A Internet das Coisas nas Empresas

Construir uma base segura para aproveitar as oportunidades de negócios com IoT.

Resumo da Solução

Alcatel·Lucent Enterprise

IoT muda fundamentalmente 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, reunindo as principais tendências técnicas e de negócios de mobilidade, automação e análise de dados. IoT refere-se à rede de objetos físicos usando sensores incorporados, atuadores e outros dispositivos que podem coletar e transmitir informações sobre a atividade da rede em tempo real. Os dados acumulados desses dispositivos podem ser analisados pela organização para:

- **Otimizar produtos e processos,** reduzindo custos operacionais, aumentando a produtividade e desenvolvendo novos produtos e serviços
- **Saiba mais sobre as necessidades e preferências dos clientes,** permitindo que as empresas ofereçam produtos e serviços mais personalizados
- **Torne os negócios mais inteligentes e eficientes,** monitorando proativamente a infraestrutura crítica e criando processos mais eficientes
- **Melhore as experiências do usuário,** oferecendo produtos e serviços novos ou aprimorados, para diferenciar seu negócio da concorrência

A implantação de IoT continua crescendo

Profissionais de TI em vários setores já estão planejando aumentar o uso de soluções de IoT em um futuro próximo. Em 2022, o mercado de Internet das Coisas deverá crescer 18%, para 14,4 bilhões de conexões ativas. Espera-se que, até 2025, à medida que as restrições de fornecimento diminuam e o crescimento acelere ainda mais, haverá aproximadamente 27 bilhões de dispositivos IoT conectados.

Fonte: https://iot-analytics.com/number-connected-iot-devices

Desafios da implantação da IoT

A IoT traz fluxos de dados sem precedentes, apresentando desafios de desempenho, operacionais e de gerenciamento para a infraestrutura de rede, juntamente com maiores riscos de segurança em todos os endpoints. Para resolver esses problemas, as organizações precisam adaptar os designs de rede tradicionais para fornecer novos níveis de inteligência, automação e segurança de rede.

As organizações precisam de uma infraestrutura de rede econômica que possa lidar com grandes fluxos de dados de forma segura, mas que também seja simples de gerenciar e operar. A infraestrutura deve:

- **Oferecer um processo simples e automatizado para a integração de dispositivos IoT.** Grandes sistemas de IoT podem conter milhares de dispositivos ou sensores, e o provisionamento e gerenciamento manual de todos esses endpoints é complexo e propenso a erros. A integração automatizada permite que a infraestrutura de rede reconheça dispositivos dinamicamente e os atribua à rede segura apropriada.
- **Fornecer os recursos de rede corretos para que o sistema IoT funcione de maneira adequada e eficiente.** Muitos dispositivos no sistema IoT fornecem informações de missão crítica que requerem um nível específico de QoS. Por exemplo, alguns casos de uso exigem reservas de largura de banda adequadas em uma infraestrutura de rede de alto desempenho para garantir a entrega e a confiabilidade do serviço.
- **Fornecer um ambiente seguro contra ataques cibernéticos e perda de dados.** Como os muitos dispositivos e sensores em rede na IoT levam a uma abundância de possíveis vetores de ataque, a segurança é fundamental para mitigar os riscos de crimes cibernéticos. A segurança é necessária em vários níveis, incluindo a segmentação das próprias redes IoT.

IoT aumenta a exposição ao crime cibernético

Com o crescimento da IoT também vem uma explosão de ameaças à segurança cibernética, pois a proliferação de sensores e dispositivos conectados expandem muito a superfície de ataque da rede. A IoT é especialmente suscetível porque muitos dispositivos IoT são fabricados sem considerar a segurança ou construídos por empresas que não entendem os requisitos de segurança atuais. Consequentemente, os sistemas IoT são cada vez mais o elo mais fraco na segurança corporativa.

O analista da Forrester, Steve Turner, disse que sua própria pesquisa sugere uma distribuição relativamente uniforme de ataques de resgate em verticais. Entretanto, incidentes de ransomware em determinados setores, como infraestrutura crítica e assistência médica, tendem a resultar em mais manchetes.[1]

Os dispositivos IoT apresentam riscos aos ativos em toda a rede. Ao estabelecer segmentos usando segmentação de rede virtual, os dispositivos IoT e os aplicativos que os controlam são isolados, reduzindo assim as ameaças sem o custo ou a complexidade de redes separadas.

[1]https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond

Construindo uma infraestrutura de rede IoT segura

Proteger o tráfego e os dispositivos de IoT é um desafio que não pode ser resolvido por uma única tecnologia de segurança. Isso exige uma abordagem estratégica que use múltiplos recursos de segurança.

