4 Maneiras Práticas de

Simplificar

Seus Processos de Segurança

Índice

Introdução

As ameaças cibernéticas estão cada vez mais sofisticadas e complexas. Por isso, é natural que as empresas busquem defesas mais poderosas e estruturadas para esse problema. O problema em ampliar a segurança por meio de maior complexidade é que os seus recursos, em especial o tempo e a equipe, não crescem automaticamente na mesma proporção.

Uma caixa de ferramentas completa não tem valor sem alguém que saiba como usar um martelo. Da mesma forma, mesmo a infraestrutura de segurança mais robusta não pode se autogerenciar. O número reduzido de funcionários no departamento de TI é um desafio para toda a indústria e não mostra sinais de mudança: **53% dos profissionais de TI em todo o mundo lutam contra a deficiência de habilidades em segurança cibernética nas empresas onde trabalham**[1]**.** Os funcionários do departamento de TI atuam em diversas áreas da empresa, divididos entre as tarefas diárias e os constantes alertas e tíquetes de suporte.

Se tudo isso soa familiar, e a segurança simplificada parece fora do alcance da sua organização, leia a seguir as quatro maneiras práticas de simplificar seus processos de segurança cibernética.

Complicado

Gerenciamento de diversas soluções pontuais

Em uma manhã de segunda-feira, você recebe um tíquete de suporte do departamento de marketing: "Não consigo acessar documentos importantes da empresa no site de hospedagem de arquivos. POR FAVOR, RESOLVA ISSO O QUANTO ANTES." Você suspira, toma vários goles de café e se prepara para passar a próxima meia hora navegando por configurações e lidando com cinco telas diferentes para resolver uma simples exceção de URL. Com um número cada vez maior de configurações, comandos e ferramentas sem sentido para gerenciar, esse é um cenário frequente para muitos administradores de rede, o que consome um tempo precioso.

Pense assim: se você tem três ou mais contas de e-mail (uma para o trabalho, outra pessoal e talvez uma dedicada a spams), provavelmente é fácil separar mensagens importantes, como "Aniversário de 80 anos da vovó!" ou a mensagem do CEO, dos spams nas suas caixas de entrada. Agora, imagine que você tem 100 contas para monitorar e em todas elas você pode receber comunicações importantes a qualquer momento. Assim fica bem mais difícil.

Simples

Gerenciamento Centralizado:

invista em produtos fáceis de configurar, implantar e gerenciar

A solução: Você já tem trabalho suficiente sem incluir alertas constantes para gerenciar e diversas telas para monitorar. Procure produtos de segurança de rede que permitam o gerenciamento contínuo usando uma única IU ou deixe todo o gerenciamento nas mãos de um provedor de soluções de TI. Caso o gerenciamento interno seja de fato a melhor opção para você, temos appliances de firewall que, além de serem fáceis de implementar e configurar, são projetados com foco no gerenciamento centralizado a partir de um único console. Isso torna o processo de gerenciamento de rede e políticas simples e direto.

Fácil de configurar: Faça atualizações de configuração ou firmware com apenas um toque para todos os appliances de firewall. Assim, você poupa tempo e garante que as políticas sejam sincronizadas em toda a organização. Crie templates de políticas em qualquer lugar e os envie rapidamente para vários appliances usando tenants com base em função.

Fácil de implementar: Oferecemos uma solução de implementação zero-touch, uma ferramenta avançada de configuração e implementação com base em nuvem que é incluída por padrão nos appliances de firewall. Basta ligar o appliance e conectá-lo à Internet. O resto pode ser configurado remotamente, onde quer que você esteja.

