기업을 위한 Alcatel-Lucent Enterprise 사이버 보안

브로슈어

Alcatel·Lucent
Enterprise

개요

사이버 보안은 오랫동안 기업에게 최우선 과제였습니다. 그러나 디지털 전환이 일어나면서 사이버 보안 요구가 변화하고 있습니다. 디지털 혁신을 통해 조직은 네트워크에서 더 많은 연결 및 모바일 장치를 사용하는 한편, 직원들은 네트워크 경계를 넘어 애플리케이션과 데이터에 점점 더 많이 액세스하고 있습니다.

전환이 가속화됨에 따라 기존의 네트워크 보안 방법은 더 이상 이를 따라갈 수 없게 되었습니다. 이 문서는 오늘날의 엔터프라이즈 사이버 보안 요구 사항을 변화시키는 힘에 대한 통찰력을공유하고 디지털 전환 시대에 데이터와 시스템을 안전하게 유지하기 위해 기업이 채택할 수있는 전략과 기술에 대한 제안을 하고 있습니다.

Alcatel-Lucent Enterprise 사이버 보안 솔루션은 디지털 방식으로 전환되는 기업의 요구 사항을 충족합니다. 사이버 보안에 대한 다각적 접근 방식을 통해 기업은 엔터프라이즈 에코시스템 전반에서 연결된 장치, 보안 데이터 및 소프트웨어 애플리케이션에 대한 정책 기반 액세스를 제공할 수 있습니다.

변화하는 챌린지

사이버 보안 위협의 성격은 변화하고 있습니다. 해커는 인공 지능(AI)과 머신 러닝(ML)을 사용하여 보다 정교하고 자동화된 공격을 만들고 있습니다. 새로운 사회 공학 기술을 통해 범죄자들은 소셜 미디어에서 발견된 정보의 조각들을 연결하여 개인 또는 조직이 보유한 데이터의 프로필을 만들 수 있습니다.

엔터프라이즈 디지털 트랜스포메이션은 사이버 보안 요구 사항에도 영향을 미치므로 복잡성이 커지고 연결된 장치의 사용이 늘어남에 따라 경계선 또한 사라지고 있습니다.

더 많은 장치, 증가하는 복잡성

기업은 클라우드, 모바일, IoT, 빅 데이터 및 고급 분석을 포함한 새로운 기술을 채택하고 있습니다. 이러한 새로운 솔루션은 보안을 살펴볼 수 있는 새로운 방식이 필요한 새로운 차원의 복잡성을 초래 합니다. 또한 연결된 장치의 수가 증가함에 따라 취약성 및 보안 위반의 가능성도 높아집니다.

예를 들어, 대부분의 경우 1세대 연결된 장치에는 암호가 필요하지 않았습니다. 장치가 네트워크에 연결되어 있기 때문에 해커는 이를 네트워크의 게이트웨이로 사용할 수 있습니다. 오늘날 하드 코딩된 암호와 같은 보안 기능은 장치에 의무화되는 경우가 많지만 침해는 불가피하며 해커가 네트워크에 계속 액세스할 수 있습니다.

소실된 방어선

대부분의 조직은 오랫동안 네트워크 내부와 외부의 사용자와 리소스를 명확하게 구분했습니다. 그러나 조직이 디지털 혁신을 수용함에 따라 통합 협업 환경의 다른 파트너 및 공급자를 포함하여 광범위한 생태계와의 교류에 더 개방적으로 변하고 있습니다. 사용자는 더 이상 네트워크 경계 내부에서 리소스에 액세스하지 않고 어디에서든 사용할 수 있습니다. 다른 네트워크의 연락처와 정보를 교환할 수 있습니다. IT 리소스도 더 이상 기업 경계 내에서 제한되지 않습니다. 온프레미스 및 클라우드에 있을 수 있으며 API를 사용하여 연결할 수 있습니다. 기업은 경계가 더 이상 존재하지 않을 때 자원을 보호할 수 있는 새로운 방법을 필요로 합니다.

