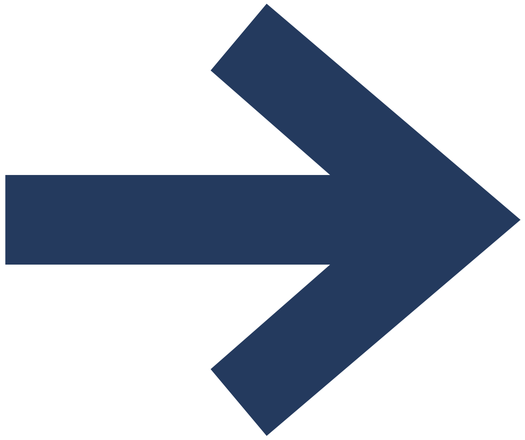
Windows 11

Começando no ponto de extremidade

Uma nova abordagem para modernizar dispositivos, sistemas e o trabalho em equipe



Os pontos de extremidade são o novo local de trabalho

Este e-book não vai dizer que o mundo mudou, que os funcionários querem mais flexibilidade, que os clientes querem mais conveniência, que os criminosos cibernéticos querem ter acesso aos seus dados ou que você pode usar a tecnologia para enfrentar esses desafios. Os líderes de TI e de negócios já sabem tudo isso.

O que pode ser menos conhecido é o conceito do foco em pontos de extremidade, como computadores pessoais e dispositivos móveis, como base para impulsionar projetos de modernização em larga escala. Tradicionalmente, para permitir o trabalho remoto, implementar novas medidas de segurança ou simplificar o gerenciamento de TI, as organizações precisavam implantar e gerenciar soluções separadas para cada objetivo. Além disso, precisavam reimplantar algumas soluções várias vezes para serem executadas em vários dispositivos.

Mas o trabalho remoto em massa inspirou (ou exigiu, dependendo do seu ponto de vista) uma nova abordagem na qual todos esses recursos são integrados ao próprio sistema operacional. Os benefícios potenciais e o retorno sobre o investimento são relevantes. Os funcionários podem aproveitar experiências mais suaves e seguras com menos tempo de inatividade, mesmo trabalhando em dispositivos pessoais, e os departamentos de TI podem administrar melhor os dispositivos, a infraestrutura e a segurança com uma única ferramenta de gerenciamento.

A modernização dos pontos de extremidade é uma forma prática de concretizar esses benefícios. É um investimento fundamental que simplifica as operações, protege dados e prepara sua organização para alcançar a resiliência e o crescimento.

Definição / modernização dos pontos de extremidade:

A prática de aprimorar a facilidade de uso, a performance de hardware e software, a funcionalidade integrada e a segurança das áreas de trabalho, tablets e dispositivos móveis dos funcionários. Isso inclui dispositivos pessoais que executam aplicações de trabalho.

Capítulo

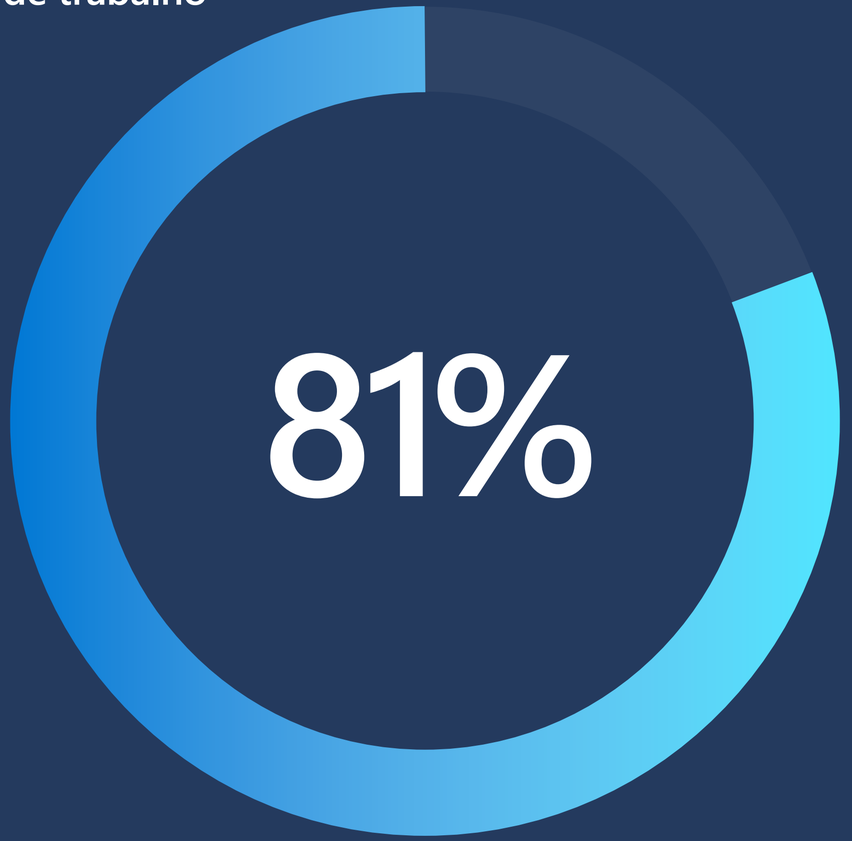
/ 01

Aumente a flexibilidade com a modernização dos pontos de extremidade

O trabalho em qualquer lugar, a qualquer hora e em qualquer dispositivo costumava ser uma vantagem. Hoje, é uma necessidade fundamental para a maioria das pessoas e empresas.[1] Na verdade, de acordo com um estudo da Forrester encomendado pela Microsoft, os empregadores indicaram que permitir o uso dos dispositivos pessoais pelos funcionários para o trabalho, e possibilitar maior flexibilidade entre o trabalho em casa e no escritório, melhora a satisfação dos trabalhadores e reduz a rotatividade.[2]

