Preocupações com segurança aumentam conforme a IoT se expande

Insights de mercado sobre o estado da segurança da IoT

ESTUDO

ECOSSISTEMAS CONECTADOS

Minimizando os riscos à segurança da IoT numa era de crescentes ameaças

Uma tendência importante que poderá ter um impacto transformador na economia digital do futuro é a Internet das Coisas (IoT). A IoT já está trazendo recursos avançados às aplicações no mundo real, desde carros conectados e medidores de energia inteligentes até monitoramentos da saúde. De acordo com uma estimativa, o número de dispositivos conectados em todo o mundo deve aumentar 12% anualmente, em média, passando de quase 27 bilhões em 2017 para 125 bilhões em 2030.[1]

A operação da IoT se baseia em diversas tecnologias fundamentais subjacentes. As principais delas são as redes de comunicações, os dispositivos e componentes de hardware, como sensores, instrumentos sem fio e softwares. Como qualquer sistema de TI, as redes e dispositivos são suscetíveis à manipulação, interrupção e invasão. E por tais dispositivos estarem conectados uns aos outros, caso um seja comprometido, um hacker tem a oportunidade de se conectar a muitos outros dispositivos na rede.

Embora a IoT ofereça muitos benefícios, ela também abre um ponto de entrada atrativo para que agentes maliciosos obtenham acesso a sistemas considerados seguros. Num momento em que os ambientes de segurança começam a sentir pressões relativas a custos e crescimento, os especialistas em segurança da IoT enfrentam uma tarefa monumental de encontrar uma maneira de proteger as redes e dispositivos contra uma rede crescente de possíveis ameaças que podem comprometer a privacidade pessoal e a segurança pública.

42%

das empresas sofreram uma invasão direta nos últimos dois anos.

59%

acham difícil a conformidade com os regulamentos de segurança.

Resumo executivo: Entendendo os riscos e desafios da IoT

Para melhor entender como as empresas estão se preparando e respondendo às ameaças atuais e emergentes à segurança da IoT, a UL se juntou à Bloomberg Next para realizar uma pesquisa com executivos e gerentes seniores dos principais setores, incluindo o de varejo, produção e saúde. A pesquisa visava os tomadores de decisões responsáveis pela coordenação, supervisão e gestão das iniciativas e práticas de segurança da IoT em suas respectivas empresas.

O estudo se concentrou em compreender diversos objetivos fundamentais:

1. Avaliar o escopo global e a profundidade da ativação da IoT nos processos, produtos e serviços.
2. Entender as atitudes relacionadas à vulnerabilidade da IoT, as áreas de preocupação e como os riscos são avaliados e minimizados.
3. Determinar a familiaridade com as normas de segurança e avaliar as variações da dificuldade de conformidade entre setores e regiões diferentes.

As descobertas revelam insights novos acerca do modo pelo qual as empresas enxergam os riscos de segurança da IoT e as medidas que estão tomando para solucionar vulnerabilidades, proteger ativos críticos e cumprir requisitos regulatórios novos e emergentes. A ameaça de uma invasão de rede é uma preocupação comum entre os gerentes da IoT — e deveria ser mesmo.

Conforme crescem as preocupações com a segurança, paralelamente à adoção da IoT, as descobertas destacam as dificuldades que as empresas estão enfrentando em seu combate às ameaças crescentes. Em outras áreas fundamentais, a pesquisa descobriu que:

- A segurança da IoT é uma preocupação importante para todos os setores, com 49% das empresas indicando que estão "muito preocupadas" com a segurança cibernética em geral.
- Enquanto a prontidão da segurança vacila, a expansão global da IoT continua a pleno vapor. A Ásia possui o maior crescimento na necessidade de minimização dos riscos à segurança, dado o rápido aumento das adoções da IoT na região.
- As empresas que sofreram uma invasão estão tomando mais medidas ativamente para reduzir os riscos, em comparação àquelas que não passaram por um ataque.
- Os ataques levam as empresas a mudar a abordagem. Mais especificamente, a busca por recursos externos tem sido mais frequente entre quem sofreu uma invasão.
- A maioria das empresas (59%) acha difícil a conformidade com os regulamentos de segurança. Esta dificuldade foi notavelmente maior na Europa (71%), o que coincide com um nível menor de familiaridade com as normas de conformidade.
- Quando se trata de implementar um novo plano de segurança da IoT, 52% das empresas planejam trabalhar com um especialista terceirizado.

Quase metade

das empresas pesquisadas relatou ter sofrido uma invasão direta nos últimos dois anos. Para empresas dos EUA, este número é notavelmente maior: 53%.

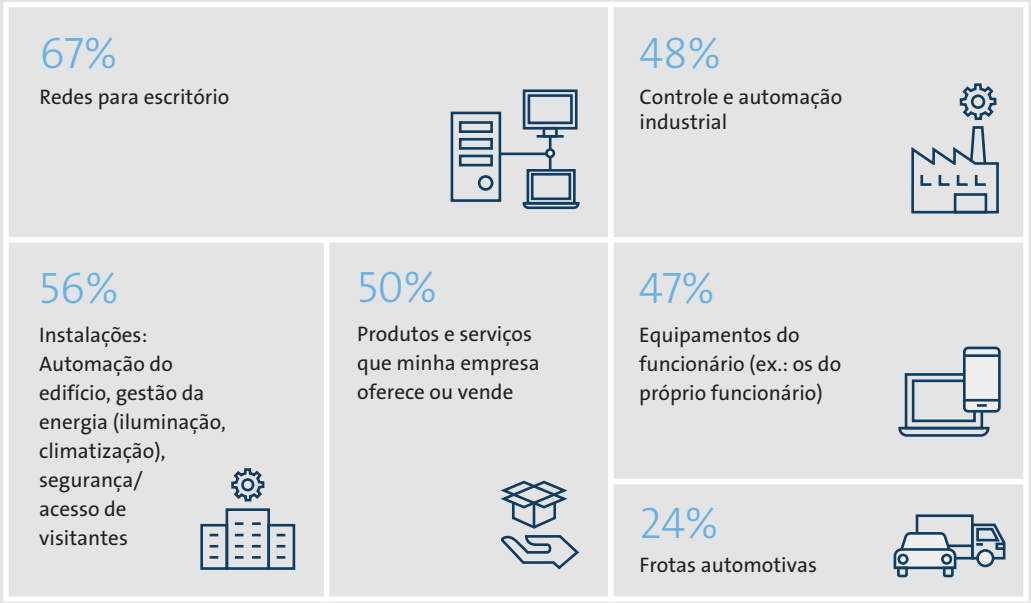
As adoções da IoT continuam a crescer

Avanços rápidos nos setores de produção, eletrônicos e TI estão intensificando a demanda por produtos e serviços da IoT. Nossa pesquisa mostra que as empresas estão implementando funções da IoT em diversos ecossistemas. As redes corporativas foram a adoção mais comum (67%), seguidas de instalações/edifícios (56%), produtos e serviços (50%), automação industrial e controles de automação (48%) e equipamentos e dispositivos para os funcionários (47%).

