복원력과 보안을 우선순위에 두기

정부 및 공공 시장을 위한 Alcatel-Lucent Enterprise 솔루션

Alcatel·Lucent
Enterprise

eBook

목차

개요

전 세계적인 챌린지와 사이버 및 물리적 위험이 증가함에 따라 정부는 위험 관리를 우선시하고 주요 인프라를 보호하며 시민을 보호해야 합니다. CloudSek에 따르면 2022년에 정부를 대상으로 한 사이버 공격이 95%나 급증했습니다.[1] 하지만, 우리는 상황에 관계없이 정부 업무는 계속 되어야 하고 시민의 안전이 보장될 것을 기대 합니다. 오늘날과 같은 글로벌 환경에서는 데이터 보안을 유지하고 데이터 주권을 보호하며 서비스 가용성을 보장하는 것이 그 어느 때보다 중요합니다.

공공 부문과 ICT가 그 어느 때보다 중요한 이유

최근 몇 년 동안 공공 부문에서 디지털 혁신이 급속히 진행되면서 점점 더 많은 시민이 디지털 서비스를 이용할 수 있게 되었습니다. 디지털 혁신으로 인해 정부 직원들도 어디서나 일할 수 있는 업무 방식을 채택할 수 있게 되었습니다. 또한 정부가 디지털 혁신을 더욱 가속화해야 한다는 압력이 커지고 있습니다. Deloitte에 따르면 정부 기관의 77%가 팬데믹 기간 동안 추진한 디지털 혁신 이니셔티브가 이미 조직에 긍정적인 영향을 미치고 있다고 답했습니다.[2]

Alcatel-Lucent Enterprise는 전 세계 정부와 협력하고 있으며 사이버 및 물리적 위험으로부터 시민, 운영 활동 및 건물을 보호하는 것이 얼마나 중요한지 잘 인식하고 있습니다. 당사 솔루션은 설계 과정의 모든 단계에서 보안과 데이터 개인 정보 보호를 고려하며 모든 유형의 조직에 맞는 복원력 있는 옵션으로 구축되었습니다. 이 eBook은 ALE 통신, 클라우드 및 네트워크 솔루션의 복원력과 보안에 대한 통찰력을 제공합니다.

1 CloudSek에 따르면 2022년 하반기에 정부를 대상으로 한 사이버 공격이 95% 급증했습니다. CSO United States, 2023년 1월.
2 https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html.

IT/OT 협업이 중요한 이유

Alcatel-Lucent Enterprise 솔루션을 사용하여 복원력과 보안을 향상하는 방법을 알아보기 전에 정보 기술과 운영 기술 관계의 변화를 인식하는 것이 중요합니다. 과거에는 IT 팀과 운영 팀이 긴밀하게 협업하지 않았으며 팀마다 고유한 기능과 책임이 있었습니다. 이제 이 두 팀은 합쳐지고 있으며 단일팀으로 기능해야 합니다. 서로의 활동을 인식하지 못하거나 조정 및 협업하지 않는 IT 팀과 운영 팀은 조직 전체를 위태롭게 합니다.

예를 들어 많은 정부 기관과 스마트 시티에 빠르게 구축되고 있는 수많은 사물 인터넷(IoT) 장치를 생각해 보겠습니다. IT 팀이 운영 팀에서 새로운 IoT 장치를 구현하고 있다는 사실을 알지 못하면 해당 장치가 조직 보안 정책을 준수하는지 확인할 수 없습니다. IoT 장치는 사이버 보안 기능 수준이 매우 다양하며 최신 보호 메커니즘이 갖춰져 있지 않거나 기능이 완전히 구현되지 않았을 수도 있습니다. 이러한 비승인 정보기술 장치들은 어떤 소프트웨어든지 실행할 수 있으므로 바이러스 및 맬웨어에 감염될 수 있습니다. 확인하지 않은 상태로 두면 네트워크에 새로운 취약성과 공격 벡터가 쉽게 도입될 수 있습니다. 이제 네트워크 보안과 복원력을 보장하는 데 필요한 IT/OT 협업이 대두되고 있습니다.

복원력 있고 안전한 네트워크 솔루션

네트워크 인프라는 정부 기관이 제대로 기능하고 시민에게 서비스를 제공하는 데 있어 필수 요소입니다. 정부 네트워크에 저장된 정보와 정부가 운영하는 중요 서비스의 민감한 특성으로 인해 네트워크 서비스의 다운타임이나 중단이 발생하면 심각한 결과를 초래할 수 있으므로 복원력과 보안을 최우선으로 고려해야 합니다. 정부가 효과적인 공공 서비스를 제공하고 민감한 정보를 보호하며 원활한 운영을 보장하기 위해서는 복원력 있고 안전한 네트워크가 필수입니다.

