비용 효율적인 제로 트러스트 네트워크 구축

네트워크 보안 극대화 및 비용 최소화

솔루션 개요

Alcatel·Lucent Enterprise

사이버 보안과 제로 트러스트

기술이 지속적으로 발전하고 사이버 위협의 수와 복잡성이 계속 증가함에 따라 사이버 보안은 점점 더 중요한 관심사가 되고 있습니다. 빠르게 진화하는 위협으로 인해 조직이 위협을 예측하고 방어하기가 어려워지고 있으므로 사이버 보안 전문가는 최신 동향과 취약성에 대한 최신 정보를 유지해야 합니다.

피싱 이메일, 사회 공학, 소프트웨어 취약점 등 소스와 공격 벡터가 다양하기 때문에 사이버 위협을 방어하려면 공격 유형별로 고유한 접근 방식이 필요합니다.

복잡한 시스템에서 모든 잠재적인 취약성을 식별하고 보호하는 것은 어려울 수 있으므로 사이버 보안 전문가는 다양한 시스템과 네트워크가 어떻게 협력하여 효과적인 보안 조치를 개발하는지 이해하는 것이 중요합니다.

사람의 실수는 사이버 보안을 위반하는 흔한 원인이며, 2025년에는 인재 부족이나 사람의 실수가 심각한 사이버 사고의 절반 이상을 차지할 것으로 추산됩니다.[1]

GDPR(일반 개인정보 보호법) 및 HIPAA(의료보험의 양도 및 책임에 관한 법률)와 같은 복잡한 사이버 보안 규정 및 표준을 충족하는 것은 전문 지식과 전문가가 필요한 또 다른 과제입니다.

1 Gartner®는 2023년을 예측합니다. 사이버 보안 업계는 사람간 거래에 주목합니다 | Bitsight, 2023년 1월.

사이버 보안 침해 프로세스

다음 그림은 사이버 공격자가 네트워크에 침입하여 귀중한 데이터를 훔치는 단계를 보여줍니다. 이는 공격자가 대상을 조사, 식별 및 선택하고 네트워크 취약성을 검색하는 정찰로 시작됩니다.

다음 단계는 공격자가 대상 엔드포인트를 손상시키고 무기화된 페이로드를 전달하는 방법을 결정하는 무기화 단계입니다.

그런 다음 공격자가 무기화된 페이로드를 트리거하고 손상된 엔드포인트에 대한 권한을 상승시켜 네트워크를 가로질러 측면 이동하는 악용이 발생합니다.

다음 단계는 공격자가 원격 셸 액세스를 설정하고 말웨어를 설치하여 지속성을 설정하는 설치 단계입니다.

명령 및 제어 단계에서 공격자는 명령 및 제어 서버에 대한 암호화된 통신 채널을 설정하여 원격으로 공격을 지시하고 목표를 실행합니다.

마지막 단계는 측면 이동 및 유출로, 공격자는 데이터 도난, 중요 시스템의 파괴 또는 수정, 서비스 거부 등 다양한 목표를 가질 수 있습니다.

공격자를 막는 열쇠는 공격 수명주기의 다양한 단계를 조기에 감지하고 진행을 방해하는 것입니다.

이를 방지하려면 취약성 및 패치 관리, 말웨어 탐지 및 예방, 위험한 애플리케이션 및 서비스 차단, 모든 네트워크, 엔드포인트는 물론 클라우드 활동 로깅 및 모니터링과 같은 다양한 조치를 취해야 합니다.

네트워크 측면에서는 애플리케이션을 세부적으로 제어하고 제로 트러스트 모델에서 영역 또는 세그먼트 간 트래픽을 모니터링하는 기술을 구현해야 합니다. 제로 트러스트는 기본적으로 모든 것을 신뢰할 수 없는 것으로 간주해야 한다는 원칙에 따라 작동합니다.

제로 트러스트 개념은 컴퓨터 네트워크에 대한 정교한 사이버 공격이 증가함에 따라 개발되었습니다. 기존 조직에서는 네트워크를 보호하기 위해 방화벽, 바이러스 백신 소프트웨어 등의 경계 기반 보안 솔루션에 의존해 왔습니다. 그러나 사이버 공격이 더욱 지능화되고 복잡해짐에 따라 이러한 경계 기반 솔루션은 충분하지 않은 것으로 입증되었으며, 대신 리소스에 대한 액세스 권한을 부여하기 전에 모든 액세스 요청을 확인하고 인증해야 합니다.