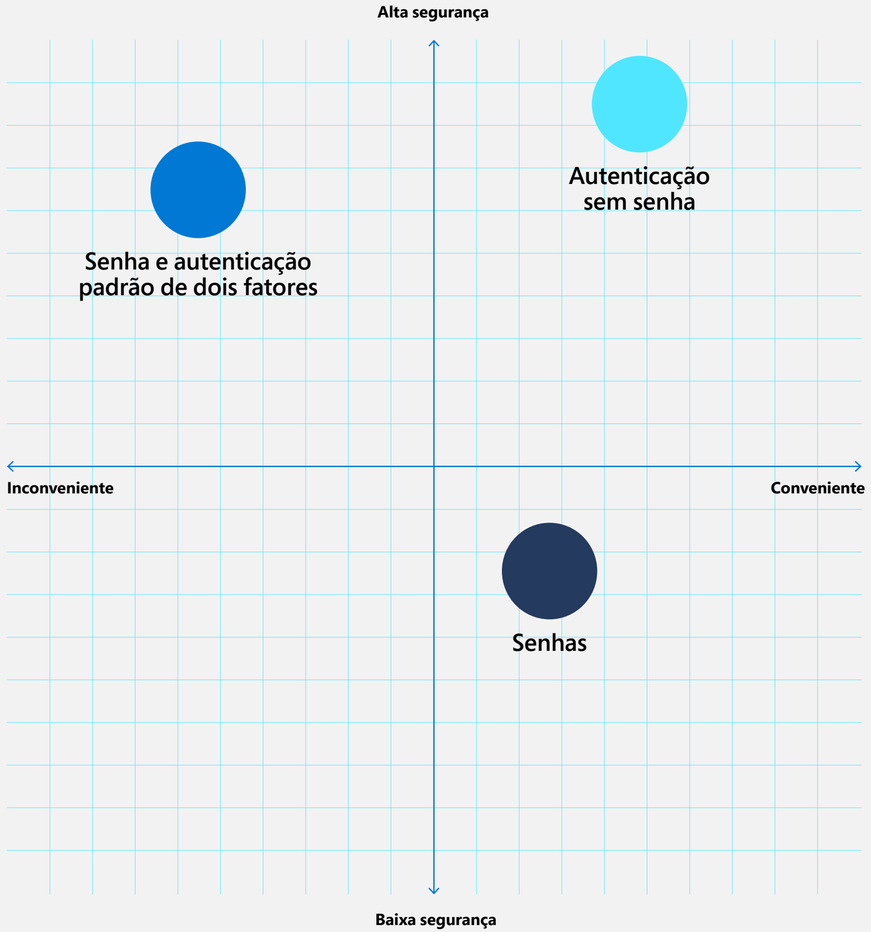
Alternar entre dispositivos não deve ser apenas possível, deve ser fácil, e precisa de uma aparência consistente. As pessoas devem ser capazes de criar apresentações em seus notebooks, editá-las em seus celulares e apresentá-las em seus tablets, tudo sem dificuldades. Toda a experiência deve ser intuitiva e perfeita para que as pessoas possam permanecer no fluxo de trabalho. Para atender a esses requisitos, os departamentos de TI estão cada vez mais focados no sistema operacional dos pontos de extremidade dos funcionários como uma estratégia de modernização fundamental.

Percentual de líderes empresariais que estão ajustando suas políticas de flexibilidade no local de trabalho



[1]"De longe o vencedor," O WorkLab Year em análise, Microsoft, 2021.
[2]The Total Economic Impact™ Of Modernizing Endpoints, estudo da Forrester Consulting encomendado pela Microsoft, setembro de 2021.

A autenticação sem senha é mais segura e mais conveniente do que outras opções



A flexibilidade começa com a TI

A flexibilidade dos funcionários começa no departamento de TI, equipando os trabalhadores de TI e segurança com as ferramentas necessárias para economizar no orçamento e fornecer suporte remoto aos pontos de extremidade.

Para tornar isso possível sem gastar muito tempo, os líderes de TI devem considerar a implantação de soluções como aplicativos de gerenciamento de pontos de extremidade que suportam o gerenciamento de dispositivos baseados na nuvem e na infraestrutura local.