Os Estados Unidos são o maior mercado de adoção da IoT, seguido pela Europa e a Ásia. A Ásia possui o maior crescimento na necessidade de minimização dos riscos à segurança cibernética, dado o rápido aumento e amplo espectro das adoções da IoT.

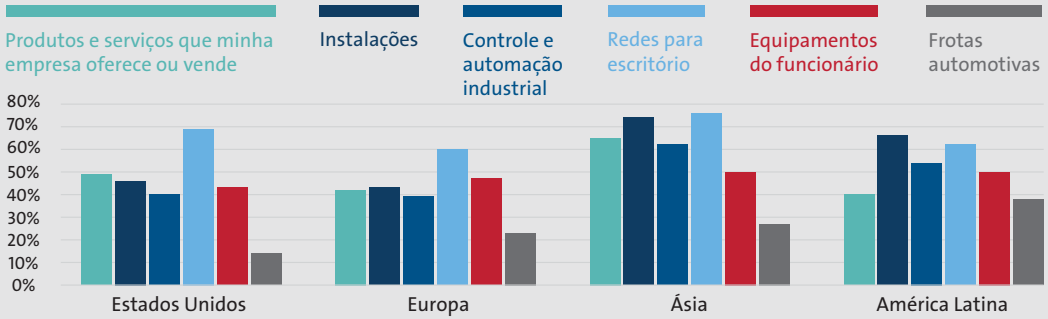
A América Latina também está passando por um crescimento substancial, principalmente no mercado de cidades inteligentes, em que as aplicações da IoT são adotadas em serviços públicos, no transporte público e no setor de saúde. Será importante monitorar esta região conforme o mercado amadurece.

Principais ambientes em que as empresas utilizam a IoT.



As empresas na Ásia adotam uma ampla gama de configurações de IoT.

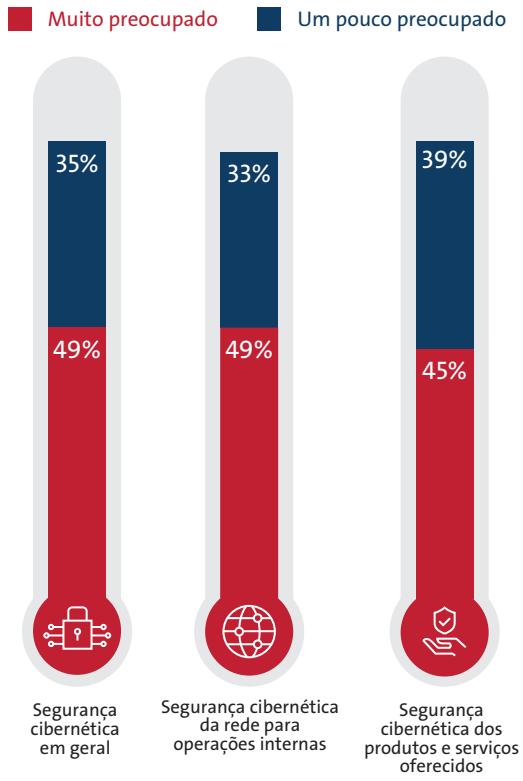
% de empresas em que cada definição está habilitada para IoT



Preocupações crescentes paralelas à adoção da IoT

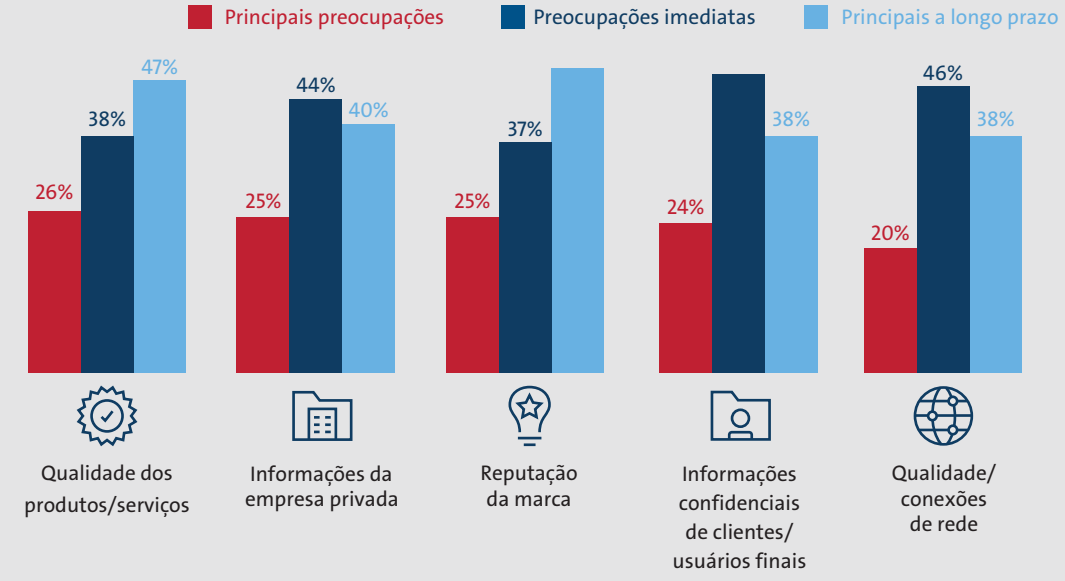
O risco de invasão é uma preocupação importante entre gerentes e executivos das empresas, com quase metade indicando que estão "muito preocupadas" com a segurança cibernética em geral.

As ameaças à segurança criam níveis elevados de preocupação entre executivos.



O desejo de apoiar e proteger o valor da marca é evidente, uma vez que os problemas na experiência dos clientes impulsionam a maioria das preocupações sobre segurança. Mais especificamente, a qualidade dos produtos, a confiança do usuário final e a reputação da marca estão entre as principais preocupações e tendem a ser problemas a longo prazo. As preocupações em torno da privacidade das informações do usuário final e da própria rede tendem a ser mais imediatas.

Os problemas na experiência dos clientes impulsionam a maioria das preocupações sobre segurança a longo prazo.



