Dez etapas simples para proteger a sua rede de varejo

Soluções de TI simples passo a passo para que pequenas empresas no varejo utilizem a tecnologia de proteção avançada de maneira acessível, fácil e rápida

SONICWALL®

Introdução

A cada ano, ataques a redes se tornam mais comuns, mais inteligentes e mais difíceis de serem detectados. Devido à natureza pública dos lojistas, os pontos de entrada para a rede vão além dos notebooks, desktops e smartphones de funcionários, e incluem o Wi-Fi público e servidores de eCommerce voltados para o público.

Dessa forma, as redes de varejo têm dois principais desafios. O primeiro é lidar com a complexidade de gerenciar vários locais remotos. O segundo é poder fornecer proteção de segurança que espelhe as mesmas ameaças daquelas enfrentadas pelas redes de grandes empresas.

Em pequenos negócios de varejo, a função de administrar a segurança de rede é sempre colocada nas mãos do proprietário do negócio ou do técnico interno padrão. Geralmente, nenhuma dessas pessoas tem o tempo, os recursos ou a experiência para trabalhar nas implantações e na administração da proteção de segurança de uma rede complexa. Em um ambiente de varejo distribuído, o departamento de TI e o departamento de segurança têm desafios específicos. Para a TI, é o gerenciamento de uma rede distribuída e complexa (que inclui o gerenciamento de switches e wireless). Para a segurança, é a implantação de políticas consistentes na organização.

É possível criar uma rede de varejo segura ao aproveitar as tecnologias modernas de segurança. Este eBook avalia os dez principais desafios de segurança para sua rede de varejo e oferece dez soluções comprovadas.

ETAPA 1

Divida a sua segurança em camadas

Seu desafio: reforçar a defesa contra novas ameaças em todas as camadas

Muitos dos ataques de hoje são combinados por meio de múltiplas tecnologias em diferentes camadas para tentar invadir a sua rede. Esses ataques podem ignorar os firewalls desatualizados que não possuem o poder de inspecionar todo o tráfego, inclusive grandes arquivos e o tráfego criptografado de HTTPS.

Sua solução: implantar um firewall de Gerenciamento unificado de ameaças

A melhor abordagem para a proteção de segurança de rede de varejo hoje em dia é o Gerenciamento Unificado de Ameaças (UTM). Em termos práticos, os firewalls UTM combinam a eficácia de vários pontos de defesa para proporcionar maior proteção em todas as camadas de funcionamento em rede. Para um lojista, o valor do UTM vem da combinação de suas tarefas complexas em um único dispositivo com um console de gerenciamento. Essa abordagem fornece uma defesa eficiente contra uma grande variedade de ameaças de segurança. Isso torna a proteção de rede mais completa, acessível e fácil de gerenciar.