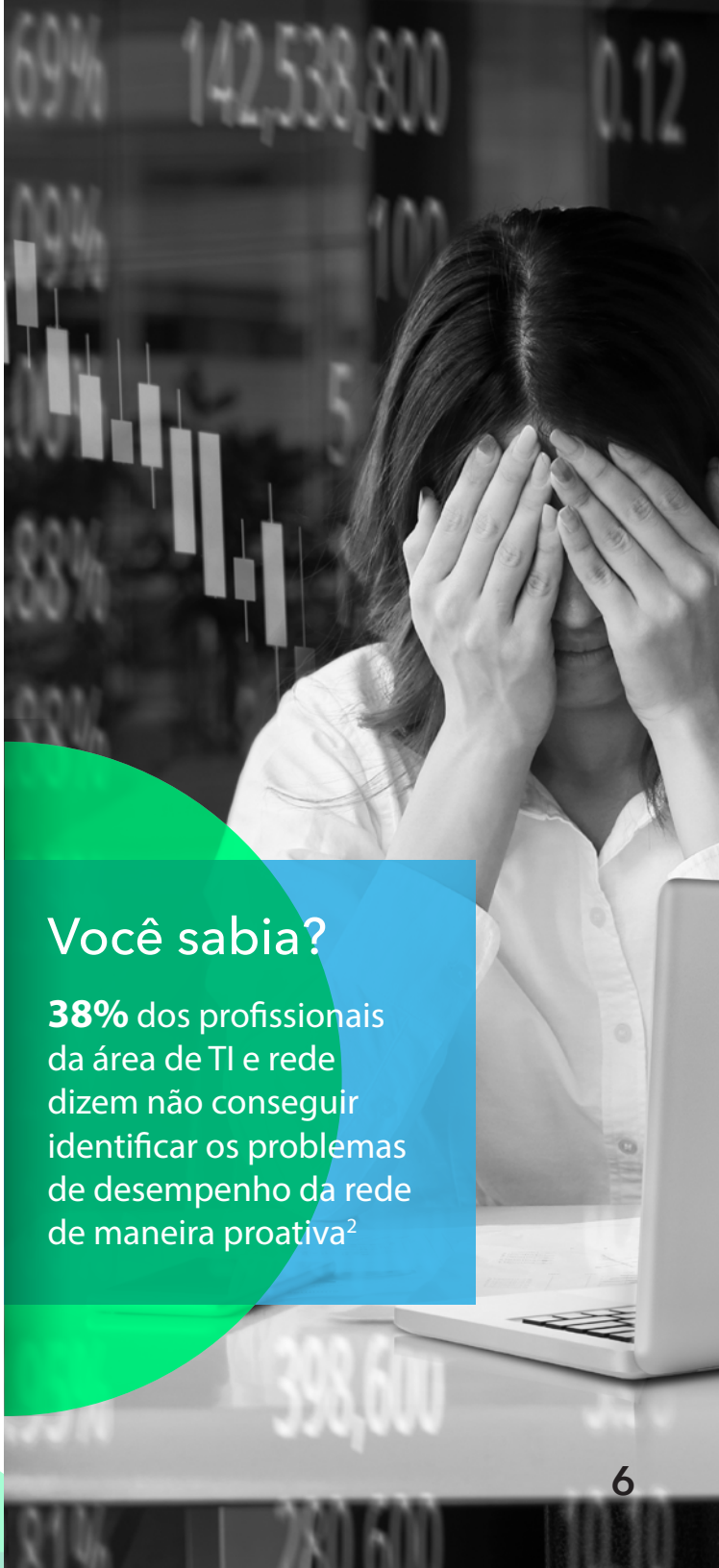
Fácil de gerenciar: Gerencie centenas de appliances de firewall a partir de um único console fácil de usar para maximizar a eficiência e simplificar a administração da rede. Com interface visual clara e linguagem simples nas mensagens de registro, você não precisa mais ficar adivinhando na hora de criar e manter uma postura forte de segurança e conformidade.

Complicado

Análise de volumes gigantescos de dados manualmente

A visibilidade detalhada da atividade em toda a rede é essencial com o crescimento do tamanho e da complexidade das nossas infraestruturas de TI. Isso permite que as equipes de TI reconheçam padrões, ameaças e falhas de segurança e possam responder antes que ocorram danos. Esses dados têm um valor inestimável, mas não serão aproveitados se os principais insights não forem acionáveis e estiverem indisponíveis para sua equipe de segurança.

