세계적 수준의 교육 및 학습을 위한 사이버 보안

백서

Alcatel·Lucent
Enterprise

목차

사이버 공격의 먹잇감

지난 몇 년 동안 학술 기관 에 대한 사이버 공격의 수와 정교함은 전 세계적으로 놀라운 속도로 증가했습니다. 일부 보고서는 교육 부문이 사이버 위기의 한가운데 있다고 선언했으며 최근 클라우드 기반 가상 학습으로의 전환이 해커에게 새로운 기회를 제공했다고 지적했습니다.[1]

안타깝게도, 이러한 종류의 대담한 진술은 실세계의 통계에 기반하고 있습니다. 2021년 8월에서 9월 사이에 교육 기관은 전 세계적으로 580만 건 이상의 악성 소프트웨어의 공격 대상이 되었으며, 이는 전체 공격의 63%에 해당합니다.[2] 2022년에 발표된 데이터에 따르면 교육 및 연구 분야가 여전히 최대 공격 대상입니다. 이 보고서에 따르면 호주/뉴질랜드는 가장 많은 공격을 받는 지역이며, 아시아와 유럽이 그 뒤를 잇고 있으며 라틴 아메리카에서 주간 사이버 공격이 가장 많이 증가했습니다.[3]

학술 기관에 대한 사이버 공격이 매우 빈번해져서, 2022년에는 FBI와 사이버 보 인프라 보안국(CISA)을 포함한 미국의 여러 기관들이 랜섬웨어의 일방적인 공격 대상이 되고 있는 교육기관들에게 경보를 발령하기 위해 힘을 모았습니다.[4]

사이버 공격, 특히 랜섬웨어 공격의 범위와 규모의 증가는 전 세계 기관들에게 심각한 영향을 미치고 있습니다. 학생들과 직원들이 소중한 수업 시간과 정보를 잃고 교육 목표는 위협을 받고 있습니다.

다음을 살펴 보시기 바랍니다.

- 2022년 9월 LA 통합 교육구(LAUSD)에 대한 랜섬웨어 공격으로 유례 없는 컴퓨터 시스템 종료가 발생하여 이메일, 컴퓨터 시스템 및 애플리케이션이 지속적으로 중단되었습니다.[5]
- 2021년 영국에서 발생한 사이버 공격으로 15개 학교의 이메일, 전화 및 웹사이트 통신이 중단되어 온라인 학습이 중단되었습니다.[6]
- 2021년 콜롬비아 보고타의 엘 보스케 대학에서 대규모 사이버 공격이 발생하여 3일 동안 기관, 학술 및 금융 플랫폼이 손상 되었습니다.[7]

또한 사이버 공격은 기관에 대한 평판과 신뢰를 떨어뜨려, 입학생을 줄이고 수익에 손실을 입힐 수 있습니다. 2022년 5월, 일리노이주에 있는 157년 역사의 링컨 대학교는 랜섬웨어 공격으로 인한 재정난 악화로 인해 영구적으로 폐교하게 되었습니다. [8]

1 미국의 학교들이 사이버 공격의 증가하는 위협에 직면하다. RealClear 교육, 2022년 5월
2 미국의 학교들이 사이버 공격의 증가하는 위협에 직면하다. RealClear 교육, 2022년 5월
3 가장 많은 사이버 공격을 목격한 교육 분야. 뉴질랜드 SecurityBrief, 2022년 8월
4 경고 AA22-249A: #StopRansomware: Vice Society. 사이버 보안 및 인프라 보안국, 2022년 9월.
5 LA 학교 구역이 계속되는 랜섬웨어 공격과 싸우며 혼란에 대해 경고하다. TechCrunch+, 2022년 9월.
6 사이버 공격으로 영국 학교 15곳의 온라인 학습이 중단되다. zdnet.com, 2021년 3월.
7 엘 보스케 대학이 디지털 플랫폼에 대한 통제권을 되찾다. NewsBeezer.com, 2021년 7월.
8 랜섬웨어 공격으로 157년 된 링컨 대학이 문을 닫다. CBS News, 2022년 5월

고정관념에서 벗어나기

안타깝게도, 학술 기관에 대한 사이버 공격은 사이버 보안에 대한 전통적인 접근 방식이 실행되는 중에도 계속해서 발생하고 있습니다. 2019년 영국의 국가 사이버 보안센터는 분석 대상인 432개 학교의 98%가 안티바이러스 솔루션을 가동하고 있었고 99%가 방화벽을 가지고 있었음에도 83%의 학교들이 최소 한 번의 사이버 보안 사건을 경험했다고 밝혔습니다.

