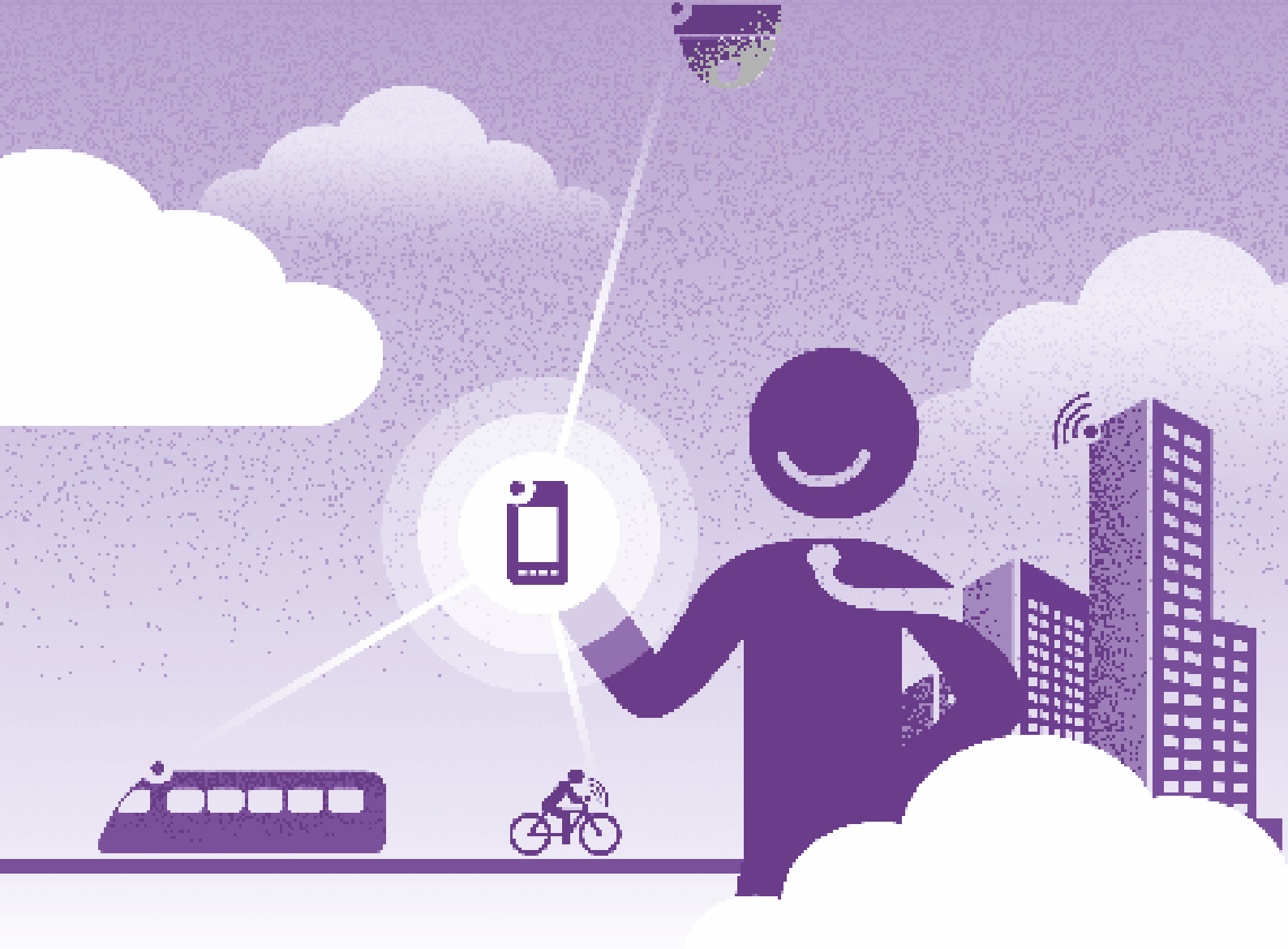


A Internet das Coisas (IoT) nas Empresas

Crie uma base segura para aproveitar as oportunidades de negócios da IoT

Resumo da Solução
IoT para Empresas

Alcatel·Lucent
Enterprise

A IoT fundamentalmente muda a equação dos negócios

A Internet das Coisas (IoT) tem o potencial de transformar os negócios, alterando profundamente a forma como as organizações coletam dados e informações, unindo as grandes tendências tecnológicas e comerciais para mobilidade, automação e análise de dados. A IoT refere-se à rede de objetos físicos interligados por meio de sensores integrados, atuadores e outros dispositivos que podem coletar e transmitir informações sobre as atividades na rede, em tempo real. Os dados acumulados por esses dispositívos podem ser analisados pela organização, a fim de:

- **Otimizar produtos e processos,** reduzindo os custos operacionais, aumentando a produtividade e desenvolvendo novos produtos e serviços.
- **Conhecer mais sobre as necessidades e preferências dos clientes**, permitindo que as empresas ofereçam mais produtos e serviços personalizados.
- **Tornar as empresas mais inteligentes e eficientes**, monitorando a infraestrutura de forma proativa e criando processos mais efetivos.
- **Melhorar as experiências do usuário**, oferecendo novos produtos e serviços para diferenciar-se da concorrência como uma empresa que se baseia em dados.

Cenários de IoT nos principais Setores

As soluções de IoT prometem tornar as empresas mais inteligentes e bem-sucedidas no que fazem. Esses benefícios são especialmente notados em determinados setores:

