TANIUM

제로 트러스트

보안 퍼펙트 스톰에 대한 최고 솔루션.

오늘날, 우리는 사이버 보안에 대한 제로 트러스트 접근 방식을 채택해야하는 여러 이벤트가 융합된 퍼펙트 스톰을 경험하고 있습니다.

원격 및 하이브리드 근무 형태 증가

클라우드 서비스로서의 전환

직장 내 모바일 디바이스 사용 증가

SW 공급망에 심각한 영향을 줄 수 있는 공격 증가

지금까지 우리는 기업의 데이터를 지키는데 있어, 이렇게 많은 도전에 직면한 적이 없으며, 네트워크에 접속 하려는 모든 사용자와 디바이스를 의심했던 적이 없었습니다. 하지만 오늘날의 IT 환경은 사용자, 디바이스, 어플리케이션, 그리고 네트워크까지도 인가된 네트워크에 연결되어 있어야 하며, 과거 검증 기록이 있다해도 신뢰해서는 안 된다라는 원칙을 가진 제로 트러스트 모델을 고려해야 합니다.

기업내 사이버 보안 및 IT 리더는 최근 몇년내 짧은 시간동안 보안대응의 복잡성이 매우 높아졌음을 실감하고 있습니다. 사이버 범죄는 점점 더 정교해지고 조직화 되었으며, 경우에 따라 몇몇 국가에서는 이런 범죄자들에게 재정지원을 아끼지 않고 돕고 있습니다.

또한, 공격 백터는 최근 몇년간 상당히 확대 되었습니다. 이는 원격 및 하이브리드 근무 형태 증가로 많은 사람들이 다양한 곳에서 개인 디바이스 및 네트워크를 사용하여 비즈니스 데이터에 접속하고 있음을 의미합니다.

게다가 퍼블릭 클라우드 서비스 도입이 늘고 다양한 클라우드를 함께 사용하는 사례가 증가하고 있습니다. 일부는 클라우드에 배포된 자원은 중앙 IT 감시 대상이 아니어서 다른 IT 자산처럼 관리되지 않는 사례도 함께 늘고 있습니다. 이처럼 클라우드, 원격근무 그리고 모바일 환경 등장으로 더이상 경계, 혹은 경계 방어의 의미는 사라졌습니다.

이러한 변화들은 조직들이 사이버 보안에 대한 제로 트러스트 모델로 전환 해야 한다는 이유입니다. 제로 트로스트의 개념은 사용자나 디바이스를 신뢰하지 않고 항상 확인 해야 한다는 것입니다.

허용 되지 않는 위험

실제로 악의적인 의도를 갖고 접속 권한을 얻으려고 시도하는 외부 엔터티는 매우 위험 합니다. 오늘날 그 누군가 또는 그 어떤것을 신뢰하기에는 너무 많은 위험에 노출되어 있습니다. 제로 트러스트로의 전환으로 확인된 것은, 기존 VPN (가상 사내망)은 더이상 네트워크에 대한 원격 접속을 완벽히 보호 할 수 없음을 깨달았다는 것입니다.

조직의 분산된 업무 환경에서 내부 직원은 온프레미스 또는 클라우드 기반으로 고객 관리 시스템(CRM) 및 전사적 자원관리 시스템(ERP)의 개인 정보 데이터 및 민감 기업 정보 데이터에 접속 할 수 있습니다. 하지만 이 모든 것은 개인 디바이스에서 이루어집니다.

기업은 보안을 강화하면서도, 사용자를 효과적으로 인증 해주는 방법이 필요합니다. 안타깝게도 기존 VPN으로는 재택 근무로 인해 발생하는 트래픽을 제어하는데 어려움을 겪고 있습니다.

최소 권한부여 원칙을 기준으로, 접속 상황과 전후맥락(Context) 판단이 가능하도록 멀티 팩터 인증 (MFA)과 네트워크 연결이 결합 되어, 기업은 클라우드 및 모바일 중심 환경에 적합한 보안 모델을 유지 할 수 있습니다.

