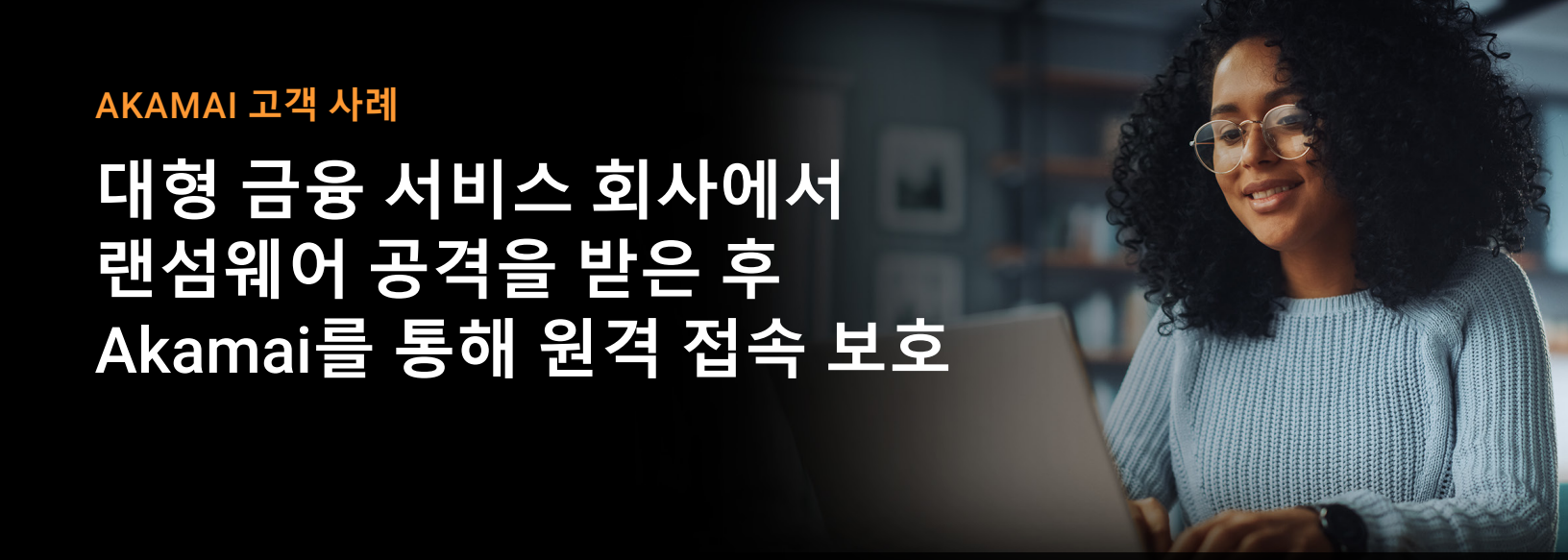
AKAMAI 고객 사례

대형 금융 서비스 회사에서 랜섬웨어 공격을 받은 후 Akamai를 통해 원격 접속 보호



포괄적인 네트워크 가시성

신속한 정책 수립

원격 근무 인력 보안

고객사

브라질에 본사를 둔 대형 금융 서비스 회사.

도전 과제

원격 접속의 증가

많은 기업과 마찬가지로 코로나19 팬데믹으로 인해 이 금융 서비스 공급업체에서도 원격 접속 요구가 증가했으며, 은행의 IT 직원 상당수가 회사에서 관리하는 디바이스를 사용해 재택 근무로 전환했습니다. 사용자가 주로 보안 기업 네트워크 외부에서 업무에 필요한 데이터와 애플리케이션에 접속하기 시작하자 기업의 공격표면이 급격히 확장되었습니다.

