Consumerização: dicas para TI gerenciar dispositivos móveis
Ryan Faas

Gestão é uma grande preocupação quando se trata de mobilidade, especialmente quando a companhia tem de lidar com dispositivos pessoais de propriedade de empregados.

Uma das maiores tendências de tecnologia este ano foi a entrada de dispositivos orientados para o consumidor no local de trabalho. De iPads e iPhones a telefones Android e tablets, 2011 ficará marcado como o ano no qual o consumo de TI alcançou uma massa crítica. Não é mais uma questão de saber se os departamentos de TI devem apoiar e abraçar o movimento 'traga seu próprio dispositivo' (Bring Your Own Device - BYOD, na sigla em inglês). Agora, a questão é mais sobre quando e como.

Os departamentos de TI têm muito a manter em mente: a identificação dos dispositivos de propriedade dos empregados na rede; a seleção de plataformas mais recomendadas para os usuários; o provisionamento de dispositivos para acesso seguro e o monitoramento centralizado (sejam eles da empresa ou de propriedade dos empregados); a criação de regras para lidar com dispositivos perdidos ou roubados; a adoção de ferramentas que facilitem a limpeza de dados corporativos nos dispositivos dos empregados; a coordenação compras em volume em lojas de aplicativos públicos (particularmente da Apple), e a publicação em apps desenvolvidas internamente.

A maioria dessas necessidades pode ser tratada com qualquer uma das muitas suites de Gerenciamento de Dispositivos Móveis (MDM, na sigla em inglês). Cada uma delas oferece um conjunto específico de plataformas suportadas, recursos e ferramentas de integração de sistemas corporativos.

Mas saber que você pode satisfazer as necessidades básicas de gestão e segurança da vasta lista de plataformas móveis em uso na empresa é um ótimo começo: o grande número e a qualidade das opções já disponíveis devem ajudar os gestores a respirar um pouco mais tranquilos. É apenas o primeiro passo de uma jornada que pode parecer ter quilômetros de distância. Os próximos passos envolve descobrir que tipo de gestão você realmente precisa, e quando. Os detalhes podem variar drasticamente de um tipo de negócio para outro e até mesmo de uma função de trabalho para outra na mesma empresa. Identificar as especificidades pode ajudá-lo a fazer a seleção e a implementação de uma estratégia mais fácil para que o MDM dê melhores resultados.

O mínimo

No nível mais básico, há três principais necessidades que devem ser padrão de qualquer estratégia móvel:

Provisionamento do dispositivo e instalação: é preciso configurar e instalar os dispositivos, os aplicativos necessários, os certificados de segurança, as contas de usuário para e-mail ou de acesso a outros recursos internos, e o acesso à rede.

Limpeza remota: a capacidade de apagar os dados é fundamental. Para os dispositivos de propriedade dos usuários, isso pode incluir a necessidade de deixar dados pessoais intactos, algo que não é tão comum quando os dispositivos são de propriedade da empresa.

Políticas de segurança: as primeiras políticas devem lidar com dispositivo de bloqueio; a requisição de uma senha, designando tempo de validade da senha e sua complexidade, autotravamento de um dispositivo quando estiver inativo, e limpeza de dados após um determinado número de tentativas falhas de desbloqueio. Políticas de segurança, muitas vezes, devem ir mais longe: exigem criptografar o dispositivo inteiro, se possível - ou, pelo menos, proteger dados específicos; configurar os serviços de VPN; limitar o acesso ao dispositivo e à plataforma padrão para a instalação de app, ou definir opções de configuração específicas, impedindo os usuários de alterá-las.

Andar na corda bamba

Em muito poucos casos, o gerenciamento dos dispositivos móveis será o mínimo suficiente. Mas o outro extremo - tudo o que você pode gerenciar - também pode não funcionar muito bem. Pode simplesmente irritar os usuários, adicionar complexidade aos processos de configuração e gerenciamento, e drenar recursos de TI.