Outra maneira de oferecer flexibilidade é migrando para a autenticação sem senha. O Windows 11 foi projetado especificamente para agilizar esse processo e simplificar a implantação, possibilitando que as pessoas entrem mais rapidamente com um toque ou olhada. É mais rápido e fácil para os funcionários, e torna a invasão muito mais difícil. Há também a autenticação multifatorial, uma parte fundamental da autenticação sem senha, que pode frustrar 99,9% dos ataques cibernéticos.[3]

A modernização dos sistemas operacionais é fundamental

Possibilitar maior flexibilidade aos funcionários não significa fornecer o celular ou notebook mais recente. Trata-se de adotar uma estratégia de TI que permita que as pessoas usem o dispositivo que quiserem com segurança integrada. Para implementar essa estratégia de forma ampla e atingir suas metas de flexibilidade, considere atualizar seu sistema operacional e, conforme necessário, quaisquer dispositivos de ponto de extremidade que não sejam compatíveis sistemas operacionais mais modernos.

[3] "Proteção sem senha: Reduza sua exposição ao risco com a autenticação sem senha", Microsoft Security, 2021.

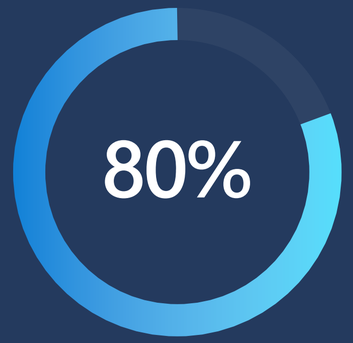
Capítulo

/ 02

Ofereça experiências incríveis aos funcionários

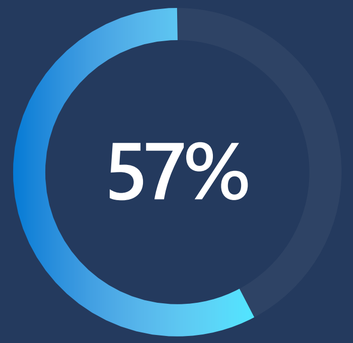
De acordo com o Índice de Tendência de Trabalho de 2022 da Microsoft, 80% dos funcionários afirmaram serem tão ou mais produtivos desde que se tornaram híbridos. 57% dos funcionários remotos pensam em mudar para o trabalho híbrido, enquanto 51% dos funcionários híbridos pensam em mudar para o trabalho remoto. Além disso, empregos remotos no LinkedIn atraem 2,6 vezes mais visualizações e quase 3 vezes mais candidatos em comparação com funções na infraestrutura local.[4] Empresas que oferecem essa flexibilidade com um ambiente de ponto de extremidade modernizado se destacarão em um mercado de talentos competitivo.

Para alcançar o sucesso, todos, incluindo os funcionários, os executivos e os trabalhadores da linha de frente precisam colaborar perfeitamente, acessar informações rapidamente e encontrar tempo para focar no trabalho e no próprio bem-estar. Os funcionários que podem facilmente completar suas tarefas em qualquer lugar são mais felizes e produtivos.[5] Ambientes de ponto de extremidade modernizados os ajudam a manter o dia controlado, e isso afeta suas opiniões sobre a organização.

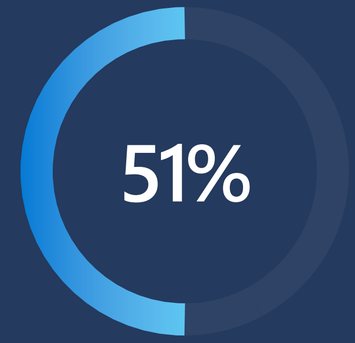


dos funcionários afirmam serem tão ou mais produtivos desde que se tornaram híbridos

mais candidatos para empregos remotos em comparação com funções no local



dos funcionários remotos pensam em mudar para o trabalho híbrido



dos funcionários híbridos pensam em mudar para o trabalho remoto

[4]Índice de Tendência de Trabalho de 2022: relatório anual: Grandes expectativas: como fazer o trabalho híbrido *funcionar,* Microsoft, 16 de março de 2022.
[5]The Total Economic Impact™ Of Modernizing Endpoints, estudo da Forrester Consulting encomendado pela Microsoft, setembro de 2021.

Crie um local de trabalho próspero

A melhoria das experiências dos funcionários com seus dispositivos não significa apenas ajudar a agilizar o trabalho. Também se trata de capacitar os trabalhadores a contribuir de forma mais significativa para a empresa. De acordo com um relatório da Forbes Insights, "os funcionários se beneficiam de uma experiência simples e consistente que melhora a eficiência, a colaboração e a comunicação com os clientes e uns com os outros."[6]

A chave para isso é a eliminação do atrito causado pela alternância entre pontos de extremidade para que os funcionários não precisem desviar o foco do trabalho se precisarem usar outro dispositivo. Por exemplo, um sistema operacional que fornece conteúdo selecionado pode ajudar os funcionários a planejar o dia e acessar facilmente pessoas e arquivos, independentemente do dispositivo. Métodos sem senha, como a digitalização de impressões digitais, PINs e reconhecimento facial simplificam o registro e o acesso ao aplicativo. Além disso, a digitação por voz e o suporte para gestos e canetas eletrônicas simplificam o trabalho em qualquer dispositivo.

