공공 부문 디지털 업무 공간에 대한 고려 사항 및 솔루션

Alcatel·Lucent
Enterprise

eBook

목차

개요

모든 공공 부문 조직에는 우리 모두가 의존하는 정부의 중요한 업무를 수행하는 근로자가 있습니다. 그들의 역할은 아무리 강조해도 지나치지 않습니다. 그들은 종종 수천 명의 삶에 직접적인 영향을 미칩니다.

디지털화는 한동안 진행되었습니다. 공공 서비스를 개선하고 비용을 절감해야 한다는 지속적인 압력으로 팬데믹은 이러한 추세를 더욱 가속화 했습니다. 그러나 2년 전만 해도 재택근무로 전환이 필요한 높은 비율의 공공 부문 근로자 수와 분산된 노동력이 등장할 것이라고 아무도 예측하지 못했습니다.

보다 디지털화된 세상을 기대하는 근로자의 과제와 분산된 인력을 지원하는 복잡한 요구 사항으로 인해 공공 부문 조직은 새로운 하이브리드 인력을 지원하기 위해 임시 솔루션에서 보다 영구적인 솔루션으로의 전환이 필요 합니다.

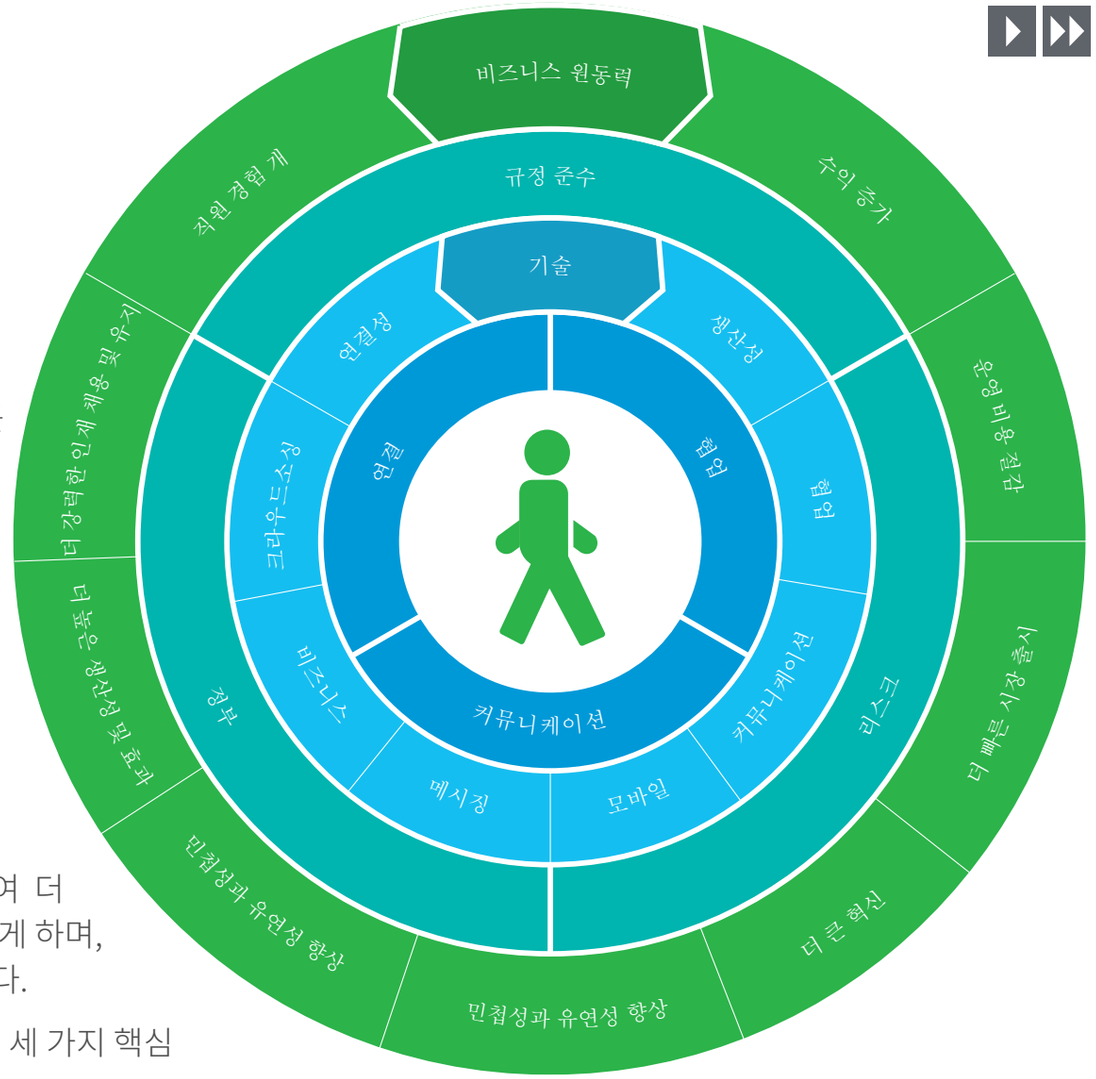
Deloitte는[1] 디지털 업무 공간이 어떻게 조화를 이루고 있으며 디지털 업무 공간이 제공하는 이점을 설명하는 훌륭한 그래픽을 보여 줍니다.