- **Saúde** – A IoT tem o potencial de redefinir como as pessoas, a tecnologia e os dispositivos interagem e se conectam uns com os outros em ambientes da área médica, ajudando a oferecer um melhor tratamento, reduzir custos e melhorar os resultados.
- **Educação** – A IoT está mudando as experiências de ensino e aprendizado com as salas de aula conectadas, e melhorando a forma como as escolas e os campus podem monitorar as operações e a segurança para a educação primária e secundária.
- **Hospitalidade** – As soluções de IoT oferecem oportunidades ao setor de hotelaria para servir melhor seus clientes, aumentando a eficiência das operações e fornecendo serviços diferenciados.
- **Governo** – A IoT fornece às agências governamentais a oportunidade de oferecer serviços de melhor qualidade, simplificar processos, cortar custos e encontrar formas inovadoras de agregar mais valor para os cidadãos.
- **Transportes** – A IoT está no núcleo das forças que remodelam os transportes, proporcionando maior segurança, mais eficiência na viagem, melhor manutenção de veículos e aeronaves e gerenciamento de tráfego estratégico.

Desafios na implantação da IoT

A IoT traz fluxos de dados sem precedentes, apresentando desafios de desempenho, operacionais e de gerenciamento para a infraestrutura da rede, junto com maiores riscos de segurança em todos os terminais. Para solucionar esses problemas, as empresas precisam adaptar seus projetos de rede tradicionais para fornecer novos níveis de inteligência, automação e segurança.

As empresas precisam de uma infraestrutura de rede com o melhor custo-benefício, que possa tratar com segurança o grande fluxo de dados, mas que também seja simples de gerenciar e operar. A infraestrutura deve:

