WHITE PAPER – **JANEIRO 2017**

REDEFINA O GERENCIAMENTO DO WINDOWS 10

Adote a verdadeira mobilidade empresarial

vmware® airwatch®

DELL

Índice

Introdução

Muitos departamentos de TI ainda são tidos como núcleos de despesa, pelo fato de suas operações estarem focadas na execução de tarefas consideradas corriqueiras – suporte contínuo a usuários, dispositivos, aplicativos e sistemas operacionais (SO).

A consumerização de TI com iniciativas do tipo BYOD (traga seu próprio dispositivo) e da nuvem móvel estão se tornando rapidamente a norma na qual as empresas estão se baseando para manter a competitividade. Isto está forçando as organizações a pensarem mais além de algo tido como básico como produtividade e colaboração do usuário e comecem a adotar iniciativas de mobilidade de negócios modernas, que exigem a reengenharia dos processos de negócios essenciais para que se adaptem ao modelo da nuvem móvel.

Com o Windows 10, a Microsoft traz ao mercado um SO móvel e pronto para a nuvem, que está prestes a ter um impacto significativo sobre as empresas no que diz respeito à estratégia dedicada à computação de usuário final (EUC). Este moderno sistema operacional oferece uma plataforma unificada para a criação de aplicativos e ampliação dos principais processos corporativos para que alcancem os usuários onde quer que estejam, independentemente de quais dispositivos Windows 10 estejam utilizando. No entanto, uma execução abrangente a nível empresarial desta visão de mobilidade de negócios apresenta seu próprio conjunto de desafios. Um estudo conduzido pela VMware em 2015, envolvendo mais de mil decisores da área de TI, identificou suas principais preocupações relacionadas à adoção de iniciativas de mobilidade:[1]

1. Redução do custo geral e da complexidade do gerenciamento
2. Garantia da segurança e do controle de dispositivos em todos os momentos
3. Diminuição do risco de perda dos dados corporativos

Com sua visão para um gerenciamento de endpoint unificado, a VMware se encontra estrategicamente posicionada para enfrentar tais desafios.

[1] VMware State of Business Mobility Report. Rep. VMware, Nov. 2015. Web. <http://www.air-watch.com/lp/vmware-state-of-business-mobility-report-2015/>.

A Solução da VMware

No âmago dessa estratégia de gestão de endpoint unificada da VMware, encontra-se a solução de gerenciamento da mobilidade empresarial (EMM) da AirWatch.

A VMware AirWatch® oferece suporte para o gerenciamento do Windows 10 e disponibiliza maneiras mais inteligentes de implementar, controlar e gerir a frota de computadores de qualquer organização. Essa solução reduz o custo total e a complexidade de gerenciamento, ao permitir que as equipes de TI consolidem as ferramentas necessárias e os painéis de gestão eliminando, assim, muitos dos problemas do gerenciamento tradicional do ciclo de vida dos computadores, como por exemplo, a necessidade de preparação e geração de imagens, a complexidade da manutenção de reguladores (drivers), o gerenciamento das atualizações de SO, firewall, antivírus e políticas de criptografia. Além disso, a AirWatch possibilita que TI controle e proteja dispositivos para os usuários através de perfis de segurança detalhados, configurações de conformidade e restrições impostas ao dispositivo. A solução também minimiza o risco de perda de dados, ao garantir que somente os dispositivos gerenciados que cumpram com as políticas de conformidade definidas pela empresa possam ter acesso a aplicativos, conteúdo e e-mail. O restante deste documento explica, em detalhes, como a solução de computação do usuário da VMware ajuda a lidar com as preocupações de uma organização no que diz repeito à adoção de iniciativas de mobilidade empresarial, particularmente no que se refere às implementações do Windows 10.

Reduza o custo geral e a complexidade do gerenciamento

O Windows 10 permite aos administradores de TI tirar proveito total das mais recentes ferramentas de gerenciamento da mobilidade empresarial (EMM). A AirWatch adota o que há de melhor nas funções tradicionais de gerenciamento do cliente e reúne os mais avançados recursos da indústria de EMM, a fim de simplificar o gerenciamento de dispositivos móveis e de desktop executando o Windows 10.

Otimize a implementação

Com a AirWatch, os administradores de TI podem simplificar de forma drástica o processo de inscrição e o provisionamento de dispositivos. A AirWatch oferece uma experiência de integração com o Windows 10 intuitiva em qualquer rede – pública (associada ao domínio em nuvem) ou privada (não associada ao domínio em nuvem) – seja em um cenário CYOD (escolha o seu próprio dispositivo), BYOD (traga o seu próprio dispositivo) ou empresarial. A AirWatch faz a integração com o Microsoft Active Directory (AD) no local e o Microsoft Azure AD na nuvem pública, sendo compatível com modelos de inscrição que usam a nuvem híbrida ou integral.