ALE 디지털 에이지 네트워크는 회복력이 뛰어나며 다른 많은 테크벤더들이 제공하는 것보다 뛰어난 성능을 제공합니다. 당사는 추가 라이선스 비용 없이 설계 초기 단계부터 네트워크와 솔루션에 보안을 내장합니다.

네트워크 솔루션을 선택하기 위한 6가지 모범 사례

1. 제로 트러스트 보안 전략을 채택하십시오. 복원력 있는 인프라를 유지하려면 네트워크를 매크로 및 마이크로 세분화하는 것이 중요합니다. 마이크로 세분화에 대한 단계적 접근 방식은 적절한 구현을 보장하고 중단을 방지하는 데 도움이 됩니다.
2. 최단 경로 브리징(SPB) 솔루션을 채택하여 중복성과 보안을 보장하십시오. 이 접근 방식을 사용하면 장애 발생 시 여러 경로에서 트래픽을 동적으로 다시 라우팅하는 동시에 효율적이고 컨테이너화된 네트워크를 구축할 수 있습니다. SPB는 MAC-in-MAC 캡슐화로 보안을 강화하고 IP 주소를 제거하여 IP 스푸핑 및 패킷 분석 공격을 차단합니다.
3. 가상 섀시 기능을 활용하여 중요 영역에서 안정성을 높이는 것을 고려하십시오. 이 기능을 활용하면 네트워크 중복성과 복원력이 향상되고 서비스 내 소프트웨어 업그레이드(ISSU)가 지원되며 전용 메시 또는 링 상호 연결이 가능해집니다. 가상 섀시는 높은 가용성을 보장하는 동시에 네트워크 관리를 단순화하는 비용 효율적인 솔루션을 제공합니다.
4. 가상 라우터 중복 프로토콜(VRRP)을 구현하는 것을 고려하십시오. VRRP는 기본 라우터에 장애가 발생할 경우 원활하게 대체할 수 있는 백업 가상 라우터를 제공하여 네트워크 복원력을 향상합니다.
5. 네트워크 스위치의 모든 구성 백업을 확보하고 최악의 상황이 발생하거나 필요한 경우 이를 복원할 수 있는 솔루션을 구현하십시오.
6. 강화된 보안 단계는 스위치에서 다양한 코드 세그먼트의 위치를 무작위로 지정하여 보안을 획기적으로 향상하는 보안 다각화 코드를 사용하는 것입니다. 이 코드는 타사 사이버 보안 전문가가 수행하는 독립적인 검증 및 확인(IVV) 프로세스와 결합될 수 있습니다. 이 프로세스는 운영 체제를 분석하고 테스트하여 잠재적인 취약점, 백도어, 말웨어 또는 시스템 악용 사례를 식별하고 제거합니다.

복원력 있고 안전한 네트워크 솔루션에 대한 투자

네트워크의 복원력과 보안을 보장하기 위해 투자하는 것은 언제나 현명한 선택입니다. 하지만 어디에 투자하는 것이 가장 좋은지 파악하는 것은 복잡하고 많은 시간이 걸리는 작업이기 때문에 사전 계획을 세우는 것이 중요합니다. 시작하기 전에 조직에 필요한 보안과 복원력을 확보하기 위해 고려해야 할 몇 가지 핵심 영역은 다음과 같습니다.

- 네트워크 설계를 검토하고 조직의 요구 사항이 네트워크에 반영되도록 업데이트 하십시오. 이러한 요구 사항에는 필수적인 정부 서비스에 영향을 미치는 민감하고 중요한 영역에 대한 적절한 수준의 복원력이 포함됩니다. 중요한 영역에서는 가능하고 적용 가능한 경우 백업 서버와 여러 개의 연결을 추가하는 것을 고려하십시오.
- 사고 대응 시간의 중요성이 점차 커지고 있음에 주목 하십시오. 예를 들어 당사는 Alcatel-Lucent OmniVista Network Advisor에서 인공 지능(AI)과 머신 러닝(ML) 기능을 사용하여 문제를 더 빠르게 식별하고 해결합니다. 이 도구는 네트워크 문제나 보안 문제를 사전에 식별하고 해결하여 문제가 최종 사용자에게 영향을 미치기 전에 해결되도록 보장합니다. 구성 감사를 수행하고 네트워크 동작에서 갑작스럽게 나타나는 변화에 대한 경고를 실시간으로 관리하여 문제를 더 신속하게 해결하고 네트워크 보안을 향상합니다.
- 열악한 환경에서는 강화 스위치 사용을 권장합니다. Alcatel-Lucent Enterprise의 내구성이 강화된 이더넷 스위치 제품군은 특히 혹독한 환경과 극한 기온에서도 탁월한 성능을 발휘하도록 설계되었습니다. 이러한 스위치는 견고한 구성 요소로 제작되고 튼튼한 케이스에 담겨 있어 내구성과 안정성을 보장하며 나머지 ALE 스위치와 동일한 운영 체제를 사용합니다. 보안을 강화하고 민감한 정보를 보호하기 위해 일부 스위치 모델에는 외부 경보 시스템을 연결할 수 있는 침입 경고 및 경보 릴레이가 장착되어 있습니다. 일부 모델은 두 종단 간의 안전한 데이터 통신을 위해 MACsec을 지원하기도 합니다. 내구성이 강화된 스위치에서 가상 섀시 기능을 사용하면 중복성, 복원력 및 확장성을 향상할 수 있습니다.

