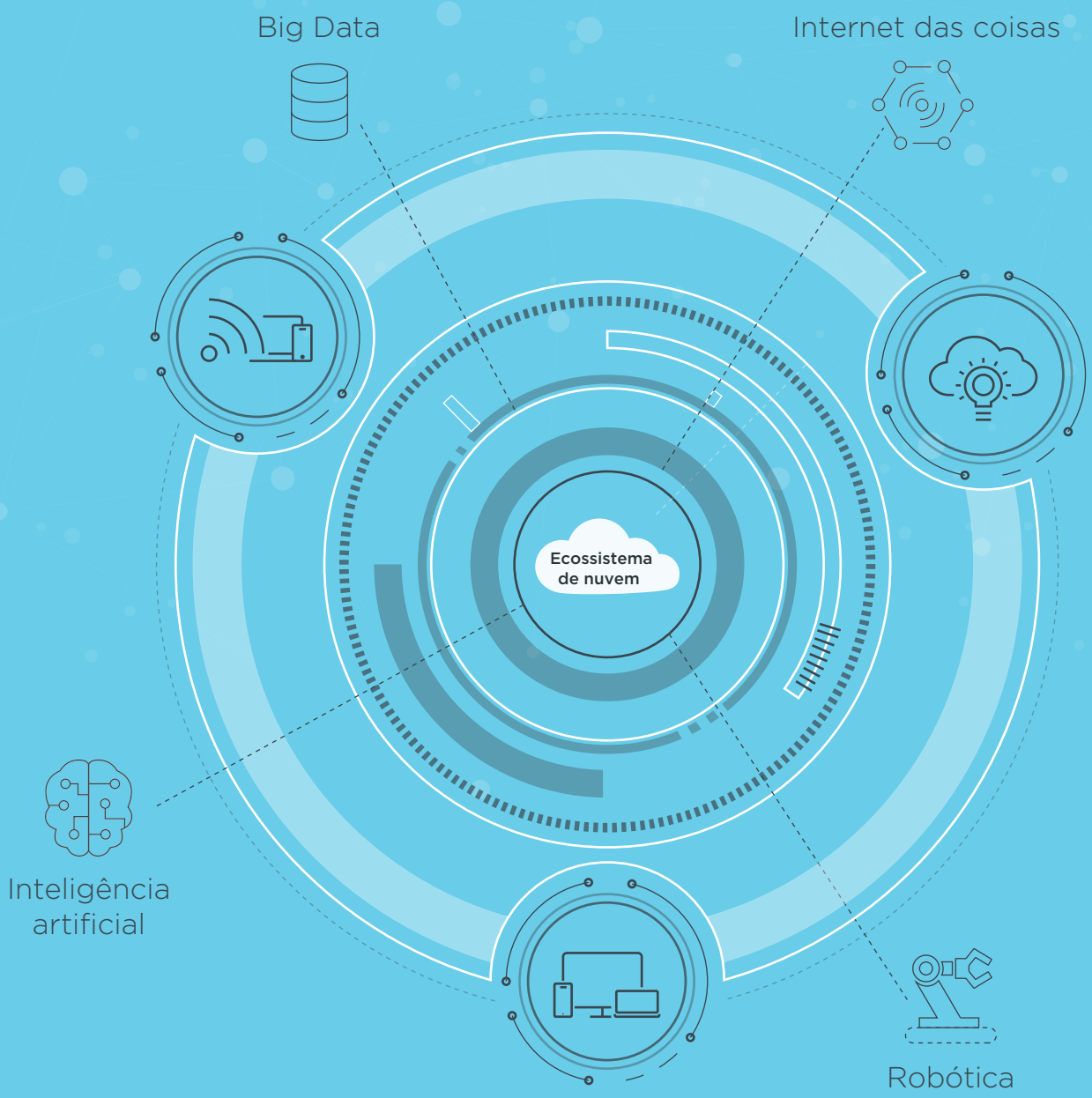
SEGURANÇA NA NUVEM COM OS DISPOSITIVOS CERTOS

Lenovo

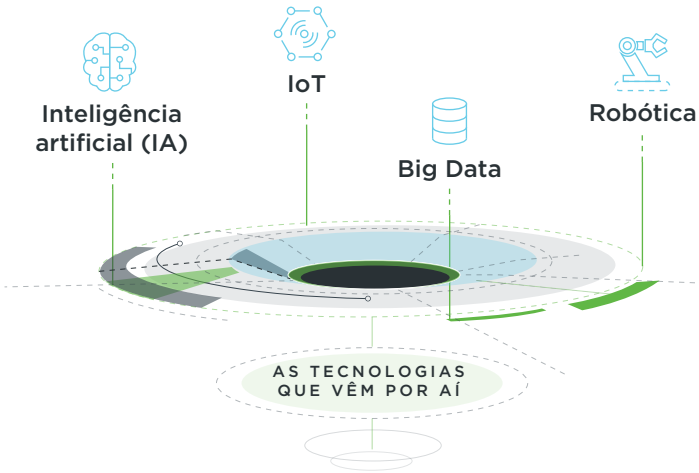


Windows 10 Pro

www.lenovo.com

A maioria das tecnologias que vem por aí, como big data, computação cognitiva, IoT, IA e robótica, depende diretamente da nuvem.

Uma vez que ela é a base para muitas das tecnologias que qualquer organização acabará por adotar (se ainda não tiver adotado), investir em uma decisão errada pode ser prejudicial aos negócios.



Os equipamentos são um aspecto importante do ecossistema de nuvem. Atualmente, a maioria das organizações está percebendo a importância de fornecer os computadores específicos para os requisitos do trabalho. Por exemplo, para gerentes de contas que estão em movimento a maior parte do tempo e precisam fazer muita coisa em trânsito, equipamentos leves, duráveis e flexíveis, como os conversíveis, são uma boa opção.

E, além de escolher o equipamento certo para os trabalhos, a estratégia para dispositivos é essencial, pois eles também decidem a prontidão de segurança da sua organização.

TRÊS ASPECTOS ESSENCIAIS DE UMA ESTRATÉGIA DE NUVEM EFICAZ

Os dispositivos corretos: para seus usuários móveis, fixos e especialistas.

Uma boa solução de nuvem: escolher a melhor para a sua empresa

Gerenciamento e segurança eficazes de dispositivos: escolher a melhor para a sua empresa

