SAMSUNG | android

Tecnologia móvel: um novo **campo de batalha** para o cibercrime?

Para as empresas britânicas, trabalhar remotamente tornou os ataques cibernéticos mais comuns e mais dispendiosos. Veja por que uma estratégia de "confiança zero" é a mais segura para a tecnologia móvel.

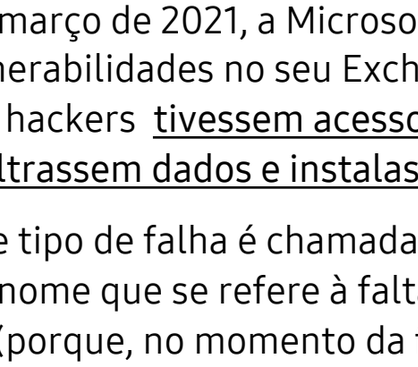
Em março de 2021, a Microsoft anunciou que várias vulnerabilidades no seu Exchange Server permitiram que hackers tivessem acesso livre a contas de e-mail, exfiltrassem dados e instalassem malware.

Esse tipo de falha é chamada de ataque de dia zero (ou dia 0), um nome que se refere à falta de tempo para se preparar para ele (porque, no momento da falha, as vulnerabilidades que os hackers exploram são desconhecidas para a equipe de segurança cibernética responsável).

Segundo os relatórios, pelo menos 7.000 empresas foram afetadas no Reino Unido. Mas este ataque de dia 0 também teve um impacto global. Algumas empresas, como a gigante de computadores Acer, foram especialmente atingidas. Seus dados foram mantidos em resgate por 50 milhões de dólares (38 milhões de libras).

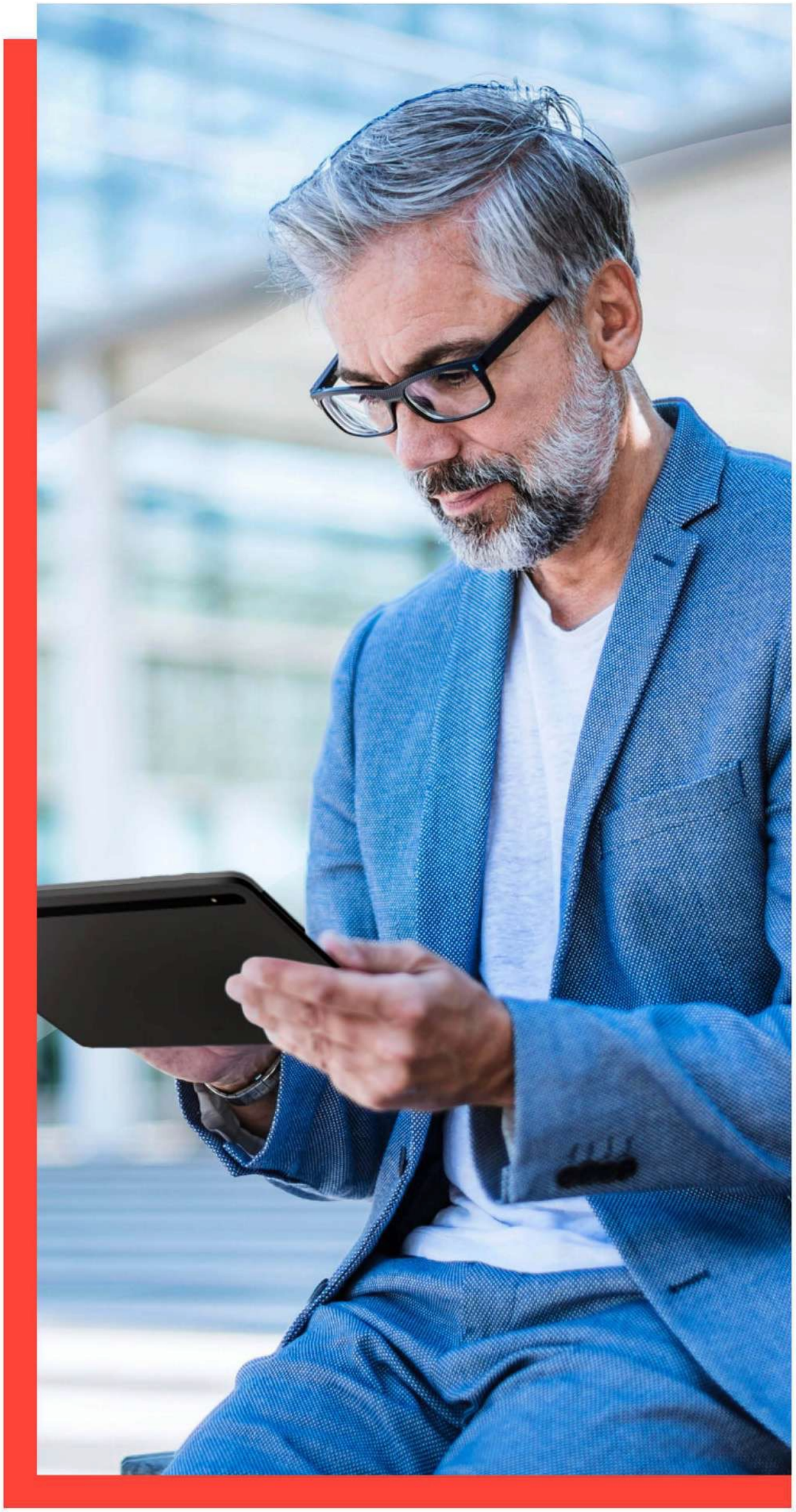
A conclusão aqui é que, na sequência da pandemia da COVID-19, os criminosos cibernéticos só se tornaram mais prolíficos. Parte da razão para o crescimento desta ameaça é o trabalho remoto. No Reino Unido, as vagas que permitiram o trabalho remoto triplicaram em 2020 e mais da metade dos londrinos agora trabalha em casa.