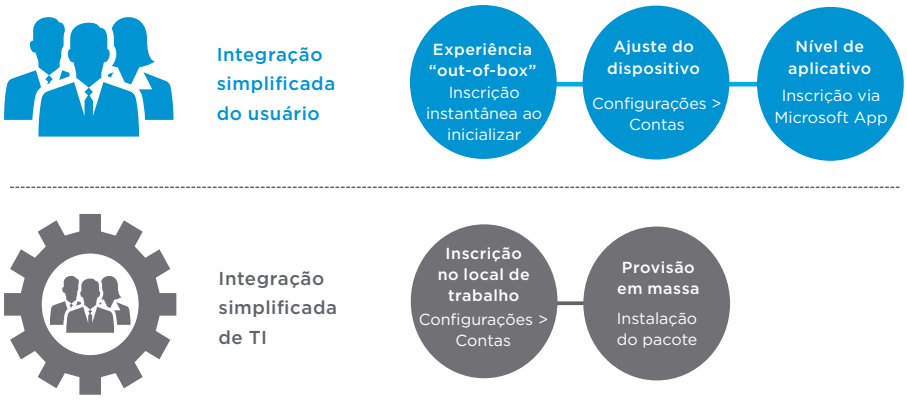

Figura 1: Casos de uso do provisionamento do Windows 10 da AirWatch

Integração simplificada do usuário

A integração com o Active Directory Azure permite que as organizações ofereçam suporte à inscrição automática do usuário sem qualquer envolvimento de TI e interação mínima do próprio usuário. A inscrição pode ser feita das seguintes maneiras:

- Com uma experiência de inscrição "out-of-box" (instantânea) ao inicializar
- Com a adição das credenciais corporativas
- Pela autenticação nos aplicativos empresarias (por exemplo: Microsoft Office)

Produtividade de TI/OpEx:

Inscrição automática do usuário com envolvimento zero de TI

Os métodos de inscrição automática usando as credenciais corporativas juntam-se aos dispositivos no domínio da nuvem e ajustam perfis, configurações, aplicativos, políticas de conformidade e conteúdo perfeitamente, bem como configuram o dispositivo para o gerenciamento pela AirWatch – tudo isso em um fluxo de trabalho otimizado.

Integração simplificada de TI

A geração de imagens e associação de domínio tradicionais sempre foram uma solução complexa e demorada para a inscrição de dispositivos. O provisionamento do tempo de execução no Windows 10 combinado com os recursos de provisionamento de produto da AirWatch permite aos administradores uma abordagem mais granular, baseada em políticas, que possibilita a inscrição de dispositivos sem a necessidade de uma nova geração de imagens para uso individual.

Produtividade de TI/OpEx:

Inscrição em massa, com um só clique, através de política sem a necessidade de uma nova geração de imagens

(Cont. de Integração simplificada de TI)

Ao utilizar a AirWatch, os administradores de TI podem importar, em massa, números de série de um dispositivo específico e mapeá-los até as contas de usuário que estão recebendo o dispositivo. A AirWatch proporciona preparo e provisionamento necessários para as URLs de serviço (detecção, registro e política), que alimenta o Designer de Configuração (ICD) e Imagens do Windows.

Combinado com seus recursos de provisionamento de produto (consulte a seção Gerenciamento do aplicativo), a AirWatch permite que TI crie um único pacote de inscrição pré-configurado, onde definições de configuração, aplicativos (incluindo EXEs e MSIs), atualizações de software, drivers, arquivos e comandos sejam distribuídos remotamente para o usuário através de e-mail ou disco de mídia, e instalado com apenas um clique. Opcionalmente, o pacote pode ser importado diretamente pelo administrador ou usuário dentro das configurações de acesso do Windows Work.

Aplicativos

- Remover Bloatware
- Instalar MSIs
- Instalar EXEs
- Instalar DLLs
- Instalar drivers
- Instalar atualizações do Windows Apps
- Implementar as chaves de licença do Windows
- Implementar scripts personalizados

Configuração

- Certificados
- E-mail
- VPN
- WiFi
- Firewall
- Anitvírus
- Criptografia
- Windows Update Client
- Restrições de aplicativos
- Adicionar contas
- Configurar o menu inicial
- Configurar o papel de parede
- Configuração de impressora

Figura 2: O pacote de provisionamento pode incluir listas de aplicativos e definições de configuração

Simplifique o gerenciamento

Dispositivos

O console da AirWatch exibe um painel de controle de dispositivo que permite aos administradores uma visão geral, rápida, e em tempo real de toda a frota de endpoints da organização – incluindo dos dispositivos Windows 10. É possível personalizar o painel de controle do dispositivo, o qual permite pesquisas e inclui funções de filtragem para que os administradores possam encontrar dispositivos específicos com base em vários critérios, como por exemplo: plataforma, versão do sistema operacional, status de conformidade, tipo de propriedade etc. O recurso de busca detalhada facilita e acelera a execução das ações de MDM e das funções administrativas em um determinado conjunto de dispositivos.

Produtividade de TI/OpEx:

Painel de controle unificado para gerenciamento e emissão de relatórios para todos os dispositivos, aplicativos e plataformas de sistema operacional

O console da AirWatch também permite uma avaliação mais rigorosa de qualquer dispositivo específico. Por exemplo, os administradores podem obter informações detalhadas sobre o status de segurança do dispositivo, ou seja, descobrir se o dispositivo Windows 10 se encontra ou não inscrito no gerenciamento, se está em conformidade com as políticas de senha e criptografia e se a postura do mesmo é de integridade, com base nas configurações definidas na declaração de integridade do dispositivo (consulte a seção Postura do dispositivo).

