

Positive Technologies
Application Firewall™



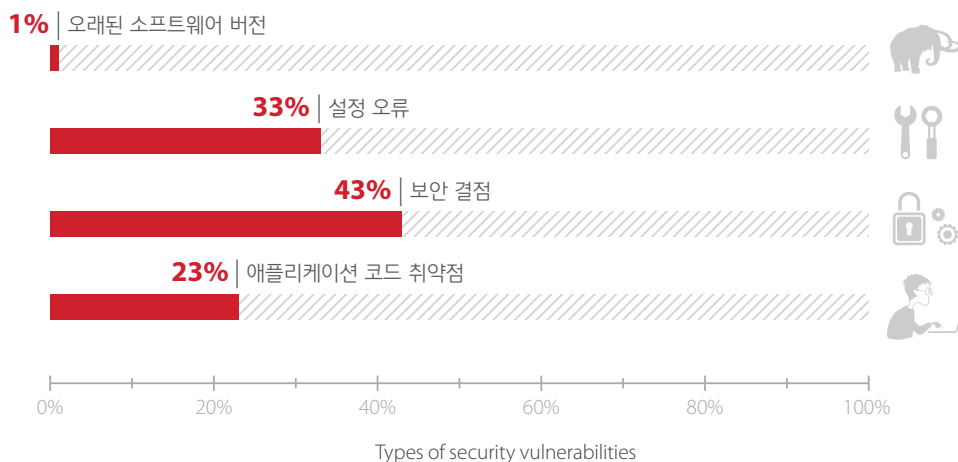
데이터 시트

최근 거의 모든 기업이 수백 개의 웹, 모바일, 또는 ERP 애플리케이션을 사용하여 사업을 운영합니다. 그러나 애플리케이션 수가 증가함에 따라 비즈니스에 피해를 주려는 목적으로 악용될 수 있는 보안 취약점도 증가하고 있습니다.

Verizon의 2016 Data Breach Investigation Report(DBIR)에 따르면, 웹 애플리케이션 공격이 데이터 보안 침해 원인 가운데 1위를 차지했습니다. 아울러, 2016년에 발생한 웹 애플리케이션 공격으로 발생한 데이터 보안 침해가 2015년의 약 7%에서 40%로 증가했습니다.

1. 애플리케이션 보안: 주요 과제

공격자들은 주로 어떤 종류의 애플리케이션 취약점을 이용할까요? Positive Technologies의 금융 기관용 엔터프라이즈 애플리케이션에 관한 연구조사 결과, 전체 문제점의 1/3만이 잘못된 패치 관리와 설정 오류로 인해 발생한 것으로 나타났습니다. 대부분의 위협은 기존 보안 스캐너, IDS, 방화벽 등으로는 해결할 수 없는 개발자 실수에서 비롯되었습니다.



그 결과, 기업 인프라의 평균 보안 수준이 최근 크게 하락했습니다. 다음은 최신 애플리케이션 보안 시스템이 직면한 주요 과제입니다.

- + Secure SDL를 구현할 경우, 코드 오류가 코딩 초기 단계에서 발견되고 수정되는 경우에 한해 코드 오류에 따른 비용을 크게 줄일 수 있습니다. 그러나, 코드 분석을 위한 효과적인 자동화 솔루션을 찾기란 어렵습니다.
- + 최신 기업 애플리케이션들은 서로 다른 언어, 프로토콜, 기술과 맞춤형 솔루션, 서드 파티 코드 등을 사용합니다. 그러한 애플리케이션을 보호하려면 애플리케이션 구조, 사용자 상호작용 패턴, 사용 컨텍스트 등에 대한 철저한 분석이 필요합니다.
- + 공격자들이 제로데이 취약점을 이용하는 경우가 많아 서명 분석은 무용지물이 되므로 적응형 솔루션, 자체 학습, 행동 분석 기법 등이 요구됩니다.
- + 최신 방화벽은 수천 개의 의심되는 인시던트를 다룹니다. 그러나 보안 전문가가 실제 위협을 식별하기 위해 그렇게 많은 인시던트를 전부 일일이 확인할 시간은 없습니다. 따라서, 보안 이벤트의 자동 분류, 우선순위 설정, 시각화 등의 도입이 시급합니다.
- + 잘 알려진 취약점들도 즉각적인 수정은 불가능합니다. ERP 또는 인터넷 뱅킹 시스템에 보안 패치를 적용하는 데에도 수개월이 걸릴 수 있습니다. 애플리케이션 보안 시스템에는 개발자가 코드를 수정하는 동안 보안 침해의 위험성을 줄여줄 수 있는 메커니즘이 반드시 필요합니다.