복원력 있고 안전한 통신 솔루션

통신은 정부가 시민, 이해관계자 및 기타 정부 기관과 상호 작용하고 중요한 정보를 전파하는 데 필수적입니다. 시민이 정부 지원을 가장 필요로 하는 위기 상황에서도 통신 시스템을 사용할 수 있어야 합니다. 복원력과 보안은 끊임없이 발전하고 있으며 정기적인 검토를 통해 Alcatel-Lucent Enterprise 통신 솔루션을 안전하고 가용성 있게 유지할 수 있습니다.

ALE 통신 솔루션은 설계 단계에서부터 안전하게 개발되었습니다. 즉, 당사는 제품을 정의하고 개발하며 고객에게 제공하는 모든 단계에서 보안을 고려합니다. 모든 하드웨어와 운영 체제가 강화되었으며 서비스 거부(DoS) 보호 기능이 내장되어 있습니다. 당사는 글로벌 보안 및 개인 정보 보호 표준(ISO 27001, ISO 27017, ISO 27018)에 대한 공인 인증 및 인가를 준수합니다. 또한 당사는 미국의 의료보험의 양도 및 책임에 관한 법률(HIPAA), 프랑스의 건강 데이터 호스팅을 위한 HDS(Hébergeurs de Données de Santé)와 같은 업계별 보안 및 개인 정보 보호 표준은 물론 유럽 연합의 일반 데이터 보호 규정(GDPR)과 같은 지역별 보안 및 개인 정보 보호 표준도 준수합니다.

통신 솔루션을 위한 6가지 모범 사례

다음은 ALE 통신 솔루션에 내장된 복원력과 보안을 완벽하게 최적화하는 데 도움이 되는 6가지 모범 사례입니다.

1. 최신 소프트웨어 버전이나 적절한 패치를 설치하여 향상된 최신 보안 기능으로 더 안전하게 보호해야 합니다.
2. 경보 모니터링 기능이 포함된 솔루션을 사용하는 것을 고려하고 적절한 임계값으로 정기적인 업데이트를 수행해야 합니다. 통신 시스템 장애나 품질 경고와 관련된 알림이 적절한 개인에게 전송되었는지 확인하십시오.
3. RADIUS 서버를 활용한 외부 인증을 사용하는 등 강력한 암호 정책을 검토하고 시행하십시오. 사용자 미리 알림을 구현하면 전화 요금 사기를 방지할 수 있습니다. 전화 요금 사기는 여전히 많은 국가에서 위협이 되고 있습니다.
4. 직원들을 대상으로 보안 인식 제고 교육을 실시하고 직원들이 위험과 예방 조치를 숙지하도록 하십시오.
5. 자동화된 원격 시스템 백업을 확보하여 구성 데이터가 손실되지 않도록 하십시오.
6. 음성용으로 특정 VLAN을 사용하는 것을 고려하십시오. 음성을 다른 트래픽과 분리하면 오염 가능성이 줄어들어 운영은 물론 정부 서비스가 중단되는 상황을 방지할 수 있습니다.

복원력 있고 안전한 통신 솔루션에 대한 투자

최근 몇 년 동안 글로벌 환경은 정부와 시민 사이에서 이루어지는 통신의 중요성을 부각시켰습니다. 정부 기관이 복원력과 보안을 강화하기 위해 통신 솔루션에 대한 투자를 계획할 때 고려해야 할 몇 가지 핵심 영역은 다음과 같습니다.