제로 트러스트 세상에서 매크로 및 마이크로 세분화

세분화에는 매크로와 마이크로의 두 가지 종류가 있습니다. 매크로 세분화에서는 물리적 네트워크가 서로 다른 논리적 세그먼트로 분할됩니다. 모든 기업은 세그멘테이션을 사용하지만 보안상의 이유로 항상 그런 것은 아닙니다. 매크로 세분화는 확장성, 관리 또는 조직의 목적을 위해 사용되는 경우가 많습니다. 이 세그먼트는 VLAN+VRF의 조합인 VLAN이 될 수 있으며 최단 경로 브리징, MPLS 또는 VXLAN 또는 GRE 터널과 관련 될 경우 VPN이 될 수도 있습니다. 서로 다른 세그먼트의 사용자 또는 장치 간 트래픽은 물리적 방화벽에 의해 제어됩니다. 두 장치가 서로 다른 VLAN에 매핑되어 방화벽을 통과하지 않고 통신할 수 있는 경우 동일한 매크로 세그먼트에 있게 됩니다. 예를 들어 카메라 및 도어락은 액세스 보안 그룹의 제어에 해당되는 반면 항온기의 경우 건물 유지 관리 그룹의 제어에 속할 수 있습니다.

마이크로 세분화는 한 걸음 더 나아갑니다. 모든 사용자가 동일하지는 않으며 사용자 모두가 모든 리소스에 액세스할 필요가 있는 것은 아닙니다. 사용자를 세그먼트에 매핑하는 동일한 프로필에는 HR 또는 Finance와 같은 역할마다 다른 사용자/장치 권한에 대한 세부적인 제어를 추가하는 정책 집합도 포함됩니다. 이를 '역할 기반 액세스'라고 하며, '최소 특권 원칙'과 직접 관련이 있습니다. 따라서 카메라와 도어락이 모두 같은 세그먼트에 있더라도 동일한 리소스를 사용할 필요가 없습니다. 카메라는 비디오 레코더, 서버 및 도어락과 통신해야 합니다. 도어록이 다른 도어락과 통신할 필요가 없기 때문에 카메라가 도어록과 통신할 필요는 없습니다. 이러한 세분화된 권한은 프로파일의 일부이며 인증 후 디바이스에 동적으로 적용되는 정책을 통해 구현됩니다.

문제는, 둘 다 정말 필요한 것일까요? 매크로 세분화 전용 접근 방식을 사용하는 문제는 방화벽에서 모든 VLAN을 종료해야 하고 성능 문제가 발생하기 때문에 방화벽에 병목 현상이 발생한다는 것입니다. 또는 배포 계층에 더 많은 방화벽을 배포할 수 있지만 성능 측면에서 보면 비용이 많이 들기 때문에 여전히 좋은 선택이 아닐 수 있습니다. 또한 방화벽이 많을수록 정책 적용 지점이 여러 개 있고 최신 상태의 정책이 유지돼야 하는 곳이 여러 개 발생하게 됩니다.

마이크로 세분화만으로도 문제가 될 수 있습니다. NAC(네트워크 액세스 제어) 정책을 통해 유일한 정책 적용이 수행되면 정책 목록이 길고 복잡해지고 장치 용량 제한을 소모시킬

수 있습니다. 이러한 두 유형의 세그멘테이션 간의 균형을 유지하면 방화벽이 서로 다른 세그먼트 간의 트래픽(수직)을 제어할 수 있으며 NAC 정책은 지정된 세그먼트(측면) 내의 트래픽을 제어합니다. 매크로 및 마이크로 세분화를 결합하여 한 보안 세그먼트에서 다른 보안 세그먼트로 유출되는 보안 위협과 동일한 세그먼트에서 옆으로 이동하는 보안 위협에 대처할 수 있습니다.

네트워크 보안에 대한 제로 트러스트 접근 방식 측면에서, 기본 원칙은 '공격자가 이미 존재하는 것처럼 행동하기'입니다. 즉, 모든 연결을 인증하는 것입니다. 어떠한 자산이나 사용자가 있다면 본질적으로 신뢰할 수 있어야 합니다. 온프레미스든 사내에 있든 상관없이 동일한 확인을 거쳐야 합니다. 내부 사용자라고 해서 무조건 신뢰할 수는 없습니다. 모든 액세스가 인증됩니다.