2. PT APPLICATION FIREWALL™을 소개합니다

Positive Technologies가 개발한 지능적 보안 솔루션 PT Application Firewall™(PT AF™)은 오늘날 다양한 웹 포털, ERP, 모바일 애플리케이션에서 비롯되는 보안 과제에 대한 본격적인 대응책입니다. PT AF는 SQLi, XSS, XXE 등 OWASP 및 WASC가 인정하는 모든 일반적 공격 유형과 HTTP Request Splitting, Clickjacking, 복잡한 클라이언트 사이드 공격(DOM 기반 XSS) 등에 대한 포괄적인 보안을 제공합니다. 혁신적 기술과 접근방식의 강력한 결합을 통해 일관된 결과입니다.

- + **지속적인 실시간 보호.** PT AF는 기존의 서명 방식을 적용하지 않고, 네트워크 트래픽, 로그, 사용자 동작 등을 분석하여 일반 작동 시간에 애플리케이션의 실시간 통계 모델을 생성하고 지속적으로 관리합니다. PT AF는 이 모델을 이용하여 비정상적 시스템 행동을 탐지합니다. 다른 보호 메커니즘과도 연동합니다. 이를 통해 클라이언트 내에 특별한 조절 없이도 제로데이 공격의 80%가 차단됩니다.
- + **주요 위협에 집중.** PT AF는 데이터 도난, 백도어 셋업 등과 같은 공격 체인을 자동 탐지합니다. 보안 전문가의 수천 개의 잠재적 공격을 일일이 살펴볼 필요 없이 가장 심각한 위협에 대한 경고만 수신합니다.
- + **P-Code: 즉각적인 차단.** 가상 패칭 기법(P-Code)이 취약한 코드가 수정되기도 전에 애플리케이션을 보호합니다. 대부분의 WAF가 각 패치의 수동적 생성을 요구하는 것과 달리, PT AF는 Positive Technologies 고유의 소스 코드 분석 기술을 안전한 익스플로잇 생성 메커니즘과 결합합니다. 이를 통해, 탐지된 취약점을 기반으로 가상 패치가 자동 생성됩니다.
- + **첨단 L7 DDoS 차단.** 세 가지 애플리케이션 스트레스 지표(RPS, 응답 시간, 오류율)를 바탕으로 PT AF는 L7 DDoS 공격을 탐지할 뿐만 아니라 예측하고 차단합니다. PT AF는 머신러닝 알고리즘을 바탕으로 지속적인 행동 프로파일링을 수행하므로, 수신되는 모든 HTTP 요청과 애플리케이션 건강 상태를 다룰 수 있습니다. DDoS 공격이 예측되면 이를 통보 받은 보안 엔지니어가 비즈니스 중단 없이 실행 계획을 능동적으로 시행할 수 있습니다. 또한, 고도의 자동화가 인간의 개입을 최소화하고, 확장된 기능이 제공되므로 서드 파티의 DDoS L7 모니터링 툴이 필요 없습니다.
- + **Bot 완화.** PT AF 내의 첨단 봇 탐지 메커니즘은 서명 기반 분석과 휴리스틱 분석의 지능적 결합을 기반으로 하여 악의적이지 않은 봇의 활동에 영향을 주지 않고 봇 공격을 성공적으로 탐지하고 차단합니다.
- + **데이터 유출 방지.** 모든 아웃바운드 트래픽이 모니터링되고, 민감한 데이터는 인력의 개입 없이 모두 자동 차단됩니다(마스킹).
- + **최종 사용자 데이터의 기밀성 극대화.** 애플리케이션 사용자에게 대한 보안을 강화하기 위해 관리자는 결제 카드 번호, 여권 정보, 보험 정보 등 민감한 데이터의 탐지를 위한 특별 규칙을 생성할 수 있습니다. 그 외에도 이러한 정보를 서드 파티, 나아가서는 PT AF를 사용하는 관리자로부터 마스킹하는 데 규칙이 사용됩니다.