Implante um firewall de Gerenciamento unificado de ameaças

SONICWALL®

ETAPA 2

Proteja seu gateway

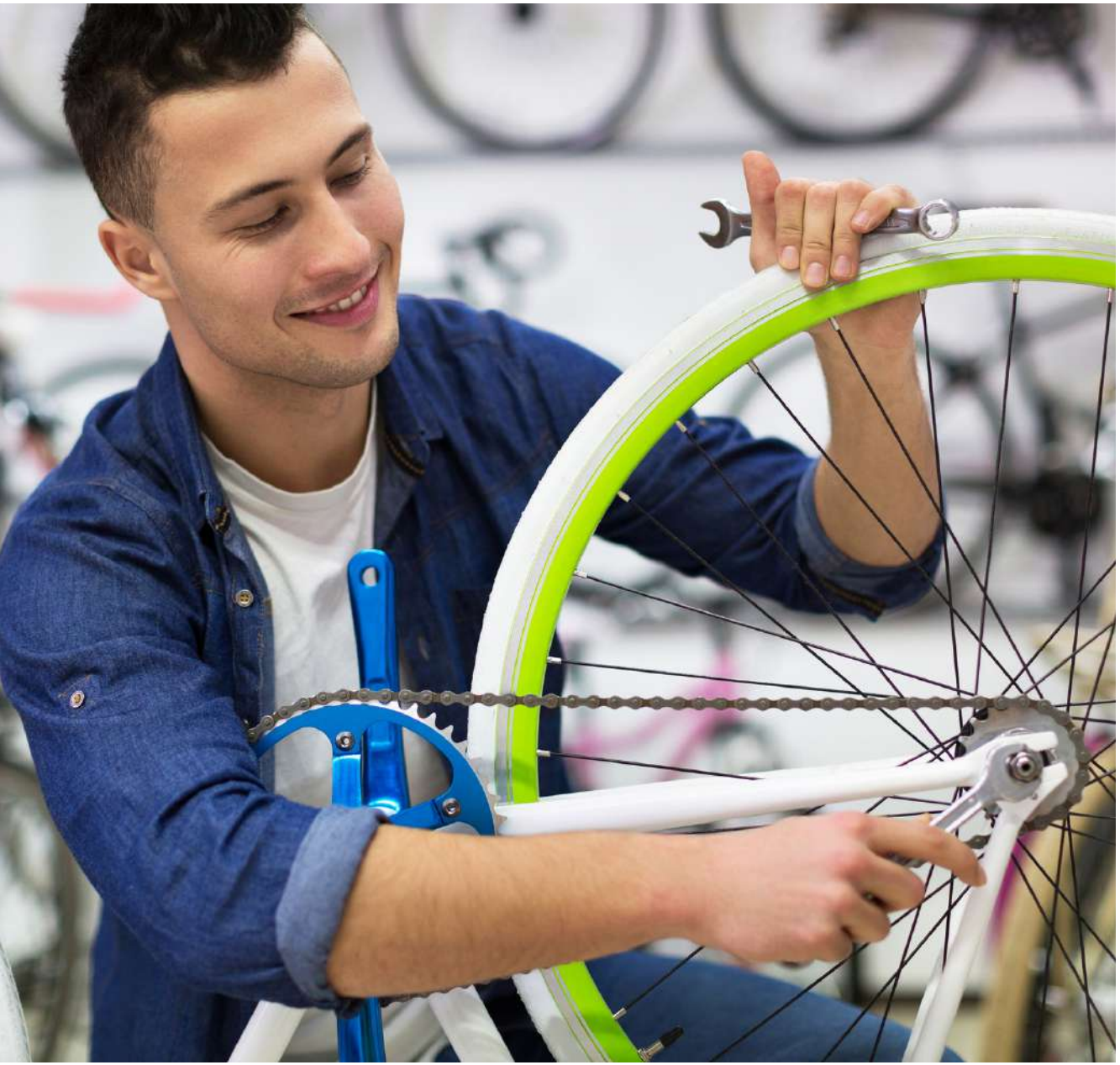
Seu desafio: bloquear as ameaças antes que elas invadam a sua rede

O eCommerce e o Wi-Fi aumentam a capacidade de alcançar um maior número de clientes em potencial ao expandir o perímetro de sua rede. No entanto, um perímetro expandido apresenta mais abordagens para ataques adicionais.

Sua solução: inspecionar todo o arquivo

A tecnologia de Inspeção detalhada de pacotes, quando implantada adequadamente no gateway, pode verificar completamente os pacotes de dados que tocam no perímetro de sua rede. Além disso, seu firewall UTM também precisa inspecionar a comunicação criptografada que vem do tráfego de HTTPS para encontrar ameaças que estão isoladas dentro de arquivos, aplicativos e anexos.

Sem limites de tamanho ou tipo de arquivo



ETAPA 3

Simplifique

Seu desafio: diminuir a complexidade

A simplicidade afeta os resultados finais. O custo total pago pela segurança não é o único medido na lista de preços de aquisição. Ele também está embutido nos custos de instalação, utilização, gerenciamento e manutenção das suas soluções.

Sua solução: simplificar a sua tecnologia

A segurança de alto desempenho não precisa ser complexa. Appliances modernos de segurança podem facilitar a configuração e o gerenciamento ao usar recursos como interfaces intuitivas baseadas na Web e assistentes de configuração fáceis de usar. Para múltiplos locais, o gerenciamento centralizado ou hospedado pode facilitar a administração e diminuir o custo de propriedade existente.

