Contornos da mobilidade moderna

Que a mobilidade é um novo paradigma não é novidade. Que está a redefinir o próprio conceito de trabalho também não. O que importa, então, dizer? Alcatel-Lucent Enterprise, Decunify, Lenovo, Microsoft, MobileIron, Noesis e Targus dão as respostas

Vânia Penedo

Para os protagonistas deste Fórum, a mobilidade tem de ser entendida como um tema que é tanto de tecnologia como de pessoas. E é difícil dizer quem influencia o quê. No entanto, é impossível falar hoje de mobilidade sem traçar um caminho que começou há dez anos, com o lançamento do primeiro iPhone – evento que acabaria por originar uma nova categoria de dispositivos móveis, os smartphones. Com eles chegariam novas arquiteturas de software, a popularização da palavra "app" e novas formas de comunicar, trabalhar e socializar.

Como recordou Daniel Madero, *country manager* da MobileIron para Portugal, Espanha e Itália, há uma década a mobilidade resumia-se ao e-mail e ao telemóvel corporativo. Hoje vivemos em plena "mobilidade moderna". "Com a nova geração de smartphones, começámos a ter um dispositivo muito distinto", sublinhou. Nascia no mundo do consumo, mas acabava por ter uma adoção "muito rápida" por parte das empresas.

A notável evolução das plataformas móveis acabou por mudar a forma como interagimos com os dispositivos: de preferência por toque, de forma intuitiva e rápida. "É fundamental entender que o smartphone é uma plataforma distinta do antigo PC, tem uma arquitetura de software muito diferente". Toda esta mudança, que acabou por influenciar outros modelos, acabou por permitir "uma transformação do negócio", segundo Daniel Madero, "que passou a aproveitar todas as potencialidades deste novo paradigma".

"Com o smartphone, os modelos tradicionais de gestão do posto de trabalho não funcionam"

Daniel Madero
Country Manager para Portugal, Espanha e Itália da MobileIron

Como observou Rui Neves, *country manager* da Targus para o mercado português, "quase toda a informação de que hoje dispomos está dentro dum smartphone".

José Manuel Oliveira, CEO da Decunify, traçou uma perspetiva para o mercado empresarial. "Nos últimos dois a três anos verificou-se um grande *boom* da adoção da mobilidade enquanto conceito de trabalho". Porque a definição do que significa trabalhar também mudou. "A imagem de uma pessoa presente fisicamente num local de trabalho começa

a não ser uma realidade", defendeu, principalmente nas grandes organizações. Luís João, *modern workplace solution sales* na Microsoft, reforçou que "trabalhar não significa estar sentado numa secretária", mas "concluir as tarefas independentemente do local onde nos encontramos".

Adotar a mobilidade significa, também, "repensar todo o negócio", observou Nelson Pereira, CTO da Noesis, que deu o exemplo de uma grande organização mundial verdadeiramente movida por este paradigma. "A Unilever, por exemplo, não tem escritórios, todos os colaboradores trabalham remotamente. Recorreu à mobilidade para melhorar a sua logística nos diversos países onde está presente e poupar recursos – dispensou, por exemplo, o POS e começou a utilizar somente smartphones e tablets". A mobilidade, observou, é uma das componentes da transformação digital e também da *Internet of Things*. "Trata-se de repensar todo o negócio e de reduzir custos através da tecnologia".

"Quando falamos em mobilidade existem requisitos muito elevados, nomeadamente ao nível da largura de banda"

José Manuel Oliveira
CEO da Decunify

Em movimento ascendente

A Microsoft tem observado um crescimento "exponencial" da mobilidade em Portugal, ao qual não é indiferente a adoção de serviços cloud. "A cloud permite que tenhamos o nosso escritório em qualquer lugar", lembrou Luís João. "E não se trata apenas do e-mail, mas da possibilidade de recorrer a software para atender uma chamada no PC, por exemplo".

Também a Lenovo vê na mobilidade empresarial uma realidade incontornável. "Um estudo curioso da

Fotografias: Rafael Antunes

Salesforce diz que 38% dos colaboradores se sentem mais produtivos a trabalhar em casa. E 11% evitam ir ao escritório quando têm de realizar uma tarefa crítica, que lhes exija mais concentração", adiantou Rui Gouveia, *channel account manager*, que partilhou uma previsão da IDC: 75% dos colaboradores serão móveis dentro de três anos. "A tecnologia tem permitido esta evolução do trabalho", destacou. "O trabalho em casa duplicou desde 2005. No passado os portáteis eram utilizados quase em exclusivo por dois tipos de profissionais, diretores e vendedores", lembrou.

Se outrora as pessoas tinham acesso apenas a um dispositivo – fixo ou móvel –, é hoje comum terem três ou quatro dispositivos ligados em simultâneo. "Até mesmo os smartwatches, o que coloca uma enorme pressão sobre a rede", observou o responsável de Canal.

Redes: wireless e seguras

Do ecossistema da mobilidade fazem parte dispositivos, aplicações e comunicações à altura das atuais exigências. Sem a evolução d a infraestrutura comunicacional, a mobilidade teria falhado. "A rede WiFi é, de facto, a principal rede de comunicações", reconheceu José Manuel Oliveira, da Decunify. A este respeito, Henrique Amaro, *technical sales and services* da Alcatel-Lucent Enterprise, realçou que a aposta da empresa vai no sentido de que a própria rede funcione de forma *seamless* e segura, seja *wired* ou *wireless*. "O objetivo é que o utilizador não sinta a diferença, o que é um desafio. Integrámos por isso nos nossos *access points* e nos *switches* a possibilidade de ter assinaturas para aplicações", referiu. "É importante dar resposta não apenas à qualidade do serviço dos novos tipos de aplicações mas também às necessidades do *IT manager*. Entendemos que, perante um ataque, tem de ser o próprio equipamento – *switch* ou *access point* – a ter a capacidade de cortar a comunicação *machine to machine*".

E que caraterísticas deve ter uma infraestrutura de comunicação interna à prova do futuro? "Para manter-se atualizada durante um período de dois anos, tem de estar bem alicerçada na componente

"Verifica-se que 90% dos utilizadores preferem trabalhar com privacidade, o que aumenta a própria produtividade"

Rui Neves
Country Manager Portugal, Itália e PALOP da Targus

Rui Gouveia

Luís João

Henrique Amaro

passiva", aconselhou Henrique Amaro. "É também necessária uma tecnologia que, a três meses, possa funcionar a 2.5 gigabits, depois a 5 e depois a 10, sem ser preciso mudar. Mas tudo isto implica custos elevados". Na componente passiva, importa apostar em equipamentos de última geração. "Quando estamos a falar de escritórios e de infraestruturas, é fundamental que se conheça a realidade do negócio e de quem trabalha. E é importante não tentarmos impor um produto que só servirá o seu propósito durante seis meses".

"Existe uma diferença entre mobilidade do dispositivo e mobilidade do utilizador"

Luís João

Modern Workplace Solution Sales da Microsoft

José Manuel Oliveira realçou que a implementação de uma rede sem fios exige o recurso a ferramentas que permitam, mesmo sem uma deslocação ao local, desenhar e otimizar a estrutura. "Temos de estar fundamentalmente preocupados com o desenho da solução. Os fabricantes têm opções muito semelhantes, ao nível da conceção dos equipamentos. Mas depois há a parte aplicacional, que faz toda a diferença". A mobilidade tem elevados requisitos, "nomeadamente ao nível da largura de banda", frisou, e esta "deve ser uma preocupação para as empresas".

Segurança é tema crítico

A segurança é hoje o tema central da mobilidade empresarial, tendo em conta os dois episódios que marcaram o ano até ao momento – o WannaCry e o Petya. "A segurança no contexto da mobilidade é e será um tema cada vez mais crítico", afirmou Daniel Madero, da MobileIron.

Se há uns anos as empresas se preocupavam sobretudo com os ataques externos, hoje percebem que o perigo também pode vir de dentro, "seja porque os utilizadores estão desprotegidos ou porque alguém de fora da empresa se liga à rede corporativa e a compromete", sublinhou José Manuel Oliveira, sem que exista um sistema de bloqueio. "Esta é uma primeira parte, a da implementação de plataformas que limitem quem se coneta à infraestrutura e para a qual as empresas já estão sensibilizadas". A segunda tem sido o aparecimento de soluções de proteção de *endpoints* que possibilitam o *Bring Your Own Device* (BYOD). "O BYOD é cada vez mais uma realidade, porque utilizamos os nossos dispositivos pessoais para fins profissionais e muitas empresas começam a adotar ferramentas que permitem criar nos dispositivos os dois ambientes, o pessoal e o profissional, mantendo a sua utilização em separado", referiu o CEO da Decunify.

Ao BYOD tem vindo a juntar-se uma outra realidade. Rui Gouveia, da Lenovo, lembrou que começa a verificar-se o *Bring Your Own Application* (BYOA), fenómeno pelo qual o utilizador recorre a aplicações de uso pessoal, como a Dropbox, por exemplo, para armazenar informação corporativa. "É necessário criar políticas e dar formação aos utilizadores", disse. No entanto, a tecnologia também tem uma palavra importante a dizer. "Se não forem implementados mecanismos que limitem essa possibilidade, as pessoas acabam por ser um risco, mesmo inconscientemente. Daí que as empresas de maior dimensão criem *app stores* próprias, para que os utilizadores utilizem apps empresariais", observou José Manuel Oliveira.