기술은 위치 또는 장치에 관계없이 통신 및 협업을 개선할 수 있는 도구를 제공하지만 원하는 결과에 대한 올바른 기술을 확보하는 것이 더 까다로울 수 있습니다.

Alcatel-Lucent Enterprise는 전 세계 고객과 협력하여 고객이 직면한 새로운 과제를 이해하고 직원이 장소와 장치에 관계없이 작업할 수 있도록 하는 디지털 기술 솔루션을 제공합니다. 디지털 업무 공간은 공공 부문 근로자를 위한 효율성을 창출하여 더 적은 이동으로 더 큰 생산성을 가능하게 하며, 이는 지구에 대한 보너스와도 같습니다.

이 eBook은 공공 부문 디지털 직장의 세 가지 핵심 요소에 중점을 두고 있습니다.

- 커뮤니케이션 및 협업
- 연결
- 보안



그리고 공공 부문 조직이 유연성, 민첩성 및 보안을 갖춘 디지털 업무 공간으로 성공적으로 전환하는 데 도움이 되는 ALE 솔루션을 살펴보겠습니다.

1 - https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/human-capital/The_digital_workplace.pdf

공공 부문 디지털 업무 공간에 대한 주요 고려 사항

커뮤니케이션 및 협업

오늘날 직원들은 직장을 집, 원격 위치, 사무실로 나눕니다. 사무실은 더 이상 일상적인 업무가 이루어지는 곳이 아닙니다. 그룹 미팅, 교육, 시민들과의 대면 만남에 더 많이 사용됩니다. 직원들은 더 이상 한 곳에서 일하고 팀을 만나러 가지 않습니다. 이는 업무 환경에 근본적인 영향을 미치며 그 어느 때보다 커뮤니케이션과 협업이 더 중요해졌습니다.

커뮤니케이션은 디지털 업무 공간의 성공을 위한 중요한 구성 요소입니다. 직원의 참여, 생산성 및 동기를 유지하는 것은 어려운 일입니다. 직원들은 일상 활동을 가능하게 하고 직장 위치 또는 장치에 관계없이 동료, 팀 및 시민과 통신하고 협업할 수 있는 커뮤니케이션 도구가 필요합니다.

연결된 커뮤니케이션을 보장하려면 다음 사항이 권장됩니다.

- 다음을 포함한 직원을 위한 고급 통신 기능 고품질 음성, 그룹 채팅, 음성 메시지 및 장치에 관계없이 통화에서 비디오로 확대하는 기능
- 화면 공유, 원격 데스크톱 제어, 대용량 파일 공유와 같은 공동 작업 기능
- 외부 연락처와의 안전한 통신 및 협업
- 즉각적인 연결과 일관된 연락처 디렉토리를 통해 조직 전체에서 통화 연속성 구현
- 모든 사람에게 최신 발표 또는 규정에 대한 최신 정보를 제공하는 뉴스 방송 채널 제공
- 커뮤니케이션과 협업은 직관적이어야 합니다.

직원이 필요한 모든 것을 갖추도록 하려면 다음 사항이 권장됩니다.

