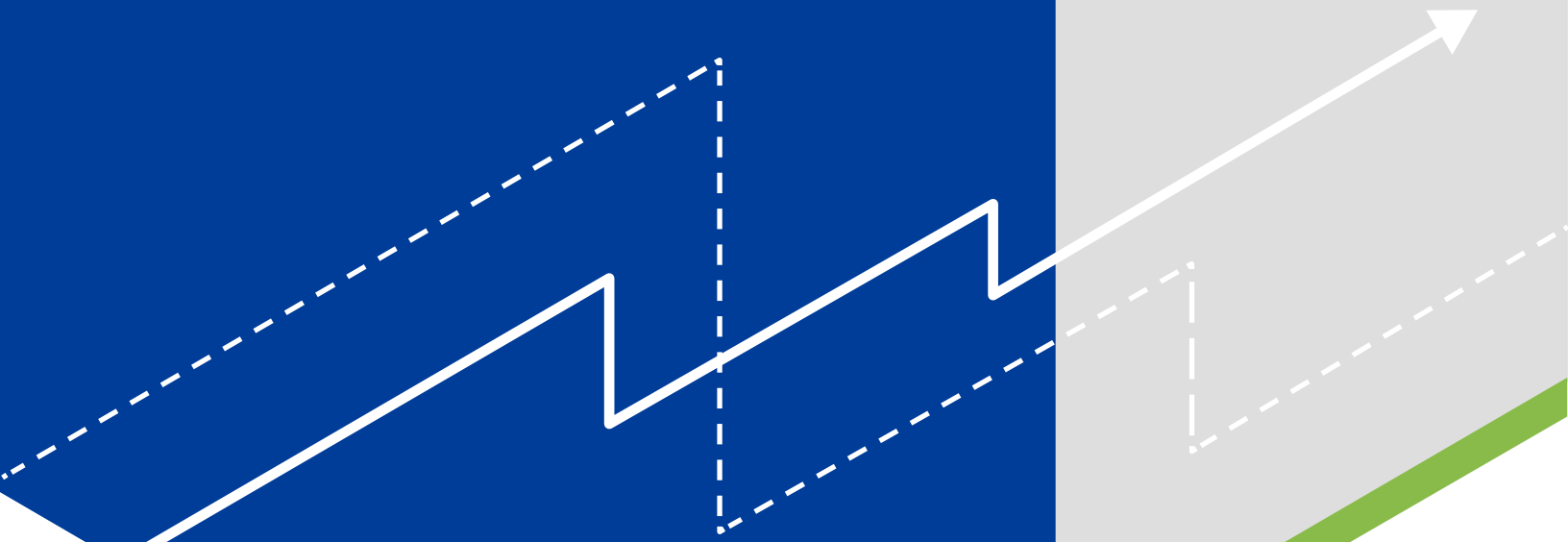
Um artigo sobre ideias inovadoras
da Forrester Consulting
encomendado pela IBM

Março de 2017

Perspectiva Mobile para 2020

O impacto da mobilidade, da Internet das coisas (IoT) e da inteligência artificial sobre o futuro da transformação dos negócios



FORRESTER®

Diretor do projeto:
Heather Vallis,
Consultor sênior de impacto no mercado

Pesquisa colaboradora: Grupo de pesquisa de Segurança e Risco da Forrester

SOBRE A FORRESTER CONSULTING

A Forrester Consulting presta consultoria baseada em pesquisa objetiva e independente para ajudar os líderes a obterem sucesso nas respectivas organizações. Variando em escopo de uma breve sessão de estratégia até projetos personalizados, os serviços de Forrester Consulting conectam você diretamente a analistas de pesquisa que aplicam insight especializado aos seus desafios de negócios específicos. Para obter mais informações, acesse forrester.com/consulting.

FORRESTER®

Resumo executivo

Conforme o mobile ganha mais capacidades e acesso a dados da empresa, os dispositivos móveis continuam a desempenhar uma importante função em como os trabalhadores executam suas atribuições. Trabalhadores da informação não estão mais atrelados aos PCs – smartphones, tablets e laptops dão flexibilidade para escolher o dispositivo mais adequado ao contexto de cada tarefa realizada. A Internet das coisas (IoT) representa o próximo salto na transformação de negócios, mudando a maneira como as empresas percebem, analisam e controlam seus mundos conectados. Porém, conforme o número de dispositivos e objetos que entram em contato com os dados organizacionais confidenciais aumenta, a complexidade de gerenciar e proteger uma superfície de ataque crescente também aumenta. Os funcionários esperam consistência no gerenciamento e nas capacidades de todos os dispositivos que usam para trabalhar; porém, a maioria das organizações adota uma abordagem desconectada, usando equipes e ferramentas distintas para segurança e gerenciamento de *endpoint*. Para reduzir a quantidade de atributo e a complexidade interna, as organizações precisam considerar abordagens tanto específicas do dispositivo quanto independentes de dispositivo, dependendo dos casos de uso, em que os controles independentes de dispositivo estão focados no aplicativo e em camadas de dados em todos os tipos de dispositivo, não importa o fator de forma.

Aplicar técnicas de inteligência artificial (IA), como computação cognitiva e aprendizado de máquina, à análise de todos os novos dados criados nesse paradigma é não apenas transformacional, como obrigatório conforme a quantidade (e a complexidade) de dispositivos aumenta. As organizações poderão pegar essa inundação de dados e descobrir insight de negócios para melhor impulsionar a convergência do gerenciamento e da segurança desses fatores forma atualmente distintos, levando a um futuro estado de gerenciamento unificado de *endpoint*.

Em outubro de 2016, a IBM contratou a Forrester Consulting para avaliar os meios pelos quais as empresas estão gerenciando e protegendo diversos fatores de forma de *endpoint* hoje e como as estratégias mudarão nos próximos três anos. Ao realizar uma pesquisa de opinião aprofundada com 556 líderes de TI e segurança nos EUA, no Reino Unido, na Alemanha, na Índia e na Austrália, a Forrester descobriu que, embora as empresas tenham uma abordagem descentralizada para gerenciar e proteger smartphones, tablets, laptops e IoT hoje, elas passarão para uma abordagem mais consolidada, e cognitiva, até 2020.

FORRESTER

PRINCIPAIS CONSTATAÇÕES

- **As empresas têm uma abordagem em silos no gerenciamento de dispositivo e *endpoint*.** A computação de usuário final não é mais um modelo padronizado. As organizações estão rapidamente mudando de uma definição de um único PC e imagem para todos os funcionários para uma abordagem que suporta diversos dispositivos para os trabalhadores. IoT é tipicamente gerenciada por linhas de negócios como parte das suas operações. Porém, a maioria das empresas ainda tem equipes e ferramentas separadas para gerenciar todos esses dispositivos. A maioria dos entrevistados (74%) relatou que a respectiva organização adota uma abordagem específica ao dispositivo para gerenciar dispositivos e *endpoints*.
- **O gerenciamento passará a ser mais centralizado nos próximos três anos.** Conforme os ambientes de *endpoint* ficarem cada vez mais complexos e as empresas examinarem mais detalhadamente os custos de propriedade do gerenciamento de *endpoint* e dispositivo, as organizações começarão a mudar de gerenciamento específico do dispositivo para gerenciamento independente de dispositivo. Até 2020, 42% das organizações adotará essa abordagem mais centralizada, contra 26% de hoje.
- **Muitas organizações terão gerenciamento unificado de *endpoint* (unified endpoint management – UEM) em vigor até 2020.** Conforme as organizações trabalham para obter uma abordagem integrada e independente de dispositivo, a implementação de UEM aumentará. Embora apenas 15% tenham essa abordagem de gerenciamento centralizado em vigor no momento, 54% terão implementado soluções de UEM até 2020.
- **Até 2020, a maioria das organizações aproveitará computação cognitiva/IA para gerar insights usando dados do *endpoint*.** Com o crescimento exponencial esperado de dados de *endpoint* de diversos dispositivos e objetos, em 2020, mais de 80% das empresas estarão usando IA/computação cognitiva para obter insights sobre segurança e negócios.