Smartphones protegem-se de forma diferente

Os smartphones são um dos alvos preferenciais dos cibercriminosos e não é difícil perceber porquê, tendo em conta o manancial de informação que concentram, onde se incluem dados confidenciais de todo o género, desde passwords a credenciais bancárias. "Com o smartphone, o controlo foi cedido ao utilizador final, o que leva a que os modelos tradicionais de gestão do posto de trabalho não funcionem nestes dispositivos", advertiu Daniel Madero. "A boa notícia é que as plataformas móveis, iOS e Android, são bastante seguras se forem bem geridas", assegurou, deixando um conselho: "É preciso começar por proteger o acesso aos serviços da empresa, *on-premises* ou em cloud". O *country manager* da MobileIron explicou ainda porque é que proteger a identidade não chega no contexto dos *smartphones*. "É um tema que se prende com a ligação do smartphone à cloud. A diferença, em relação a um *browser*, é o facto dos smartphones utilizarem por norma *apps* que sincronizam informação na cloud e a guardam no dispositivo, podendo compartilhá-la com outras *apps* que a podem partilhar com outras clouds, e assim sucessivamente. Nos smartphones, gerir a identidade do utilizador não é suficiente".

Portanto, alertou, importa que, nestas plataformas, se controle não apenas a identidade, mas os dispositivos e as aplicações que estão a ser utilizadas. "Estes três elementos têm de ser de confiança. É algo que se controla com uma boa solução de *enterprise mobility management*, em conjunto com extensões de controlo de federação de acesso à cloud", disse.

Autenticação biométrica: o fim das passwords?

A cloud é um dos motivos pelos quais proteger o perímetro não chega, em contexto de mobilidade. Numa arquitetura desta natureza, lembrou Luís João, o utilizador pode aceder à informação corporativa

José Manuel Oliveira

dentro ou fora das "muralhas" que protegem as infraestruturas de rede das empresas.

Para a Microsoft, a identidade é, compreensivelmente, o primeiro pilar da segurança, pela natureza do sistema operativo e da arquitetura do PC. Luís João referiu que 82% dos ataques são ataques à identidade. "As empresas podem ter o melhor sistema do mundo, mas se alguém sabe a palavra-passe tem imediatamente acesso. Outra estatística diz que 73% das palavras passe são reutilizadas no local de trabalho", alertou. A tecnológica tem, por isso, apostado na autenticação biométrica e em mais do que um fator de autenticação. "É preciso ter a certeza de que a pessoa é quem diz que é".

As palavras-passe, no entanto, deverão ter os dias contados. "Dentro de poucos anos, uma das grandes revoluções que vamos observar é a inexistência de *passwords*", anteviu o representante da Microsoft. Daniel Madero realçou que se trata de uma tendência já em voga nos smartphones, dispositivos onde o recurso à impressão digital é cada vez maior.

Luís João sublinhou, em relação à proteção dos dispositivos móveis e das aplicações, que se verifica uma tendência: a adoção de soluções de *mobile device management* (MDM) e também de *mobile application management* (MAM), uma subcategoria do *enterprise mobility management*, para garantir que a pessoa está a trabalhar de forma segura.

Não esquecer a privacidade

Outra forma de o assegurar passa pela salvaguarda da privacidade. "A mobilidade tem esse problema – muitas vezes esquecemo-nos que estamos expostos quando estamos a trabalhar num PC num local público, porque não sabemos quem está ao nosso lado. Podemos ter os melhores sistemas, mas se não protegermos a identidade a pessoa ao nosso lado pode ter acesso a informação de forma gratuita", advertiu Rui Neves, da Targus. Esta questão também se aplica em ambientes de *open space*. "Verifica-se que mais de 90% dos utilizadores preferem trabalhar com privacidade, o que aumenta a própria produtividade", destacou.

Hardware ao serviço do trabalho colaborativo

O impacto que o smartphone teve sobre o PC é inegável. A portabilidade passou a ser caraterística-

"Temos assistido à adoção crescente dos tablets híbridos e dos convertíveis"

Rui Gouveia
Channel Account Manager da Lenovo

-chave dos dispositivos de computação, como notou Rui Gouveia, da Lenovo, com os utilizadores a privilegiarem também a autonomia, o peso e a espessura dos portáteis. "Também temos assistido à adoção crescente dos novos modelos, como os tablets híbridos e os convertíveis". Este último formato, em particular, tem tido bastante sucesso. "A flexibilidade do utilizador e a mobilidade trazem alguns desafios", alertou, porque "a durabilidade e a resiliência também são importantes". Resistir a salpicos, choques, vibrações é fundamental, o que tem levado a Lenovo a apostar no cumprimento de standards de nível militar.
Com os *millennials* a imporem-se no mercado de trabalho, realçou Rui Gouveia, e os espaços dos escritórios a diminuírem, "as ferramentas de colaboração são fundamentais".

Criar cenários de colaboração foi a aposta da Microsoft aquando do lançamento do Surface. "Observámos que existiam clientes com necessidades diferentes. Começámos a ver até em cenários mais tradicionais, como o da banca, que seria vantajoso um dispositivo mais versátil e ergonómico, *touch,* que permitisse a utilização da caneta para assinatura digital, por exemplo", indicou Luís João.

Experiência de utilização é rainha

A mobilidade empresarial é também um tema de informação. "Importa considerar a questão dos documentos e, por isso mesmo, é cada vez mais importante falar em experiência", lembrou Luís João. Ou seja, trata-se da possibilidade de, num momento, trabalhar num tablet e de seguida passar para o PC ou para o smartphone mantendo forma de utilização. "Existe uma diferença entre mobilidade do dispositivo e mobilidade do utilizador", distinguiu.

Segundo Henrique Amaro, é na integração que os fabricantes estão a apostar, "em algo que possa funcionar em qualquer dispositivo e com o mesmo nível de acesso". José Manuel Oliveira notou que as pessoas trabalham cada vez mais em tablets e que, por isso, os fabricantes de software "estão a adaptar as suas aplicações ao *mobile*".

A chave para esta continuidade da experiência de utilização em qualquer dispositivo são as aplicações, que tiveram, também elas, de evoluir. "Toda a nova

Daniel Madero

Nelson Pereira

Rui Neves

panóplia de dispositivos, dos smartphones aos tablets, tem nos permitido desenvolver aplicações cada vez mais dinâmicas, conetadas e online", realçou Nelson Pereira, CTO da Noesis. "Tudo é centralizado e acedido da mesma forma, sempre atualizado a qualquer hora", frisou.

"Toda a nova panóplia de dispositivos, dos smartphones aos tablets, tem-nos permitido desenvolver aplicações cada vez mais dinâmicas e online"

Nelson Pereira
CTO da Noesis

No desenvolvimento de software a experiência *mobile* é "inevitável": "Nenhuma aplicação é hoje desenvolvida de forma fechada", realçou. Quando o tema é o desenvolvimento para ambientes *mobile,* há quase sempre uma questão que se impõe: web ou aplicação nativa? "Por web temos de ter ligação à internet. Nas *apps* nativas, conseguimos guardar e fazer cache, sincronizando novamente quando há ligação. Tudo isto a está a evoluir. As organizações estão a apostar na mobilidade para a sua transformação e a cloud fez maravilhas para empresas, como a Noesis, que desenvolvem software".

A mudança imposta às aplicações depende muito da forma como as pessoas querem trabalhar. "Vivemos num mundo síncrono e assíncrono. O primeiro é o do tempo real, da comunicação por chat. O assíncrono é do e-mail e da troca de documentos. Estes dois mundos estão a juntar-se", salientou Luís João. Nelson Pereira reforçou a mensagem de que "o sincronismo é precioso" no mundo de hoje e Daniel Madero lembrou que é importante que a infraestrutura de comunicações tenha a capacidade de manter as aplicações atualizadas, "de forma segura e escalável".

Posto de trabalho do futuro

Com o posto de trabalho a ser cada vez menos um local, o que esperar daqui para a frente? "O posto de trabalho, quando existe, é ocupado pela primeira pessoa que chega". Este conceito, apontado por José Manuel Oliveira, da Decunify, dá pelo nome de *hot desking*. Rui Neves, da Targus, chamou-lhe uma tendência ao nível do espaço de trabalho. "Com as *hot desks*, as secretárias partilhadas, as organizações conseguem reduzir custos e manter o mesmo espaço", sublinhou, alertando para a necessidade de as empresas terem *docking stations* universais que permitam conetar um amplo conjunto de periféricos. A tendência será, também, a criação de diversos ecossistemas dentro de um escritório, segundo o *country manager* da Targus.

Daniel Madero, da MobileIron, sublinhou que, para a maioria dos trabalhadores, hoje em dia, parte do posto de trabalho "é algum tipo de dispositivo". Os dispositivos, esses, "já não são diferentes arquiteturas, são diferentes *form factors*".