As áreas de preocupação variam em setores específicos:

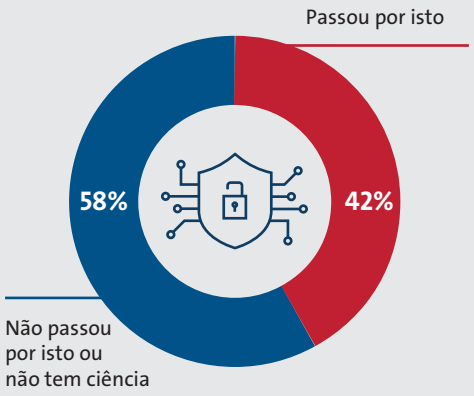
- No setor de saúde, proteger as informações confidenciais do usuário final é a prioridade.
- Na produção, a qualidade e a conexão da rede são a prioridade.
- No varejo, a reputação da marca e a confiança dos clientes são mais importantes.

O perigo oculto das invasões não detectadas

Cada dispositivo novo da IoT acrescenta outro caminho para ataques aos sistemas de TI, e é preciso apenas uma vulnerabilidade em um único dispositivo para que haja uma ameaça a todo um ecossistema. Nossa pesquisa mostrou que 42% das empresas sofreram uma invasão direta nos últimos dois anos — motivando-as a fortalecer suas defesas.

Embora o número de ataques informados seja alarmante, talvez mais perturbador seja a incapacidade das empresas de detectar uma invasão em andamento — criando uma falta de conscientização generalizada. Na verdade, quase metade (48%) das empresas não consegue detectar as invasões quando elas ocorrem, de acordo com um relatório de pesquisa publicado pela empresa de segurança digital Gemalto.[2]

Quase metade das empresas sofreu uma invasão direta.



200 dias
— o tempo médio até a detecção de uma invasão.[3]

Um grande desafio é o tempo demasiadamente longo que frequentemente se leva para se detectar uma invasão, o que pode aumentar o perfil de risco da empresa e criar uma falsa sensação a respeito do possível impacto e do grau de perigo da ameaça. De acordo com um relatório da Verizon, o tempo de espera (quanto tempo leva até a detecção da invasão) tem sido, em média, de mais de 200 dias — apesar de levar apenas poucos minutos para se comprometer dados sensíveis.[3]

Embora tais descobertas tenham implicações importantes, a questão mais imediata é: Das 55% de empresas do nosso estudo que não passaram por uma invasão, quantas delas já sofreram a invasão mas nem sabem ainda?

Os registros da atividade de rede são um dos recursos mais importantes para a detecção de ameaças, mas a pesquisa mostra que só 21% das empresas utilizam os próprios dados de registro adequadamente.[4] Raramente, tais registros são verificados proativamente em relação à possibilidade de acesso não autorizado ou um incidente de segurança. Desta forma, a maioria das empresas não faz ideia das invasões e ataques que ocorrem em seus sistemas da IoT.

Quase metade
das empresas não consegue detectar as invasões quando elas ocorrem.[2]

Preparação para um ataque: Da complacência à prontidão

Os riscos relativos aos dispositivos conectados são muito dinâmicos, visto que a própria IoT se adapta e expande em um ritmo acelerado. Além disso, há poucas barreiras contra invasores que tentam atacar um dispositivo da IoT. Ao contrário de um notebook ou computador, que costumam estar equipados com software de segurança e gozam os benefícios de atualizações periódicas da segurança, a única defesa de um dispositivo da IoT pode ser um nome de usuário e senha.

A IoT também gera dados com uma ampla gama de requisitos de segurança. Alguns fluxos de dados demandam uma proteção mínima, enquanto outros podem incluir informações altamente sensíveis — como dados financeiros e aqueles que contêm registros médicos confidenciais — e demandam medidas de segurança importantes. O rápido crescimento e maturidade dos ambientes da IoT traz consigo um interesse em atacar os ativos das empresas, com o objetivo de obter vantagem financeira ou simplesmente causar caos e interrupções. Embora as empresas de todo o mundo estejam preocupadas com invasões à IoT, as medidas de preparação vacilam — ao passo que a própria IoT se expande.

As empresas costumam subestimar a possibilidade de desastre e estão muito despreparadas para as invasões, QUANDO elas acontecem.

As empresas que sofreram uma invasão estão tomando mais medidas ativamente para solucionar as preocupações de segurança cibernética, estando, portanto, mais bem preparadas.

Contratar especialistas externos para ajudar a gerir processos de segurança da IoT é algo mais frequente entre quem sofreu uma invasão.

Ataques à IoT — Do potencial à realidade

Os setores com uma infraestrutura fundamental estão especialmente vulneráveis a ataques à IoT que possam comprometer dados sensíveis e interromper operações cruciais à missão. Somente nos últimos anos, tivemos diversos exemplos de alto perfil que mostram como as vulnerabilidades de software podem trazer consequências perigosas e possivelmente custosas.

Em 2016, uma invasão perpetrada pelo botnet Mirai infectou diversos dispositivos da IoT e, então, os utilizou para iniciar um enorme ataque distribuído de negação de serviço (DDoS) ao provedor de serviços de domínio Dyn.[5] O ataque tirou do ar diversos sites, incluindo o Shopify, a Netflix e o Twitter. O incidente abriu um precedente perigoso em relação a como os dispositivos conectados podem ser "recrutados" pelos invasores e utilizados para fins maliciosos, sem que os proprietários dos dispositivos sequer tomem conhecimento.

Na conferência de segurança DEF CON de 2016, fechaduras de portas, termostatos, refrigeradores e cadeiras de roda estavam entre os dispositivos da IoT que cederam aos ataques de hackers durante uma série de demonstrações.[6] Os tipos de vulnerabilidades identificados durante o evento variavam de decisões ruins de design a falhas na codificação. No total, 47 vulnerabilidades que afetam 23 itens relacionados à IoT, de 21 fabricantes, foram reveladas.

Em março de 2017, o WikiLeaks revelou que a CIA possui ferramentas para invadir dispositivos da IoT, como Smart TVs, para gravar conversas remotamente em hotéis ou salas de conferência — abrindo uma caixa de Pandora de possíveis problemas de privacidade.[7]

Em maio de 2017, o Serviço Nacional de Saúde (NHS) do Reino Unido ficou vulnerável ao vírus WannaCry, que derrubou sistemas de TI em muitas das organizações do NHS, incluindo cerca de 30 fundações hospitalares e 70.000 dispositivos do NHS. Deixados de fora do sistema pelo malware de criptografia de arquivos, muitos escritórios da NHS tiveram que voltar a utilizar caneta e papel, e milhares de operações e consultas foram canceladas.[8]

A pesquisa mostra que as ações são tomadas somente depois de uma experiência pessoal. Mais especificamente, as empresas que sofreram uma invasão estão tomando mais medidas ativamente para reduzir os riscos, em comparação àquelas que não passaram por um ataque.