Hoje, muitas soluções de visibilidade de rede no mercado oferecem grandes volumes de dados, mas há pouca preocupação com a classificação de prioridades. Essa abordagem sobrecarrega a maioria das equipes de segurança com quantidades aparentemente infinitas de alertas de segurança, que não podem ser pesquisados nem priorizados. Um produto de visibilidade realmente eficaz reconhecerá as limitações de largura de banda inerentes a muitas equipes de TI e destacará com eficácia os eventos mais importantes para manter a integridade da rede.



Você sabia?

38% dos profissionais da área de TI e rede dizem não conseguir identificar os problemas de desempenho da rede de maneira proativa[2]

Simples

Dados Acionáveis:

use soluções automatizadas de visibilidade e geração de relatórios

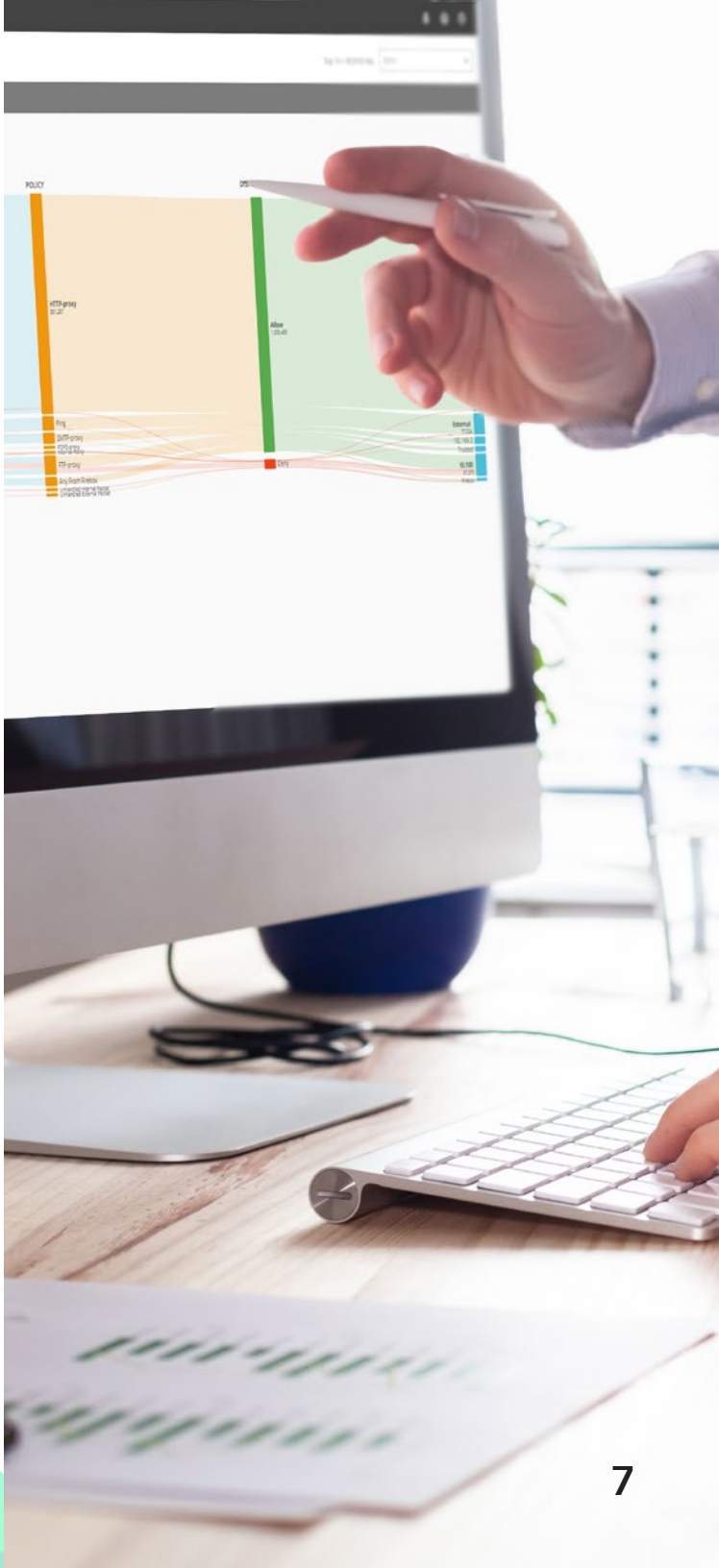
Qual é a solução? Geralmente, os clientes optam pela compra de segurança no formato de um serviço, e nosso conjunto de tecnologia inclui ferramentas de visibilidade para que possamos gerenciar sua segurança de forma eficaz e oferecer relatórios valiosos. Como opção, nossa solução de visibilidade baseada em nuvem permite que sua equipe interna faça o gerenciamento, além de oferecer insights rápidos, confiáveis e acionáveis para que você possa identificar padrões de forma ágil e tomar decisões mais bem-informadas. Com painéis incorporados e recursos de geração de relatórios, você pode reunir informações sobre eventos de segurança, auditorias de conformidade e padrões na rede rapidamente. Na plataforma do Cloud, é possível monitorar e acessar insights importantes sobre a segurança da sua rede em tempo real e onde quer que você esteja. Sabe o que é ainda melhor? Você não precisa de infraestrutura de hardware.

