dados corporativos, acima dos 40 por cento dos dias atuais.[3] É claro que o uso de dispositivos móveis no local de trabalho não é mais uma tendência - é uma nova realidade corporativa.

"A ascensão de programas como "Traga o seu Próprio Dispositivo" (BYOD) é a única mudança mais radical na economia da computação do cliente, para o negócio desde que os PCs [4] invadiram o local de trabalho. Toda empresa precisa de uma posição claramente articulada em BYOD, mesmo que opte por não permitir isso."[5]

Desafios de mobilidade para empresas

Como a tecnologia móvel é nova e está em constante mudança, algumas das melhores práticas foram criadas para fornecer às empresas planejamento para a implementação de estratégias de mobilidade eficazes. Como resultado, muitas empresas não sabem como ou por onde começar.

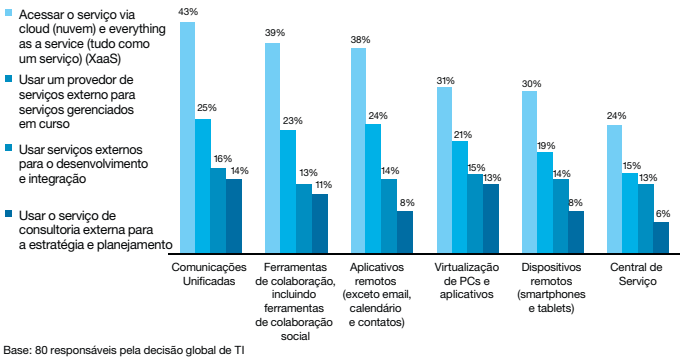
Segurança, privacidade e governança de uso também são as principais preocupações – devido ao cruzamento de dados pessoais e corporativos em muitos dispositivos móveis. Na verdade, 71 por cento dos CEOs e gerentes de TI entrevistados indicaram que a segurança era seu desafio empresarial mais

significativo quando se trata de mobilidade.[6] E suas preocupações não são injustificadas. Em seu sétimo estudo anual patrocinado pela Symantec, o Ponemon Institute informou que o custo médio organizacional de uma violação de dados é de US$5.500.000 e de US$194 por registro.[7]

O estudo também indicou que 39 por cento das organizações tinham uma violação de dados, como resultado de um dispositivo móvel de funcionário ou contratado que foi perdido ou roubado – isso incluiu laptops, smartphones, tablets e drives USB que continham informação confidencial e sensível. Além disso, 37 por cento diz respeito a um ataque malicioso ou criminal, e 24 por cento de falhas do sistema envolvido, incluindo uma combinação de falhas de TI e de processos de negócios.[8]

As organizações não podem pagar as consequências potencialmente desastrosas de navegar cegamente na rápida evolução do labirinto da mobilidade. É por isso que muitas empresas estão buscando cada vez mais a ajuda de profissionais altamente qualificados que podem fornecer os recursos e as tecnologias necessários para ajudar as organizações a reduzir os riscos e implementar programas corporativos de mobilidade sustentáveis. Um parceiro de mobilidade para empresas também pode oferecer o conhecimento das melhores práticas que obteve ao ajudar diversas outras, em vários setores, a criar estratégias bem-sucedidas.

Como você está planejando implementar a sua mobilidade, colaboração e estratégia de social business para enfrentar os desafios relacionados?



Base: 80 responsáveis pela decisão global de TI
Fonte: Um estudo encomendado pela Forrester Consulting em nome da IBM, maio 2012

Guia para desenvolvimento, gerenciamento e suporte de dispositivos móveis corporativos

Há quatro etapas para a implementação de um programa corporativo de mobilidade eficaz e sustentável:

1. **Definir uma estratégia remota:** esclarecer seus objetivos de mobilidade, determinar qual o tipo de programa que você suportará (BYOD versus dispositivo de propriedade da empresa) e avaliar as considerações de custo

2. **Implementar o seu programa corporativo de mobilidade:** determinar quais as ferramentas que você usará para construir o seu programa e preparar sua rede corporativa para suportá-lo

3. **Proteger e gerenciar seus dispositivos móveis:** escolher tecnologias para ajudar a proteger os dispositivos móveis conectados à sua rede e desenvolver uma política de segurança

4. **Suporte:** fornecer suporte contínuo de correção de problemas para dispositivos móveis

Cada estágio é descrito abaixo em detalhes.

Etapa um: desenvolvimento da estratégia de mobilidade

Uma das etapas mais importantes para a criação de um programa corporativo de mobilidade deve ser a definição de uma estratégia que governará a forma escolhida por você para desenvolver e implementar a mobilidade no seu local de trabalho. Essa estratégia deve começar com um pensamento claro sobre suas necessidades, desejos e objetivos.

As perguntas que você terá que responder incluem:

- Por que queremos implementar um programa corporativo de mobilidade? Qual é a nossa visão final? Quais os benefícios que esperamos realizar?

- Quais são as considerações de custo de um programa de mobilidade? Será que os custos superam os benefícios para a nossa situação?
- Possuiremos ou solicitaremos que os funcionários comprem e usem os seus próprios dispositivos móveis? De quanto será, se houver, o reembolso que forneceremos?
- Planejamos desenvolver aplicativos de mobilidade customizados, terceirizar o desenvolvimento de aplicativos ou comprar aplicativos prontos?