- 직원의 의무, 이동성, 비즈니스 애플리케이션 액세스 필요성을 기반으로 사용자 프로필 및 커뮤니케이션 요구 사항 평가
- 일선 직원에게 이동 중에도 정보와 커뮤니케이션에 빠르게 액세스할 수 있는 최적화된 장치를 제공합니다.

- 시민 서비스 직원이 CRM 또는 비즈니스 앱과 통합된 통화 및 상호 작용 관리에 대한 액세스를 최적화 하도록 지원합니다.
- 백오피스 직원과의 협업을 지원하여 시민 서비스 및 첫 통화 해결률을 개선합니다.
- 데이터 개인 정보 보호를 위한 현지/국가 법적 요구 사항 평가

재택근무 시 뛰어난 성과를 달성하려면 다음 사항이 권장됩니다.

- 모든 장치에서 협업할 수 있는 화면 공유 기능이 포함된 그룹 채팅, 음성 및 화상 회의 역량
- 하나의 기본 인프라를 사용하여 모든 프로필을 연결하는 통화 연속성
- 1시간 이상 전화를 사용하고 다음과 같은 중요한 통화를 관리하는 직원을 위한 DeskPhone 옵션: 시민 서비스, 의료 및 응급 상황
- 선호하는 비즈니스 앱 내 커뮤니케이션을 통해 사용자가 쉽게 채택하고 데스크탑을 항시 깔끔하게 유지할 수 있도록 지원
- 민감한 정보에 안전하게 액세스하기 위한 보안 원격 액세스

연결

디지털 업무 공간은 고품질의 탄력적이며 안전한 연결에 의존합니다. 새로운 작업 방식이 정상화되고 디지털 업무 공간이 형성됨에 따라 직원을 연결하기 위한 디지털 인프라가 갖춰져야 합니다. 위치에 관계없이 몇 가지 핵심 사항을 고려해야 합니다.

- 보안이 최우선 순위여야 합니다. 네트워크 내에 여러 계층의 보안이 있는 네트워크 솔루션이 필요합니다. 제로 트러스트 프레임워크는 모든 장치 또는 사용자가 보안 위험 요소라고 가정합니다. 네트워크 액세스 제어가 활성화되어 있어야 합니다.
- 어디서나 애플리케이션에 안전하게 액세스 하려면 사용자 기반 액세스 연결이 필요합니다. 사용자 기반 프로필은 위치에 관계없이 서비스 손실이 없는 안전하고 유연한 연결을 제공합니다.
- 보안 및 데이터 개인 정보 보호 요구 사항이 높은 원격 작업자는 집이나 지점에서 회사 네트워크에 연결할 수 있어야 합니다. 이를 통해 기업 정책 및 보안이 유지되고 IT 팀이 제어를 유지할 수 있습니다.
- 이제 작업자는 사무실과 가정에서 실시간 애플리케이션(음성, 비디오)에 랩톱을 사용합니다. 이는 많은 공공 부문 조직에 큰 변화입니다. 무선 네트워크는 더 넓은 영역에서 실시간 애플리케이션의 더 많은 사용을 지원할 수 있어야 합니다. 네트워크 범위를 지정할 때 이점을 고려해야 합니다.
- 더 많은 작업자가 무선으로 연결함에 따라 무선 네트워크의 탄력성이 우선 순위 목록으로 올라갔습니다. 액세스 포인트에 인텔리전스가 있는 분산 무선 네트워크는 단일 장애 지점이 없으며 액세스 포인트가 다운되는 경우 네트워크의 다른 액세스 포인트가 서비스를 인수합니다. 또한 분산된 무선 지능형 네트워크는 네트워크에서 중복이 필요하지 않으므로 시간과 비용을 모두 절약할 수 있습니다.
- 디지털 혁신의 가속화된 속도는 이미 일상적인 작업을 처리하고 있는 IT 팀에 부담을 줍니다. 얻을 수 있는 효율성을 고려해야 합니다. 네트워크에서 관리 인터페이스와 운영 체제의 수를 줄이면 작업 부하와 교육 시간이 줄어듭니다. 또한 자동화는 배포 및 운영 네트워크 관리 시간을 줄여줍니다.
- 고품질 액세스가 필수적입니다. 디지털 업무 공간은 연결성이 떨어지고, 증가된 생산성이 손실될 경우 더 큰 생산성을 허용할 수 있도록 효율성을 생성합니다.