Para ajudar as organizações a aproveitar os benefícios e mitigar os riscos da implantação de IoT, a Alcatel-Lucent Enterprise (ALE) oferece uma estratégia de rede de confiança zero com segurança multinível.

A estratégia da ALE oferece proteção em todas as camadas da infraestrutura, desde o usuário ou dispositivo, até a própria camada de rede. A macro e microssegmentação da rede garante uma abordagem simples e segura para dispositivos integrados com segurança e fornece os recursos de rede certos para executar o sistema de maneira adequada e eficiente, tudo em um ambiente seguro para proteger as organizações contra ataques cibernéticos.

Segmentação de IoT

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

- Com a macrossegmentação, os dispositivos são colocados em "segmentos virtuais", usando técnicas de virtualização de rede que permitem que vários dispositivos e redes usem a mesma infraestrutura física, permanecendo isolados do resto da rede.
- Com a microssegmentação, diferentes regras de QoS e segurança podem ser aplicadas aos dispositivos dentro de cada segmento virtual. Isso adiciona maior granularidade e aumenta a segurança da rede, impedindo que diferentes tipos de dispositivos no mesmo segmento interajam uns com os outros quando não deveriam fazê-lo.
- Ao segregar a rede com macro e microssegmentação, se um dispositivo estiver comprometido em uma parte da rede, a violação não apenas não afetará dispositivos ou aplicativos em outros segmentos virtuais, mas também não poderá se propagar dentro do segmento afetado para outros tipos de dispositivos.
- Quando um novo dispositivo IoT é conectado, a rede reconhece automaticamente seu perfil e atribui o dispositivo ao ambiente virtual apropriado.
- A comunicação é limitada aos dispositivos nesse ambiente virtual e ao aplicativo no data center que controla esses dispositivos.
- Como todos os usuários também possuem perfis na rede ALE, o acesso aos segmentos virtuais IoT pode ser limitado a indivíduos e grupos autorizados.

Segurança em profundidade

- Além da segmentação de IoT, as tecnologias de rede ALE fornecem segurança em camadas em vários níveis da rede.
- No nível do usuário, os perfis garantem que os usuários sejam autenticados e autorizados com os direitos de acesso apropriados.
- No nível do dispositivo, a rede garante que os dispositivos sejam autenticados e estejam em conformidade com as regras de segurança estabelecidas.
- No nível do aplicativo, a rede pode estabelecer regras em relação a cada aplicativo ou grupo de aplicativos, incluindo bloqueio, limitação de largura de banda e controle de quem pode acessar qual aplicativo.
- No nível da rede, os switches ALE se beneficiam de um código diversificado e seguro. Isso protege as redes contra vulnerabilidades intrínsecas, explorações de código, malware incorporado e potenciais backdoors que possam comprometer switches, roteadores e outros hardwares de missão crítica.
- A análise inteligente da ALE usa inspeção profunda de pacotes e outras tecnologias para detectar os tipos de dados e aplicativos que se movem pela rede, tornando possível identificar padrões de tráfego incomuns, atividades não autorizadas e invasões da rede.

Gerenciamento operacional e da rede, de ponta a ponta

As soluções de rede ALE também oferecem vantagens operacionais e de gerenciamento significativas.

- A ALE permite que várias redes virtuais separadas operem em uma única infraestrutura comum, eliminando a necessidade de investimento CAPEX em várias infraestruturas físicas.
- A solução de acesso unificado da ALE permite que tecnologias com e sem fio funcionem juntas como uma rede única e robusta, com um conjunto comum de serviços de rede, uma estrutura de políticas, um esquema de autenticação comum e um único banco de dados de autenticação.
- As soluções de rede ALE também possuem um sistema de gerenciamento único para todos os elementos da infraestrutura, incluindo gerenciamento unificado de redes LAN com fio e WLAN sem fio. O Alcatel-Lucent OmniVista® 2500 Network Management System e o Alcatel-Lucent OmniVista® Cirrus Network Management as a Service para gerenciamento baseado em nuvem, fornecem um único painel para gerenciar ambientes virtuais, switches, access points e todos os outros componentes de rede.

Um portfólio de rede de alto desempenho

Os switches, pontos de acesso e controladores 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 de organizações de todos os tamanhos. A ALE também oferece uma seleção de switches, pontos de acesso e roteadores robustos para implantações de rede ao ar livre ou em ambientes adversos.