54% das organizações terão soluções de UEM em vigor até 2020.

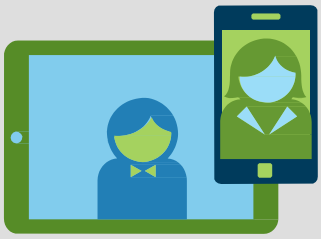
O ambiente de dispositivo corporativo atual é complexo

As empresas atuais estão expandindo as capacidades de dispositivos móveis que oferecem aos funcionários. O uso de dispositivos móveis para realizar tarefas relacionadas ao trabalho tornou-se a regra para a maioria dos trabalhadores: De acordo com uma recente pesquisa da Forrester, 72% dos trabalhadores usam um dispositivo móvel pelo menos semanalmente para trabalhar (veja a Figura 1).[1] Porém, os dispositivos móveis são apenas um dos tipos de ferramentas na caixa de ferramentas do funcionário moderno – aproximadamente metade (49%) dos trabalhadores da informação usa pelo menos três dispositivos para trabalhar semanalmente.[2] Nesse ambiente de trabalho moderno, é importante que os funcionários possam selecionar o dispositivo adequado para cada tarefa que eles executam. Embora smartphones e tablets deem aos funcionários a flexibilidade para acessar rapidamente as informações em trânsito ou atender a clientes em tempo real, laptops e PCs ainda desempenham uma função vital no ambiente de computação corporativo atual. Quase todos os trabalhadores da informação (99%) usam um desktop ou laptop pelo menos semanalmente.[3] Essa proliferação e sofisticação de dispositivos impõe desafios de gerenciamento consideráveis às empresas: Aproximadamente um terço (34%) dos tomadores de decisões de TI e segurança consultados mencionou o aumento no número de dispositivos com suporte por usuário entre os cinco principais desafios de gerenciamento de *endpoint*.

A proliferação de dispositivos com suporte por usuário é um importante desafio de gerenciamento de *endpoint* para **34% das organizações**.

Figura 1

O panorama de dispositivos corporativos: não é mais um modelo padronizado



72% dos trabalhadores usam um dispositivo móvel

49% dos trabalhadores da informação usam pelo menos três dispositivos para trabalhar semanalmente

99% dos trabalhadores da informação usam um desktop ou laptop pelo menos semanalmente

Base: 7.342 trabalhadores da informação globais
Fonte: Pesquisa de telecomunicações e mão de obra de mobilidade da Forrester Data Global Business Technographics®, 2016

FORRESTER®

As empresas estão gerenciando dispositivos em silos

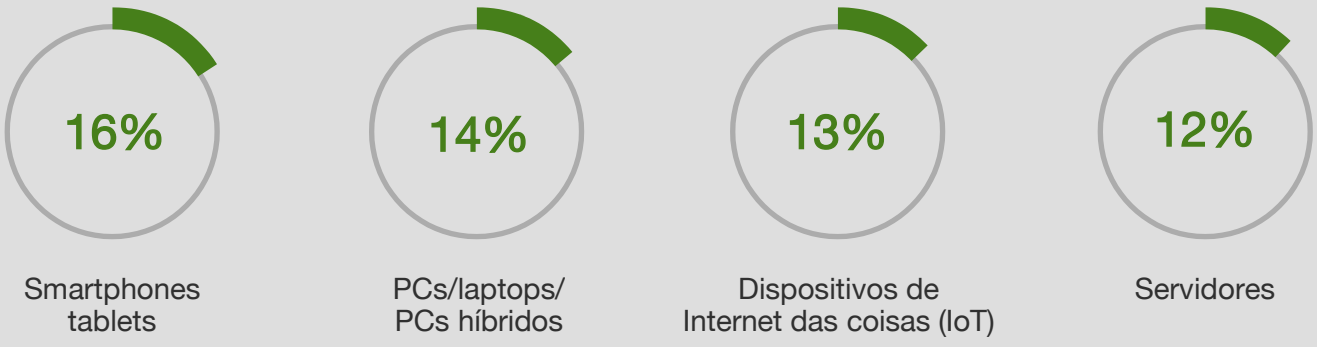
Para trabalhar com eficiência em um ambiente de dispositivos diversificado, os funcionários precisam de conveniência e consistência, não importa o dispositivo que estão usando. Dados e ferramentas disponíveis em um PC devem, idealmente, também estar acessíveis por meio de um dispositivo móvel. Porém, a abordagem descentralizada que muitas organizações adotam quanto ao gerenciamento e à segurança de dispositivos torna difícil, se não impossível, atingir esse objetivo.

AS ORGANIZAÇÕES CARECEM DE UMA EQUIPE DE GERENCIAMENTO DE *ENDPOINT* CENTRALIZADA

Apesar do aumento no uso de diversos dispositivos, muitas organizações ainda estão mantendo seus dispositivos em silos de gerenciamento. Menos de um quinto dos tomadores de decisão de segurança e TI consultados tem uma equipe dedicada para gerenciar tanto dispositivos móveis quanto *endpoints* tradicionais. A maioria das empresas consultadas indicou ter grupos separados para gerenciar dispositivos móveis (smartphones e tablets), PCs, laptops e PCs híbridos; servidores/ e dispositivos da IoT (veja a Figura 2).

Figura 2

"No momento, qual grupo na sua organização é o principal responsável por gerenciar o seguinte?"
(Equipes de *endpoint* móvel/tradicional combinadas)



Base: 556 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

FORRESTER

ENDPOINTS SÃO GERENCIADOS NO NÍVEL DO DISPOSITIVO

Considerando essa falta de conexão entre o pessoal que gerencia fatores de forma de *endpoint* corporativo, não é surpresa que a abordagem dominante para gerenciar e proteger dispositivos também esteja desconectada. De acordo com nossa pesquisa, 74% das organizações estão usando uma abordagem específica ao dispositivo, gerenciando fatores de forma de dispositivo separadamente. Isso provavelmente se deve em parte às limitações das ferramentas de gerenciamento de PC tradicionais. De acordo com uma pesquisa da Forrester com tomadores de decisão de telecomunicações, 49% afirmou investir em ferramentas de gerenciamento de mobilidade corporativa (enterprise mobile management – EMM), porque as ferramentas de gerenciamento de PC não têm capacidade para gerenciar dispositivos móveis.[4] O resultado é que a maioria das organizações usa uma solução para gerenciar os PCs e outra para gerenciar dispositivos móveis. Embora isso não seja uma grande inconveniência ao realizar tarefas básicas de gerenciamento, qualquer correção, implementação de software, política e configuração pode se mostrar difícil. Felizmente, os sistemas operacionais de PC estão se aproximando daqueles de dispositivos móveis em termos de facilidade de gerenciamento e segurança. Uma abordagem distinta ao gerenciamento de *endpoint* apresenta diversos desafios, incluindo:

- ***Endpoints* são gerenciados por meio de diferentes consoles.** Usar diferentes soluções para gerenciar dispositivos empresariais significa trabalhar com pelo menos dois consoles diferentes com interfaces com o usuário (UI) e funções diferentes. 30% dos tomadores de decisão de segurança e TI consultados identificaram a "necessidades de acessar diversos consoles para gerenciar diferentes *endpoints*" como um dos cinco principais desafios de gerenciamento de *endpoint*. Essas ferramentas distintas também dificultam a distribuição de software entre ambientes corporativos complexos (35%). Além disso, na ausência de uma solução única de gerenciamento para gerenciar diversos dispositivos, as organizações carecem de visibilidade consolidada entre todos os endpoints – um problema mencionado por 26% dos respondentes (veja a Figura 3).

