Como determinar os níveis de garantia de segurança para seus produtos de IoT

Empowering Trust®

Resumo executivo

Há não muito tempo, poucas de nossas informações e sistemas eram digitalizados. Se pensarmos em 1989, a World Wide Web acabava de ser inventada, e nenhum usuário doméstico tinha acesso à Internet. Nossas fotos ainda eram tiradas em filmes fotográficos, e a fotografia digital não chegaria ao público até 1994, quando a Apple lançou a primeira câmera digital, e 2000, quando a Canon Ixus chegou ao mercado. Durante o início da década de 90, a maioria das pessoas não tinha celulares – e, os poucos que circulavam por aí, ficavam dentro de pastas devido ao seu grande tamanho.

O software malicioso na época, diante disso, consistia principalmente em projetos de pesquisa acadêmica e programas para irritar os outros, feitos só por diversão. Esse programa não era capaz de criptografar imagens da sua família e pedir dinheiro para devolvê-las, não capturava gravações de pessoas em suas próprias casas para chantageá-las, não controlava o aquecimento ou nossas fechaduras e não poderia recrutar os dispositivos que colocamos em nossas casas para serem usados como parte de um exército global capaz de derrubar o tráfego da Internet em todo o mundo.

Nada disso era possível, porque a maioria dos nossos dados e sistemas ainda eram basicamente analógicos. Em 1989, segurança e proteção eram basicamente sinônimos relacionados à segurança física.

Hoje, meros 30 anos depois, confiamos o controle de nossos dados, e às vezes até de nossas vidas, aos sistemas de computação ao nosso redor. A segurança física, e a proteção dos nossos dados, dinheiro e bens, sempre precisa levar em conta a segurança do software nos sistemas que controlam ou têm acesso a tais coisas.

E *tudo* possui software hoje em dia.

Esse conceito já foi entendido no contexto de sistemas de computador de uso geral há algum tempo, certamente desde meados dos anos 90, quando o uso da Internet cresceu significativamente com a World Wide Web. No entanto, agora estamos diante de um novo estágio da evolução para nossos sistemas conectados – os da IoT – que traz novas considerações e requisitos de segurança.

Este documento tratará da definição da IoT e por que sua segurança é um problema mais difícil de ser solucionado do que a segurança de dispositivos de computação de uso geral. Além disso, o white paper também explorará como a segurança de IoT pode ser melhor abordada ao entender os riscos envolvidos e usar classificações da segurança implementada em sistemas de IoT para pautar decisões de compras e determinar qual é a classificação certa para o seu produto.

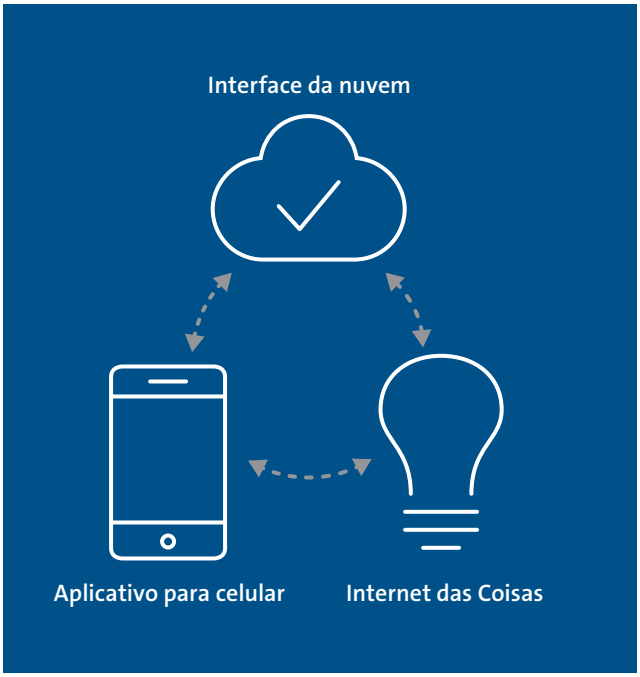
Definição da IoT

Embora o termo IoT signifique, literalmente, "Internet das Coisas" (do inglês, Internet of Things), é um pouco mais complexo definir claramente o que se enquadra ou não na definição de IoT. Muitos dispositivos inteligentes não se conectam diretamente à Internet – usando proxies ou hubs ou apenas conexões locais por Bluetooth ou ZigBees sem fio. A grande maioria dos sistemas de IoT conta com aplicativos de suporte ou serviços na nuvem que aumentam ou são basicamente essenciais para a operação do próprio aparelho.