Cenários de IoT nos principais setores

As soluções de IoT prometem tornar as organizações mais inteligentes e bem-sucedidas no que fazem. Esses benefícios são especialmente notáveis em certas verticais.

Setor de Saúde

A IoT tem o potencial de transformar o setor de saúde alterando profundamente a forma como hospitais, clínicas e outras instalações de atendimento coletam e usam dados, reunindo as principais tendências técnicas e comerciais de mobilidade, automação e análise de dados para melhorar os cuidados ao paciente. Os dados coletados desses dispositivos podem ser analisados pela organização para:

- Melhorar o atendimento ao paciente, oferecendo serviços de atendimento novos ou aprimorados que ajudam a diferenciar uma organização de saúde orientada por dados
- Otimizar processos, desenvolvendo novos serviços, fluxos de trabalho e soluções que aumentam a eficiência e reduzem os custos operacionais
- Conhecer melhor as necessidades e preferências dos pacientes, permitindo que as organizações de saúde ofereçam atendimento e experiências mais personalizadas
- Tornar as redes hospitalares mais inteligentes, monitorando proativamente a infraestrutura crítica e automatizando a implantação e o gerenciamento da infraestrutura de TI

O crescimento da IoT na área da saúde também traz uma explosão de ameaças à segurança cibernética, pois a proliferação de sensores e dispositivos conectados expande muito a superfície de ataque à rede. IoT para a saúde é especialmente suscetível porque muitos dispositivos de IoT são fabricados sem considerar a segurança, ou construídos por empresas que não entendem os requisitos de segurança atuais. Consequentemente, os sistemas IoT podem representar potencialmente o elo mais fraco na segurança cibernética de hospitais, clínicas e instalações de atendimento.

Setor de Educação

As instituições educacionais não são exceção na IoT, em qualquer lugar do mundo. Um mundo em que as tecnologias estão sendo projetadas em todos os produtos imagináveis. A IoT traz inúmeros benefícios para universidades e escolas, trazendo uma nova geração de coisas inteligentes que podem melhorar imensamente a experiência de aprendizado e aumentar significativamente a segurança do campus. Dispositivos IoT, sejam pequenos como um sensor de luz ou grandes como placas inteligentes, trazem grandes mudanças na forma como os ambientes escolares são gerenciados e na maneira como os alunos aprendem. Dispositivos IoT:

- Crie novas maneiras para os alunos aprenderem, apoiando experiências de aprendizado mais personalizadas e dinâmicas, como livros didáticos digitais imersivos e aprendizado baseado em jogos
- Mude a forma como os professores ministram aulas e realizam testes com equipamentos audiovisuais inteligentes, gravadores de vídeo digital para captura de aulas e testes on-line
- Simplifique as operações para os administradores escolares, monitorando proativamente a infraestrutura crítica e criando processos mais eficientes e econômicos para climatização (HVAC), iluminação e gerenciamento de ambiente
- Ofereça um ambiente mais seguro para alunos e professores com câmeras de vigilância digital, fechaduras inteligentes e ônibus escolares conectados

Nessas escolas e universidades remodeladas, os administradores podem coletar, armazenar e analisar grandes quantidades de dados sobre o ambiente e o desempenho dos alunos. Isso dará às escolas a inteligência de que precisam para melhorar os processos para o sucesso dos alunos, permitindo que identifiquem as lacunas a serem preenchidas.