Crie uma cultura inclusiva

Os departamentos de TI podem ajudar a promover uma cultura positiva e próspera entre as equipes híbridas, implementando tecnologias que apoiam a participação de pessoas com diferentes estilos de comunicação e origens. Um ambiente de pontos de extremidade unificado promove a colaboração entre dispositivos, locais e documentos. Adotar ferramentas que usam princípios de design intuitivos facilita o início e a participação em reuniões e conversas com pessoas no escritório e ao redor do mundo.

Um local de trabalho inclusivo que capacite os funcionários a ser quem são e realizar tarefas é um poderoso diferencial para as organizações empresariais. A modernização dos seus pontos de extremidade ajuda a oferecer experiências digitais que tornam o local de trabalho mais produtivo e divertido.

[6]"Section IV: Endpoint Modernization," Reimagining Endpoints: Productive and Secure Computing in Today's Hybrid, Front-Line and Edge Environments, Forbes Insights em associação com a Microsoft, 2021.

Capítulo

/ 03

Proteja pessoas, dados e serviços

Conforme os funcionários aumentam a quantidade e a variedade de dispositivos usados para trabalhar, incluindo dispositivos pessoais, os departamentos de TI lutam para manter os pontos de extremidade atualizados e em conformidade. Um estudo com líderes de TI empresariais revelou alguns desafios comuns[7]:

- Conjuntos de soluções de segurança díspares e ultrapassadas.
- Dependência excessiva de VPNs, gerenciamento de identidades desatualizado e controles inadequados de gerenciamento de dispositivos.
- Aumento do risco de violação de dados, políticas restritivas de autenticação que degradam a experiência dos trabalhadores e obstáculos à integração de novas tecnologias e funcionários.

Para enfrentar esses desafios, as organizações estão adotando cada vez mais a **Arquitetura de confiança zero** como uma abordagem holística para garantir a segurança em ambientes com dispositivos pessoais, ativos baseados em nuvem e usuários remotos.[8]

A segurança dos pontos de extremidade começa com uma abordagem holística de confiança zero

Os princípios da confiança zero são:

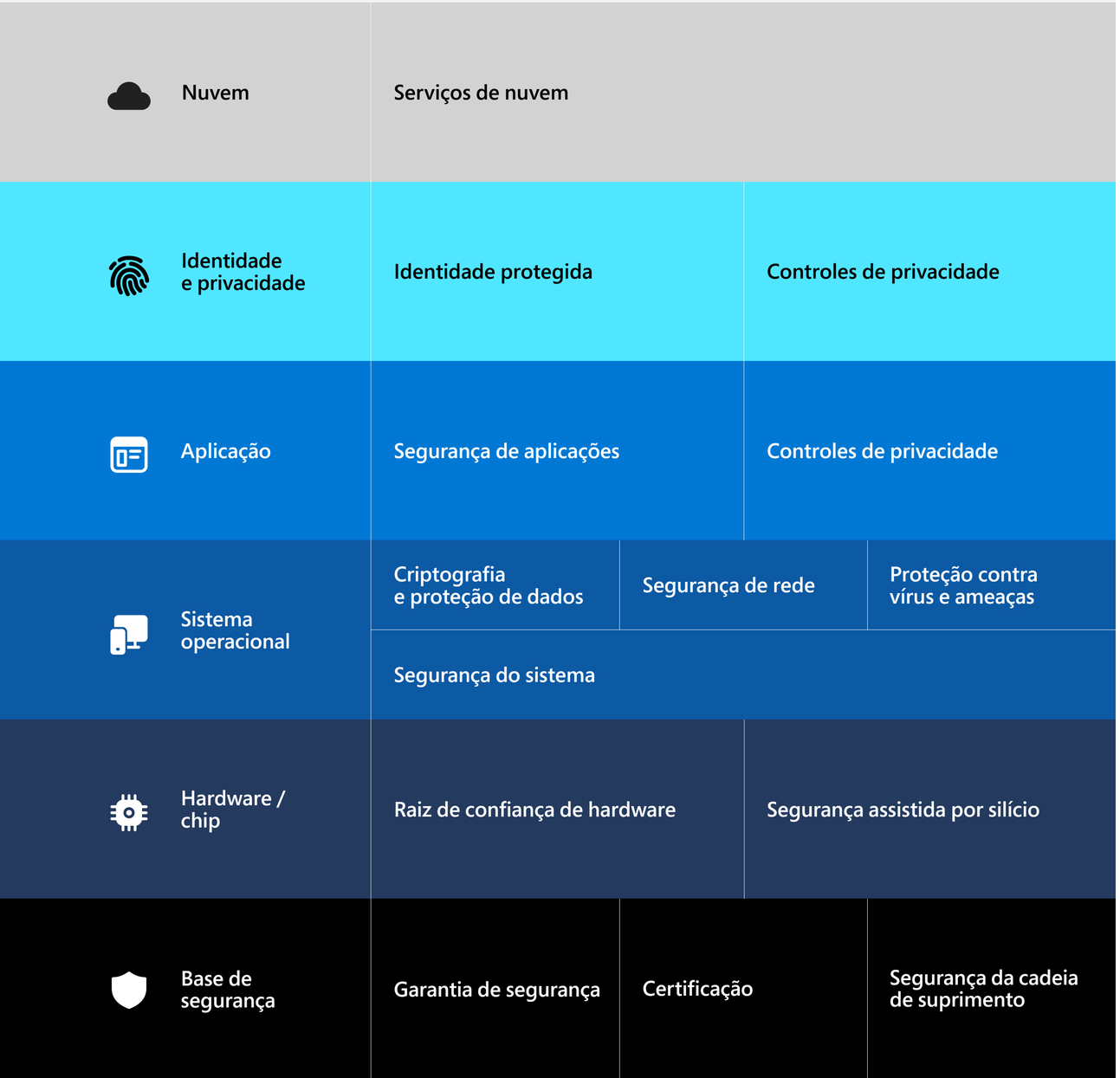
1. **Verifique explicitamente.** Sempre autentique e autorize com base em todos os pontos de dados disponíveis.
2. **Use o acesso menos privilegiado.** Limite o acesso do usuário com acesso na hora certa e apenas o suficiente, além de políticas adaptativas com base em risco e proteção de dados.
3. **Presuma violações.** Minimize o raio de impacto e o acesso ao segmento. Verifique a criptografia de ponta a ponta e use análises para aprimorar a visibilidade, a detecção de ameaças e as defesas.