성공적인 랜섬웨어 인시던트

재택 근무 모델로 전환한 직후 은행은 중요한 Oracle Cloud 데이터베이스가 랜섬웨어 공격에 당했고, 나중에서야 VDI 환경에서 공격이 시작된 사실을 알게 되었습니다. 보안 및 IT는 신속한 조치를 취해 민감한 금융 데이터의 손실을 제한해야 했습니다. 또한 원래 공격 기법을 파악하고 방어할 수 없다면 랜섬웨어가 백업 서버와 기업의 프로덕션 환경 모두에 측면으로 확산될 리스크가 있다는 점도 알고 있었습니다. 이 같은 리스크가 현실이 되면 은행은 막대한 데이터 및 재정적 손실을 입을 것이 당연했습니다.

솔루션 선택

Akamai Guardicore Segmentation은 이미 은행의 다른 분야에서 널리 사용되고 있었습니다. 랜섬웨어 공격이 발생하기 전에 이 플랫폼은 온프레미스, 가상, 베어메탈, VDI 인프라, 그리고 Azure 및 OpenShift 컨테이너 환경을 아울러 워크로드를 포함하는 23,000대가 넘는 서버에 대한 세그멘테이션 정책을 관리하고 적용하는 작업을 담당했습니다.

Large Financial Services Company

업계
금융 서비스

솔루션
Akamai Guardicore Segmentation

주요 장점

- 측면 이동을 통한 랜섬웨어 확산 방어
- 네트워크 흐름에 대한 정밀한 가시성 제공
- VDI 환경을 세그멘테이션해 원격 접속 보호
- 신속한 인시던트 대응 지원

Akamai

이 솔루션은 소프트웨어 기반 세그멘테이션 솔루션으로, 이전에는 은행이 관리자 점프 박스 접속 관리 및 Swift 애플리케이션 세그멘테이션 등 여러 가지 보안 및 컴플라이언스 이니셔티브를 실현하는 데 사용되었습니다. 대응 팀은 뛰어난 가시성과 신속한 정책 수립을 지원하는 플랫폼의 역량을 파악한 후 Akamai Guardicore Segmentation의 기능을 활용해 유출 문제를 신속하게 해결했습니다.

Akamai Guardicore Segmentation의 장점

프로세스 수준의 가시성

은행의 대응 팀은 플랫폼을 통해 과거의 통신 흐름을 조사했습니다. 그리고 Oracle Cloud 데이터베이스와 통신하는 데이터베이스 관리자의 원격 VDI 연결에서 랜섬웨어가 처음 침투한 사실을 추적했습니다.

신속한 정책 수립

공격 기법을 탐지한 후 팀은 VDI 세그멘테이션을 신속하게 추적해 이 부분의 해결을 최우선 과제로 삼았습니다. 정책 계획 프로세스는 토요일에 시작되었고 Akamai Guardicore Segmentation의 가시성 기능을 사용해 잠재적인 정책 요구사항을 파악했습니다. 그리고 다음 주 화요일까지 Oracle Cloud에 대한 3,000개가 넘는 VDI 연결과 관련해 적용 가능한 정책이 수립되었습니다.

랜섬웨어 복구

팀은 백업 애플리케이션에 Akamai 에이전트를 배포하고 애플리케이션 링펜싱을 설정해 자산과 통신할 수 있는 대상을 프로세스 수준까지 정의했습니다. 그런 다음 유출된 영역에 배포해 글로벌 거부 룰을 사용함으로써 랜섬웨어의 추가 전파를 차단했습니다.

원격 작업자 접속으로 인한 추가적인 리스크를 줄이기 위해 콜 센터 직원이 사용하는 두 가지 VDI 솔루션에 대한 정책도 수립해 은행 엔드포인트 간 무단 측면 이동 방지를 한층 더 강화했습니다.

불과 3일 만에 세그멘테이션 정책을 적용함으로써 금융 서비스 기업은 랜섬웨어 인시던트의 영향을 크게 줄이고 원격 접속 보안을 크게 개선할 수 있었습니다.

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.

> [Akamai Guardicore Segmentation] 솔루션이 제공하는 가시성은 어둠을 밝혀주는 한 줄기 빛과도 같았습니다.
>
> 대형 금융 서비스 회사의 인프라 보안 책임자