74% das organizações estão adotando uma abordagem específica ao dispositivo para o gerenciamento de *endpoint*.

Figura 3

"Quais são os principais desafios de gerenciamento de *endpoint* da sua organização?" (selecione até cinco)

Base: 556 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

Monitoramento contínuo e cumprimento de políticas é o **desafio de gerenciamento de *endpoint* nº 1.**

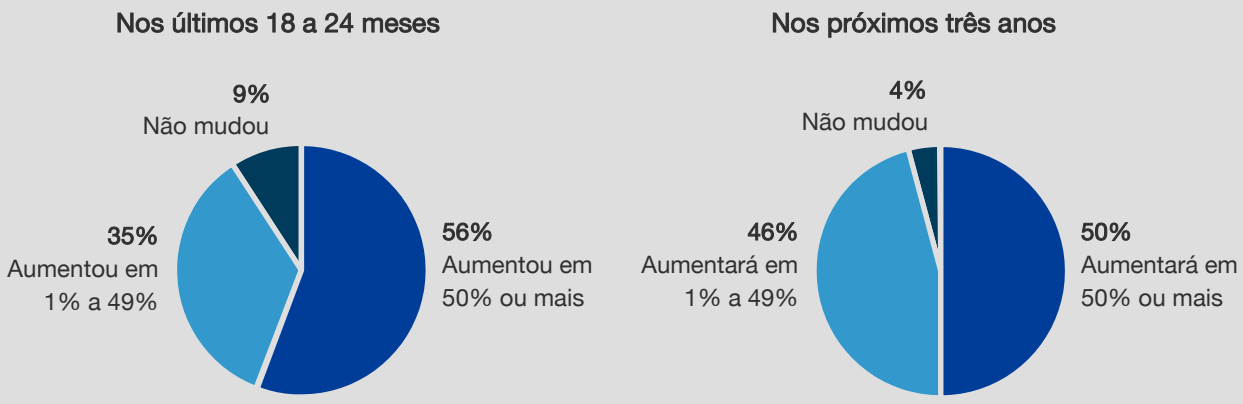
› **Cada solução de gerenciamento precisa ser integrada a outros sistemas separadamente.** Monitoramento contínuo e cumprimento de políticas foi o desafio de gerenciamento de endpoint nº 1 para os respondentes da pesquisa, mencionado por 35%. Para estabelecer monitoramento, políticas e controles consistentes em todos os dispositivos, as soluções de gerenciamento de dispositivo precisam ser integradas a outras soluções corporativas, como controle de acesso à rede (NAC) e gerenciamento de acesso e identidade (IAM). Ainda assim, 30% dos entrevistados relatou falta de integração entre soluções pontuais entre os principais desafios. Quando os dispositivos são gerenciados por meio de diferentes soluções, integrações do sistema precisam ocorrer para cada solução de gerenciamento – o que significa que as integrações precisam ser feitas diversas vezes. Duplicação de esforços aumenta a chance de que sejam cometidos erros, que podem prejudicar a experiência do funcionário e criar lacunas de segurança.

FORRESTER®

- **Volumes crescentes de dados de *endpoint* são coletados por meio de ferramentas distintas.** 56% dos entrevistados indicaram que a quantidade de dados coletados pela organização tinha aumentado entre 1% e 49% nos últimos 18 a 24 meses, e outros 35% relataram um aumento de 50% ou mais (veja a Figura 4). E, essa inundação de dados apenas aumentará nos próximos anos: Embora 46% prevejam que a quantidade de dados de *endpoint* coletados vá aumentar entre 1% e 49% nos próximos três anos, 50% está se preparando para um crescimento de 50% ou mais. As organizações podem obter inteligência significativa de dados de *endpoint*, especialmente para fins de detecção de ameaça e remediação. Porém, a coleção de dados de *endpoint* por meio de ferramentas separadas significa que as organizações carecem de visibilidade entre dispositivos, aumentando o risco de que ameaças em potencial não sejam tratadas de maneira oportuna. Além disso, dados fragmentados tornam difícil obter insights que potencialmente poderiam informar melhorias operacionais e de negócios.
- **É difícil garantir a segurança de dispositivo.** Conforme o número de dispositivos que acessa os dados corporativos aumenta, o mesmo acontece com a superfície de ataque da organização. De acordo com um recente estudo da Forrester, entre os trabalhadores da informação que usam um smartphone pelo menos semanalmente para trabalhar 49% escolheram eles próprios o dispositivo, em vez de seguirem uma lista aprovada pela empresa ou usar um telefone concedido pela empresa.[5] Garantir a segurança desses dispositivos é um desafio considerável. Mais de 30% dos respondentes que consultamos mencionaram "impedir que os usuários inscrevam dispositivos não autorizados" e "garantir que os dispositivos de propriedade do funcionário sejam confiáveis" entre os principais desafios.

Figura 4

"Como a quantidade de dados de *endpoint* coletados pela sua organização mudou nos últimos 18 a 24 meses? Como mudará nos próximos três anos?"



Base: 556 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

IoT contribui para o gerenciamento da complexidade

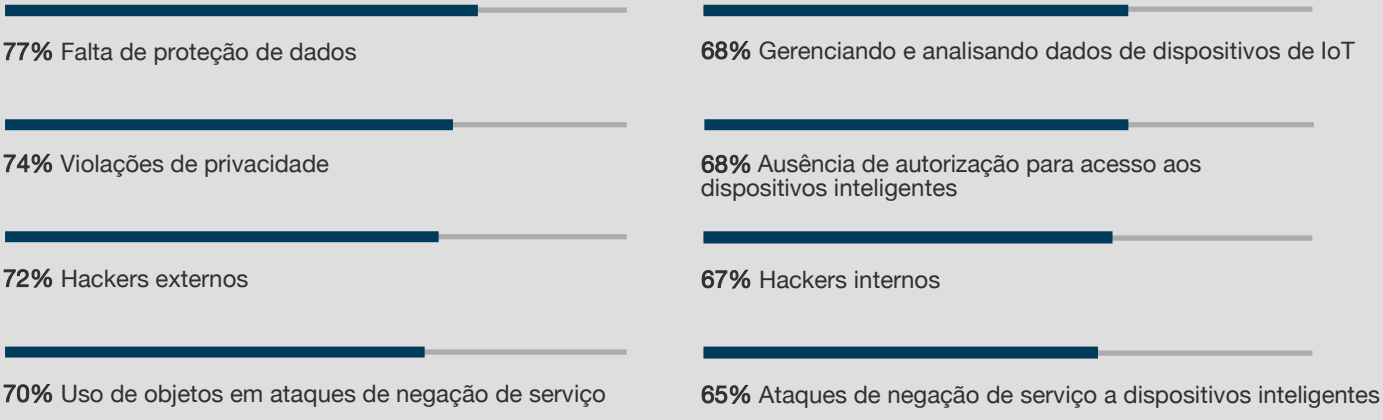
Para a maioria das organizações, a IoT não é uma questão de "se", mas de "quando". 50% dos profissionais de TI e segurança consultados indicaram que suas organizações estão gerenciando dispositivos de IoT agora; 88% preveem que elas estarão gerenciando esses dispositivos até 2020. Ainda assim, a maioria (68%) está muito ou extremamente preocupada com o gerenciamento e a análise de dados de dispositivos de IoT.