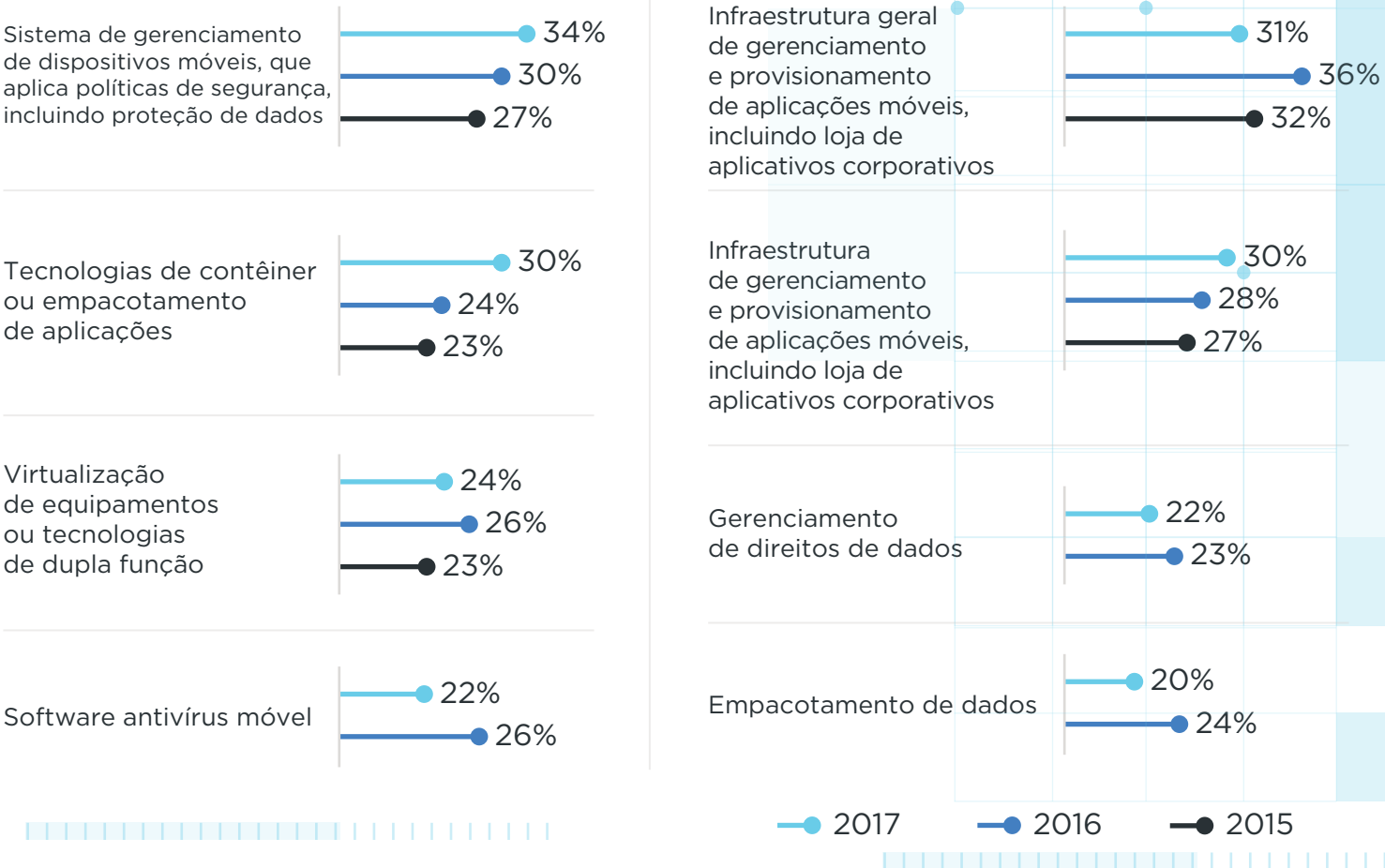
Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

OS DISPOSITIVOS SÃO DECISIVOS

Eles são uma porta de entrada para a rede da sua organização. Assim, ao investir em sua estratégia de segurança, não se esqueça de que sua infraestrutura é tão forte quanto seu elo mais fraco. Não deixe que esse elo seja o computador de algum funcionário.

Adoção de tecnologia de segurança móvel



Fonte:
Forrester Business Technographics 2017

Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

A força de trabalho moderna precisa trabalhar em vários locais, como aeroportos, sites de cliente, cafeterias, etc. A nuvem se tornou um grande facilitador de produtividade e eficiência. Porém, ao mesmo tempo, isso também abriu caminhos para brechas de segurança.

- Acesso não autorizado aos dispositivos
- Uso do Wi-Fi público
- Download de aplicativos/ software de fontes não autorizadas
- Danos acidentais
- Roubo/perda de dispositivos

Cerca de 62% das violações de segurança hoje ocorrem devido a erros dos funcionários.[1]

Windows 10 Pro

Fonte:
[1]:https://www.tektonikamag.com/index.php/2017/07/24/security-breaches

Clique aqui para conhecer as soluções de segurança da Lenovo

Acesso não autorizado aos computadores

Apenas tentar proteger o acesso aos dados por meio de senhas pode não ser a melhor maneira de proteger os dispositivos contra usuários não autorizados.

Quase 40% das pequenas e médias empresas estão planejando investir em abordagens de autenticação de dois fatores nos próximos 12 meses.

Aspectos a considerar para impedir o acesso não autorizado:

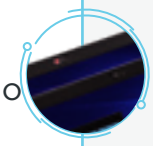
Autenticação biométrica
Autenticação avançada multifatorial, como tecnologias de reconhecimento facial e leitor de impressão digital, para proteger os usuários e seus dados.