더 효과적으로 사이버 공격을 예방하려면, 학술 기관들이 사이버 보안에 대한 전통적인 접근에서 더 발전해야 합니다. 성과 해자, 심층 방어 보안 같은 접근 방식은 더 단순했던 시대에는 효과적이었지만, 더 이상 적절한 보호를 제공하지 못합니다. 인터넷과 휴대용 장치가 대세인 시대에 네트워크 에지와 승인되지 않은 네트워크 접근 가능성은 이제 물리적 캠퍼스 경계를 훨씬 넘어 확장될 수 있습니다.

어떤 사용자, 장치, 애플리케이션도 절대적으로 신뢰하지 말아야 합니다.

오늘날 효과적으로 위협에 대응할 수 있는 유일한 네트워크 사이버 보안 전략은 캠퍼스 내부, 클라우드 또는 캠퍼스 외부 등 어디에 있든 사용자, 장치 또는 애플리케이션을 신뢰하지 않는 것입니다. 이 전략은 제로 트러스트 네트워크 액세스(ZTNA)로 알려져 있으며 5가지 중요한 주장들에 기반합니다.

- 네트워크는 적대적입니다.
- 외부 및 내부 위협은 항상 존재합니다.
- 위치는 신뢰를 결정하기에 충분하지 않습니다.
- 모든 장치, 사용자 및 네트워크 흐름은 인증되고 승인되어야 합니다.
- 정책은 동적이어야 하며 가능한 한 많은 데이터 소스를 사용해야 합니다.

ZTNA 보안 구현에 대한 올바른 접근 방식을 통해 기관은 기술과 위협 대신에, 교육과 학습에 집중할 수 있습니다.

이제부터 제로 트러스트로

기관이 ZTNA 사이버 보안 전략을 발전시킬 때, 제로 트러스트로 나아가는 것이 일련의 여정이라는 것을 명심하는 것이 중요합니다. 이것은 하룻밤에 이루어지지 않습니다. 간단히 구매하여 실행할 수 있는 제로 트러스트 솔루션이나 솔루션 세트는 존재하지 않습니다. 모든 기술에 걸쳐 완전한 제로 트러스트 환경을 구현하려면 시간이 걸립니다.

또한 학술 기관들이 사이버 보안에 균형 잡힌 접근 방식을 개발하고 유지하는 것이 중요합니다. 구현된 보안 메커니즘이 너무 융통성이 없거나 제한적이라면, 사람들은 장치, 데이터, 애플리케이션을 보호하기 위해 의도된 그 절차를 피해 작업할 방법을 찾을 것입니다. 사람들은 자신이 소유한, 허가받지 않는 액세스 포인트, 장치, 애플리케이션을 추가하여 지루한 사이버 보안 점검 및 소프트웨어 업그레이드를 피해 더 신속히 작업을 완료하려는 유혹을 받을 것입니다. 이것은 "비승인 정보기술"로 알려진 전략이며 많은 사이버 보안 위험을 안고 있습니다.

또한, 각 기관은 클라우드에 저장된 데이터용 방화벽 정책과 액세스 제어 목록(ACL) 뿐만 아니라, 네트워크에 걸쳐 이동하는 데이터가 충족해야 하는 개인정보 보호 규정을 확인하고 검토해야 할 것입니다.

규제 요건을 검토할 때, 국내 및 국제 개인정보 보호 규정들을 고려하는 것이 중요합니다. 예를 들어, 미국에서 학술 기관들은 가족의 교육권 및 프라이버시에 관한 법률(FERPA)과 의료보험의 양도 및 책임에 관한 법률(HIPAA)을 준수해야 합니다. 또한 EU 개인정보 보호법(GDPR)은 EU 국가에서 온 입학생이 있는 모든 기관에 대해 그 기관의 위치와 상관없이 적용된다는 것을 명심해야 합니다.

귀하의 사이버 위험 및 규제 요건을 파악 하시기 바랍니다.

ZTNA 전략 개발을 시작하기 전에, 현재 그 기관이 직면한 위험과 그 심각성을 철저히 평가해야 합니다. 위험 평가를 준비할 때, 다음과 같은 일반적인 함정을 찾아보십시오.