As empresas estão adotando dispositivos e aplicativos de IoT que mudarão significativamente a maneira como elas fazem negócios e atendem aos clientes.[6] Porém, conforme o uso desses dispositivos expande-se em ambientes corporativos, o mesmo acontece com os riscos de segurança associado a implementá-los. Conforme a maturidade dos dispositivos de IoT aumenta, passando de objetos simples a dispositivos totalmente autônomos e conectados, a quantidade e a sensibilidade dos dados coletados, analisados e utilizados para tomar ações aumenta significativamente.[7] As principais preocupações entre os respondentes incluem falta de proteção de dados (77%), violações de privacidade (74%), hackers externos (72%) e o uso de dispositivos de IoT em ataques de negação de serviço (70%) (veja a Figura 5). Para minimizar o risco e manter a competitividade, as organizações precisarão criar uma estratégia para gerenciar e proteger aplicativos e dispositivos de IoT, bem como analisar o grande volume de dados coletados.

88% das organizações preveem que gerenciarão dispositivos da IoT até 2020.

Figura 5

"Ao pensar na Internet das coisas (IoT), qual é o grau de preocupação da sua organização com o seguinte?"
(Porcentagem de organizações muito ou extremamente preocupadas)



Base: 556 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

FORRESTER

Perspectiva Mobile para 2020

A abordagem de gerenciamento centrado no dispositivo atual não é apenas complexa, mas também de alto custo. Ferramentas e equipes de gerenciamento separadas significam que as organizações estão dedicando recursos consideráveis a tarefas e funções que podem ser redundantes e ineficientes. Conforme cada vez mais dispositivos chegam à organização, os funcionários exigem um aumento na experiência de computação mais consistente. Enquanto no passado, os usuários tinham experiências muito distintas e diferentes em dispositivos móveis e PC, os sistemas operacionais de PC modernos estão fechando, e continuarão a fechar, essa lacuna de experiência. Com o aumento no controle dos custos para gerenciar esse ambiente, as empresas precisarão aprimorar a estratégia de gerenciamento de *endpoint*.

Olhando para o futuro até 2020, **a consolidação de equipes e ferramentas** será fundamental para **reduzir o custo de gerenciar dispositivos móveis e outros *endpoints.***

REDUZIR O TCO DO GERENCIAMENTO DE DISPOSITIVO E *ENDPOINT* SERÁ FUNDAMENTAL

As empresas estão sob pressão para reduzirem os gastos geral de TI, serem mais eficientes e focarem no custo total de propriedade (TCO) dos seus investimentos. Enquanto 73% dos respondentes relataram que as respectivas organizações estão priorizando reduzir o TCO do gerenciamento de dispositivo e do *endpoint* no momento, a pressão vai apenas aumentar nos próximos anos. Até 2020, 81% das organizações tornará a redução do TCO uma prioridade importante ou principal (veja a Figura 6). Porém, as empresas atuais precisarão superar os desafios de sistemas, ferramentas e equipes distintos e uma abundância excessiva de dados para atender à exigência de reduzir os custos de gerenciamento.

A CONSOLIDAÇÃO TERÁ UM PAPEL CENTRAL NA REDUÇÃO DO TCO

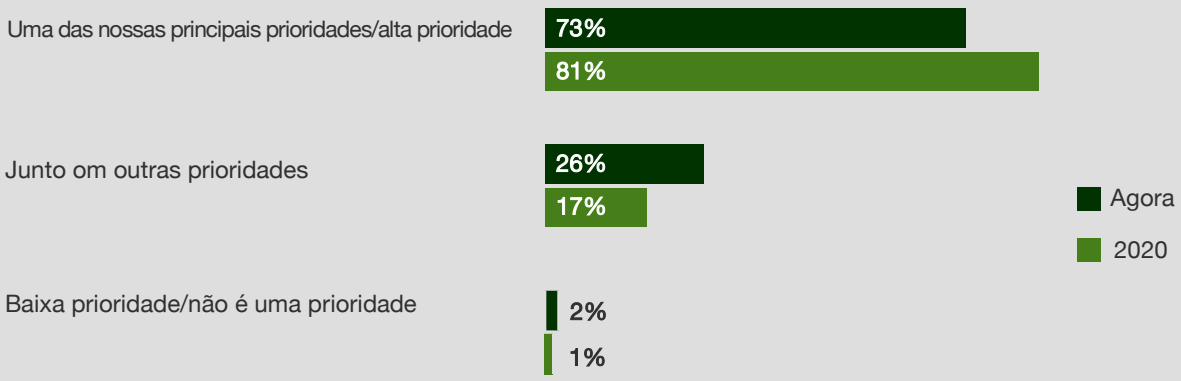
As empresas precisarão criar um plano para enfrentar os desafios de gerenciamento de dispositivo e *endpoint* para reduzir o TCO, e elas devem começar no nível básico. Olhando para o futuro até 2020, a consolidação de equipes e ferramentas será fundamental para reduzir o custo de gerenciar dispositivos móveis e outros *endpoints*. O estudo revelou que as organizações preveem lidar com o TCO derrubando silos de departamentos com uma equipe de gerenciamento centralizado (83%) e consolidando o software de gerenciamento em uma única plataforma ou fornecedor (72%) (veja a Figura 7). Outras medidas de corte de custos incluem usar uma licença de plataforma cruzada para simplificar o faturamento (78%), passar para um modelo de assinatura de software (73%) e passar para a nuvem com um ambiente híbrido ou de software-as-a-service (SaaS) (71%).

Reduzir o TCO de gerenciamento de dispositivo e *endpoint* será uma prioridade alta ou a principal para **81% das empresas.**

Figura 6

"Qual prioridade a sua organização está atribuindo no momento à redução do custo total de propriedade (TCO) para gerenciar dispositivos e endpoints?"