Acesse informações de nível executivo na sua rede, como:

- Principais usuários
- Principais destinos
- Principais aplicativos
- Principais domínios

Veja as informações mais recentes sobre segurança de seu firewall, como:

- Principais sites de botnet bloqueados
- Principais clientes e destinos bloqueados
- Principais ataques de malware avançados bloqueados
- Prevenções contra intrusões



Complicado

Wi-Fi desprotegido e de baixo desempenho

Mesmo com todas as facilidades que o acesso Wi-Fi oferece às empresas modernas, desde programas BYOD (Traga seu próprio dispositivo) a forças de trabalho móveis, ele também gera importantes preocupações de segurança na sua rede corporativa. Agora, a web oferece diversos recursos virtuais para a invasão de Wi-Fi. Isso inclui vídeos com instruções no YouTube, que instruem até criminosos cibernéticos principiantes e ajudam a propagar as seis categorias conhecidas de ameaças de Wi-Fi.

Access point Evil Twin | **Rogue Client** | **Access point mal configurado** | **Access point vizinho** | **Access point clandestino** | **Rede Ad-Hoc**

Com muitas equipes de TI já dedicando recursos consideráveis a problemas relacionados a redes Wi-Fi (senhas esquecidas em aplicativos móveis, sincronização de e-mail e dificuldades de acesso a redes sem fio, por exemplo) a maioria não possui largura de banda para implantar diversas soluções para se proteger contra cada uma dessas seis categorias de ameaças de Wi-Fi, muito menos administra-las. Você precisa de uma solução única, fácil de implantar e gerenciar, que seja compatível com os requisitos de desempenho do seu ambiente específico e também o proteja contra as categorias de ameaça de Wi-Fi.

Você sabia?