Simplifique a sua tecnologia

ETAPA 4

Mantenha um preço acessível

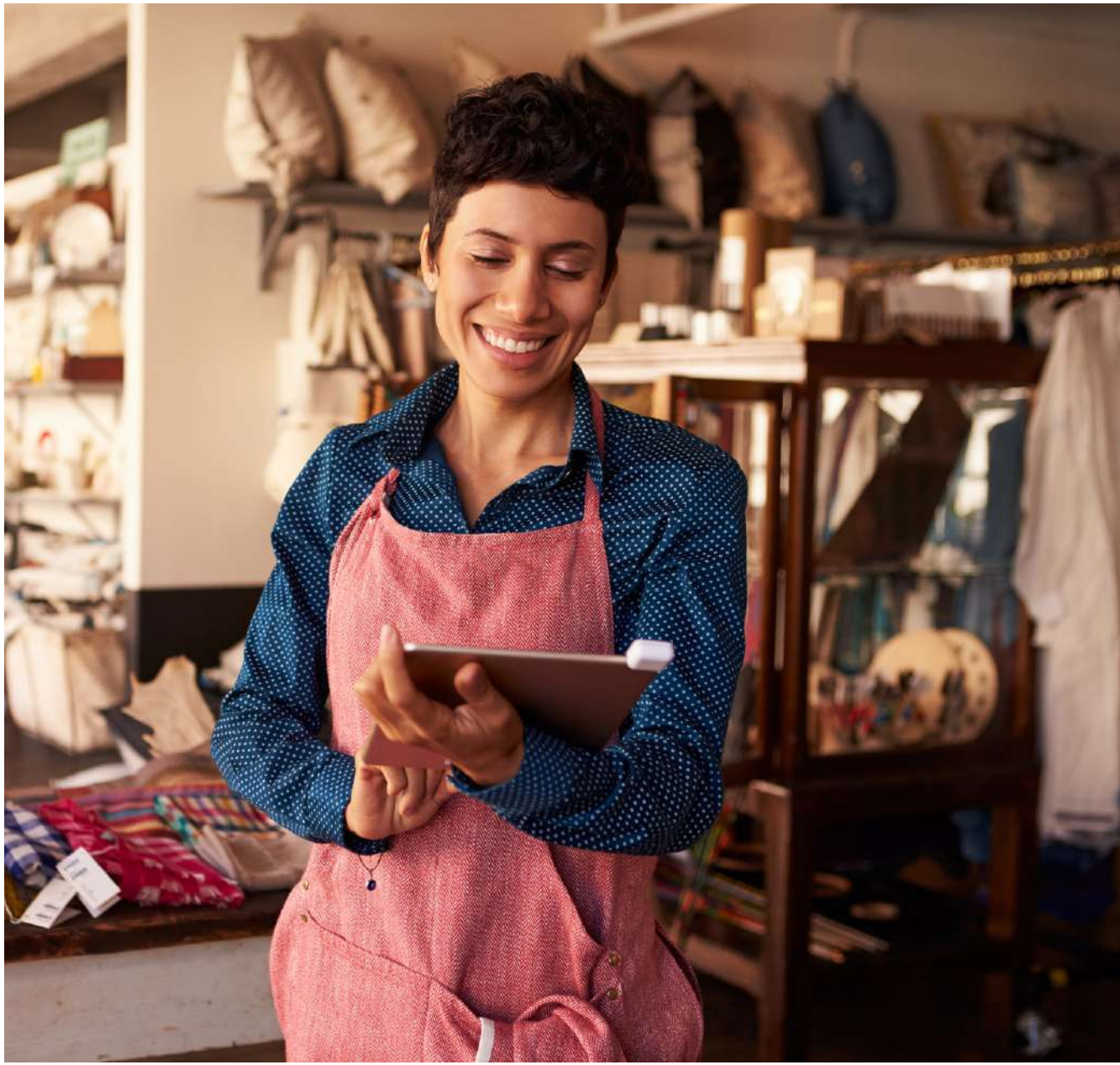
Seu desafio: garantir uma proteção abrangente com um pequeno orçamento

