DEMONSTRAÇÃO

JANEIRO DE 2025

Protegendo o endpoint: Como a Dell ajuda a equilibrar a adoção de IA com resiliência cibernética

Gabe Knuth, analista sênior

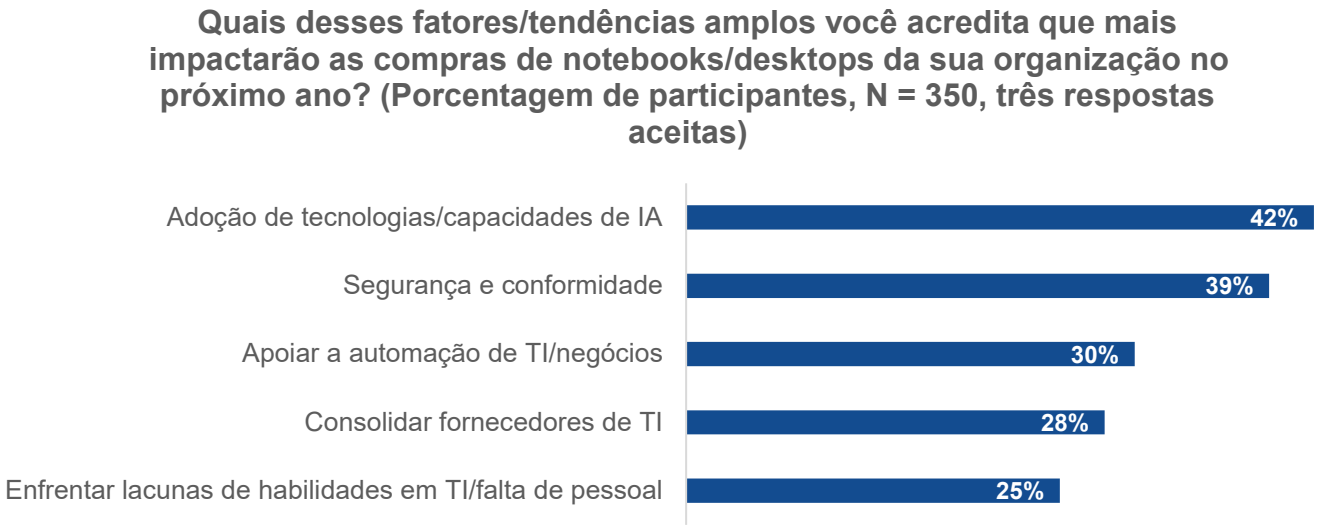
Resumo: O papel da segurança de endpoints está crescendo à medida que a adoção de IA por organizações e cibercriminosos aumenta. Pesquisas recentes do Enterprise Strategy Group da Informa TechTarget destacam as pressões duplas enfrentadas pelas equipes de TI: lidar com ameaças cibernéticas sofisticadas enquanto impulsionam inovações transformadoras.[1] Este documento explora como a combinação de segurança abaixo do nível do sistema operacional, práticas seguras de cadeia de suprimentos e serviços abrangentes da Dell a posiciona como um parceiro confiável para organizações que buscam fortalecer sua postura de segurança.

Visão geral – o problema

À medida que as organizações enfrentam ameaças cibernéticas em constante evolução, a segurança frequentemente se torna a base de qualquer decisão tecnológica. Isso é tão verdadeiro na nuvem e no data center quanto nos PCs, onde, segundo uma pesquisa recente do Enterprise Strategy Group encomendada pela Dell, a segurança está entre os principais fatores que influenciam compras de desktops e notebooks (veja a Figura 1). O mais notável sobre isso é que as organizações deram à adoção de tecnologias e recursos de IA um nível semelhante de prioridade, ressaltando que as organizações estão enfrentando desafios para integrar tecnologias transformadoras como a IA e, ao mesmo tempo, proteger os endpoints contra ameaças cibernéticas cada vez mais sofisticadas.

[1] Fonte: Pesquisa personalizada do Enterprise Strategy Group encomendada pela Dell, *Client Trends and Competitive Landscape* (Tendências do Cliente e Panorama Competitivo), junho de 2024. Todas as referências e gráficos desta apresentação são provenientes desse estudo, salvo indicação em contrário.

