Case Study

AhnLab

HTTPS SaaS 환경에서 가시성과 행위 제어를 동시에 확보한 보안 전략

업종
IT

규모
대기업

도입제품
AhnLab TrusGuard

J사는 클라우드 기반 업무 환경과 SaaS 애플리케이션 사용이 확대되면서, 기존 네트워크 보안 체계의 한계에 직면했다. 특히 HTTPS 기반 암호화 트래픽과 CDN 환경이 확산되면서 서비스 식별과 사용자 행위에 대한 가시성이 저하되었고, 기존 정책으로는 이를 효과적으로 통제하기 어려운 상황이었다. 이에 J사는 암호화 트래픽 가시성 확보와 사용자 행위 기반 보안 통제를 핵심 과제로 네트워크 보안 구축이 필요했다.

Key Results

- HTTPS 기반 환경에서도 완전한 트래픽 가시성 확보
- SaaS 애플리케이션에 대한 행위 기반 보안 통제 구현
- CDN 및 공유 IP 환경에서의 정밀한 애플리케이션 식별 및 제어
- SSL 예외 정책을 통한 서비스 안정성 유지
- 보안 수준과 업무 연속성을 동시에 보장하는 균형 잡힌 보안 운영 체계 구축

주요 과제 (Key Challenges)

J사가 직면한 과제는 단순히 보안 장비의 성능 문제가 아니라, 변화한 업무 환경에 기존 보안 모델로는 더 이상 충분히 대응하기 어려워졌다는 점이었다.

1) CDN 기반 서비스 환경에서의 애플리케이션 식별 불가

많은 글로벌 SaaS 애플리케이션이 CDN을 기반으로 동일한 IP와 도메인을 공유하는 구조를 가진다. 이로 인해 기존의 IP/FQDN 기반 정책으로는 업무용 서비스와 비업무 서비스의 구분이 불가능했으며, 서비스별로 상이한 정책을 적용하는 것도 어려웠다.

2) HTTPS 암호화로 인한 보안 가시성 상실

대부분의 업무 트래픽이 HTTPS 기반 협업 도구로 전환되면서, 기존 보안 장비로는 트래픽 내부의 콘텐츠와 사용자 행위를 식별할 수 없었다. 이로 인해 내부 데이터 흐름에 대한 통제와 모니터링이 제한되었고, 보안 사각지대가 발생했다.

3) 사용자 행위 기반 정책 부재

기존 정책은 IP, 포트, URL 중심으로 설계되어 있었기 때문에,파일 업로드, 메일 전송, 외부 공유와 같은 실제 사용자 행위 단위의 통제가 불가능했다. 이는 내부자에 의한 정보 유출 및 비인가 행위에 대한 대응력을 크게 제한하는 요소였다.

해결 방안(Solutions)

J사는 기존 네트워크 중심 보안 모델에서 벗어나 가시성 확보, 행위 기반 제어, 안정성 유지 세가지 축을 중심으로 네트워크 보안 구조를 재설계했다.

동작 방식(Operational Flow)

1. 사용자가 HTTPS 기반 SaaS 서비스에 접속
2. 트래픽이 TrusGuard를 경유하며 SSL 세션 재구성
3. 트래픽 복호화를 통해 내부 콘텐츠 확보
4. 애플리케이션 제어 엔진이 콘텐츠 및 행위 분석 수행
5. 정책에 따라 허용, 차단, 세션 종료 등의 제어 실행
6. 특정 서비스는 예외 정책에 따라 복호화 없이 통과

1) SSL Inspection을 통한 가시성 확보

TrusGuard는 HTTPS 트래픽을 중간에서 복호화하여, 암호화된 구간 내부의 요청 정보, 콘텐츠, 트래픽 흐름 등 분석이 가능하다. 이를 통해 기존에는 확인할 수 없었던 SaaS 애플리케이션 내부의 동작과 데이터 흐름까지 가시화할 수 있게 되었다.