보안

커뮤니케이션 보안

정부 및 공공 부문 조직은 사이버 공격의 주요 대상입니다. 사용 가능한 가장 안전한 장비를 구현하는 것이 필수적입니다. 통합 관리 도구는 모든 요소에 대한 보안 감독을 허용해야 합니다.

또한 사이버 공격자가 모든 액세스 지점에 포함된 코드의 증가하는 양을 악용함에 따라 모바일 장치는 통신 환경을 변화시키고 보안의 필요성을 높입니다. 국방 등급 암호화, 데이터 개인 정보 보호 및 보안 통신 환경에는 효율적이고 관리하기 쉬운 안전하고 사용 가능한 인프라가 필요합니다.

ALE의 권고 사항:

통신 시스템 업데이트 및 모니터링:

- 시스템 업데이트는 사이버 보안 측면에서 매우 중요합니다. 이렇게 하면 소프트웨어 취약성으로부터 보호하여 통신 시스템을 최신 상태로 유지할 수 있습니다.
- 네트워크 관리 시스템에서 사용 임계값 및 경고를 구성하여 의심스러운 활동을 추적하기 위해 통신 시스템 모니터링을 활성화 합니다.

인증 및 암호화:

- 모든 기기(전화 및 게이트웨이)와 통신 시스템 간의 상호 인증 사용
- 프로토콜 중독 공격 및 메시지 가로채기 공격을 방지하려면 신호를 암호화 해야 합니다.
- 도청을 피하기 위해 IP 통신을 암호화 해야 합니다.

시스템을 이중화하고 보안 구성 요소를 추가하십시오.

- 위험은 결코 0과 같을 수 없습니다. 게이트웨이 또는 기본 통신 시스템이 다운된 경우 공간적 이중화가 있을 때 백업 시스템이 원활하게 인계받을 수 있습니다.
- Session Border Controller 또는 Reverse Proxy와 같은 통신 시스템을 보호하는 데 필요한 구성 요소를 추가하고 알림 서버는 필요한 사람들에게 경고하는 데 사용됩니다.

교육:

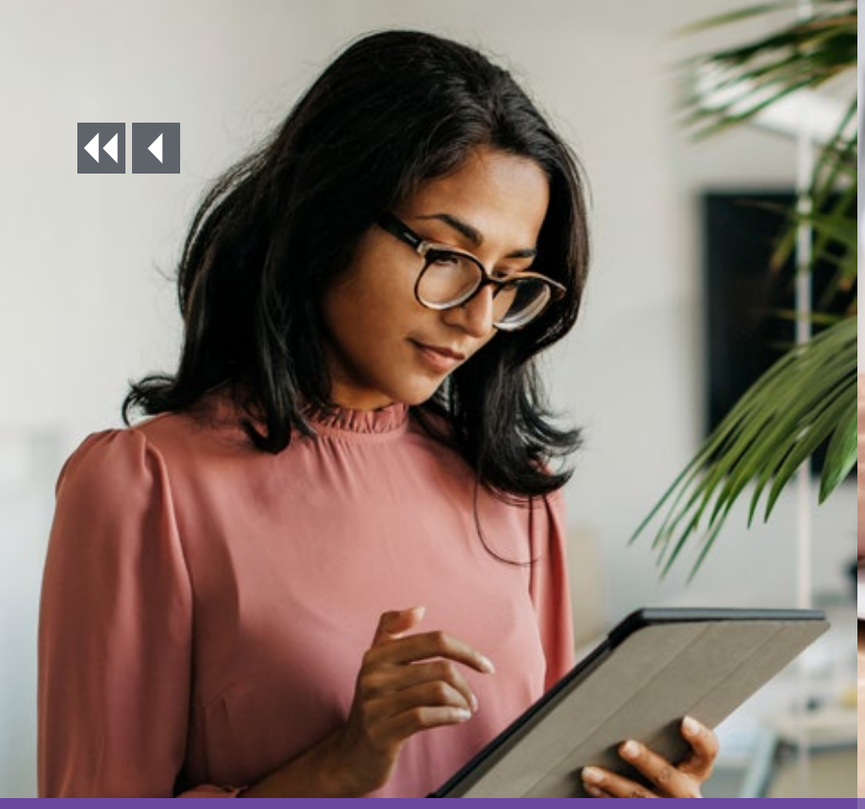
- 사용자 및 관리자 교육 비밀번호 업데이트 알림, 사이버 범죄 퇴치 방법 및 전화의 자물쇠 아이콘이 있는 암호화된 통화 인식 방법에 대한 교육을 포함하여 팀 내에서 모범 사례를 적용합니다.

