AKAMAI 솔루션 설명서

엔드포인트 보호를 위한 Akamai Guardicore Segmentation

마이크로세그멘테이션을 고려할 때 대부분의 보안팀은 중요한 애플리케이션과 서버처럼 기업 네트워크 내부에 위치한 자산을 보호하는 것을 생각합니다. 그러나 마이크로세그멘테이션은 데이터 센터와 워크로드를 넘어 엔드포인트 디바이스까지 확장되어야 합니다. 엔드포인트는 종종 최초 감염 지점이 되며 XDR 및 NGAV는 최종 사용자 디바이스에서 위협을 탐지하도록 설계되었지만 피싱, 소셜 엔지니어링 등 다양한 공격 기법에 의해 우회될 수 있습니다. 엔드포인트에 마이크로세그멘테이션을 적용하는 것은 인터넷을 통한 최초 감염과 네트워크의 다른 부분으로의 측면 이동을 모두 방지하는 효과적인 방법입니다.

작은 불편이 큰 문제로

오늘날 사이버 위협은 과거보다 더 침투적이고, 더 큰 피해를 초래하고 있습니다. 공격의 주요 표적은 여전히 데이터 센터지만, 감염은 대부분 사용자의 실수를 유도하기 쉬운 최종 사용자 디바이스에서 시작됩니다. 랜섬웨어를 포함한 이러한 위협으로부터 조직을 보호하기 위해서는 멀티 보안 레이어를 갖춘 종합적인 보안 전략이 필요하며, 이는 제로 트러스트와 같은 포괄적인 프레임워크를 기반으로 구축되어야 합니다. 그러나 어떠한 보안 전략을 선택하더라도 보안의 빈틈이 생기고 악용되는 것은 피할 수 없는 현실입니다.

흔히 악용되는 빈틈 중 하나는 피싱이나 RDP와 같은 내장 서비스를 무력화하는 방법으로 단일 엔드포인트에 접속한 후, 고위 권한이나 관리자 권한을 가진 머신을 찾을 때까지 측면 이동을 통해 가능한 많은 엔드포인트를 감염시키는 것입니다. 최초 감염은 경미한 피해만 남기고 복구할 수 있으며, 반드시 측면 이동이 시작되기 전에 차단해야 합니다. 스크린샷 캡처, 정보 유출, 암호화 등 공격이 본격화되면, 원래는 작은 규모로 통제 가능했을 유출이 보안 전문가와 기업 전체에 심각한 위협으로 확산되는 악몽이 될 수 있습니다.

빈틈 메우기

머신 러닝과 기타 신기술이 멀웨어 대응 및 EDR/XDR 솔루션 분야에서 상당한 진전을 이뤘지만, 유출은 여전히 발생하고 있습니다. 엔드포인트 보안 솔루션은 모든 멀웨어를 탐지할 수 없으며 탐지하더라도 감염과 탐지 사이의 시간 차이로 인해, 공격자는 개방된 포트를 스캔하고, 내장 OS 서비스를 탈취해 머신 간 이동을 시도하고, 민감한 비즈니스 핵심 자산에 접근하는 방법을 찾을 수 있습니다.

오늘날의 보안 위협에 효과적으로 대응하려면 '모든 감염이 탐지 및 차단되지는 않는다'는 전제를 바탕으로 한 사후 대응(post-breach) 관점이 필요합니다. 따라서 보안팀은 불가피하게 발생한 감염이 최초 감염된 엔드포인트에서 더 이상 확산되지 않도록 해야 합니다. XDR 또는 NGAV는 유용한 텔레메트리 데이터를 제공하며 대부분의 유출을 탐지할 수 있지만, 이러한 탐지 중심 툴을 보완하고 잠재적 영향 범위를 제한하는 가장 효과적인 방법은 엔드포인트에 마이크로세그멘테이션을 적용하는 것입니다.