- IT로 관리되지 않는 사물인터넷(IoT) 장치 이러한 "불량" 장치들은 보안 정책을 따르지 않고 안티 바이러스 보호를 갖추지 않은 구식 펌웨어를 실행하여, 범죄자들이 그것들을 공격의 진입 지점으로 사용할 가능성이 증가하게 됩니다.
- 네트워크에 액세스하는 승인되지 않은 장비 및 개인 소유 장치. 이러한 비승인 정보기술 장치들은 어떤 소프트웨어든지 실행할 수 있으므로 네트워크를 공격할 준비가 된 바이러스 및 악성 소프트웨어에 이미 감염되었을 수 있습니다.
- 일관성 없는 보안 정책. 이러한 비일관성은 신뢰할 수 없는 당사자의 표적이 될 수 있는 네트워크 보호의 취약성을 야기합니다.
- 고정적 보안 세분화 및 절대적인 신뢰를 설정한 네트워크. 사이버 보안에 대한 이러한 전통적인 접근 방식은 처음에 신뢰한 사용자, 장치, 애플리케이션을 계속 신뢰할 것인지에 대해 더 이상 확인하지 않아 네트워크를 공격하도록 허용할 수 있습니다. 또한 이러한 접근 방식은 사이버 공격은 내부에서 유래될 수 없다고 가정하는데 이것은 사실이 아닙니다.

ZTNA 사이버 보안으로 가는 5단계 방법론

ZTNA 사이버 보안 전략을 개발할 때 다음의 5단계가 가장 중요합니다. 이러한 단계들은 네트워크가 승인되지 않은 사용자, 장치, 애플리케이션이 네트워크에 접근하는 것을 중단시키는 종합적인 보호 메커니즘 세트를 갖도록 보장하는 데 도움이 됩니다.

- **1단계: 모니터링** 라이브 네트워크를 모니터링하여 네트워크 및 이를 위해 사용하는 프로토콜에 대한 정보를 요청하거나 전달하는 모든 장치 및 애플리케이션 (승인 및 비승인)의 인벤토리를 생성합니다. 네트워크에서 이 정보를 수집하고 유형, 제조업체, 모델, 운영 체제 및 기타 요소별로 장치를 분류하는 인벤토리 보고서를 생성할 수 있는 많은 도구가 있습니다. 네트워크에 서로 다른 애플리케이션 트래픽 플로우를 식별하는 플로우 모니터링 도구도 사용할 수 있습니다.
- **2단계: 인벤토리 평가 및 검증** 유형 및 역할별로 장치 및 애플리케이션을 평가하는 것부터 시작하십시오. 예를 들어, 장치나 애플리케이션이 교육이나 사물인터넷 용도로 사용됩니까? 비즈니스, 사교, 학술, 연구 목적과 관련됩니까? 효율, 안전, 보안, 개인정보 보호를 개선하는 데 도움이 됩니까? 규제 요건을 충족해야 합니까? 이러한 과정을 거치면 공격 표면을 즉시 줄이기 위해 제거할 수 있는 비승인 정보기술 장치를 식별하는 데 도움이 됩니다.
- **3단계: 인증, 권한 부여, 감사 및 관리에 대한 접근 방식 계획** 최상의 결과를 얻으려면 매크로 세분화 및 마이크로 세분화를 포함하는 다차원 계획을 준비 하십시오. 매크로 세분화는 가상 LAN(VLAN), 가상 라우팅 및 포워딩(VRF), 가상 사설망(VPN) 및 기타 접근 방식을 사용하여 네트워크에서 사용자, 장치 및 애플리케이션을 분리합니다. 마이크로 세분화는 그러한 사용자들, 장치들, 애플리케이션들이 그 네트워크 세그먼트 및 보안 정책과 어떻게 일치하는지 규정합니다.
- **4단계: 시뮬레이션.** 3단계에서 개발된 접근 방식을 시험하고 검증한 다음 도출된 통찰을 사용하여 보안 정책을 세밀하게 조정하고 모든 시나리오를 포괄하는지 확인 하십시오. 이 단계에서는 그러한 접근 방식의 모든 측면들을 시험하는 것이 중요합니다. 예를 들어 시뮬레이션에는 인증서 발급, 정책 구성, 검사 시나리오 구성, 로그 흐름 시뮬레이션 및 방화벽 통합 테스트가 포함되어야 합니다.
- **5단계: 시행** 보안 정책이 완성되고 세밀하게 조정되면, 그러한 정책들은 사용자, 장치, 애플리케이션이 액세스를 시도하는 네트워크 에지에서 시행될 수 있습니다. 시험되고 검증된 보안 정책이 적용되면 승인되지 않은 장치가 네트워크에 액세스하지 못하도록 차단되고 예기치 않은 흐름이 삭제됩니다. 또한 장치들이 검사될 수 있고 그 상황에 대해 IT 팀에게 경고가 전송될 수 있습니다. 이러한 메커니즘은 위험한 운전자가 고속도로에 진입하는 것을 방지하는 일련의 검문소 같은 역할을 합니다.