제로 트러스트 접근 방식으로 조직은 공격 대상을 줄이고, 검증된 컨텍스트 및 승인된 사용자만이 민감 데이터 접속을 할 수 있도록 하였습니다. 이로써 위험을 크게 줄일 수 있는 결과를 가져 왔습니다.

과거 제로 트러스트 접근 방식은 네트워크 접속 및 싱글 사인 온(SSO)을 통한 ID 및 접속 관리 (IAM)에 중점을 두었습니다. 하지만 원격 근무로 인해 최종 사용자가 접속 해야하는 범위가 넓어지고 있어, 어느 디바이스에서든 접속 가능해야 하므로, 디바이스 상태가 점점 더 중요해지고 있습니다.

보안 프로토콜에 장치 유효성 검사를 추가함으로써 기업은 자격 증명이나 장치를 훔치는 범죄자로부터 방어하고 이를 MFA와 함께 사용하여 네트워크 및 데이터에 접속 할 수 있습니다.

네트워크 환경 내에 규정을 준수하지 않거나, 심각한 취약점 대해 모니터링 하는경우, 민감 데이터 손상을 보호하는 방법은 디바이스를 보호 하는 방법 입니다. 그렇기 때문에 제로 트러스트 접근 방식의 일부인 엔드포인트 통합 관리 솔루션을 채택하는 것이 중요합니다.

VPN에 대한 우려

Tanium의 연구에 따르면 원격 근무로 인해 사용자가 다양한 곳에서 접속 하면서 생긴 과도한 VPN이 두번째로 큰 보안 문제였습니다. 레거시 VPN의 문제점은 트래픽 흐름의 보안을 위협할 뿐 아니라, 엔드포인트와 관련된 보안 위협을 증가 시키는 것에 기여하고 있다는 것 입니다.

팬데믹이 발생하고, 대부분의 기업은 직원에게 원격 근무를 허용 하였습니다. 이때 VPN을 사용하여 분산된 직원들의 접속을 지원하였지만, 결과는 좋지 않았습니다. 많은 사용자들은 이미 VPN을 통한 원격 접속에 익숙하지만, 안전하지 않은 디바이스를 사용하는 사용자에게 보안 접속를 허용하는 것은 이상적인 툴은 아닙니다.

VPN은 사용자가 원격에서 일할 때, 홈 네트워크를 겨냥한 위협에 적절하게 방어하지 못합니다. 또한 기업은 원격 혹은 하이브리드 업무 환경의 근무 인력을 지원하기 위해서는 많은 VPN이 필요하며, 이를 관리 및 유지하기 위해서는 매우 큰 부담을 갖을 수 있습니다.

제로 트러스트에 집중

많은 원격 근무자에게 보안 접속를 제공하기 위해서 조직은 VPN 외의 다른 방법을 모색하고, 사이버 보안에 있어 제로 트러스트 모델을 전적으로 채택해야 합니다.

제로 트러스트 전략과 툴을 사용하면, 보다 세분화된 접속 제어가 가능하고 사용자가 포괄적인 권한을 획득하지 못하기 때문에, 보안팀은 애플리케이션에 대한 보안 접속을 제공하기가 더 용이합니다. 접속 권한은 매우 구체적이며 지속적으로 확인 되어야 합니다.

"제로 트러스트"는 이미 보안 시장에서 많이 사용되나, 정의하는 사람에 따라서 의미가 상이할 수 있습니다. 이 접근의 방식은 다음 세 가지가 포함되어야 합니다.

1. 사용자 자격 증명
2. 사용자가 접속 하려는 데이터
3. 사용자가 접속 권한을 얻기 위해 사용하는 디바이스(엔드포인트)

최소 권한부여 원칙을 기준으로, 접속 상황과 전후맥락(Context) 판단이 가능하도록 멀티 팩터 인증 (MFA)과 네트워크 연결이 결합 되어, 기업은 클라우드 및 모바일 중심 환경에 적합한 보안 모델을 유지 할 수 있습니다.