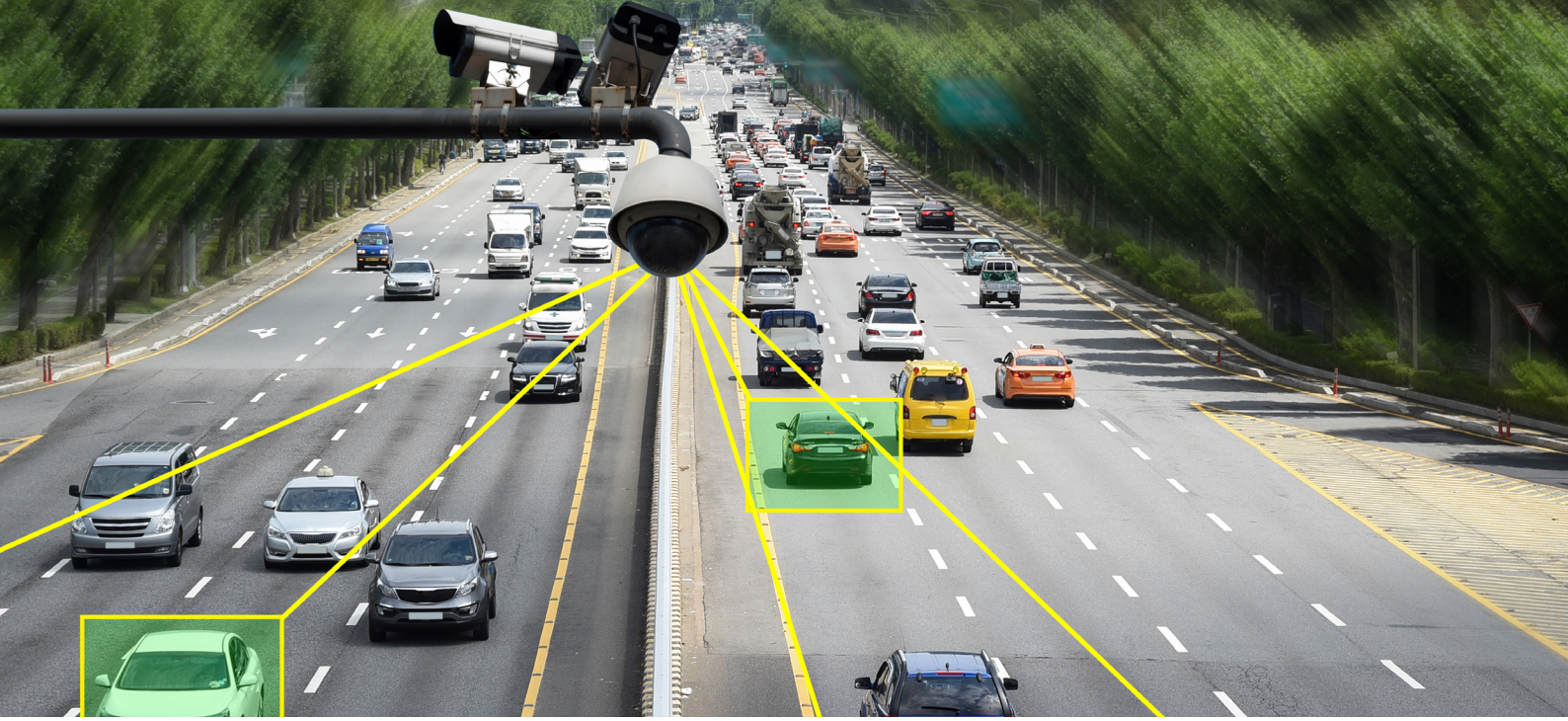
Essas mudanças transformadoras trazem oportunidades e ameaças. É imprescindível empregar uma estratégia de defesa em profundidade, que forneça conexões seguras aos dispositivos IoT e evite violações que possam atingir a privacidade dos dados dos alunos e a segurança da pesquisa ou colocar em risco a autenticidade e a integridade dos dados.

Setor Público

Governos e municípios estão se juntando ao fluxo de IoT. As cidades inteligentes estão apresentando grandes oportunidades de negócios e novos meios para servir e proteger os cidadãos. Nessas cidades conectadas, as empresas de serviços públicos estão lançando medidores inteligentes para criar sistemas de preços adaptáveis, e os desenvolvedores estão implementando sensores e componentes de automação em novas propriedades. Os estacionamentos inteligentes economizam o tempo dos cidadãos e os tornam mais eficientes, e as lixeiras inteligentes exigem ação quando se aproximam do transbordamento. A IoT ajuda municípios e governos a coletar informações de mobilidade e tendências de dados, que fornecem análises críticas vitais para a formulação da estratégia da cidade e o planejamento de longo prazo. A IoT traz:

- Cidadãos e entidades públicas mais bem conectados para fornecer serviços e recursos de alta qualidade, seguros e responsivos, que melhorem o envolvimento e a confiança entre os governos e o público que atendem, aumentando a habitabilidade, a funcionalidade e a sustentabilidade
- Maior segurança no trânsito, entendendo melhor as operações do sistema de transporte por meio de dados de sensores que monitoram tudo, desde anomalias nas velocidades dos trens, temperaturas das estradas e localização em tempo real dos ônibus de transporte público
- Congestionamento e uso de energia reduzidos por meio de tecnologias da Cidade Inteligente, que aproveitam dados em tempo real para melhorar a forma como os funcionários dimensionam os recursos para atender às demandas e fornecer a agilidade para reagir rapidamente a padrões de tráfego que mudam constantemente, variações no uso de água ou energia, ou mudanças na qualidade do ar
- Melhor desempenho operacional e manutenção, monitorando proativamente a infraestrutura pública crítica e criando processos mais eficientes para reduzir os custos operacionais e melhorar a capacidade do sistema
- Melhoria da segurança pública, respondendo às emergências de forma mais rápida e eficaz