A AirWatch também dispõe de um extenso conjunto de relatórios pré-configurados e recursos de registro de eventos que fornecem aos administradores estatísticas direcionadas a resultados em suas implementações do Windows 10. Os administradores de TI também podem criar relatórios personalizados, definir listas de distribuição e automatizar a entrega de relatórios e cronogramas, tudo isso dentro de um único console de administração centralizado.

Inventário do dispositivo

A AirWatch apresenta recursos de inteligência de ativos embutidos no console. Os administradores de TI encontram à sua disposição vários detalhes de inventário para os dispositivos, tais como: dispositivos em grupos organizacionais próprios e com aplicativos específicos instalados, status de conexão de rede, informação sobre se o dispositivo está comprometido e muitos outros relatórios pré-configurados e detalhados.

Figura 3: Painel de dispositivos da AirWatch

Aplicativos

Um dos desafios que os administradores de TI enfrentam ao lidar com o gerenciamento de computadores é um ecossistema de aplicativos fragmentado. Com o Windows 10, as organizações já não precisam de várias ferramentas de distribuição para cada tipo de aplicativo e os administradores podem habilitar os usuários com acesso a qualquer aplicativo - seja ele um EXE ou um pacote MSI, um aplicativo da web, remoto ou universal - de uma mesma loja de aplicativos. A nova loja é compatível com aplicativos que mantêm um único código base nas plataformas do Windows: móveis e desktop. Este recurso economiza tempo para os desenvolvedores e permite que os administradores concentrem-se no gerenciamento unificado de endpoints.

(Cont. de Aplicativos)

A AirWatch permite que os gestores implementem um catálogo de aplicativos unificado, para que os usuários possam acessar aplicativos corporativos aprovados a partir de um único local. As políticas de configuração de aplicativos da AirWatch garantem também que apenas aplicativos confiáveis executem nas máquinas dos usuários (consulte a seção Grupos de aplicativos).

Produtividade de TI/OpEx:

Instalação automática de aplicativos pelo usuário

A integração com o VMware® Identity Manager, que é uma solução de infraestrutura como serviço (IaaS), permite que a equipe de TI tenha controle e acesso seguro a aplicativos empresariais com uma disposição apropriada ao acesso de um toque para os usuários que estejam utilizando esses aplicativos em qualquer lugar e em qualquer dispositivo (consulte a seção Login único).

O VMware AirWatch® App Catalog™ integra-se completamente com a Microsoft Store e permite a instalação automática de aplicativos que são atribuídos ao usuário com base na plataforma, grupo de usuários, função e muito mais. O mesmo permite que desenvolvedores e administradores visualizem as estatísticas de instalação dos aplicativos, coletem avaliações/comentários, enviem notificações de atualizações, instalem aplicativos nos dispositivos dos usuários de forma silenciosa e criem uma identidade visual personalizada, bem como categorias para o catálogo. É possível enviar o AirWatch App Catalog para dispositivos automaticamente durante o fluxo de trabalho da inscrição do Windows 10 ou, sob demanda, como um web clip.

Com a criação da Windows Store for Business, a Microsoft proporciona a desenvolvedores, decisores e administradores um local onde podem enviar, encontrar, adquirir, gerenciar e distribuir aplicativos do Windows 10 para suas organizações. A AirWatch está muito feliz em trabalhar em conjunto com a Microsoft no sentido de integrar com a Windows Store for Business para que os administradores possam acessar, implementar e usar aplicativos do Windows 10 em suas respectivas empresas.

Provisionamento de produto

A AirWatch possibilita a entrega remota de aplicativos, arquivos e comandos através de "perfis de produto". Os recursos de provisionamento de produto da AirWatch permitem que os administradores enviem aplicativos, drivers, atualizações de firmware, pacotes complexos ou scripts para que seus desktops corporativos, executando Windows, mantenham-se atualizados e sempre prontos para o uso. Os administradores podem simplificar ainda mais as tarefas de provisionamento de produto e distribuição de software através da criação de horários automatizados e fluxos de trabalho para a instalação, que também podem ser configurados para instalar - dependendo de certas condições - tais como: rede, cronograma ou potência. A AirWatch é totalmente compatível com a instalação básica de MSIs, indo mais além, ao apresentar um mecanismo de script de automação de tarefas tradicional, o qual oferece recursos que normalmente exigiriam uma ferramenta de gerenciamento de ciclo de vida do PC (PCLM). Isso permite que os administradores escolham os melhores recursos PCLM tradicionais, quando de sua transição para o novo EMM baseado em fluxo de gerenciamento.

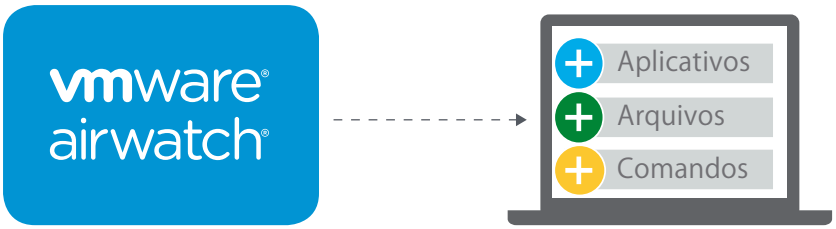

Figura 4: O provisionamento de produtos da AirWatch

Inventário do aplicativo

A AirWatch é compatível com cobrança, emissão de relatórios e controle de inventário integral para Windows Desktop (legado) e aplicativos do Metro (moderno). Os administradores de TI podem visualizar relatórios pertinentes ao status da implementação, às versões dos aplicativos e à presença dos mesmos em dispositivos selecionados, bem como uma lista de aplicativos com seus respectivos custos. Podem também acessar muitos outros recursos de inventário de aplicativos.