Para o melhor ou para o pior, trabalhar longe do escritório veio para ficar. Mas sua implementação foi apressada e não sem consequências.



das empresas têm visto um aumento nos ataques cibernéticos desde a mudança para o trabalho remoto.

Ainda mais preocupante é que, para os invasores cibernéticos, as grandes empresas não são o único alvo. Na verdade, um relatório da Hiscox descobriu que uma pequena empresa no Reino Unido é invadida com sucesso a cada 19 segundos.



Para melhor ou para pior, o trabalho longe do escritório veio para ficar. Mas sua implementação foi apressada e não sem consequências.

Novos pontos de vulnerabilidade

O recente aumento dos ataques cibernéticos contra empresas pode ser largamente colocado aos pés da "Shadow IT", um termo abrangente para aplicativos e serviços não autorizados pelo departamento de TI da empresa.

Para sermos justos com os funcionários, a razão mais comum para baixarem aplicativos não aprovados é um esforço sincero para fazerem o seu trabalho de forma produtiva.

Os culpados comuns da Shadow IT incluem conversores gratuitos para download de PDF para documento e JPEG para vetor. Embora essas ferramentas online possam oferecer uma solução rápida, elas também costumam conter malware no código e, portanto, os funcionários inadvertidamente integram hackers.

Mas o risco da Shadow IT tem sido agravado pela ascensão da IoT, a Internet das Coisas.

Hoje, há **11 bilhões** de dispositivos conectados, e a previsão é que esse número quase duplique nos próximos cinco anos.

Não pensamos duas vezes sobre o nosso telefone de trabalho se conectar ao nosso alto-falante Bluetooth. Mas até os objetos mais aparentemente benignos, como uma boneca de brinquedo, são potenciais pontos de vulnerabilidade quando se conectam à Internet.

Novos pontos de vulnerabilidade

> A sofisticação do cibercrime não está no indivíduo. Está na plataforma.

Brett Johnson, um prolífico hacker que se tornou um especialista white-hat, sugere que noventa por cento de todos os ataques usam explorações conhecidas, como dispositivos Bluetooth desavisados.

Existem vários guias de instruções online. Os cibercriminosos entendem o poder da rede. Se os dados necessários para realizar um ataque não estiverem disponíveis instantaneamente, eles recorrerão aos fóruns para obter o que precisam.

