SOLUTION BRIEF

제로 트러스트를 위한 Tanium

디바이스 상태 유효성 검사가 ID 유효성 검사만큼 중요한 이유

제로 트러스트란?

제로 트러스트란, 어떤 사용자 혹은 디바이스든 신뢰하지 않고 항상 확인 한다는 개념입니다. 다음 세가지 항목을 통해, 성공적인 제로트러스트 접근 방식에 대해 알아 봅시다.

- 사용자 자격 증명
- 사용자가 접근하려는 데이터
- 사용자가 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.

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

디바이스 검증은 성공적인 제로 제로트러스트 결과의 핵심

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 가능 해야 하므로, 디바이스 상태가 점점 더 중요해지고 있습니다.

조직은, 디바이스 유효성 검사를 추가함으로써 멀티 팩터 인증 (MFA)을 통해 네트워크에 접속 하려는 탈취된 자격 증명 또는 디바이스로부터 보호 할 수 있습니다. 또한 네트워크 환경 내에 규정을 준수하지 않거나, 심각한 취약점 대해 모니터링 하는경우, 민감 데이터 손상을 보호하는 방법은 디바이스 자체를 보호 하는 방법 뿐입니다.

그렇기 때문에 제로 트러스트 접근 방식의 일부인 엔드포인트 통합 관리 솔루션을 채택하는 것이 중요합니다.

조직 규모의 맞게 디바이스 상태를 원활하게 검증

Tanium은 실시간으로 엔드포인트에 대한 가시성과 제어를 제공합니다. 조직의 규모가 클수록 실시간 정확한 엔드포인트 데이터가 필요하며, 이를 통해 규정 준수 및 디바이스 상태를 확인 할 수 있습니다. 인증만으로는 디바이스가 안전하다고 확실 할 수 없으며, 사용자가 디바이스 없이 시스템에 접근 할 수 없기 때문에 그 어느것도 안전하다고 할 수 없습니다.

Tanium을 사용하면 ID 확인 및 접속 정책이 적용 되더라도, 제로 트러스트 접근 방식이기에 아무도 신뢰 하지 않고 지속적으로 디바이스 상태를 확인 할 수 있습니다.

또한 Tanium은 조직은 이미 사용 중인 제로 트러스트 툴과 연동하여 사용 할 수 있습니다.

제로 트러스트를 위한 구성요소

디바이스 규정 준수 및 모니터링 시행
디바이스의 보안 상태를 확인 하고, 문제가 발생 했을 경우 IT 팀이 조치 할 수 있도록 합니다.

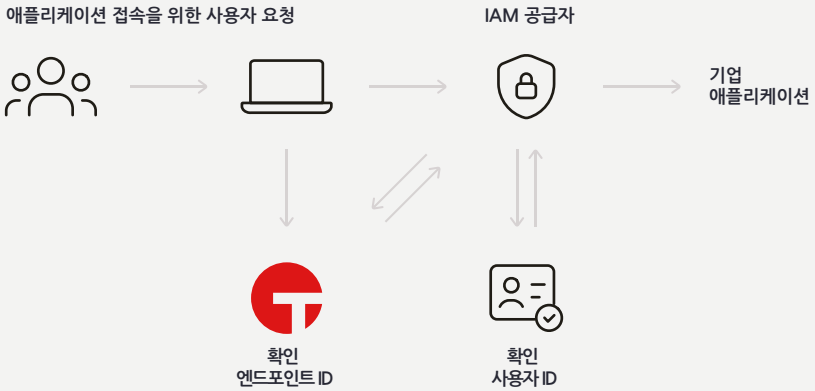
ID 및 접속 관리(IAM)
인증 확인은, 개인 정보를 확인하고, 역할 기반 규칙 (RBAC) 및 접속을 비교합니다.

네트워크 접속
조직은 사용 중인 사용자의 개인 정보 및 디바이스를 기반으로 리소스 및 네트워크 세그먼트에 대한 접속을 제어할 수 있어야 합니다.

제로 트러스트 실행과 함께 Tanium이 지원하는 디바이스 검증 방법에 대해 자세히 알아보십시오.

Tanium을 통한 제로 트러스트 구현시 얻는 장점

- **모든 엔드포인트에 대한 다양한 가시성을 제공하고,** 조직내 환경에 어떠한 디바이스가 연결 되어 있는지 확인 할 수 있습니다.
- 단 몇 분안에 규모에 상관없이 엔드포인트 데이터에 대한 **신뢰할 수 있는 데이터를 제공하는 유일한 툴을 제공합니다.**
- 중요한 데이터를 저장하는 시스템에 대한 접근을 제한하여 **공격 대상을 줄입니다.**
- 접속의 전제 조건으로 **디바이스 상태를 확인합니다.**
- 정책이 시행되고 있음을 알고, **지속적으로 규정을 준수하**고 문제발생시 이를 진단하고 해결할 수 있는 권한을 갖습니다.
- **민감 데이터** 찾아 유출되는 것을 방지합니다.
- **조치를 취할 수 있는 권한을 갖고** 적절하지 않은 것이 있으면 신속하게 대응합니다.
- Tanium API를 사용한 제로 트러스트 실행을 위해 **이미 사용 중인 툴과 연동합니다**.
- 사용자와 데이터가 상호 작용하는 시스템의 위험 지수를 보여주는 대시보드를 **통해 위험 프로필을 실시간으로 파악할 수 있습니다**.
- 모든 직원의 요구 사항을 충족하는 제로 트러스트 접근 방식을 설계하는 데 도움이 되는 **자산 활용 기준점을 만듭니다**.



제로 트러스트 접근 방식에서 상태 유효성 검사를 포함하지 않는 것은, 위협을 완전히 관리하지 못하는 것입니다.

조직은 보안을 위해 사용자와 엔드포인트에 대하여 조직내 환경에서 발생하는 모든 일을 쉽게 모니터링하고 제어해야 합니다. 이를 위해서는 원격근무, 클라우드 서비스, 모바일 환경에 적합한 보안 모델이 필요합니다. 제로 트러스트는 이러한 새로운 환경을 위해 만들어졌으며, 대규모 제로 트러스트 보안의 핵심은 바로 엔드포인트 가시성 확보 입니다.

Tanium의 통합 엔드포인트 관리 플랫폼이 어떻게 제로 트러스트 방식을 지원할 수 있는지아래 사이트를 통해 확인 하십시오
www.explore.tanium.com/zero-trust .

Tanium은 포춘지 선정 100대 기업의 절반 이상과 많은 정부 기관, 미군이 신뢰하는 플랫폼으로 모든 엔드포인트에서 가시성과 통제력을 확보할 수 있도록 합니다. Tanium의 접근 방식은 IT 운영, 보안 및 위험 관리 팀이 규모에 맞게 네트워크를 관리, 보안, 보호할 수 있도록 합니다. 어디서나 모든 엔드포인트를 확인하고 제어하십시오. That's power of certainty.

www.tanium.com을 방문하고 LinkedIn및 Twitter를 팔로우하십시오.