네트워크 보안

사이버 보안은 오랫동안 정부 기관의 최우선 과제였습니다. 그러나 디지털 전환이 일어나면서 사이버 보안 요구 또한 변화하고 있습니다. 혁신이 가속화됨에 따라 기존의 네트워크 보안 방법은 뒤떨어지기 시작했습니다. 네트워크 아키텍처의 기본 구성 요소로서 보안은 처음부터 기본 제공되어야 하며 모든 네트워크 액세스(유선 및 무선)에 보편적으로 적용되어야 합니다. 다음은 모든 수준에서 네트워크를 보호하기 위해 고려해야 할 몇 가지 영역입니다.

- **사용자 수준:** 사용자가 항상 올바른 액세스 권한으로 인증되고 승인되는지 확인합니다 (정책 및 프로필 사용).
- **장치 레벨:** 장치가 인증되고 IT에서 설정한 보안 규칙을 준수하는지 확인합니다. 이는 장치가 네트워크에 연결되기 전에 빠른 보안 검색을 수행하는 장치에 설치된 에이전트를 통해 달성할 수 있습니다. 예를 들어; 스캔을 통해 네트워크에 연결된 장치에 최신 바이러스 백신 소프트웨어와 최신 버전의 운영 체제가 있는지 확인할 수 있습니다.
- **애플리케이션 수준:** 특정 애플리케이션과 관련된 규칙 설정 (차단, 대역폭 제한 또는 사용할 수 있는 사용자 식별 포함)
- **스마트 분석:** 스위치 및 액세스 포인트의 분석 기능은 네트워크, 사용자, 기기 및 네트워크에서 사용되는 애플리케이션에 대한 가시성과 세부 정보를 제공하는 데 도움이 됩니다. 이것은 심층 패킷 검사 및 기타 역량을 사용하여 네트워크를 통해 이동하는 데이터 및 애플리케이션의유형을 감지하여 비정상적인 네트워크 트래픽 패턴과 무단 활동 및 네트워크 침입을 식별할 수 있습니다.
- **네트워크 세그멘테이션 기술**: IoT 장치를 보안 가상 컨테이너에 위치 시킴으로써 여러 디바이스와 네트워크가 동일한 물리적 인프라를 사용하고 나머지 네트워크와 격리된 상태로 유지됩니다. 가상 네트워크의 한 부분에서 위반이 발생하더라도 네트워크 또는 애플리케이션의 다른 영역에는 영향을 미치지 않습니다.

이러한 보안 기술은 "절대 신뢰하지 않음 - 항상 확인"이라는 전제에서 작동하는 네트워크 아키텍처의 다음 수준인 제로 트러스트 아키텍처 프레임워크를 구축하는 데 도움이 됩니다. 모든 사용자는 애플리케이션 및 데이터에 대한 액세스 권한을 부여받기 전에 인증, 권한 부여 및 지속적으로 검증되어야 합니다.



디지털 업무 공간

유연한 클라우드 모델

모든 것을 하나로 연결

공공 부문 디지털 업무 공간에 대한 ALE 솔루션

커뮤니케이션 및 협업

Alcatel-Lucent Enterprise DAC (디지털 에이지커뮤니케이션)은 디지털 혁신을 해결하기 위해 포괄적인 온프레미스 및 클라우드 기반 커뮤니케이션 및 협업 솔루션을 제공합니다. 디지털 업무 공간은 원격 근무가 일상화된 분산 업무 환경으로 진화하고 있으며, 동료, 시민, 파트너를 연결하는 실시간 커뮤니케이션이 필수적입니다. Alcatel-Lucent Enterprise 통신 솔루션은 장소, 상황, 장치에 상관없이 통화 연속성을 가능하게 합니다.