네트워크가 기업 주변에 지어진 요새로 여겨지는 전통적인 보안 접근 방식을 고려한다면 요새는 방화벽을 나타내므로 외부의 모든 것은 신뢰할 수 없기 때문에 면밀히 조사될 것이고, 내부의 모든 것은 암시적으로 신뢰되고 허용됩니다. 그러나 마이크로 세분화, 특히 소프트웨어 정의 마이크로 세분화는 한 걸음 더 나아갑니다. 요새와 건물 주변의 보안 외에 인증이 필요한 경비원도 존재 합니다. 이 신뢰 경계는 흐릿하고 분산되어 있으며 모바일입니다. 특정 위치, 스위치 포트 또는 VLAN과 연결되어 있지 않습니다. ID, 장치, 상황 및 시간에 따라 다릅니다. 이것이 소프트웨어 정의이고 즉시 조정이 가능합니다. 이 접근 방식의 핵심은 구성 요소가 관리되고 워크플로우의 위협이나 변화에 대응하기 위해 필요에 따라 대응하고 재구성할 수 있어야 한다는 것입니다.

진화하는 기업을 위한 솔루션

Alcatel-Lucent Enterprise는 여러 계층의 보호를 통해 연결된 장치 및 애플리케이션에 대한 심층적인 보안을 제공하는 엔터프라이즈 사이버 보안에 대한 다각적 접근 방식을 제공합니다.

유연한 연결성

당사의 접근 방식은 디지털 혁신을 촉진하는 수많은 연결된 사용자, 장치 및 애플리케이션에 대해 네트워크 및 사이버 보안 정책을 빠르고 쉽게 구성할 수 있는 유연한 자율 네트워크부터 시작합니다.

과거에는 IT가 중단/수정 작업을 수행했습니다. IT 부서는 새로운 장비를 설치하고 가동하며 지루한 수동 프로세스를 사용하여 네트워크를 관리해 왔습니다. Alcatel-Lucent Enterprise 디지털 에이지 네트워킹은 사용자 및 장치를 특정 애플리케이션에 쉽고 안전하게 연결할 수 있는 스마트하고 자동화된 네트워크를 제공합니다. ALE Interlligent Fabric(iFab) 기술을 사용하여 구축된 디지털 에이지 네트워킹은 iFab와 업계 표준의 최단 경로 브리징 (SPB) 을 결합합니다. 이러한 기술은 네트워크 생성 및 구성을 단순화하는 동시에 빠른 다중 경로 라우팅 및 링크 집계를 통해 여러 네트워크 연결을 병렬로 결합하여 처리량을 높이고 이중화를 제공합니다.

IT 팀은 당사 솔루션을 통해 네트워크 서비스, 아키텍처, 액세스 정책, IoT 컨테이너를 정의하고 네트워크를 자동으로 구축할 수 있습니다. 네트워크 설계 후 이동, 변경 또는 추가가 필요한 경우 네트워크는 필요한 조정을 자동으로 적용하고 이로인한 변화를 감지할 수 없게 합니다. 예를 들어 스위치가 사용 중단되면 네트워크가 해당 스위치를 중심으로 자동으로 다시 라우팅 됩니다.

기업들은 자율 네트워크를 사용하여 수동 구성 오류를 줄이고 조직 내에서 빠르게 변화하는 속도를 따라갈 수 있도록 자동화의 이점을 누릴 수 있습니다. 자동화는 수작업을 없애기 때문에 IT는 더 많은 비즈니스 엔진 동력이 될 수 있습니다.

지능적이고 자동화된 정책을 통한 액세스 제어

기업은 Digital Age Networkwork를 사용하여 사용자가 액세스하고 사용할 수 있는 애플리케이션과 장치를 제어하는 사용자 액세스 규칙과 정책을 정의하고 사용자가 어디를 가든

사용자를 팔로우할 수

- 특정 시스템
- 인터넷 서비스
- 계약자 기반 정책에 따른 기타 파트너

또한 ALE에서는 실내 길 찾기 탐색, 자산 및 인력 추적과 같은 위치 기반 서비스를 제공하여 조직이 사용자 위치를 고려한 정책을 설정할 수 있습니다.