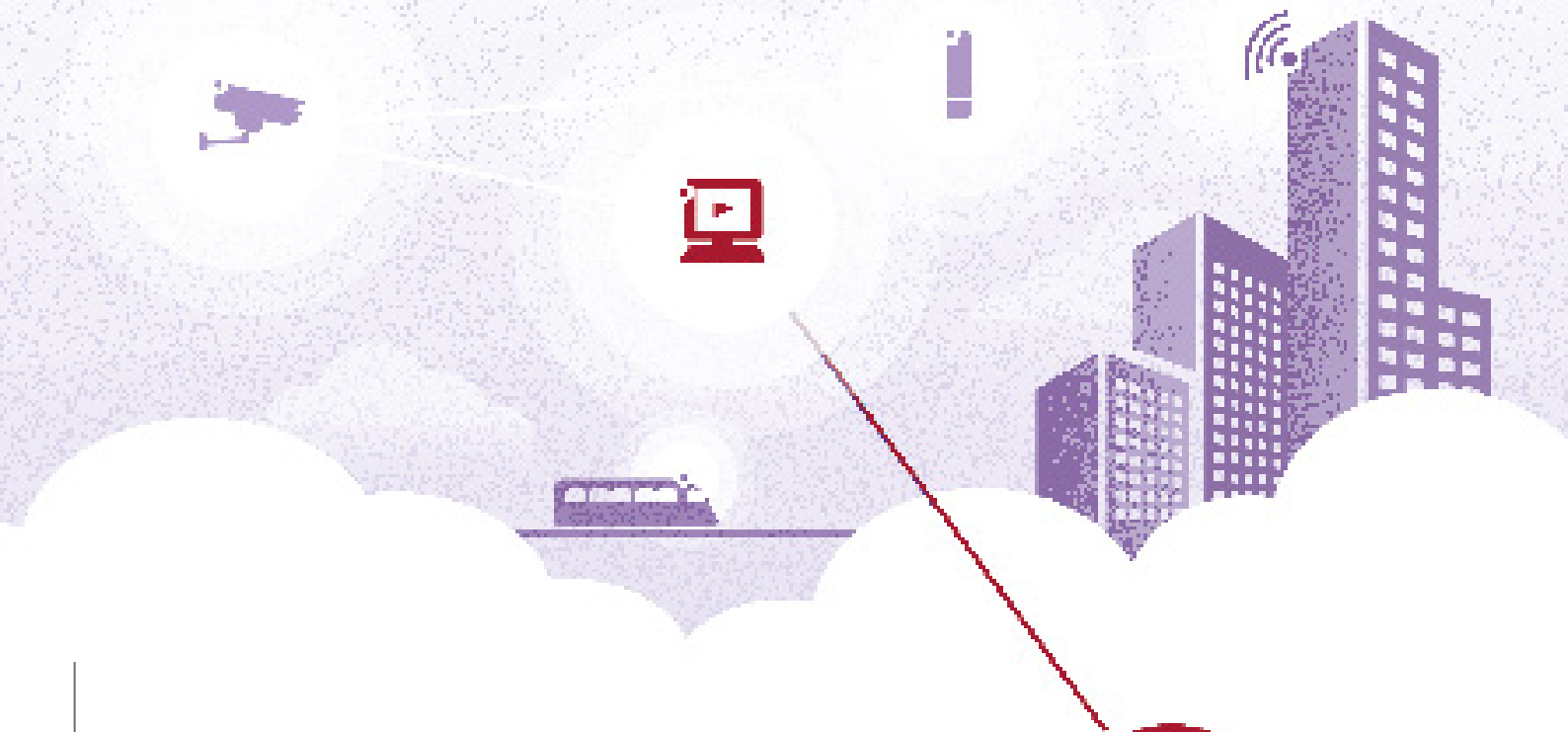
- **Utilizar um processo simples e automatizado para a integração de dispositivos IoT.** Grandes sistemas IoT podem conter milhares de dispositivos e sensores, portanto adicionar e gerenciar manualmente todos esses terminais é complexo e propenso a erros. A integração automatizada permite que a infraestrutura de rede reconheça dinamicamente os dispositivos e os atribua para a rede de segurança correta.
- **Fornecer os recursos de rede apropriados para que o sistema de IoT funcione de forma adequada e eficiente.** Muitos dispositivos no sistema de IoT utilizam informações essenciais, que exigem um nível específico de QoS. Por exemplo, alguns aplicativos requerem uma determinada largura de banda, em uma infraestrutura de rede de alto desempenho, para garantir a confiabilidade e o fornecimento do serviço.
- **Fornecer um ambiente seguro contra ataques cibernéticos e perda de dados.** Os inúmeros dispositivos e sensores conectados na rede IoT levam a uma abundância de possíveis vetores de ataque, e por isso a segurança é fundamental para reduzir os riscos de crimes cibernéticos. A segurança é necessária em vários níveis, incluindo a contenção das próprias redes IoT.