Benefícios dos programas empresariais de mobilidade: Há uma infinidade de benefícios, mas os mais comuns incluem:

- Aumento da satisfação dos funcionários – Os funcionários gostam de trabalhar a partir de dispositivos móveis, especialmente os dispositivos e plataformas de sua escolha. Eles também aproveitam a flexibilidade de trabalhar em quase qualquer local e em sua conveniência.
- Recrutamento e retenção mais fáceis de funcionários – Os funcionários tendem a preferir trabalhar para empresas que suportam a tecnologia móvel no local de trabalho.
- Maior produtividade – Ao permitir que os funcionários trabalhem praticamente a qualquer hora e em qualquer lugar, eles podem fazer mais, dentro e fora do escritório. Além disso, o desenvolvimento de aplicativos customizados ajuda os funcionários a realizar suas atividades de maneiras novas e mais inovadoras.
- Melhoria das relações com os clientes – aplicativos móveis especializados (apps) podem permitir que as empresas vendam os seus produtos por meio de dispositivos móveis e forneçam à sua equipe de vendas os dados do cliente em tempo quase real. Estas capacidades podem ajudar as empresas a monitorar "o pulso" de um cliente, atender às suas necessidades e desejos mais rapidamente, proporcionando um melhor atendimento.

Considerações gerais de custos: As economias de custos que as empresas têm relatado variam muito. Os fatores podem incluir investimentos em software, infraestrutura (incluindo os próprios dispositivos móveis, se você escolher uma abordagem de dispositivo de propriedade da empresa), em pessoal ou serviços de suporte relacionados, desenvolvimento de aplicativos e até mesmo possíveis atualizações de rede. Você também vai querer considerar os custos menos óbvios, como taxas de licenciamento de software, reembolso oferecido pela empresa para dispositivos móveis, as taxas de uso internacionais, impostos, seguros e custos intangíveis diversos. Mas, claro, muitos dos benefícios dos programas empresariais móveis – como o aumento da produtividade, a inovação do local de trabalho, economia de tempo e satisfação dos funcionários – são imensuráveis. E as empresas que terceirizam serviços corporativos de mobilidade, muitas vezes, experimentam uma economia significativa.

Os CIOs relataram ganhos de produtividade de 20 por cento e redução de custos quando eles terceirizaram os serviços de local de trabalho flexível.[9]

BYOD versus dispositivos de propriedade da empresa: Os custos do programa corporativo de mobilidade também estão ligados ao tipo de programa que você implementar.

Por exemplo, os programas de BYOD podem ser mais caros e complexos, devido ao entrelaçamento de dados privados e corporativos em dispositivos móveis e às medidas mais complicadas necessárias para manter os dispositivos pessoais seguros. De acordo com o Aberdeen Group, uma empresa com 1.000 dispositivos móveis BYOD gastará uma média de US$170.000 a mais por ano do que uma organização com uma política corporativa responsável adquirida centralmente. Os custos do BYOD incrementais e difíceis de controlar incluem:

- Desagregação do faturamento da transportadora
- Aumento de relatórios de despesas apresentados para reembolso de funcionário
- Incluir um fardo na TI para gerenciar e proteger dados corporativos em dispositivos de funcionários
- O aumento da carga de trabalho em outros grupos operacionais que não são normalmente encarregados de suporte à mobilidade
- O aumento da complexidade do cenário móvel resultante com o consequente aumento de custos de suporte[10]

O controle e a facilidade de gerenciamento é outro fator a ser considerado. Se você selecionar possuir e gerenciar dispositivos móveis, pode ser mais fácil protegê-los e gerenciar a conformidade com as políticas corporativas – porque é possível criar a infraestrutura sobre a qual você entregará dados corporativos e aplicativos. Mas o controle pode vir em detrimento da satisfação do usuário – porque muitos funcionários preferem, de forma inflexível, trabalhar com seus próprios dispositivos. Para facilitar um amplo suporte de sua abordagem de dispositivo de propriedade da empresa, obtenha o retorno de seus funcionários com relação aos tipos de dispositivos e aplicativos que eles gostariam de usar. Eles são mais propensos a aceitar as limitações de um programa que ajudaram a construir. Além disso, se você está fornecendo os dispositivos móveis, seus funcionários esperarão que a sua organização forneça um alto nível de suporte ao usuário final. Portanto, você precisará de uma equipe adequada e experiente no local para suportar essas novas demandas.

Considerações de estratégia – como um parceiro empresarial pode ajudar: Um parceiro de mobilidade ajuda a avaliar como a mobilidade pode beneficiar seus funcionários, clientes e negócios em geral. Eles podem fornecer estratégia e consultoria para ajudá-lo a esclarecer e priorizar suas necessidades e objetivos, avaliar o seu retorno tangível e intangível sobre o investimento e desenvolver um plano em etapas para a implementação do programa. Eles podem até mesmo oferecer serviços de gerenciamento de despesas de telecomunicações para ajudá-lo a otimizar e gerenciar melhor seus gastos com mobilidade. E um parceiro pode praticamente eliminar a meticulosa investigação e os desafios logísticos que começar do zero implica – para ajudá-lo a obter o seu programa instalado e funcionando mais rapidamente.

dEtapa dois: a implementação do programa de mobilidade

Depois de esclarecer as suas metas do programa, é preciso começar a avaliar como implementá-las tecnicamente.

As perguntas que você terá que responder incluem:

- Quais dispositivos vamos suportar (telefones, tablets, laptops)? Quais são as vantagens e desvantagens do suporte a diferentes dispositivos e sistemas operacionais? Com base nesta análise e nas preferências do usuário final, quais dispositivos e sistemas operacionais móveis queremos suportar?
- Quais são os dados e os aplicativos que devemos tornar acessíveis aos usuários finais? Devemos conceder acesso total ou restrito?
- Quais serviços suportaremos?
- Quem são os funcionários e os stakeholders que têm necessidades de mobilidade de maior prioridade? Devemos limitar a adoção corporativa móvel a esses indivíduos ou estender o acesso a todos os funcionários?
- Quais cenários de uso de dispositivos móveis podem justificar o desenvolvimento de aplicativos móveis especiais?