Mantenha os espiões longe
Tecnologia que impede que curiosos tenham acesso a dados confidenciais.

Acesso restrito à porta
Evite o roubo de dados através de portas USB, permitindo o acesso apenas a usuários autorizados.

ThinkPad T480s

Leitor de impressão digital Match-on-Chip com Intel® Authenticate
Proteja seus dados com soluções avançadas de segurança biométrica.



Windows Hello e ThinkPad Glance
Esse recurso avançado de reconhecimento facial ajuda a manter afastados os usuários indesejados.

Acesso via Smart Card
Uma maneira altamente segura de armazenar informações de login em cartões invioláveis, sem recorrer a senhas.

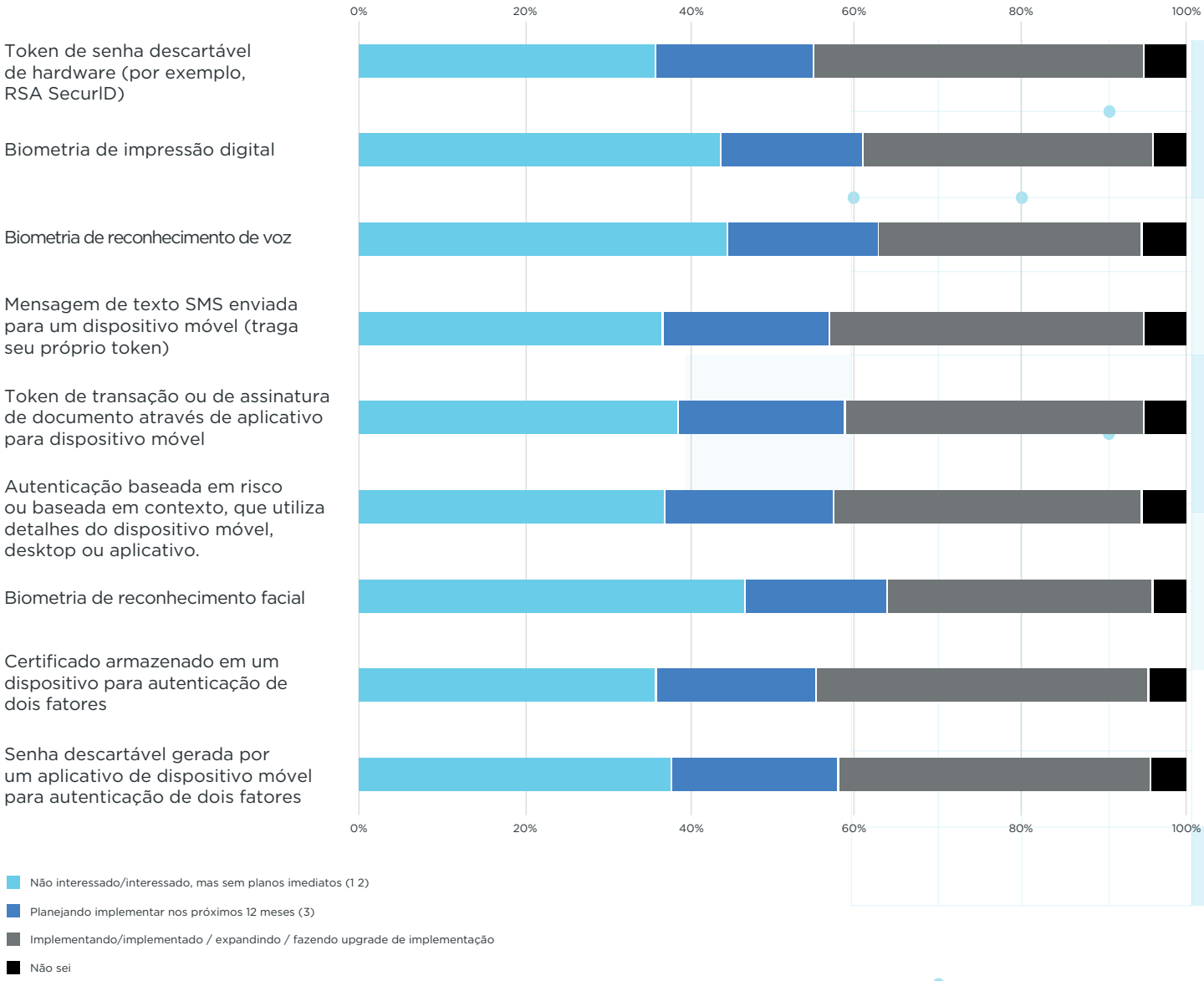
Proteção USB inteligente
Evite o comprometimento de dados, restringindo o acesso às portas.

Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

Acesso não autorizado aos dispositivos

Quais são os planos da sua empresa para adotar as seguintes abordagens de autenticação de dois fatores? (Entrevistados organizados em: expandindo/em expansão + implementado/ em implementação)



- Não interessado/interessado, mas sem planos imediatos (1 2)
- Planejando implementar nos próximos 12 meses (3)
- Implementando/implementado / expandindo / fazendo upgrade de implementação
- Não sei

Fonte:
Forrester Business Technographics 2017

Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

Uso do Wi-Fi público

A maioria de nós não pensa duas vezes antes de se conectar a redes Wi-Fi públicas, que representam vários tipos de ameças, como ataques Man-in-the-Middle (MitM), em que os hackers interceptam seus dados; redes Wi-Fi "piratas" configuradas por hackers e que até parecem legítimas; ataques de Endpoint, em que os hackers podem acessar seu notebook; e worms que transmitem vírus para o seu dispositivo.

Qualquer que seja o modo, **o relatório anual de investigação de violações de dados da Verizon descobriu que 89% de todos os ciberataques envolvem motivos financeiros ou de espionagem**[2]. Claramente, nenhuma organização quer passar por isso.

Portanto, para evitar ataques maliciosos aos seus dados, os dispositivos devem ter:

Acesso Wi-Fi seguro
Uma solução incorporada para reconhecer redes Wi-Fi seguras.

Ameaças contidas
Aplicativos que garantem que o malware não entre diretamente nos computadores.

Criptografia de dados
Aplicativos que criptografam dados na nuvem e fornecem autenticação segura.

ThinkPad X1 Carbon

Lenovo Vantage
Monitore a segurança do Wi-Fi em tempo real, para evitar redes maliciosas e perigosas.

Go-Trust®
Ative a autenticação multifatorial com sua impressão digital e seu telefone para desbloquear computadores e contas na nuvem*.

*não pré-carregado

Fonte:
[2] https://www.mishcon.com/news/firm_news/89_of_breache s_had_a_financial_or_espionage_motive_04_2016

Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

Download de aplicativos/ software de fontes não autorizadas

80% dos profissionais de segurança de TI dizem que suas maiores ameaças são de funcionários desonestos, exploits de malware ou software não autorizado.[3]

Estima-se que 57% dos funcionários instalam software não autorizado nos computadores da empresa, e mais de dois terços desse software traz consigo vírus e outro malware.[4]

Por isso, é importante que os dispositivos tenham:

Recursos de segurança integrados
Software que permite que os computadores reconheçam aplicativos inseguros.

Visibilidade e controle de TI
Melhore a segurança, permitindo que as equipes de TI tenham visibilidade dos computadores e rede.

Gerenciamento de dispositivos móveis
Certifique-se sobre a segurança dos dados, estejam eles armazenados em um dispositivo ou na nuvem.

Lenovo Vantage
Permita que a TI detecte ameaças que circundam o notebook e tome as medidas necessárias.

Intel® Active Management Technology (Intel® AMT)
Acesse remotamente um dispositivo para descobrir, ativar, monitorar, proteger e gerenciar, mesmo que esteja desligado.