Os ataques também levam as empresas a mudar a abordagem. Mais especificamente, a busca por recursos externos tem sido mais frequente entre quem sofreu uma invasão.

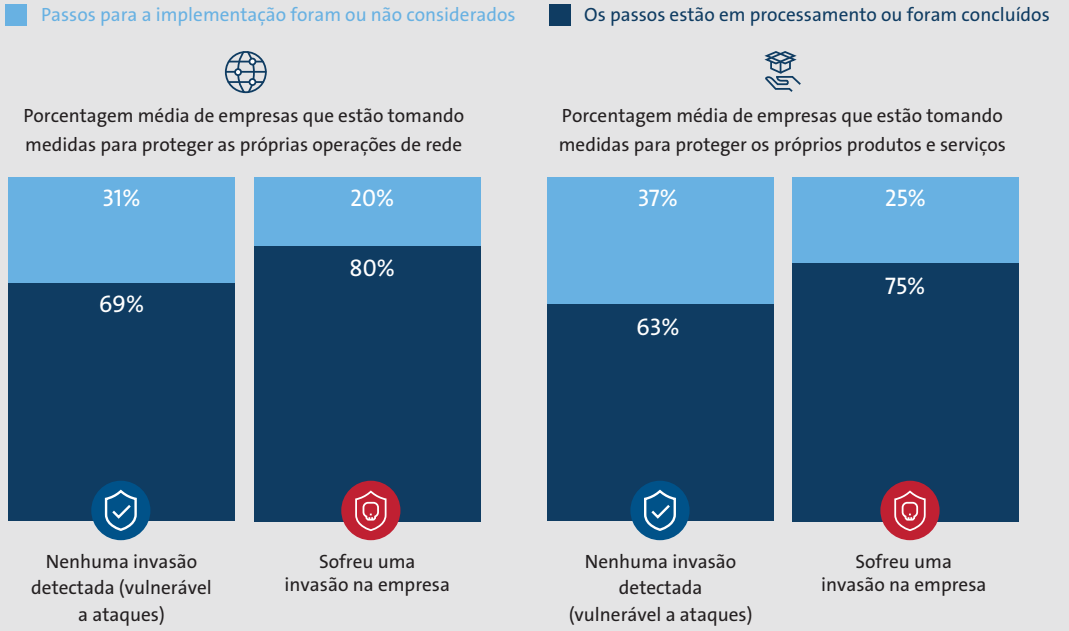
73%

das empresas que sofreram uma invasão contrataram recursos externos.

Somente 14%

das empresas instituíram um processo de auditoria formal para ajudar a entender se os dispositivos delas estão protegidos e quantos eles são.[10]

Medidas tomadas para se reduzir os riscos quando se trata de operações de rede e produtos e serviços.



A experiência pessoal supera a condescendência

A falta de condutas proativas é um comportamento humano comum, caracterizado por uma tendência à normalidade — as pessoas subestimam naturalmente a possibilidade de desastre e seu impacto potencial. É a mesma razão pela qual as pessoas que vivem em áreas que passam por inundações frequentes costumam ignorar a necessidade de se fazer seguro contra enchentes. Na realidade, cerca de 70% das pessoas aparentemente apresentam tendência à normalidade em desastres.[9]

As pessoas costumam presumir que, como nunca enfrentaram um desastre, isto não vai acontecer com elas. Em termos de segurança cibernética, isto costuma resultar em situações em que as pessoas deixam de se preparar adequadamente para — ou até mesmo considerar — a possibilidade de ser vítimas de um ataque aos dados.

Solucionando fraquezas ocultas

As vulnerabilidades de segurança estão sendo solucionadas ativamente pelos desenvolvedores de dispositivos, mas permanecem uma preocupação. Para empresas de diversos setores, uma das causas mais prejudiciais, porém menos identificadas, dos ataques à segurança cibernética, pode ser encontrada em softwares de terceiros adquiridos ou baixados para uso nas operações e sistemas internos, ou para integração aos produtos acabados.

Infelizmente, embora os componentes de softwares de terceiros possam ajudar a aumentar a produtividade no setor de desenvolvimento, e até mesmo resultar em mais qualidade dos produtos, o uso extensivo deles também trouxe novos riscos à segurança cibernética, deixando setores de infraestrutura crucial ainda mais vulneráveis aos ataques cibernéticos.

Sem procedimentos e sistemas adequados para se avaliar e controlar componentes e softwares de terceiros obtidos na cadeia logística de softwares, as empresas podem acabar, desavisadamente, usando ou integrando softwares com segurança insuficiente aos sistemas operacionais ou produtos finais, podendo ser facilmente atacados ou comprometidos.

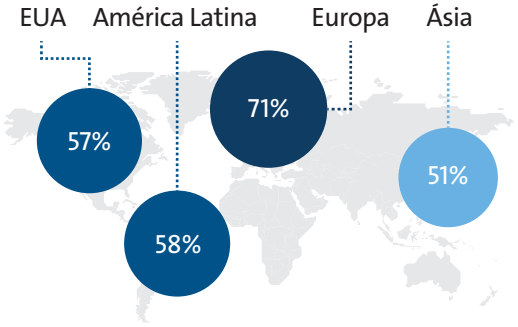
Para empresas de setores de infraestrutura crucial, estes e outros fatores de risco aumentam a importância de se avaliar as vulnerabilidades da cadeia logística de softwares, e de se desenvolver e implementar programas que possam ajudar a reduzir os riscos associados a softwares de terceiros.

Padrões regulatórios: Buscando clareza em um mar de complexidade

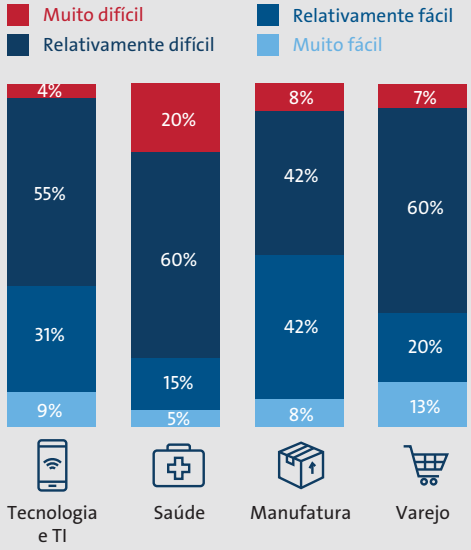
A orientação dos governos e de seus respectivos corpos legislativos pode ajudar a criar uma estrutura e ecossistema seguros para a IoT. Não obstante, embora os padrões de segurança da IoT sejam bem-vindos e muito necessários, a conformidade pode ser desafiadora.