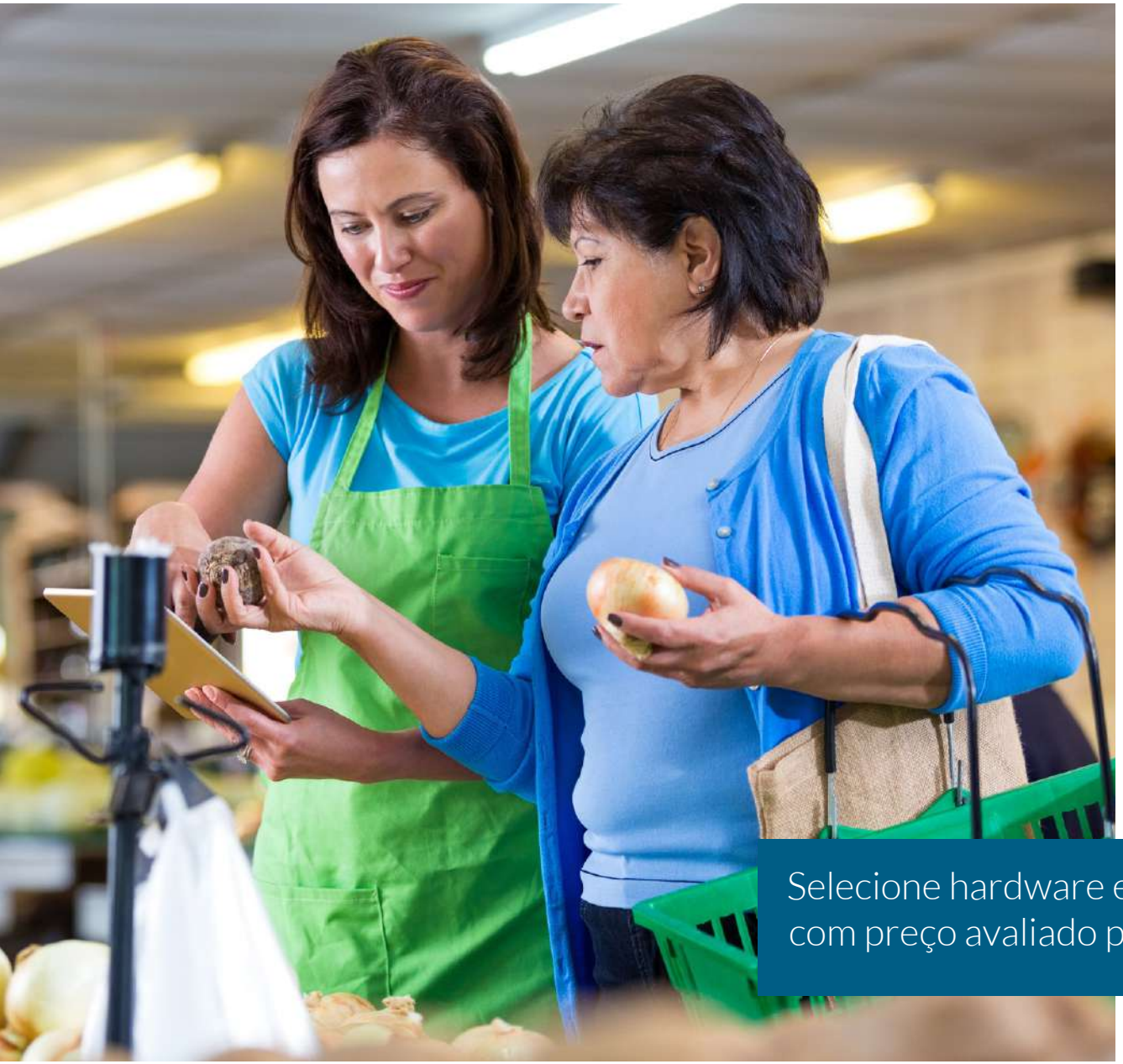
Todas as organizações, não importa o tamanho, precisam da mesma proteção usada pelos maiores bancos, hospitais, universidades e governos. Muitas vezes, obter a melhor proteção significa gastar além do orçamento.