- Devemos limitar o nosso programa de mobilidade a locais estratégicos da empresa ou lançar um programa para toda a empresa que possa suportar vários sites em todo o mundo?
- Até que ponto os nossos sistemas de mobilidade e corporativos precisam ser integrados?
- Como podemos suportar o ótimo desempenho de nossas redes para facilitar o sucesso do nosso programa de mobilidade?

Determinar quais dispositivos suportar: É quase impossível suportar de forma segura e logística cada novo tablet e smartphone que chega ao mercado. Uma abordagem mais eficaz oferece suporte a dispositivos e sistemas operacionais específicos e define estes dispositivos (bem como a sua explicação para o porquê do suporte a eles) em sua política móvel – um tópico que abordaremos mais adiante neste artigo. Idealmente, a sua decisão deve ser baseada nos usos atuais e potenciais dos dispositivos móveis em sua empresa, e em um reconhecimento das preferências dos seus funcionários.

Mas, em geral, suportar mais plataformas significa mais complexidade. Portanto, uma das maneiras mais fáceis para reduzir a complexidade é limitar o número de dispositivos e plataformas que você suporta. Mas também é imperativo considerar as vantagens e desvantagens de várias plataformas, como a Research in Motion (RIM) BlackBerry, Apple iOS, Android e Windows. E quando se consideram as vantagens, priorizar o que é mais e menos aceitável para a sua organização a partir de um ponto de vista de segurança. Muitas empresas apoiam o uso de telefones BlackBerry devido ao seu design seguro. E, embora as plataformas iOS e Android possam suportar níveis mais elevados de segurança, as versões mais antigas do Microsoft Windows e Android não podem. Para ajudar a facilitar a segurança, a compatibilidade de aplicativos e seus encargos de serviços de mesa (desktop), é uma boa prática limitar o número de plataformas e versões de sistemas operacionais (SO). E, conforme o seu programa de infraestrutura e segurança evoluir ao longo do tempo, será possível expandir lentamente o seu suporte a dispositivo e plataforma.

A escolha de dados e aplicativos para acesso móvel: Depois de ter reduzido os dispositivos e sistemas operacionais que você suportará, o próximo passo é determinar os dados e aplicativos que você tornará acessíveis a funcionários específicos. Por exemplo, se você trabalha em um ambiente de cuidados com a saúde, pode exigir diferentes níveis de acessibilidade móvel para enfermeiros e médicos do que para os administradores. Recomendamos a compilação de uma equipe encarregada pela coleta de informações de seus funcionários para obter mais detalhes sobre as suas necessidades reais e percebidas para a tecnologia móvel no local de trabalho. Esta informação ajuda a debater de forma mais eficaz os processos de negócios específicos – em toda a empresa – que poderiam ser facilitados por meio do acesso a dados específicos e aplicativos existentes ou customizados em dispositivos móveis. Então, para reduzir a complexidade, priorize quais os usuários terão acesso móvel a estes recursos corporativos. E não se esqueça de "testar as águas" em primeiro lugar, estendendo o acesso apenas aos seus usuários de maior prioridade, em oposição a todos os funcionários.

Geralmente, para dar início, aplicativos de email e calendário são comuns e mais fáceis. Se os seus funcionários já estiverem usando dispositivos móveis para acessar seu email e calendário, é aconselhável fazer um inventário dos dispositivos e plataformas que eles estão usando para ajudar a gerenciar a conformidade de segurança antes de atualizar ou expandir o seu programa corporativo móvel. Se você está iniciando um programa de BYOD, perceba que o middleware de sistema de mensagens móveis possui uma funcionalidade limitada (consulte "Limpar e travar dispositivo" nas páginas 8-9).

Ativando os serviços para funcionários: Além de permitir aplicativos, também é possível optar por ativar determinados serviços através de dispositivos móveis. Estes podem incluir funções de negócios sociais, tais como sistema de mensagens instantâneas, gerenciamento de risco empresarial (ERM) e

gerenciamento de relação com o cliente (CRM), sistemas para acesso às vendas, finanças e dados de recursos humanos (RH). Priorize a ordem em que você tornará esses serviços acessíveis aos funcionários – porque, uma vez que as as tecnologias móveis são suportadas dentro do seu local de trabalho, os seus funcionários virão à procura de inúmeros recursos.

Preparando a sua rede: O gerenciamento eficiente de rede é, muitas vezes, esquecido durante o planejamento de programas corporativos móveis, mas pode fazer toda a diferença para o sucesso ou o fracasso de suas iniciativas móveis. Em geral, uma rede em expansão que suporta um número crescente de dispositivos e enormes volumes de dados, exigirá maior largura de banda e fortes capacidades de supervisão da rede. Isso significa que você precisa de soluções que possam automatizar as mudanças de configuração, analisar o desempenho, gerenciar a segurança, fornecer uma série de outras funções de gerenciamento e suportar a escalabilidade massiva (como ferramentas de rede baseadas em nuvem ou virtualizadas).

O tempo de atividade também se torna uma preocupação maior. Conforme as redes crescem, a chance de erro e os riscos de segurança também aumentam. E esses riscos aumentados, tornam as capacidades de gerenciamento de eventos, análise de causa raiz, gerenciamento de mudanças e configuração, relatórios de desempenho e gerenciamento de terminal mais confiávies, eficazes, e ainda mais necessários.