Em nossa pesquisa, a maioria das empresas (59%) acha difícil a conformidade com os regulamentos de segurança. A dificuldade de conformidade foi notavelmente maior na Europa (71%), o que coincide com um nível menor de familiaridade com as normas de conformidade — somente 39% (muita familiaridade), em relação a 66% nos EUA.

Porcentagem de empresas que acham desafiadoras as normas de conformidade.



A percepção da dificuldade de conformidade varia de acordo com o setor.



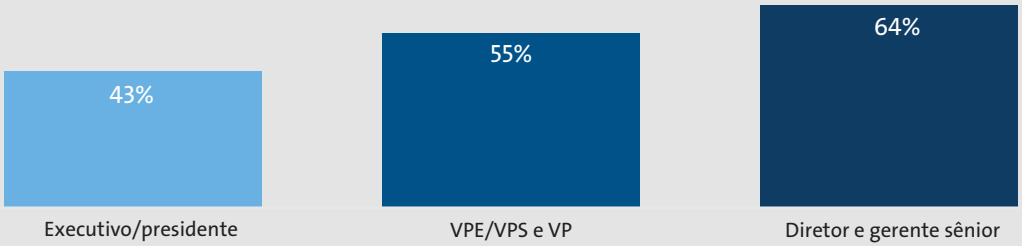
A porcentagem de empresas que encontram dificuldades de conformidade é notavelmente maior nos setores de saúde e varejo, 80% e 67%, respectivamente. O setor de produção considera a conformidade mais fácil do que outros setores, com somente metade informando uma dificuldade.

A função também influencia a percepção da dificuldade. Isto é, quanto mais próximo alguém está do processo de conformidade (táticas e implementação), mais desafiador ele é.

Somente cerca de metade está "muito familiarizado" com as normas do próprio país para a segurança de dispositivos conectados. Uma familiaridade um pouco maior com as normas do setor em relação ao país pode sugerir que estas são priorizadas.

A percepção da dificuldade varia de acordo com as funções de gerência.

Quanto mais perto um gerente está de lidar com as táticas de conformidade e a implementação (ex.: diretores X executivos), maior a percepção da dificuldade



Combatendo o aumento de ataques automatizados

O aumento de botnets e outros ataques automatizados e distribuídos cria uma ameaça que vai muito além de uma única empresa ou setor. Conforme a economia conectada se desenvolve, também cresce o potencial desses vários tipos de ataques de criar uma variedade de perigos digitais.

Para solucionar tais ameaças, o governo dos EUA está trabalhando com as partes interessadas para definir uma série de metas e ações voltadas a aumentar a resiliência do ecossistema. Como uma estrutura orientadora, os departamentos de Comércio e de Segurança Interna dos Estados Unidos publicaram um relatório voltado a promover ações contra tais ameaças. O relatório "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" (Aumentando a resiliência da internet e do ecossistema de comunicações em relação a botnets e outras ameaças automatizadas e distribuídas) atende a uma ordem executiva de maio de 2017 de fortalecimento da segurança cibernética das redes federais e da infraestrutura crucial.[11]

Como parte do esforço da iniciativa privada, o Council to Secure the Digital Economy (CSDE) publicou o guia International Anti-Botnet Guide de 2018, que oferece um conjunto de práticas básicas voluntárias e recursos avançados. Em resposta às preocupações a respeito de uma regulamentação excessiva, o CSDE orientou que "soluções dinâmicas e flexíveis, informadas por padrões consensuais voluntários, impulsionadas por demandas do mercado e implementadas pelas partes interessadas são a melhor resposta a estes desafios sistêmicos em evolução".[12]

As normas de segurança ajudam a definir o futuro da IoT

Para equilibrar o crescimento das preocupações com a segurança da IoT e os desafios do ritmo acelerado de inovação, a UL criou um programa de certificação da segurança cibernética (CAP), de acordo com a nova série de Normas UL 2900. O objetivo do CAP é oferecer um conjunto de requisitos que os fabricantes de produtos conectáveis em rede possam usar voluntariamente para definir uma base de proteção contra as vulnerabilidades e fraquezas do software.

A UL está também contribuindo e liderando o desenvolvimento de diversas normas e programas novos e emergentes de gestão de risco/segurança cibernética, incluindo:

- ISO 18013 Diretrizes para o formato do design e o conteúdo dos dados de uma carteira de direção em conformidade ISO (IDL, na sigla em inglês), com relação tanto aos recursos visuais para leitura humana e as tecnologias ISO para leitura de máquina.
- FIPS 140 Normas de segurança de computadores do governo dos EUA que especifica requisitos para os módulos de criptografia, que incluem componentes tanto de hardware como de software.
- ISO 2434 Recomendações de segurança cibernética sobre mobilidade (incluindo veículos conectados e autônomos).
- UL 5500 Norma da UL que abrange as atualizações remotas de software, além da compatibilidade de hardware necessária para a segurança da atualização remota de software.

Embora não haja uma solução milagrosa para atender a todas as necessidades de segurança cibernética dos fabricantes, tais diretrizes e recomendações foram criadas para evoluir e incorporar critérios técnicos adicionais, conforme as necessidades de segurança do mercado forem se transformando.

Os gastos com a segurança da IoT ganham um impulso

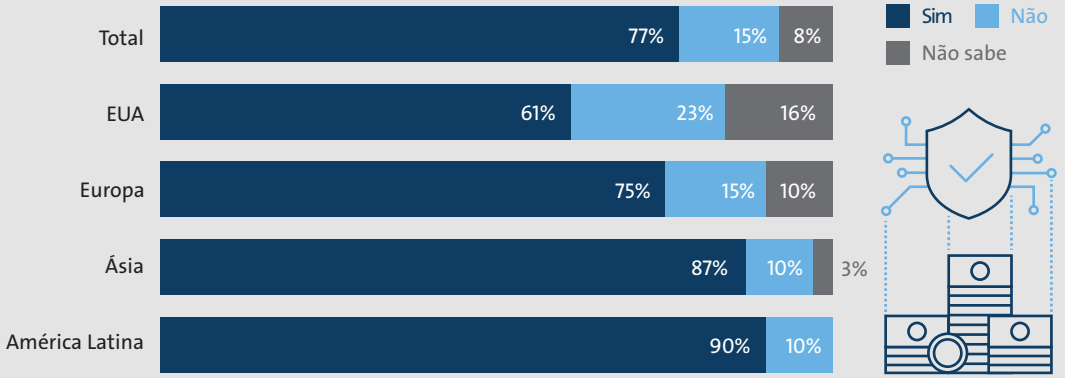
As empresas dos diversos setores estão percebendo rapidamente que a segurança da IoT não é algo que possa ser ignorado ou negligenciado. Cada novo dispositivo conectado representa outro obstáculo para as empresas, e basta um único dispositivo para corromper todo o ecossistema e destruir as operações comerciais.