- 중복성과 복원력이 있는 아키텍처. 아키텍처는 완전한 중복성과 복원력이 있어야 합니다. 중요 지역에서 통화 서버를 복제하고 원격 사이트 중복성을 구현하며 중요 애플리케이션 서버를 복제하면 추가적인 보호 기능을 제공할 수 있습니다.
- Rainbow 및/또는 Alcatel-Lucent 시각적 알림 지원(VNA)을 사용하여 워크플로를 만들고 자동 트리거(사람, IoT, 시스템 트리거)를 설정하여 시스템 문제 발생 시 사람들에게 알려 신속하게 조치를 취하고 복구 프로세스를 가속화할 수 있도록 하십시오.
- 강력한 암호화를 구축하십시오. 암호화는 음성 품질 및 성능에 영향을 미치지 않고 솔루션에 기본적으로 설계된 업계 표준을 기반으로 합니다.

- ALE 통신 솔루션을 보완하는 데 적합한 협업 도구인 Alcatel-Lucent Enterprise의 Rainbow™를 구현하십시오. Rainbow는 음성, 영상, 인스턴트 메시징 등 포괄적인 기능 세트를 제공하여 원활한 통신과 효율적인 협업을 지원합니다. Rainbow를 사용하면 이미지, 영상, 비디오 감시 피드를 교환하여 상황별 인식을 강화하고 더 나은 의사 결정을 내릴 수 있습니다. Rainbow는 또한 온프레미스와 클라우드가 서로 안전하게 연결되는 하이브리드 통신을 제공합니다. 이 하이브리드 통신은 복원력 있는 통신을 보장하여 Rainbow를 통해 동료와 고객과의 연결을 유지하고 어려운 상황에서도 중단 없는 연결을 제공합니다. 하이브리드 통신은 또한 클라우드와 온프레미스 운영이 서로 다른 위치에서 수행되어 궁극적인 복원력을 제공함으로써 통신을 유지할 수 있다는 장점이 있습니다.
- 보안 요구 사항이 더욱 엄격한 기관의 경우 Rainbow Edge는 프라이빗 클라우드 인스턴스를 기반으로 한 온프레미스 대안을 제공합니다. 이 인스턴스는 모든 데이터 센터에서 호스팅될 수 있으므로 서버, 스토리지, 네트워크를 완벽하게 제어할 수 있으며 기관에서는 요구 사항에 맞게 인프라를 맞춤화하고 구성할 수 있습니다. 개인화된 보안 정책을 구현하고 리소스를 자율적으로 관리할 수 있습니다. 이와 같은 수준의 제어 기능은 인프라에 대한 완전한 가시성과 권한을 제공하여 기관이 정보에 입각한 결정을 내리고 목표에 맞춰 성능을 최적화할 수 있도록 지원합니다.
- 안전한 분산형 인력 통신 전략을 정의하십시오. ALE는 다음과 같이 분산된 직원, 모바일 직원, 재택근무 직원을 위한 다양한 통신 및 협업 옵션을 제공합니다.
  - Rainbow
  - IP 데스크톱 소프트폰
  - ALE 소프트폰
  - VPN이 내장된 데스크폰 및 내장된 보안 기능(VPN)을 통해 대량 배포 가능

사람과 자산 보호

ALE는 유연하고 안전하며 가용성이 높은 실시간 통신 및 알림 시스템을 제공합니다. 이러한 솔루션은 공공 안전 또는 스마트 시티 제어 센터 운영과 통합될 수 있으며 통화 배정 및 우선순위 지정을 간소화하고, IoT 데이터와의 상황별 정보 교환을 용이하게 하고, 긴급 대응자와 다양한 이해관계자 간의 협업 노력을 강화하여 더 나은 의사 결정과 조정을 가능하게 합니다.

건물, 장소, 도시 내에서 IoT 장치를 상호 연결하는 기능은 분석 및 AI와 결합되어 통신 환경을 근본적으로 변화시키고 있습니다. 센서, 비디오 감시, Rainbow 워크플로 및 AI를 통합하면 사후 대응적 접근 방식에서 사전 예방적 접근 방식으로 전환할 수 있으므로 시간과 비용 측면에서 프로세스 효율성이 향상됩니다. 이러한 통합은 상황을 전체적으로 이해할 수 있도록 촉진하고 의사 결정 과정을 지원하며 결과적으로 비상 대응 시간을 단축합니다. 또한 자산 추적 및 스마트 잠금장치와 조명 제어와 같은 기능을 통해 운영이 간소화됩니다. 더욱이 통신 내용과 작업을 기록하는 기능은 사후 분석을 단순화하여 보안 프로세스를 강화하고 잠재적인 책임을 완화합니다. 이러한 발전을 이루기 위해서는 어디에서나 접속 가능한 Wi-Fi와 간편한 IoT 온보딩을 지원하는 통신 환경이 매우 중요합니다.