Uma abordagem gradual viável para a implementação da estratégia de mobilidade

Ao desenvolver um programa de mobilidade, evite a tentação de fazer tudo ao mesmo tempo – mesmo se você estiver trabalhando com um parceiro corporativo. Tenha uma visão mais ampla em mente ao dar pequenos passos em direção a seus objetivos. Dessa forma, é possível gerenciar e resolver problemas que você pode enfrentar ao longo do caminho antes de passar para a iniciativa mais complexa.

Aqui está um exemplo de implementação de um programa corporativo de mobilidade, que você pode implementar ao longo de vários meses.

1. Gerenciar os dispositivos existentes que acessam seu email, calendário e outras aplicações móveis: Usando as ferramentas de gerenciamento de infraestrutura ou software de gerenciamento de dispositivos móveis (MDM), faça um inventário do número de dispositivos móveis que avaliam sua rede. E preste muita atenção à forma como eles estão acessando a rede (como através de uma rede privada virtual [VPN] ou WiFi) e quais dados e aplicativos estão acessíveis nesses dispositivos. Se possível, você também deve determinar o status de segurança desses dispositivos, incluindo procedimentos de autenticação e segurança de aplicativo. Se você não puder acessar esta informação, devido à falta de ferramentas MDM e relatórios no local, é possível estabelecer um prazo para suspender o uso do acesso móvel atual e anunciar políticas e procedimentos mais rigorosos e mais recentes para os seus funcionários, quando você tiver a capacidade técnica para suportá-los.

2. Expandir o acesso gerenciado a todos os funcionários: No mínimo, a maioria de seus funcionários quer ter acesso a email corporativo e aplicações de calendário. A expansão desses recursos a todos os funcionários, não só contribui para aumentar a satisfação, mas também pode lhe dar uma melhor visão da logística de implementação da mobilidade em toda a empresa. Esse insight pode determinar a permissão do acesso móvel para toda a empresa para outros dados e aplicações.

3. Fixar no dispositivo de armazenamento de conteúdo e sincronização: É possível permitir o armazenamento de dados apenas na rede – para evitar cópias locais de armazenamento nos dispositivos, o que seria um risco se eles fossem perdidos ou roubados. É possível escolher métodos tais como criptografia e conteinerização para armazenar de forma mais segura o conteúdo.

4. Fazer inventário e priorizar aplicativos off-the-shelf (COTS) para software existente usado pela organização: Isso ajuda a fornecer o que seus funcionários precisam para serem mais produtivos com mobilidade.

5. Desenvolver ou contratar aplicativos customizados conforme necessário: Considere quais serviços e processos podem exigir o desenvolvimento de aplicativos customizados, e desenvolva-os com base em suas prioridades de mobilidade.

6. Implemente aplicativos móveis quando sua infraestrutura de segurança estiver em ordem: Os aplicativos corporativos que são habilitados para o acesso móvel devem, pelo menos, se igualar à segurança dos aplicativos que não estão habilitados para esse tipo de acesso. Se você não puder implementar aplicações que passem este padrão de segurança, limite sua implementação a aplicações de mobilidade mais confiáveis.

Etapa três: gerenciamento de segurança

Depois de ter determinado a tecnologia que usará para construir e gerenciar o seu programa corporativo móvel, você precisa de um plano para ajudar a proteger todos os dispositivos móveis conectados à sua rede.

As perguntas que você terá que responder incluem:

- Como podemos gerenciar melhor a segurança de dispositivos, aplicativos e acesso a dados?
- Como podemos gerenciar dados quando um funcionário deixa a empresa ou quando um dispositivo é perdido ou roubado?
- Como podemos proteger melhor os dispositivos móveis de ameaças comuns, como vírus, malware e ataques?
- Qual é o nível mínimo de segurança que vamos considerar aceitável; e poderemos implementá-lo, dadas as fronteiras de nossa cultura corporativa?
- Como podemos distribuir de forma mais segura os dispositivos móveis, aplicativos corporativos e gerenciar o processo de migração e adoção?
- O que deve ser incluído em uma política de segurança móvel, e como podemos gerenciar melhor a conformidade com as leis de privacidade de dados?

Embora a segurança móvel continue a ser uma das principais preocupações para as organizações, existem inúmeras maneiras de proteger dados em dispositivos móveis. Se você já tiver determinado os dispositivos móveis que a sua organização suportará e o nível mínimo de segurança que exigirá, pode ser muito mais fácil escolher as ferramentas certas para suportar de forma mais segura a sua empresa móvel.

Existe uma grande variedade de meios e métodos de segurança a escolher, alguns dos quais incluem:

Mobile device management (MDM): Representa a abordagem de TI tradicional de monitorar um dispositivo por meio de um agente de software que é instalado no dispositivo e um servidor que é operado no local ou através de serviços via cloud-based. MDM é útil para praticamente qualquer dispositivo que precise ser relatado ou verificado. Além disso, ele pode ajudá-lo a implementar, gerenciar e até mesmo distribuir aplicativos corporativos Over the Air (OTA) em toda a empresa. O MDM pode até mesmo deixá-lo ver quais aplicativos os usuários têm instalado, proibir o acesso a aplicativos restritos e sugerir novos aplicativos ou atualizações. Algumas ferramentas também incluem uma variedade de portais de autoatendimento do usuário que permitem aos funcionários redefinir sua senha, bloquear seu dispositivo e limpar, parcial ou totalmente, o seu dispositivo remotamente, caso ele seja perdido ou roubado. A implementação do MDM no local pode resultar em despesas altas. Mas os sistemas software como serviço (SaaS) baseados em nuvem são mais rápidos de configurar, fáceis de atualizar e possuem custo reduzido.