Figura 1. Os 5 principais fatores que afetam as compras de endpoint



Fonte: Enterprise Strategy Group, uma divisão da Informa TechTarget

É claro que isso era esperado. A inteligência artificial já está se mostrando transformadora em sua aplicação voltada ao usuário, portanto sua ascensão na lista de prioridades era praticamente certa. Mas tudo o que a IA faz pela produtividade do usuário, pela criatividade e pelos negócios em geral também se aplica aos agentes mal-intencionados, o que significa que esse tandem de adoção de IA e segurança (ou trio, se você considerar conformidade separadamente) provavelmente estará interligado para sempre.

Enquanto o uso da IA e suas preocupações ainda estão sendo definidos por muitas organizações, os desafios relacionados à segurança já estão bem estabelecidos, como:

- Acompanhar os ciclos de atualização de hardware e software (citado por 32% dos entrevistados).
- Proteger dados confidenciais em notebooks e desktops (29%).
- Possibilitar o trabalho híbrido (27%).
- Apoiar uma força de trabalho em expansão (27%).
- Lidar com a gestão de patches (20%).
- Gerenciar o uso não autorizado de aplicativos ou mudanças de configuração (17%).

Esses desafios "clássicos", somados ao surgimento da IA e ao aumento da sofisticação e volume dos ataques, pintam um cenário desafiador para o setor de TI. Na prática, não é possível bloquear tudo, por isso, é fundamental aproveitar todas as ferramentas disponíveis para enfrentar os desafios de hoje e os que estão por vir.

O que as organizações podem fazer?

Para enfrentar esses desafios, as organizações precisam aproveitar os recursos de segurança que podem fortalecer suas iniciativas atuais. Frequentemente, isso significa ir além das medidas básicas de segurança e do treinamento de usuários, optando por uma abordagem mais ampla e em várias camadas que possa melhorar a resiliência cibernética a longo prazo.

Uma das camadas frequentemente ignoradas (ou pelo menos subestimadas) é o papel da segurança em nível de hardware, ou "abaixo do sistema operacional". A segurança baseada em hardware reduz a superfície geral

de ataque de uma máquina, o que pode atenuar os ataques antes que eles tenham a chance de se consolidar. Uma segurança mais robusta na base complementa ferramentas baseadas em software para configuração, análise e correção, o que reduz a carga sobre os recursos de TI constantemente ocupados com alertas e problemas detectados.

Se o hardware é tão poderoso, por que costuma ser negligenciado? Com muita frequência, o hardware é visto como uma commodity, um mal necessário que requer aplicação de patches e manutenção ou, pior ainda, é implementado e esquecido por completo. Na verdade, cada nova geração de chipsets traz recursos de segurança mais avançados, capazes de proteger contra ataques de firmware e hardware. Mais recentemente, o hardware passou a incorporar medidas de segurança integradas que trabalham em conjunto com ferramentas de segurança do sistema operacional para detectar comportamentos anômalos profundos em aplicações.

Embora a atualização de um dispositivo ou de seu firmware tenha sido historicamente vista como algo feito apenas quando estava desatualizado ou com problemas, a realidade é que essas atualizações geralmente melhoram a postura geral de segurança, especialmente porque essas atualizações são para dispositivos de usuários finais! Por isso, os recursos de segurança lideram a lista de critérios para a escolha de um fornecedor de CPU (consulte a Figura 2).[2]