Sua solução: consolidar a sua segurança

Reduza os custos de hardware, instalação, operações e sobrecarga administrativa por meio da consolidação de múltiplas ferramentas de segurança em apenas um appliance acessível e fácil de gerenciar. De maneira otimizada, esse appliance deve incluir filtragem de conteúdo, prevenção contra intrusões, antispyware, antimalware e aplicativos nativos para acesso remoto de qualquer dispositivo. Para interromper as ameaças atuais, a segurança consolidada também deve incluir a capacidade de inspecionar arquivos criptografados sem limitações de tamanho de arquivo.

Consolide sua segurança





ETAPA 5

Livre-se dos gargalos

Seu desafio: manter o seu firewall atualizado com sua compilação de rede

Mesmo se o seu firewall tiver apenas dois anos, ele pode comprometer a segurança e a eficácia de sua rede. Você não deveria precisar recorrer ao desligamento dos recursos de segurança para manter o desempenho. Análises programadas das melhorias de rede devem considerar o firewall como um componente principal.

Sua solução: selecionar hardware e software de alto desempenho com preço avaliado para pequenas empresas.

Para um melhor desempenho, sua solução deve fornecer uma taxa de transferência que não cause impacto sobre ele, ao mesmo tempo que mantém a máxima segurança. A tecnologia de microprocessadores de múltiplos núcleos permite que os appliances UTM projetados para pequenas empresas alcancem uma eficiência significativa de rede.

Selecione hardware e software de alto desempenho com preço avaliado para pequenas empresas