Para capitalizar totalmente os imensos benefícios da IoT, as empresas precisam, primeiramente, criar uma base sólida de segurança. Investimentos estratégicos inteligentes na segurança da IoT terão um papel central nesta iniciativa.

Nossa pesquisa mostra que as empresas continuam investindo na segurança da IoT. De fato, a maioria das empresas (77%) planeja aumentar os gastos com segurança da IoT nos próximos cinco anos. A probabilidade de aumento dos gastos é notavelmente maior nos participantes da Ásia e América Latina, chegando a 87% e 90%, respectivamente.

Os aumentos nos gastos de planejamento da segurança cibernética são notavelmente maiores nos setores de saúde e varejo, 85% e 83%, respectivamente.

Porcentagem do planejamento de aumento dos gastos com a segurança cibernética da IoT nos próximos 5 anos.

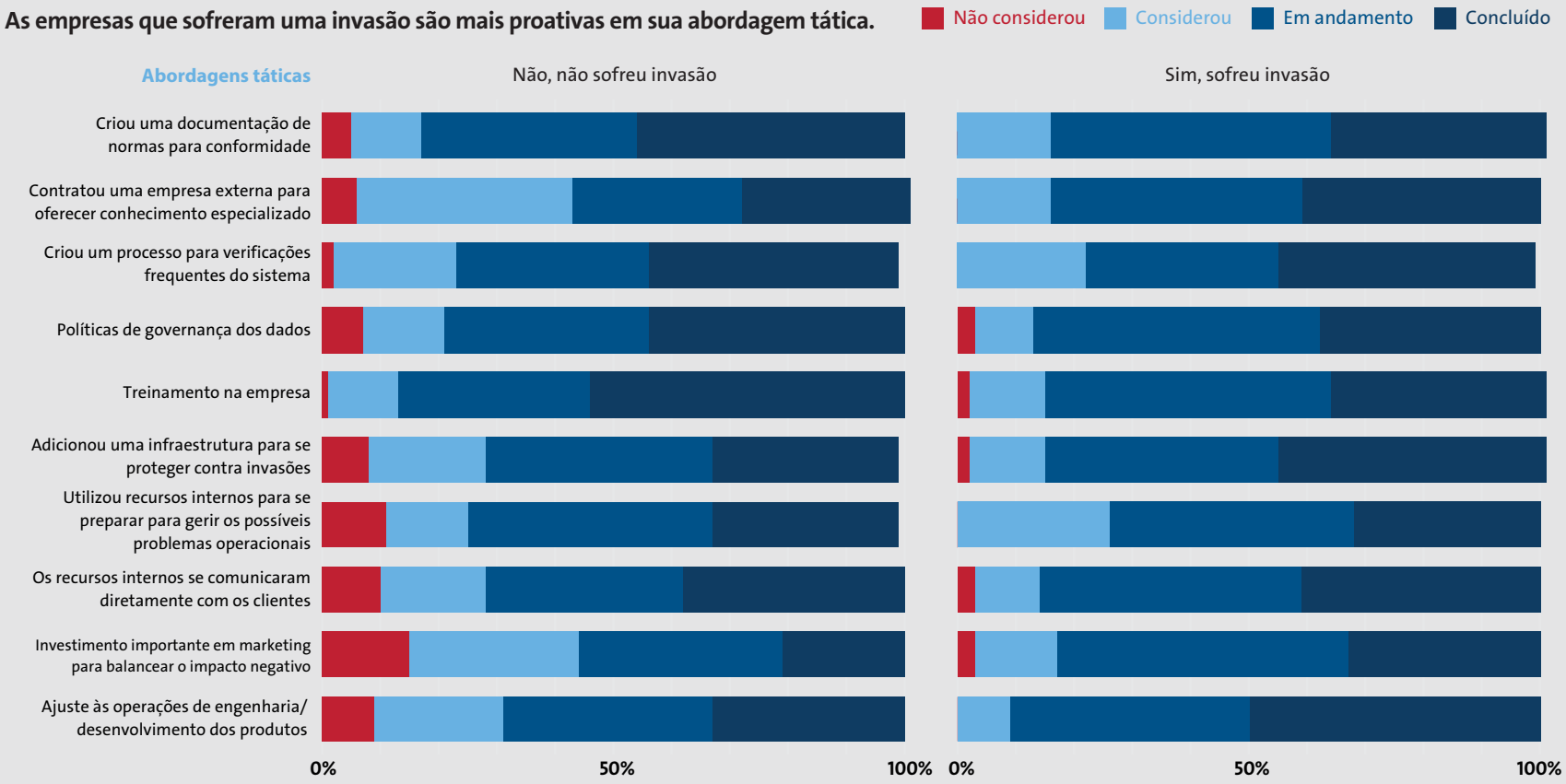


Incidentes que demandam ação

As empresas estão implementando uma gama de táticas para solucionar preocupações de segurança da IoT, com diferentes estratégias para quem sofreu ou não uma invasão. Para empresas que sofreram uma invasão, uma gama de táticas foram colocadas em andamento ou já concluídas.

O potencial das tecnologias da IoT se reflete nas projeções de receita e crescimento do mercado da IoT. De acordo com uma estimativa, o mercado global de IoT crescerá de US$ 157 bilhões em 2016 para **US$ 457 bilhões até 2020**, obtendo uma taxa de crescimento anual composta (CAGR) de 28,5%.[13]

As empresas que sofreram uma invasão são mais proativas em sua abordagem tática.

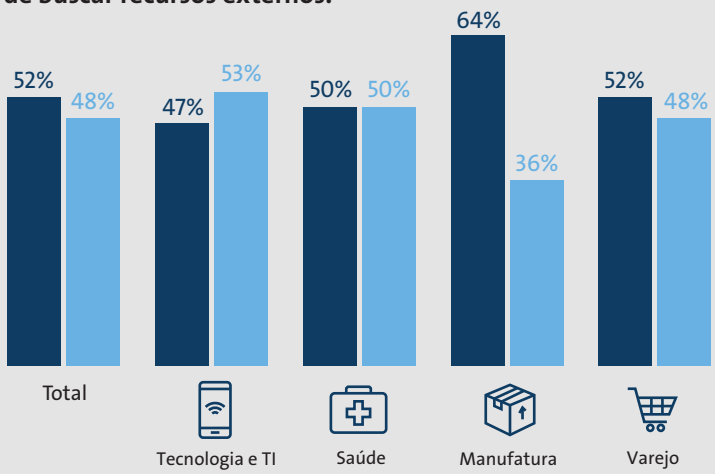


Quando se trata de implementar um novo plano de segurança da IoT, 52% das empresas planejam trabalhar com um especialista terceirizado. Este número foi particularmente elevado para os participantes do setor de produção (64%). As principais razões para a ponderação do auxílio de um especialista terceirizado foram: "gama mais ampla de conhecimentos" e "facilitação da conformidade regulatória".