ALE 주요 통신 기능:

- 조직 내부와 외부의 **원활한 연결**. 기본 통신 인프라는 PSTN, TDM, IP, SIP, VoWIFI, DECT와 같은 다양한 표준 기술을 통해 장치에관계없이 하이브리드 작업자를 백오피스 및 일선 직원과 연결하고 IT가 서비스 품질(QoS)을 모니터링할 메트릭을 제공합니다.
- **회사 전화와**소프트폰에서의 단일 번호 라우팅은 하이브리드 업무에 적합합니다. 재택근무 또는 사무실 근무에 상관없이 통화가 끊기지 않고 착신 전환이 필요하지 않습니다.

- ALE DeskPhone은 현장 로밍 **중 알림 및 알람을 포함하여 일선 모바일 직원을 위한 3D Symphonic** HD 품질의 견고한 핸드셋 및 스마트폰 앱을 제공합니다.
- **통화 그룹**및 대기열과 같은 고객 인사말 및 상담원 기능에 쉽게 액세스하여 고객 서비스 직원이 모든 고객 통화에 응답할 수 있습니다.
- 긴급 호출 위기 회의 를 사용하면 버튼 하나만 누르면 사전 정의된 연락처를 재난 또는 위기 관리 회의에 자동으로 참가할 수 있습니다.
- **엔드 투 엔드 암호화**는 공공 부문 조직에 필요한 보안 및 개인정보 보호를 보장합니다.

- 디지털 작업 공간을 위한 커뮤니케이션 및 공동 작업은 **간단한 클릭 투 콜** 연락처 또는 회의 시작 또는 그룹 채팅, 화면 및 파일 공유, 오디오 및 화상 회의와 같은 고급 기능을 통해 쉽게 이루어집니다. 웹 클라이언트로 사용할 수 있는 단일 앱에서 이 모든 것이 가능합니다. 별도의 설치가 필요하지 않습니다. PC는 물론 Android 및 iOS 장치에서도 앱을 사용할 수 있습니다. ALE 솔루션을 사용하는 고객은 WebRTC 기술이 적용된 기존 핸드셋을 사용할 수 있습니다.
- Microsoft®Teams 및 Google용 커넥터를사용하면 디지털 업무 공간에서**근무하는 직원**이 전체 조직과 쉽게 커뮤니케이션할 수 있습니다. SaaS CRM 및 ITSM용 Connector를 사용하면 직원이 비즈니스 앱에서 커뮤니케이션하고 협업할 수 있습니다.

연결

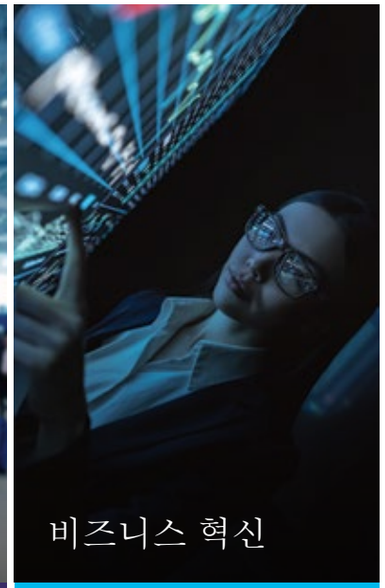
Alcatel-Lucent Enterprise Digital Age Networking 은자율 네트워크가 초고속 컨버전스 시간, 보안 네트워크 액세스 제어 및 보장된 Qo S(서비스 품질)를 제공하는 Alcatel-Lucent OmniSwitch® (LAN)및 Alcatel-Lucent OmniAccess® Stellar (WLAN)를 통해 탄력적이고 원활한 연결 환경을 제공합니다. 액세스 포인트에 WLAN 제어 기능이 내장된 차세대 엔터프라이즈 Wi-Fi를 사용하면 물리적 중앙 집중식 컨트롤러의 필요성이 없어집니다. ALE 솔루션은 온프레미스와 클라우드에서 관리할 수 있습니다.