Os profissionais de TI estão fazendo planos para mais IoT

Profissionais de TI de vários setores já estão planejando o aumento no uso de soluções de IoT, em um futuro próximo. De acordo com a pesquisa da 451 Research de 2017, Tendências na Internet das Coisas, 67% dos profissionais de TI pesquisados disseram que suas empresas já implantaram uma solução de IoT ou tinham um sistema IoT em piloto. 21% dos entrevistados disseram que suas empresas planejavam implantar soluções de IoT dentro de 12 meses, e 11% dizem que suas empresas planejam implementar IoT em mais de um ano.

A IoT contribui para a exposição da Empresa aos crimes cibernéticos

O crescimento da IoT também traz uma explosão de ameaças à segurança cibernética, pois a proliferação de sensores e dispositivos conectados expande muito a superfície de ataque da rede. A IoT no ambiente corporativo é especialmente sensível, porque muitos dispositivos IoT são fabricados sem ter a segurança em mente, ou são criados por empresas que não entendem os requisitos de segurança atuais. Consequentemente, cada vez mais, os sistemas de IoT representam o elo mais fraco na segurança da rede corporativa.



- O ataque DDoS (Distributed Denial of Service) na Dyn em Outubro de 2016 que derrubou grande parte da internet, foi realizado por meio de dispositivos de rede invadidos, como câmeras de vigilância e gravadores digitais de vídeo.[1]
- Hackers atacaram a rede do sistema públlico de trânsito de São Francisco, Muni, em Novembro de 2016, tornando inoperáveis as máquinas de bilhetes e outras infraestruturas de computação, como parte de um esquema de ransomware.[2]

O sistema de chaves eletrônicas do Romantik Seehotel Jaegerwirt, na Áustria, foi invadido em janeiro de 2017 deixando os hóspedes trancados para fora de seus quartos. O hotel permaneceu impedido de acessar seu próprio sistema de computadores até pagar os dois resgates em Bitcoins.[3]

Criando uma infraestrutura de rede IoT segura

Proteger o tráfego e os dispositivos IoT é um desafio que não pode ser resolvido por qualquer tecnologia de segurança. Exige uma abordagem estratégica que tira proveito de várias medidas de segurança.

Para ajudar sua empresa a aproveitar os benefícios e reduzir os riscos da implantação de IoT, a Alcatel-Lucent Enterprise (ALE) oferece uma estratégia de segurança em vários níveis. A estratégia da ALE fornece proteção em cada camada da infraestrutura, a partir de cada usuário e dispositivo individual até a própria infraestrutura da rede. Ela também fornece uma estratégia de contenção de IoT para simplificar e proteger a integração de dispositivos, e oferece os recursos de rede apropriados para que o sistema funcione de forma correta e eficiente, tudo em um ambiente seguro para garantir a proteção das organizações contra ataques cibernéticos.

IoT containment

Para habilitar o IoT Containment, todos os usuários, dispositivos e aplicativos dentro da rede da ALE são associados a perfis. Esses perfis, que definem funções, autorizações de acesso, níveis de QoS e outras informações sobre políticas, são transmitidos a todos os switches e pontos de acesso na rede.

- Os dispositivos são atribuídos a "recipientes (containers) virtuais" usando técnicas de virtualização de rede, permitindo que vários dispositivos e redes usem a mesma infraestrutura física, enquanto permanecem isolados do resto da rede.
- Nesses "recipientes virtuais", as regras de QoS e segurança são aplicadas.
- Com a divisão da rede em "containers" virtuais, caso ocorra alguma violação em uma parte da rede virtual, isso não afetará outros dispositivos ou aplicativos em outras redes virtuais.
- Quando um novo dispositivo IoT estiver conectado, a rede reconhecerá automaticamente seu perfil e atribuirá o dispositivo ao ambiente virtual adequado.
- A comunicação é limitada aos dispositivos dentro desse ambiente virtual, e aos aplicativos do datacenter que controlam esses dispositivos.
- Como todos os usuários têm perfis dentro da rede da ALE, o acesso aos "containers" virtuais de IoT pode ser limitado a indivíduos e grupos autorizados.

