AKAMAI 고객 사례

통신 인프라 공급업체

Akamai와의 협력으로 랜섬웨어를 차단

100만 달러의 잠재적 손실 방지

잠재적 섀도우 IT 방지

East-West 트래픽 가시성

고객사

오늘날 빠르게 변화하는 세계에서 기업과 주민들이 연결되도록 지원하는 미국의 통신 인프라 공급업체가 있습니다. 이 기업은 고객이 일상 생활에서 사용하는 셀 타워와 파이버 네트워크로 이루어진 광범위한 네트워크를 책임지고 있습니다.

도전 과제

제한적인 엔드포인트 가시성과 제어

기업 전체에 배치된 노트북은 6천 개가 넘습니다. IT 보안 팀은 이렇게 널리 배치된 노트북으로 인해 더 광범위한 환경에 IT 리스크가 발생하지 않을지 우려하고 있었습니다. 또한 기업의 파워 유저(Power User)에 의해 발생하는 섀도우 IT 작업 문제도 해결해야 했습니다.

최종 사용자 컴퓨팅 팀에서 몇 가지 보안 조치를 취했지만 범위는 제한적이었습니다. 사용자의 시스템 접속을 정밀하게 제어하거나 P2P 통신을 제한해 멀웨어 전파를 효과적으로 차단할 방법이 없었습니다. 이 기업은 멀웨어 전파에 대해 크게 우려하고 있었습니다.

이러한 문제를 해결하기 위해 이해 관계자들은 직원의 디바이스에 대한 가시성과 세부 세그멘테이션 제어를 확장할 수 있는 솔루션을 도입해 비즈니스 보안 체계를 개선하려고 했습니다. 또한 이를 통해 무단 측면 이동을 관측하고 방지할 수 있다고 판단했습니다.

솔루션 선택

보안 관계자들은 한동안 Akamai Guardicore Segmentatio을 검토하면서 여러 사이버 보안 사용 사례에 이 플랫폼을 활용하는 데 관심을 가졌습니다. 이 기업은 정밀한 가시성과 간편한 정책 생성 프로세스에서 커다란 잠재력을 확인하기 위해 단계적 접근 방식을 채택하기로 결정했습니다.

통신 인프라 공급업체

위치
미국

업계
통신 인프라

솔루션
Akamai Guardicore Segmentation

주요 장점
- 랜섬웨어 차단
- 섀도우 IT 차단
- East-West 트래픽 가시성

Akamai의 소프트웨어 정의 세그멘테이션 정책은 기본 인프라와 연동되지 않기 때문에 이 기업은 매우 다양한 보안 이니셔티브에 대응할 수 있었습니다. 하지만 직원 노트북의 리스크가 높은 것으로 밝혀지면서 팀은 엔드포인트에 Akamai 에이전트를 배포하는 것을 우선 순위로 정했습니다.

Akamai Guardicore Segmentation

일단 프로젝트가 시작되자 Akamai의 효율적인 Windows 에이전트를 기업의 컴퓨터에 신속하게 롤아웃했습니다. 이를 통해 사용자 접속 및 노트북 활동에 대한 프로세스 수준의 가시성을 확장할 수 있었습니다.

그런 다음 IT 보안 팀은 정확한 환경 데이터를 기반으로 이러한 엔드포인트에 대한 보안 제어를 중앙에서 생성하고 관리할 수 있었습니다. 그리고 로그인 시도 실패 등 특정 Microsoft RDP(Remote Desktop Protocol) 활동에 대한 알림을 비롯한 여러 정책을 즉시 설정했습니다.

세분화된 가시성

배포 직후, 비정상적인 RDP 관련 활동을 보고하도록 설정된 정책이 많은 알림을 전달했습니다. 로그인 실패가 관측된 후 공격자가 실패한 로그인 정보로 무차별 대입 공격을 시도한 것이 곧바로 드러났습니다.

IT 보안 팀은 상황을 면밀히 모니터링했습니다. 해커들이 공격을 계속 진행했기 때문에 Akamai 에이전트를 이용해 모든 엔드포인트에서 RDP를 차단하기로 결정했습니다. 몇 번의 클릭만으로 RDP를 비활성화하는 새로운 세그멘테이션 룰을 생성하고 적용해 엔드포인트가 하나라도 감염되기 전에 공격자를 막았습니다.

랜섬웨어 차단

사후(Postmortem) 프로세스에서 보안 팀은 널리 알려진 주요 랜섬웨어 위협 공격자를 가리키는 모든 지표를 빠르게 파악했습니다.

만약 공격이 성공했다면, 공격자들은 일반적인 기법을 계속 동원해 금품 요구 메시지를 보내기 전에 입수할 수 있는 모든 데이터를 암호화하려고 했을 것입니다. 이 기업의 규모와 현재의 트렌드를 고려해볼 때, 공격자는 분명 100만 달러 이상의 금액을 요구했을 것입니다. ERP 시스템과 같은 비즈니스 크리티컬 자산이 감염되었다면 심각한 장애와 다운타임이 발생했을 것입니다.

그러나 신속한 조치를 취한 보안팀과 Akamai 덕분에 이 기업은 공격 시도의 영향을 전혀 받지 않았습니다.

섀도우 IT 차단

외부 위협의 차단 외에도 보안팀은 Guardicore Centra 보안 플랫폼을 사용해 내부 문제를 해결할 수 있었습니다. Akamai가 지원하기 전에는 엔드포인트 가시성이 제한적이어서 일부 사용자가 공식 프로세스를 우회해 기업의 정책을 준수하지 않고 독자적으로 활동하기가 더 쉬웠습니다. 엔드포인트에 보안 제어를 적용하는 새로운 인사이트와 기능을 통해 IT 보안팀은 섀도우 IT를 억제할 수 있었습니다. 여기에는 DevOps 팀원이 공식 채널을 거쳐 승인을 받지 않으면 독자적으로 새로운 리소스를 이용하지 못하게 하는 기능이 포함되었습니다.

Akamai와의 협력으로 방어 확장

이 통신 인프라 공급업체의 경우 엔드포인트 보안은 시작에 불과합니다. 곧 더 많은 새로운 기능을 살펴보고, 데이터 센터에 Akamai를 롤아웃하며, Citrix 환경을 보호하고, 외부 벤더사에 써드파티 접속 제어를 적용할 계획입니다.

이 기업은 Guardicore 플랫폼의 유연한 특성 덕분에 M&A 전략이나 디지털 트랜스포메이션 이니셔티브가 미래에 어떻게 전개되든, 환경 내 모든 곳에서 첨단 위협에 대응하는 보안 기능을 확장할 수 있다고 확신합니다.

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.