장점

제로 트러스트 구현
제로 트러스트를 구축하려면 마이크로세그멘테이션이 반드시 필요합니다

커버리지 확장
Windows 및 Mac 노트북과 디바이스까지 지원합니다

최초 감염 예방
탐지에 의존하지 않고 엔드포인트를 보호합니다

대응 시간 단축
의심스러운 측면 통신을 클릭 한 번으로 차단합니다

Akamai

2021년, Guardicore의 의뢰로 Vanson Bourne이 실시한 조사에 따르면, 참여한 보안 전문가의 92%는 포괄적인 세그멘테이션을 통해 기업이 사이버 공격으로 심각한 피해를 입거나 대규모 데이터 유출을 겪는 것을 방지할 수 있었다고 답했습니다. 그러나 단 2%만이 세그멘테이션을 네트워크 외부까지 확장해 엔드포인트를 포함한 모든 중요 자산을 보호하고 있습니다. 이러한 큰 격차는 대다수의 보안팀이 세그멘테이션과 같은 기술을 모든 자산에 적용하지 못하고 있음을 보여주며, 공격자들이 바로 이 보안의 빈틈을 노려 네트워크에 침투하고 있다는 사실을 시사합니다.

Akamai Guardicore Segmentation으로 엔드포인트 보호

Akamai Guardicore Segmentation(이전 Guardicore Centra)은 엔드포인트와 네트워크 자산 간의 통신을 모니터링하고 제어하는 단일 플랫폼을 제공해 Linux, Windows는 물론 이제 Mac 머신까지 지원합니다. Akamai의 에이전트 기반 접근 방식은 개별 프로세스와 서비스 수준까지 연결을 가시화할 수 있으며, 자체 드라이버를 통해 기본 운영 체제와 무관하게 통신을 제한하는 정밀한 보안 정책을 적용할 수 있습니다.

한 사례에서 고객은 엔드포인트에 에이전트를 설치한 뒤, 해당 엔드포인트 간 불필요한 통신을 차단하는 정책을 수립했습니다. 이처럼 측면 이동 차단은 마이크로세그멘테이션의 핵심이지만 지금까지는 데이터 센터 내 자산에만 적용되었고 엔드포인트에는 적용되지 않았습니다. 이 특정 사례에서 고객은 서버와 애플리케이션이 아닌 엔드포인트를 마이크로세그멘테이션했기 때문에 멀웨어로 인한 초기 측면 이동을 막고 킬 체인의 첫 번째 링크에서 차단할 수 있었습니다.

고객은 공격자가 인터넷에 연결된 노트북을 감염시키기 위해 RDP 무차별 대입 기술을 사용한다는 사실을 파악한 후, 인터넷에서 모든 최종 사용자 디바이스로의 인바운드 RDP를 차단하는 새로운 정책을 추가했습니다. 고객은 클릭 몇 번만으로 새로운 세그멘테이션 정책을 생성하고 적용해 처음부터 미래의 공격자가 머신을 감염시키지 못하게 막았습니다. 사후 분석에서 보안팀은 널리 알려진 주요 랜섬웨어 위협 공격자를 가리키는 모든 지표를 빠르게 파악했습니다. 만약 공격자가 공격에 성공했다면 일반적인 기법을 계속 사용해 입수할 수 있는 모든 데이터를 암호화하고 랜섬 요구 메시지를 보내려 했을 것입니다. ERP 시스템과 같은 비즈니스 크리티컬 자산이 감염되었다면 심각한 장애와 다운타임이 발생했을 것입니다.

점차 복잡해지는 위협에 대응하려면 새로운 보안 전략이 필요합니다. XDR과 NGAV는 당분간 사라지지 않겠지만, 엔드포인트와 데이터 센터 자산을 보호해 불가피한 유출의 영향 범위를 제한하려면 마이크로세그멘테이션을 활용하는 것이 가장 효과적인 방법입니다. Akamai Guardicore Segmentation은 엔드포인트 간 무단 또는 불필요한 측면 이동을 완전히 차단합니다. 기존 엔드포인트 보안을 마이크로세그멘테이션으로 보완하면 방해가 되고 비용이 많이 드는 보안 사건을 더 쉽게 방지할 수 있습니다. 더불어 종합적인 보안 전략으로 사용할 경우, 제로 트러스트 상태로 향하는 여정에서 다음 단계로 나아갈 수 있습니다.

> Akamai Guardicore Segmentation은 비즈니스를 방해할 수 있는 공격이 확산하는 것을 억제합니다.
>
> **CISO**
>
> 대표적인 생명 보험 회사

마이크로세그멘테이션을 활용한 엔드포인트 보호, 랜섬웨어 방지, 제로 트러스트로의 전환에 대한 자세한 정보는 akamai.com를 방문하거나 Akamai 영업팀에 문의하세요.