시간에 민감하고 안전하며 가용성이 높은 실시간 통신 플랫폼의 경우 원활한 운영을 보장할 수 있는 견고한 인프라가 필수적입니다. 기술 인프라에는 적절한 소프트웨어, 고가용성 네트워킹 프로토콜과 에코시스템에 원활하게 통합되고 제한된 공기 흐름, 충격, 기상 이변 등 혹독한 환경 조건을 견딜 수 있는 견고한 네트워크 스위치를 통합하기 위한 유연성이 포함되어야 합니다. 견고한 장비를 선택하면 견고하지 않은 장비는 내구성이 떨어질 수 있는 혹독한 환경에서도 오랫동안 사용할 수 있습니다.

물리적 보안 시스템 분야에서는 위험이 더 높습니다. 매 분과 모든 영상은 당국이 위법 행위를 식별하거나, 사고 근원을 파악하거나, 재해 원인을 이해하는 데 매우 중요한 역할을 할 수 있습니다. 강력한 비디오 감시 인프라가 필수적입니다.
네트워킹 인프라는 감시 카메라에 충분한 대역폭과 PoE(Power over Ethernet)를 제공할 뿐만 아니라 비디오 감시 관리 시스템과도 원활하게 통합되어야 합니다. 이러한 통합은 원활한 운영과 손쉬운 문제 해결을 통해 효율적이고 안정적인 감시 네트워크를 보장합니다. 운영 팀은 특히 모든 비디오 프레임이 중요한 환경에서 모든 영상 문제를 신속하게 해결할 수 있어야 합니다.Alcatel-Lucent OmniSwitch® 솔루션 통합은 주요 비디오 관리 시스템과의 플러그인을 통해 이루어지며 이를 통해 이 중요한 목표를 달성할 수 있습니다.

게다가 조직 내에서 자산을 추적하거나 개인 또는 장비의 위치를 찾아야 하는 상황이 발생할 수 있습니다. 효과적인 자산 추적 솔루션은 사람과 자산의 위치를 쉽고 정확하게 찾을 수 있는 능력에 달려 있습니다. 이러한 시스템은 또한 개인의 위치가 파악되면 신속하게 지원 인력을 파견할 수 있도록 하여 안전과 보안을 강화합니다. Alcatel-Lucent OmniAccess® 자산 추적 솔루션을 사용하면 직원과 장비의 위치를 빠르게 찾아 평면도 맵에 표시할 수 있습니다. 자산 추적은 또한 사용 패턴 정보를 제공합니다. 자산을 과도하게 활용하거나 충분히 활용하고 있지 않는지를 아는 것은 귀중한 정보를 제공할 수 있습니다.

데이터 주권 및 보안

Alcatel-Lucent Enterprise는 종단 간 사이버 보안에 필요한 모범 사례를 구현하는 데 있어 다른 테크벤더보다 앞서 있습니다. ALE는 다음과 같은 기업입니다.

- 새로운 기능에 대한 위험 평가를 수행하고 솔루션에 기본 암호화와 같은 사이버 보안 기능을 구현할 때 국립과학기술원(NIST) 모범 사례와 권장 사항을 따릅니다.
- 공통 기준 EAL2+ 인증을 받았습니다.
- 모든 클라우드 기반 솔루션에 ISO 27001 표준을 적용합니다.
- ZTNA, 세분화된 네트워크 분할, 매우 구체적인 보안 정책을 지원하여 무단 활동 발생 위험을 최소화합니다.
- 당사 제품을 대상으로 침투 테스트와 같은 고도로 전문화된 보안 관련 테스트를 실시합니다.
- HDS, HIPAA, 가족의 교육권 및 프라이버시에 관한 법률(FERPA) 등 당사 제품이 주요 산업 인증을 획득하도록 보장합니다.
- ALE International은 유럽 연합 네트워크 및 정보 보안 지침(NIS 2)을 준수합니다.

당사는 공인된 사이버 보안 전문가로서 유럽 연합의 사이버 보안 지침 제안에 기여하고 있습니다. 또한 사이버 보안 전문 지식을 활용하여 고객이 고유한 요구 사항에 맞는 안전한 통합 통신 및 협업 솔루션의 적절한 조합을 선택하고 구현할 수 있도록 돕고 고객사 직원을 대상으로 사이버 보안 모범 사례에 대한 교육을 실시합니다.

Alcatel·Lucent Enterprise