Suporte ao Office 365

Para as organizações que usam o Microsoft Office 365, a AirWatch e o VMware Identity Manager facilitam e automatizam o processo de provisionamento de acesso para os vários aplicativos do Office 365, ao sincronizar com os grupos de usuários de serviços de diretório (LDAP) existentes. Tal integração garante uma identidade comum para autenticação e acesso condicional aos aplicativos, para que somente usuários autorizados - em dispositivos gerenciados e com licenças adquiridas - tenham permissão para acessar os vários serviços do Office 365.

E-mail

Produtividade de TI/OpEx:

Suporte e gerenciamento centralizado para várias infraestruturas de e-mail

A AirWatch oferece recursos abrangentes para o gerenciamento do e-mail do Windows 10, com o objetivo de proteger e oferecer suporte à infraestrutura de e-mail corporativo de qualquer organização, permitindo que apenas usuários e dispositivos em conformidade tenham acesso ao mesmo. A AirWatch é compatível e permite o acesso no próprio cliente de e-mail nativo (Microsoft Outlook) ou através do uso do aplicativo VMware AirWatch® Inbox™, possibilitando, também, a implementação de várias configurações de gerenciamento de e-mail[2] dentro da mesma empresa, incluindo o Exchange Online e o Office 365. Isso permite que os administradores de TI centralizem o gerenciamento de distintos ambientes de e-mail através de ramificações ou grupos de usuários e ofereçam suporte a cenários de atualização ou migração, onde uma parcela dos endpoints esteja em um ambiente diferente.

Conteúdo

O VMware AirWatch® Mobile Content Management ajuda as organizações a disponibilizar e permitir acesso seguro ao conteúdo em todos os dispositivos Windows, sejam eles desktop ou móveis. Os profissionais de TI podem configurar e fazer o upload de conteúdo gerenciado no console, sincronizar servidores de arquivos corporativos (por exemplo, Microsoft SharePoint, Microsoft OneDrive, compartilhamentos de rede etc.) e também habilitar espaço para conteúdo pessoal dos usuários, os quais podem acessar e compartilhar dados de forma segura, usando o VMware AirWatch® Content Locker™.

[2] Windows Desktop: Exchange Server, Exchange Online, Office 365; Windows Phone: Exchange Server, Exchange Online, Office 365, Lotus Traveler, Novell GroupWise, Google Apps for Work.

Funções de cliente tradicionais

Os métodos tradicionais de gerenciamento dos computadores Windows dependem em grande escala dos objetos de política de grupo (GPO), os quais exigem que os dispositivos estejam conectados à rede corporativa e precisem reiniciar a fim de obter políticas. Além disso, as organizações muitas vezes exigem uma infraestrutura de gestão baseada em EMM separada, dedicada à proteção e ao gerenciamento de seus endpoints móveis e àqueles que não estão executando o Windows.

CapEx/Infraestrutura:
Consolide ou elimine licenças para ferramentas de gerenciamento de PC tradicionais

Com o Windows 10, no entanto, percebemos uma transição fundamental dos GPO para o gerenciamento de plataforma baseado em EMM. Administrados pela AirWatch, os dispositivos Windows 10 podem ser configurados com atualizações feitas de maneira remota e sem fio (over-the-air) e em tempo real, em qualquer rede pública ou privada. A AirWatch também oferece suporte a configurações nativas do sistema operacional para criptografia, antivírus, malware e firewall, eliminando a necessidade de aquisição e compatibilidade com software e agentes de terceiros. A AirWatch permite, ainda, a coexistência do tradicional gerenciamento baseado em GPO com a atual abordagem baseada em EMM, para que os administradores não sejam forçados a escolher entre uma e outra. Ao reunir o que há de melhor na tradicional gestão do ciclo de vida do PC (PCLM) e em EMM, a AirWatch objetiva elevar a produtividade, reduzir custos e melhorar a segurança dos endpoints.

Atualizações

O Windows 10 apresenta um novo serviço de atualização que foi concebido com a mobilidade e a nuvem em mente. O mesmo transforma a noção de melhoria do sistema operacional a partir de um modelo de “limpar e substituir” para um onde atualizações periódicas do SO são enviadas de maneira remota e sem fio (over-the-air). Essa nova versão atualizada do Windows como um serviço também oferece planos de manutenção ou atualização de ramificações, que permitem aos administradores controlar o cronograma de implementação com base na abordagem preferencial da empresa, bem como sua receptividade aos updates de segurança e recursos. Tais mudanças indicam que as organizações exigem agora uma ferramenta de gerenciamento baseada na nuvem para se manter à frente dos novos recursos de atualização.

(Cont. de Atualizações)

A AirWatch oferece controle granular sobre como as atualizações do Windows são gerenciadas e disponibilizadas para toda a organização. O administrador de TI pode escolher dar acesso para que os usuários controlem as atualizações do sistema operacional por conta própria ou optar por aplicar as atualizações do dispositivo através de assinatura nas fontes de atualização do Windows. A AirWatch integra-se com o novo serviço de atualização da Microsoft e também é compatível com o Windows Server Update Services (WSUS) empresarial, que já exista na organização.