Mas quando o tema é trabalho, lembrou Henrique Amaro, da Alcatel-Lucent Enterprise, dois fatores são determinantes: produtividade e redução de custos. "Dentro de cada empresa, haverá departamentos onde continuará a fazer sentido que as pessoas ocupem um lugar fixo. O hardware terá de se adaptar a estas múltiplas realidades", indicou.

Do ponto de vista humano, o trabalho remoto tem um revés: o isolamento. Rui Neves falou num "renascimento do escritório em si" e Nelson Pereira relembrou a importância da colaboração e da proximidade. "As metodologias de desenvolvimento de software, por exemplo, dizem que as equipas têm de trabalhar em conjunto, em nome de resultados superiores", defendeu. A resposta poderá estar na realidade virtual (RV). "Os óculos de RV vão proporcionar o posto de trabalho do futuro. Permitirão reuniões virtuais, mas vão dar-nos a sensação de que estamos fisicamente próximos", defendeu. "A realidade virtual vai avançar no sentido de nos aproximar digitalmente". Sobre o posto de trabalho do futuro, foi perentório: "A colaboração será um fator essencial. Vão ser investidos muitos milhões em ferramentas de colaboração".

"Entendemos que, perante um ataque, tem de ser o próprio switch ou access point a ter a capacidade de cortar a comunicação machine to machine"

Henrique Amaro
Technical Sales and Services da Alcatel-Lucent Enterprise

Alcatel·Lucent Enterprise

OmniAccess Stellar WLAN, para uma infraestrutura de WiFi escalável e segura

Com a OmniAccess Stellar, a Alcatel-Lucent Enterprise disponibiliza uma nova solução WiFi com arquitetura de próxima geração, que recorre a um controlo distribuído para proporcionar uma infraestrutura sem fios segura, com alta disponibilidade e qualidade, para empresas verdadeiramente mobile e de qualquer dimensão

AP1101
802.11ac: Wave 1

AP1221/AP1222 - 802.11ac: Wave 2

AP1231/AP1232 - 802.11ac: Wave 2

AP1251 - 802.11ac: Wave 2

No passado, o mercado de WiFi empresarial começou com access points (APs) autónomos, com cada AP a ter de ser configurado individualmente. Esta abordagem não se adequava a instalações em empresas de maior dimensão, o que levou ao aparecimento do primeiro controlador centralizado WLAN – um dispositivo montado em rack ou servidor, que funciona com APs simples, disponibilizando-lhes centralmente o firmware e configuração de forma automática. Deste modo, oferece-se um único ponto de gestão de toda a rede sem fios. Hoje podemos virtualizar o controlador e implementar e executar de forma distribuída no próprio AP, com inteligência coordenada. Esta é a escolha das soluções Alcatel-Lucent Enterprise: os APs inteligentes e avançados são geridos como um único sistema e lidam com o tráfego de controlo de forma distribuída e coordenada.

Benefícios do controlo distribuído

Este tipo de arquiteturas proporciona diversas vantagens, nomeadamente a redução das despesas de capital, quando nenhum controlador é estritamente necessário. Além disso, a Alcatel-Lucent Enterprise fornece uma única licença para a gestão do AP, que inclui todas as funcionalidades necessárias para uma rede sem fios de última geração (deteção de intrusão, firewall, inspeção profunda de pacotes), reduzindo assim os custos de software. Há também menores gastos operacionais, porque não ter controladores significa menos equipamento para operar e gerir.
Maior resiliência é outro dos benefícios, porque não existe um único ponto de falha. Por outro lado, não há constrangimentos de tráfego e menor latência — o tráfego não é mais encaminhado para o controlador centralizado, mas comutado diretamente para o switch.
Por último, destaca-se a maior escalabilidade: nenhum controlador a mais será necessário, independentemente do tamanho da instalação. Quando for necessário crescer, basta apenas adicionar novos *access points*.

OmniVista 2500 NMS

A família OmniVista 2500 NMS inclui agora as funcionalidades específicas de gestão da solução OmniAccess Stellar, e gestão de políticas unificadas UPAM. A Versão 4.2.2 do OmniVista 2500 incorpora três novos tipos de solução de gestão das licenças Stellar: licenças de AP (OV-AP-NM-xx), licenças UPAM para gestão de convidados (OV-GA-xx) e licenças UPAM para gestão de dispositivos BYOD (OV-BYOD-xx).
As licenças de "AP" para gestão unificada (AP1101, AP1221, AP1222, AP1231, AP1232, AP1251) incluem o registo de pontos de acesso, topologia, resolução de problemas, operações, *smart analytics* e gestão de configurações, incluindo regras de acesso unificado baseadas em perfis. Também incluem funcionalidades específicas de rádio, como a gestão de RF (rádio frequência), WIPS (Wireless Intrusion Prevention), ferramentas de planeamento/mapa de cobertura.
A autenticação unificada Policy Manager (UPAM) integrada disponibiliza a funcionalidade para autenticação avançada, oferecida por licenças específicas para o acesso de visitantes e BYOD (Bring Your Own Device).
Com suporte para as soluções OmniAccess Stellar, a Versão 4.2.2 do OmniVista 2500, "OV-Starter Pack", agora inclui 10 licenças para pontos de Acesso, 10 licenças para o acesso de visitantes e 10 licenças para BYOD de forma gratuita.
Esta solução integra-se com as últimas soluções de segurança nesta área. Graças à compatibilidade com o software de gestão OV2500 e firmware AOS dos switches da Alcatel-Lucent Enterprise, dispõe de tecnologia DPI (Deep Packet Inspection) para análise de tráfego inteligente de aplicações Layer 7.
Esta nova solução permite escalar da pequena solução empresarial até soluções de grande porte e distribuídas geograficamente, com possibilidade de ligação à nuvem, serviços integrados de BYOD, NAC e Guest Portal.

Dois tipos de instalação

A família OmniAccess WLAN Stellar pode ser instalada de duas maneiras diferentes, dependendo do tipo de cliente e suas necessidades: WiFi Enterprise e WiFi Express. A primeira, oferece opções avançadas para a gestão de radiofrequência (RF), WIDS/WIPS de deteção e prevenção, plantas e mapas de cobertura para o planeamento de uma solução física em WLAN, como um RADIUS integrado, BYOD e um Portal GUEST avançado. O administrador de rede pode obter uma visão completa das aplicações em execução na rede sem fios e configurar controlos e políticas apropriados.
A configuração WiFi Express, funciona num grupo de APs autónomo e de arquitetura simplificada, com uma Página de GUEST e gestão de Rádio Frequência (RF) simples, permitindo instalações em "plug-and-play", por exemplo, para PME. Este grupo de pontos de acesso é um sistema independente, sem recurso a qualquer ferramenta de gestão e é expansível para já a 32 APs só com dispositivos AP1101, ou até 64 em um grupo misto com APs da gama superior (exemplo: 4x AP12xx e 60x AP1101 ou 64x AP12xx).

Info Alcatel-Lucent Enterprise

www.al-enterprise.com

Alcatel·Lucent Enterprise

Intelligent Wi-Fi that can multitask.

Hardworking Wi-Fi, where everything simply connects

Alcatel-Lucent OmniAccess® Stellar WLAN incorpora a transição atualmente em curso nas redes sem fios. Descubra como uma solução exigente de Wi-Fi pode funcionar com instalação rápida, gestão sem esforço, excelente desempenho, segurança e automação, hoje e no futuro.

ALE | Where Everything Connects

Rui Duro | Sales Manager Check Point Portugal

Smartphones infetados: o espião no seu bolso

As empresas devem proteger os telefones móveis da mesma maneira que o fazem com os computadores

Nos últimos anos, os smartphones iniciaram um percurso que os leva, cada vez mais, a ter um protagonismo muito importante na vida das pessoas, tornando-se aliados e elementos inseparáveis do nosso quotidiano pessoal e profissional. Estes dispositivos armazenam informações importantes e confidenciais e os cibercriminosos sabem bem disto. Credenciais de acesso, dados bancários, fotos, contas de email ... os hackers podem usar qualquer parte deste conteúdo para deitar a mão a quantias significativas de dinheiro, e invadir contas bancárias com ataques de ransomware móvel, ameaçando divulgar ou reter informações confidenciais tanto pessoal como empresarial - ou vender os dados roubados no mercado negro.

Através do malware móvel, os criminosos podem assumir o controlo de um smartphone, instalar aplicações fraudulentas, fazer compras online, ouvir as suas conversas telefónicas e ler as suas mensagens, saber a sua localização exata ou ativar o microfone e câmara, entre muitas outras atividades tão assustadoras como ilegais. Além disso, os dispositivos móveis são uma porta de acesso fácil às redes das empresas: se um telefone infetado for ligado à mesma WiFi que outros dispositivos da empresa, o malware pode entrar e infetar servidores e todos os computadores.