Gestão demais é uma grande preocupação quando se trata de mobilidade, especialmente quando você está gerenciando os dispositivos pessoais de propriedade de empregados.

Há uma linha além da qual a gestão vai parecer intrusiva, e se você atravessá-la, é provável que você acabe com uma cultura em que os trabalhadores usam ativamente seus dispositivos, mas evitam deixar os gerentes ou profissionais de TI saberem que eles o fazem. Demasiada interferência percebida pode inibir os funcionários de dar, de forma voluntária, detalhes sobre seus dispositivos, os usos que fazem e se tiveram problemas que podem comprometer a segurança da empresa.

Em suma, a TI tem de caminhar em uma linha tênue, e é uma linha que pode variar muito de uma organização para outra e mesmo entre diferentes papéis na mesma empresa.

Identificação de usuários diferentes

Uma vantagem que todos os fornecedores de suites MDM abraçam é a ideia de que você vai querer gerenciar dispositivos diferentes de forma diferente. Isso não é um conceito novo - afinal, permissões de arquivos e recursos de gerenciamento de cliente são comuns no desktop.

Com isso em mente, a melhor opção é criar uma série de perfis de gerenciamento ou configurações [detalhes que podem variar dependendo do fornecedor ou plataforma, mas com conceito universal]. Você pode então gerenciar múltiplas camadas de perfis, conforme necessário, e aplicá-las variando os critérios. Este modelo é, de fato, o recomendado pela Apple para a gestão de dispositivos iOS como o iPhone e o iPad nas organizações.

Você pode, por exemplo, ter um conjunto de perfis com base na plataforma móvel e liberar o OS. Como cada nova versão dos sistemas iOS e Android ampliam os recursos de gerenciamento e segurança disponíveis para a empresa, você poderia ter acesso a alguns recursos suportados pela versão instalada do sistema operacional, como se um dispositivo pode ou não armazenar dados usando a criptografia disponível no dispositivo ou permitir a criação de perfis para os usuários que viajam e precisam de acesso a dados de roaming aplicados aos dispositivos de propriedade da empresa.

A maioria dos fornecedores de suites MDM pode ligar para soluções de diretório e de gestão já existentes, como o Active Directory. Isso permite adaptar os perfis de usuário existentes em torno do seu grupo com carcaterísticas comuns.

Embora cada organização tenha suas próprias necessidades, é possível oferecer algumas diretrizes para o nível e o tipo de uso apropriado para determinados usuários. Considere os seguintes exemplos como base de partida para desenvolver uma estratégia de gerenciamento móvel. Nota: você pode facilmente misturar e combinar vários dos exemplos em sua estratégia de mobilidade.

Completamente bloqueado: o usuário não tem capacidade de adicionar ou alterar apps, mexer com as definições de configuração, ou modificar contas de e-mail. O acesso a redes corporativas sem fio não é proibido.

Restrição de compra: o objetivo principal é evitar a adição de aplicativos móveis, particularmente aqueles que podem levar a problemas de segurança. Dependendo de propriedades da plataforma e do dispositivo, isso pode ser aplicado também para a compra e instalação de conteúdo, como na loja iTunes da Apple. Bom para dispositivos de propriedade da empresa.

Restrição de conteúdo: limita o conteúdo que pode ser acessado a partir de um dispositivo, incluindo áudio/vídeo, websites e, potencialmente, meios de comunicação social. Bom para dispositivos de propriedade da empresa, especialmente se eles estão voltados para o cliente. Por exemplo, se forem usadas como ferramenta de vendas ou de informações ou em uma sala de aula.

Definições pré-configuradas: útil, com ou sem gestão, permite configurar automaticamente serviços corporativos e contas do usuário com recursos comuns, como acesso a redes Wi-Fi, udo de VPNs, e-mail de usuário ou contas Exchange. O objetivo é fazer com que o usuário seja identificado rapidamente, para não limitar o acesso. Bom para qualquer implementação, particularmente quando um dispositivo irá alternar entre o uso pessoal e profissional.

