CMT vs. MDM/EMM

QUEM VENCERÁ?

Em um corner, temos a client management tool (CMT). Forte e robusta, ela dá à TI a visibilidade e o controle dos servidores e dos sistemas operacionais (SOs) da organização. A CMT tem sido uma campeã do gerenciamento de TI, responsável por grande parte do inventário e da aplicação de correção concluídos nas últimas décadas. A CMT também permite a detecção de vulnerabilidades e ataques nos *endpoints* e ajuda os administradores de TI a eliminá-los.

No outro corner, vemos o gerenciamento de dispositivos móveis/gerenciamento de mobilidade corporativa (mobile device management – MDM/enterprise mobility management – EMM). O MDM foi criado para gerenciar smartphones e tablets na empresa. O EMM foca em maximizar a segurança e a produtividade simultaneamente. Ele subiu rapidamente nos *ranks* ao habilitar aplicativos (apps), documentos e conteúdo para os usuários. Ao dar suporte para *bring your own device* (BYOD), o EMM reduz os custos e aumenta a satisfação dos usuários.

ROUND 1 — SUPORTE DE DISPOSITIVOS E OS

Ao toque do gongo, ambos os oponentes estão fortes nos seus corners.

O CMT dá um golpe forte com seu suporte para servidores, Linux, UNIX e Microsoft Windows – então um leve jab com suporte limitado para Apple macOS.

O MDM/EMM, um canhoto, então pega o CMT com a guarda baixa com suporte para Apple iOS, Google Android, macOS e Windows.

Conforme o round chega ao fim, temos um empate. As vaias são imediatamente ouvidas do público, uma vez que nenhum dos oponentes parece conseguir gerenciar wearables e dispositivos da Internet das coisas (IoT).

ROUND 2 — REGISTRO DE USUÁRIO E DISPOSITIVO

O CMT mostra seu tamanho para começar o round, ostentando inscrição de agente peso-pesado com pacotes tradicionais do Microsoft Win32 e Mac PKG/DMG. Adotando uma abordagem mais prática à instalação que seu oponente, o CMT gosta de ser instalado manualmente via sneakernet, USB ou site de download. Uma grande vantagem é a habilidade de ser integrado e incluído como *ghost* em uma imagem de OS.

Enxuto e ágil, o MDM/EMM dança com seu oponente peso-pesado, livre das exigências de registro em domínio. Os usuários e seus dispositivos podem ser instalados diretamente over-the-air (OTA) e raramente precisam de intervenção da TI. Mostrando sua velocidade, o MDM/EMM pode dar suporte a programas de inscrição de dispositivo de suporte, inscrição sem necessidade de configuração e implementação sem interação para tornar a configuração da empresa uma tarefa muito fácil. Continuando a acumular os jabs, o MDM/EMM integra-se à infraestrutura existente, como Microsoft Active Directory/protocolo LDAP (AD/LDAP).

Para terminar o round, o CMT é golpeado pelas opções de inscrição de interface de programação de aplicativos (API) e baseadas em aplicativo do MDM/EMM.

Enquanto os oponentes voltam para seus corners, MDM/EMM parece estar assumindo a liderança.

ROUND 3 — APLICATIVOS E CONTEÚDO

CMT e MDM/EMM entram no round dando golpes e com muito contato. Ambos podem distribuir aplicativos, documentos e arquivos.

MDM/EMM amplia seu alcance um pouco mais com opções de distribuição para smartphones e tablets. Ele continua aproveitando o momento ao oferecer aos usuários acesso a repositórios de conteúdo criptografados, além de suporte a compartilhamentos de arquivo de terceiros, como o Box. Além disso, conecta-se com lojas de aplicativos públicas para facilitar a distribuição e a acessibilidade de aplicativos.

O público está de pé. Está tentando descobrir qual oponente permitirá conexão única (SSO) para aplicativos na nuvem e web via desktop e dispositivos móveis para assegurar acesso rápido, intuitivo e seguro.

ROUND 4 — ATUALIZAÇÃO DE VERSÃO E ATUALIZAÇÃO

A CMT envia correções Microsoft, macOS e de terceiros por push, bem como configuração do cliente, mudanças de registro e ações baseadas no cliente. Adicionar pacotes de software personalizados para um impacto ainda maior.

Tomando uma surra nas cordas, o MDM/EMM pode realizar algum gerenciamento de correção. Porém, está limitado pelas restrições da plataforma de OS móvel. O CMT, por sua vez, é otimizado para gerenciamento de PC e Mac tradicional.

O CMT está machucado, mas de alguma maneira superou o MDM/EMM no round 4.

ROUND 5 — SEGURANÇA E CUMPRIMENTO DE POLÍTICA

Entrando no round final, ambos os oponentes ainda têm cartas na manga, com a habilidade de detectar dispositivos fora de conformidade e realizar ações em tempo real.

O CMT percebe a ameaça, entende-a e age – concentrando-se mais na segurança e na conformidade de servidores, laptops e desktops. Instilando confiança no cliente, o CMT dá suporte a regulamentos de privacidade e dados populares, como Center for Internet Security (CIS), Defense Information Systems Agency Security Technical Information Guides (DISA STIGs), United States Government Configuration Baseline (USGCB) e Payment Card Industry Data Security Standards (PCI-DSS).

MDM/EMM prevê problemas com dispositivos móveis, definindo políticas específicas para tentar contrapor-se a qualquer elemento que afete o seu ambiente.

Do nada, o MDM/EMM acerta um golpe arrasador, apresentando um contêiner protegido para e-mails, contatos, calendários, bate-papo e navegador seguro também – uma verdadeira vantagem para uma loja BYOD ao preservar a privacidade do usuário enquanto separa dados pessoais e profissionais.