ETAPA 6

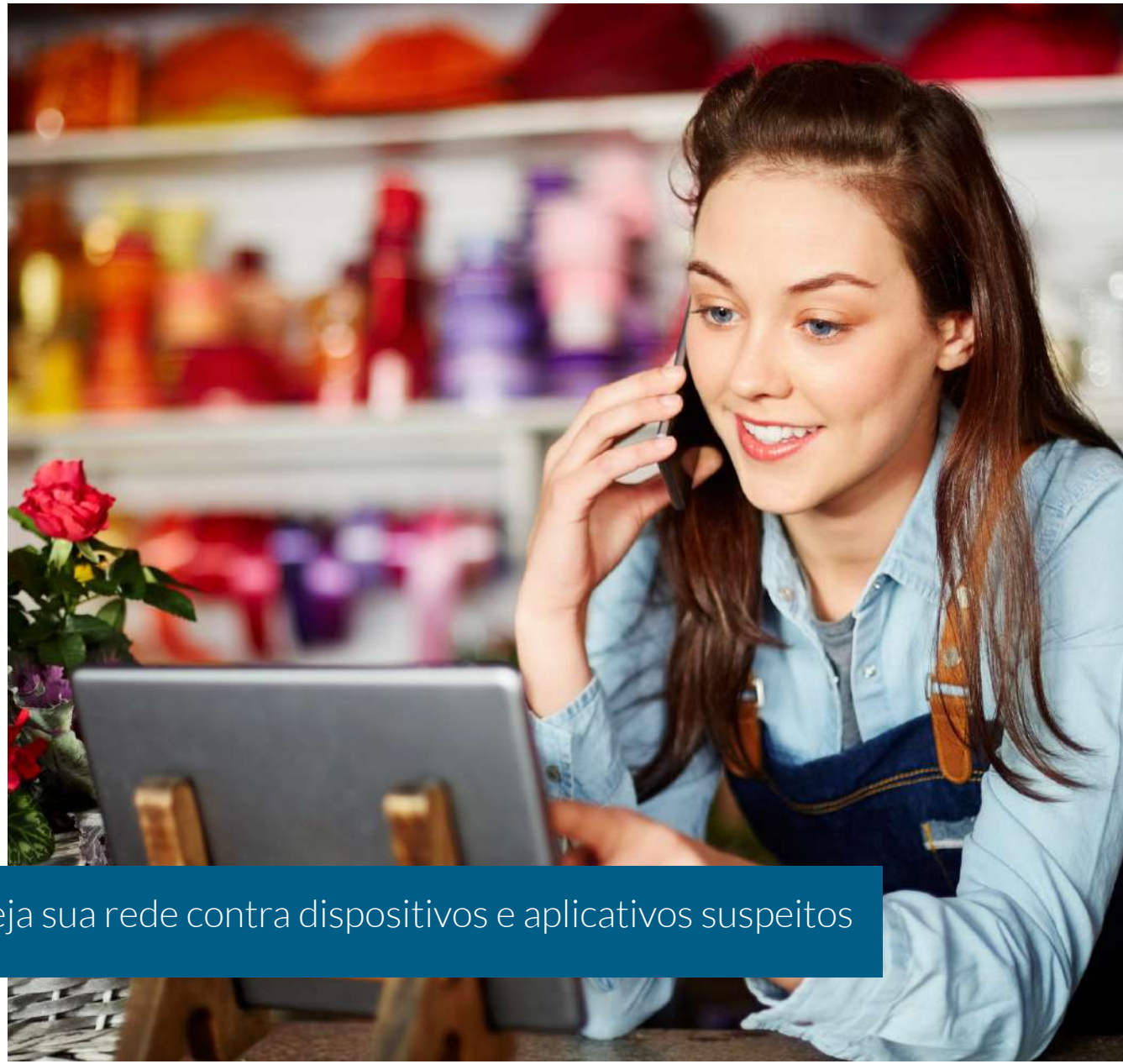
Mantenha os sistemas atualizados

Seu desafio: monitorar o que usa a sua rede

As pessoas utilizam uma combinação de dispositivos e software para realizar seus trabalhos. Diversos dispositivos e aplicativos podem abrir as portas para criminosos cibernéticos. Controlar o que tem acesso à rede e os dispositivos de segurança pode congestionar os sistemas de segurança do lojista.

Sua solução: proteger sua rede de dispositivos e aplicativos suspeitos

No mais alto nível, um firewall deve poder colocar em quarentena os dispositivos de funcionários e convidados que não possuem a proteção antivírus atual. Para uma proteção ainda maior, saber quais dispositivos estão na rede e garantir que os convidados e funcionários tenham o software mais recente pode reduzir a exposição a vulnerabilidades.



Proteja sua rede contra dispositivos e aplicativos suspeitos

ETAPA 7

Mantenha sua rede produtiva

Seu desafio: eliminar o tráfego desnecessário

As redes de negócios atuais podem ser atingidas por spam, por atividade não autorizada da Web e pelo tráfego na rede social, o que não ajuda na manutenção da produtividade. Você pode até não conhecer a pessoa no final do corredor que faz download de vídeos e deixa sua rede lenta.

Sua solução: implementar o gerenciamento de conteúdo e aplicativos

Insista em um firewall que mostre a você todas as atividades da rede de todos os usuários em tempo real. Em um ambiente onde existem funcionários e convidados, pode ser interessante possuir políticas de uso distintas. Para os funcionários, elas devem permitir que você crie regras facilmente a fim de restringir o uso de aplicativos e subaplicativos desnecessários (por exemplo, o Facebook pode ser aceitável para propósitos de marketing, mas os jogos do Facebook não). Para os convidados, você pode considerar restringir as atividades, como proibir os usuários de acessar sites ofensivos ou inapropriados.