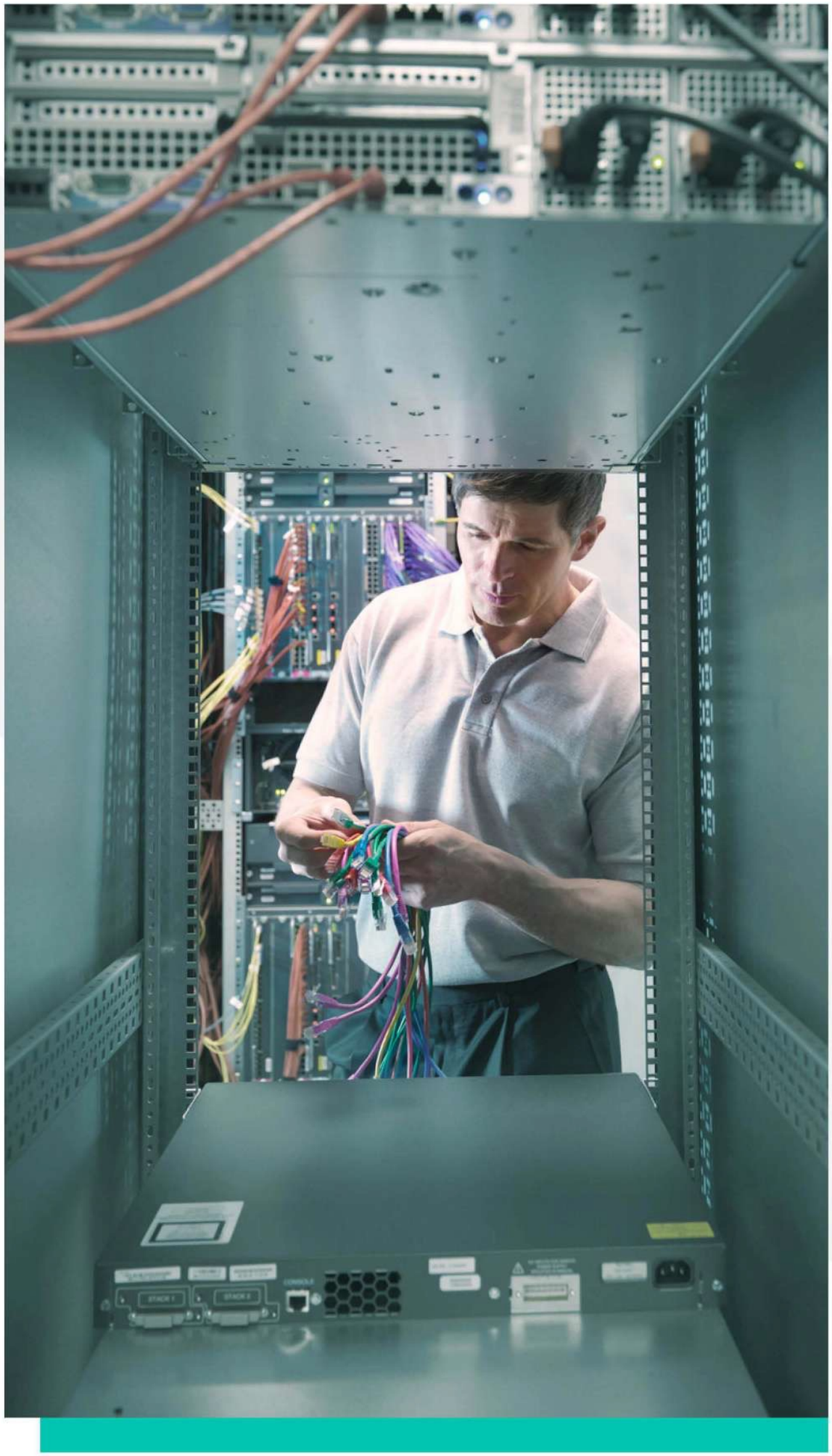
“Você nunca irá cobrir todas as vulnerabilidades que sua empresa possui. Isso é um fato."

80%

das organizações de TI encontraram dispositivos de IoT em suas redes que não instalaram, protegeram ou gerenciaram. Há uma tentativa de invasão em dispositivos de IoT em média 5.200 vezes por mês.

Então qual a probabilidade de que sua empresa esteja exposta?

Parte do problema é que esta tecnologia ainda está na sua infância. Sem a largura de banda para criptografia, a maioria dos dispositivos de IoT são inerentemente inseguros e, portanto, os cibercriminosos os usam para saltar para o alvo real. Sem a proteção certa, algo tão inocente como ligar seu celular de trabalho ao novo purificador de ar que você comprou pode custar caro.



Novos pontos de vulnerabilidade

Violações de dados custam milhões às empresas

No ano passado, o custo médio de uma violação de dados no Reino Unido aumentou, de 2,98 para 3,59 milhões de libras. Uma parte considerável deste custo vem de clientes perdidos.

Em uma violação de dados típica, 38% do total (1,21 milhão de libras) deve-se a clientes em fuga, a uma reputação prejudicada e a disfunções técnicas.

É claro que estes números são pequenos em comparação com o que a IBM chama de “mega-violação”, quando são explorados entre 50 e 65 milhões de registros, cujo preço médio é de 306 milhões de libras.

"Se você estiver implantando um ransomware, isso normalmente significa algum tipo de ataque de engenharia social". Johnson explica, da perspectiva de um black-hat, como pode ser pouco desafiador invadir uma organização.