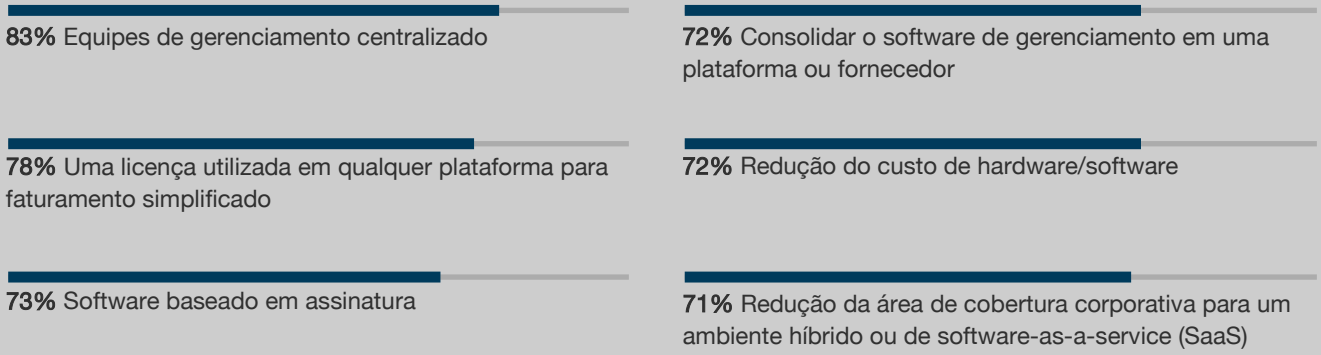
"Em que medida você prevê que a redução do TCO de gerenciar dispositivos e *endpoints* será uma prioridade da sua organização para o ano de 2020?"



Base: 548 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente familiarizados com o TCO de priorização da organização de gerenciamento de dispositivo/*endpoiint*
(os percentuais podem não totalizar 100 devido a arredondamento)
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

Figura 7

"Pensando no futuro até o ano de 2020, qual é a probabilidade de que sua organização vá usar cada um dos seguintes métodos para reduzir o custo total de propriedade (TCO) de gerenciar dispositivos móveis e *endpoints*?"
(Percentual provável ou altamente provável)



Base: 556 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

FORRESTER

O GERENCIAMENTO DE *ENDPOINT* COMEÇARÁ A MUDAR PARA UMA ABORDAGEM INDEPENDENTE DE DISPOSITIVO

Controles independentes de dispositivo estão focados na segurança do aplicativo e nas camadas de dados entre todos os tipos de dispositivo, não importa o fator de forma. Conforme as organizações avançam para consolidação organizacional e tecnológica, elas também precisarão mudar a abordagem para gerenciar dispositivos e *endpoints*. Hoje, a maioria das organizações (74%) adota uma abordagem específica para o dispositivo; porém, as organizações começarão a se afastar dessa maneira isolada de gerenciar dispositivos e *endpoints* nos próximos três anos. Até 2020, 42% preveem que estarão passando para uma abordagem independente de dispositivo – uma alta com relação aos 26% de hoje.

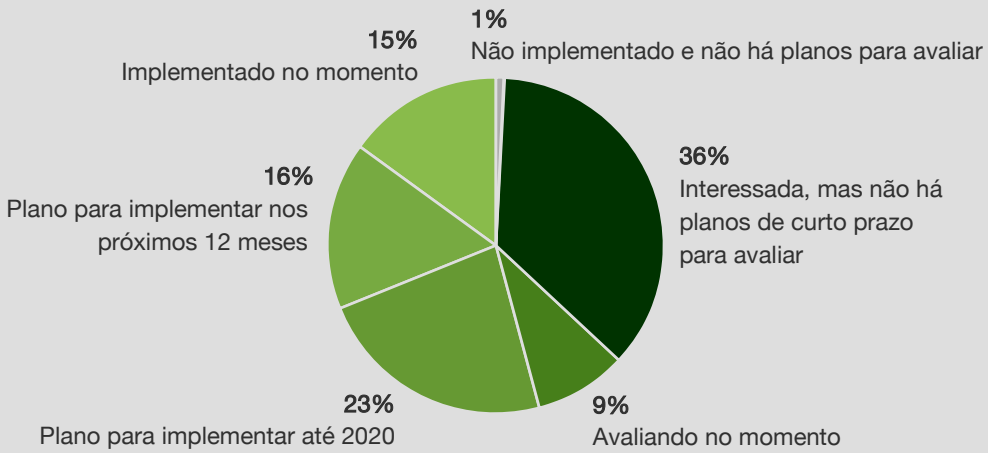
GERENCIAMENTO UNIFICADO DE ENDPOINT FORNECERÁ A BASE PARA A CONSOLIDAÇÃO

O gerenciamento unificado de *endpoint* (unified endpoint management – UEM) é uma abordagem para proteger e controlar tanto *endpoints* tradicionais quanto dispositivos móveis de maneira conectada e coesa usando um único console. Embora algumas organizações (15%) já tenha adotado UEM hoje, a implementação aumentará conforme as organizações trabalham para empregar uma abordagem de gerenciamento mais integrada e independente de dispositivo. 16% das organizações adotarão UEM dentro dos próximos 12 meses; até 2020, 54% terão esse método em vigor (veja a Figura 8).

Até 2020, 42% das organizações preveem que terão passado para uma abordagem de gerenciamento independente de dispositivo – uma alta de **26% com relação a hoje**.

Figura 8

"Quais são os planos da sua organização para implementar gerenciamento unificado de *endpoint*?"



Base: 556 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

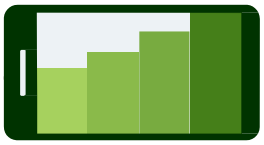
A implementação de UEM aumentará nos próximos três anos conforme as organizações trabalham para adotar uma abordagem de gerenciamento independente de

FORRESTER

A adoção de UEM será conduzida por diversos fatores, incluindo:

- **Proliferação de dispositivo.** Entre os respondentes na organização que estão usando ou planejamento implementar UEM, o principal condutor para a adoção foi uma maior necessidade de gerenciar um número de dispositivos em rápida expansão, mencionada por 43%. Alimentando esse crescimento está a entrada de dispositivos de propriedade do funcionário: 32% relataram que políticas de bring-your-own-device (BYOD) para smartphones, tablets, laptops e desktops são um ímpeto para a adoção de UEM (veja a Figura 9).