O usuário global de BYOD (Traga seu próprio dispositivo) poupa 37 minutos de horas de trabalho por semana ao usar seu dispositivo móvel.[3]

Simples

Rede Wi-Fi mais Segura e Protegida:
ofereça um Ambiente Sem Fio Confiável

A solução: Ter uma conexão Wi-Fi eficiente e segura não precisa ser difícil. Nossos serviços de Wi-Fi em nuvem oferecem uma estrutura verificada pela Miercom para a criação de uma rede Wi-Fi completa, de alto desempenho, simples de gerenciar e protegida das seis categorias de ameaças conhecidas. Além disso, os ambientes gerenciados por Wi-Fi em nuvem vêm com as vantagens do Discover, um aplicativo dentro do Wi-Fi Cloud que oferece informações valiosas sobre desempenho e integridade da rede. No Discover, você encontra um conjunto completo de recursos de integridade de rede, solução de problemas e visibilidade acionável, como:

Jornada do cliente: Um snapshot em tempo real de todos os seus locais para identificar rapidamente clientes que estejam enfrentando problemas, que mesmo não relacionados ao Wi-Fi, impactam sua experiência, como falhas na associação, autenticação ou na própria rede.

Rede de referência: Cada cliente e AP dentro do alcance das suas redes é rastreado em busca de desempenho, conectividade e experiência em aplicativos para definir o que é ou não normal. Quando uma anomalia é detectada, o Discover fornece visibilidade total para identificar a causa raiz, gerando recomendações para resolver problemas de rede, mesmo quando eles não são relacionados ao Wi-Fi.

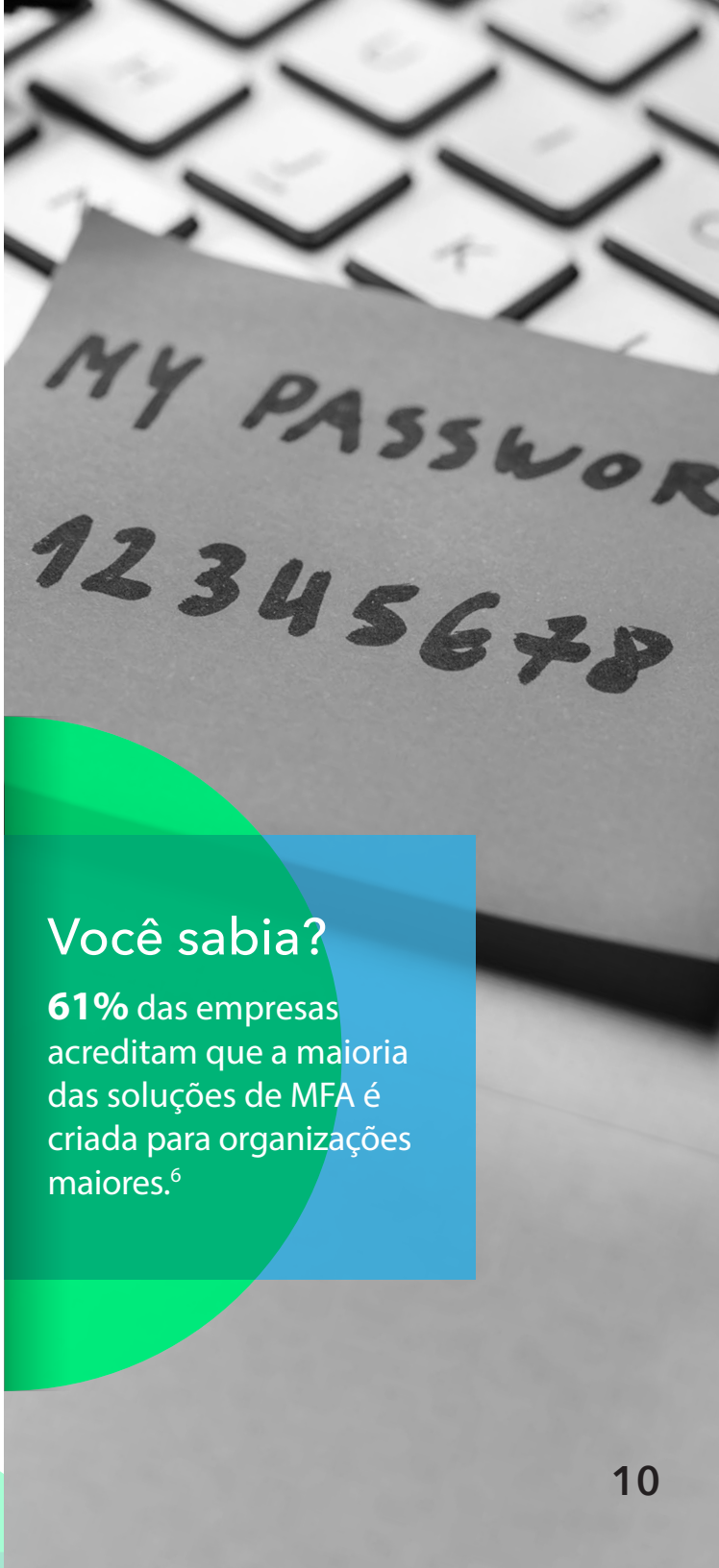
Alertas: Com o recurso de alertas do Discover, a manutenção dos acordos de nível de serviço (SLAs) ficou muito fácil. Mantenha seus recursos de rede Wi-Fi, com fio e de aplicativos funcionando sem problemas.