Produtividade de TI/OpEx:

Elimine a complexidade de gerenciamento de atualizações, patches, drivers e outras tarefas tradicionais associadas ao ciclo de vida do PC

Os administradores podem definir políticas sobre como as atualizações são enviadas para o dispositivo, seja automaticamente ou autorizadas pelo usuário, bem como definir janelas de manutenção - tais como dia e hora preferidos para a instalação - para que as atualizações não interfiram com a produtividade do usuário. A AirWatch oferece também opções que permitem selecionar se as atualizações para outros produtos da Microsoft e de terceiros podem ser instaladas simultaneamente com as do Windows, e se as compilações do programa Windows Insider devem ser enviadas ou não para os usuários. A AirWatch também é compatível com o novo recurso de otimização de entrega de atualizações para transferências do tipo “peer-to-peer” do Windows 10. Assim, os usuários recebem atualizações e aplicativos mais rapidamente.

Antivírus e Malware

Os administradores também podem gerenciar políticas para o antivírus nativo Windows Defender e criar políticas de conformidade provenientes da AirWatch. Também é possível habilitar o monitoramento em tempo real, estabelecer atualização de definições e janelas de digitalização, adicionar exclusões, escolher ações automáticas através de níveis de ameaça diferentes e definir várias outras políticas avançadas de monitoramento e verificação. Além das políticas nativas do Windows Defender, os administradores podem configurar regras de conformidade para as soluções antivírus de terceiros assegurando, assim, a ativação do monitoramento e a atualização das definições de vírus e dos arquivos de assinatura.

Firewall

As políticas de firewall vigentes para redes privadas e públicas são outras funções de gerenciamento de cliente tradicionais que agora podem ser geridas de forma mais eficiente através do console da AirWatch.

Criptografia

A AirWatch possibilita a configuração de políticas de criptografia BitLocker para que as organizações possam, de forma silenciosa, criptografar um disco inteiro ou apenas a partição do sistema operacional. Os administradores podem caucionar a chave de recuperação do BitLocker dentro do console da AirWatch, bem como o Portal Self-Service (SSP) do usuário – como parte da permissão de um novo modelo de serviço automático que reduz a carga sobre a equipe de TI.

Habilite o serviço automático para o usuário

A AirWatch também permite uma série de recursos automáticos para o usuário, os quais diminuem ainda mais a carga sobre os profissionais de TI quando da assistência a usuários e clientes, permitindo que se concentrem em tarefas de capacitação mais relevantes.

Portal Self-Service (SSP)

Além da inscrição automática do dispositivo por parte do usuário e da instalação de aplicativos e atualizações, a AirWatch permite que os administradores configurem o Portal Self-Service (SSP), o que ajuda a mitigar o nível de suporte oferecido por TI e diminui a quantidade de pedidos de assistência, capacitando os usuários para que monitorem e gerenciem remotamente seus próprios dispositivos. Os usuários podem apagar dados empresariais de seus dispositivos, visualizar a chave pessoal de recuperação do BitLocker, enviar mensagens, bem como executar muitas outras tarefas de gerenciamento de dispositivo por conta própria através do Portal Self-Service. A tabela abaixo lista as tarefas compatíveis com o SSP para dispositivos Windows móveis e desktops:

Produtividade de TI/OpEx:

A gestão self-service por parte do usuário reduz as chamadas ao serviço de assistência e a sobrecarga de TI

Ações:	Apagar dispositivo	Coletar dados	Apagar dados do dispositivo	Apagar dados corporativos	Bloquear dispositivo/tela	Localizar dispositivo	Enviar mensagem	Baixar o Agent	Recuperar a chave do BitLocker	Apagar inscrição	Visualizar a mensagem de inscrição	Reenviar mensagem de inscrição	Gerar token de aplicativo	Revogar token de aplicativo	Gerenciar e-mail	Revisar Termos de Uso	Carregar certificado de S/MIME
Windows Desktop	X	X		X	X		X	X	X	X	X	X	X	X	X	X	X
Windows Mobile	X			X	X	X	X			X	X	X	X	X	X	X	X

Tabela 1: Recursos do Portal Self-Service (SSP) da AirWatch para dispositivos Windows 10

Proteja e controle dispositivos Windows 10

A proteção de dispositivos Windows 10 móveis e desktops começa com registro dos endpoints sob gerenciamento do EMM. Isso garante que apenas os endpoints gerenciados consigam ter acesso a aplicativos, recursos e repositórios corporativos. Após a inscrição do dispositivo, a AirWatch permite a configuração de perfis de segurança, políticas de conformidade e restrições, o que proporciona um maior controle e segurança e garante que os dispositivos não sejam adulterados.

Perfis de dispositivo

Os perfis de dispositivo são os principais meios para gerenciamento e proteção de dispositivos usados pela AirWatch e contêm os payloads (ajustes, configurações e restrições) que as organizações desejam impor aos seus dispositivos Windows 10. Esses payloads ajudam os administradores a definir políticas que atenuam os principais problemas associados à garantia de identidade/acesso (ex. código de acesso, credenciais e Passport for Work); dados (ex. proteção de dados e criptografia) e proteção contra ameaças (ex. antivírus e firewall) para os usuários de dispositivos Windows 10.