공격 대상을 줄이고, 검증된 컨텍스트 및 인가된 사용자만이 민감 데이터에 접속 할 수 있도록 하였습니다. 이는 위험을 줄이는 역할을 합니다.

디바이스 유효성 검사는 성공적인 제로 트러스트 전략의 핵심중 하나이며, 현재 다양한 곳에서 많은 사용자가 접속 되므로, 디바이스 상태는 매우 중요합니다. 대부분의 디바이스는 조직내의 새로운 "경계" 대상이며, 디바이스 유효성 검사를 통해 조직은 사이버 범죄자가 네트워크에 접속 하는데 사용할 수 있는 분실된 자격 증명 또는 분실된 디바이스로부터 보호 할 수 있습니다.

따라서, 엄격한 엔드포인트 관리를 실행 하는 것이 제로 트러스트 접근 방식에서 매우 중요합니다. 실시간 정확한 엔드포인트 관리가 되지 않을 경우, 조직은 컴플라이언스 준수 및 접속 된 디바이스 검증 상태를 확인 할 수 없습니다. 인증만으로는 디바이스 보안을 보장 할 수는 없습니다.

올바른 툴을 사용하면, 보안팀은 ID 확인 및 접속 정책이 적용 되더라도, 제로 트러스트 접근 방식은 아무도 신뢰 하지 않기에 지속적으로 디바이스 상태를 확인 할 수 있습니다. 궁극적으로 조직은 새로운 제로 트러스트 솔루션을 이미 사용중인 툴과 통합 할 수 있어야 합니다.

제로 트러스트 실행의 핵심 구성요소에는 다음이 포함되어야 합니다.

디바이스의 보안 상태를 확인하고, 보안팀이 문제가 발생 했을 경우 조치를 취할 수 있도록 디바이스 컴플라이언스 모니터링을 시행

사용자의 ID를 인증하고, 업무 역할 기반에 따라 규칙 및 접속을 비교하는 ID 및 접속 관리

사용자의 페르소나 및 사용 중인 디바이스를 기반으로 리소스 네트워크 세그먼트에 대한 접속을 제한하는 네트워크 접속 제어

“후회하는 것보다 조심하는 것이 낫다”

디바이스, 다양한 엔드포인트, 애플리케이션, 네트워크 및 사용자 등 그 어떤 것도 신뢰하지 말라는 제로 트러스트의 개념은 부정적으로 들릴 수 있습니다. 하지만 이 모델이 실제로 보여주는 것은 현재 조직이 매우 어려운 시기에 운영되고 있으며, 데이터 유출 및 랜섬웨이 공격이 발생했을 때 매우 위태로울 수 있다는 것입니다.

많은 사람들이 개인 디바이스 및 네트워크를 사용하여 다양한 곳에서 일하고 있습니다. 기업은 그 어느 때보다 클라우드 서비스에 의존하고 있으며, 공격은 더욱더 정교해졌습니다. 이는 **공급망 전체에 영향을 미칩니다.**