Para fins deste documento, usaremos o termo IoT para nos referir a qualquer conjunto de funções que inclua no mínimo um componente físico que possa ser conectado por uma rede com ou sem fios. O escopo então inclui todos os componentes de um sistema: os componentes físicos, o software que está nos diversos elementos de computação e qualquer software de um aplicativo móvel ou instância da nuvem.

Dessa forma, incluímos na definição objetos como alto-falantes Bluetooth ou fechaduras inteligentes que não possuem conexão com a Internet. Essa é uma definição importante, já que a segurança de uma fechadura é claramente de grande importância, embora a de um alto-falante não ganhe tanto destaque.

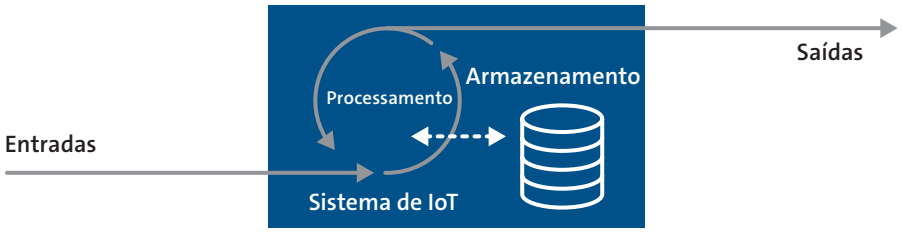
Por que consideramos a segurança desses dois objetos de modo diferente quando eles se conectam usando a mesma tecnologia sem fio? Que regras podemos usar para determinar as ameaças que se aplicam a qualquer tipo de dispositivo e quais dessas ameaças implicam nos níveis de segurança necessários para tal dispositivo?



Os riscos da IoT

Ao tratar da segurança necessária para qualquer sistema de IoT, é importante entender os riscos que esse sistema enfrenta, o que pode dar errado e por que uma pessoa maliciosa pode estar interessada em comprometê-lo. Basicamente, isso se limita a oportunidade e valor; quão facilmente um sistema pode ser acessado e qual valor essa pessoa maliciosa pode obter com tal acesso e/ou ataque (basicamente, qual é o alvo do ataque).

No nível mais fundamental, qualquer sistema de computação – inclusive a IoT – pode ser resumido em um sistema de entradas, saídas, armazenamento e processamento, como ilustrado abaixo:



Na maior parte do tempo, o foco se dá em entradas, nos dados do usuário, como o fator que define a razão pela qual um sistema de IoT pode ser atacado. No entanto, todos os aspectos (armazenamento, poder de processamento, largura de banda de saída e dados, funções de rede e local de um dispositivo) podem ser considerados ativos de valor inerente para um criminoso. Por exemplo: uma câmera na sua casa voltada para a rua pode ser considerada como tendo pouco valor em termos de dados. Mas essa mesma câmera pode ser atacada para se tornar parte de um botnet de escala nunca antes vista, usada por criminosos para saber quando você saiu de casa ou esconder a aproximação deles, atacar a privacidade de outras pessoas na sua rua ou atacada como o primeiro passo de um ataque múltiplo na rede como um todo.

A tabela abaixo contém exemplos de ativos que um sistema de IoT pode ter e que podem ser atacados por um criminoso, como eles podem ser atacados e por quais finalidades:

Ativo-alvo	Tipo de ataque	Exemplo de objetivo/finalidade de ataque
Dados armazenados ou acessados	Roubo de dados	Monetização/chantagem
	Modificação de dados	Ransomware
	Extração de dados ou código de todo o sistema	Engenharia reversa de código
Poder de processamento	Uso de recursos de processamento	Mineração de criptomoedas Quebra de senhas
Operação/ funções de sistema	Desativação de operação	Ransomware/chantagem
	Alteração de operação	Repetição de imagens de câmera de segurança
	Determinação de operação	Saber se as pessoas estão em casa
	Explorar operações privilegiadas	Abrir portas trancadas
Operação/ funções de rede	Uso de largura de banda	Ataque de DDoS
	Exploração de funções de rede confiável	Modificação de DNS
Local de rede	Acesso a outras redes ou sistemas	Atacar outros sistemas
	Capturar tráfego de rede	Roubar dados de outros sistemas

Devido a essa pluralidade de ameaças, infelizmente não é fácil dizer se um determinado tipo de dispositivo ou sistema de IoT tem qualquer valor para um criminoso. Esse valor costuma ser determinado pela maneira pela qual o sistema é implantado e usado, em vez do tipo de sistema em si.