출처: XDR for Dummies, Palo Alto Networks Special Edition, 2022(입문자를 위한 XDR, Palo Alto Networks 특별판, 2022)

제로 트러스트 전략 발전

Alcatel-Lucent Enterprise는 단순성과 비용 효율성을 바탕으로 고객이 보안을 강화하고 제로 트러스트 환경으로 전환할 수 있도록 지원합니다. ALE에서는 고객의 네트워크 및 데이터 보안을 보장하기 위해 제로 트러스트 모델 구현의 중요성을 이해하고 있습니다. ALE는 조직이 제로 트러스트 네트워크를 구현하고 사이버 위협으로 인한 문제를 해결할 수 있도록 설계된 다양한 솔루션을 제공합니다.

네트워크 강화

ALE는 **내부 및 외부 모두에서 강화된 네트워크**를 제공합니다. 보안 인프라부터 시작하여 장치 자체가 손상되지 않도록 보장합니다. 당사의 Alcatel-Lucent OmniSwitch® 제품군은 안전한 Alcatel-Lucent 운영 체제(AOS)에서 실행됩니다. AOS는 안전하고 다양한 코드를 사용하여 잠재적인 취약점과 공격으로부터 네트워크를 보호합니다. 코드는 버퍼 오버플로 공격으로부터 보호하는 데 사용되는 ASLR(Address Space Layout Randomization)을 통한 소프트웨어 다양화를 통해 현재 및 미래의 위협을 해결하기 위해 지속적으로 업데이트됩니다. IV&V(독립적인 검증 및 확인)는 잠재적인 취약점, 백도어, 악성 코드 및 시스템 악용에 대해 AOS 소스 코드를 분석하고 테스트하는 데에도 사용됩니다. 타사 사이버 보안 전문가는 소프트웨어 무결성을 보장하기 위해 일반 가용성 소프트웨어 이미지에 대해 실행되는 이러한 테스트를 수행합니다.

제로 트러스트 네트워크 액세스를 보장하기 위해 매크로 및 마이크로 세분화를 적용합니다. 둘 다 제로 트러스트 보안 전략의 중요한 구성 요소입니다. **매크로 세분화**는 기능, 애플리케이션 또는 사용자 그룹을 기반으로 네트워크를 별도의 영역 또는 도메인으로 분할하는 것을 의미합니다. 이는 높은 수준의 네트워크 분할을 제공하여 조직이 중요한 자산과 리소스를 나머지 네트워크로부터 격리할 수 있도록 해줍니다. 반면, **마이크로 세분화**는 네트워크를 개별 사용자나 기기별로 보다 세부적으로 세분화하는 데 중점을 둡니다. 이 접근 방식은 네트워크 액세스에 대한 보다 세밀한 제어를 제공하므로 조직은 개별 사용자 또는 장치 수준에서 보안 정책을 시행할 수 있습니다.

SPB(최단 경로 브리징) 및 **UNP(범용 네트워크 프로파일)**는 네트워크의 매크로 및 마이크로 세분화를 지원하는 강력한 솔루션을 제공하여 범위를 제한하여 보안과 성능을 향상시킵니다

SPB는 대규모 네트워크에서 다중 경로 라우팅을 허용하는 동시에 네트워크 인프라의 구성 및 관리를 단순화하는 레이어 2 네트워크 프로토콜입니다. 가상 네트워크 분할과 같은 기능은 무단 액세스 및 사이버 공격에 대한 추가 보호 기능을 제공합니다. 네트워크 인프라에 SPB를 사용함으로써 조직은 향상된 네트워크 효율성과 보안의 이점을 누릴 수 있으며 자신감을 갖고 비즈니스 목표를 달성하는 데 도움이 됩니다.

ALE UNP는 네트워크 관리자가 ID, 위치 및 장치를 기반으로 네트워크 액세스를 위한 사용자 프로필을 생성하고 관리할 수 있게 해주는 강력한 Alcatel-Lucent Enterprise 스위치 기능인 프로필 기반 액세스 제어입니다. 중앙 집중식 네트워크 정책 관리를 구현하여 정책 구성 및 시행을 단순화할 수 있습니다. ALE UNP를 구현함으로써 조직은 네트워크 가시성, 보안 및 제어를 강화하는 동시에 네트워크 성능을 향상하고 자산을 보호하며 가동 중지 시간을 줄일 수 있습니다.

