



O QUE ESTÁ NA SUA REDE?

Levando em consideração a Internet das Coisas (IoT), uma força de trabalho móvel permanente e o BYOD, as organizações de hoje enfrentam uma infra-estrutura de TI cada vez mais complexa e mais exposta aos ataques cibernéticos do que nunca.

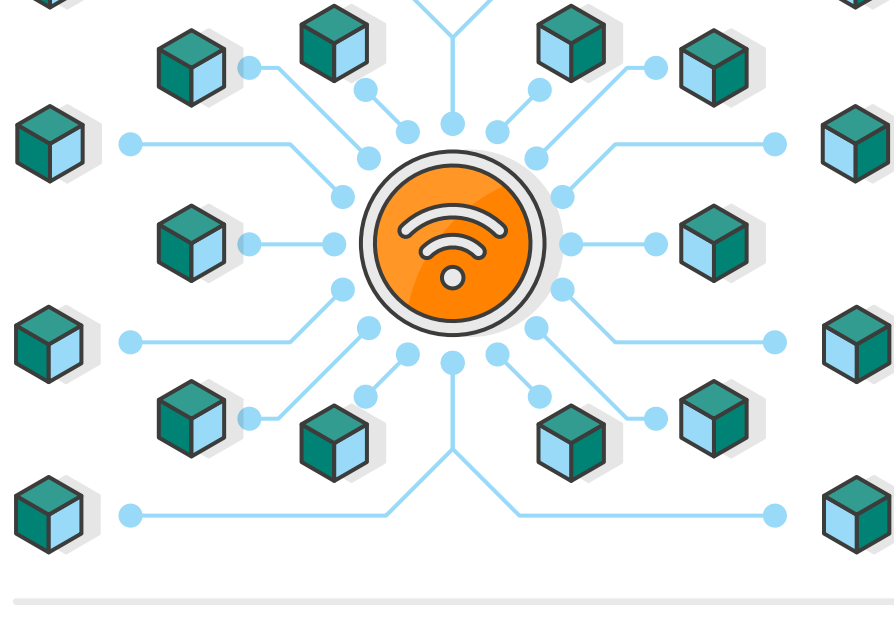
Sua empresa está pronta?

IoT: está aqui... e está crescendo!

O crescimento da IoT é exponencial—ultrapassando facilmente a capacidade da sua organização para gerenciá-la e protegê-la.

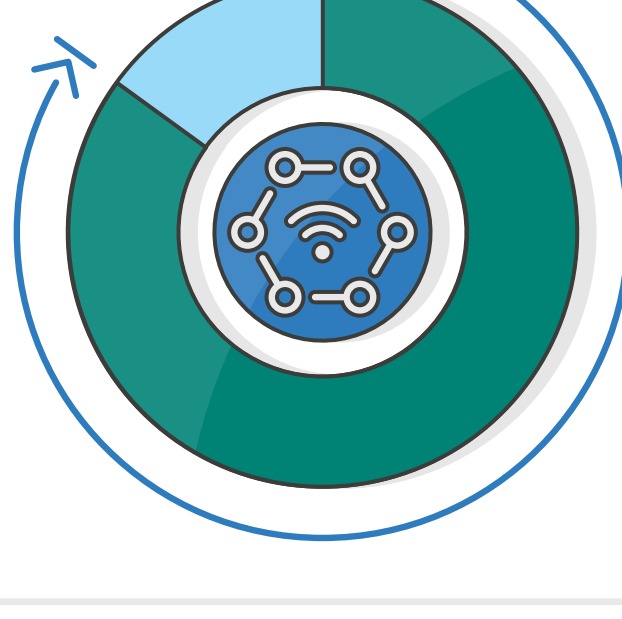
8,4 bilhões de "coisas"

A expectativa é que sejam conectadas às redes em 2017.¹



85% das empresas

implementará IoT em suas redes em 2019.²



Mas como você garante o negócio e a infraestrutura da IoT?