Restrições para chamadas/mensagens/roaming: indicada principalmente para dispositivos de propriedade da empresa. A ideia é evitar sobrecarga no plano de chamadas. Idealmente, esta é determinada pelas necessidades do empregado e deve ser parte do pacote de uma empresa de serviços mais amplo.

Apps pré-instaladas: similar às definições de pré-configuração, isso garante que os aplicativos necessários - inclusive personalizados em aplicações internas ou aplicativos de uma loja pública - são pré-instalados em um dispositivo. Isso é particularmente útil se os aplicativos são comprados em volume. A abordagem requer normalmente o uso de uma solução de MDM que ofereça uma loja de aplicativos para usuários privados.

Restrição de sincronização: limitar que computadores e serviços de um dispositivo móvel possam sincronizar dados. Isso se aplica geralmente a backups no iTunes usando a iCloud, mas poderia se aplicar a outras plataformas e serviços. O objetivo é impedir a criação de um backup externo de dados da empresa. Deve ser usado para todos os dispositivos de propriedade da empresa, mas pode ser problemática para dispositovos de propriedade ddos usuários.

Acesso seguro habilitado: envolve a configuração de serviços de segurança disponíveis para garantir que os dados são transmitidos de/para um dispositivo de forma segura. Isto poderia significar a configuração de uma VPN, bem como acesso SSL para serviços como e-mail ou servidores web, com provisionamento de certificados de segurança necessários.

Serviço de nuvem habilitado: o dispositivo é pré-configurado para acesso privado ou a serviços da empresa na nuvem pública.

Restrição de acesso à nuvem pessoal: limitar ou impedir o acesso aos serviços de nuvem pessoal, incluindo a iCloud. Pode ser desafiador quando aplicada aos dispositivos de propriedade do empregado.)

Restrições de localização de dados: impedir o dispositivo de utilizar os serviços de localização inteiramente ou limitar o acesso a aplicativos que trabalham com dados de localização. Esse é um desafio particular, dada a onipresença de recursos baseados em localização em dispositivos móveis, hoje. Uma solução: criar uma lista branca de aplicativos autorizados a usar dados de localização.

Trabalhando com usuários

A gestão da mobilidade e as abordagens BYOD podem trazer novas capacidades para os profissionais e desafios para a TI . É importante perceber que a equipe de Tecnologia da Informação já não pode, sozinha, decidir sobre soluções ou a correção de problemas. A relação entre TI e usuários precisa ser colaborativa.

Parte dessa colaboração é uma operação de TI que escuta e responde às necessidades do usuário, suasideias e até mesmo críticas. O fato de que os dispositivos de propriedade pessoal

permite aos usuários usar o dispositivo sem o conhecimento da equipe de TI é um desafio que anima a trabalhar com os usuários e não contra eles.

Isso significa proporcionar educação ao usuário em áreas como segurança, gestão de custos e questões legais ou regulamentares - uma abordagem que muitas vezes ajuda a desenvolver interações mais amigáveis e ajuda os trabalhadores a entenderem e aceitarem os limites que a TI precisa impor.

Um trabalho em progresso

Em última análise, a gestão de dispositivos móveis e o apoio dos funcionários na aquisição de tecnologia são conceitos muito novos. Não há regras rígidas e rápidas, e, em muitas situações, há uma orientação limitada - interna ou externa - para trabalhar. Isso pode fazer o trabalho envolvido parecer assustador, mas também pode oferecer oportunidades para novas ideias e trabalhar de forma mais colaborativa - os benefícios podem se estender para além dessas áreas limitadas para outros projetos ou upgrades, e como eles são planejados ou considerados.

A consumerização de TI vai ganhar força em 2012. Levar os usuários e profissionais de TI a trabalharem juntos agora só vai facilitar o processo de gestão.

Fonte: **Computerworld [Portal].**
Disponível em: <http:/ / computerworld.uol.com.br/ >Acesso em 14 dez. 2011.