No entanto, ao configurar sua solução de MDM, considere o que a sua cultura corporativa permitirá, especialmente para dispositivos pessoais. Você pode, por exemplo, ser capaz de colocar um agente em um telefone Android que pode fazer o inventário de software detalhado, desativar a câmera, rastrear a localização do sistema de posicionamento global (GPS) e fazer limpezas parcial ou total do telefone. Mas será que a sua cultura corporativa suportará esses recursos ou irá considerá-los muito invasivos?

Conteinerização: Alguns programas MDM incorporam capacidades de conteinerização que usam criptografia e outros métodos para criar uma barreira entre os dados pessoais e corporativos em dispositivos móveis – tornando-os adequados e eficazes para os programas de BYOD. Embora algumas organizações possam optar por combinar MDM e conteinerização para a redução de custos e por razões de gerenciamento de fornecedores, descobrimos que manter métodos de conteinerização separados do MDM pode reduzir significativamente a complexidade.

Limpar e travar um dispositivo: Um dos maiores desafios de proteção de dispositivos móveis é a natureza móvel dos próprios dispositivos. Seu tamanho portátil o torna fácil de ser perdido, e seu uso móvel requer mecanismos de monitoramento e de gerenciamento para proteger os dados corporativos confidenciais. Limpar ou apagar todos os dados do dispositivo

móvel após um determinado número de tentativas de senha inválidas pode ajudar a reduzir o risco de um ataque de força bruta. Além disso, uma "limpeza local" iniciada por um usuário final ou administrador é uma prática recomendada quando um dispositivo for perdido ou roubado, ou quando um funcionário deixar a empresa ou se mudar para uma posição diferente dentro da sua empresa. Bloquear um dispositivo após o tempo limite de inatividade também pode ajudar a reduzir os riscos de segurança.

Se você está apenas começando um programa de BYOD e não deseja instalar um agente MDM em dispositivos de propriedade pessoal, você deve considerar que o middleware de sistema de mensagens móveis não permite a limpeza parcial ou a separação de dados.

Criptografia e alternativas de armazenamento de dados: A criptografia de dados em dispositivos móveis pode proporcionar um nível adicional de segurança. A criptografia baseada em hardware, um dos métodos mais comuns, oferece uma vantagem sobre a criptografia de software, porque ela é construída no dispositivo e pode melhorar o desempenho. Navegador e aplicativos virtualizados podem oferecer alternativas para o armazenamento de dados em dispositivos móveis. Pouco ou nenhum dado é armazenado efetivamente no dispositivo, em vez disso, os dados são solicitados e exibidos, conforme o necessário, reduzindo o risco de perda de dados. No entanto, o acesso à rede é necessário, por isso, os usuários não podem acessar dados quando estiverem offline ou desconectados. Além disso, o desempenho pode ser menor do que o de um cliente nativo ao acessar dados locais no dispositivo móvel, ou o tempo de resposta do usuário final pode ser maior.

Autenticação com base no usuário e prevenção a fraude: Autenticação com duas etapas e baseada no usuário – para registro no dispositivo e, em seguida, para a rede corporativa – pode ser definida como a exigência mínima necessária para ajudar a controlar e monitorar quem está acessando seus dados corporativos e aplicativos.

Um código numérico ou alfanumérico padrão pode ser necessário ao efetuar login no dispositivo, e um método mais avançado de autenticação – como um cartão inteligente, certificado digital ou token – pode ser usado para acessar a rede.

Embora alguns dispositivos suportem apenas senhas, o BlackBerry também suporta cartões inteligentes. Mas as medidas de segurança avançadas podem ser integradas em aplicativos móveis. Por exemplo, é possível exigir procedimentos de autenticação adicionais para acesso a dados e aplicativos especialmente sensíveis. Estes podem incluir indicadores biométricos, tais como voiceprint, que você pode verificar em relação aos seus registros. Um método de autenticação de várias camadas é uma forma eficaz de reduzir violações de segurança.

Além disso, se você planeja permitir acesso de Virtual Private Network (VPN) à sua intranet corporativa, inclua a capacidade de ajudar a controlar quais endereços de Internet Protocol (IP) podem ser acessados.

No entanto, todos estes métodos podem ser dispendiosos e complexos para implementar. Portanto, é importante equilibrar custo e facilidade de gerenciamento ao decidir qual a autenticação e os métodos de prevenção contra fraude implementar.

Gerenciamento de ameaça a dispositivo móvel: Praticamente todos os dispositivos móveis podem ser infectados com malware. Mas uma abordagem eficaz para minimizar malwares é a implementação de medidas de proteção que são semelhantes às do ambiente desktop e laptop. Isto implica a necessidade de todos os clientes instalarem e executarem automaticamente software anti-malware e realizarem varreduras regulares em

tempo real. Será necessário aconselhar de forma proativa seus funcionários para baixar e instalar apenas aplicativos confiáveise tomar as medidas apropriadas, tais como verificações de vírus, quando os aplicativos suspeitos forem identificados. Criar uma loja de aplicativo customizado que permite que seus funcionários façam o download de aplicativos corporativos e não corporativos também pode limitar o malware em sua rede.