Segurança aprofundada

Além do IoT Containment, as tecnologias de rede da ALE fornecem a segurança por camada, nos vários níveis da rede.

- No nível do usuário, os perfis garantem que os usuários sejam autenticados e autorizados com os direitos de acesso adequados.
- No nível do dispositivo, a rede assegura que os dispositivos sejam autenticados e estejam de acordo com as regras de segurança estabelecidas.
- No nível do aplicativo, a rede pode estabelecer regras sobre cada aplicativo ou grupo de aplicativos, incluindo bloqueio, limitação de largura de banda e controle de quem pode acessar quais aplicativos.
- No nível da rede, os switches da ALE utilizam o secure diversified code. Ele protege redes contra vulnerabilidades intrínsecas, quebras de código, malwares infiltrados e possíveis backdoors que poderiam comprometer os switches, roteadores e outros hardwares essenciais.
- A função "smart analytics" da ALE usa inspeção profunda de pacotes e outras tecnologias para detectar os tipos de dados e aplicativos se movimentando pela rede, tornando possível identificar padrões incomuns de tráfego e atividades não autorizadas.

Gerenciamento e operação da rede, de ponta a ponta

As soluções de rede da ALE também oferecem às corporações vantagens significativas para operação e gerenciamento.

- A ALE permite que várias redes distintas operem em uma única infraestrutura comum, eliminando a necessidade de mais investimento CAPEX em múltiplas redes físicas.
- A estrutura de Acesso Unificado da ALE permite que as tecnologias com fio e sem fio trabalhem juntas, como uma rede única e robusta, com serviços de rede, regras de políticas, um esquema de autenticação em comum, e uma única base de dados de autenticação.
- As soluções de rede da ALE também têm um único sistema de gerenciamento para todos os elementos da infraestrutura, incluindo gerenciamento unificado das redes LAN com fio e sem fio. O gerenciamento Alcatel-Lucent OmniVista® 2500 oferece um painel de controle unificado para gerenciar ambientes virtuais, switches, Access Points e todos os outros componentes da rede.»

Um portfólio de rede de alto desempenho

Os switches, Access Points e controladoras da ALE suportam a última geração de recursos de alta largura de banda e baixa latência, e podem gerenciar um grande número de dispositivos em ambientes de alta densidade. Os produtos e soluções de rede da ALE atendem às necessidades de rede das empresas de todos os tamanhos. A ALE também oferece uma seleção de switches robustos, Access Points e roteadores para implantações externas ou em condições adversas.

Redes e estratégias IoT seguras. Aqui, e agora

Os produtos e soluções da ALE criam a base para uma rede segura, que ajuda as organizações a implantarem sistemas de IoT que podem revelar informações para otimizar produtos e processos, tornar os negócios mais inteligentes e eficientes, e fornecer melhores experiências para seus clientes. As estratégias de IoT Containment e segurança por camada, da ALE, reduzem os riscos e simplificam a configuração das redes de IoT ao facilitar a integração dos dispositivos, com operações mais eficientes e mais segurança. A ALE ajuda as instituições a utilizarem todos os possíveis benefícios da IoT, com melhores níveis de inteligência, automação e segurança da rede.

Quer saber mais?

Para obter mais informações sobre as soluções de IoT da ALE, vá para ALE IoT Security.

Somos a ALE.

Fazemos com que tudo se conecte, fornecendo uma tecnologia que funciona, para você. Com nosso alcance global e foco local, oferecemos redes e comunicações. Localmente. De forma híbrida. Na nuvem.

1 Hacked Cameras Were Behind Friday's Massive Web Outage
2 Metro transport systems eyed after hack attack in San Francisco
3 Hackers Use New Tactic at Austrian Hotel: Locking the Doors

00303777-ptbr (dezembro de 2019)