Trabalhando com um terceiro especializado para implementar estratégias de segurança cibernética nas redes e produtos/serviços relacionados à IoT

Cumpre uma norma ou plano de desenvolvimento existente para as redes e produtos/serviços relacionados à IoT

As empresas do setor de produção têm maior probabilidade de buscar recursos externos.



89%

dos participantes planejam apresentar novos produtos ou serviços que solucionem riscos nos próximos 5 anos. 62% indicaram que estão planejando fazer isso no próximo ano.

19%

das empresas planejam investir mais de US$ 100 milhões nos próximos cinco anos para proteger produtos e serviços de IoT. 40% planeja investir de US$ 20 a 100 milhões.

52%

das empresas planejam trabalhar com um especialista terceirizado para implementar novos planos de segurança da IoT. As principais razões para a ponderação do auxílio de um especialista terceirizado foram: "gama mais ampla de conhecimentos" e "facilitação da conformidade regulatória".

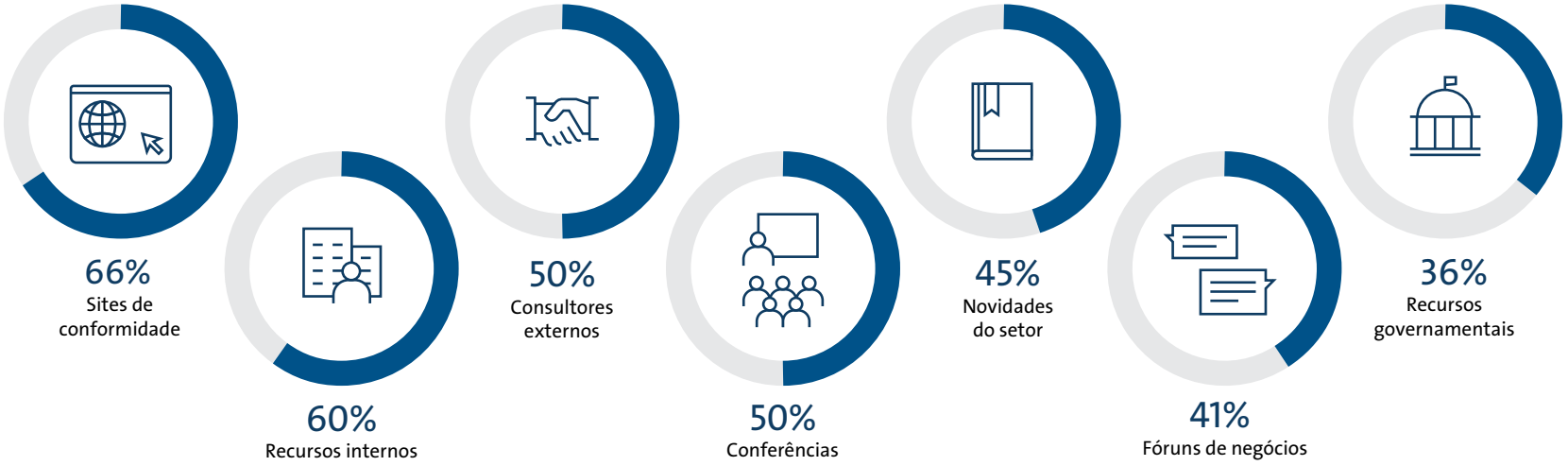
Busca de orientações sobre a conformidade regulatória

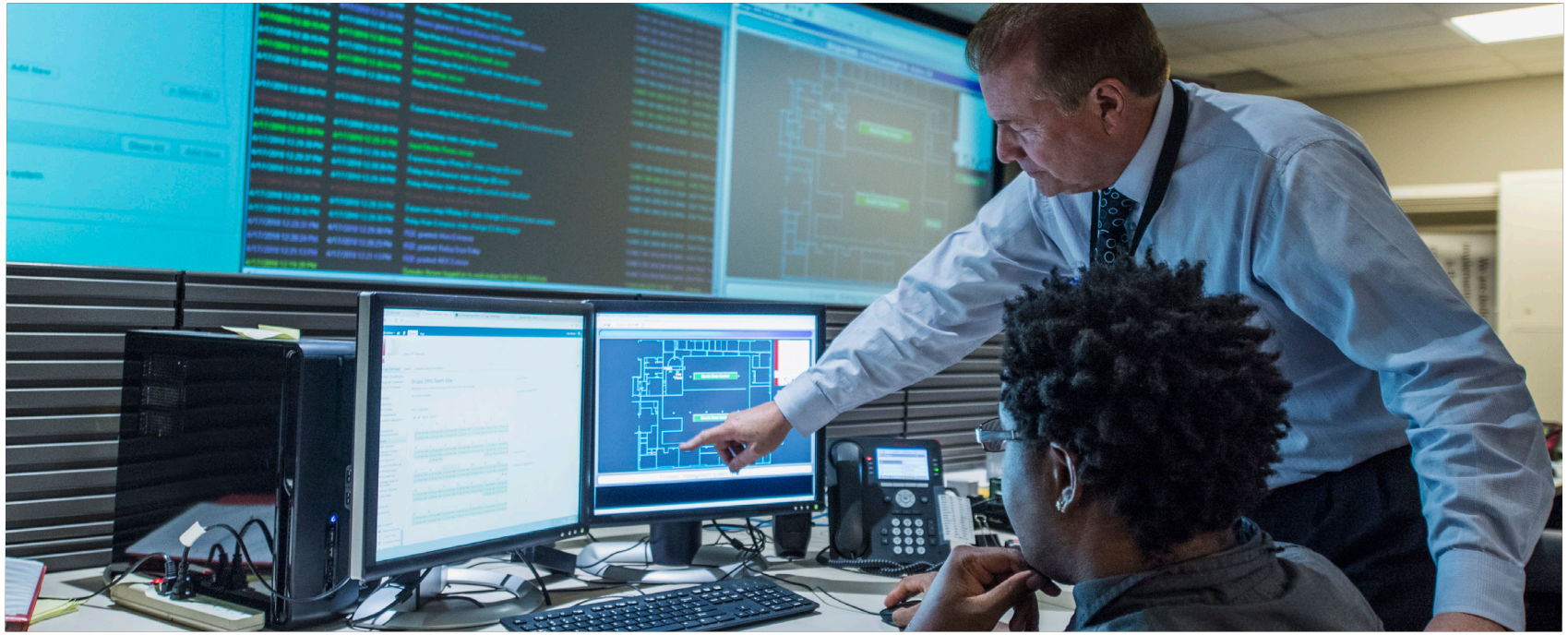
Para se manter informadas sobre o ambiente regulatório atual em plena transformação, as empresas dependem de uma combinação de recursos. Os sites de conformidade estão no topo da lista, seguidos dos recursos internos e do conhecimento externo.