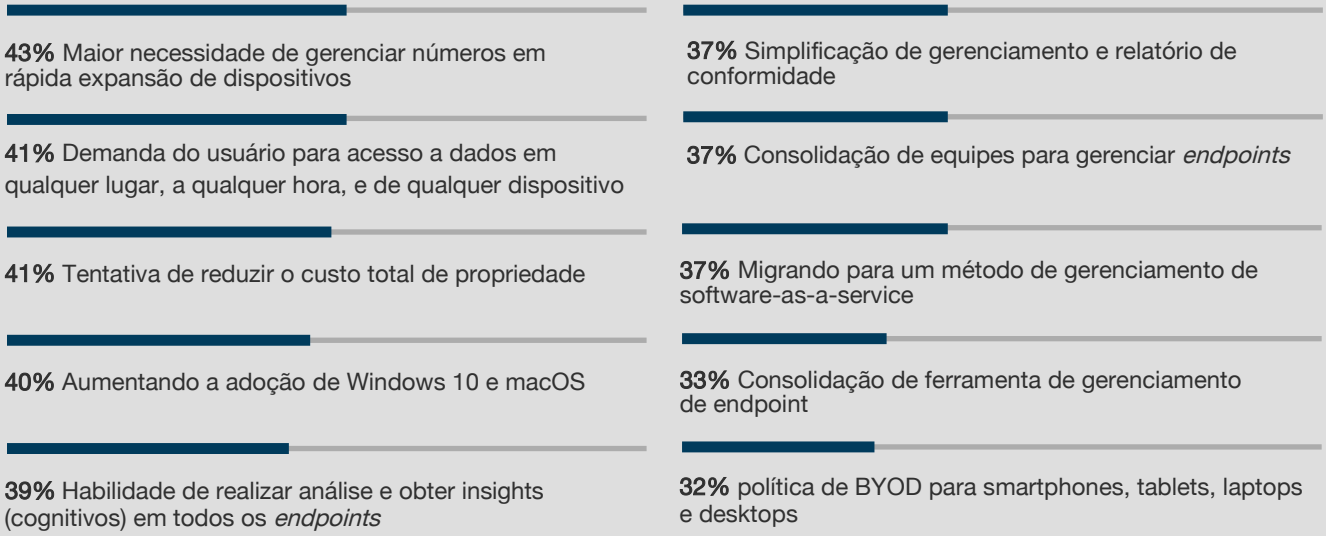
  Um dos principais motivos pelos quais os funcionários estão levando não apenas os próprios dispositivos móveis, como também seus PCs para o escritório, é que os PCs atuais evoluíram, agindo mais como dispositivos móveis. Os sistemas operacionais de laptops modernos estão se aproximando da facilidade de gerenciamento e da segurança dos SOs de dispositivos móveis. De fato, 40% dos respondentes mencionou a adoção crescente de Windows 10 e macOS como um condutor motivador para implementar UEM.
- **Centralização do gerenciamento de *endpoint*.** UEM fornece um ponto central pelo qual as organizações têm visibilidade e controle de todos os dispositivos de funcionários. Essa abordagem centralizada ao gerenciamento significa que as organizações podem consolidar equipes de gerenciamento de *endpoint* e ferramentas, reduzindo funções e tarefas redundantes e diminuindo o TCO. Aproximadamente um terço dos entrevistados estão recorrendo a UEM em um esforço de centralizar equipes (37%) e ferramentas de gerenciamento de endpoint (33%), enquanto 41% veem UEM como um meio para reduzir os custos de gerenciamento de *endpoint*.



O **motivador primário** para a adoção de UEM é uma **maior necessidade de gerenciar um número de dispositivos em rápido crescimento.**

Figura 9

"Quais são os fatores que levaram, ou estão levando, a sua organização a implementar UEM?" (Selecione todas as opções que se aplicam)



Base: 304 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, endpoint ou cliente em empresas que planejam implementar UEM até 2020
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

FORRESTER

- **Demanda por acesso a dados a qualquer hora, em qualquer lugar.** Os funcionários não estão mais presos às suas mesas. Eles estão realizando tarefas relacionadas a trabalho usando diversos dispositivos a cada dia. Para trabalharem com eficiência, eles precisam de acesso aos mesmos aplicativos e dados, não importa o dispositivo que estejam usando. Cerca de dois quintos dos tomadores de decisão de segurança e TI consultados indicaram que a decisão de implementar UEM está sendo conduzida por essa demanda do usuário final de acesso a dados entre dispositivos.
- **Necessidade de capacidades de análise aprimoradas entre todos os *endpoints*.** 39% dos respondentes indicou a habilidade de realizar análise e obter insights entre todos os *endpoints* como um motivador para a adoção. Embora certamente seja possível coletar dados específicos do dispositivo por meio de ferramenta de gerenciamento de dispositivo individuais, a menos que essas ferramentas estejam integradas a outros sistemas de gerenciamento e inteligência, as organizações terão um panorama incompleto. Esse insight é fundamental ao tentar detectar campanhas de ameaça que abrangem vários tipos de *endpoint*, como detectar movimentação lateral entre o laptop e o smartphone corporativo de um funcionário ou qualquer ataque direcionado contra usuários específicos envolvendo vários fatores de forma de *endpoint*. O UEM não apenas atua como um importante ponto de integração para outros sistemas corporativos cruciais, como também consolida dados de endpoint para análise mais significativa e insights acionáveis.

AS EMPRESAS APROVEITARÃO A INTELIGÊNCIA ARTIFICIAL PARA INTERPRETAR DADOS DO *ENDPOINT*

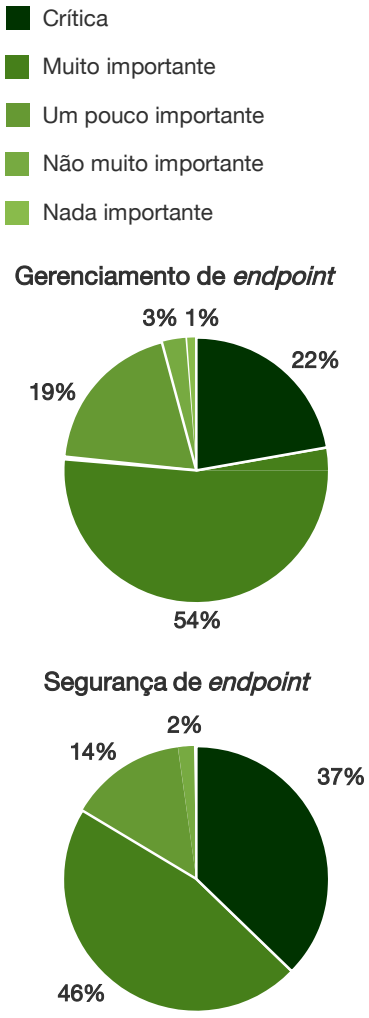
A inteligência artificial (também conhecida como IA ou computação cognitiva) existe desde os anos de 1950s, mas tornou-se cada vez mais popular nos últimos anos devido aos avanços em aprendizado profundo e armazenamento e processamento de dados.[8] De acordo com uma recente pesquisa da Forrester, o investimento em IA/computação cognitiva aumentará em mais de 300% em 2017 em comparação a 2016.[9] IA/computação cognitiva está evoluindo rapidamente para automatizar muitas tarefas manuais, melhorando a capacidade das empresas de gerar insights de negócios acionáveis, obter eficiências operacionais e identificar e remediar as ameaças. IA/computação cognitiva está permitindo que pessoas e sistemas trabalhem juntos de maneira mais colaborativa e eficiente.

Investimento em computação cognitiva/IA vai **aumentar 300%** em 2017.

Conforme o volume de dados coletados de *endpoints* aumenta e as empresas trabalham para consolidar o gerenciamento de dispositivo e *endpoint*, a IA/computação cognitiva passará a ser uma necessidade. De acordo com os respondentes da pesquisa, mais de 80% implementarão IA/computação cognitiva até 2020 para analisar o enorme volume em constante crescimento de dados de *endpoint* coletados. Os profissionais de segurança e TI consultados reconhecem o valor de aplicar IA/computação cognitiva aos dados de *endpoint* da organização, sendo que a maioria indica que elas desempenham um papel muito importante ou crítico no gerenciamento de *endpoint* (76%) e nas estratégias de segurança de *endpoint* (83%) (veja a Figura 10).

Figura 10

"Qual é, ou será, a importância do papel da inteligência artificial/ computação cognitiva na estratégia de segurança e gerenciamento de *endpoint* da sua organização?"