Política de segurança móvel: Finalmente, você precisará criar e aplicar políticas para ajudar a proteger sua organização de ameaças de segurança e de dever financeiro. As políticas de segurança móvel devem ser construídas com a orientação dos advogados da empresa e da equipe de TI, ou dos parceiros empresariais móveis que conhecem os detalhes técnicos de suas medidas de segurança móvel. Os pontos-chave da sua política de segurança de mobilidade devem incluir:

- Os dispositivos móveis que você suportará – incluindo os dispositivos de propriedade da empresa e pessoais, o nível de suporte ao usuário final que você fornecerá e como acessar o suporte. Você também pode querer explicar o porquê do suporte de plataformas específicas em detrimento de outras. Por exemplo, você pode optar por suportar apenas as plataformas que permitem a criptografia, o que descartará determinados dispositivos.
- As definições de todos os termos-chave, incluindo termos básicos, tais como dispositivos móveis e gerenciamento de dispositivos móveis.
- Quem terá acesso aos dados e aplicativos específicos?
- Os dados e as atividades que sua empresa monitorará e acompanhará, a diferenciação entre os dispositivos de propriedade corporativa e pessoal. Isso pode incluir mensagens de texto, email, navegar na Internet, downloads, rastreamento de GPS, mensagens instantâneas, armazenamento de arquivos multimídia e muito mais.
- A política de privacidade que detalha o que você vai e não vai fazer com a informação que é monitorada e controlada na empresa e nos dispositivos de propriedade do funcionário.
- As ações específicas que sua empresa tomará se o usuário final violar as políticas de uso da empresa.
- Medidas defensivas definidas, como limpezas remotas, que a empresa tomará se o dispositivo for perdido ou roubado, ou se o funcionário mudar para outra posição dentro da empresa ou for demitido.

O acordo deve ser assinado pelos supervisores e funcionários. Depois de desenvolver a sua política oficial de segurança móvel, certifique-se de anunciá-la a toda a organização e distribuir as atualizações à sua política conforme você alterá-la. E divulgar a sua política de segurança móvel em boletins de notícias, redes sociais corporativas e em sua Intranet.

Recomendações de estilo de política de segurança de mobilidade do Gartner[11]

- Mantenha o documento de política curto, o ideal é não mais do que algumas páginas.
- Tenha o cuidado para usar as palavras imperativas apropriadamente, como “deve”, “deveria” e “pode”. Os padrões fornecem instruções que devem ser seguidas. As diretrizes fornecem sugestões que devem ser consideradas. Verifique se as questões e critérios de decisão mostram quando um padrão ou diretriz pode ou não ser aplicável.
- Coloque discussões detalhadas do processo e explicações tutoriais em apêndices ou documentos externos, em vez de incluir no corpo do documento.
- Nunca duplique o material que pertence a outro documento, especialmente envolvendo documentos sob o controle de outra pessoa. Forneça citações claras de documentos externos. Estabeleça uma linha de comunicação com todos esses proprietários do documento.
- Evite instruções condicionais ambíguas, como “sempre assim, exceto quando dessa maneira”, e instruções com base em testes negativos aninhados, como “se não for desta forma, então, não será dessa maneira.” Conduza com condições positivas que são claramente qualificadas.
- Faça afirmações absolutas (“sempre”) apenas quando a condição for verdadeiramente absoluta.
- Expanda acrônimos apenas uma vez, no primeiro uso.
- Forneça um glossário de termos, incluindo a repetição de acrônimos, como a última entrada no final do documento.

Não se esqueça da satisfação do usuário final: Ao definir as políticas de segurança, estar consciente da qualidade da experiência do usuário. Por exemplo, exigir diferentes aplicativos para dispositivos móveis com relação a desktop pode limitar o sucesso de seu programa. Bloqueio de recursos para aplicativos também pode reduzir a popularidade do seu programa. Além disso, os funcionários esperam alertas de notificação automática quando o dispositivo não está em conformidade e orientação para auto-correção. Certifique-se de dar-lhes tal orientação, comunicando regularmente as suas políticas de segurança de conformidade.

Etapa quatro: suporte diário

Você precisará gerenciar a segurança de seus dispositivos móveis em uma base regular e fornecer suporte aos seus usuários finais.

As perguntas que você terá que responder incluem:

- Qual o nível de gerenciamento e de suporte que podemos prestar aos dispositivos corporativos ou de propriedade pessoal?
- Temos recursos internos suficientes para a implementação e suporte, ou devemos procurar ajuda exterior?

Equipe para suporte: as ferramentas de MMS e software de gerenciamento de segurança podem ajudar a controlar e monitorar a atividade do dispositivo móvel em sua rede. Mas você precisará da equipe para suportar estas capacidades e ajudar continuamente a proteger sua rede contra ameaças de tecnologias móveis.

Seu programa corporativo móvel também deve fornecer algum nível de suporte aos usuários finais. Ao lançar um programa corporativo móvel, o índice de volume de dispositivo por funcionário pode aumentar de forma significativa, então, será preciso ter uma equipe e orçamento para suportar essas novas demandas. E a sua equipe terá um profundo conhecimento da tecnologia móvel para gerenciar novos pedidos de suporte do usuário final.

Abordagens com suporte à entrega: você precisará criar um modelo de abordagem para gerenciar o fornecimento de suporte. Algumas organizações designarão um determinado período de tempo – normalmente de meia hora a uma hora – para trabalhar em um problema de dispositivos móveis. Outras podem optar por fornecer suporte apenas para problemas de rede, em oposição aos próprios dispositivos móveis. Algumas empresas chegam a criar listas de discussão, portais da web e wikis que incentivam os usuários finais a compartilhar suas experiências sobre questões de suporte. Por exemplo, um usuário pode postar uma pergunta sobre como configurar o Microsoft ActiveSync no seu dispositivo que outros funcionários podem responder. Outra opção é exigir que os usuários finais comprem um seguro que cubra o suporte e substituição de dispositivos perdidos ou danificados, caso em que sua política móvel deverá definir as seguradoras aceitáveis, bem como a ajuda de custos para o seguro.

