Tornar a resiliência e a segurança uma prioridade

Soluções Alcatel-Lucent Enterprise para o setor de educação

Alcatel·Lucent Enterprise

e-Book

Índice

Visão geral

Com os crescentes desafios globais e o aumento dos riscos cibernéticos e físicos, os campi devem priorizar o gerenciamento de riscos, garantir a infraestrutura crítica e proteger alunos e professores. Segundo a EdTech Magazine, os ataques cibernéticos contra universidades aumentaram 70% em 2023.[1] A expectativa é que os serviços de educação continuem, independentemente da situação, e que os alunos e funcionários sejam mantidos em segurança. No cenário global atual, é mais importante do que nunca manter a segurança dos dados, proteger a soberania dos dados e garantir a disponibilidade do serviço.

O setor de Educação, e por que a TIC é mais importante do que nunca

Nos últimos anos, a transformação digital no setor de educação avançou rapidamente, com um número crescente de alunos e funcionários acessando serviços digitais. A transformação digital também permitiu que alguns funcionários de instituições educacionais adotassem um estilo de trabalho 'de qualquer lugar'. Há uma pressão crescente nos campi para acelerar ainda mais a transformação digital. Segundo a Educause, “o ensino superior já não está imune às elevadas expectativas e preferências dos estudantes pelos serviços digitais”.[2]

A Alcatel-Lucent Enterprise trabalha com instituições educacionais no mundo todo e reconhece a importância de proteger alunos, funcionários, operações e edifícios contra riscos físicos e cibernéticos. Nossas soluções consideram a segurança e a privacidade dos dados em todas as etapas do processo de design e são desenvolvidas com opções resilientes para atender a todos os tipos de organização. Este e-Book fornece insights sobre resiliência e segurança para suas soluções de rede, nuvem e comunicações ALE.

1 Ciberataques contra governos aumentaram 95% no último semestre de 2022, diz CloudSek. CSO Estados Unidos, Janeiro de 2023.

2 https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html.

Por que a colaboração TI/TO é fundamental

Antes de explorarmos como melhorar a resiliência e a segurança com as soluções Alcatel-Lucent Enterprise, é importante reconhecer a mudança no relacionamento entre tecnologia da informação e tecnologia operacional (TI/TO). No passado, as equipes de TI e operações não colaboravam estreitamente e cada uma tinha suas próprias funções e responsabilidades. Esses dois mundos agora estão convergindo e precisam trabalhar como um só. Equipes de TI e operações que não estão cientes das atividades umas das outras, ou que não se coordenam e colaboram, colocam toda a organização em risco.

Vamos considerar, por exemplo, o grande número de dispositivos de internet das coisas (IoT) que estão sendo rapidamente implantados em muitos campi. Quando a equipe de TI não está ciente da implementação de novos dispositivos IoT pela equipe de operações, ela não pode garantir que esses dispositivos estejam em conformidade com as políticas de segurança da organização. Os dispositivos de IoT vêm com níveis altamente variáveis de recursos de segurança cibernética e podem não estar equipados com os mecanismos de proteção mais recentes, ou seus recursos podem não ter sido totalmente implementados. Esses dispositivos não autorizados de TI paralela podem executar qualquer tipo de software e estar infectados com vírus e malware. Se não forem verificados, podem facilmente introduzir novas vulnerabilidades e vetores de ataque na rede. Estamos vendo agora o surgimento da colaboração TI/TO necessária para garantir a segurança e a resiliência da rede.

e-Book
Tornar a resiliência e a segurança uma prioridade

Soluções de rede resilientes e seguras

A infraestrutura de rede é essencial para o funcionamento dos campi, assim como para a oferta de serviços aos estudantes e funcionários. Devido à natureza sensível das informações contidas nas redes dos campi e aos serviços críticos operados pelas instituições educacionais, interrupções ou falhas nos serviços de rede podem ter consequências graves, tornando a resiliência e a segurança uma prioridade. Redes confiáveis e seguras são essenciais para que os campi ofereçam serviços eficazes aos estudantes, protejam informações sensíveis e garantam operações sem interrupções.