De acordo com um relatório do Instituto Ponemon, um único terminal infetado pode levar uma empresa a incorrer num prejuízo de cerca de 9.000 euros. As soluções de segurança para dispositivos móveis e terminais devem ter a capacidade de enfrentar desafios que vão desde as vulnerabilidades do sistema ao *rooting*, passando pelas alterações de configuração, aplicações fraudulentas ou maliciosas, trojans, malware e ataques de rede. Então, como podemos proteger-nos? A resposta não é fácil, mas a base é simples: oferecer aos colaboradores das empresas uma solução abrangente de segurança para dispositivos móveis.

As empresas devem proteger os telefones móveis da mesma maneira que o fazem com os computadores. Uma solução perfeita deve ter várias camadas e impedir a transferência de dados entre as aplicações

Rui Duro, Sales Manager Check Point Portugal

pessoais e profissionais instaladas no mesmo dispositivo. Também deve incluir tecnologias de prevenção de ameaças para proteger os dispositivos de aplicações maliciosas. Além disso, é necessário formar os colaboradores para que tenham conhecimentos básicos de cibersegurança. De acordo com o Relatório de Segurança 2016 da Check Point, em 2017 um em cada cinco trabalhadores será responsável por uma violação de segurança que afetará gravemente os dados da sua empresa.
Alguns conceitos fundamentais parecem básicos, mas que não podem deixar de ser transmitidos e repetidos até à exaustão junto dos colaboradores das empresas:

- Não faça download de aplicações a partir de lojas não oficiais
- Tenha especial cuidado com as mensagens recebidas no smartphone, sobretudo se forem provenientes de um remetente desconhecido ou o assunto e conteúdos forem suspeitos
- Não clique em janelas pop-ups
- Não se conecte a redes WiFi públicas não seguras.

As mesmas ameaças conhecidas, desconhecidas e de dia zero que atacam portáteis e desktops fixaram agora os smartphones como os seus alvos preferenciais. É imperativo proteger estes dispositivos de forma eficiente, tanto quando saem da rede como enquanto estão ligados a ela.

SandBlast Mobile

Os dispositivos móveis são hoje uma parte importante do ecossistema pessoal e empresarial, armazenando e proporcionando acesso à informação da empresa. Mas também introduzem um novo vetor de ataque, pelo que as empresas têm que os proteger adequadamente. E isto terá, necessariamente que ser feito através da implementação de uma solução de segurança avançada de múltiplas camadas, como a SandBlast Mobile, capaz de assegurar a deteção e bloqueio das aplicações maliciosas e dos ataques de rede, detetar vulnerabilidades em dispositivos Android e iOS e mitigar todas as vulnerabilidades dos dispositivos, independentemente do sistema operativo.

Principais características

Deteta, bloqueia e mitiga ameaças móveis avançadas:
- Protege dados empresariais sensíveis, quer estejam a ser utilizados ou não, em dispositivos móveis iOS e Android contra ciberataques
- Melhora a visibilidade e proteção através da integração com os sistemas de mobilidade e segurança existentes (MDM, MAM, NAC, SIEM, etc.)
- Permite uma resposta rápida aos ataques de ameaças persistentes avançadas (APT) de plataforma cruzada
- Preserva a experiência do utilizador e a sua privacidade, ao mesmo tempo que assegura a proteção exigida pelos regulamentos internos ou externos à empresa.

Info Check Point
www.checkpoint.com

Check Point
SandBlast™
MOBILE

PREVENÇÃO DE ATAQUES MÓVEIS

SandBlast Mobile previne o mais alargado leque de ataques a dispositivos móveis do mercado, graças ao seu incomparável índice de deteção e bloqueio de ameaças avançadas, conhecidas e desconhecidas, para iOS e Android, de acordo com a avaliação realizada pela Miercom aos produtos de segurança móvel disponíveis em 2017.

Proteção Completa com a única solução de defesa contra ameaças móveis

Prevenção Completa com a primeira funcionalidade antiphishing por SMS do mercado

Visibilidade Completa e em tempo-real sobre todas as ameaças móveis que possam ter um impacto negativo no seu negócio

Para saber mais como prevenir o próximo ciberataque móvel, contacte-nos:

info_iberia@checkpoint.com
+351 217 223 647

Check Point®
SOFTWARE TECHNOLOGIES LTD

RTLS - Sistemas de Localização em Tempo Real

RTLS são sistemas que identificam automaticamente a localização de objetos e pessoas, através de Tags, que comunicam com equipamentos Wi-Fi, geograficamente posicionados, que vão permitir obter uma localização mais precisa

As Tags não são mais que dispositivos que transmitem sinais Wi-Fi e que permitem que qualquer dispositivo móvel, com Wi-Fi ativo, esteja apto a ser localizado. Os dados recolhidos pelas Tags são enviados para o servidor, onde está a ser executado o software de monitorização.

Quer se trate de pessoas ou objetos, um sistema de localização em tempo real pode informar-nos da localização exata pois enquanto os objetos se movem, a Tag envia transmissões para recetores fixos no espaço. Os dados dos recetores e das transmissões indicam a localização física da Tag e do item correspondente.

Esta solução pode ser aplicada em diferentes ambientes e com aplicações distintas. Passamos a citar alguns exemplos:

- **Armazéns:**

  a) permite identificar a localização de um qualquer equipamento ou carga;

  b) permite rastrear os movimentos de equipamentos e cargas com registo automático de toda a operação obtido pelo RTLS. Será possível, assim, a empresa definir novas práticas operacionais e reduzir tempos de viagem, além de poder avaliar o desempenho dos operadores;

  c) permite uma maior precisão do inventário.

- **Hospitais/Indústria:**

  a) cada equipamento pode ser localizado com precisão e, com a colocação de Tags especiais, é possível verificar temperaturas e níveis de humidade.

  b) verificar onde existe maior afluência de pessoas e/ou localizar colaboradores. Esta tecnologia permite aos hospitais identificar se existem pacientes ou visitantes, dentro de uma zona restrita ou numa área não segura.

  c) em situações de emergência pode ser útil para os elementos de uma equipa médica convocarem outros colegas, visto ser fácil para os mesmos localizarem o pedido de ajuda.

- **Espaços de atendimento ao público:** controlo de tempos de espera.

- **Espaços comerciais/públicos:** como forma de controlo para a evacuação de pessoas, em caso de emergência, sendo possível verificar se ainda se encontram pessoas dentro do espaço;

Com o RTLS podemos ainda compreender melhor e envolver os visitantes à medida que estes se movimentam por um espaço ou estabelecimento, dando informação específica, orientada ao local onde o utilizador se encontra. Por exemplo, num supermercado é possível direcionar para promoções de determinados artigos mediante a sua localização.

O sistema de localização em tempo real é uma poderosa ferramenta de gestão para o otimização de processos de negócio. Além de melhorar a eficiência, minimiza desperdícios e automatiza processos, fazendo com que os dados recolhidos possibilitem decisões mais inteligentes e uma gestão efetiva de recursos.

A Decunify pode apoiá-lo em todas as fases do processo, desde a conceção à implementação e suporte da solução RTLS mais adequada para a sua empresa. Aumente a eficiência do seu negócio trazendo inovação.

Info Decunify

www.decunify.com/pt

Advertorial

SOLUÇÕES DE COMUNICAÇÕES

- DATACENTERS E SALAS TÉCNICAS
- CABLAGEM ESTRUTURADA E DE ENERGIA
- REDES LOCAIS E WIRELESS (WI-FI)
- VOZ, VÍDEO CONFERÊNCIA E COMUNICAÇÕES UNIFICADAS
- SEGURANÇA FÍSICA E LÓGICA
- CLOUD
- BUSINESS ANALYTICS
- MULTIMÉDIA
- IMAGING & PRINTING

DECUNIFY

grupo decsis

www.decunify.com
decunify@decunify.com
229 439 660 | 214 489 570

ThinkPad
Pensar a produtividade a um outro nível

Há 25 anos que os ThinkPad são sinónimo de inovação, fiabilidade e desempenho para os utilizadores profissionais com diferentes necessidades

Os portáteis Lenovo da gama ThinkPad, desenvolvida especificamente para o mercado empresarial, são sinónimo de performance e robustez. Os ThinkPad são submetidos a testes de resistência de nível militar, para garantir uma utilização intensiva a toda a prova. A série X é a prova de que resistência e design podem andar de mãos dadas – com design *slim*, ultra leves e uma longa vida de bateria, são a opção que faz sentido para os profissionais que procuram mobilidade mas que não podem sacrificar a produtividade. Na gama ThinkPad X, há três form factors que se destacam – X1 Carbon (laptop), X1 Yoga (convertível) e X1 Tablet (híbrido) – que podem ser configurados de acordo com as necessidades de cada cliente.

ThinkPad X1 Carbon para performance a toda a prova

A robustez do X1 Carbon só é igualada pela sua versatilidade e performance. Com um chassis de fibra de carbono reforçado, este ultrabook é ultra leve: pesa 1.13 Kg e tem somente 16 mm de espessura. A fibra de carbono está ao nível da que existe em satélites e é mais resistente do que a utilizada em carros de Fórmula 1, pesando um terço do que pesa o alumínio, com elevada capacidade de absorção de choques e resistência a líquidos e poeiras.

O X1 Carbon inclui processadores Intel de 7ª geração e Windows 10 Pro, além de Thunderbolt 3, e ecrã de 14 polegadas Quad-HD num chassis de 13. Entrega até 15.5 horas de bateria útil, e carrega até 80% em apenas uma hora.