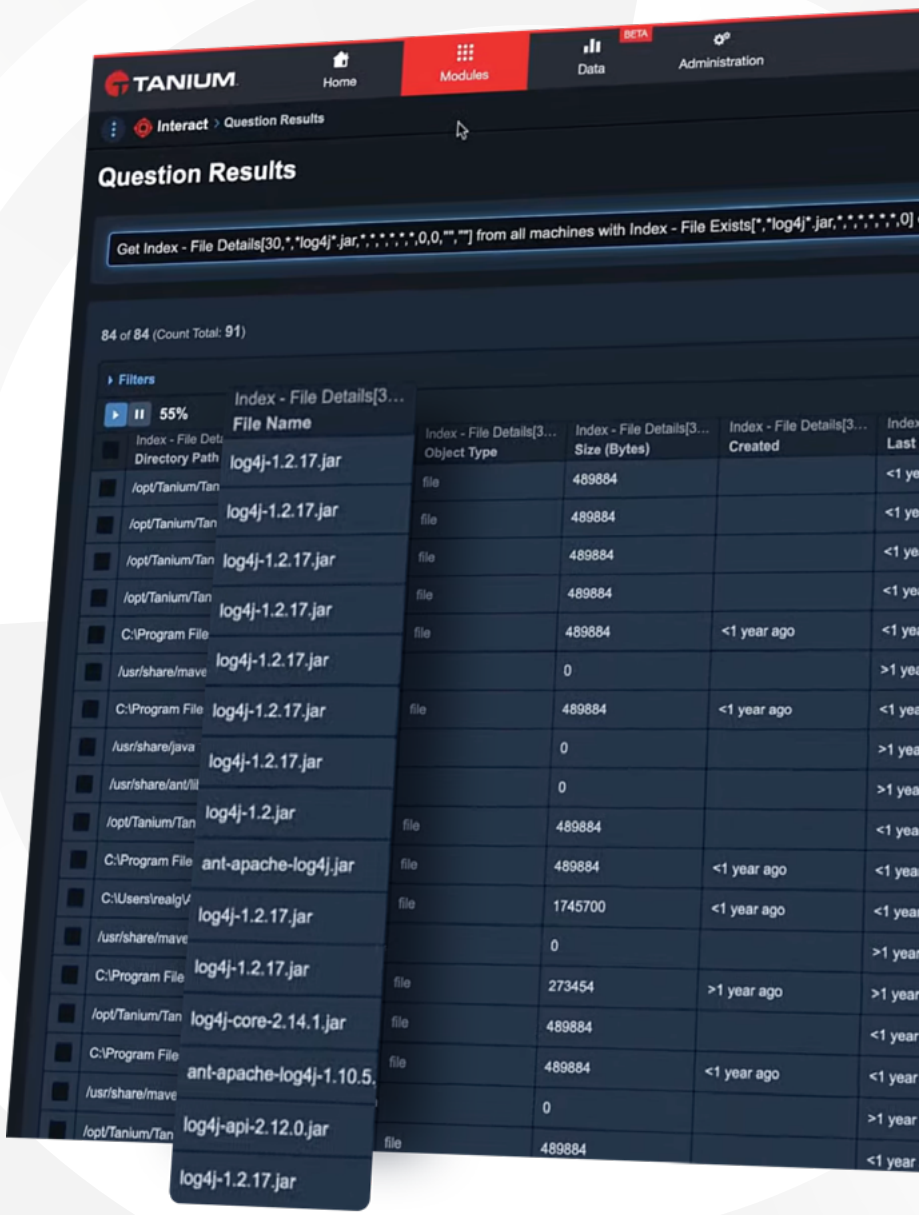
조직은 데이터 리소스를 항상 보호하고, 어떠한 문제가 발생 하지 않도록 네트워크에 접근 하려는 사용자 및 디바이스를 확실하게 관리 해야 합니다. **제로 트러스트 전략** 구현은 이러한 보안 수준을 만드는데 가장 효과적인 방법 입니다.

퍼펙트 스톰의 가장 확실한 예 - Log4j

2021년 12월 에 발견된 **Log4j 취약점**은 사이버 보안 팀이 왜 제로 트러스트 보안 아키텍처를 구현해야 하는 이유를 보여주는 가장 최근 사례 중 하나입니다.

보안 사고는 매일 발생 하고 있으며, 그 중 일부는 SW 공급망 전체에 영향을 미치는 랜섬웨어 공격으로 많은 헤드라인을 장식합니다. 아파치 로깅 서비스의 일부인 Java 기반 로깅 유틸리티 Log4j의 경우, 보안 연구원들이 임의 코드 실행과 관련된 제로데이 보안 취약점을 발견했습니다.

이것은 결코 안일하게 생각할만한 취약점이 아닙니다. 보안 전문가들은 이 결함이 최근 몇년 동안 가장 크고 심각한 발견이라고 설명 했습니다. 그리고 이는 조직이 어떻게 위험에 처할 수 있는지를 보여주는 분명한 사건 입니다. 새로운 소프트웨어 취약점은 항상 발견 되고 있으며, 그 중 일부는 매우 심각한 보안 위반 및 데이터 손실로 이어질 수 있습니다.