Implementação, segurança e suporte – como um parceiro corporativo móvel pode ajudar: parceiros corporativos móveis podem fornecer a você as habilidades, tecnologias, treinamento e suporte necessários para a implementação e o gerenciamento de programas empresariais de mobilidade mais rápido e mais rentável do que as soluções locais. Ambas as soluções pontuais e de ponta a ponta podem incluir:

- Compra, preparo e configuração do dispositivo móvel
- Desenvolvimento da estratégia de mobilidade
- Gerenciamento de dispositivos móveis e desenvolvimento de aplicativos
- Gerenciamento de segurança hospedado e no local
- Desenvolvimento de política móvel
- Suporte de Help Desk ao usuário final
- Serviços de otimização de rede, elaboração de relatórios, monitoramento e integração
- Rastreamento de conformidade e execução
- Serviços de manutenção e depósito
- Soluções corporativas de mobilidade gerenciadas são projetadas para fornecer estratégia de ponta a ponta, implementação e suporte diário

Recursos e soluções de mobilidade da IBM

IBM Mobile Enterprise Services para a mobilidade gerenciada

IBM Mobile Enterprise Services para mobilidade gerenciada é projetado para fornecer MDM avançado, estratégia e suporte a uma variedade de dispositivos e sistemas operacionais, que inclui smartphones e tablets RIM BlackBerry, Apple iOS e Google Android, assim como muitos dispositivos robustos baseados em Microsoft Windows Mobile. Podemos adquirir, instalar, configurar, executar e gerenciar os dispositivos por meio de diversas plataformas. E nós oferecemos um modelo de precificação mais flexível que é construído em torno das exigências dos seus dispositivos, das necessidades de uso e opções de serviço.

Nossos serviços de estratégia ajudam a avaliar o seu negócio e o ambiente de TI para a disposição da mobilidade e projetar um plano para gerenciamento de dispositivos móveis. A chave entre as recomendações que podemos fazer são as políticas de segurança fortes da empresa e estruturas de governança que ajudam a gerenciar as questões de conformidade, tanto dentro quanto fora da organização. A nossa estratégia de infraestrutura de mobilidade e capacidade de planejamento pode ajudá-lo a fazer escolhas adequadas com base em seus perfis de usuários e necessidades de negócio.

IBM Integrated Communications Services

Serviços de comunicações integradas concentram-se em projetar, implementar e gerenciar suas comunicações e ambientes de rede para ajudar a otimizá-los para as comunicações empresariais virtualmente unificadas “a qualquer hora, em qualquer lugar”. Essas soluções são projetadas para que você possa suportar ambientes chave de rede e construir uma vantagem diferenciada por meio da inovação empresarial.

IBM Telecom Expense Management Services

Serviços de Telecom Expense Management (TEM) pode ajudá-lo a ganhar mais rapidamente a visibilidade em seus padrões de gastos com comunicações e identificar áreas de economia a curto e longo prazo por meio de serviços de consultoria, software e gerenciamento.

IBM Mobile Foundation

A oferta IBM Mobile Foundation é projetada para reunir recursos de mobilidade chave em um único pacote integrado e ajudá-lo a lidar com toda a variedade de desafios e oportunidades que o canal móvel apresenta. O IBM Mobile Foundation oferece uma variedade de capacidades de desenvolvimento, conectividade e gerenciamento de aplicativos que suportam uma grande variedade de dispositivos móveis e tipos de aplicativos de mobilidade.

A oferta IBM Mobile Foundation inclui os seguintes produtos (que podem ser adquiridos como produtos independentes):

- IBM Worklight® para ajudar a construir, executar e gerenciar aplicativos móveis de diversas plataformas
- IBM WebSphere® Cast Iron® Hypervisor Edition para ajudá-lo a conectar aplicativos móveis em nuvem e a sistemas de "back-end"
- IBM Endpoint Manager for Mobile Devices para ajudá-lo a controlar e gerenciar dispositivos de usuário final

IBM Mobile Foundation está disponível em duas configurações:

- Enterprise Edition – Um pacote business-to-enterprise (B2E), com Worklight, WebSphere Cast Iron Hypervisor Edition e Endpoint Manager for Mobile Devices, que é utilizado pelas empresas para gerenciar aplicativos internos
- Consumer Edition – Um pacote de business-to-consumer (B2C), com Worklight e WebSphere Cast Iron Hypervisor Edition, que é usado para aplicativos comerciais e voltados para o cliente

IBM Sametime

IBM Sametime® é um software líder de mercado que pode oferecer acesso mais simples e mais transparente para as mensagens instantâneas da empresa, presença real, reuniões online, telefonia, videoconferência e muito mais – onde quer que as pessoas estejam trabalhando. O software Sametime pode fornecer uma maneira mais imediata e de baixo custo para ajudar a melhorar o envolvimento do cliente e para ajudar as equipes a tomar decisões rápidas baseadas em experiências com pessoas dentro e fora de seu negócio sem os custos de viagem.

IBM Connections

IBM Connections incorpora recursos sofisticados de análise, monitoramento de dados quase em tempo real e redes de colaboração mais rápidas, tanto dentro quanto fora da organização. Esses recursos podem ser acessados no local, no IBM SmartCloud ™ ou por meio de uma ampla variedade de dispositivos móveis. Ele integra fluxos de atividade, calendário, wikis, blogs, capacidade de email e muito mais. Ele também permite a colaboração instantânea com apenas um clique e a capacidade de construir comunidades sociais, mais ricas em segurança, tanto dentro quanto fora da organização para ajudar a aumentar a lealdade do cliente e os resultados corporativos de velocidade.