ALE 주요 연결 기능:

- **단일 NMS(네트워크 관리 시스템)**는 두 가지 정책 및 구성 규칙 집합으로 두 개의 관리 시스템을 처리할 필요가 없으므로 IT 관리자의 작업 부하를 줄이는 추가 수준의 유무선 네트워크를 제공합니다. Alcatel-Lucent OmniVista® 네트워크 관리 시스템 은 IT 효율성과 민첩성을 향상시킬 수 있는 통합 관리 및 네트워크 전반의 가시성을 제공합니다.
- 보안 네트워크 인프라의 **자동 프로비저닝** 은 추가, 이동 및 변경을 단순화하는 동시에 네트워크 유지 및 운영에 필요한 시간을 줄여 비용과 위험을 줄이면서 운영 효율성을 창출합니다.
- **최단 경로 브리징(SPB)** 은 덜 복잡한 네트워크의 생성 및 운영을 지원하도록 설계되었으며 노드 간의 네트워크 유형을 동적으로 구축하고 유지합니다. SPB 로드는 사용 가능한 모든 물리적 연결을 공유하고 사용하여 더 많은 대역폭을 사용할 수 있습니다.
- **하이브리드 작업자(옵션 1). 보안 원격 액세스는** 원격 액세스 포인트(RAP)를 통해 활성화됩니다. 엔터프라이즈 네트워크는 메인 사이트 외부로 쉽게 확장할 수 있어 원격 작업자가 회사 LAN 에 있는 것처럼 연결할 수 있습니다. 모델에 따라 RAP는 IP 전화 또는 기타 IoT 장치에 유선 연결을 제공할 수도 있습니다. 유무선 네트워크 전반에 걸쳐 중앙 집중식 통합 보안 정책으로 액세스가 지원되므로 관리가 쉽고 강력하고 일관된 보안이 보장됩니다.
- **하이브리드 작업자(옵션 2) SD-WAN 및 SASE**. SASE(Secure Access Service Edge)는 원격 사이트, 지사 및 원격 작업자를 안전하게 연결합니다.재택 근무자를 위한 SASE 솔루션은 회사 데이터 센터, 사설 데이터 센터, 인터넷 또는 공용 클라우드의 애플리케이션에 대한 보안 액세스를 제공하는 사용자 노트북의 소프트웨어로 구성되며 작업자 사이트에 추가 하드웨어가 필요합니다. SASE는 URL 필터링 및 애플리케이션 방화벽을 포함한 차세대 방화벽(NGFW)과 차세대 침입 방지 시스템(NGIPS)을 포함한 통합 위협 관리(UTM)로 고급 보안을 제공합니다. 바이러스 백신 및 멀웨어 방지 기능 또한 제공합니다.

필수적인 네트워크 운영 자동화 및 사용자 경험 개선

안전한 IoT 온보딩 및 관리를 통한 디지털화의 확장



자동화된 워크플로를 통해 혁신 가속화

보안

커뮤니케이션 보안

작은 지방 정부 기관이든 대규모 국가 정부 기관이든 귀하의 통신 네트워크는 해커의 표적이 될 위험이 있습니다.

ALE 주요 보안 기능:

- 상호 인증, 암호화 및 보안 경계 요소(SBC)를 사용하여 Alcatel-Lucent Enterprise에서 완전히 개발 및 운영하는 온프레미스 통신 시스템(PBX 및 전화)과 클라우드 인프라 간의 **보안 연결**
- **고가용성**, 공간 이중화 아키텍처, 온프레미스, 프라이빗 또는 퍼블릭 클라우드, 서비스 거부(DoS) 공격에 대한 보호, 강화된 하드웨어 및 운영체제를 통한 내장 보안
- 음성 품질 및 성능에 영향을 미치지 않으면서 솔루션에 기본적으로 구현된 업계 표준을 기반으로 하는 강력한 암호화로 **통신 기밀을 유지** 하여 고객과 직원이 기대하는 경험을 제공합니다.
- 역할 기반 액세스 제어 및 저장된 데이터 암호화를 통한 **데이터 개인 정보 보호 및 보호** . 이렇게 하면 진화하는 비즈니스 환경에서 수집된 모든 중요한 데이터가 엔드 투 엔드로부터 완전히 보호되고 사용자가 제어할 수 있습니다.
- **일반 데이터 보호 규정(GDPR), ISO27001, Common Criteria** EAL2+, HDS("Hébergeur Données Santé" 프랑스의 데이터 환자 보호 규정 준수를 위한 ALE 클라우드 서비스 인증)
- 적극적인 취약성 관리, 정기적인 최신 소프트웨어 및 정책 플랫폼을 위한 제품 보안 사고 대응 팀(PSIRT)의 **프로세스로서의 보안**

인증

ANSSI (CSPN)

ENS(Esquema Nacional de Seguridad)

외부 위협 및 사고로부터 정보 시스템을 적절하게 보호하는 시스템을 갖추기 위해 스페인 국가 안보 시스템(Spanish National Security System)에서 제정한 인증입니다.