As Redes da Era Digital da ALE são resilientes e vão além do que muitos outros provedores de tecnologia oferecem. Incorporamos segurança em nossas soluções desde os estágios iniciais de design, sem custos adicionais de licenciamento.

7 práticas recomendadas para suas soluções de rede

A seguir estão 7 práticas recomendadas para garantir que você aproveite ao máximo a resiliência e a segurança incorporadas à sua solução de rede Alcatel-Lucent Enterprise.

1. Revise sua solução com seu parceiro de negócios regularmente para garantir que a versão mais recente do software, os patches e as atualizações de segurança estejam instalados. Uma ferramenta de gerenciamento de ciclo de vida como o ALE PALM, que fornece informações sobre obsolescência e fim de vida útil, também é uma vantagem. Os campi podem planejar com antecedência a substituição de hardware e antecipar a implantação.
2. O ALE Secure Diversified Code randomiza o local de diferentes segmentos de código em seus switches, aumentando drasticamente a segurança. Além disso, o código diversificado seguro da ALE está sujeito a um processo independente de verificação e validação (IVV), conduzido por um especialista terceirizado em segurança cibernética que analisa e testa o sistema operacional ALE para identificar e eliminar quaisquer vulnerabilidades potenciais, backdoors, malware ou explorações do sistema em todas as novas versões.
3. Adote uma nova estratégia de segurança e implemente o acesso à rede baseado em confiança zero. A macro e a microssegmentação de sua rede são cruciais para manter uma infraestrutura resiliente. Siga a abordagem em fases da ALE para microssegmentação, a fim de garantir uma implementação adequada que não cause consequências perturbadoras. Monitore, valide, planeje, simule e aplique.
4. Use o Shortest Path Bridging para obter redundância, com a capacidade de redirecionar dinamicamente o tráfego usando vários caminhos no caso de falha de um caminho. Ele também cria uma rede eficiente e automaticamente conteinerizada.
5. Considere a possibilidade de aproveitar os recursos de chassi virtual para aumentar a confiabilidade em áreas críticas, pois isso traz redundância e resiliência para a sua rede, dando suporte a atualizações de software em serviço (ISSU) e permitindo interconexões em anel. O chassi virtual apresenta uma solução econômica para simplificar o gerenciamento da rede e, ao mesmo tempo, garantir alta disponibilidade.
6. Use os recursos do Alcatel-Lucent OmniVista® Network Management System. O OmniVista Resource Manager garante que você tenha todos os backups de configuração dos switches de rede e que possa restaurá-los no pior caso, ou quando houver necessidade. Esta ferramenta poderosa cuida de todo o ciclo de vida de backup e restauração.
7. Implemente o protocolo VRRP (Virtual Router Redundancy Protocol). O VRRP aumenta a resiliência da rede fornecendo um roteador virtual de backup que pode assumir o controle imediatamente se o roteador principal falhar.

Investir em soluções de rede resilientes e seguras

Investir para garantir que sua rede seja resiliente e segura sempre faz sentido. Entretanto, entender onde investir melhor pode ser complexo e levar tempo – planejamento é fundamental. Antes de começar, aqui estão algumas áreas importantes a serem consideradas para garantir que você obtenha a segurança e a resiliência que sua organização precisa:

- Junto com seu parceiro de negócios, revise e atualize o design da rede para garantir que os requisitos da sua organização estejam refletidos na rede, incluindo o nível apropriado de resiliência para áreas sensíveis e críticas que impactam serviços essenciais do campus. Para áreas críticas, considere adicionar servidores de backup e múltiplas conexões sempre que possível e aplicável.
- Melhore a resposta a incidentes utilizando recursos de inteligência artificial (IA) e aprendizado de máquina (ML) com o Alcatel-Lucent OmniVista Network Advisor. Essa ferramenta garante que os problemas sejam resolvidos antes que afetem os usuários finais, identificando e abordando proativamente problemas de rede ou segurança. Ela agiliza a solução de problemas e melhora a segurança da rede por meio de auditorias de configuração e administração de alertas em tempo real sobre quaisquer mudanças repentinas no comportamento da rede.
- Considere switches reforçados para ambientes adversos. A família Alcatel-Lucent Enterprise de switches Ethernet robustos foi projetada especificamente para se destacar em ambientes desafiadores e temperaturas extremas. Esses switches são construídos com componentes robustos e alojados em gabinetes resistentes, garantindo durabilidade e confiabilidade, além de terem o mesmo sistema operacional dos outros switches ALE. Para aumentar a segurança e proteger informações sigilosas, alguns modelos são equipados com alertas de intrusão e relés de alarme que permitem a conexão de sistemas de alarme externos. Alguns modelos até suportam MACsec (controle de acesso à mídia e segurança) para comunicações de dados seguras. Com o recurso de chassi virtual em switches robustos, você pode obter redundância, resiliência e escalabilidade aprimoradas.
- Forneça treinamento técnico da ALE para a equipe operacional da rede, para ajudá-la a detectar e reagir rapidamente aos problemas.

Soluções de comunicação resilientes e seguras

As comunicações são cruciais para que instituições educacionais interajam com estudantes, funcionários e outras entidades, além de serem essenciais para a disseminação de informações importantes. Sistemas de comunicação devem estar disponíveis em tempos de crise, quando estudantes e funcionários mais precisam de assistência no campus. A resiliência e a segurança estão evoluindo, e revisões regulares ajudarão a manter sua solução de comunicações Alcatel-Lucent Enterprise sempre segura e disponível.

As soluções de comunicação da ALE são seguras desde o conceito. Isso significa que consideramos a segurança em cada etapa da definição, do desenvolvimento e da entrega do produto. Todo o hardware e os sistemas operacionais são reforçados, e a proteção contra ataques de negação de serviço (DoS) está integrada. Estamos em conformidade com certificações e acreditações reconhecidas para padrões globais de segurança e privacidade (ISO 27001, ISO 27017 e ISO 27018). Também seguimos padrões específicos de segurança e privacidade do setor, como a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) nos Estados Unidos e o Hébergeurs de Données de Santé (HDS) para hospedagem de dados de saúde na França, além de padrões regionais de segurança e privacidade, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia.

7 práticas recomendadas para suas soluções de comunicação

A seguir estão 7 práticas recomendadas para garantir que você otimize totalmente a resiliência e a segurança das suas soluções de comunicação ALE.

1. Analise regularmente o status do sistema com seu parceiro de negócios para garantir que a versão mais recente do software, os patches e as atualizações de segurança estejam instalados e que seu contrato de SPS esteja atualizado
2. Revise regularmente os componentes de segurança e continuidade de serviço em seu Alcatel-Lucent OmniVista 8770 Network Management System, que inclui informações e recursos valiosos de resiliência e segurança para sua solução de comunicações
    - Considere o backup automatizado do sistema remoto para evitar a perda de dados de configuração
    - Configure o monitoramento de alarmes e garanta que ele seja atualizado regularmente com os limites corretos. Além disso, verifique se as notificações de falhas no sistema de comunicação ou alertas de qualidade estão sendo enviados para os indivíduos certos
3. Revise e aplique uma política de senha forte, de preferência usando autenticação externa (servidor RADIUS) e defina lembretes para os usuários para ajudar a evitar toll fraud (fraude de chamadas), que ainda são uma ameaça em muitos países
4. Treine os funcionários e garanta que estejam cientes dos riscos e das medidas de prevenção
5. Analise os servidores de aplicativos essenciais aos negócios quanto à condição, adequação e capacidade de serviço
6. Considere uma VLAN específica para voz. Separar os dados de voz de outros tipos de tráfego reduz a chance de contaminação, o que poderia interromper operações e, potencialmente, os serviços do campus
7. Certifique-se de que seus Session Border Controllers (SBCs) estejam configurados corretamente. Os requisitos podem ter mudado ao longo do tempo

Investir em soluções de comunicação resilientes e seguras

Nos últimos anos, o ambiente educacional tem destacado a importância da comunicação com alunos, professores e outros funcionários. A seguir estão algumas áreas importantes a serem consideradas pelos campi que planejam investir em uma solução de comunicação para aumentar a resiliência e a segurança.