Os recursos do governo foram citados pelos participantes como a ferramenta menos utilizada para suporte e orientação sobre conformidade. Embora as empresas planejem utilizar recursos do governo, a posição inferior no ranking enfatiza a tendência a priorizar as normas de conformidade do setor.

De acordo com a Gartner, os gastos com segurança da IoT atingirão **US$ 840 bilhões** até 2020[14]. Ao mesmo tempo, mais de 25% dos ataques identificados nas empresas terão relação com os sistemas de IoT, estimulando as empresas a aumentar ainda mais os orçamentos de segurança da IoT.

As empresas utilizam uma gama de ferramentas de monitoramento da conformidade. Recursos atualmente empregados para o treinamento de conformidade





Segurança eficaz: a base do sucesso da IoT

A IoT apresenta um mundo de oportunidades e desafios para as empresas de todos os setores. De um lado, ela oferece uma plataforma diversificada e personalizada para o engajamento dos clientes e a eficiência operacional. Do outro, muitos elementos são extremamente complexos, o que eleva o risco de afastar os clientes quando a segurança falhar. Encontrar o delicado equilíbrio entre a inovação e a proteção será o principal diferencial das marcas voltadas aos clientes nos próximos anos.

A segurança é essencial para a defesa e a operação responsável dos dispositivos da IoT. Na realidade, é a base fomentadora da IoT. Assim, é crucial que as empresas definam estratégias robustas de mitigação, que possam identificar ameaças de forma efetiva e frustrar os ataques conforme eles surgirem. Até que as proteções adequadas estejam em vigor, os dispositivos da IoT continuarão a sofrer o peso das vulnerabilidades.

Embora criar uma estrutura de segurança eficaz da IoT seja um processo a longo prazo, as empresas não podem hesitar. As táticas e estratégias estão sendo formuladas hoje, e as empresas de vanguarda já estão colocando seus planos em ação, para garantir que seus ecossistemas de IoT estejam preparados para adotar e auxiliar de forma eficaz o rápido aumento de "coisas" conectadas.

Sobre a UL

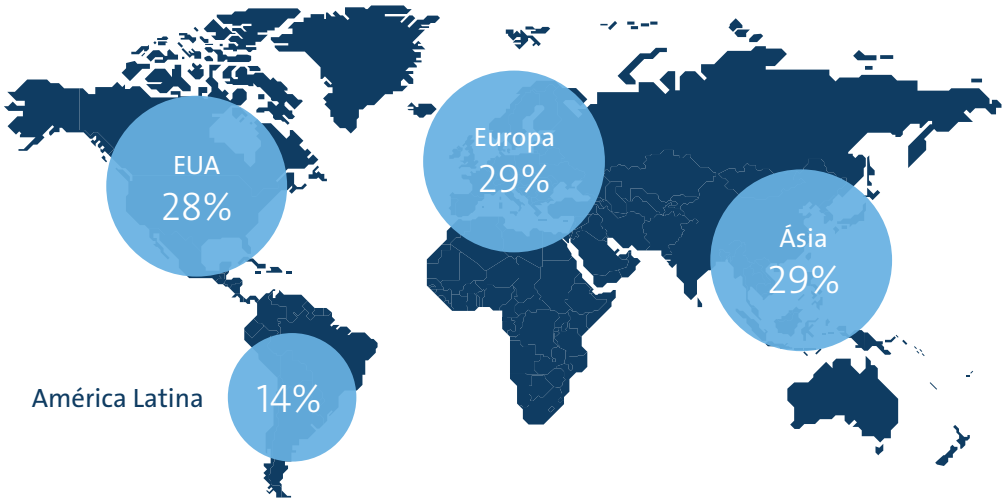
Em todo o mundo, a UL trabalha para ajudar consumidores, compradores e formuladores de políticas a navegar pelo risco e complexidade do mercado. A UL oferece uma segurança de ponta a ponta vital e confiável, criada para o nosso mundo interconectado. Possuímos um conhecimento ímpar no desenvolvimento de estruturas de segurança, criando programas de segurança para TI e ecossistemas interconectados. Nós possibilitamos que as empresas implementem inovações sem comprometer a segurança, ajudando-as a preservar a confiança dos clientes enquanto ampliam o acesso ao mercado.

Como colaboradora e parceira do setor de TI, a UL busca criar normas e políticas que ajudam a garantir a segurança a adoção segura de novas tecnologias conectadas. A UL está preparada para oferecer serviços, soluções e treinamento para ajudar as empresas a fortalecer as próprias marcas. Nós convidamos você a tomar proveito de nossos insights de ponta e especialistas de domínios, para posicionar a sua marca para um sucesso sustentável e de longo prazo.

Sobre o estudo

As descobertas deste relatório se baseiam em uma pesquisa com 349 participantes dos Estados Unidos, Europa, Ásia e América Latina. Os participantes da pesquisa são gerentes seniores, diretores, tomadores de decisões de IoT e pessoas em cargos mais elevados, responsáveis pela coordenação e gestão das iniciativas e práticas de segurança da IoT em suas respectivas empresas.

Detalhamento por país



Para mais informações, acesse UL.com/insights.

Fontes

1. "The Internet of Things: A movement, Not a Market," IHS Markit, out. 2017
2. "State of IoT Security," relatório de pesquisa, Gemalto, 2017
3. "Tales of Dirty Deeds and Unscrupulous Activities," Data Breach Investigations Report (DBIR) de 2018, Verizon, 2018
4. "Why Security Breaches Go Unnoticed for Months," 451 Research, junho de 2017
5. "DDoS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, 2016
6. "Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON," IT World, 2016
7. "WikiLeaks discloses details of CIA hacking IoT, mobile devices," Internet of Business, 2016
8. "Worldwide ransomware hack hits hospitals, phone companies," CNET, maio de 2017
9. "The frozen calm of normalcy bias," Gizmodo, recuperado, maio de 2017
10. "Second Cybersecurity Insights Report, Exploring IoT Security," AT&T, 2016
11. "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" — um relatório para o presidente, o secretário de Comércio e o secretário de Segurança Interna dos EUA, maio de 2018
12. "International Anti-Botnet Guide," o Council to Secure the Digital Economy (CSDE), 2018
13. "Market Pulse Report, Internet of Things (IoT)," GrowthEnabler, 2017
14. "Forecast: IoT Security, Worldwide," Gartner, 2016.

UL.com