2) 애플리케이션 기반 행위 제어

TrusGuard를 통해 복호화된 트래픽은 애플리케이션 제어 엔진에서 분석되며, URL, 헤더, 파일 유형, 요청 방식 등을 기반으로 사용자 행위를 식별한다.
예를 들어, 파일 업로드 요청, 메일 첨부파일 전송, 외부 공유 시도와 같은 행위를 구분하여 정책을 적용할 수 있으며, 이를 통해 단순 접속 제어를 넘어선 행위 기반 보안 정책 적용이 가능해졌다.

3) SSL 예외 정책을 통한 서비스 안정성 확보

SSL 복호화 시 일부 애플리케이션에서 인증 오류나 서비스 장애가 발생할 수 있다. TrusGuard는 이러한 서비스에 대해 선택적으로 복호화를 제외하는 예외 정책을 제공함으로써, 보안성과 서비스 가용성 사이의 균형을 유지할 수 있도록 했다.

도입 효과 (Business Outcomes)

TrusGuard 도입을 통해 J사는 보안 운영 방식을 근본적으로 변화시킬 수 있었다.

1) 사용자 행위 기반 통제 체계 확립

단순한 네트워크 접근 제어에서 벗어나, 애플리케이션 내부의 실제 사용자 행위를 기준으로 정책을 적용할 수 있게 되었다. 이를 통해 데이터 유출 가능성을 줄이고, 비인가 행위에 대한 대응력을 강화했다.

2) CDN 기반 SaaS 환경에 대한 통제 가능

IP 또는 도메인 기반 정책의 한계를 극복하고, 콘텐츠 기반 분석을 통해 CDN 환경에서도 애플리이션 단위 제어가 가능해졌다.

3) 암호화 환경에서의 가시성 확보

HTTPS 트래픽 내부까지 분석이 가능해지면서, 기존에 보이지 않던 트래픽 흐름과 사용자 활동을 식별할 수 있게 되었고, 보안 모니터링의 정확성과 범위가 크게 향상되었다.

4) 보안성과 업무 연속성의 균형 확보

SSL 예외 정책을 통해 서비스 장애 없이 안정적인 운영을 유지하면서도, 필요한 구간에서는 강력한 보안 정책을 적용할 수 있는 유연한 운영 체계를 구축했다.

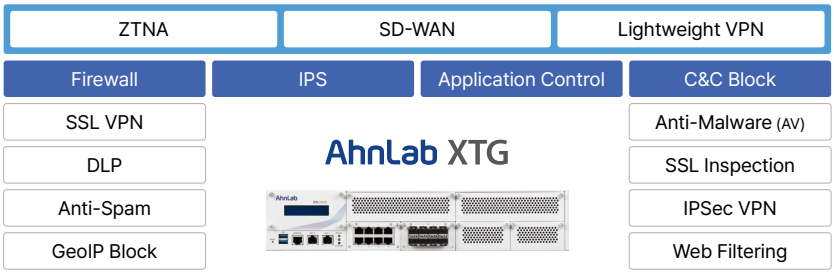
J사의 사례는 오늘날 기업 보안이 더 이상 단순한 네트워크 접근 제어로는 충분하지 않다는 점을 보여준다. 특히 SaaS와 HTTPS 중심 환경에서는, 가시성 확보와 사용자 행위 기반 제어가 결합된 보안 모델이 필수적이다.

AhnLab TrusGuard는 SSL Inspection과 애플리케이션 제어, 그리고 유연한 예외 정책을 통해 이러한 요구를 현실적인 방식으로 구현하며, 암호화된 환경에서도 실질적인 통제가 가능한 차세대 보안 운영 모델을 제공한다.

기존 환경 대비 개선 효과

Before	After
IP 기반 제어	행위 기반 제어
HTTPS 가시성 부족	전체 가시성 확보
SaaS 통제 불가	기능 단위 제어
장애 발생	예외 정책으로 안정

TrusGuard를 넘어, AhnLab XTG로 진화한 보안



더 강력해진 성능과 ZTNA 기반 보안 전략을 확인해 보세요.

제품 자세히 보기 →

데모 요청 →