UPAM(통합 정책 액세스 관리) 기능은 사용자가 연결할 때마다 자동으로 정책을 적용하므로 사용자가 허용된 액세스 권한만 갖도록 합니다. 사용자가 장치를 사용하여 네트워크에 로그인하고 자격 증명이 확인되면 다시 인증할 필요가 없습니다. 장치가 켜져 있고 시스템에서 자동으로 해당 사용자에 대한 정책을 적용하는 경우 사용자는 연결 상태를 유지할 수 있습니다.

정책을 통해 조직 내부 또는 외부의 모든 사용자가 허용된 영역에만 액세스할 수 있으며 액세스 제어가 일관되게 적용됩니다. 이는 사이버 보안을 강화하는 동시에 엔터프라이즈 워크플로우를 간소화 합니다. 사용자는 번거로운 보안 로그인 절차 없이 필요한 시스템과 정보에 신속하게 액세스할 수 있습니다.

장치의 취약성 감소

기업은 많은 IoT 장치에 연결 됩니다. Alcatel-Lucent 엔터프라이즈 디지털 에이지 네트워킹 솔루션을 사용하면 조직이 각 장치를 컨테이너화하여 가상 네트워크 세그먼트를 만들어 모든 장치가 공격 지점이 되는 것을 방지할 수 있습니다. 디지털 에이지 네트워킹의 컨테이너화를 통해 단일 물리적 네트워크에서 여러 가상 네트워크를 만들 수 있으며 IT 부서의 구현이 간편하며 단일 관리 시스템으로 관리할 수 있습니다. 이 솔루션은 네트워크의 각 장치를 자동으로 검색합니다. 장치가 네트워크에 연결되면 온프레미스 또는 클라우드에서 사용할 수 있는 Alcatel-Lucent OmniVista® 네트워크 관리 시스템은 장치를 식별하려고 시도합니다. 관리 시스템에 해당 장치가 데이터베이스에 없는 경우 2억 2천만 개 이상의 장치로 구성된 클라우드 기반 데이터베이스를 참조합니다.

예를 들어, 장치가 식별되면 시스템은 보안 카메라로 분류합니다. 해당 장치가 보안 카메라에 대해 승인된 공급업체 목록에 있는 경우 네트워크에 연결됩니다. 그렇지 않으면 연결되지 않을 것입니다. 그런 다음 장치의 가상 컨테이너에 솔루션이 설정되고 나머지 네트워크에서 세그먼트화 됩니다.누군가 네트워크로 연결된 장치를 해킹하면 해당 공격자는 해당 장치를 사용하여 나머지 네트워크에 액세스할 수 없습니다.

신뢰할 수 있는 환경을 위한 인공 지능

장치가 연결되면 위협을 식별하고 신뢰를 유지하기 위해 장치를 지속적으로 모니터링해야 합니다. ALE 분석 및 애플리케이션 가시성을 통해 네트워크 관리자는 장치별로 네트워크에서 어떤 일이 벌어지고 있는지 확인할 수 있습니다. 애널리틱스는 정상적으로 예상되는 네트워크 동작과 비정상적인 패턴이 발생할 때의 차이를 식별합니다. 네트워크 에지에서 응용 프로그램의 동작을 모니터링하여 애플리케이션에 연결할지 여부를 결정하고 허용된 애플리케이션에서 비정상적인 동작(예: 필요한 것보다 많은 데이터를 생성하는 비디오 카메라)을 감지할 수 있습니다.

장치에서 이상 또는 비정상적인 동작이 발생하면 네트워크 보안 관리자가 개입할 수 있도록 애널리틱스에서 표시를 하게 됩니다. 현재 조사는 수동으로 수행되어야 하지만 ALE는 AI와 ML을 사용하여 응답을 자동화하기 위해 노력하고 있습니다.