Com a AirWatch, os administradores podem construir perfis tanto para dispositivos móveis como desktops do Windows 10 e atribuí-los a grupos inteligentes específicos — que são grupos personalizáveis definidos pelo administrador e que determinam quais plataformas, dispositivos e usuários recebem aplicativos, políticas de conformidade e perfis. A tabela 2 identifica os payloads de perfil dos dispositivos Windows aos quais a AirWatch oferece suporte.

Payloads	Código de acesso	Wi-Fi	VPN	Credenciais	Restrições	Proteção de dados	Passport for Work	Firewall	Modo aplicativo único	Antivirus	Criptografia	Atualizações do Windows	Web Clips	EAS	SCEP	Controle de aplicativos	Serviços web do Exchange	E-mail	Acesso atribuído	Configurações personalizadas
Windows Desktop	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x
Windows Mobile	x	x	x	x	x	x	x		x		x	x		x	x	x		x	x	x

Tabela 2: Payloads da AirWatch para dispositivos Windows 10

Restrições para o dispositivo

Os perfis dos dispositivos Windows 10 (móveis e desktops) na AirWatch também incluem opções que permitem a habilitação de um grande número de restrições a nível de dispositivo, destinadas a um maior controle através do MDM. Os administradores de TI podem agora definir restrições em torno de:

Proteção/Controle: Controles granulares para restrições a nível de aplicativo e dispositivo

- Administração do dispositivo: por exemplo, permitir que os usuários inscrevam ou redefinam seus dispositivos
- Segurança e privacidade: por exemplo, permitir o uso de serviços de localização ou dados de telemetria
- Configurações de dispositivos: por exemplo, permitir que os usuários alterem as configurações de data e hora ou de idioma
- Funcionalidade do dispositivo: por exemplo, permitir a utilização da câmera, Bluetooth e Cortana
- Aplicativos: por exemplo, permitir somente a utilização de aplicativos confiáveis e atualizações automáticas
- Rede: por exemplo, permitir dados celulares em roaming e conexão automática com as configurações de Wi-Fi
- Navegador: por exemplo, permitir o preenchimento automático de formulários para navegador, cookies e pop-ups

Grupos de aplicativos

A AirWatch é compatível com perfis de controle de aplicativos para o Windows 10, permitindo que os administradores criem regras para aplicativos aprovados e os não aprovados para, assim, impedir que os usuários baixem e instalem aplicativos não aprovados de uma loja pública. As políticas de AppLocker podem ser provisionadas para bloquear o uso de outros aplicativos instalados anteriormente que são restritos, conforme definido pela configuração do controle de aplicativos.

Mecanismo de verificação de conformidade

Proteção/Controle:

Mecanismo de verificação de conformidade em tempo real com políticas automatizadas de escalonamento

A AirWatch oferece um mecanismo de verificação de conformidade em tempo real que garante que todos os dispositivos respeitem as políticas de gerenciamento e controle definidas pelo administrador de TI. Essas políticas de segurança são específicas para cada tipo de plataforma e englobam vários critérios de conformidade, como por exemplo: perfis de dispositivo (senha, antivírus e criptografia); lista de aplicativos (aprovados, não aprovados e necessários), status de comprometimento (integridade do dispositivo) e outros identificados na tabela abaixo. Os administradores também podem configurar regras de escalonamento automatizadas que executam ações específicas, tais como notificação do usuário e bloqueio ao acesso a aplicativos. Essas normas permitem, ainda, períodos de carência quando se determina que um dispositivo está fora de conformidade. As regras de escalonamento automático reduzem a sobrecarga de TI com a tarefa de monitorar periodicamente toda a frota de dispositivos para constatar se está em conformidade. Também aumentam a postura geral de segurança, garantindo que apenas dispositivos em conformidade tenham acesso a dados e aplicativos empresariais.

Políticas de conformidade:	Status do antivírus	Status de comprometimento	Dispositivo visto pela última vez	Criptografia	Status do Firewall	Aceitação dos Termos de Uso	Modelo	Versão do SO	Código de acesso	Roaming	Alteração do cartão SIM	Status da atualização automática do Windows
Windows Desktop	x	x	x	x	x	x		x	x	x		x
Windows Mobile			x	x		x	x	x	x		x	

Tabela 3: Políticas de conformidade da AirWatch para dispositivos Windows 10

Postura do dispositivo

A declaração de integridade do dispositivo no Windows 10 verifica o status de inicialização (ex. inicialização segura e versão do gerenciador de inicialização) e o status de segurança (ex. BitLocker e proteção do dispositivo), com o objetivo de auxiliar a identificar se o dispositivo está comprometido. O console da AirWatch permite que os administradores escolham atributos específicos da declaração de integridade do dispositivo para poder marcar o dispositivo como comprometido. O mecanismo de verificação de conformidade analisa para saber se algum desses atributos falhou e, então, age de acordo com o definido pelo administrador. Já que a AirWatch obtém as informações da declaração de integridade do dispositivo diretamente do Trusted Platform Module (TPM) – um componente de hardware criptografado incorporado no dispositivo – em vez do sistema operacional, a detecção do comprometimento funciona mesmo se o kernel do SO estiver comprometido.