- Arquitetura redundante e resiliente. A duplicação de servidores de chamadas em áreas críticas, a implementação de redundância em locais remotos e a duplicação de servidores de aplicativos críticos podem oferecer proteção adicional.
- Os clientes que usam TDM DECT devem considerar a possibilidade de estender a cobertura a áreas críticas para oferecer resiliência em caso de falha do sistema IP
- Crie um fluxo de trabalho usando o Rainbow e/ou o Visual Notification Assistant (VNA) da Alcatel-Lucent, com acionadores automáticos (acionador humano, IoT ou sistema) para notificar as pessoas-chave sobre os problemas do sistema, para que eles possam agir rapidamente e acelerem o processo de recuperação
- Implemente uma criptografia forte. A criptografia é baseada em padrões do setor integrados na solução, sem nenhum impacto sobre a qualidade e o desempenho da voz

- Implemente o Rainbow™ da Alcatel-Lucent Enterprise, a ferramenta colaborativa ideal para complementar as soluções de comunicação da ALE. O Rainbow oferece um conjunto abrangente de recursos, incluindo voz, vídeo e mensagens instantâneas, possibilitando comunicações contínuas e colaboração eficiente. Com o Rainbow, você pode trocar imagens, vídeos e feeds de vigilância por vídeo, aprimorando a percepção contextual e permitindo uma melhor tomada de decisões. O Rainbow também oferece comunicações híbridas com conectividade segura entre ambientes locais e na nuvem. Garante comunicações robustas, mantendo você conectado a colegas e clientes, fornecendo conectividade ininterrupta mesmo em situações desafiadoras. As comunicações híbridas também têm a vantagem de que as operações locais ou na nuvem sejam executadas em locais diferentes, para obter o máximo em resiliência e comunicações abertas.
- Para campi com requisitos de segurança mais rigorosos, o Rainbow Edge oferece uma alternativa local com uma nuvem privada. Pode ser hospedado em qualquer data center, fornecendo controle total sobre servidores, armazenamento e redes, permitindo que as instituições educacionais personalizem e configurem a infraestrutura de acordo com suas necessidades. Políticas personalizadas de segurança podem ser implementadas, e os recursos podem ser gerenciados de forma autônoma. Esse nível de controle fornece visibilidade e autoridade completas sobre sua infraestrutura, permitindo que os campi tomem decisões bem embasadas e otimizem o desempenho em alinhamento com seus objetivos.
- Defina uma estratégia de comunicação segura para a força de trabalho distribuída. A ALE oferece diversas opções de comunicação e colaboração para funcionários distribuídos, móveis ou que trabalham em casa, incluindo:
  - Rainbow
  - IP Desktop Softphone
  - Softphone ALE
  - Deskphone com VPN incorporada, que pode ser implementado em massa com segurança incorporada (VPN)

Proteger seu pessoal e seus ativos

A ALE oferece sistemas de comunicação e notificação em tempo real flexíveis, seguros e altamente disponíveis. Essas soluções podem ser integradas às operações do centro de controle do campus, otimizando o envio e a priorização de chamadas, facilitando a troca de informações contextuais com dados de IoT e fortalecendo a colaboração entre diferentes partes interessadas, permitindo uma melhor tomada de decisão e coordenação.

A capacidade de interconectar dispositivos de IoT em edifícios, combinada com análise e IA, está transformando fundamentalmente o cenário das comunicações. Por meio da integração de sensores, vigilância por vídeo, Rainbow e IA, a mudança de uma abordagem reativa para proativa aumenta a eficiência de tempo e custos. Essa integração facilita uma compreensão contextual abrangente, apoia os processos de tomada de decisão e, consequentemente, reduz os tempos de resposta às solicitações.