Sob outra perspectiva: a segurança dos sistemas de IoT tem mais a ver com onde eles estão situados e os dados e recursos que ele possui do que o tipo de dispositivo que ele é. Esse "tipo" pode ajudar a definir os dados e recursos, mas não é o fator primário. Um alto-falante inteligente conectado diretamente à Internet e que oferece visões internas da casa, através de uma câmera integrada com grandes recursos de largura de banda e processamento, é um alvo mais atraente do que um alto-falante Bluetooth que simplesmente toca música de um telefone conectado.

O problema da segurança de IoT

Ao entender os vários aspectos da segurança de IoT – os tipos de ameaças e riscos envolvidos – fica clara a necessidade de tratar da segurança nesses sistemas. No entanto, isso também nem sempre é coisa simples. Os sistemas de IoT muitas vezes são um conjunto de diferentes elementos de processamento e diferentes códigos executados em locais distintos com segurança lógica e física diferentes. Se o “onde” é importante, ter vários locais pode tornar as coisas ainda mais complexas.

E a complexidade é inimiga da segurança.

Um problema fundamental com a segurança de IoT é que, embora a segurança muitas vezes não custe muito para ser bem implementada, ela não é gratuita. A boa segurança é uma função do bom design, o que implica em mais tempo e conhecimento nas fases iniciais de desenvolvimento do produto. Quanto mais complexo for o design, mais elementos e tipos de código envolvidos, mais difícil é integrar tudo em um sistema seguro.

A manutenção de sistemas complexos também é igualmente assustadora. Manter sistemas atualizados ao longo do tempo, com atualizações de segurança e patches, exige ter profissionais para tal: profissionais capazes de entender o que a segurança significa para os produtos criados hoje e capazes de acompanhar as novidades em pesquisa de segurança para saber também como a segurança será amanhã, mas que trabalhem em produtos após a receita inicial do mesmo tenha sido recebida. Quanto mais complexo for um sistema, mais difícil é acompanhar todas essas questões de segurança e mais pessoas exige.

Diante da demanda global por mão de obra com essa qualificação, esses profissionais valem ouro. Dessa forma, o bom design e a manutenção contínua possuem um custo tangível, como funções de mão de obra adicional e tempo necessários. De mesma importância, o teste real e a validação de recursos de segurança também têm custos. Testes de segurança "rápidos" podem ser realizados com custos menores, mas isso só proporciona um nível baixo de certificação para a propriedade de segurança que está sendo testada. Para ter maior garantia, você precisa realizar testes mais detalhados, o que leva mais tempo e custa mais caro. Esse custo se agrega ao custo de design e manutenção, que, no total, precisa reduzir as pequenas margens dos sistemas de IoT ou aumentar seu preço no ponto de compra.

Devido a isso, na sua origem, a segurança é, na verdade, principalmente um problema *comercial*.

Classificar a segurança da IoT

Como acomodamos esse custo de segurança? Se considerarmos que o custo de segurança pode ser uma porcentagem máxima do custo de um dispositivo (caso contrário, o consumidor buscará outras soluções), então precisa ser levado em conta que dispositivos de menor custo precisam gerenciar isso com níveis inferiores de segurança. Isso não quer dizer que não deve haver um nível básico aceitável de segurança para todo e qualquer dispositivo, mas que a determinação do nível aceitável pode ser uma função do tipo de dispositivo e implementação.