Proteção/Controle:

Uma combinação de controles de hardware e software para verificar a postura do dispositivo

Figura 5: Declaração de integridade de dispositivos Windows 10

Autenticação

Senhas e nomes de usuários podem ser esquecidos, compartilhados ou usados de forma irregular (ex. a técnica de hacking conhecida como “pass the hash”), colocando dados corporativos em risco. O Windows 10 reúne uma combinação de autenticadores e hardware sólidos e segurança baseada em virtualização (proteção de credenciais). Com a AirWatch, os administradores podem estabelecer políticas de autenticação definidas especificamente para o Windows 10, as quais atenuam o risco das credenciais serem exploradas e põem fim aos ataques do tipo “pass the hash”.

Autenticação multifator (MFA)

O Windows 10 apresenta o Microsoft Passport - uma autenticação multifator (MFA) incorporada ao sistema operacional e substituições de nível empresarial que oferecem uma proteção maior para senhas. A AirWatch integra-se com os novos recursos de segurança do Windows 10: o Windows Hello (autenticação com base em biometria) e o Passport PIN. Com a AirWatch, é possível definir políticas para gestos de verificação de usuário, configurar os requisitos de resistência e complexidade do número de identificação pessoal (PIN), bem como provisionar certificados para identificar usuários.

Proteção/Controle:

Compatibilidade com MFA e SSO para maior segurança de autenticação

Login Único (SSO)

O SSO garante que os usuários efetuem o login em seus dispositivos uma única vez para acessar todos os aplicativos da organização recomendados e que se encontram disponíveis, sem que precisem voltar a fazer o login outras vezes. O VMware Identity Manager, uma solução baseada em nuvem, possibilita a integração dos serviços de diretório locais para implementações no local (LDAP), usando asserções SAML para federar identidade para a nuvem. A identidade federada permite o SSO em todos os aplicativos do Windows 10 – incluindo SaaS, Office 365, Outlook e os móveis. Além de reduzir o número de chamadas relacionadas a “senhas esquecidas”, o recurso de login único oferece maior segurança, pois os usuários já não precisam armazenar/arquivar senhas em lugares onde possam ser comprometidas; com o acesso a todos os aplicativos podendo ser facilmente desligado para evitar o vazamento de dados no caso do empregado deixar a empresa.

Minimize o risco de perda de dados

A segurança é a base de todos os aspectos da estratégia de prevenção de perda de dados e do gerenciamento de mobilidade da AirWatch. A proteção de dados nos endpoints do Windows 10 começa com a garantia de acesso seguro aos próprios servidores de aplicativos, para que apenas os aplicativos gerenciados e os usuários autorizados possam ter acesso a tais servidores. Com a AirWatch, os administradores de TI podem definir políticas de prevenção de perda de dados avançadas nos dispositivos Windows 10, com o objetivo de controlar e proteger os dados da empresa, ao mesmo tempo em que administram os cuidados com a privacidade dos dados pessoais dos funcionários. O VMware Identity Manager integra-se com os recursos de gerenciamento de mobilidade corporativa da AirWatch, a fim de proporcionar um maior rendimento à empresa. Essa solução integrada também minimiza o risco de perda de dados, ao garantir que apenas os dispositivos gerenciados que cumpram com as políticas de conformidade definidas pela empresa possam ter acesso a aplicativos, conteúdo e e-mail.

VPN por aplicativo (Per-App VPN)

As organizações podem empregar gateways de VPN para assegurar conexões seguras provenientes dos endpoints. Vale salientar, no entanto, que as VPN de nível de dispositivo não conseguem distinguir entre aplicativos empresariais, pessoais e não autorizados em um endpoint e, portanto, vão permitir o fluxo de tráfego entre o dispositivo e o centro de dados durante o tempo em que a conexão estiver ativa.

CapEx/Infraestrutura:

Elimine a necessidade de serviços e licenças de VPN de terceiros

Os recursos de VPN por aplicativo da AirWatch permitem segurança a nível de aplicativo com micro-segmentação no lado do cliente, garantindo que apenas os usuários habilitados, com aparelhos validados, e usando aplicativos autorizados estejam acessando a conexão do centro de dados quando quer que seja. Usando o perfil de VPN do Windows 10, os administradores podem escolher aplicativos específicos que têm permissão de acesso a recursos corporativos, os quais podem ser endereços IP, portas ou locais de intranet - do tipo SharePoint. Os recursos de VPN por aplicativo impedem o acesso a dados corporativos através de qualquer outro aplicativo desprotegido ou não confiável. O VMware AirWatch® Tunnel™ – um serviço de VPN incorporado – elimina a necessidade de se utilizar terceiros e uma taxa extra de licenciamento, garantindo que o serviço de VPN seja distribuído com um custo total de propriedade (TCO) mais baixo. Além de apoiar um serviço de VPN nativo, a AirWatch também se integra com serviços de VPN existentes nas organizações.

Figura 6: O App Tunnel da AirWatch e VPN por aplicativo

Acesso condicional

A integração com o VMware Identity Manager permite que os administradores concedam acesso condicional aos recursos da empresa com base no fato de o dispositivo se encontrar ou não sob gerenciamento e dos requisitos de conformidade estarem sendo cumpridos. O mecanismo de verificação de conformidade da AirWatch avalia continuamente para saber se o dispositivo está em concordância, com base em critérios de atribuição de perfil de conformidade sólidos (segundo identificado na tabela 3) para controlar o acesso a qualquer aplicativo (móveis, desktop, SaaS e universal); diversos repositórios de dados (através do AirWatch Content Locker); várias implementações de e-mail e qualquer tipo de dispositivo.