Fonte:
[3] https://www.avecto.com/news-and-events/news/80-of-it-security-professionals-say-their-greatest-threats-are-from-rogue-employees-malware-exploits-or-unauthorized-software

[4] https://blog.samanage.com/it-asset-management/alert-unauthorized-software-on-network/

Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

Danos acidentais

A perda de dados não ocorre apenas por causa do roubo ou Wi-Fi desprotegido. Computadores e líquidos não foram feitos para ficarem juntos. Algo tão trivial quanto derrubar café pode arruinar o seu equipamento e, portanto, os dados contidos nele. Por isso é importante que as empresas façam tudo o que estiver ao seu alcance para garantir a segurança das máquinas.

A segurança completa dos equipamentos pode ser garantida com:

Dispositivos duráveis e confiáveis
Que sejam resistentes e que superem seja lá o que vier.

Backup automático
Para manter dados seguros instantaneamente e sem paralisações.

Serviços para danos imprevistos
Um serviço de garantia que cobre danos não intencionais.

Testes com especificações militares
Os ThinkPads são avaliados em 12 testes militares e passam por mais de 200 comprovações de durabilidade.

OLDB

Backup de Dados Online (Online Data Backup, OLDB)
Com essa solução você garante o backup e recuperação automática dos seus dados.

Proteção contra danos acidentais (Accidental Damage Protection, ADP)
Proteção para o equipamento em caso de picos e energia não intencionais, derramamentos de líquidos ou impactos, além de danos ao LCD.

Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

Roubo/perda de dispositivos

CPUs modernas são relativamente menores; uma vantagem para os usuários, mas para os ladrões também. Não apenas notebooks, mas desktops e discos rígidos também estão sujeitos a roubo. Outro desafio para as organizações é a perda de equipamentos, o que, na maioria dos casos, ocorre com notebooks e tablets. Nessa situação, não é apenas o computador que fica comprometido, mas os dados da sua empresa na nuvem também correm risco se o computador não estiver seguro o suficiente.

De acordo com uma nova pesquisa da NetEnrich, 42% dos profissionais de TI disseram que suas organizações sofreram perdas de dados importantes de dispositivos móveis.[5]

Assim, as organizações devem impedir a violação de dados por meio de:

Criptografia de dados
Tecnologia para criptografar dados, de modo a impedir o ataque de hackers e roubos.

Proteção contra roubo físico de dados
Inovações que impedem o roubo do disco rígido.

Limpeza remota de dados
Tecnologia que permite à TI controlar os equipamentos e apagar dados remotamente.

ThinkCentre M910 SFF

Discrete Trusted Platform Module (dTPM)
Criptografe seus dados, senhas e muito mais, para melhorar a segurança.

Disco rígido removível
Remova fisicamente seu disco rígido para maior segurança.

Intel® Active Management Technology (Intel® AMT)
Apague remotamente os dados de um dispositivo comprometido para evitar que ataques de malware se espalhem.

Windows 10 Pro

Fonte:
[5]: https://blogs.absolute.com/the-impact-of-corporate-data-lo ss-from-mobile-devices/

Clique aqui para conhecer as soluções de segurança da Lenovo

CONCLUSÃO

A estratégia certa pode beneficiar sua empresa em vários estágios:

- Garantir que os dispositivos não sejam o elo vulnerável da infraestrutura de TI da sua organização.
- Garantir que os dispositivos não sejam o elo vulnerável em sua infraestrutura de TI
- A força de trabalho moderna espera contar com tecnologia e equipamentos que complementem seu estilo de trabalho e que não estejam ultrapassados.

De acordo com uma pesquisa da Microsoft, 93% dos colaboradores disseram que a tecnologia os ajuda a prosperar no trabalho e que ter uma tecnologia moderna e atualizada no escritório é importante.[6]

Então, escolha com cuidado.

Fonte:
[6]: https://toggl.com/employee-retention-strategies-millennials

Windows 10 Pro

Clique aqui para conhecer as soluções de segurança da Lenovo

Lenovo

5 motivos
pelos quais a Lenovo faz a diferença

Reconhecida
ao redor do mundo

Expertise
em diversas
categorias

Confiança em
nossos produtos

Tecnologias
impulsionadoras
de negócios

Rede de
suporte flexível

Windows 10 Pro

www.lenovo.com