ISO27001 - 017/018

The Agency for Digital Italy는 각료 회의 의장직을 맡고 있습니다. 보안을 보장하는 주요 데이터에 대한 사용, 저장 및 액세스를 규제합니다.

BSI 인증

정보 기술 보안을 위한 연방 사무국(Bundesamt für Sicherheit in der Informationstechnik). ANSSI(2021년 3분기)의 CSPN과 동일

네트워크 보안

연결된 장치의 수가 증가하고 네트워크 경계가 사라지고 변화가 계속 가속화됨과 동시에 디지털 전환은 사이버 보안 요구 사항을 크게 바꿔 놓았습니다. Alcatel-Lucent Enterprise 디지털 에이지 네트워킹은 오늘날의 디지털 전환 시대에 IT 자산과 데이터를 안전하게 보호합니다. 이 솔루션을 사용하면 사용자 액세스를 면밀히 관리하고, IoT, 모바일 및 네트워크 장치로 인해 발생하는 취약성을 줄이고, 피할 수 없는 침해가 공격 지점을 제공하지 못하게 하고 신뢰할 수 있는 엔터프라이즈 에코시스템을 제공할 수 있습니다.

ALE 솔루션은 다음을 통해 설계 시 안전합니다.

- 다음을 포함한 독립적인 제3자 확인 및 검증을 사용하여 네트워크 기기 수준에서 보안 및 보증을 촉진하는 **다중화된 보안 코드**:
  - 다음을 포함한 취약점을 제거하기 위한 사이버 보안 전문 회사의 소스 코드 분석, 화이트 박스 및 블랙 박스 테스트:
    - ¬ 백도어 위협
    - ¬ 임베디드 말웨어
    - ¬ 악용 가능한 취약점
    - ¬ 독점 및/또는 기밀 정보 노출
- **소프트웨어 다양화:** ALE 소프트웨어는 ASLR(Address Space Layout Randomization)을 구현합니다. 각 스위치 부팅은 소프트웨어 악용을 방해하거나 방지하기 위해 고유한 메모리 레이아웃을 동적으로 생성합니다.
- 제로 트러스트 보안 **(마이크로 및 매크로 세분화):** 제로 트러스트 프레임워크는 해커가 있다고 가정합니다. 엔터프라이즈는 더 이상 암시적 신뢰 영역으로 간주되지 않습니다. 여기에는 모든 연결 인증과 같은 작업이 포함됩니다. 어떠한 자산이나 사용자가 있다면 본질적으로 신뢰할 수 있어야 합니다.
- **기본적 보안:** OmniSwitch에서 원격 액세스를 사용 설정해야 합니다. 이는 스위치/라우터에 대한 모든 액세스가 기본적으로 켜져 있고 관리자가 장치를 보호할 수 있는 방법을 알아내야 하는 대부분의 다른 스위치와 반대입니다.
- **빌트인 서비스 거부(DoS) 보호:** 일반적으로 CPU 사용률을 100%로 만드는 데 사용되는 다양한 DDOS 공격으로부터 OS 및 관리 모듈 보호
- 구매 및 추적할 **소프트웨어 패키지 없음**: ALE 보안 코드를 비롯한 모든 기능이 스위치 가격에 포함되어 있으므로 추가할 모듈이나 업그레이드할 필요가 없습니다. 모든 소프트웨어가 포함되어 있습니다.
- **자동화된 안전한 IoT 온보딩:** 기기 지문, 분류 및 컨테이너화를 통해서 구현

EU GDPR

미국 연방

미국 공동 상호 운용성

미국 MIL-STD

미국 무역 협정법(TAA)

자세히 알아보기

디지털 작업 공간을 위한 Alcatel-Lucent Enterprise Public Sector 솔루션에 대해 자세히 알아보거나 ALE에 문의하여 요구 사항을 논의하세요.

www.al-enterprise.com/en/industries/government

Alcatel·Lucent Enterprise