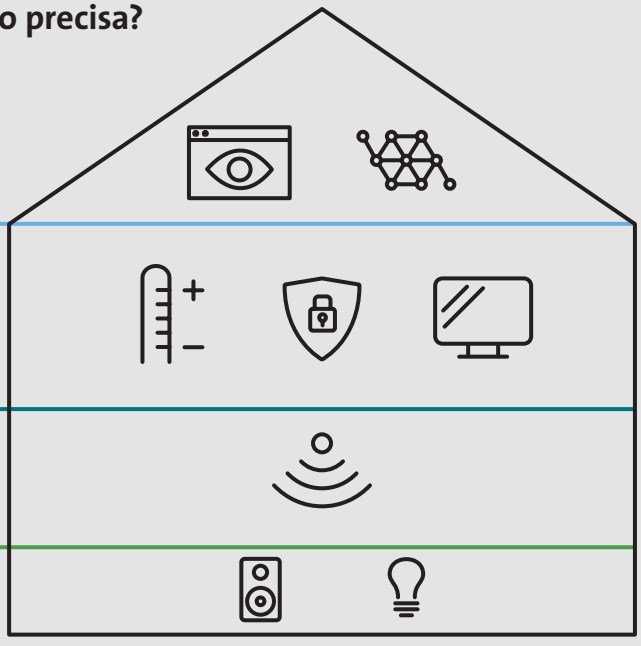
No entanto, a segurança também não pode ser pautada puramente por custos. Já demonstramos que a probabilidade de um ataque de um sistema é maior de onde ele está do que o seu tipo. Felizmente, com frequência (embora, *infelizmente*, nem sempre) há uma correlação entre a acessibilidade de um sistema e o custo para o consumidor. Por exemplo: lâmpadas inteligentes de IoT muitas vezes se conectam a uma rede sem fio curta, como um ZigBee, e dessa forma não podem ser acessadas pela Internet. Dessa forma, o risco apresentado por esses dispositivos é reduzido: eles não podem acessar a LAN diretamente e não podem ser acessados diretamente por criminosos pela Internet, não contêm dados sigilosos e possuem pouquíssimos recursos de largura de banda ou processamento.

Um criminoso pode conseguir usar uma lâmpada para ajudar a determinar se uma pessoa está em casa, de forma que a segurança ainda é importante para esses produtos, mas esses dispositivos costumam ser acessados ou agrupados em um hub, que oferece recursos adicionais de segurança. Por último, tudo isso é então conectado atrás de um roteador ou firewall que, felizmente, proporciona ainda mais defesas de segurança para a rede interna.

Dessa forma, lâmpadas podem não exigir um alto nível de certificação de segurança, mas os hubs aos quais elas se conectam precisam. Roteadores e firewalls precisam dos mais altos níveis de segurança, assim como outros dispositivos que podem possibilitar o acesso direto à Internet através do firewall apesar de outros recursos de segurança da rede.

Isso nos oferece uma visão em camadas da segurança exigida para sistemas em uma casa, escritório ou outro ambiente, com as camadas definidas pela acessibilidade e valor do próprio sistema. Esse tipo de configuração de camadas é ilustrado abaixo.

Qual a garantia de segurança que um dispositivo precisa?

	Exemplos de produtos	
Alta garantia Dispositivos diretamente acessíveis pela Internet Dispositivos de segurança ou perímetro da Internet	• Câmeras • Babás eletrônicas • Roteadores, modens • Hubs expostos à Internet	
Garantia alta a média Dispositivos com funções "inteligentes" relacionadas à segurança, que podem ou não estar conectados diretamente à Internet Dispositivos com acesso à Internet	• Aquecedores • Fechaduras • TVs • Alto-falantes controlados por voz	
Garantia média a baixa Dispositivos com conexão de redes para a LAN mas não diretamente para a Internet	• Hubs locais • Pontes • Pontos de acesso	
Baixa garantia Dispositivos não conectados diretamente à LAN	• Alto-falantes Bluetooth • Lâmpadas inteligentes (sem Wi-Fi)	

Sistemas menos acessíveis, e com menos dados e recursos valiosos, podem basicamente atender a um nível menor de segurança – e um nível inferior de garantia de segurança – do que aqueles nas partes periféricas da rede, que precisam de uma classificação mais alta. É claro que esses níveis aceitáveis de segurança dependem em grande parte de como os sistemas de IoT são implantados e usados, o que costuma ser difícil de determinar por um fabricante antes da venda. Um cliente pode acabar decidindo usar lâmpadas com Wi-Fi e conectá-las diretamente à Internet, o que aumentará o risco e, por isso, exigirá níveis maiores de segurança.