SPB와 UNP를 함께 사용하면 네트워크 관리자는 네트워크 인프라를 효율적으로 관리하고 보호하여 다음을 수행할 수 있습니다.

- **네트워크 전반에 걸쳐 일관되게 정책을 적용합니다.**
- **다른 장치에서 IoT 장치를 분할하고 격리합니다.**
- **네트워크의 공격 표면 최소화**

강력한 인증

ALE는 UPAM(통합 정책 인증 관리자)을 통해 강력한 인증을 제공합니다.

사이버 보안의 핵심 구성 요소는 사용자, 장치 또는 시스템의 신원을 확인하는 프로세스인 인증입니다. 여기에는 일반적으로 사용자 이름 및 비밀번호와 같은 특정 형태의 식별 정보를 제공하여 사용자 또는 장치가 자신이 주장하는 사람인지 확인하는 작업이 포함됩니다.

ALE 솔루션은 다양한 사용자 인증 방법을 지원합니다.

- 네트워크 인증 프로토콜인 **802.1X**를 사용하면 사용자 이름 및 비밀번호와 같은 자격 증명을 제공하여 기기가 보안 네트워크에 연결할 수 있습니다. 장치가 802.1X를 사용하여 네트워크에 연결을 시도하면 네트워크에 대한 액세스가 허용되기 전에 먼저 인증을 받습니다. 이상적인 환경에서는 장치가 802.1x를 통해 인증됩니다. 인증은 방화벽과 공유할 수 있는 기록을 생성합니다.
- 기기가 802.1x를 지원하지 않는 경우 **MAC 주소** 인증이 옵션을 제공합니다. MAC 주소는 네트워크에 있는 모든 장치의 디지털 ID 카드입니다. 이는 고유하며 각 장치를 식별하고 컴퓨터나 휴대폰의 이름표와 유사하게 장치 간의 통신을 허용합니다.
- ALE는 **기기 및 시스템 지문 인식**을 지원합니다. 다른 802.1X 또는 MAC 인증을 통해 반환된 프로필이 없으면 지문 채취를 시도합니다. 컴퓨터 보안에서 지문 인식은 OS, 소프트웨어, 개방형 포트 등 장치나 시스템에 대한 정보를 수집하여 이를 식별 및 분류하고 잠재적인 위험과 취약성을 평가하는 프로세스입니다. IoT 인벤토리 데이터베이스에 등록된 장치의 프로필에 매핑하는 데에도 사용할 수 있습니다.
- ALE는 또한 프로필이 반환되지 않는 경우를 대비해 "catch all" 기본값을 제공합니다. 기본 포괄 규칙은 제한된 액세스를 허용하거나 기본 인증이 실패할 경우 액세스를 완전히 거부할 수 있습니다.

이러한 다양한 유형의 인증을 실행하려면 사용자 및 장치의 자격 증명을 생성하고 관리할 수 있는 장소가 필요합니다. ALE 통합 액세스 솔루션의 구성 요소인 UPAM이 필요합니다. 이는 네트워크에 중앙 집중식 AAA(인증, 권한 부여 및 계정) 서비스를 제공합니다. 이를 통해 네트워크 관리자는 신원과 위치 등을 기반으로 네트워크 액세스를 위한 사용자 프로필을 생성하고 관리할 수 있습니다. UPAM은 Alcatel-Lucent OmniVista® 네트워크 관리 시스템을 통해 구성 및 관리할 수 있으므로 네트워크 관리자는 네트워크 액세스 정책을 정의하고 시행할 수 있습니다.

사고 대응

네트워크 사고에 신속하게 대응하는 것은 DDoS(분산 서비스 거부)와 같은 보안 공격으로 인한 시스템 및 네트워크 손상을 최소화하고 가동 중지 시간을 줄이는 핵심 요소입니다.

Alcatel-Lucent OmniVista Network Advisor를 사용하여 위험을 최소화하고 경험 품질(QoE)을 극대화하며 보안을 강화하세요. **OmniVista Network Advisor**는 실시간 네트워크 모니터링을 제공하고 문제 발생 시 경고를 발행하며 DDoS 공격을 포함한 다양한 네트워크 및 보안 관련 문제에 대한 솔루션을 제안하는 AI 기반 지능형 자율 시스템입니다. 구성 감사 및 네트워크 성능 분석을 지속적으로 수행하여 잠재적인 문제를 즉시 **식별**하고, 이를 **완화**하며, IT 개입을 최소화하거나 전혀 하지 않고도 네트워크를 **최적화**할 수 있습니다.