Ambos os oponentes voltam para seus corners esgotados e feridos. Algumas vaiais e incentivos são escutados enquanto o CMT recebe um "V" para o round. Muitos estão gritando que é uma decisão questionável.

O RECÉM-CHEGADO

GERENCIAMENTO UNIFICADO DE *ENDPOINT*

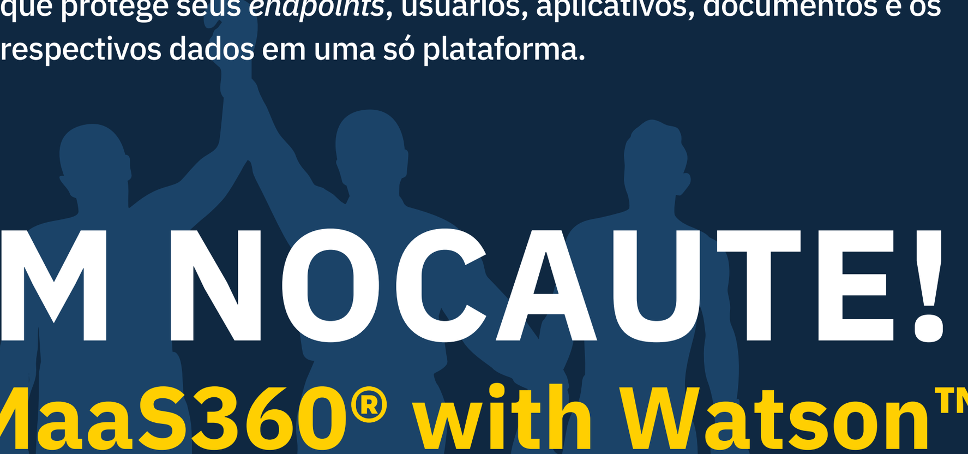
O gerenciamento unificado de *endpoint* (unified endpoint management – UEM) entra no ring para resolver o empate.

Ele possibilita segurança e produtividade para os usuários e todos os dispositivos, incluindo smartphones, tablets, laptops, desktops, wearables e IoT – tudo com a mesma ferramenta de gerenciamento de TI moderna.

Faz tudo pelo que CMTs, MDMs e EMMs são conhecidos – oferecendo o mais amplo nível de suporte de plataformas antigas para Windows 10 e macOS. Ele pode enviar correções de atualizações de aplicativos de terceiros, bem como distribuição e instalação de aplicativo para cargas úteis Win32, PKG/DMG e AppX. Ele inclui um catálogo de aplicativo universal com suporte para todas as principais plataformas de dispositivo móvel e *endpoint*.

Como se a balança já não estivesse pendendo para o seu lado, o UEM fornece gerenciamento e cumprimento de política consistentes em todos os fatores de forma, tornando extremamente fácil definir definitivamente todos os *endpoints* usados para trabalhar. Detecção e remediação de vulnerabilidade dão ambas um murro de segurança.

E o novato tem um gancho de direita sinistro, adicionando insights cognitivos, análise de dados contextual e capacidades comparativas originadas na nuvem ao seu arsenal. O UEM o ajuda a entender as minúcias de dispositivo móvel que você encontra diariamente, ao mesmo tempo em que protege seus *endpoints*, usuários, aplicativos, documentos e os respectivos dados em uma só plataforma.



É UM NOCAUTE!

IBM® MaaS360® with Watson™ UEM tem as melhores soluções de MDM/EMM e CMT.

CONFERINDO A TABELA DE DESEMPENHO

Legenda: Com suporte ✓ Sem suporte ✗ Com suporte limitado ◆

Função	CMT	EMM	UEM
Atualizações de correção e de terceiros (distribuição e instalação)	✓	✗	✓
Mudanças de registro	✓	✗	✓
Inventário de software e hardware	✓	✓	✓
Gerenciamento de Linux	✓	✗	✓
Inscrição de OTA	✓	✓	✓
Distribuição de aplicativo Win32 e PKG	✓	✗	✓
Imagem	✓	◆	◆
Catálogo unificado de aplicativos	✗	✗	✓
Gerenciamento de identidade e acesso	✗	✗	✓
Um único painel para todos os *endpoints*	✗	✗	✓
Gerenciamento de políticas via API	✗	✓	✓
Integração com lojas de fornecedores	✗	✓	✓
Políticas baseadas em local	✗	✓	✓
Redução do custo total de propriedade (TCO)	✗	✓	✓
Gerenciamento leve	✗	✓	✓
Contexto baseado no usuário	✗	✓	✓
Configurações de Wi-Fi	✗	✓	✓
Configurações do Microsoft ActiveSync	✗	✓	✓
Integrações de AD/LDAP	✗	✓	✓
Colocação de aplicativos na listagem negra/lista de aplicativos confiáveis	✗	✓	✓
Ações em tempo real (limpeza/limpeza seletiva/localização e mais)	✗	✓	✓
Gerenciamento de FileVault (Apple) BitLocker (Windows)	✗	✓	✓
Proteção de informações do Microsoft Windows (somente Windows)	✗	✓	✓

SUA SOLUÇÃO ATUAL PODE ENFRENTAR A CAMPEÃ?

Clique e descubra mais

Testemunhe a vitória.

IBM MaaS360 | With Watson

Com o gerenciamento unificado de *endpoint*, você obterá todos os recursos de MDM, EMM e CMT, com insights cognitivos adicionais e análise de dados contextual. Para obter mais informações, acesse www.unifiedendpointmanagement.com

IBM

WG912374-BRPT-00