Complicado

Lançamentos de MFA com uso intensivo de recursos

Atualmente, a segurança por senha é um dos maiores desafios enfrentados pelas organizações, com **81% das violações de dados sendo causada pelo uso de senhas fracas ou roubadas**[4]. Por isso, as empresas estão avaliando o uso de produtos de autenticação multifator (MFA) para adicionar camadas de segurança no acesso a recursos corporativos.

Gerenciar o uso de muitos produtos de MFA tem sido um desafio para as equipes de TI. Os lançamentos tradicionais de MFA baseados em hardware consomem tempo e recursos, dificultando o equilíbrio entre a implementação e as prioridades existentes, sem falar no envio constante de tíquetes de serviço. Além disso, muitos lançamentos de MFA exigem compromissos significativos com treinamento por parte da equipe de TI, sendo que uma das reclamações mais comuns em relação a soluções tradicionais é a usabilidade (ou a falta dela). **Na verdade, 24% das empresas que não usam uma solução de MFA listam a dificuldade em implementar, manter e sustentá-la, como fatores-chave para a adoção**[5].



Você sabia?

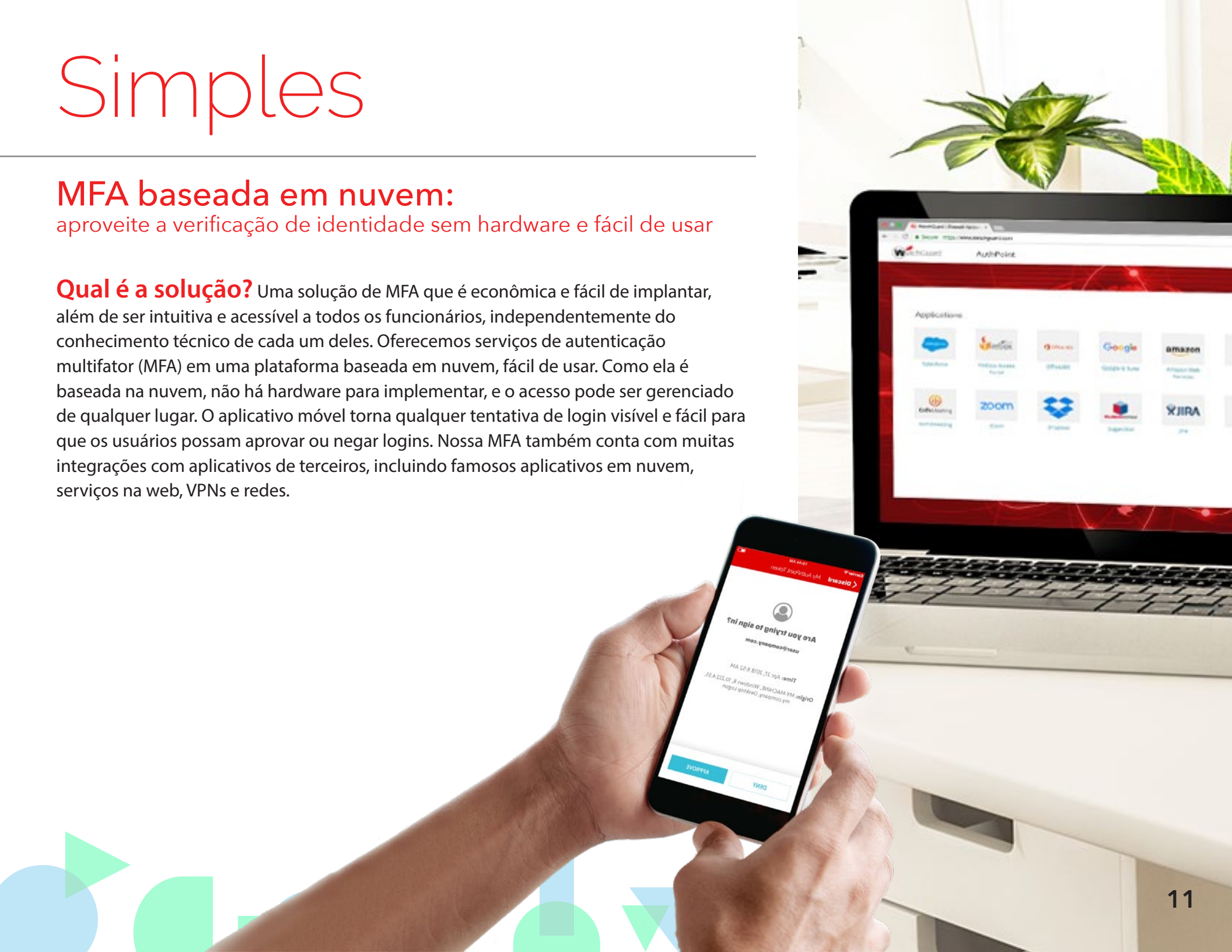
61% das empresas acreditam que a maioria das soluções de MFA é criada para organizações maiores.[6]

Simples

MFA baseada em nuvem:

aproveite a verificação de identidade sem hardware e fácil de usar