Para garantir uma autenticação segura, o X1 Carbon suporta Windows Hello, incluindo uma câmara de infravermelhos para reconhecimento facial avançado. Está disponível com Windows 10 Pro Signature Edition e inclui LTE-A (4G).

ThinkPad X1 Yoga para elevada versatilidade

Este convertível é a definição de flexibilidade e um clássico que continua a adaptar-se a todo e qualquer ambiente ou circunstância. Com 14 polegadas, o X1 Yoga permite quatro modos de utilização, ou quatro posições, graças à dobradiça 360° - pode ser utilizado como um tablet, cem por cento estendido, em modo tenda ou como um laptop tradicional.

O X1 Yoga destaca-se por ser o primeiro laptop pensado para o mercado profissional com ecrã OLED. Tem resolução WQHD e integra uma caneta stylus *built-in* que carrega sempre que é guardada (cinco segundos dão acesso a 100 minutos de utilização), caraterística que garante que está sempre pronta a utilizar, tendo suporte para todas as aplicações Office 2016. O X1 Yoga pesa 1,27 Kg e, tal como o X1 Carbon, tem na bateria um dos seus pontos mais fortes – até 15.5 horas, carregando a 80% em apenas uma hora. Em nome de uma verdadeira conetividade, está disponível com modem 4G Qualcomm Snapdragon X7 LTE. O X1 Yoga inclui ainda conexão Thunderbolt 3 , para uma rapidez de transferência até 40 Gbps.

ThinkPad X1 Tablet para máxima customização

Utilizadores de elevada mobilidade que necessitam da performance de um laptop e da polivalência de um tablet para se manterem produtivos.

Um tablet com design modular com teclado destacável que supera os tradicionais híbridos dois-em-um pela possibilidade de adaptação a diversas necessidades – desde a exibição de conteúdos multimédia com a projeção de apresentações ou para maior autonomia. Tudo depende dos módulos opcionais, que acrescentam funcionalidades – o Módulo de Apresentação e o Módulo de Produtividade. Por exemplo, o de produtividade aumenta a autonomia do dispositivo para 15 horas, ao passo que o de apresentação inclui um micro projetor para criar um ecrã de 60 polegadas e uma porta HDMI.

Com ecrã FHD+ de 12 polegadas, o tablet pesa apenas 795 gramas e tem 8,4 mm de espessura (1100 gramas com teclado).

Embora seja um tablet é testado em 12 testes de grau militar e passa em mais de 200 testes de qualidade, sendo desenhado para sobreviver a todos os imprevistos do dia-a-dia. Inclui ainda LTE-A (4G) e suporte on-site.

A experiência de escrita com a caneta stylus recorre à tecnologia Active Capacitive da Lenovo, com um novo algoritmo de firmware que bloqueia qualquer toque acidental sobre o ecrã. A experiência de utilização é significativamente melhorada com a app WRITEit, que estabiliza a utilização da caneta e a integra com centenas de aplicações.

Info Lenovo

www.lenovo.com/pt

Different is better

Lenovo

THINKPAD
-VS-
ESPAÇOS LIMITADOS

A versátilidade do X1 Yoga transforma qualquer área num centro de produtividade graças ao seu design convertível.

Different adapts better.

ThinkPad X1 YOGA

SAIBA MAIS EM WWW.LENOVO.COM/PT/PT

Ultrabook, Celeron, Celeron Inside, Core Inside, Intel, Intel Logo, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Inside Logo, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, vPro Inside, Xeon, Xeon Phi, and Xeon Inside are trademarks of Intel Corporation in the U.S. and/or other countries.

GDPR e dispositivos móveis: um desafio acrescido

É imperativo que os equipamentos móveis adotem uma abordagem muito mais proativa no cumprimento do novo Regulamento Geral de Proteção de Dados (GDPR, em inglês) da União Europeia

O GDPR foi aprovado em abril de 2016 e entrou em vigor a 25 de maio do mesmo ano. O cumprimento obrigatório dar-se-á a 25 de maio de 2018. O regulamento será aplicado aos 28 países europeus, que ficam submetidos a um único regime legal de privacidade e segurança dos dados dos seus cidadãos.

É um regulamento pelo qual esperámos durante anos, sobretudo como utilizadores, uma vez que, desta forma, estamos protegidos do abuso das grandes empresas europeias e, especialmente, estrangeiras, que se têm dedicado a comercializar os dados pessoais dos cidadãos europeus.

Muitas são as dúvidas que ainda nos chegam em reuniões e apresentações com clientes. Ficamos bastante surpreendidos quando todo o tipo de empresas, grandes e pequenas, nos dizem: "é a primeira vez que oiço falar deste regulamento".

Um projeto de implementação das ferramentas tecnológicas necessárias ao cumprimento do GDPR afeta a quase totalidade dos processos das empresas. Na MobileIron, a nossa especialidade são as plataformas móveis, mais concretamente os smartphones, tablets, portáteis, cloud e IoT. Centramo-nos em como podemos ajudar as empresas a tornarem-se "GDPR Mobile Compliant".

Tenhamos em conta um modelo tradicional de negócio: um funcionário, um posto de trabalho. Comparemos agora com o modelo atual: um funcionário, cinco postos de trabalho. Porquê cinco? Em muitos casos, temos um smartphone, um tablet e um portátil da empresa, disponibilizados pela empresa. Para além do mais, em algumas ocasiões, acabamos por utilizar também o nosso smartphone e tablet pessoais. Quem não utilizou já os seus equipamentos pessoais para aceder a algum correio ou aplicação da empresa em algum momento, por necessidade?

Tendo em conta o cenário de um funcionário/cinco postos de trabalho, a complexidade para gerir, controlar e tornar seguros os dispositivos das plataformas móveis torna-se fulcral. Isto implica gerir cinco vezes mais dispositivos, de marcas diferentes, com sistemas operativos Android, iOS e Windows e, geralmente, em ambientes de mobilidade, é necessária uma solução profissional, com experiência, ágil e potente e, ao mesmo tempo, simples de operar.

O que até agora se denominava de MDM[*1] poderia ajudar a a cumprir muitos dos artigos do GDPR quando se trata da sua aplicação às plataformas móveis[*2]. No entanto, atualmente, os EMM[*4] e as novas plataformas de UEM[*5], como a da MobileIron, são as únicas soluções que nos garantem o cumprimento integral do GDPR em plataformas de mobilidade.

Daniel González Fernández, Security Specialist for Corporate Mobile Platforms, MobileIron Iberia

Um problema associado à segurança dos dispositivos e das aplicações móveis é o acesso à cloud a partir de dispositivos móveis, já que se ativa a funcionalidade dos dados off-line. O que acontece quando acedemos a uma aplicação cloud a partir de um smarphone ou tablet? Identificamo-nos com um nome de utilizador e uma senha. Poderemos até ter um duplo fator de identificação, como por exemplo um sms, um token, etc. Mas o que acontece quando o dispositivo de acesso não é seguro? E se o dispositivo estiver em *root* ou em *jailbreak*? A cloud poderia detetá-lo? A resposta é não. Existe alguma solução para esta situação, que nos coloca perante uma possível fuga de dados?

A MobileIron lançou uma solução chamada Access que, combinada com o EMM, é capaz de garantir que qualquer sistema cloud que utilize o protocolo de federação de identidades samlv2 seja executado apenas em plataformas móveis seguras. Deste modo, a MobileIron pode ajudar a que as empresas sejam "GDPR mobile compliant".

As empresas encontram-se em estádios de preparação muito diferentes. A maioria está a fazer avaliações detalhadas com as suas equipas legais e de compliance. No entanto, ainda não consideraram o impacto específico do GDPR sobre as suas plataformas móveis. Chegou o momento de os equipamentos móveis adotarem um enfoque muito mais proativo para o cumprimento do GDPR. É muito provável que existam muitos mais equipamentos móveis do que servidores e PCs juntos.

O GDPR centra-se sobre o poder da informação, dos dados. O primeiro passo é avaliar os fluxos de trabalho dos dados em toda a organização, de modo a assegurar a proteção adequada e a garantir que os dispositivos ou aplicações não autorizadas nunca tenham acesso aos dados empresariais. Como refere a IDC[*6], as soluções de gestão de mobilidade empresarial como as da MobileIron são cruciais para o cumprimento do GDPR.

Evitar as sanções é muito importante. E os danos reputacionais? As organizações devem prestar especial atenção ao artigo 32. Este artigo introduz o conceito de "estado da técnica", que obriga a que a organização utilize as tecnologias mais modernas. Manter as tecnologias de segurança desatualizadas pode aumentar substancialmente o risco de incumprimento.

