

Cibersegurança abrangente no campus

É necessária uma estratégia abrangente de segurança cibernética para impedir que usuários, dispositivos e aplicativos não autorizados acessem a rede nesta era de confiança zero.

Cinco passos para proteger seu campus

As estratégias de segurança tradicionais não são mais suficientes para afastar os malfeitores. A seguir estão cinco etapas para uma estratégia de **Zero Trust Network Access (ZTNA)**, para oferecer o conceito de “não confiar em ninguém”.

1

Monitorar. Crie um inventário de todos os dispositivos e aplicativos — autorizados e não autorizados — que solicitam ou entregam informações na rede, assim como os protocolos que usam.

2

Avaliar e validar seu inventário. Avalie dispositivos e aplicativos por tipo e função. Isso pode identificar dispositivos de TI ocultos que podem ser eliminados para reduzir imediatamente a superfície de ataque.

3

Planejar sua abordagem para autenticação, auditoria de autorização e administração.

Desenvolva um plano multidimensional que inclua macrossegmentação e microssegmentação.

4

Simular. Teste e valide a abordagem desenvolvida na Etapa 3. Use os insights resultantes para ajustar as políticas de segurança.

5

Aplicar. As políticas de segurança podem ser aplicadas na borda da rede, onde usuários, dispositivos e aplicativos tentam acessá-la.

Riscos, regras e recompensas

Ao embarcar em sua jornada ZTNA, é importante considerar os **riscos, regras e recompensas**.

Riscos a considerar:

- Dispositivos não autorizados não gerenciados pela TI podem causar estragos
- Políticas de segurança inconsistentes introduzem fraqueza
- Redes com segmentação de segurança estática e confiança implícita permitem que usuários, dispositivos e aplicativos anteriormente confiáveis não sejam verificados



Regras a cumprir:

- Os regulamentos dos EUA incluem a Lei de Privacidade e Direitos Educacionais da Família (FERPA) e a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA)
- O Regulamento Geral de Proteção de Dados da UE (GDPR) se aplica a todas as instituições com matrículas de estudantes da UE, independentemente de onde a instituição esteja localizada



Benefícios recebidos:

- **Proteção ampla:** Autentique cada conexão e atribua permissões a cada usuário e dispositivo com listas de controle de acesso à rede e acesso baseado em funções
- **Reduza o risco de propagação de ataques:** Ofereça controle granular por meio da microssegmentação do tráfego do usuário em um macrossegmento
- **Reputação aprimorada:** As práticas recomendadas com processos diligentes podem impulsionar a marca e a imagem pública de uma instituição
- **Resultados acadêmicos aprimorados:** Tecnologias digitais inovadoras melhoram as oportunidades de aprendizado e o sucesso dos alunos
- **Aumento da eficiência de TI:** Garanta o uso adequado dos recursos de rede e tome decisões bem embasadas sobre novas estratégias de tecnologia
- **Benefícios financeiros:** Reduza o risco de que medidas de mitigação caras sejam necessárias em resposta a ataques cibernéticos



Seu parceiro de cibersegurança

Um parceiro experiente pode fornecer insights e soluções comprovadas de segurança cibernética. Trabalhamos com você para fornecer soluções de rede seguras, que se ajustam à sua estratégia.



Segurança certificada:

As soluções de rede ALE atendem aos principais padrões de segurança, incluindo:

- Diretrizes e especificações do International Common Criteria para segurança de TI
- Testes de conformidade do US Joint Interoperability Test Command (JITC)
- Padrão de Processamento de Informações Federais dos EUA (FIPS) 140-2



As soluções ALE expandem os investimentos de nossos clientes ao se integrarem com firewalls da Palo Alto Networks e Fortinet.

Experiência certificada:

Somos um parceiro confiável de segurança cibernética com instituições em todo o mundo, incluindo:

- [Universidade Estadual da Califórnia, nos EUA \(CSU\)](#) - nossas soluções permitem uma **rede confiável e flexível** com segurança aprimorada, Wi-Fi em todos os lugares e serviços de nuvem abertos e compartilhados
- [Centro Paula Souza, no Brasil](#) - nossas soluções oferecem a **segurança, alta velocidade e desempenho** que os usuários exigem
- [Universidade de Linköping](#) - nossas soluções fornecem acesso de rede **resiliente e seguro** para alunos e professores, convidados, parceiros externos, inquilinos em edifícios universitários e provedores de serviços



[Saiba como podemos ajudar sua instituição acadêmica](#) a se concentrar no ensino e na aprendizagem, enquanto nós nos concentramos em proteger sua rede.