A Microsoft incentiva o uso de controles de confiança zero para fornecer visibilidade, automação e coordenação entre identidades, pontos de extremidade, aplicações, redes, infraestruturas e dados.

Confiança zero em toda a propriedade digital

[7]The Total Economic Impact™ of Zero Trust Solutions from Microsoft: Cost Savings and Business Benefits Enabled by Microsoft's Zero Trust Solutions. Um estudo encomendado conduzido pela Forrester Consulting em nome da Microsoft. Dezembro de 2021.
[8]McKendrick, Joe. Reimagining Endpoints: Productive and Secure Computing in Today's Hybrid, Frontline, and Edge Environments.

As seis camadas da segurança de confiança zero



A confiança zero se estende do chip até a nuvem

As estratégias robustas de segurança de ponta a ponta devem:

- **Separar o hardware do software** para proteger contra ameaças. O dispositivo de ponto de extremidade fica protegido antes mesmo de ser inicializado.
- **Proteger o sistema operacional** contra o acesso não autorizado a dados críticos.
- **Priorizar a segurança da aplicação** e evitar o acesso a códigos não verificados.
- **Proteger as identidades dos usuários** com a segurança sem senha.
- **Trazer a segurança à nuvem** para ajudar a proteger dispositivos, dados, aplicativos e identidades remotamente.

A segurança de confiança zero dos pontos de extremidade começa com o isolamento baseado em hardware no nível do chip. Dados confidenciais são armazenados atrás de barreiras de segurança e mantidos separados do sistema operacional, de modo que as chaves de criptografia e as credenciais do usuário fiquem protegidas contra acessos não autorizados.

As organizações devem implementar recursos de segurança para hardware e sistemas operacionais que:

- **Protejam e mantenham a integridade do sistema** conforme o firmware é carregado, impedindo que firmwares ou softwares não autorizados sejam iniciados antes da inicialização do sistema operacional.
- **Usem o TPM** (módulo de plataforma confiável) 2.0 para recursos como o Windows Hello e o BitLocker.
- **Criem segurança baseada em virtualização** usando a virtualização de hardware da CPU para proteger uma região de memória isolada do sistema operacional do host para proteger as informações e a integridade do código.

Um desenvolvimento empolgante na tecnologia de raiz de confiança de hardware é o Pluton, um processador de segurança projetado pela Microsoft para frustrar ataques sofisticados. O chip pode ser configurado como o TPM do dispositivo ou como um processador de segurança em casos sem TMP, como a resiliência da plataforma.


Chart
Sales Goal
67%
Junk
Yesterday
Wanda Howard
Tomorrow's Sync
12:55 PM
Let's make sure that we come prepared to
Elvia Atikins
Team Pictures
12:55 PM
We look forward to meeting our fall intervi
Tomorrow, 11:00 AM (30m
RSVP
Alpine Ski House
Opportunity
South Africa Coffee
Opportunity
People
Aadi Kapoor
Files
Trade financing proposal
South African deck
Aida Proposal estimates
12:40
Microsoft