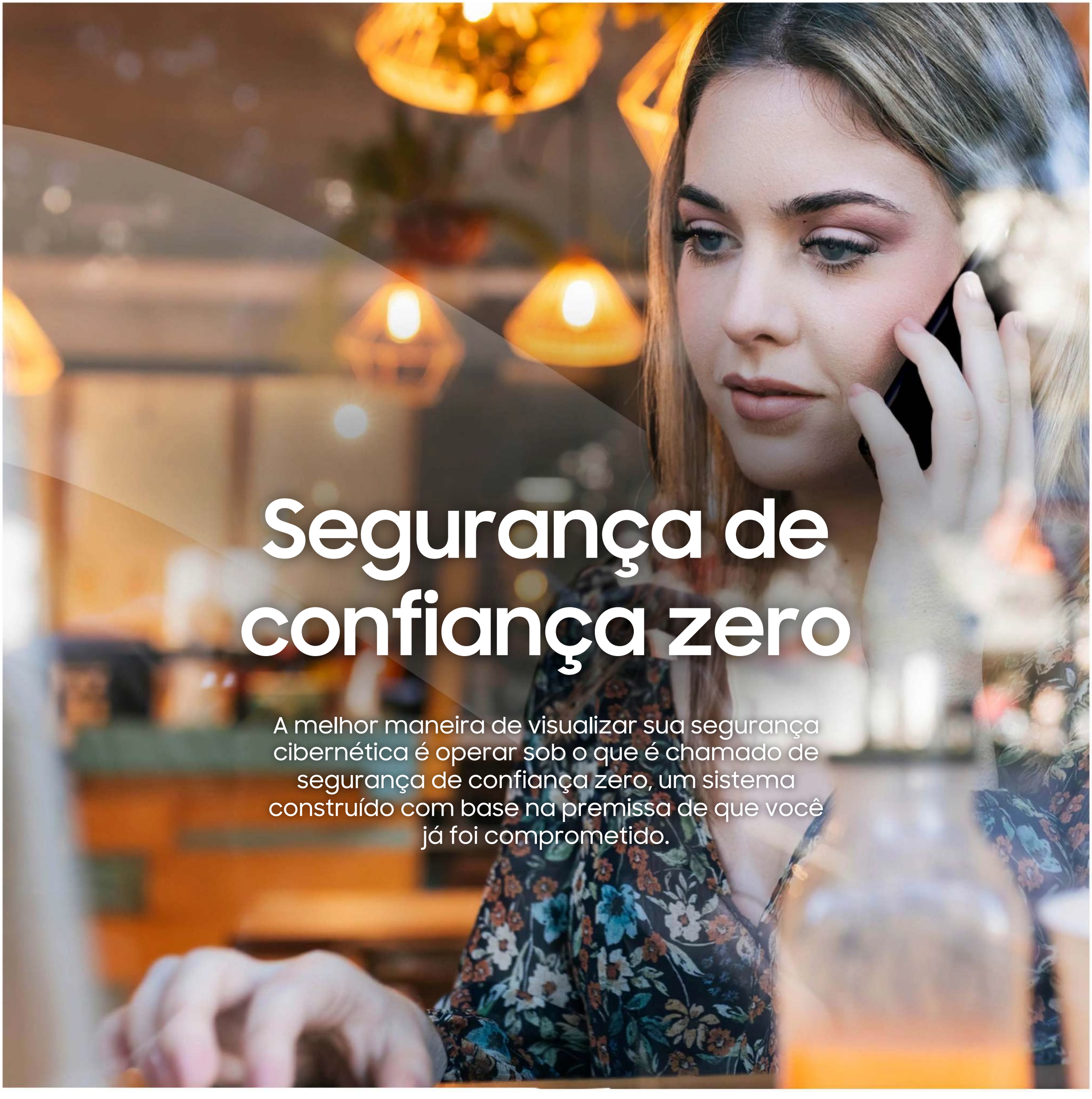
“Por que eu tentaria passar pela força bruta por um firewall aprovado industrialmente se a única coisa que preciso fazer é enviar um e-mail para alguém que está atrás desse firewall?”

A despesa pesada das violações de segurança também é o resultado da perda de tempo e recursos. Quando ocorre um ataque cibernético, especialmente em uma rede grande, eliminar o malware leva meses.

De acordo com a IBM, o número médio de dias decorrido antes de uma violação de dados ser contida é 287. Para colocar isso em perspectiva, se sua empresa for vítima de um ataque cibernético em 1º de janeiro, ele não estará contido até 14 de outubro.