Base: 481 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente em empresas que implementaram, planejam implementar ou estão investigando IA/computação cognitiva Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

FORRESTER

Os respondentes da pesquisa identificaram benefícios de negócios e relacionados à segurança de aproveitar IA/computação cognitiva:

- **Aplicando IA/computação cognitiva à segurança.** IA/computação cognitiva pode ajudar as organizações a fazer melhorias moderadas a significativas às capacidades de detecção e remediação de ameaça, incluindo a habilidade de analisar ameaças em tempo real (80%), melhorar as eficiências do processo de segurança (79%), reconhecer padrões em dados de segurança que indiquem ameaças (78%) e sugerir ou automatizar ações corretivas (74%) (veja a Figura 11).

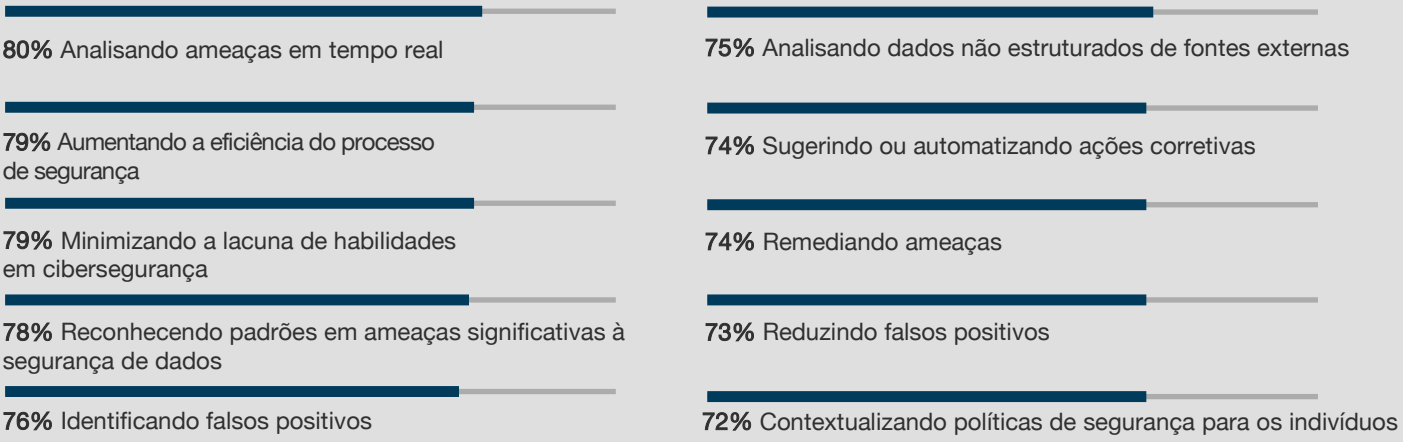
  Tecnologias de IA/computação cognitiva podem analisar com eficiência dados de *endpoint* ou estruturados, encontrando padrões e fazendo conexões de maneira muito mais rápida que os analistas humanos conseguem e ajudando a encontrar ameaças e a identificar falsos positivos. IA/computação cognitiva também podem ser aproveitadas para automatizar processos de segurança manuais, como correlacionar informações sobre ameaça, pesquisar ameaças e investigar alertas, permitindo aos analistas consultar várias fontes de dados não estruturados simultaneamente, acelerando o processo de pesquisa e investigação. Por exemplo, prevenir e detectar ransomware moderno requer insight de todos os executáveis que são executados no *endpoint*, bem como comportamento em memória para impedir variantes avançadas de malware sem arquivo. Correlacionar e obter insights desses dados seria incrivelmente difícil sem o uso de IA/computação cognitiva.

- **Aproveitando IA/computação cognitiva para ganhos de insight e produtividade.** A maioria dos entrevistados reconheceu que IA/computação cognitiva também pode aumentar as eficiências de negócios e a produtividade. 81% afirmam que a tecnologia pode ajudar a gerar melhorias moderadas a significativas em eficiências de operações e administração (veja a Figura 12). Além disso, IA/computação cognitiva pode ajudar a resolver deficiências de aptidão e de pessoal de mobilidade, que foram mencionadas por 75% e 71% dos respondentes, respectivamente. Ao automatizar tarefas e funções, o gerenciamento de dispositivo torna-se mais eficiente, menos manual e mais econômico.

  IA/computação cognitiva pode fornecer às empresas insights eficientes pelo uso de interfaces cognitivas em sistemas complexos, análise de dados avançada e tecnologia de aprendizado de máquina. Essa tecnologia pode promover decisões de negócios mais rápidas ajudando a fechar a lacuna entre insights e ação. Os respondentes da pesquisa reconhecem o valor de aproveitar IA/computação cognitiva para esse fim, com três quartos indicando que a tecnologia melhoraria a capacidade de descobrir insights de dados não estruturados em software de mobilidade (77%), analisar dados de IoT (76%), fornecer importantes insights de negócios para beneficiar a empresa (76%) e, por fim, ajudá-los a tomar decisões orientadas a dados (76%).

Figura 11

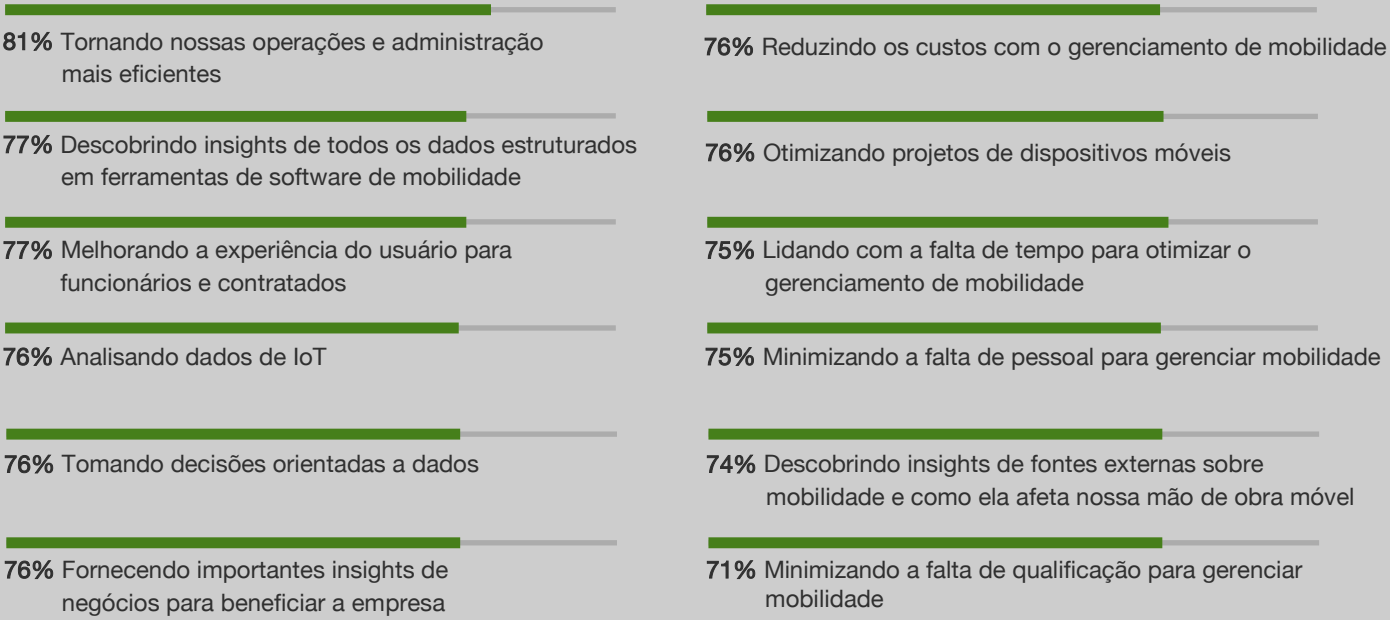
"Em que medida a computação cognitiva/inteligência artificial melhorou, ou poderia melhorar, as capacidades da sua organização nas seguintes áreas de insight de negócios ou produtividade?"
(Percentual de melhoria moderada ou significativa)