Positive Technologies 는
2017년 가트너 매직쿼드란트
(Gartner Magic Quadrant)
웹 애플리케이션 방화벽
부문에서 3년 연속 비저너리로
선정되었습니다.

자세한 내용은 당사 웹 사이트
ptsecurity.com을 방문하십시오.

기타 기능:

- + **능동적 방어.** 쿼리, 데이터, 쿠키를 능동적으로 방어하므로, 개발자가 필요한 보안 툴을 간과한 경우에도 CSRF와 같은 공격을 차단할 수 있습니다.
- + **효율적 통합.** 기업의 정보 보안 관리 시스템과 효과적으로 통합합니다. 안티바이러스, DLP, 안티 DDoS, SIEM은 물론, Check Point, Arbor 등 서드 파티 솔루션과 통합하여 첨단 다계층 보호를 제공합니다.
- + **보안 우회로부터 보호.** PT AF는 보호 대상 서버 기술 스택에 관련하여 데이터를 처리하고, XML, JSON 및, 오늘날의 포털과 모바일 애플리케이션에 주로 사용되는 기타 프로토콜을 분석합니다. 이로써, HPC, HPP, Verb Tampering 등 대다수의 방화벽 우회 방식을 차단할 수 있습니다.
- + **PCI DSS와의 컴플라이언스.** 그 밖의 국제, 국내, 기업 보안 표준과의 컴플라이언스를 보장합니다.

3. 유스 케이스: 특별한 상황

Positive Technologies의 전문가들은 15년 이상의 보안 연구 경험 및 방대한 취약점 지식 기반을 바탕으로 여러 업계에서 다양한 규모의 기업들을 보호해 왔습니다. 각 업계마다 실제 보안에 중요한 고유의 특징과 요구사항이 있습니다. PT Application Firewall 구축에는 각 고객의 특정 요구사항을 충족하는 설정이 포함됩니다.



은행 및 금융 기관

고유의 과제:

- + 아래와 같은 주요 애플리케이션을 고객과 협력사가 모두 사용합니다: 인터넷 뱅킹, 코어 뱅킹 시스템, CRM, 상거래 등
- + 은행이 자체적으로 취약점을 수정할 수 없는 서드 파티 애플리케이션이 많습니다.
- + 1년 365일 24시간 운영으로 인해 취약점 해결책 개발과 구축의 여지가 거의 없습니다.
- + 보안 기능이 거의 없는 레거시 시스템이 사용되고 있습니다.
- + 악의적 사용자, 수동 및 자동 공격에 관심이 집중되어 있습니다
- + PCI DSS 및 기타 규제 당국의 요구사항이 존재합니다.