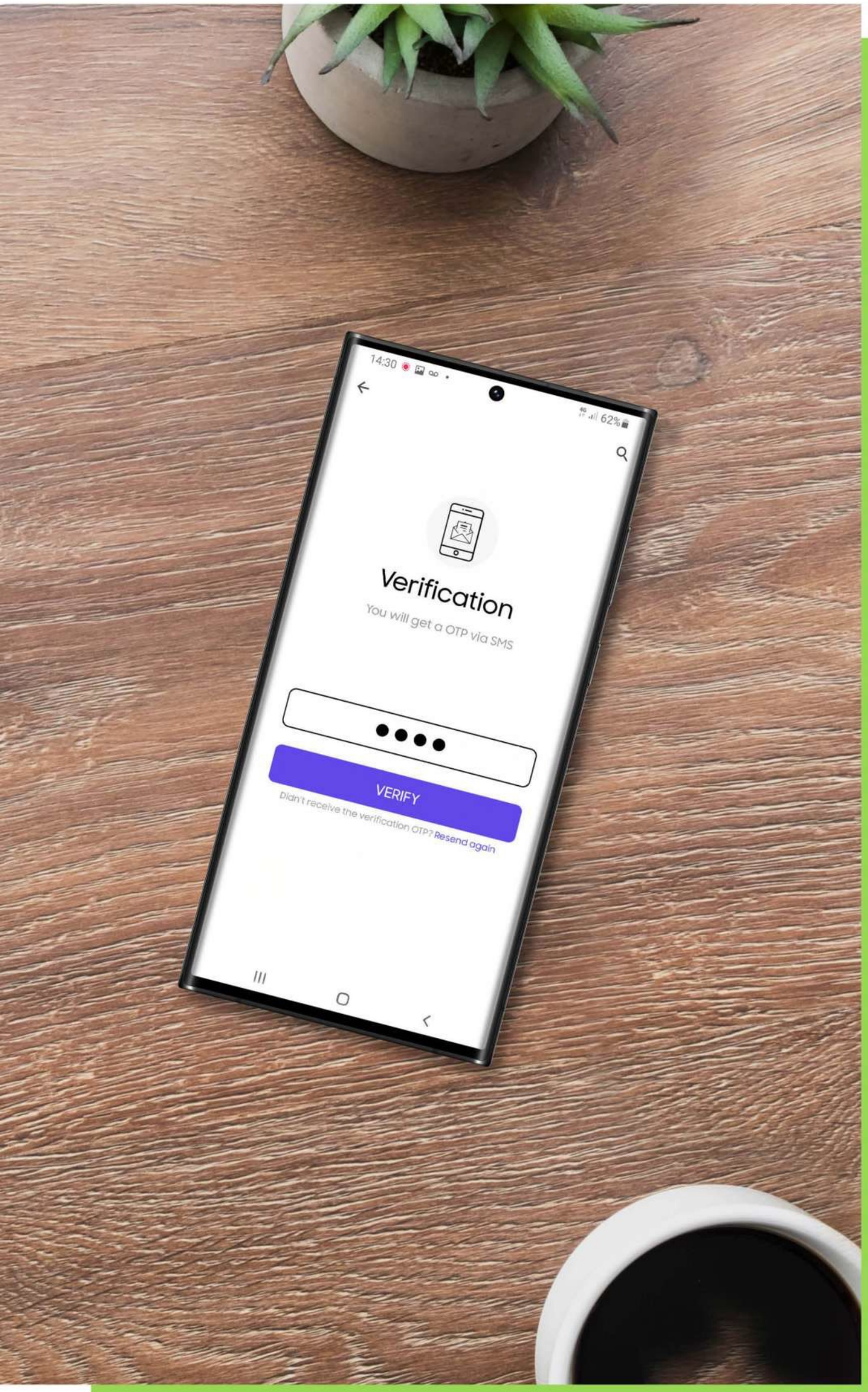
Este período de tempo aumenta quando os funcionários trabalham em casa. O mesmo relatório da IBM descobriu que as empresas com mais de metade de seus funcionários que trabalham remotamente demoraram 58 dias a mais para identificar e conter violações do que aquelas que tinham mais funcionários no escritório.

As violações de dados custam milhões às empresas



Segurança de confiança zero

A melhor maneira de visualizar sua segurança cibernética é operar sob o que é chamado de segurança de confiança zero, um sistema construído com base na premissa de que você já foi comprometido.



Se você já usou a verificação em duas etapas, então está familiarizado com o princípio básico da abordagem de confiança zero, que permite que um funcionário remoto se conecte com segurança a qualquer empresa de qualquer lugar.

Cada vez que um usuário tenta acessar os recursos da empresa, o funcionário precisa verificar sua identidade de alguma forma, como reconhecer o login em um dispositivo móvel.
Este controle de verificação permite ao departamento de TI conceder diferentes níveis de acesso, dependendo das condições de entrada.

Este é o modo padrão em segurança de confiança zero: o acesso a aplicativos e serviços é estritamente condicional. O ônus da prova recai sobre o usuário para confirmar sua identidade. Este processo também coleta outras informações úteis para a cibersegurança, como o estado de um dispositivo, sua localização e a hora do dia.

Esta visibilidade melhorada em toda a rede torna mais fácil detectar e parar violações trazidas pelo malware. E, de acordo com um relatório da Forrester, ao cessar a exfiltração de dados para as mãos de agentes maliciosos, o método de confiança zero também reduz as despesas de segurança.

Estes fatos explicam porque três em cada cinco líderes empresariais dizem que sua abordagem de segurança de confiança zero permitiu uma melhor transformação digital.

Segurança de nível de defesa para proteção em qualquer lugar

O departamento de TI tinha um trabalho mais fácil defendendo os dispositivos sob sua responsabilidade quando todos eles estavam no mesmo edifício. Mas agora que os funcionários deixaram a segurança relativa dentro das paredes do escritório, os líderes empresariais precisam de uma nova abordagem para gerenciar o risco atual.

Você pode ajudar a proteger seus dados e aplicativos empresariais críticos empregando algumas medidas básicas de segurança, como autenticação biométrica, confiança zero e hardware e software seguros. Mas isso não é tudo o que você pode fazer.