Links:
*1 MDM - Mobile Device Management
*2 Plataformas móveis – Smartphones o teléfonos inteligentes, tablets, portátiles e IoT
*3 * segurizar" mejor que "securizar: más información en la web http://www.fundeu.es/recomendacion/segurizar-securizar-securitizar/
*4 EMM - Enterprise Mobile Management
*5 UEM - Unified Enterprise Management
*6 Market Analysis Perspective: Western Europe Enterprise Mobility, 2017» de IDC Europe, feb. 2017.
*7 Portuguese data protection legislation: https://www.cnpd.pt/bin/legis/nacional/lei_6798.html

Info

www.mobileiron.com
www.ingecom.net

Proteja as informações da empresa onde quer que vá

MobileIron

Como MobileIron pode ajudar a cumprir com a Lei de Proteção de Dados europeia no mundo da mobilidade

Baixe o documento EMM www.mobileiron.com/GDPR

Romano Zanon | South Europe Regional Marketing, OKI Europe

Transformação digital e mobilidade, uma relação de simbiose

A transformação digital, um dos fenómenos da atualidade, é sem dúvida uma oportunidade para os negócios e, em particular, para as empresas que se dedicam ao negócio da impressão

Com o aumento contínuo da popularidade dos tablets, smartphones e dispositivos móveis, a impressão de documentos a qualquer momento e em qualquer local confere um novo significado à impressão oferecendo aos colaboradores a possibilidade de imprimir em qualquer ocasião e à medida das suas necessidades.

Assistimos a um processo de transformação profundo no âmbito profissional e que envolve em especial o espaço das empresas e os locais de trabalho, que atualmente vão muito além do espaço físico da secretária, da cadeira e do próprio computador. Graças às novas tecnologias é possível criar escritórios virtuais. Perante esta realidade, as empresas são chamadas a liderar a atual transformação digital, com a digitalização de documentos a assumir um papel fundamental para uma correta gestão da informação que lhes permita tomar as decisões mais acertadas.

Hoje em dia, é comum as empresas utilizarem um sistema misto de gestão documental, combinando o papel com o digital. No entanto, o processo de introdução de novas tecnologias e de transformação digital está a ser desigual. Este facto é especialmente notório na gestão documental: apesar de se registar um aumento do número de empresas que lidam com volumes de dados elevados, apenas um terço das PME europeias está a preparar-se para o mundo digital*. Isto significa que os dois terços restantes podem estar a desperdiçar poupanças importantes em termos de tempo e produtividade e a perder terreno face à concorrência, para além de estarem sujeitas a riscos de segurança mais elevados.

Romano Zanon, South Europe Regional Marketing, OKI Europe

Na altura de simplificar a transição dos processos em papel, os dispositivos móveis representam um contributo significativo. Aumentar a mobilidade do posto de trabalho é um fator-chave para impulsionar a digitalização que, por sua vez, é essencial para assegurar a produtividade numa realidade laboral em que os colaboradores estão em constante mobilidade.

Impressão inteligente que se converte num centro de trabalho documental

Os multifunções (MFP) inteligentes deixaram de ser encarados como um elemento estático nos escritórios e estão a transformar-se em verdadeiros aliados da mobilidade, oferecendo aos utilizadores mais e melhores opções de gestão dos fluxos de trabalho. Num mundo digital, as necessidades de digitalização e gestão documental alteraram-se e foi necessário adaptar a oferta de soluções em conformidade com a nova realidade.

Atualmente, a cloud é um elemento fundamental e estes equipamentos oferecem impressão segura a partir de dispositivos móveis, como tablets ou smartphones, enquanto mantêm a confidencialidade dos dados empresariais perante qualquer ameaça de segurança ou vírus. Ao proporcionar acesso a funcionalidades de digitalização, os utilizadores podem digitalizar informação para acesso mediante pesquisa ou gerir o envio de um documento para um destino específico, eliminando a necessidade de manter um registo em papel. Isto traduz-se em escritórios menos saturados de papel e permite às empresas equipar-se melhor para gerar fluxos de trabalho mais produtivos e conectados.

O portefólio de equipamentos multifunções da OKI inclui uma vasta gama de dispositivos inteligentes que associam o software sofisticado à tecnologia avançada, permitindo otimizar os fluxos de trabalho, simplificando a distribuição e gestão de documentos e dando resposta às necessidades reais das pequenas e médias empresas no ambiente de trabalho em constante evolução.

Compatíveis com um conjunto de aplicações de impressão móvel que permitem imprimir remotamente, como o AirPrint, da Apple Inc, o Google Cloud Print da Google, o Cortado Workplace e o EPrint da Microtech Corp, os MFP Smart da OKI asseguram às empresas a liberdade e flexibilidade que necessitam para imprimir diretamente a partir de um smartphone ou tablet.

Saiba mais em www.oki.pt/mobileprinting

* Estudo da IDC - "Os processos empresariais estão a inibir as suas oportunidades de mercado? Impressão e gestão de documentos económicas através de MFPs Smart"

Info OKI

www.oki.pt

Poupe até 900€ em impressoras e MFPs OKI selecionados e faça crescer o seu negócio!

Até **900€** de desconto imediato*

Impulsione as suas vendas, aumente os lucros e atinja os seus objetivos comerciais!

Beneficie destes preços promocionais em equipamentos a cores e ofereça aos seus clientes dispositivos de elevada qualidade, com funcionalidades adequadas às suas necessidades.

Modelo	PVR	PVR Promo*	Poupe	Período promocional
C332dn	104,77 €	84,77 €	20 €	01/09 - 31/12/2017
MC363dn	263,25 €	163,25 €	100 €	01/09 - 31/12/2017
C823n	773,90 €	523,90 €	250 €	01/09 - 31/12/2017
C823dn	888,36 €	638,36 €	250 €	01/09 - 31/12/2017
MC853dn	1899,17 €	999,17 €	900 €	01/09 - 31/10/2017
MC853dnct	2155,26 €	1255,26 €	900 €	01/09 - 31/10/2017
MC853dnv	2436,13 €	1536,13 €	900 €	01/09 - 31/10/2017

C332dn

MC363dn

C823dn

MC853dn

Saiba mais em:
www.oki.com/pt/printing/promotions/resellers

www.okipartnernet.pt

*Promoção válida para toda a Revenda Informática. Termos e condições aplicáveis. Preço promocional calculado com base no Preço de Venda a Revenda (PVR). Preços sem IVA e sem compensação da lei da cópia privada. Sujeito à disponibilidade de stock. Limite de 60 unidades por modelo durante o período promocional. Campanha não acumulável com outras em vigor.

© 2017 OKI Europe Ltd

Print Smart, Print OKI

Rui Neves | Country Manager Italy, Portugal and PALOP (Lusophone Africa) da Targus

Novos espaços de trabalho

Na última década assistimos a uma profunda transformação da forma como as infraestruturas empresariais evoluíram. Coworking, Virtual Office e Hot Desking são alguns dos conceitos que pareciam miragens, mas com os quais convivemos hoje na realidade empresarial

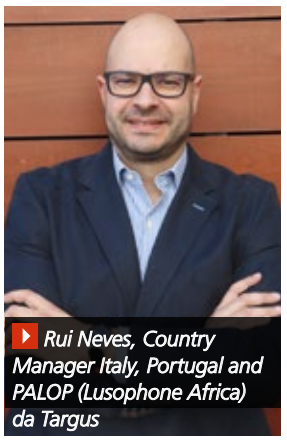
O que tornou possível em grande medida possível esta transformação do espaço físico de trabalho foi a evolução tecnológica e as múltiplas possibilidades criadas para a acompanhar. Por outro lado, a conjuntura económica impôs uma necessidade de adaptação, com grande foco na necessidade de redução dos custos da operação empresarial.

Falar em escritório, hoje em dia, é falar numa pluralidade de realidades, desde a mais convencional conceção do espaço de trabalho empresarial até às mais atuais tendências anteriormente referidas.

O escritório atual não é um espaço físico e estanque, é transportável, partilhável e versátil. Responde às necessidades e conveniências de empresas e colaboradores. Se olhar para o que se passa à sua volta vai notar que um pouco por todo o lado, por todo o tipo de empresas, de todas as dimensões, encontramos estas novas formas de encarar o espaço de trabalho.

Hot Desking, todos os lugares são um posto de trabalho

Já reparou como cada vez mais empresas aderiram ao Hot Desking? Esta opção consiste essencialmente em eliminar os lugares fixos e em garantir as condições para que qualquer colaborador possa utilizar qualquer secretária da empresa. E como é que isto se faz, se cada colaborador tem gadgets diferentes, logo diferentes necessidades individuais de conexão aos periféricos, à corrente, etc.? Simples, utilizando universal docking stations em cada posto de trabalho, o que permite ficar operacional ligando apenas um cabo.



Rui Neves, Country Manager Italy, Portugal and PALOP (Lusophone Africa) da Targus

Uma excelente opção de flexibilização e rentabilização do espaço. Naturalmente que há departamentos mais vocacionados para esta partilha de secretária, mas é um caminho que vale a pena considerar seriamente.

Acessórios para um escritório móvel

Trabalhar remotamente passou de sonho a realidade para muitos trabalhadores que escolhem locais fora da empresa para trabalhar. Uma opção em que o conforto e a mobilidade são assegurados por acessórios Targus, como as malas e ratos que permitem erguer o escritório em qualquer lugar. Outros acessórios, como os ecrãs secundários, são ideais para um escritório em casa.