이러한 5단계 과정을 따르는 것은 기관들이 ZTNA 사이버 보안으로 전환하는 것을 돕지만 그것만으로는 충분하지 않습니다. 성공하려면 모든 ZTNA 사이버 보안 전략에는 교육, 패치 관리, 활발한 비승인 정보기술 관리에 대한 종합적인 접근 방식이 수반되어야 합니다.

부분들의 합 이상

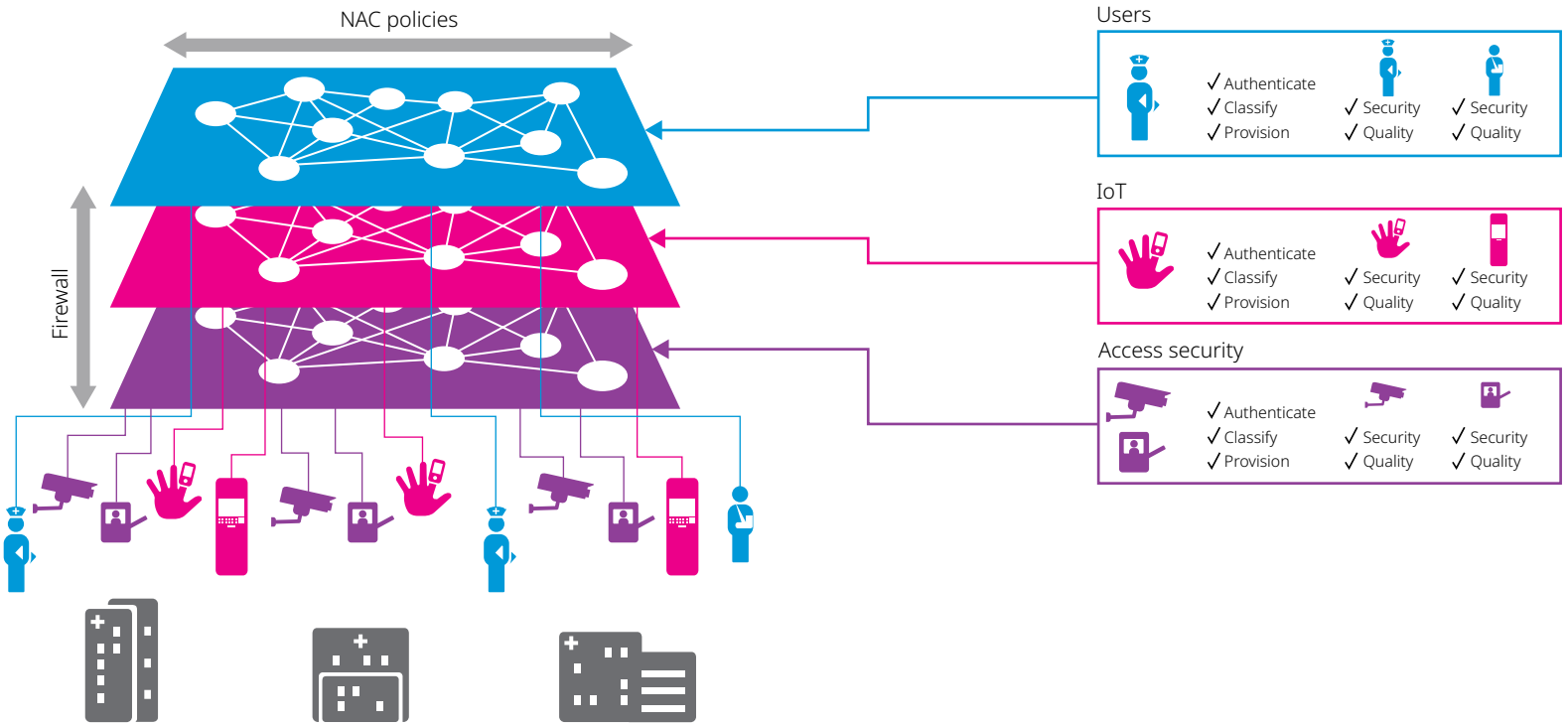
ZTNA 사이버 보안으로 가는 단계별 접근 방식을 따르면, 교육 기관들은 기관 운영의 모든 측면에 걸쳐 중요한 이점들을 실현할 수 있습니다. 가장 분명한 이점은 승인되지 않은 네트워크 접근을 예방 및 탐지하는 것과 관련되며, 그 외에도 수많은 교육적, 사업적 이점이 있습니다.