네트워크 보안

오늘날 조직은 네트워크에서 IoT 디바이스를 보호해야 할 필요성을 인식하고 있지만 스위치 및 액세스 포인트와 같이 네트워크의 기반을 형성하는 디바이스를 고려하지 못할 수 있습니다. Alcatel-Lucent Enterprise는 이러한 장치의 위협을 줄이기 위해 많은 기술을 사용합니다. ALE 솔루션:

- OS 소프트웨어를 강화하여 안전하고 다양한 코드 제공
- 써드파티 검증 및 인증을 위해 OS 소프트웨어를 전송하여 간편한 진입 지점이나 백도어가없는지 확인합니다.
- 스위치가 부팅될 때마다 메모리가 컴파일되고 다른 방식으로 나타나는지 확인합니다.스위치가 동일하게 작동하지만 내부적으로 두 개의 메모리 구성이 동일하진 않습니다. 누군가ALE 스위치에 침입 한다면 같은 방식으로는 다른 스위치에 액세스할 수 없습니다.
- DoS(Denial of Service) 보호 기능 내장 CPU는 비정상적인 양의 네트워크 트래픽을 감지하고필요한 경우 CPU를 자동으로 종료할 수 있습니다.
- JDIC 및 FIPS와 같은 여러 보안 인증
- 지속적인 소프트웨어 업그레이드 수행

수신 및 발신 트래픽에 대한 보안 연결

유입 트래픽의 경우 ALE의 VPN은 로컬 네트워크에 대한 암호화된 연결을 제공하는 반면 종단 간 트래픽은 MACsec 암호화(IEEE 802.1AE라고도 함)를 사용하여 보호되어 네트워크를 통과할 때 정보를 보호하고 재부팅 없이 TLS 및 HTTPS와 같은 서비스를 다시 로드해도 네트워크가 중단되지 않습니다.

보고

ALE 보고를 통해 서로 다른 사람이 네트워크의 상태, 상태 및 성능, 애플리케이션 실행 방식, 사용자 만족도에 대한 정보에 액세스할 수 있습니다. 예를 들어 IT 부서에서 네트워크 성능 및 운영에 대한 데이터를 볼 수 있습니다.

사업부(Line of Business)는 센서 또는 원격 측정 시스템과 같은 장비가 서버와 태블릿에 데이터를 원활하게 전송하도록 보장할 수 있습니다. IT 부서는 직원이 업무를 수행하는 데 더 많은 시간을 할애할 수 있도록 네트워크가 서비스를 제공하고 있는지 여부와 네트워크를 최대한 활용하고 있는지 여부를 결정할 수 있습니다.

산업 별 사이버 보안

교육

교육 기관이 스마트 캠퍼스 전략을 채택함에 따라 더 많은 연결 및 모바일 장치가 네트워크에 추가되고 IoT(사물 인터넷) 기기가 네트워크 경계를 넘어 애플리케이션과 데이터에 점점 더 액세스하게 될 것입니다.

대규모 캠퍼스 인프라에서 연결성과 혁신이 구현됨에 따라 사이버 위협에 즉시 취약해집니다. 스마트 캠퍼스를 위한 Alcatel-Lucent Enterprise 디지털 에이지 네트워킹은 오늘날의 디지털 혁신 시대에 IT 자산과 데이터를 안전하게 보호합니다. 이 솔루션을 통해 교육기관은 사용자 액세스를 면밀히 관리하고, IoT, 모바일 및 네트워크 장치로 인해 발생하는 취약성을 줄이며 피할 수 없는 침해가 공격 지점을 제공하지 못하도록 하는 동시에 학생과 직원이 요구하는 서비스와 애플리케이션을 지원할 수 있습니다.

교통

기술 혁신으로 인한 운송 시스템의 발전은 기존에 구축된 기반을 기본으로 해서 전환 되어야 할 것입니다. 모든 운송 생태계가 작동하도록 지원하는 장치와 시스템을 통합하려면 빠르고 안정적이며 안전한 연결이 필요합니다. 센서, 카메라, 표지판 및 교통 통제 시스템을 원활하게 연결하려면 교통 데이터 네트워크가 IoT를 인식해야 합니다. 또한 네트워크 보안은 데이터와 네트워크의 무결성을 보호하는 데 매우 중요합니다.