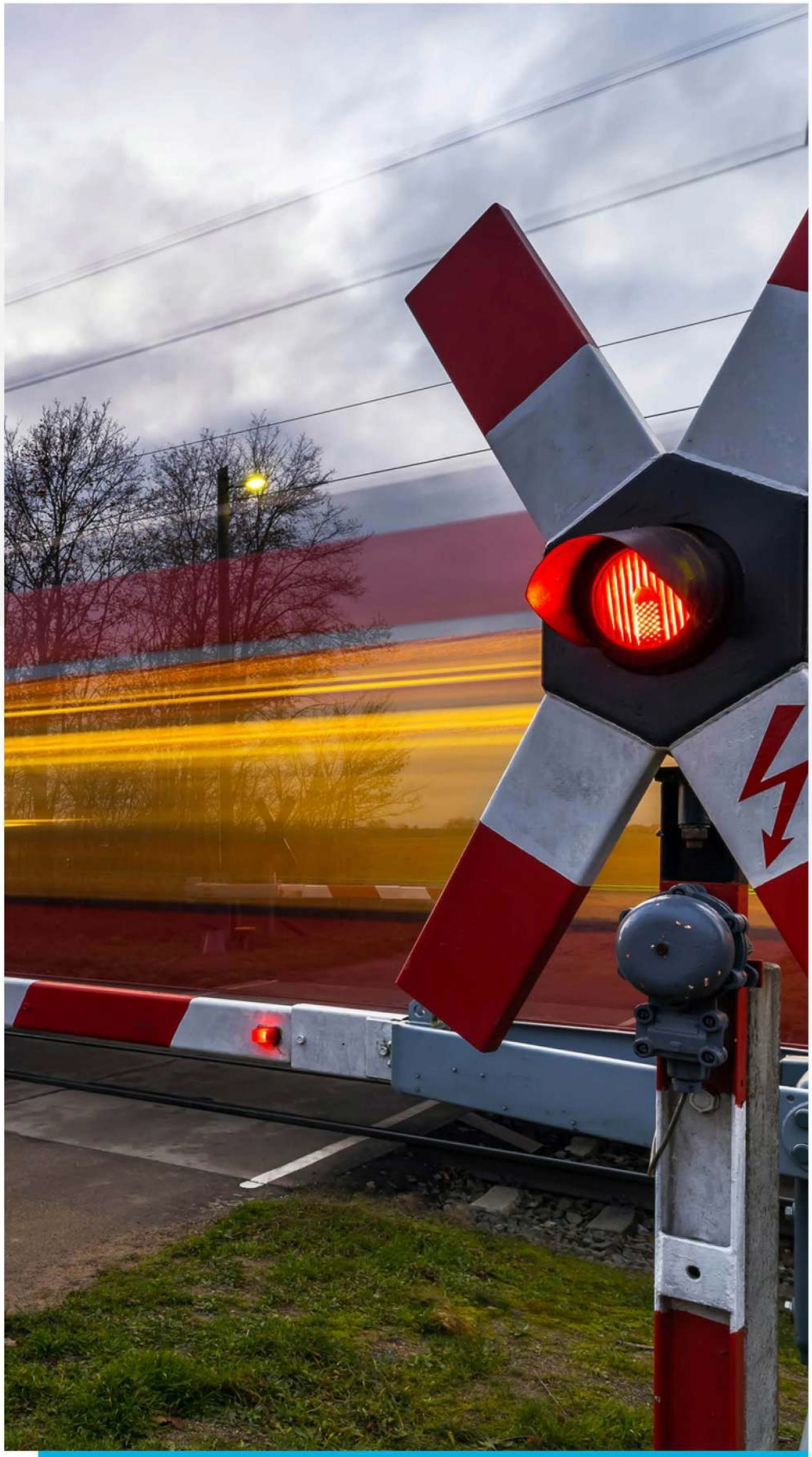
Ferramentas de segurança Samsung x Android

Privacy Dashboard: Esta ferramenta permite aos usuários gerenciar as permissões de aplicativos e ver quais deles acessaram sua localização, câmera ou microfone nas últimas 24 horas

Google Play Protect: Proteção sempre ativa que analisa todos os aplicativos do dispositivo para detectar malware e aplicativos prejudiciais. A API SafetyNet Attestation e a API Safety VerifyApps podem ser usadas para verificar se um dispositivo foi enraizado e se há a presença de malware.