Os Diretores de Informações e os Diretores de Segurança da Informação já o descobriram:

8 de cada 10 organizações

sofreram uma violação de segurança relacionada à IoT.³



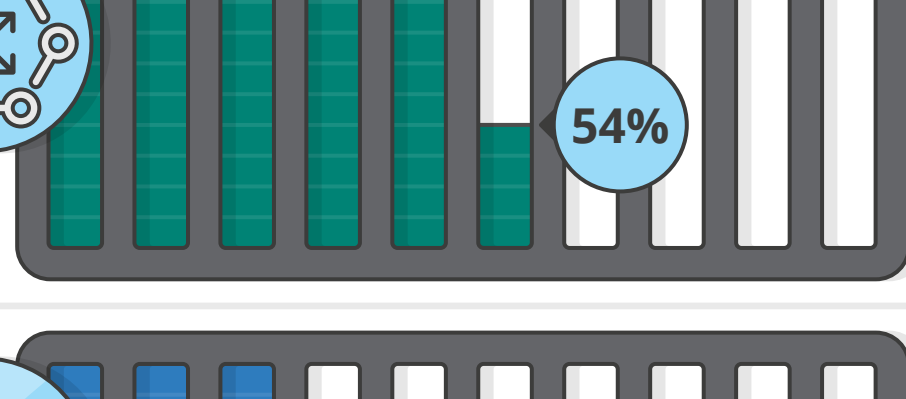
A segurança de IoT é uma dor de cabeça para TI

O negócio implementa os requisitos de TI, com mais aplicativos e dispositivos para ativar, bem como mais "coisas" que monitoram e precisam ser monitoradas, cada um com seu próprio aplicativo, em toda sua rede corporativa. O resultado: os riscos de segurança **aumentam**, enquanto a visibilidade e a produtividade **caem**.

Segundo a pesquisa do ESG, mesmo os profissionais da cibersegurança estão sentindo a tensão da IoT⁴:

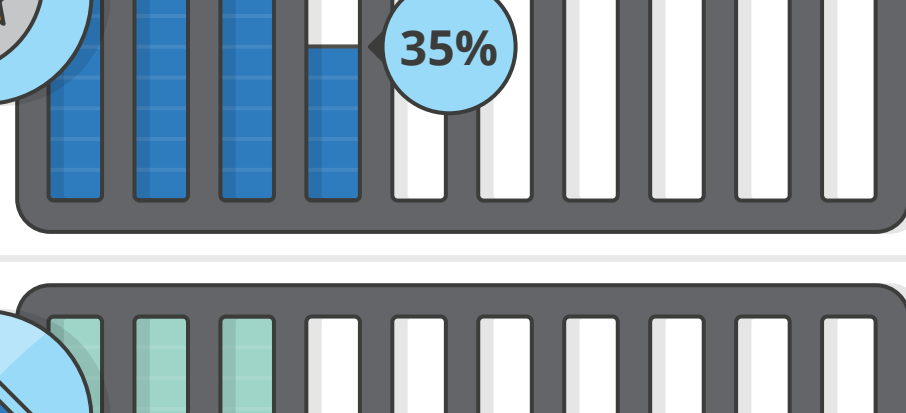
54%

A maioria diz que a falta de habilidades de segurança cibernética aumentou a carga de trabalho, aumentando a fadiga dos analistas.



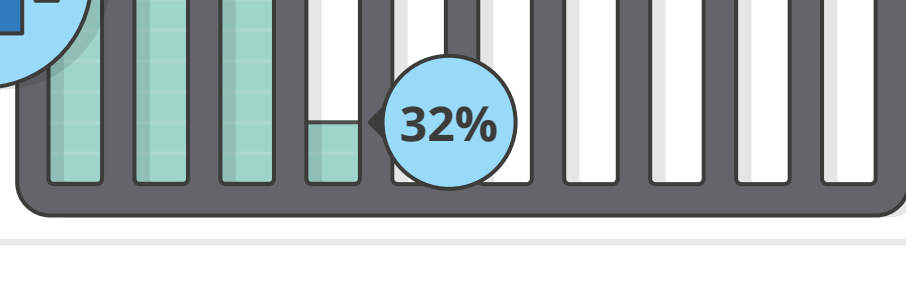
35%

Mais de 1/3 não pode utilizar as tecnologias de segurança para todo seu potencial, diminuindo a eficiência.



