# 제로 트러스트 데이터센터 보안

온프레미스나 클라우드 어디든 데이터센터에는 조직의 가장 귀중한 정보인 민감한 데이터와 애플리케이션이 있습니다. 이러한 데이터는 저장된 위치에 관계없이 항상 강력하게 보호되어야 합니다. 이러한 데이터를 안전하게 보호하기 위해서는 제로 트러스트 데이터센터의 구성 요소를 이해하고 조직 보안 체계를 구축하는 것이 매우 중요합니다.

### 가시성 부족

네트워크 전반의 가시성은 애플리케이션 및 네트워크 상태를 신속하게 진단하고 잠재적으로 악의적인 활동을 식별하는 데 필수입니다. 제대로 볼 수 없으면 지킬 수도 없습니다.

### 조직의 핵심 자산

민감한 비즈니스 크리티컬 데이터와 애플리케이션은 조직의 핵심 자산이며, 온프레미스나 클라우드 어디든 존재합니다. 이러한 정보가 공격자의 손에 들어가면 비즈니스에 중대한 악영향을 미칩니다.

### 도처에 도사린 위협

여러 벡터에서 위협이 네트워크로 침입하며, 각 공격의 목적은 다양합니다. 인텐트 또는 사용하는 기술에 상관없이 적절한 도구를 원활하게 사용해 데이터센터를 지키는 것이 중요합니다.

### 데이터센터 내부 보안

방화벽은 서비스와 애플리케이션 그룹들 사이의 East-West 및 North-South 서버 간 통신을 한번 더 체크하고, 다양한 서버에 있는 모든 리소스와 애플리케이션이 감염되지 않도록 보장합니다. 관리자는 트래픽과 각 사용자가 특정 애플리케이션에 액세스하는 방식을 설정할 수 있습니다.

### 비즈니스 연속성

조직은 믿을 수 있는 연결을 필요로 하며, 데이터센터의 위치와 상관없이 비즈니스 연속성을 유지하고 일관적인 보안 정책과 함께 고품질 서비스 경험 및 액세스를 제공해야 합니다. 데이터센터 간 통로를 지키는 보안관과 같이, 관리 기능은 오케스트레이션과 모니터링을 지원해 언제 어디서든, 온프레미스나 클라우드에 구축할 수 있도록 돕습니다.

### 클라우드 워크로드 보호

개별 애플리케이션은 반드시 보호되어야 합니다. 별도의 체크포인트로서 각 애플리케이션에 컨테이너화된 방화벽이 구축될 수 있습니다. 공격자가 귀중한 자산이 저장된 공간에 침입하면 이를 막을 문지기가 있습니다. 클라우드 워크로드 보호는 애플리케이션에 내장되어 있습니다. 귀중한 자산이 움직이면 게이트를 닫아 공격자를 가두고 이들을 추방시킵니다.

### Data Center Interconnect

Data Center Interconnect(DCI)는 데이터센터 로케이션 간의 커뮤니케이션을 위한 통로입니다. 대부분의 조직은 여러 데이터센터 환경이 혼합되어 있습니다. 클라우드 및 온프레미스 환경 사이의 트래픽을 보호하려면 강력한 라우터를 보유하는 것이 중요합니다. 그렇게 해야 공격자가 데이터센터 내부로 침입해도 다른 위치로 이동하지 못하기 때문입니다.

### 데이터센터 내 공격자 포위

어떤 보안 체계를 갖추든 공격자들은 언제나 데이터센터의 취약점을 악용할 기회를 찾을 것이므로 반드시 이에 대비해야 합니다. 관측, 파악, 조치는 보안의 중요 요소입니다. 데이터센터를 보호하려면 클라이언트에서 워크로드까지 모든 연결 포인트에서 광범위한 가시성, 인텔리전스, 실행 역량을 갖춘 위협 인식 네트워크를 구현해야 합니다.

### 데이터센터 WAN 게이트웨이

데이터센터 WAN 게이트웨이는 데이터센터의 입구입니다. 방화벽은 데이터센터에 들어오고 나가는 트래픽을 체크하고 사용자와 디바이스가 데이터센터에 대한 적절한 액세스 권한을 가지고 있는지 확인하며 보호합니다. 데이터센터로 들어오는 보안 체크포인트처럼, 멀웨어가 숨어 들어오지 않도록 들어오는 트래픽을 체크합니다.

## 클라우드 시대의 위협 인식 네트워크

제로 트러스트 데이터센터는 위협 인식 네트워크를 제공하며 궁극적으로는 복잡성을 줄이고 운영을 간소화는 동시에 보안을 강화합니다. 조직이 위협 인식 네트워크를 갖추면 공격을 일찍 탐지하고 공격자들이 침투하지 못하도록 해 사용자, 애플리케이션, 인프라는 물론 귀중한 자산을 지킬 수 있습니다.

juniper NETWORKS

PN: 3050145