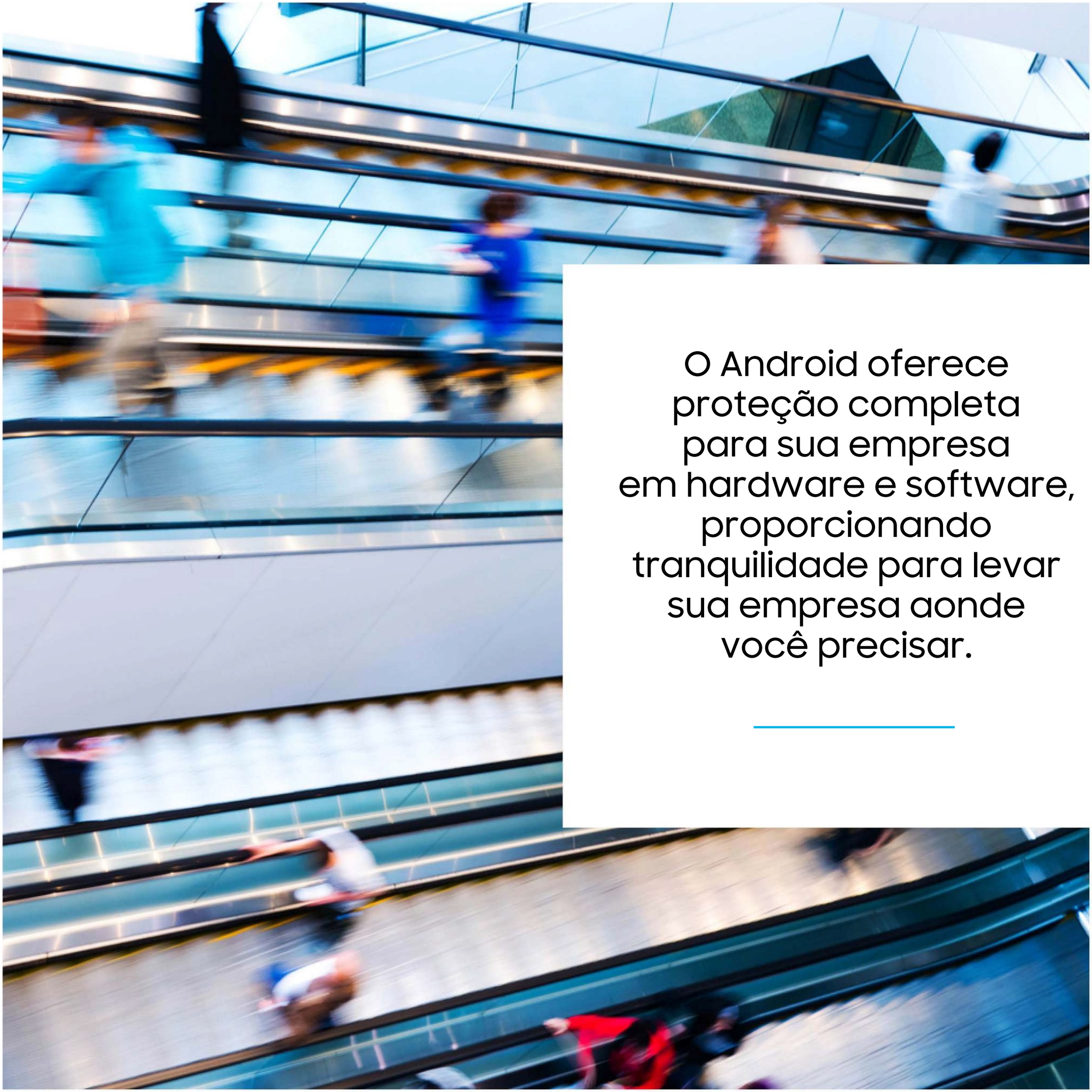
Perfil de Trabalho do Android: Permite aos funcionários trabalharem de forma segura nos seus dispositivos móveis habilitados pessoalmente. Perfis pessoais e de trabalho separam os aplicativos sem compartilhamento de dados, garantindo a privacidade do usuário e a segurança dos dados da empresa.

Segmentação de Rede 5G: Com o Android 12, há conectividade dedicada para todos os aplicativos no perfil de trabalho. Garante qualidade de serviço, velocidades mais rápidas e alta segurança para dados de trabalho



O Android expandiu o papel dos chamados provedores de identidade, como ForgeRock e Okta, para cultivar um ambiente de confiança zero. Ajudando os funcionários a se afastarem do WebView para autenticação de usuários e permitindo que os provedores de identidade coletem sinais de confiança do dispositivo, o Android está melhorando a segurança do usuário, ao mesmo tempo que permite o logon único em aplicativos nativos e na web (para que você só precise se verificar uma vez).