Capítulo

/ 04

Reduza riscos e vulnerabilidades

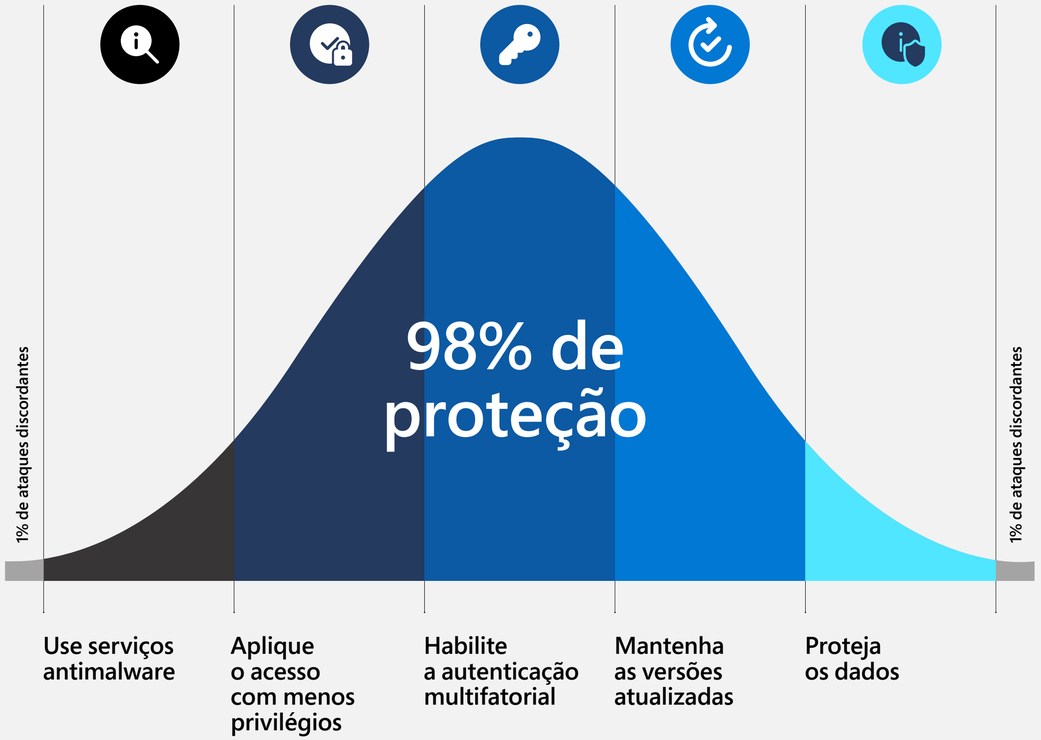
A percepção comum é que os ciberataques são operações complexas e difíceis de impedir. Mas a realidade é que a maioria dos ataques acontece devido a falhas dos funcionários em seguir as melhores práticas básicas de segurança para criar senhas e identificar tentativas de phishing. Na verdade, senhas roubadas são, de longe, a maneira mais comum de invasão a contas empresariais e dados. Mesmo ataques de agentes de estado-nação normalmente dependem de táticas simples como sprays de senha, que se utilizam de funcionários usando senhas fracas.[9]

Só em 2021, a Microsoft detectou e bloqueou mais de 25 bilhões de tentativas de sequestro de contas corporativas.[10] Não foram ataques sofisticados. Eram tentativas simples de acesso à força e senhas roubadas.

Por que, então, tantos departamentos de TI têm dificuldades para evitar essas violações? A explicação é simples: é mais um problema de indivíduos do que um problema de tecnologia. Mesmo que os departamentos de TI precisem continuar educando os funcionários sobre práticas básicas de segurança, existem duas soluções de modernização de ponto de extremidade que ajudam a reduzir a parte "individual" do problema e, portanto, a grande maioria dos ataques: a autenticação multifatorial e as correções.

[9] "Identity is the New Battleground," Cyber Signals, dezembro – janeiro de 2021.
[10] Ibid.

A curva da segurança cibernética: práticas básicas ainda protegem contra 98% dos ataques



Menos de 20% dos clientes da Microsoft usam a autenticação multifatorial.[11]

[11]Relatório de Defesa Digital da Microsoft, outubro de 2021.

O básico dos procedimentos de segurança

- **Uma abordagem de** segurança zero para a autenticação. A confiança zero assume que a segurança do sistema operacional já foi violada e exige que os funcionários verifiquem consistentemente suas identidades usando a autenticação multifatorial.
- **Autenticação multifatorial.** Os funcionários fornecem várias formas de identificação, como tokens de hardware e dados biométricos para acessar suas contas e dados.
- **A autenticação sem senha** elimina a necessidade de senhas geradas por funcionários, que geralmente são o elo mais fraco da segurança de uma organização.
- **Atualização e correção de software,** uma maneira simples e eficaz de prevenir ataques. Os departamentos de TI devem implementar atualizações automáticas para fortalecer a segurança em toda a organização.

Proteção avançada contra ameaças

Além dos cuidados básicos de segurança, a implementação de uma proteção avançada contra ameaças que detecte e responda a ataques antes que eles possam causar danos é fundamental. As organizações devem usar:

- **Um firewall do host,** como o Windows Defender Firewall, para limitar os dispositivos que podem entrar na rede e os dados que podem ser enviados internamente, além de exigir autenticação de qualquer dispositivo que tente se comunicar com dispositivos na rede.
- **Softwares antivírus diversificados** que unem Machine Learning, análise de big data e pesquisa aprofundada sobre resiliência para fornecer proteção abrangente a dispositivos de ponto de extremidade. O antivírus do Microsoft Defender é um exemplo bem conhecido.