파트너십 및 통합

인증의 중요한 측면은 방화벽과의 통합입니다. 예를 들어, Fortinet 과의 통합을 통해 LAN 및/또는 WLAN 네트워크에 인증된 사용자 또는 장치는 Fortinet 방화벽에도 동시에 원활하게 인증될 수 있습니다.

Palo Alto Networks(PAN) 차세대 방화벽 통합을 사용하면 LAN 및/또는 WLAN 네트워크에 인증된 사용자 또는 기기를 동시에 원활하게 PAN 방화벽에 인증할 수도 있습니다.

Versa Networks와의 파트너십을 통해 사용자, 데이터, 애플리케이션 또는 기기의 위치에 관계없이 중요한 리소스에 안전하게 액세스할 수 있습니다. 이는 중앙 사이트나 데이터 센터에서 멀리 떨어져 있는 지역 사무실이나 지점이 있는 기업에 특히 유용합니다. 다중 네트워크 홉이 필요하고 추가 비용이 발생할 수 있는 기존의 광역 네트워크(WAN)와 달리 SASE 및 SD-WAN은 클라이언트-클라우드 시대에 비용 효율적이고 안전한 솔루션을 제공합니다. 이 두 가지 솔루션을 결합함으로써 기업은 IT 인프라 관리를 단순화하고 기업/DC, 지역/지사 사무실 및 재택/모바일 작업자를 포함하여 어디서나 작업할 수 있는 시나리오를 위해 인터넷 및 비즈니스 애플리케이션에 안전하게 액세스할 수 있습니다.

ALE-Versa Titan 제품은 SASE(Secure Access Service Edge)와 클라우드의 SD-WAN 서비스를 결합한 포괄적인 솔루션입니다. 여기에는 린 IT를 위한 클라우드 제공 SD-WAN을 제공하는 Versa Titan SD-WAN과 제로 트러스트 네트워크 액세스(ZTNA)와 함께 차세대 방화벽 기능 및 지리적 차단 기능을 갖춘 Versa Secure Access(VSA)가 포함됩니다. (ZTNA)를 사용하여 어디서나 작업할 수 있습니다. 또한 Versa 보안 웹 게이트웨이(SWG)는 안전한 원격/홈 오피스 연결을 위한 안전한 웹 브라우징 및 인터넷 애플리케이션 액세스(SaaS)를 제공합니다. Versa Titan 웹 포털 및 앱은 동일한 공급업체에서 제공하는 모든 SASE 구성 요소를 사용하여 단일 플랫폼에서 통합 네트워킹 및 보안 서비스를 제공합니다. 네트워크 및 보안 정책을 포괄하는 단일 정책 저장소를 통해 기업은 IT 관리를 단순화하고 중요한 리소스에 대한 안전한 액세스를 보장할 수 있습니다.

제로 트러스트 방법론

제로 트러스트 모델을 구현하려면 조직은 먼저 일관되지 않은 정책, 암시적 신뢰, 취약한 IoT 장치 등 기존 보안 인프라의 문제를 해결해야 합니다. 목표는 이러한 문제를 해결하기 위한 네트워크 액세스 및 역할 기반 액세스 제어, 세분화 및 모니터링 기능을 구축하는 것입니다. 적절한 세분화를 통해 민감한 리소스를 분할하고 필요한 사람에게만 액세스를 제한할 수 있습니다. 모니터링 및 격리 기능을 통해 고객은 잠재적인 위협을 식별하고 격리할 수 있습니다.

ALE 솔루션으로 제로 트러스트 네트워크를 구축하기 위한 간단하면서도 강력한 방법론에는 여러 단계가 포함됩니다.