No entanto, há algumas questões gerais que podem ser feitas para ajudar a determinar os riscos apresentados por um sistema, e, dessa forma, o nível de segurança que é necessário. Eles são fornecidos na tabela à direita, mostrando as recomendações para altos níveis de garantia até os níveis mais baixos. O item superior válido para qualquer sistema é o nível pretendido. Por exemplo, pense em uma fechadura Bluetooth. Talvez ela só seja acessível por conexões de roteador não ligadas à Internet (que é recomendado para um baixo nível de garantia), mas, já que oferece segurança física e funções relacionadas, um nível maior de certificação é então adequado.

Usando esta tabela, fabricantes e fornecedores podem determinar com facilidade qual é o nível mínimo de certificação para seus produtos. Isso não significa que níveis superiores não são uma boa ideia. Níveis superiores sempre são melhores, e podem ajudar com a diferenciação de produtos no mercado. Essa tabela é fornecida apenas como uma orientação inicial, a fim de ajudar a determinar o nível mínimo que pode ser adequado.

Também é esperado que essas recomendações mudem ao longo do tempo, ou que os requisitos e a certificação em cada nível passem por alterações, conforme a maturidade geral da segurança do cenário de IoT evolua. Isso seria similar a como a norma de segurança veicular do Programa de Avaliação de Novos Veículos da Australásia (ANCAP) incluiu itens adicionais de segurança ao longo do tempo, conforme a segurança dos automóveis evoluiu.

Agora que temos diretrizes sobre quais níveis podem ser adequados, também contamos com uma maneira de ilustrar para o comprador do sistema de IoT que nível de segurança um sistema de fato atingiu, como isso foi avaliado e o que implica para a implantação esperada do sistema. Isso permite que o usuário selecione um sistema que pode ser mais caro, mas com classificação superior de segurança, se planejar implantá-lo de forma que implique em mais riscos,

Pergunta de definição de escopo do sistema	Nível de garantia de segurança mínima recomendada
O sistema implementa funções de segurança ou relacionadas, como controle de climatização, rede ou segurança física?	Alta
O sistema exige, ou pode ser configurado para ter, uma conexão direta com a Internet?	Alta
O sistema tem acesso a dados sigilosos, como gravações de áudio ou vídeo, detalhes de pagamento etc.?	Média a alta
O sistema (mesmo no caso de um hub que se conecta a outros sistemas) possibilita a conexão direta à Internet (saída de conexão, em vez de entrada como no caso acima)?	Média a alta
O sistema atua como um hub ou ponte entre diferentes redes para a LAN do cliente e não oferece acesso direto à Internet?	Média a baixa
O sistema só pode ser acessado por redes não roteáveis para a Internet e de baixa largura de banda, como ZigBee ou áudio Bluetooth?	Baixa

como conectá-lo à Internet, usá-lo para armazenamento ou processamento de dados sigilosos ou mesmo conectá-lo a outros sistemas de alto valor.

Elevar a segurança básica e deixar a cargo do clientes as opções de segurança de acordo com as suas necessidades é tarefa para os sistemas de classificação de segurança.

A jornada de segurança

Outro ponto positivo de classificar a segurança dos sistemas, em vez de fornecer uma saída binária segura/insegura, é que ajuda a incentivar o investimento e crescimento em segurança de IoT. Não é realista esperar que todos os produtos lançados amanhã automaticamente atendam aos mais altos padrões de segurança definidos. Na verdade, é provável que atender aos mais altos níveis de segurança só seja possível com um novo design completo, ou com mudanças culturais extensas em como os produtos são projetados, construídos, enviados e mantidos.

Isso apresenta um dilema para um programa de segurança de aprovação/reprodução. Reduzimos o nível dos requisitos para o patamar mínimo alcançável pela maioria dos produtos de hoje, com a consciência de que esse não é o nível final que realmente queremos alcançar, ou elevamos os padrões para onde acreditamos que devam estar e simplesmente esperamos a indústria se adequar?

Se o padrão estiver muito baixo, podemos no mínimo obter validação de requisitos mínimos, mas não haveria incentivo ou reconhecimento para as empresas ultrapassarem esses requisitos para demonstrarem sua consideração pelos clientes. Se o patamar estiver muito alto, podemos garantir que os produtos que atendam esses requisitos estejam bastante seguros, mas não é útil se nada puder atender a esse nível e toda a indústria fica desestimulada.

Qualquer solução falha em fornecer informações úteis para consumidores sobre como produtos diferentes aplicaram e implementaram suas práticas de segurança.