보호의 확대

기술적인 관점에서, 종합적인 네트워크 접근 제어 목록 및 역할 기반 접근 제어는 네트워크에 접근하는 각 사용자 및 장치에 대해 허가를 부여하고 모든 연결을 인증하는 기능을 제공합니다. 결과적으로 기관들은 불량 사용자 및 장치들이 네트워크 리소스 및 데이터에 접근하는 것을 훨씬 더 어렵게 만드는 세밀한 보호 수준을 구축합니다.

또한 매크로 세그먼트 내에 추가 세그먼트 사용자 트래픽으로 마이크로 세분화를 사용하는 기능은 네트워크 내에서 공격으로 인한 정지 위험을 줄이기 위해 사용자 및 장치의 액세스에 대한 더 세밀한 제어를 가능하게 합니다. 마이크로 세분화로, VLAN과 같은 매크로 세그먼트 내의 사용자 트래픽은 시각, 액세스 위치, 사용자가 학생인지, 교수인지 행정 직원인지 및 기타 액세스 제어 같은 요소에 기반하여 분리될 수 있습니다 (그림 1). 동일한 보안 정책은 그 사람의 위치와 상관없이 그 사람을 따라가므로, 기관들이 사이버 보안에 대해 더 통일된 접근 방식을 구현하도록 합니다.

그림 1. 매크로 세분화와 마이크로 세분화를 결합하여 네트워크 접근 제어 강화



보상받기

해당 네트워크의 정보 보호 및 보안을 세심하게 보호하는 노력 및 성실함으로 잘 알려진 학술 기관들은 평판, 교육 브랜드, 공적 이미지를 개선할 수 있습니다. 사이버 공격으로부터 스스로를 보호하고 그러한 사건에 필연적으로 수반되는 부정적인 명성을 피하는 능력은 학생들을 유치하고 유지하여 장기적인 성공을 강화하는 데 도움이 됩니다. 또한 학술 기관들은 다른 기관이 모방할 수 있는 사이버 보안 모범 사례로 간주되어 전 세계 교육 네트워크를 대상으로 하는 사이버 공격에 대한 방어를 강화하는 데 도움이 됩니다.

ZTNA 사이버 보안 전략은 향상된 학술 결과물에도 기여합니다. 더 안전한 네트워크를 통해, 교수진 및 학생들은 학습 기회와 학생의 성공을 고무시키는 혁신적인 디지털 기술을 안심하고 이용할 수 있습니다. 예를 들어:

- 교수진은 학생들에게 영감을 주고, 최첨단 혁신을 소개하고, 교실에 있든 원격으로 참여하든 학급 토론 및 활동에 적극적으로 참여하도록 격려하는 보다 창의적이고 참여적인 대화형 수업을 개발하고 제공할 수 있습니다.
- 학생들은 새로운 기술을 실험하고 어디에서나 학생 및 교수진과 공개적으로 협업하고, 최신 디지털 혁신을 과제에 구현하여 잠재력을 보여줄 수 있습니다.

신뢰할 수 있는 네트워크 기반을 통해 각 교육 기관은 교육과 학습에 집중할 수 있습니다.

교육 IT 팀들에게도 ZTNA 사이버 보안 전략은 유익합니다. 학술 기관의 사이버 보안 상황을 더 깊이 이해함으로써, IT 팀들은 클라우드 퍼스트 접근 방식 채택 또는 개인 소유 장치의 업무 활용(BYOD) 지원과 같은, 새로운 기술 전략에 대해 더 많은 정보에 입각한 결정을 내릴 수 있습니다. 동시에, 그들은 캠퍼스의 디지털 인프라를 더 잘 보호하고 제어하며, 가치 있는 네트워크 리소스 및 대역폭의 적절한 사용을 보장할 수 있습니다.