Qual é a solução? Uma solução de MFA que é econômica e fácil de implantar, além de ser intuitiva e acessível a todos os funcionários, independentemente do conhecimento técnico de cada um deles. Oferecemos serviços de autenticação multifator (MFA) em uma plataforma baseada em nuvem, fácil de usar. Como ela é baseada na nuvem, não há hardware para implementar, e o acesso pode ser gerenciado de qualquer lugar. O aplicativo móvel torna qualquer tentativa de login visível e fácil para que os usuários possam aprovar ou negar logins. Nossa MFA também conta com muitas integrações com aplicativos de terceiros, incluindo famosos aplicativos em nuvem, serviços na web, VPNs e redes.



Conclusão

Ter tempo e recursos limitados pode dificultar o gerenciamento da segurança de TI da sua organização. Por isso, nossas soluções são projetadas com foco em processos simplificados de configuração, implementação e gerenciamento contínuo. Sua rede já é bastante complexa. Mantê-la segura, não precisar ser.

[1] StationX, "Previsões para 2019: a escassez de habilidades de segurança cibernética está aumentado", janeiro de 2019
[2] APM Digest, "Veja por que as equipes de TI perdem muito tempo com a solução de problemas de rede", março de 2019
[3] Information Age, "A relação entre a cultura Wi-Fi e BYOD", abril de 2017
[4] CSO, "Senhas invadidas causam 81% das violações de dados", maio de 2017
[5] WatchGuard, "Já que as senhas são falhas, qual a solução?", maio de 2018
[6] WatchGuard, "Já que as senhas são falhas, qual a solução?", maio de 2018

lb informática

geral@lbinformatica.pt

+351 253 433 386 / 936 100 030

www.lbinformatica.pt