Quando o acesso a recursos corporativos é solicitado pelo usuário, o VMware Identity Manager valida se o dispositivo se encontra sob gerenciamento e concordância, segundo relato do mecanismo de verificação de conformidade. Os controles de acesso adaptáveis são compatíveis com a autenticação baseada em reivindicação, a qual pode estar dependente de usuários ou grupos, tipo de dispositivo, tipo de aplicativo, gerenciamento de dispositivos e rede (domínio). As políticas de acesso condicional também se estendem para o Exchange Online ou configurações EAS.

Prevenção contra a perda de dados

Os administradores de TI podem impor recursos avançados de prevenção de perda de dados, os quais impedem que os usuários copiem/colem e abram anexos ou arquivos empresariais fora do contêiner seguro (AirWatch Content Locker). O VMware AirWatch® Mobile Content Management™ possibilita a criptografia a nível de documento, permite a criação de autorizados e não autorizados com base nos tipos de arquivo e protege dados em trânsito e em repouso, ao fazer uso da criptografia de 256 bits AES. Além disso, os recursos de gerenciamento de e-mail da AirWatch evitam o vazamento de dados de e-mail corporativo, ao assegurar que os anexos de e-mail e hiperlinks sejam abertos somente no interior de um contêiner seguro, em um navegador gerenciado ou em uma caixa de correio sob gestão.

Proteção/Controle:

Uma postura de segurança de ponta a ponta melhor, com micro-segmentação no lado do cliente, acesso condicional e prevenção de vazamento de dados

Proteção de Dados Empresariais (EDP)

Além de recursos de prevenção de perda de dados nativos, a AirWatch está muito feliz em fazer parceria com a Microsoft para oferecer suporte a recursos de proteção de dados empresarias (EDP) para as organizações que participam do programa Microsoft TAP e certas compilações do Windows Insider. Os recursos de EDP da AirWatch para a compilação do Windows Insider, permitem que os administradores designem áreas de trabalho confiáveis ou aplicativos modernos, os quais têm permissão para abrir ou descriptografar dados corporativos. Os administradores podem configurar limites protegidos da empresa – intervalos de IP, nomes de domínio ou servidores proxy – que são locais seguros para os dados corporativos. Qualquer informação recolhida de dentro da empresa por aplicativos confiáveis será criptografada. Níveis de execução flexíveis na AirWatch podem permitir ou impedir determinados grupos de usuários de mover dados e compartilhar recursos, tais como: copiar/colar, arrastar e soltar etc.

Resumo

A mobilidade corporativa está se transformando rapidamente em um espaço de trabalho digital que capacita funcionários ao disponibilizar conjuntos de ferramentas ideais – dispositivos com os quais se mostram mais familiarizados, processos de transformação de negócios e acesso a dados e recursos – para que desempenhem bem suas funções. Ao passar de um sistema operacional centralizado em PC (legado) para um outro, moderno, agnóstico, que independe de dispositivo, o Windows 10 apresenta oportunidades para que as organizações adotem cenários de mobilidade corporativa palpáveis, que apóiam administradores, desenvolvedores e usuários sem distinção:

- Ao adotar o gerenciamento de mobilidade empresarial (EMM) como a ferramenta ideal de gestão, o Windows 10 permite que os administradores de TI ofereçam suporte eficiente a vários tipos de dispositivos e casos de uso de propriedade.
- Uma plataforma universal de aplicativos permite aos desenvolvedores criar ou reformular os processos de negócio das organizações usando uma base de código único, que implementam nos dispositivos dos usuários através de uma interface unificada.
- O sistema operacional foi projetado para funcionar perfeitamente em toda essa área de trabalho unificada, bem como na plataforma de dispositivos móveis, proporcionando aos usuários uma experiência de produtividade consistente em qualquer lugar, ainda que em trânsito.

Ao passo que as empresas miram o futuro da mobilidade de negócios, seus líderes descobrem a necessidade adotar uma solução coesa, construída especificamente para tal propósito, a qual proporcione uma experiência "simples para o consumidor, segura para a empresa" para todas as partes interessadas envolvidas. As soluções de computação para usuários da VMware, são construídas especificamente para enfrentar os desafios mais comuns relativos à adoção das iniciativas de mobilidade. Tendo o VMware AirWatch® Enterprise Mobility Management™ e o VMware Identity Manager como carros-chefe, essa solução de gerenciamento de endpoint unificada reduz o custo e a complexidade de gestão da frota de dispositivos Windows 10 das organizações, propicia controle granular para garantir a fiscalização e a segurança de endpoints e habilita recursos avançados de prevenção de perda de dados.

Recursos Adicionais

Para mais informações, visite o site www.air-watch.com/br/solucoes/plataforma.

Para começar o seu teste gratuito da AirWatch, visite o site www.air-watch.com/lp/free-trial.

Para obter mais informações, visite www.dell.com/datasecurity ou entre em contato conosco através do e-mail DataSecurity@Dell.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com