Implemente o gerenciamento de conteúdo e aplicativos

ETAPA 8

Mantenha a compatibilidade

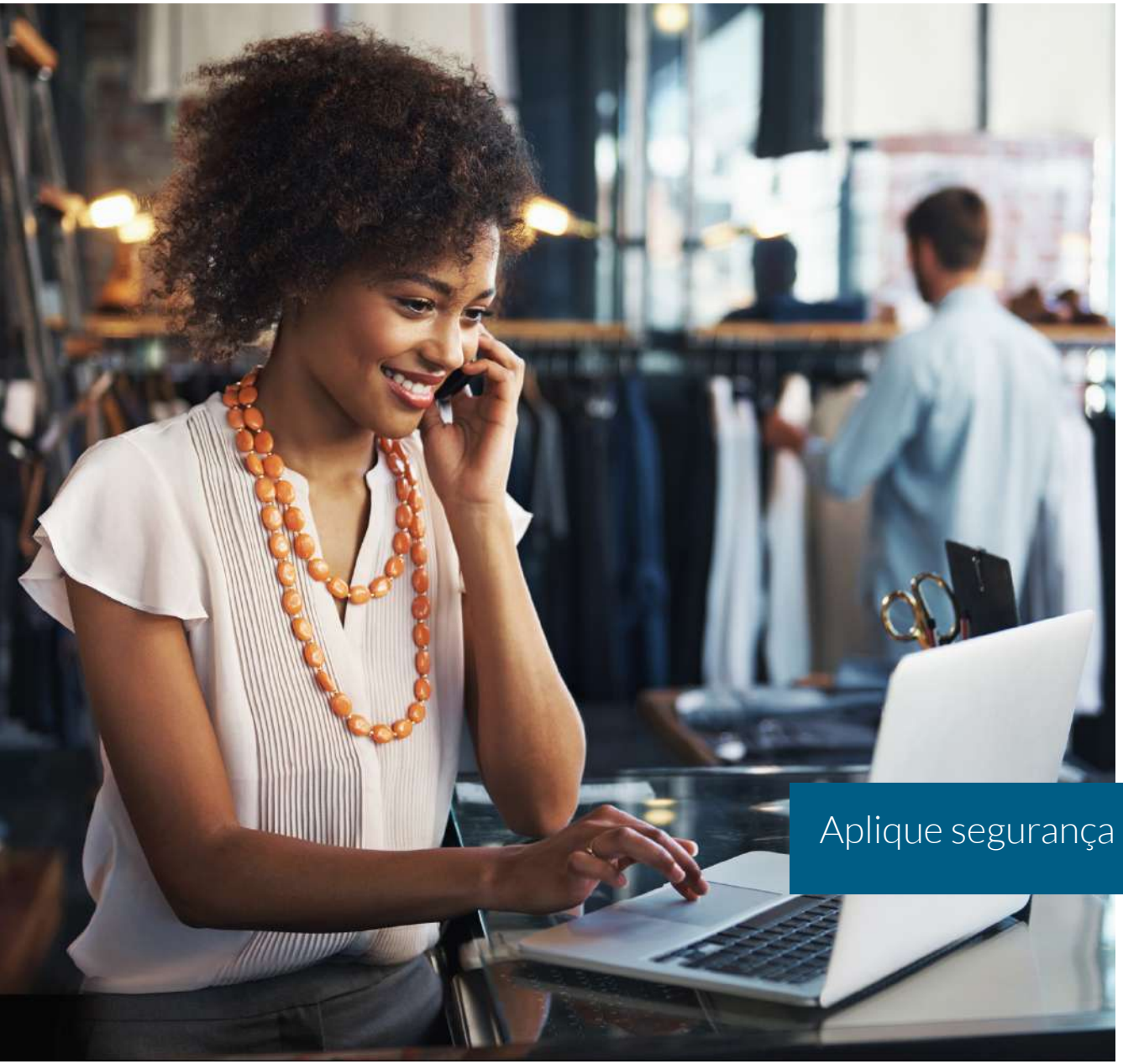
Seu desafio: seguir as normas e evitar as multas

Se o seu negócio aceitar pagamentos com cartão de crédito, é essencial manter a conformidade com os padrões do PCI. O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) possui seis metas de alto nível, inclusive a criação e manutenção de uma rede segura, o monitoramento e o teste frequente de redes e a implementação de medidas eficientes de controle de acesso. Essas metas levam a requisitos específicos que garantem que os dados do cartão de crédito, inclusive as informações pessoais dos titulares do cartão, estejam protegidos e em segurança. Manter a conformidade com o PCI pode ajudar seu negócio a evitar penalidades caras, mas isso não deve ser visto como uma solução de segurança de rede completa, e sim como um importante ponto de passagem ao longo da sua jornada para tornar sua rede o mais segura possível.