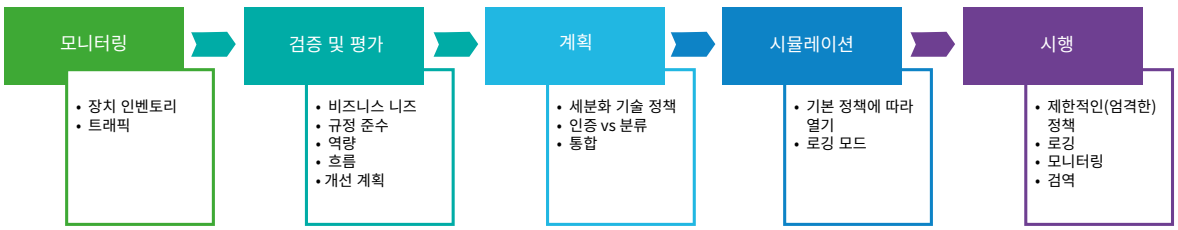
- **모니터링**: 기기 인벤토리 및 트래픽을 포함하여 모니터링을 수행해야 합니다.
- **검증 및 평가**: 검증 및 평가에는 비즈니스 요구 사항, 규정 준수 요구 사항, 기능 및 흐름 분석이 포함됩니다.
- **계획**: 평가 결과에 따라 해결 계획을 수립해야 합니다. 계획에는 올바른 분할 기술과 정책을 선택하는 것뿐만 아니라 인증과 분류, 통합을 고려하는 것도 포함됩니다.
- **시뮬레이션**: 시뮬레이션 단계에서는 정책이 기본적으로 로깅 모드로 열려 있으며 기타 기능이 테스트됩니다.
- **시행**: 시행 단계에는 제한적인 정책 구현, 로깅, 모니터링 및 격리 조치 수행이 포함됩니다.

총 소유 비용

총 소유 비용(TCO)은 제품이나 서비스의 수명 전체에 걸쳐 소유 및 운영과 관련된 모든 비용을 포함합니다. 여기에는 구매 가격, 유지 관리, 지원, 업그레이드 등이 포함됩니다. 예산 초과를 완화하고 보다 정확한 투자 수익(ROI)을 제공할 수 있는 장기적인 가치를 제공하는 비용 효율적인 솔루션을 선택하는 것이 중요합니다.

초기 자본 투자와 시스템 라이선스 및 운영을 유지하는 데 필요한 지속적인 비용 간의 차이를 고려하십시오. 방화벽과 같은 일부 구성 요소는 순전히 보안에 중점을 두고 있지만, 다른 구성 요소도 보다 심층적인 보안 전략을 구축하는 데 중요합니다. 여기에는 정책 관리, 효율적인 경로 네트워크 분리 기술(자동화된 고급 매크로 및 마이크로 세분화), 자동 가상 네트워크(VLAN) 할당, 네트워크 암호화 프로토콜, 애플리케이션 가시성, 운영 체제 코드의 독립적 검증 및 인증이 포함됩니다.

ALE의 네트워크 사이버 보안 전략은 위에서 언급한 네트워크 보안의 필수 요소를 무료로 해결하는 반면, 다른 공급업체의 대안은 운영 및 유지를 위해 특정 전문 지식과 수많은 비용이 많이 드는 요소 및 라이선스를 요구합니다. ALE 접근 방식은 강력하고 효율적인 네트워크 사이버 보안을 보장하는 동시에 고객에게 상당한 경제적 이점을 제공합니다.



결론

강력한 보안을 위해 제로 트러스트 네트워크를 구현하면 생성 및 유지 관리 측면에서 복잡성과 비용 등 여러 가지 문제가 발생할 수 있다는 것은 분명합니다. 그러나 ALE는 이러한 문제를 해결하기 위한 특별하고 비용 효율적인 접근 방식을 제공합니다. 이 문서에 제시된 다른 구성 요소 외에도 고급 매크로 및 마이크로 세분화 기술은 최신 사이버 보안 요구 사항을 해결하기 위해 제로 트러스트 네트워크를 구현하는 간단하고 합리적인 비용의 수단을 제공합니다. 우리는 고객이 사이버 보안 문제를 해결할 수 있도록 돕기 위해 최선을 다하고 있으며 우리의 접근 방식이 이러한 목표를 달성하는 데 도움이 될 수 있다고 믿습니다.

ALE 솔루션에는 탄력적이고 안전한 지능형 패브릭(iFab)과 UNP, 그리고 프로필 기반 액세스 제어를 제공하는 UPAM을 갖춘 강력한 네트워크 액세스 제어(NAC)가 포함됩니다. 당사의 혁신적인 OmniVista Network Advisor 솔루션은 원활한 운영과 신속한 복구 및 공격 방지를 보장합니다. 또한 Versa Networks와 같은 SASE 공급업체와 파트너십을 맺고 Palo Alto Networks와 같은 방화벽 공급업체와 통합하여 고객에게 보다 포괄적이고 통합된 보안 솔루션을 제공합니다.

Alcatel·Lucent Enterprise