IBM Mobile Security

IBM Mobile Security pode ajudá-lo a impedir malware, proporcionar conectividade segura, oferecer acesso mais seguro a dados e sistemas corporativos, construir aplicativos mais seguros e uma plataforma de aplicativo móvel mais confiável. Nossos principais produtos de segurança incluem painéis de visualização única e funcionalidades integradas para ajudar a proteger melhor praticamente qualquer tipo de terminal ou rede, seja um smartphone, um PC, um servidor ou um roteador. Oferecemos:

- IBM Security Access Manager – para ajudá-lo a simplificar o gerenciamento de senhas, reforçar a segurança de acesso e gerenciar melhor a demonstração de conformidade
- Redes corporativas sem fio – soluções de rede seguras e robustas sem fio que podem entregar comunicações praticamente "a qualquer hora, em qualquer lugar"

- Appliance WebSphere DataPower® Service Gateway XG45 – para ativar os serviços mais seguros da web, aplicativos e dados com visibilidade e com governança de serviços customizáveis, escaláveis e automatizadas
- Hosted Mobile Device Security Management – para ajudar a proteger seus dispositivos móveis contra malware e outras ameaças, proporcionando o conhecimento, tecnologia e gerenciamento contínuo que podem tornar a segurança do dispositivo móvel praticamente "completa"
- IBM AppScan® – para fornecer testes de segurança de aplicativos e soluções de gerenciamento de riscos
- IBM Lotus® Mobile Connect – para oferecer conexões mais seguras a partir de dispositivos móveis populares para soluções corporativas hospedadas

Por que a IBM?

Por mais de 15 anos, a IBM tem fornecido soluções de mobilidade para centenas de clientes e gerenciado centenas de milhares de dispositivos móveis em todo o mundo. Através da IBM, é possível acessar uma ampla variedade de serviços e soluções inovadoras que abrangem todo o ciclo de vida do ambiente de mobilidade – desde o desenvolvimento de estratégia e implementação de gerenciamento de segurança até o suporte diário. Você também pode usar nossa grande infraestrutura global, que inclui mais de 5000 comunicações integradas e profissionais de redes, com 70 serviços de call centers no local de trabalho em todo o mundo, 9 centros de operações de segurança, 12 centros de entrega de mobilidade e de suporte e mais de 30 laboratórios de pesquisa de suporte à mobilidade.[12] E como um líder no segmento de mercado, nós podemos ajudá-lo a reduzir a complexidade, fornecendo a capacidade de suportar quase todas as suas necessidades de TI e praticamente eliminar os desafios da prestação de serviços de vários fornecedores.

A IBM oferece suporte à escolha do funcionário em dispositivos móveis

Mais da metade da população global de funcionários da IBM é remoto. A empresa precisava expandir seu programa de mobilidade corporativa – lançado em 2004, com um único dispositivo corporativo emitido – para acomodar uma variedade de novas plataformas móveis que entram no local de trabalho. Ao longo de três anos, a IBM fez um piloto de acesso de mobilidade com diferentes dispositivos e sistemas operacionais, incluindo novos equipamentos como tablets, conforme o mercado ia evoluindo. O software de colaboração IBM tornou-se parte integrante da solução. Em 2011, a implementação da produção em larga escala estava em andamento, com a mobilidade vista como um serviço de infraestrutura básica. Hoje, o programa abrange 120 mil usuários remotos, incluindo 80 mil dispositivos de propriedade pessoal, e continua a se expandir.[13]

"O programa BYOD da IBM é realmente sobre o suporte aos funcionários na forma como eles querem trabalhar. Eles encontrarão o instrumento mais adequado para fazer seu trabalho. Eu quero me certificar de que posso capacitá-los a fazer isso, mas de uma forma que proteja a integridade do nosso negócio."

– IBM CIO Jeanette Horan

Para obter mais informações

Para saber mais sobre produtos e serviços IBM para programas empresariais de mobilidade, entre em contato com seu representante IBM.

Além disso, a IBM Global Financing pode ajudá-lo a adquirir as soluções de TI necessárias ao seu negócio da maneira mais econômica e estratégica possível. Faremos parceria com clientes de crédito qualificado para personalizar uma solução financeira de TI para atender às suas metas comerciais, permitir o gerenciamento de caixa eficaz e aprimorar seu custo total de propriedade. A IBM Global Financing é a escolha mais inteligente para financiar investimentos de TI críticos e levar seu negócio adiante. Para obter mais informações, visite: **ibm.com**/financing/br

[11] Gartner, "Seven Steps to Planning and Developing a Superior Mobile Device Policy", 5 de outubro de 2011.

[12] As estatísticas estão atualizadas até novembro de 2012.

[13] As estatísticas estão atualizadas até 2012.

IBM Corporation
International Business Machines Corporation
Route 100
Somers, NY 10589 U.S.A.

Novembro de 2012

[1] IBM: "Alcançando o sucesso com um ambiente de trabalho flexível", Maio de 2012.

[2] Ibid.

[3] Gartner, "Seven Steps to Planning and Developing a Superior Mobile Device Policy," 5 de outubro de 2011.

[4] Computadores pessoais.

[5] Gartner, "O Gartner diz que os programas Traga seus Próprios Dispositivos (BYOD), anunciam a mudança mais radical para as empresas no mercado de computação desde a introdução do PC", 29 de agosto de 2012.

[6] IBM, "Achieving success with a flexible workplace", Maio de 2012.

[7] Ponemon Institute, "2011 Cost of Data Breach Study: Estados Unidos", Março de 2011.

[8] Ibid.

[9] IBM, "Alcançando o sucesso com um ambiente de trabalho flexível", Maio de 2012.

[10] Aberdeen Group, "Custos ocultos, Valor invisível", 17 de agosto de 2012.

Por favor, recicle

ENW03011-BRPT-00