마지막으로 중요한 포인트는, 기관들의 공격 표면을 제한하면 사이버 공격에 대응하는 고비용의 솔루션 필요성이라는 위험을 줄이기 때문에 재정적 이점을 가져올 수 있습니다.

전문적인 보안을 위한 전문가 파트너

ZTNA 사이버 보안 전략을 구현하는 학술 기관들은 입증된 ZTNA 네트워킹 솔루션 뿐만 아니라 전문적인 통찰 및 지침을 제공할 수 있는 경험이 풍부한 파트너와 일해야 할 것입니다.

Alcatel-Lucent Enterprise는 풍부한 경험으로 학술 기관들이 전 세계적으로 ZTNA 사이버 보안을 진행하도록 지원합니다. 당사는 ZTNA 전략을 구현하기 위해 이러한 기관들이 취해야 하는 단계들을 이해하고 귀하의 전략에 적합한 보안 네트워킹 솔루션을 제공하기 위해 협력합니다. 그 이후에, 귀하의 기관은 마이크로 세분화 및 역할 기반 접근 제어 같은 핵심 사이버 보안 메커니즘을 최적으로 활용하기 위해, 네트워크 보안에 대한 다층적 접근방식을 구현할 수 있습니다.

종합적인 보안

ALE 네트워킹 솔루션은 다음을 포함하여 주요 보안 표준에 부합 합니다.

- IT 보안을 위한 국제 공통 기준 지침 및 사양
- 미국 합동 상호운용성 시험 사령부(JITC) 적합성 시험
- 미국 연방 정보 처리 표준(FIPS) 140-2

방화벽과 네트워크 인프라 간의 통합 강화는 기관들이 승인되지 않은 악의적인 활동원을 정확하게 찾아내고 공격하는 장치를 검사하는 데 도움이 됩니다. 당사의 솔루션은 Palo Alto Networks 및 Fortinet으로부터 방화벽을 통합하여 당사 고객의 투자를 확대합니다.

경험의 확장

당사는 전 세계 학술 기관의 사이버 보안 상태를 개선하기 위해 일하는 믿을 수 있는 협력사입니다.

- 미국의 캘리포니아 주립 대학은 당사의 네트워킹 및 네트워크 관리 솔루션을 도입하여 향상된 보안, 전방위 Wi-Fi 및 개방형 공유 클라우드를 구축하고 전반적인 캠퍼스 경험을 개선 및 안정적이고 유연한 네트워크를 구축했습니다. 고도로 안정된 네트워크는 그 대학의 20개 이상 캠퍼스에 걸쳐 50만 명 이상 사용자들을 안전하게 지원하고 인프라 비용으로 1억 달러 이상을 절약하도록 도왔습니다.
- 브라질의 산업인력양성원에서 당사의 스마트하고 안전한 네트워킹 솔루션은 사용자가 더 빠르고 효율적으로 작업하는 데 필요한 빠른 속도와 성능을 제공합니다. 직원 및 방문자를 위한 통합 인증은 사용자 친화적인 보안 경험을 제공합니다. 사물인터넷 컨테인먼트 기술은 안전하고 제어된 방식으로 장치를 네트워크에 연결합니다. 또한 IT 직원은 네트워크 운영 및 통합된 네트워크 사용 정책을 완벽하게 파악할 수 있습니다.
- 스웨덴의 린셰핑 대학교에서 당사의 네트워킹 솔루션은 학생과 교수진은 물론 손님, 외부 파트너, 대학 건물의 입주자 및 서비스 제공업체에게 탄력적이고 안전한 네트워크 액세스를 제공합니다. 물리적 및 논리적 네트워크 아키텍처가 완전히 분리되기 때문에 학생과 교직원은 어떤 장치를 사용하든 어디서나 할당된 네트워크 세그먼트에 자동으로 안전하게 연결할 수 있습니다.

자세히 알아보기

귀하의 학술 기관이 제로 트러스트 네트워크 접근 사이버 보안 전략을 통해 어떻게 발전할 수 있는지 확인 하시려면 ALE 웹사이트를 방문 하거나 지금 바로 문의 하여 상담해 보시기 바랍니다.

Alcatel·Lucent
Enterprise