Funcionalidades como rastreamento de ativos e controle de fechaduras e iluminação inteligentes otimizam as operações. E a capacidade de gravar comunicações e registrar ações simplifica a análise pós-evento, aprimorando os processos de segurança e reduzindo possíveis responsabilidades. Para alcançar esse nível de evolução, é fundamental um ambiente conectado com acesso Wi-Fi onipresente e fácil integração de IoT.

Para plataformas de comunicação em tempo real sensíveis ao tempo, seguras e altamente disponíveis, uma infraestrutura robusta é vital para garantir operações contínuas. Sua infraestrutura de tecnologia deve abranger o software adequado, protocolos de rede de alta disponibilidade e a flexibilidade para incorporar switches robustos que possam se integrar perfeitamente com seu ecossistema, e suportar condições ambientais adversas como fluxo de ar limitado, choques e temperaturas climáticas extremas. Equipamentos robustos garantem longevidade em locais tão desafiadores.

Quando se trata de sistemas de segurança física, os riscos são altos. Cada minuto e cada trecho de vídeo podem ser cruciais para identificar irregularidades, localizar a origem de um incidente ou compreender a causa de uma ocorrência no campus. Uma infraestrutura robusta de vigilância por vídeo é essencial.

A infraestrutura de rede deve não apenas fornecer largura de banda suficiente e energia via Ethernet (PoE) para câmeras de vigilância, mas também integrar-se perfeitamente aos sistemas de gestão de vídeo. Essa integração garante uma rede de vigilância eficiente e confiável com operação tranquila e fácil solução de problemas. Isso permite que a equipe de operações resolva prontamente quaisquer problemas de vídeo, principalmente em ambientes ou situações em que cada quadro de vídeo é crítico.As integrações da solução Alcatel-Lucent OmniSwitch®, realizadas por meio de plugins com os principais sistemas de gerenciamento de vídeo, ajudam você a alcançar esse objetivo vital.

Quando o rastreamento de ativos ou a localização de pessoas ou equipamentos dentro de sua organização se torna necessário, uma solução eficaz de rastreamento de ativos pode localizar pessoas e ativos de forma fácil e precisa. Esse sistema também aumenta a segurança e a proteção, permitindo o envio rápido de assistência quando a localização dos indivíduos é conhecida. Com a solução Alcatel-Lucent OmniAccess® Asset Tracking, equipes e equipamentos podem ser localizados rapidamente e mostrados em uma planta do ambiente. O rastreamento de ativos também fornece informações sobre padrões de uso, ajudando os campi a avaliarem se os ativos estão sendo utilizados em excesso ou subutilizados.

Soberania e segurança dos dados

A Alcatel-Lucent Enterprise supera outros provedores de tecnologia na implementação das melhores práticas necessárias para a cibersegurança de ponta a ponta. Na ALE, nós:

- Seguimos as melhores práticas e recomendações do National Institute of Science and Technology (Instituto Nacional de Ciência e Tecnologia, NIST) ao realizar avaliações de risco em novos recursos e ao implementar em nossas soluções recursos de segurança cibernética, como criptografia nativa.
- Temos a certificação Common Criteria EAL2+ (Avaliação de Garantia de Nível 2 ou superior).
- Aplicamos as normas ISO 27001 a todas as nossas soluções baseadas em nuvem
- Apoiamos a ZTNA, segmentação de rede granular e políticas de segurança altamente específicas para reduzir o risco de atividades não autorizadas
- Executamos em nossos produtos testes de segurança altamente especializados e específicos, como testes de penetração
- Garantimos que nossos produtos obtenham as principais certificações do setor, como HDS, HIPAA e conformidade com a Lei de Privacidade e Direitos Educacionais da Família (FERPA)

Como especialistas reconhecidos em segurança cibernética, contribuímos para as propostas da União Europeia em relação às diretrizes de cibersegurança. Também aproveitamos nossa expertise em cibersegurança para ajudar os clientes a escolher e implementar a combinação certa de soluções seguras de comunicações unificadas e colaboração para atender às suas necessidades, além de treinar seus funcionários nas melhores práticas de cibersegurança.

Alcatel·Lucent Enterprise