Base: 481 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente em empresas que implementaram, planejam implementar ou estão investigando computação cognitiva/IA
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

Figura 12

"Em que medida a computação cognitiva/inteligência artificial melhorou, ou poderia melhorar, as capacidades da sua organização nas seguintes áreas de insight de negócios ou produtividade?"
(Percentual de melhoria moderada ou significativa)



Base: 481 profissionais de TI e segurança envolvidos com segurança e gerenciamento de dispositivo móvel, *endpoint* ou cliente em empresas que implementaram, planejam implementar ou estão investigando computação cognitiva/IA
Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

FORRESTER

O que significa

A proliferação de dispositivos forçará as organizações a buscar maneiras de simplificar a prática de segurança e gerenciamento de dispositivo do usuário final. Hoje, a maioria das organizações trata dispositivos móveis, PCs e IoT separadamente, mas isso mudará ao longo dos próximos três a cinco anos conforme mais equipes de TI adotam ferramentas que lhes permitem realizar um gerenciamento de *endpoint* unificado. A adoção será acelerada pelos novos avanços na computação, como nos campos de inteligência artificial, computação cognitiva e processamento de linguagem natural, permitindo aos administradores rapidamente consultar os respectivos ambientes e adotar ações coordenadas em pontos de controle de PC, dispositivo móvel e IoT. Além disso, novas capacidades de análise apresentarão oportunidades para as equipes de gerenciamento e segurança de *endpoint* obterem insights de negócios mais profundos e significativos das quantidades crescentes de dados de *endpoint* enquanto reduzem o atrito operacional e o TCO.

Figura 13

Unified Endpoint Management (Gerenciamento Unificado de *Endpoint*)

Fonte: um estudo encomendado e realizado pela Forrester Consulting em nome da IBM, janeiro de 2017

Principais recomendações

Comece a mudar sua estratégia de gerenciamento de *endpoint* para UEM hoje mesmo:

Identificar maneiras de reduzir o atrito operacional. UEM apresenta oportunidades em áreas como operações de segurança, automação de gerenciamento e inteligência de negócios. Busque fornecedores que se integrem às ferramentas utilizadas pela sua equipe e identifique como automação e análise de dados avançada podem ajudar.

Dobrando a aposta em controles centrados em dados e aplicativos. Sua estratégia de UEM será complementada por eficientes tecnologias de gerenciamento e em nível de dados e aplicativos, como contêineres de dados que protegem e-mail corporativo, navegação na web e aplicativos corporativos. Se você ainda não estiver fazendo isso, comece a mudar seu foco de gerenciamento e segurança centrados no dispositivo para estratégias centradas em aplicativos e dados. Isso permitirá que você proteja o que importa, seus dados e aplicativos sigilosos, enquanto aumenta a tolerância a risco no nível do dispositivo.

Entender que a IoT será uma grande oportunidade para muitos setores. Os líderes de TI e segurança precisam trabalhar com as linhas de negócios para entender as oportunidades e os desafios da IoT e começar a conversar com fornecedores de UEM sobre como eles podem ajudar você a gerenciar esses *endpoints*.

Unificar seu controle e sua inteligência de segurança. Quando você tiver inteligência de *endpoint* unificada, análise de dados avançada e IA/computação cognitiva poderão ser aplicadas para coletar dados para obter insights de negócios que promovam vantagem competitiva e acelerem seu tempo para contenção quando surgirem eventos de segurança.

FORRESTER®

Anexo A: Metodologia

Neste estudo, a Forrester realizou uma pesquisa on-line com 556 organizações nos EUA, no Reino Unido, na Alemanha, na Índia e na Austrália para avaliar os meios pelos quais as empresas estão gerenciando e protegendo diversos fatores de forma de *endpoint* atualmente e como as estratégias mudarão nos próximos três anos. Os participantes da pesquisa incluíram líderes de segurança e TI em organizações com 1.000 funcionários ou mais. Havia uma distribuição uniforme de respondentes de organizações com 1.000 a 9.999 funcionário e organizações com 10.000 funcionários ou mais. Foi oferecido um pequeno incentivo aos respondentes como agradecimento pelo tempo dedicado à pesquisa. O estudo foi realizado em janeiro de 2017.

Anexo B: Material suplementar

PESQUISA DA FORRESTER RELACIONADA

"Build A Cross-Functional Mobile Security Team", Forrester Research, Inc., 22 de fevereiro de 2017

"The State Of Enterprise Mobile Security: 2016 To 2017", Forrester Research, Inc., 12 de janeiro de 2017

"Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution", Forrester Research, Inc., 2 de novembro de 2016

"Quick Take: Your Next Security Analyst Could Be A Computer", Forrester Research, Inc., 10 de maio de 2016

"Secure IoT As It Advances Through Maturity Phases", Forrester Research, Inc., 7 de janeiro de 2016

"The Forrester Wave™: Enterprise Mobile Management, Q4 2015", Forrester Research, Inc., 4 de dezembro de 2015

Anexo C: Notas finais

PESQUISA DA FORRESTER RELACIONADA

[1] Fonte: Pesquisa de telecomunicações e mão de obra de mobilidade da Forrester Data Global Business Technographics®, 2016.

[2] Fonte: Pesquisa de telecomunicações e mão de obra de mobilidade da Forrester Data Global Business Technographics, 2016.

[3] Fonte: Pesquisa de telecomunicações e mão de obra de mobilidade da Forrester Data Global Business Technographics, 2016.

[4] Fonte: Pesquisa de mobilidade da Forrester Data Global Business Technographics, 2015.

[5] Fonte: Pesquisa de telecomunicações e mão de obra de mobilidade da Forrester Data Global Business Technographics, 2016.

[6] A Internet das coisas (IoT), ou o que a Forrester chama de mundo conectado, combina tecnologias que permitem que dispositivos, objetos e infraestrutura interajam com sistemas de monitoramento, análise de dados e controle por redes estilo Internet. Essas soluções ativadas para IoT são muito promissoras, com o potencial de revolucionar a experiência de cliente, melhorar a segurança, aprimorar a integridade e eliminar ineficiências.

[7] Fonte: "Secure IoT As It Advances Through Maturity Phases", Forrester Research, Inc., 7 de janeiro de 2016.

[8] A Forrester define a inteligência artificial (IA) como a teoria e as capacidades que buscam simular a inteligência humana por meio de experiência e aprendizado. Hoje, a IA atua principalmente em uma inteligência aumentada – ela aprimora a inteligência humana fornecendo conhecimento contextual de dados que a mente humana sozinha não consegue acessar nem processar.

[9] Fonte: "Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution", Forrester Research, Inc., 2 de novembro de 2016.