Segurança de nível de defesa para proteção em qualquer lugar



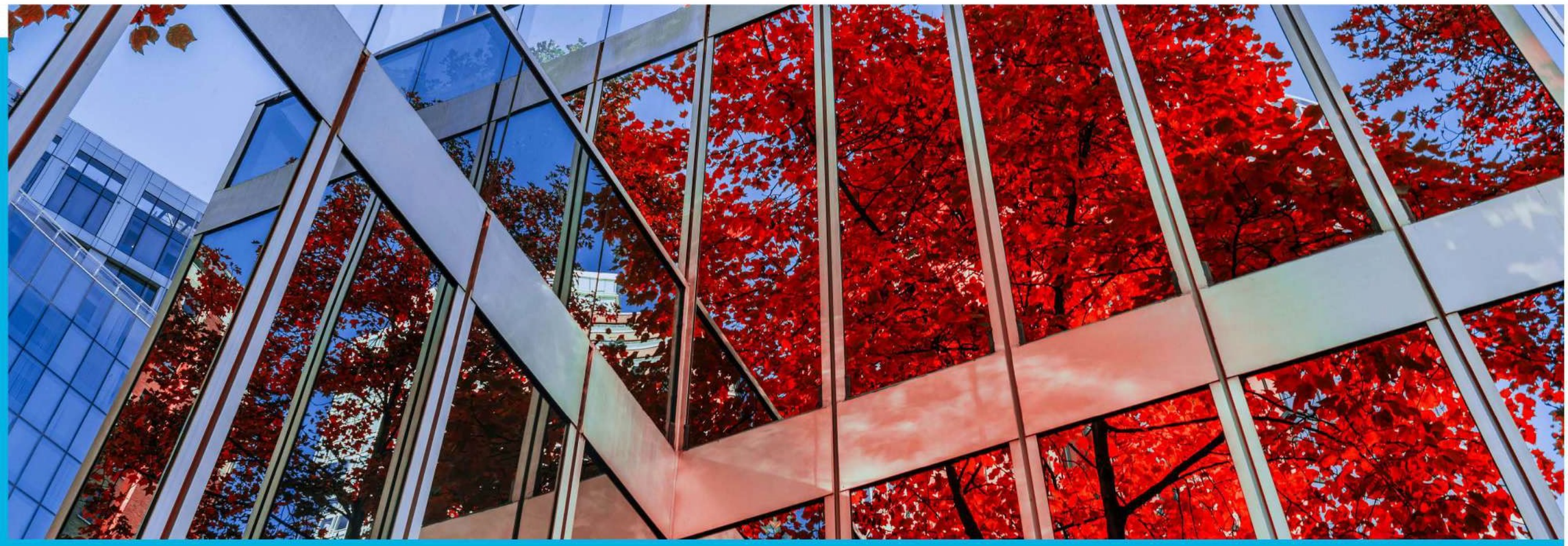
O Android oferece
proteção completa
para sua empresa
em hardware e software,
proporcionando
tranquilidade para levar
sua empresa aonde
você precisar.

Os dispositivos Samsung fazem parte do Android Enterprise Recommended, excedendo os rigorosos requisitos definidos pelo Google. Os dispositivos recebem patches de segurança regulares, juntamente com atualizações importantes garantidas, proporcionando segurança, eficiência e produtividade excepcionais.

Com um dispositivo Samsung equipado com o sistema operacional Android, você tem a **confiança** de que seus dados estão **protegidos** - onde quer que seu pessoal esteja trabalhando.

Você também pode controlar suas atualizações de segurança com o Knox E-FOTA, que permite personalizar como e quando as atualizações são entregues na sua frota. Você pode até forçar atualizações críticas em todos os dispositivos, sem que os usuários realizem qualquer ação. Dessa forma, você pode garantir que todos os dispositivos tenham medidas de segurança atualizadas para proteger contra as ameaças atuais. E você pode restringir os funcionários de fazerem o download de qualquer coisa que possa deixar seus dispositivos móveis expostos a ataques.

O Samsung Knox, juntamente com o sistema operacional Android, entregam a melhor segurança para sua empresa.



O Enterprise Edition da Samsung oferece outras formas de manter a sua frota protegida. Você receberá até cinco anos de atualizações de segurança, o que significa que seus dispositivos sempre terão os patches de segurança e manutenção mais atualizados do Android e da Samsung. Com um controle flexível de aplicativos com o Google Play gerenciado e uma proteção de aplicativos em tempo real com o Google Play Protect, seus funcionários podem implementar e baixar os aplicativos de que precisam sem comprometer a segurança da sua empresa.

Não há dúvida de que os dispositivos conectados à internet tornam a vida mais fácil. Mas trabalhar remotamente abriu um novo cenário de ameaças para as empresas britânicas. As organizações precisam de abordagens que desafiam a percepção das ameaças da tecnologia móvel e dos dispositivos de IoT. É provável que o departamento de TI nunca tenha esperado que a máquina de café fosse infectada com malware.

A melhor maneira de ver o mundo pós-pandemia da segurança online é olhar para ele através de uma lente de confiança zero — um sistema de segurança que assume que os seus dados já fora comprometidos.

Com uma força de trabalho móvel crescente, a higiene da cibersegurança é cada vez mais importante. Isso envolve uma estratégia de confiança zero, autenticação biométrica e criptografia de dados de clientes. São ferramentas inquestionavelmente importantes para proteger seus dados críticos e seus processos empresariais.

Com estes em vigor, os criminosos cibernéticos enfrentam atritos impenetrados. E isso é o suficiente para manter sua empresa segura.

A abordagem de multi-camadas do Android para a segurança

Gerenciamento de Segurança: Controles de política aplicados pelo gerenciamento do Knox.

Serviços de Segurança do Google: Análise, verificação e correção de aplicativos do Google Play Protect e antiphishing do Google Safe Browsing.

Plataforma do Sistema Operacional: A segurança completa da plataforma garante a integridade do dispositivo e dos dados.

Hardware: A segurança com suporte de hardware obrigatória protege tarefas e operações críticas.

Permita que sua empresa funcione de forma aberta e segura. Para saber mais, fale com o seu Gerente de Conta Samsung, ou visite nosso website.