Figura 2. 5 principais fatores na escolha de um fornecedor de CPU

Fonte: Enterprise Strategy Group, uma divisão da Informa TechTarget

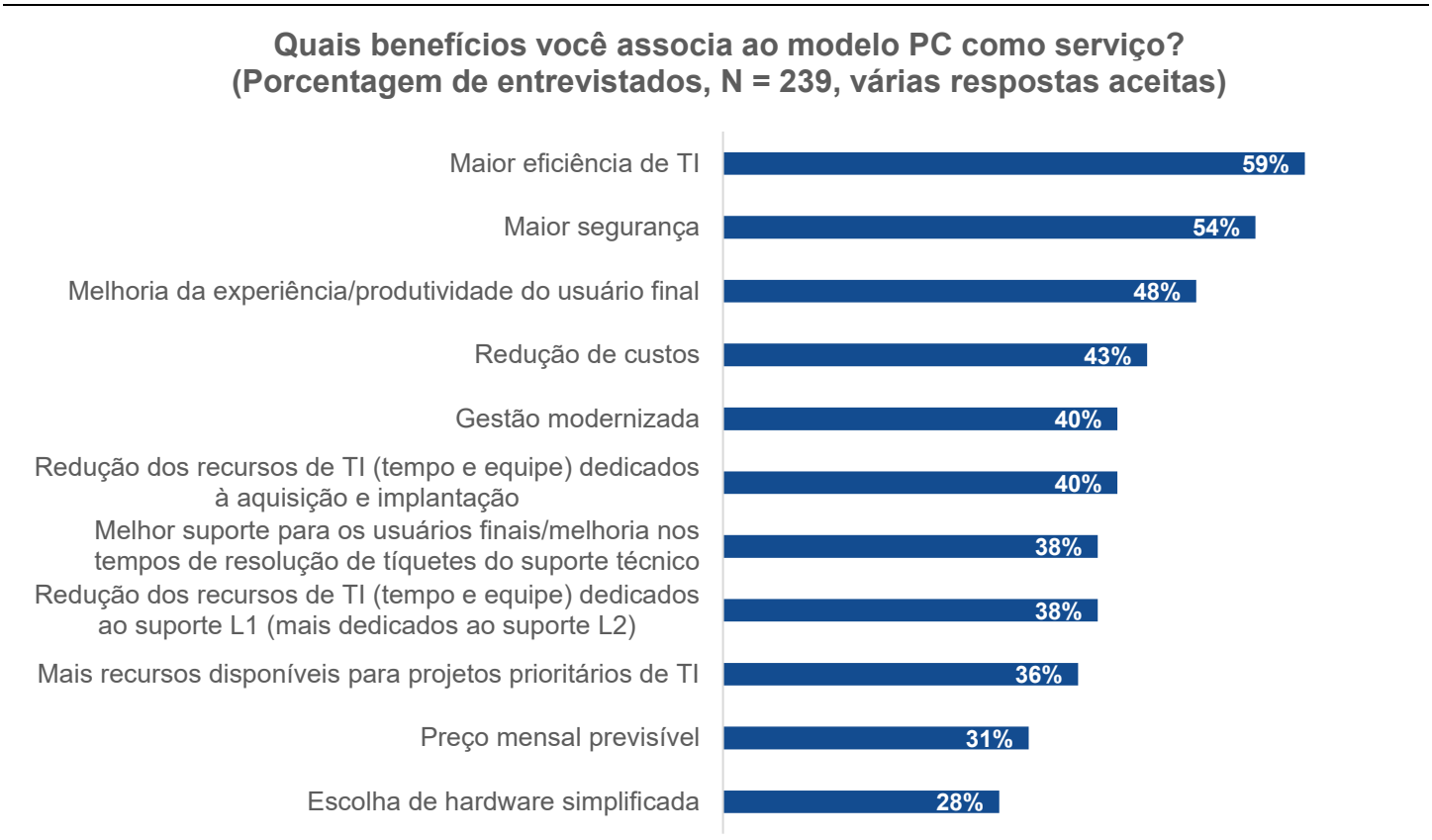
Há também elementos de segurança que não são considerados com frequência pelos administradores, como a segurança da cadeia de suprimentos, que foi citada por 40% das organizações como um dos principais desafios de aquisição de notebooks/desktops (atrás do gerenciamento de custos, das crescentes demandas dos usuários finais e da velocidade de atendimento).

Tudo isso reforça a necessidade de as organizações trabalharem com fornecedores que demonstrem um compromisso sério com a segurança de hardware e da cadeia de suprimentos. Isso ajudará com as aquisições, com certeza, mas lembrar os 32% das organizações que têm dificuldade em acompanhar os ciclos normais de atualização ou os 20% que disseram que o gerenciamento de patches é um desafio sugere que as organizações também poderiam usar ajuda com as tarefas diárias de segurança.

[2] Fonte: Resultados completos da pesquisa do Enterprise Strategy Group, *Tendências de dispositivos de endpoint*, fevereiro de 2024.

Levando isso em conta, não é surpreendente que as empresas estejam cada vez mais recorrendo a serviços gerenciados como o PC como Serviço (PCaaS). O PCaaS simplifica a aquisição e o suporte, oferecendo dispositivos e níveis de serviço variados com um custo operacional mensal. A pesquisa perguntou aos entrevistados que usam o PCaaS sobre os principais benefícios que associam a ele, e o aumento da eficiência da TI (59%), o aumento da segurança (54%) e a melhoria da experiência/produtividade do usuário final (48%) tiveram destaque nos resultados (consulte a Figura 3), mostrando que há potencial para que os serviços também desempenhem um papel fundamental em uma abordagem de segurança em várias camadas.