O nível de segurança cibernética, no entanto, deve ser alto, muito alto. Nas cidades com IoT, onde nem todos os aplicativos, sensores e dispositivos são projetados tendo a segurança em mente, você precisa de uma infraestrutura inteligente e automatizada que possa colocar esses dispositivos em categorias separadas e impedi-los de conversar com o que não deveriam. Essa conteinerização melhorará significativamente a segurança e colocará as instituições do setor público no caminho certo para avançar em direção a um ambiente baseado em confiança zero, criando várias camadas de proteção em uma estratégia cibernética de defesa em profundidade.



Setor de Transportes

A Internet das Coisas (IoT) está transformando o setor de transporte, alterando profundamente a forma como os sistemas coletam dados e informações, reunindo automação e análise de dados. Sensores, atuadores e outros dispositivos podem coletar e transmitir informações sobre a atividade em tempo real na rede. Esses dados podem então ser analisados pelas autoridades de transporte para melhorar a experiência e a segurança do viajante, reduzindo o congestionamento e a energia usada e, ao mesmo tempo, otimizando o desempenho operacional.

A IoT está no centro das forças que reformulam o transporte para fornecer maior segurança, viagens mais eficientes, manutenção aprimorada de veículos e aeronaves e gerenciamento de tráfego mais estratégico. Exemplos de aplicação da IoT nos transportes incluem:

- Eficiências, para aumentar a capacidade do sistema e melhorar a segurança e o conforto dos passageiros, reduzindo custos e riscos
- Sinais dinâmicos de mensagens na estrada, para sistemas de transporte inteligentes que exibem o status da estrada em tempo real, taxas de pedágio, fechamento de faixas e viagens
- Veículos autônomos, com a capacidade de monitorar seu ambiente, prever o comportamento, comunicar-se com outros veículos e seus arredores e reagir instantaneamente a cenários rodoviários da vida real
- Vigilância por vídeo, para proteger o movimento de pessoas e multidões, automatizar e fornecer detecção precoce de comportamentos suspeitos e bagagens abandonadas

Os ataques cibernéticos podem afetar as operações diárias por longos períodos. Não apenas o serviço é interrompido, mas a exposição de dados altamente confidenciais também é um grande risco quando se trata desse setor. Enquanto alguns ataques de segurança cibernética são uma tentativa de ganhar dinheiro, outras tentativas visam causar caos e desordem ao desligar sistemas inteiros. Interrupção de semáforos, bloqueio de acesso a arquivos e dados importantes, interrupção de serviços de folha de pagamento e comprometimento de máquinas de bilhetes e catracas de cobrança são apenas alguns deles.

- Em 2018, a Bay & Bay Transportation foi vítima de um ataque maciço de ransomware que bloqueou os sistemas usados para gerenciar sua frota de 300 caminhões
- Em 2018, hackers desligaram 2.000 computadores pertencentes ao Colorado Department of Transportation, interrompendo as operações por semanas. Mais recentemente, cibercriminosos se infiltraram em três dos 18 sistemas de computador da Metropolitan Transit Authority de Nova York.
- O primeiro semestre de 2020 revelou um aumento impressionante nos incidentes de ransomware, com um aumento geral de 715% ano a ano
- Em 2020, os endereços de e-mail e detalhes de viagens de 9 milhões de clientes da EasyJet foram roubados. Desses, 2.208 tiveram seus dados de cartão de crédito comprometidos. Esse ataque cibernético, juntamente com a chagada da pandemia global, resultou na perda de 45% do valor das ações da companhia aérea e na primeira perda anual em seus 25 anos de existência.

Redes e estratégias seguras de IoT estão disponíveis hoje

Os produtos e soluções da ALE criam uma base de rede segura para ajudar as organizações a implantar sistemas de IoT que podem revelar os insights para otimizar produtos e processos, tornar os negócios mais inteligentes e eficientes, e oferecer aos clientes experiências aprimoradas. As estratégias da ALE para contenção e segurança em camadas reduzem os riscos e simplificam a configuração de redes IoT, facilitando o uso de dispositivos integrados, proporcionando operações mais eficientes e aumentando muito a segurança. A ALE ajuda as organizações a desbloquearem todos os benefícios potenciais da IoT, fornecendo níveis aprimorados de inteligência, automação e segurança de rede.

Quer saber mais?

Para obter mais informações sobre as soluções de IoT da ALE, acesse Segurança de IoT da ALE.

Alcatel·Lucent Enterprise