Nesta modalidade de escritório, as empresas têm de considerar as questões de segurança, dado que não controlam o local onde a pessoa vai trabalhar. Para responder a esta necessidade nada melhor do que ecrãs de privacidade, que reduzem o ângulo de visualização, protegendo as informações mais sensíveis em tablets e monitores.

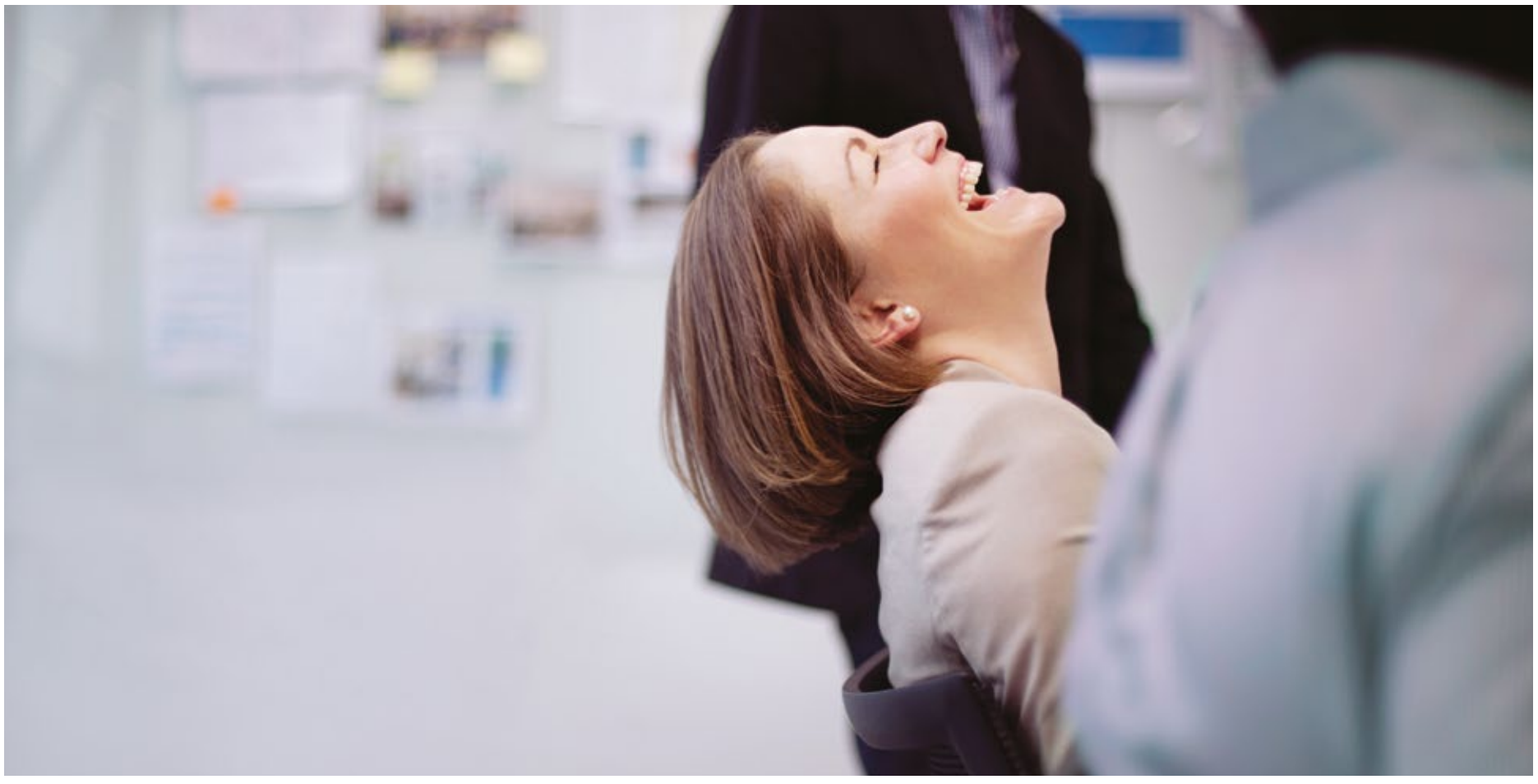
A versão mais radical destas novas tendências é o escritório virtual. Levada ao extremo esta opção pode significar eliminar por completo o espaço físico de uma empresa. Nesta configuração nenhum os colaborador trabalha nas instalações da empresa, com exceção de alguns momentos em que necessitam de ter uma presença física, como uma morada, um espaço de reunião, ou um serviço de recepção. Popular entre startups e trabalhadores por conta própria, as virtudes deste modelo são a ausência de compromissos de longa duração e, claro, a redução de custos. É também uma solução interessante para as filiais nacionais de grandes empresas.

O que importa perceber é que, para sobreviver, as empresas têm de continuar a adaptar-se. A forma como o farão depende das necessidades de empresas e trabalhadores. É apenas necessário assegurar as ferramentas mais seguras e cómodas para aderir ao trend.

Info Targus

www.targus.com

Vários dispositivos **sem** complicações de cabos



Potencie a produtividade da sua força de vendas com a Targus Universal Docking

Conecte-se em qualquer lugar.

CONETIVIDADE SEM COMPLEXIDADE.

WWW.TARGUS.COM

Let's talk Targus®

TOSHIBA
Leading Innovation

João Dessa | Sales manager B2B da Toshiba

30 anos de mobilidade e segurança no ADN

Os trabalhadores são mais exigentes do que nunca e procuram estar inseridos em ambientes que promovam o trabalho em mobilidade. No entanto, para as organizações, ter dispositivos seguros é imperativo. A Toshiba é o único fabricante que o consegue assegurar integralmente

Em Portugal, como nos demais países da Europa, as empresas enfrentam o desafio da transição para uma estratégia de trabalho móvel, produtiva e segura. A mobilidade empresarial, para estar à altura das exigências do trabalhador móvel, tem que refletir a necessidade de um hardware de fácil utilização, suficientemente poderoso e de fácil transporte que permita o desempenho de múltiplas funções em simultâneo, e ao mesmo tempo muito seguro na prevenção de ciberataques.

Efetivamente, o local de trabalho de hoje pode estar alojado em qualquer lugar, seja no escritório, em casa, no comboio, nas instalações de um cliente ou fornecedor. Como tal, os colaboradores precisam de dispositivos que lhes permitam trabalhar de forma produtiva em qualquer ambiente.

Esta crescente necessidade, de trabalho à distância, amplifica as vulnerabilidades. Muitas vezes, de forma involuntária, os utilizadores agem de forma não segura, colocando os dados em risco.

João Dessa, sales manager B2B da Toshiba

Para os departamentos de TI, o utilizador é frequentemente o elo mais fraco na cadeia de segurança. Daí a urgência de retirar esta ameaça das mãos dos utilizadores. Por um lado, as ameaças à segurança de TI e proteção de dados continuará a crescer. Ataques recentes como o "WannaCry" já se repetiram e infelizmente irão continuar a surgir. Paralelamente, na direção oposta, a implementação do novo Regulamento Geral de Proteção de Dados (RGPD), a 25 de maio de 2018, aproxima-se rapidamente.

Os CIO, IT Managers e as equipas de IT das empresas em geral estão, por isso, sob uma enorme pressão, seja porque querem evitar os ciberataques e/ou porque precisam de estar assegurar compliance com as normas do RGPD. Segundo a Gartner, mais de 50% das organizações afetadas pela nova regulamentação não estarão em total conformidade com as suas exigências.

É neste ponto que as equipas de IT se encontram neste momento. A "pressão" evidente a que estão sujeitas representa, porém, uma excelente oportunidade para acrescentarem valor às suas organizações, conjugando segurança e mobilidade como primeiras prioridades nas suas estratégias.

O Toshiba Mobile Zero Client (TMZC) vem dar resposta a esta dupla necessidade, porque disponibiliza as funcionalidades e os dados ao utilizador remoto através da sua solução de VDI (virtual desktop infrastructure), eliminando a possibilidade de armazenamento de malware do dispositivo e de roubo de dados em caso extravio ou roubo do equipamento. Em simultâneo, contribui para retirar o tal risco da esfera dos utilizadores, ajudando a cumprir o RGPD.

Sem dúvida que é mais fácil gerir os desktops numa localização central, data center, do que numa localização remota ou mobile, até porque os administradores de IT conseguem muito mais controlo sobre os dispositivos, centralizando as permissões e gestão de acesso a dados.

O TMZC não comporta qualquer sistema operativo instalado localmente nem qualquer tipo de storage local, HDD ou SDD, não permitindo instalação de informação no equipamento. O dispositivo torna-se assim num sofisticado terminal móvel que permite ao utilizador aceder às funcionalidades e dados da VDI da sua empresa.

O foco da Toshiba, cem por cento no mercado profissional, para além de nos distinguir de toda a nossa concorrência, permitiu-nos não só ter soluções disponíveis para o mercado empresarial, como por exemplo o TMZC, como também seguir com o que acreditamos ser a excelência do hardware mobile, sendo a nova gama "X" espelho disso mesmo.