Capítulo

/ 05

Habilite o gerenciamento unificado

Uma vantagem fundamental da modernização dos pontos de extremidade é a oportunidade de unificar simultaneamente suas ferramentas de gerenciamento de TI, economizar o tempo da equipe de TI e minimizar os custos de administração. Além de aumentar a eficiência, o uso do centro de controle unificado para gerenciar os pontos de extremidade da organização aumenta a velocidade, a escala e a consistência dos esforços de segurança da sua rede.

A obtenção de um painel de controle administrativo unificado e incorporado ao seu sistema operacional, como no Windows 11, permite que você:

- Gerencie os dispositivos de ponto de extremidade, a segurança e os recursos de nuvem em um único lugar.
- Proteja, implante e gerencie dispositivos empresariais e pessoais sem interromper o trabalho.
- Simplifique a TI com ferramentas que possibilitam o trabalho em conjunto entre diferentes fornecedores e soluções.
- Implemente atualizações de segurança, correções e políticas mais facilmente em toda a organização.
- Avalie rapidamente a conformidade de computadores e dispositivos individuais ou de toda a empresa.
- Proteja-se mais eficazmente contra a violação de informações com a criptografia de todos os dados do sistema.

Gerenciamento de segurança avançada

Vamos conferir mais de perto dois recursos de gerenciamento unificado de segurança que as organizações que usam o Windows devem usar integralmente: o **gerenciamento avançado de política de grupo** e o **gerenciamento moderno de administração de BitLocker**.

Gerenciamento avançado de política de grupo

O uso do gerenciamento avançado de política de grupo para manter as configurações do usuário e da área de trabalho atualizadas permite que os administradores de rede agilizem o trabalho em uma escala maior. Além disso, ele ajuda a reduzir o tempo de inatividade das máquinas dos funcionários em toda a organização.

Em vez precisar configurar cada computador em um ambiente do Active Directory do Windows Server, você pode usar um console central para configurar todos os sites, domínios e unidades organizacionais. Além de reduzir o custo total de propriedade, isso fornece mais controle granular para a equipe de TI sobre as principais atualizações de ponto de extremidade.

Gerenciamento moderno de administração de BitLocker

O uso do gerenciamento moderno de administração de BitLocker agiliza a implantação e o monitoramento de dispositivos protegidos pelo BitLocker e permite que você proteja os pontos de extremidade da rede de forma mais eficiente contra a perda e o roubo de dados.

Isso permite que sua equipe de TI automatize a criptografia de volume em computadores clientes em toda a organização, centralize o monitoramento e a emissão de relatórios de conformidade e simplifique a recuperação de chaves. Ele também permite que seus funcionários aproveitem as ferramentas self-service para recuperar dispositivos criptografados sem precisar entrar em contato com o suporte técnico. Tudo isso ajuda a escalar a implantação do dispositivo e a reduzir o custo de provisionamento e suporte a drivers criptografados.

Capítulo

/ 06

Aumente a produtividade de TI

As equipes de TI estão diante de dois tipos de benefícios de negócios com a modernização dos pontos de extremidade: a **simplificação ou automação de tarefas rotineiras** e a **consolidação ou eliminação de soluções redundantes.**

Simplificação ou automação de tarefas rotineiras

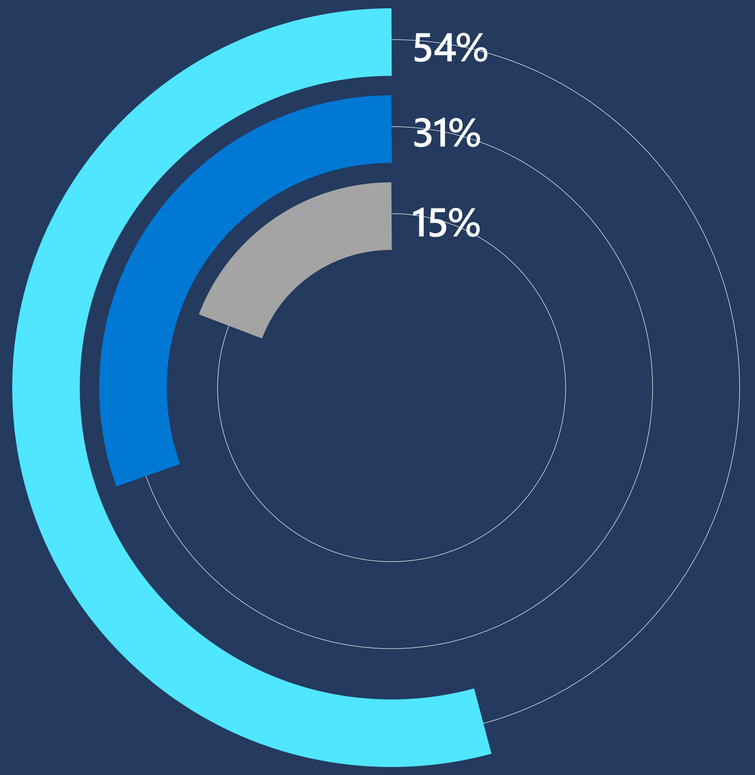
Sabemos que os sistemas operacionais modernizados fornecem aos usuários de pontos de extremidade experiências mais suaves, com maior segurança e flexibilidade e que reduzem os riscos integrados. Mas, para as equipes de TI que gerenciam a tecnologia de ponto de extremidade, esses benefícios também significam um aumento na produtividade. O tempo anteriormente gasto em tarefas repetitivas e cotidianas é poupado para a realização de tarefas mais valiosas. Isso é especificamente benéfico para departamentos de TI menores com recursos e funcionários limitados.