Sua solução: integrar o gerenciamento de conformidade

Procure por uma solução de rede fácil de ser implementada e que o coloque na direção certa. O primeiro requisito para conformidade com o PCI é alterar as senhas em todos os dispositivos de segurança de rede. Uma simples pesquisa na Internet pode descobrir esses padrões. Faça com que as senhas sejam difíceis de serem adivinhadas e as mantenha longe dos olhares curiosos. Os melhores firewalls integrarão vários recursos de segurança, inclusive detecção de malware, prevenção contra intrusões e bloqueio de inclusão de números de cartões de crédito não autorizados em e-mails de saída, tudo em um único dispositivo. Além disso, os firewalls de próxima geração fornecerão a aplicação de política de segurança de rede abrangente, junto com geração de relatórios e gerenciamento eficientes.

Integre o gerenciamento de conformidade



ETAPA 9

Proteja suas redes wireless

Seu desafio: evitar ataques baseados em wireless

A conectividade wireless aprimora a experiência de varejo. No entanto, também abre mais caminhos para o ataque. Além disso, uma solução de segurança wireless exige com frequência a adição de um controlador caro e de outro console de gerenciamento.

Sua solução: aplicar segurança de rede wireless

Uma abordagem simples seria trazer o wireless para o perímetro de segurança. Com isso, as políticas de segurança definidas por você também podem ser aplicadas aos usuários wireless. A segurança wireless também deve poder isolar os funcionários dos convidados para garantir privacidade e confidencialidade.

Aplique segurança de rede wireless

ETAPA 10

Prepare-se para o inesperado

Seu desafio: preparar-se para interrupções não planejadas

Mesmo a melhor rede de segurança UTM necessita de uma solução de recuperação de desastres. Desastres em grande escala mostraram o quão expostas a eventos inesperados as pequenas empresas podem estar. Mas os negócios não são interrompidos apenas por desastres naturais, pandemias, ataques terroristas ou coisas do tipo. Incêndios, falhas elétricas, falhas de equipamentos, roubo ou perda de notebooks podem ser desastrosos para negócios de varejo. Esses eventos podem interromper suas operações por tempo indeterminado, caso você não esteja devidamente preparado.

Sua solução: estabelecer um plano de backup

Ter a capacidade de restaurar um arquivo individual ou toda a rede estará ao alcance de praticamente todos os lojistas. O backup para um local de negócios secundário seguro ou de terceiros faz com que os sistemas de negócios possam ser restaurados e que operem mesmo se o local principal estiver comprometido. A tecnologia de recuperação sem sistema operacional (BMR) permite que sistemas operacionais inteiros, como bancos de dados ou servidores de arquivos, sejam recuperados para novas ou diferentes plataformas de hardware caso o dispositivo original não possa ser restaurado.

Estabeleça um plano de backup

Conclusão

A segurança de rede de varejo pode ser um problema complexo, mas, conforme apresentado neste eBook, não precisa ser. Há maneiras fáceis de começar a abordá-la com soluções de TI para pequenas empresas. Procure por um consultor confiável que possa ajudá-lo a traçar um roteiro para a segurança de rede de pequena empresa. Insista na segurança sem comprometimentos que combine desempenho e proteção e que se encaixe em seu orçamento.

Sobre nós

Em uma história de mais de 25 anos, a SonicWall tem sido a parceira de segurança confiável do setor. Desde a segurança de rede até a segurança de acesso e de e-mail, a SonicWall tem evoluído continuamente seu portfólio de produtos, o que permite que as organizações inovem, acelerem e cresçam. Com mais de um milhão de dispositivos de segurança em quase 200 países e territórios no mundo todo, a SonicWall permite que seus clientes digam sim com confiança para o futuro.

Se você tiver dúvidas sobre o possível uso deste material, entre em contato com:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Acesse o nosso site para obter mais informações.
www.sonicwall.com

Ebook-10Steps-SecureRetailNetwork-US-KJ-29255-D1

SONICWALL®