ALE는 보안 다각화된 코드를 사용하여 네트워크 무결성을 개선하고 네트워크 사이버 공격에 대한 보안을 강화합니다. CodeGuardian은 내재적 취약성, 코드 악용, 내장형 멜웨어 및 임무 수행에 필수적인 동작을 저해하는 잠재적 백도어 공격으로부터 네트워크를 보호합니다. ALE는 또한 IoT에 대한 핑거 프린팅을 제공하여 차량, 센서 및 카메라를 포함한 각 장치를 식별하여 네트워크에 보안 위협을 가하지 않도록 합니다. ALE 심층 보안 전략은 공통 기준(EAL2 및 NDCPP), JITC, FIPS 140-2 및 NIST를 포함한 정부 기관으로부터 최고 수준의 인증을 받았습니다.

헬스케어

헬스케어는 해커가 가장 많이 목표로 삼은 산업 중 하나였으며, 여전히 그렇습니다. 그리고 문제는 계속 커지고 있습니다. Protenus Breach Barometer에 따르면 2018년에 헬스케어 산업은 총 503개의 breach를 통해서 1500만 건의 환자 기록이 침해 받았고 이는 2017년 대비 세 배에 달하는 기록이라고 밝혔습니다.[1]

의료 데이터는 매우 중요하기 때문에 데이터 침해가 발생하곤 합니다. 개별 환자 기록에는 이름, 현재 및 이전 주소, 근무 기록, 개인 친척의 이름 및 연령, 신용 카드 및 은행 번호와 같은 재무 정보를 포함한 모든 정보가 포함됩니다.[2]

ALE 디지털 에이지 네트워킹은 헬스케어 생태계 전반에 걸쳐 연결된 의료 기기, 환자 데이터 및 소프트웨어 애플리케이션에 대한 안전한 정책 기반 액세스를 통해 신뢰를 유지하는 사이버 보안에 대한 다각적 접근 방식을 제공합니다.

정부

중앙 정부와 도시 차원에서 디지털의 역할이 확장됨에 따라 교통, 인프라 유지 보수 및 환경 모니터링을 지원하는 디지털 자산의 보호가 취약해 지고 있습니다. 데이터 보안, 취약성 및 신뢰도 관리에 대한 정부 사이버 보안 정책을 수정해야 합니다.

사이버 보안에 대한 ALE 접근 방식은 네트워크에서 소프트웨어에 이르기까지 서비스의 모든 계층을 보호하기 위해 엔드 투 엔드, 서비스 중심 보안 접근 방식을 제공합니다. 장치 측면에서 공공 부문 조직은 컨테이너화를 사용하여 장치가 공격 지점이 되는 것을 방지하기 위해 가상 네트워크 세그먼트를 만들 수 있습니다.

호스피탈리티

IoT의 성장과 함께 센서 및 연결된 장치의 확산이 네트워크 공격 가능성을 크게 증가시킴에 따라, 사이버 보안 위협의 폭발이 예상되고 있습니다. 많은 IoT 장치가 보안을 염두에 두지 않고 제조되거나 현재의 보안 요구 사항을 이해하지 못하는 회사에 의해 구축되기 때문에 IoT가 특히 보안에 취약할 수 있습니다. 결과적으로, IoT 시스템은 점점 더 기업 보안의 약한 연결 고리가 되고 있습니다.

이를 위해서는 여러 보안 보호 장치를 활용하는 전략적 접근 방식이 필요합니다. 호텔, 카지노, 리조트 및 기타 호스피탈리티 비즈니스가 이점을 활용하고 IoT 배포의 위험을 완화할 수 있도록 ALE는 개별 사용자 및 장치에서 네트워크 계층에 이르기까지 인프라의 모든 계층에서 보호 기능을 제공하는 다단계 보안 전략을 제공합니다. 또한 장치 온보딩을 간소화 및 보호하고 시스템을 적절하고 효율적으로 실행하는 데 적합한 네트워크 리소스를 제공하는 IoT 억제 전략을 제공하여 사이버 공격으로부터 조직을 보호할 수 있습니다.

1 https://healthitsecurity.com/news/the-10-biggesthealthcare-data-breaches-of-2019-so-far

2 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-tohackers/#2bb1f96b50cf

요약

연결된 장치의 수가 증가하고 네트워크 경계가 사라지고 변화가 계속 가속화됨과 동시에 디지털 변환은 엔터프라이즈 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.