Os ganhos potenciais de eficiência incluem:

- **Redução de chamadas ao suporte técnico.** Ao usar ferramentas como o PIN do BitLocker ou um portal de self-service, os usuários de pontos de extremidade têm o poder de resolver mais desafios tecnológicos por conta própria. Quando os funcionários cuidam de tarefas como atualizar aplicativos ou credenciais de acesso, o suporte técnico economiza tempo para focar em outros projetos.
- **Implantação de soluções e atualizações em escala.** A maioria das equipes de TI ainda provisiona e atualiza dispositivos de ponto de extremidade no local.[12] Pontos de extremidade modernizados permitem implantações fáceis com recursos de implantação remotos e automatizados.
- **Gerenciamento global da política.** Sistemas de gerenciamento de pontos de extremidade modernizados permitem que as equipes de TI gerenciem a maioria das tarefas, como conformidade e segurança, a partir de um único centro de controle. O gerenciamento central das políticas facilita a manutenção das configurações da área de trabalho em toda a empresa e reduz o tempo de inatividade dos funcionários.

[12]The Total Economic Impact™ Of Modernizing Endpoints, estudo da Forrester Consulting encomendado pela Microsoft, setembro de 2021.
[13]Ibid.

A maioria dos departamentos de TI corporativos fornece, atualiza e protege pontos de extremidade no local



Feito no local pela equipe de TI

Feito remotamente pela equipe de TI

Feito remotamente por usuários finais

Base: 301 global IT decision-makers
Source: A commissioned study conduzido pela Forrester Consulting em nome da Microsoft, março de 2021.[13]

Quero comprar uma única licença. Não quero comprar duas licenças para o mesmo recurso.[14]

— Diretor de serviços de usuário e operações de segurança de uma organização farmacêutica

Consolidação ou eliminação de soluções redundantes

Pontos de extremidade modernizados também oferecem às equipes de TI a oportunidade de consolidar, ou mesmo eliminar, os serviços e soluções díspares ou redundantes. Isso poupa orçamento, tempo e recursos para outros projetos.

Soluções de software díspares geram tanto despesas quantificadas quanto não quantificadas. **As despesas quantificadas** são custos medidos com um valor monetário, como os contratos de taxas de licenciamento e os custos de suporte ao fornecedor. **As despesas não quantificadas** incluem investimentos mais difíceis de medir, como o tempo e o esforço de um funcionário para aprender a usar uma nova solução de software e implementá-la dentro de um ecossistema de software existente.

Os pontos de extremidade modernizados não somente têm o software mais recente, mas também têm várias soluções integradas ao sistema operacional. Com um pacote de soluções projetadas para trabalharem em conjunto desde o início, as equipes de TI podem reduzir o número de serviços redundantes e poupar tempo e recursos que antes eram dedicados à manutenção de soluções. Do ponto de vista da otimização de custos, as oportunidades são inúmeras. O estudo da Forrester Consulting Total Economic Impact™ Of Modernizing Endpoints encomendado pela Microsoft estima que a eliminação de soluções de software redundantes reduz os custos em mais de USD 607.000,00 ao longo de três anos para uma organização composta de 4.000 funcionários.[15]

[14] Ibid.
[15] Ibid.

Avalie e desenvolva a estratégia de ponto de extremidade da sua organização

Pode parecer surpreendente que um e-book que recomenda a modernização dos pontos de extremidade também recomende que algumas empresas mantenham suas estratégias de ponto de extremidade atuais. O fato é que muitas organizações tiveram êxito na implantação do trabalho remoto, melhoraram suas ferramentas de colaboração no local de trabalho, implementaram medidas avançadas de segurança e unificaram seu gerenciamento de TI com soluções separadas e complementares. Afinal, a Microsoft tem ajudado as organizações a fazer isso a muito tempo.

Mas a realidade é que, atualmente, faz mais sentido que o Windows considere os dispositivos de trabalho e pessoais, as ferramentas de local de trabalho, os recursos da nuvem e a segurança como se fossem interoperáveis por padrão, porque isso é verdade para a maioria dos funcionários e departamentos de TI. Mesmo que o Windows 10 continue sendo uma plataforma de inovação para muitas organizações de sucesso, o Windows 11, que pode ser implantado no mesmo ambiente que o Windows 10, foi projetado especificamente para atender a essas necessidades de forma mais holística.

Onde quer que você esteja na jornada de modernização de pontos de extremidade, esperamos que as orientações deste e-book forneça informações úteis para que você avalie e desenvolva a estratégia de ponto de extremidade da sua organização.

Saiba mais sobre o Windows 11
Ou explore a documentação de implantação