보안 기본 사항

제로 트러스트 접근 방식 구축과 함께 조직은 보안 기본 사항에 주의를 기울여야 합니다. 예를 들어, 취약점을 발견 했다면 패치를 즉각적으로 배포해야 합니다. Log4j 이슈로 인해서 우리는 패치가 왜 중요한지 보여주었습니다.

패치를 배포하고 설치를 해야하지만 생각만큼 결코 쉽게 되지 않습니다. 패치 관리 프로그램은 인터넷, 기업 및 조직 네트워크에 연결되어 사용되는 모든 디바이스가 대상이 되어야 합니다.

또 다른 좋은 방법은 시스템이 공격에 취약한 모든 엔드포인트를 재평가하는 것입니다. 여기에는 네트워크 시스템에 대한 관리 접속 권한이 있는 모든 시스템 및 장치에 대한 감사 수행과 네트워크에 연결된 모든 센서 또는 기타 사물 인터넷(IoT) 장치에 대한 보안 보호 평가가 포함됩니다.

장기적으로 기업은 증가하는 데이터 양을 수집, 저장 및 분류 하는 방법을 재 평가해야 합니다. 이는 개인 정보나 지적 재산과 같은 가장 민감 데이터 접속에 대하여 보다 엄격한 보안 제어가 적용되도록 데이터를 세분화 할 수 있어야 할 것 입니다.

또한 기업은 방심하지 않고 MFA 및 강력한 암호 정책을 적용해야 합니다. 해커가 사용자의 암호를 추측 했다는 것은 이미 네트워크가 손상되었다는 것이며, 이는 더 복잡한 암호 또는 MFA 사용 정책이 필요함을 의미합니다.

기업의 임직원 사용자가 사이버 보안에 대한 인지가 다소 부족 할 수 있으므로, 다양한 교육 프로그램을 제공하여 조직의 모든 사용자가 이를 습득 할수 있도록 하는것이 좋습니다. 이러한 교육 프로그램은 피싱 및 기타 공격을 나타내는 징후와 범죄자들이 민감한 정보 또는 네트워크 액세스를 위해 자주 사용하는 사회 공학 기술을 보여줘야 합니다.

제로 트러스트 모델을 구축하고, 사이버 보안 “기본” 관리를 통해, 조직은 랜섬웨어를 포함한 최신 위협으로부터 스스로를 방어 할 수 있습니다.

우리는 단순 ID 관리 및 사용자 인증 하는 것 이상의 보안이 필요합니다. 무결성이 입증될 때까지 네트워크에 침입하려는 모든 사람 및 그 어떤 것들을 침입자라고 가정 해야 합니다.

다음 단계

Tanium의 통합 엔드포인트 관리(XEM) 플랫폼이 어떻게 제로 트러스트 방식을 지원하는지 알아보십시오.

자세히 알아보기

업계 유일의 XEM(통합 엔드포인트 관리) 공급자인 Tanium은 복잡한 보안 및 기술 환경 관리에 대한 레거시 접근 방식의 패러다임 전환을 주도합니다. Tanium만이 IT, 컴플라이언스, 보안 및 위험을 단일 공유 목적을 위한 공통 분류, 장치 전반에 걸친 포괄적인 가시성을 제공하는 단일 플랫폼으로 통합하여 사이버 위협으로부터 모든 팀, 엔드포인트 및 워크플로를 보호합니다. 즉, 중요한 정보와 인프라를 대규모로 보호합니다. 포춘지 선정 100대 기업의 절반 이상과 미군은 사람들을 보호하고, 데이터를 방어하고, 시스템을 보호하고, 어디서나 모든 엔드포인트, 팀, 워크플로를 확인하고 제어할 수 있는 Tanium을 신뢰합니다. The power of certainty.

www.tanium.com을 방문하고 LinkedIn 및 Twitter를 팔로우하십시오.