Figura 3. PCaaS traz benefícios abrangentes, incluindo maior segurança



Fonte: Enterprise Strategy Group, uma divisão da Informa TechTarget

Como a Dell pode ajudar

Como líder em todas as áreas abordadas até aqui (IA, segurança, experiência do usuário e mais), a Dell está em uma posição única para ajudar seus clientes a atingirem seus objetivos. A Dell entende que a segurança deve ser abrangente durante todo o ciclo de vida do dispositivo, desde a cadeia de suprimentos até a reciclagem. A Dell mantém controle rígido sobre sua cadeia de suprimentos, garantindo segurança e disponibilidade por meio de fabricantes de chips, instalações e canais de distribuição globais e diversificados.

Seus desktops e notebooks comerciais apresentam segurança abaixo do sistema operacional por meio do Dell Trusted Device e do Dell SafeBIOS, um conjunto de recursos que protege a integridade do dispositivo até os níveis de BIOS e firmware. Esse recurso, combinado com o silício de núcleo da Intel, significa que os dispositivos

comerciais da Dell oferecem segurança abrangente em nível de hardware que minimiza a pegada de ataque de cada dispositivo. Essa combinação de Dell Trusted Devices com processadores Intel é um dos motivos pelos quais a Dell é reconhecida como líder em segurança de endpoints. A Dell também inclui software próprio para garantir que o firmware, BIOS e drivers do dispositivo estejam sempre atualizados, o que é especialmente importante para organizações que enfrentam dificuldades com uso não autorizado de aplicativos e gestão de patches.

Por fim, a Dell oferece uma variedade flexível de serviços para apoiar organizações sobrecarregadas pelas crescentes demandas de gerenciamento de segurança de endpoints. ProSupport e ProSupport Plus oferecem assistência técnica avançada e resolução preditiva de problemas, garantindo que os dispositivos permaneçam seguros e operacionais com o mínimo de tempo de inatividade. Para organizações que desejam simplificar ainda mais as operações de TI, o Dell APEX PC-as-a-Service (APCaaS) entrega uma solução completa ao agrupar hardware, software e serviços de ciclo de vida em um modelo de assinatura previsível.

Essa abordagem holística, combinando uma cadeia de suprimentos sofisticada, hardware de ponta, software robusto e serviços flexíveis, oferece às organizações a vantagem inicial necessária para enfrentar os problemas de segurança atuais dos endpoints, permitindo que as equipes de TI mantenham uma postura de segurança forte, mesmo diante da crescente complexidade e escassez de recursos.

Conclusão

A segurança é um desafio constante para as equipes de TI, e está ficando ainda mais difícil, já que a mesma tecnologia que fortalece os negócios também ajuda os criminosos. Mas isso não precisa ser uma batalha perdida. Mesmo com tendências emergentes como a IA ganhando prioridade, é importante manter o foco na necessidade de uma segurança abrangente dos endpoints. As organizações podem tomar medidas significativas para enfrentar seus desafios criando uma abordagem em várias camadas que aproveite o hardware, o software e os serviços.

Frequentemente, isso significa trabalhar com parceiros confiáveis, e é por isso que o portfólio da Dell se destaca. O foco da Dell em segurança em nível de hardware, proteções de ciclo de vida ponta a ponta e ofertas de serviços flexíveis garante que os clientes tenham as ferramentas e o suporte necessários para lidar com as tarefas diárias de segurança e com objetivos estratégicos de longo prazo, tudo isso enquanto adotam e extraem valor das tecnologias emergentes. Em resumo, as soluções da Dell estão bem preparadas para atender às demandas dos ambientes modernos de TI.

Num mundo onde IA e segurança se tornam prioridades igualmente críticas, as organizações devem adotar estratégias que façam do endpoint tanto uma ferramenta de produtividade quanto um elemento-chave dos objetivos de cibersegurança. A capacidade da Dell de unir essas prioridades em uma abordagem unificada a torna a escolha natural para organizações que valorizam inovação, confiabilidade e tranquilidade.

Para mais informações, visite dell.com/endpoint-security.

Sobre o Enterprise Strategy Group O Enterprise Strategy Group da TechTarget fornece inteligência de mercado focada e acionável, pesquisa de demanda, serviços de consultoria de analistas, orientação estratégica de GTM, validações de soluções e conteúdo personalizado que dá suporte à compra e venda de tecnologia empresarial.

contact@esg-global.com

www.esg-global.com