A inovação tecnológica presente no nosso ADN permite-nos estar a par da incontornável tendência "thin and light" do mercado, com os recentes Portégé X30 (13,3", 1,05Kgs), Tecra X40 (14", 1,25Kgs) e o híbrido convertível, Portégé X20 (12,5", 1,1Kgs). Deste modo conseguimos dar resposta à crescente necessidade de mobilidade dos utilizadores empresariais e entregar caraterísticas de segurança importantes, como a Identificação Facial, além dos habituais sensores de impressão digital biométricos, TPM e encriptação de dados/passwords na BIOS do dispositivo.

O facto da Toshiba manter o fabrico da BIOS "in house" continua a ser um importante fator diferenciador face à nossa concorrência e que nos destaca enquanto fabricante especialista em mobilidade desde 1985 – A Toshiba não recorre a terceiros para fabricar os seus produtos empresariais e atesta a fiabilidade e robustez de toda a sua oferta com os Testes de Durabilidade de Elevada Qualidade (H.A.L.T.) e a Garantia adicional de Fiabilidade Garantida (http://www.toshiba.pt/generic/reliability/).

A Toshiba continua a ser pioneira em inovação tecnológica de mobilidade e segurança, evidenciando estar à altura das atuais necessidades e desafios do mercado corporate.

Info Toshiba
www.toshiba.pt

TOSHIBA
Leading Innovation

Toshiba recomenda o Windows 10 Pro

Tecra X40-D-10G

O seu portátil empresarial de vanguarda que preenche todos os requisitos

O Tecra X40 da Toshiba está na vanguarda da funcionalidade empresarial. A geração mais recente de processadores Intel® Core™ U Series e a nossa tecnologia Hybrid Cooling única proporcionam uma produtividade otimizada e sem compromissos, com uma autonomia da bateria até 11 horas. Protegido por uma estrutura alveolar em magnésio que foi testada segundo a norma MIL STD 810G e pela BIOS interna da Toshiba, a segurança e a durabilidade são asseguradas em todos os locais onde trabalhar. Além disso, o ecrã tátil In-Cell de 14 polegadas, antirreflexo, e um vasto conjunto de opções de conetividade libertam as possibilidades de trabalhar à sua maneira onde quer que esteja. O Tecra X40 é o portátil empresarial que preenche todos os requisitos.

GARANTIA DE FIABILIDADE
Devolução do dinheiro + Reparação gratuita

- 16.9mm — Portátil ultrafino: 16,9 mm
- 11 hour — Autonomia da bateria de 11 horas, com carregamento rápido
- 1.25 kg — Ultraleve 1,25 kg
- Autenticação de dois fatores
- Ecrã tátil InCell

www.toshiba.pt/b2b

Canalys Channels Forum 2017

O presente e o futuro do Canal na era da DX

A edição deste ano do Canalys Channels Forum EMEA, que terá lugar em Veneza, de 3 a 5 de outubro, abordará as oportunidades que a transformação digital (DX) traz ao Canal, tendo em conta um princípio fundamental: proteger os negócios do presente e prepará-los para o futuro

Vânia Penedo

"Limitless Landscape" é o tema principal do Canalys Channels Forum (CCF) EMEA de 2017, que irá considerar a forma como a atual paisagem digital está a ser transformada e moldada pelas principais tendências tecnológicas e de negócio. O evento, que tem como principais *keynotes* a Dell EMC, a HP, a HPE e a Lenovo, e onde são esperados cerca de mil visitantes, vai abordar a proliferação de dispositivos e sensores que estão por detrás da Internet of Things (IoT) e que têm conduzido a uma explosão do volume de dados que estão a ser gerados. Esta crescente corrente de informação tem levado ao aumento exponencial da procura por processamento e armazenamento, e da infraestrutura necessária ao seu suporte.

Jordan de Leon, Canalys senior analyst

Ao longo dos três dias, em Veneza, Itália, o Canalys Channels Forum equacionará a próxima fase da cloud, os requisitos que estão a acelerar a adoção do multi-cloud e das soluções híbridas, e a forma como a própria inteligência artificial está a ser utilizada para gerir *workloads* em ambientes *edge* distribuídos, não deixando de parte a revolução trazida pela robótica.

Mecanismos para ser bem-sucedido

A grande prioridade, no entanto, será a de ajudar as empresas do Canal a protegerem e ampliarem os seus negócios, através da partilha dos mecanismos necessários e das evoluções nas estratégias, tecnologias e programas dos *vendors*. O evento promete ainda ajudar a identificar as oportunidades desta nova e mutável realidade, explorando a emergência do *edge computing*, vital para assegurar uma ausência de limites à latência e à largura de banda que a IoT exige.

No meio de toda esta transformação, o que preocupa realmente os Parceiros? "Faturar, ser rentável e, ao mesmo tempo, permanecer relevante para os clientes", adianta ao *IT Channel* Jordan de Leon, Canalys *senior analyst.* "Por isso, no CCF, queremos garantir que estamos a facultar uma visão sobre futuras oportunidades, mantendo ao mesmo tempo um olhar sobre as necessidades do negócio a curto prazo", destaca o analista. E porque a ênfase do CCF tem sido a de construir e alimentar uma rede de relações que potencie oportunidades negócio, a organização introduziu este ano algumas mudanças na agenda, "para que haja ainda mais tempo livre para estas reuniões 1:1, que são fundamentais", acrescenta.

Evoluir para os serviços, cautelosamente

O CCF EMEA promete tocar nos temas mais importantes para a sustentabilidade e rentabilidade do Canal: o que é hoje real e o que devem os Parceiros começar a planear? Que competências devem adquirir? Onde devem investir (tecnologia /vendas), de modo a serem bem-sucedidos na era das tecnologias e serviços digitais? "As exigências sobre os Parceiros estão a mudar", sublinha Robin Ody, Canalys *research analyst*. "Os clientes estão à procura de um maior conhecimento proveniente dos seus ambientes de IT, recorrendo à tecnologia e aos dados para endereçar novos e específicos problemas de negócio". No entanto, adverte, embora o negócio de revenda tradicional esteja a mudar, "ainda representa uma ampla fatia da receita". Se os Parceiros fizerem a transição para os modelos assentes no serviço "demasiado depressa", diz o analista, podem deparar-se com uma quebra elevada nas receitas, tanto do negócio de hardware como de software. "Gerir e combinar os modelos antigos com os atuais de forma cautelosa é a chave", defende.

Robin Ody, Canalys research analyst

Segundo Jordan de Leon, os *vendors* estão agora "a encorajar os Parceiros a transformarem-se em *providers* da transformação digital". O analista da Canalys observa que tal exige "grandes mudanças" na cultura interna das empresas, nos seus processos e no conjunto de competências, bem como no sistema de recompensas dos próprios *vendors*.

Vendors e Canal – relação em mudança?

Robin Ody defende que os Parceiros de Canal têm o "papel chave" de ajudar os vendors "a perceber melhor as preocupações dos seus clientes" e, portanto, a desenvolver tecnologias e soluções "mais competitivas". Os Parceiros de Canal, por seu turno, por terem a confiança dos clientes do seu lado e as competências necessárias, têm a oportunidade de desenvolver relações "mais fortalecidas" e de prestar consultoria". Os mais pioneiros, adianta, "estão a investir em novas capacidades", até porque têm cada vez maior responsabilidade em relação às estratégias de negócio dos seus clientes. "Se um Parceiro conseguir compreender as necessidades do seu cliente, e entregar tecnologia e serviços que as satisfaçam, será uma adição importante ao ecossistema de Canal de um *vendor*", realça. "Os *vendors* devem reconhecer este aspeto e desenvolver relações mais colaborativas com os seus Parceiros, desde o desenvolvimento de produto aos modelos de consumo e de *engagement*, aos próprios programas de Canal".

Ody carateriza o Canal de heterogéneo, com muitos nichos diferentes, e por isso mesmo "capaz de endereçar muitas preocupações distintas". O analista frisa que "os *vendors* continuam a necessitar do Canal para escalar".

O programa do CCF EMEA 2017 abordará ainda o que significa ser um *digital provider* e implementar a venda digital, os modelos de consumo em mudança, o investimento em formação necessários aos novos serviços e o efeito da regulamentação, como o Regulamento Geral de Proteção de Dados, sobre o Canal e sobre os consumidores finais.

O IT Channel, enquanto media partner do CCF, assegurará uma cobertura alargada no evento

Info **Canalys Channels Forum 2017**

www.canalyschannelsforum.com/emea

A SUA MISSÃO É CRÍTICA.
É ESSA A NOSSA PRIORIDADE.

Quando o seu desafio diário é gerir sistemas de dados, o seu principal objetivo é maximizar resultados e obter acesso imediato e seguro aos seus dados críticos. A Vertiv, antiga Emerson Network Power, possibilita o seu sucesso ao proporcionar soluções de infraestruturas e gestão – incluindo as marcas ASCO®, Chloride®, Liebert®, NetSure™ e *Trellis*™ – que sejam eficientes, fiáveis e económicas. É assim que criamos valor para os nossos clientes: fazendo da sua missão crítica a nossa própria missão.

Visite **VertivCo.com/datacenter-pt** para obter mais informações.

VERTIV™