Abordar a segurança da IoT através de classificações – Uma solução comercial

Impulsionar um nível elevado de maturidade de segurança em sistemas de IoT exige a compreensão de ambos aspectos comerciais por trás do design e implantação da IoT, além dos riscos que pautam o nível de certificação que é necessária para diferentes tipos e usos de produto. O risco é uma função de diversos fatores diferentes: que dados o sistema pode acessar, quanta largura de banda e poder de processamento ele tem, a que outros sistemas ele tem acesso ou controle, e quão facilmente esses sistemas de IoT podem ser acessados e atacados.

O ideal é que a segurança de IoT possa ser encarada de forma objetiva como binário seguro/não seguro, mas isso simplesmente não é possível e não proporciona uma representação justa dos esforços empregados pela indústria. Alcançar os mais altos níveis de segurança não acontece por acidente, e tanto o design de produtos seguros quanto os testes de segurança exigem tempo e dinheiro. Isso tem impactos sobre a viabilidade comercial dos produtos, potencialmente reduzindo a capacidade de investir na proteção da próxima geração de dispositivos.

Com legislação a caminho que obriga certos requisitos mínimos para a segurança de IoT, e diversos órgãos de indústria já traçando seus próprios conjuntos de requisitos de segurança de IoT, quais são as melhores formas de alcançar a conformidade, competir no mercado e ainda manter uma linha de produtos comercialmente viável?

Para responder a essa pergunta, não podemos esperar os mais altos níveis de segurança para todos os sistemas desde o início. Essa simplesmente não é uma postura comercialmente viável. Em vez disso, precisamos adotar uma abordagem gradual para a segurança de IoT e impulsionar uma base mínima de segurança para todos os dispositivos, com proteção cada vez maior para sistemas suscetíveis a maiores riscos.

Ao longo do tempo, conforme a compreensão do mercado sobre necessidade e design de segurança evolua, os níveis e sistemas aos quais são aplicados podem ser elevados. Essa consciência ajudará a aumentar a pressão comercial por sistemas seguros. No momento, os clientes já desistiram da segurança da IoT de vez ou simplesmente esperam que ela seja parte do produto, sem qualquer entendimento real se está presente ou não. Para solucionar esse problema, precisamos tornar a segurança mais visível para o consumidor. Mas, sem níveis, tudo que nos resta é aceitar os padrões mais baixos que podem ser normalmente alcançados ou evitar a adoção de normas de segurança que exigem uma mudança rápida demais na postura de segurança.

Elevar a segurança precisa envolver trabalhar com a indústria em vez de contra a indústria. Precisamos apresentar soluções em vez de simplesmente catalogar os problemas e garantir que os aspectos comerciais da segurança sejam abordados. Para isso, precisamos ser capazes de demonstrar facilmente aos consumidores que produtos investiram mais tempo e esforço na segurança – e isso só pode ser feito através de uma metodologia de classificação.

Qual classificação é a correta para você ou seus produtos? Para responder a essa pergunta, você precisa entender o seu mercado, saber quem são seus clientes e como sua tecnologia é usada. A abordagem de camadas apresentada neste documento, usando informações de acesso e ativos, oferece uma forma rápida de determinar isso.

Para saber mais, fale com a UL através do e-mail IMSecurity@ul.com ou acesse IMS.UL.com/IoT-Security-Rating.

Segurança Cibernética UL

A Classificação de Segurança de IoT da UL entra para uma lista crescente de soluções de segurança de IoT da UL, incluindo o Nível de Confiança Cibernética de Fornecedores da UL, Programa de Certificação de Segurança Cibernética da UL, IEC 62443 e outros serviços de treinamento e orientação que abordam avaliações de segurança em ecossistemas, segurança e qualidade de cadeia de suprimentos e mercados regulados para segurança.

Sobre a UL

A UL ajuda a criar um mundo melhor aplicando a ciência para solucionar desafios de segurança, proteção e sustentabilidade. Geramos confiança, possibilitando a adoção segura de produtos e tecnologias novos e inovadores. Todos na UL compartilham a paixão por fazer do mundo um lugar mais seguro. Todo o nosso trabalho, desde a pesquisa independente e o desenvolvimento de normas, testes e certificação até soluções analíticas e digitais, ajuda a melhorar o bem-estar global. Empresas, indústrias, governos, autoridades regulatórias e o público confiam em nós, para que possam tomar decisões mais inteligentes.

Para saber mais, acesse UL.com.

UL.com