32%

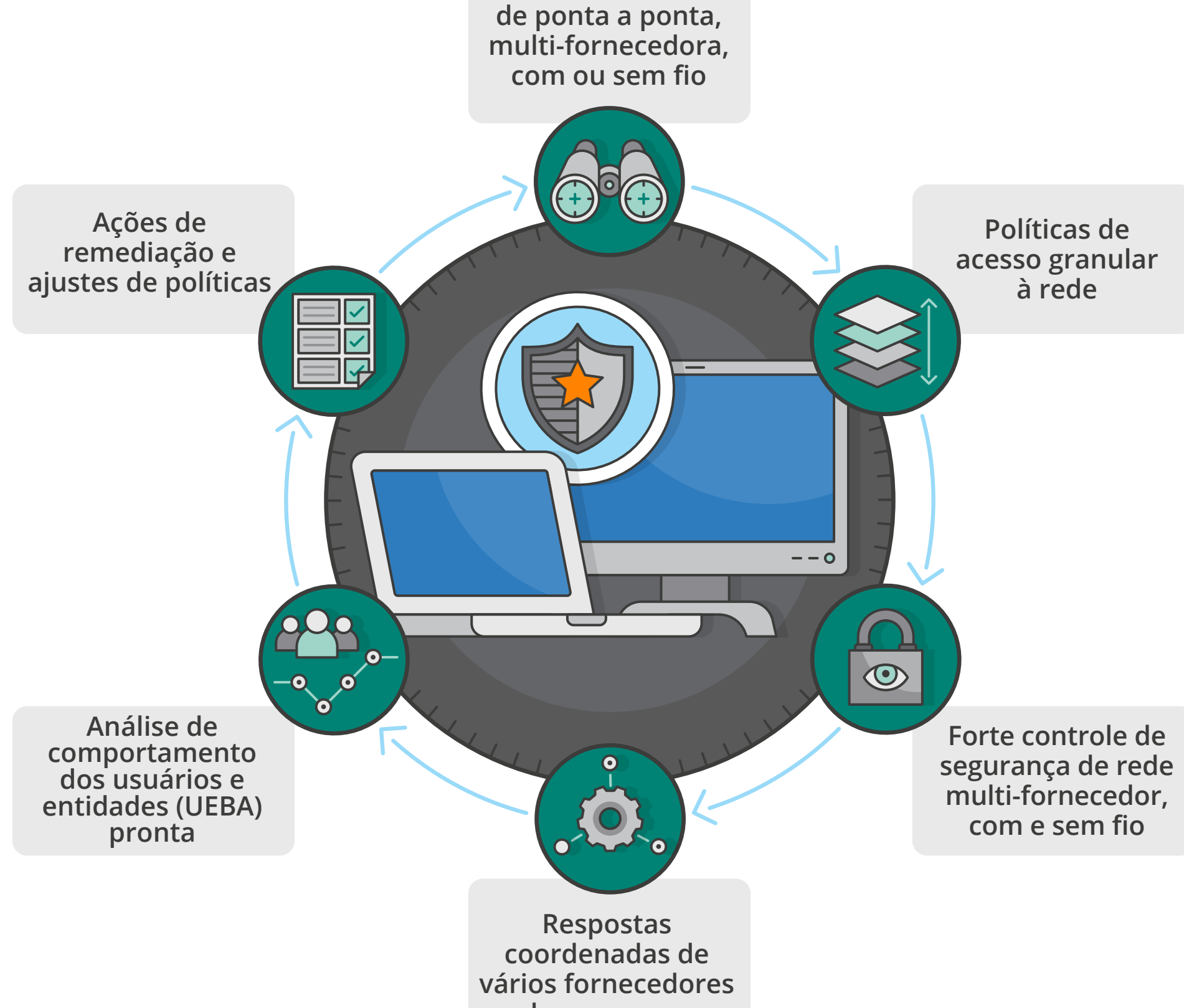
Cerca do mesmo número relataram maior desgaste e volume de negócios, exacerbando a situação.



Alívio para suas dores de segurança

A implantação e retenção do controle da IoT, bem como dos dispositivos corporativos e BYOD, são simples, os CISO podem trabalhar com os CIO para permitir negócios seguros. Mas qual é a melhor maneira de prosseguir?

Faça uma abordagem de "loop fechado" para a segurança da rede com⁴:



APRESENTAÇÃO DO ARUBA CLEARPASS

O Aruba ClearPass fecha o loop, desse modo apenas a IoT aprovada, autenticada e saudável, bem como os dispositivos corporativos e BYOD podem se conectar à sua rede.

1

IDENTIFICA
dispositivos em sua rede, quantos, como eles se conectaram e seus sistemas operacionais.

2

APLICA
políticas precisas para fornecer acesso adequado aos usuários, independentemente do usuário, tipo de dispositivo ou localização.

3

PROTEGE
recursos através de controles dinâmicos de políticas e correção de ameaças reais que se estendem a sistemas de terceiros.

Encontre a paz mental



Aruba, a Hewlett Packard Enterprise Company, é um fornecedor líder de soluções da próxima geração.

Mantenha sua rede segura e gere valor, para que você possa se concentrar na prevenção, detecção e resposta a ameaças com o Aruba ClearPass.

Quão segura é a sua rede empresarial?

Descubra agora com nossa Avaliação de Segurança Empresarial.

AVALIE SEU RISCO