PT AF 솔루션:

- + 백도어, 민감한 정보, 평문 데이터 흐름 등의 탐지
- + 은닉 마르코프 모델 기반의 자체 학습 메커니즘
- + 사용자 모니터링 및 핑거프린팅, 웹 사기 탐지
- + 가상 패치
- + 단순 결함의 수정되는 동안 정상 애플리케이션 운영 지원
- + 신용카드 번호 등 최종 사용자의 기밀 데이터에 대한 보안 강화

언론

고유의 과제:

- + 인터넷 사용자 누구라도 애플리케이션 이용 가능
- + 콘텐츠의 잦은 새로 고침 및 다양한 다른 사이트들(광고, 소셜미디어, 파트너 등)과의 연동
- + 온라인 스트리밍 및 데이터 통산용 XML 게이트웨이
- + 해커비스트, 경쟁사, 범죄자 등의 공격

PT AF 솔루션:

- + 애플리케이션 파라미터를 이용한 자동 학습
- + 애플리케이션 레벨 DDoS 공격의 차단
- + 사이트 해킹 및 데이터 유출의 탐지
- + 서명 기반 메커니즘과 유리스틱 메커니즘, 평판 서비스 등이 고객의 의심되는 행동을 탐지하는 데 이용됩니다.

통신

고유의 과제:

- + 자체 서비스 포털, 고객용 VAS/MSS 포털, 모바일, 클라우드 애플리케이션 등 여러 다양한 애플리케이션
- + 통합 및 긴밀한 연동은 하나의 요소에서 발생한 장애가 기업의 모든 부분에 문제를 야기하는 '눈사태적인' 반응으로 이어집니다.
- + 단순 대량 서비스와 결제 시스템과의 통합은 사기의 위험성을 야기합니다.

PT AF 솔루션:

- + VAS /MMS 모델의 지원: 고객 애플리케이션의 보호
- + 서명 기반 메커니즘과 유리스틱 메커니즘, 평판 서비스 등이 고객의 의심되는 행동을 탐지하는 데 이용됩니다.
- + 애플리케이션 레벨 DoS 공격의 차단
- + 모바일 애플리케이션 버전의 보호

유틸리티

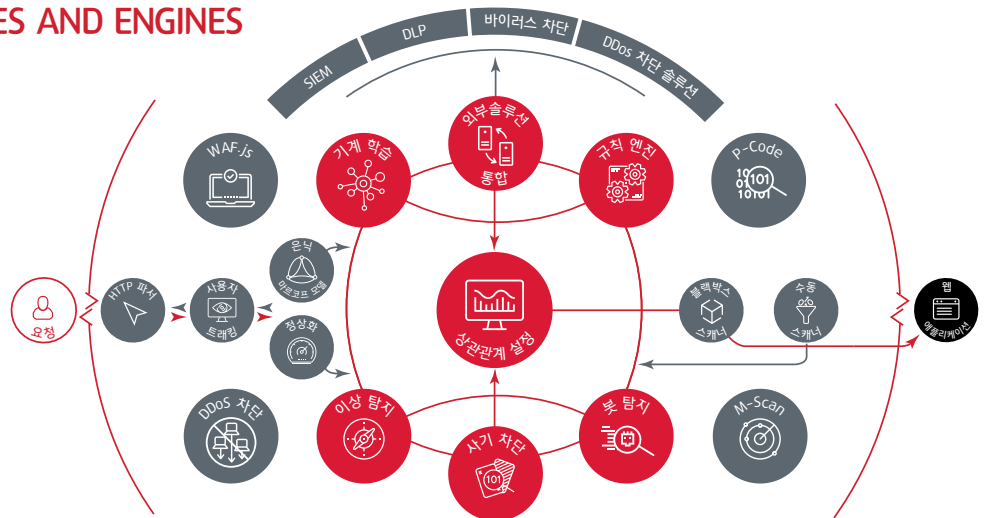
고유의 과제:

- + ERP 시스템은 회계, 관리, 구매 등 다양한 프로세스를 통합 게이트웨이를 통해 인터넷 액세스(SRM, CRM, HCM)로 제어합니다.
- + 시스템은 시스템 통합 업체가 유지보수하고 지원하는 경우가 많아 원격 제어가 필요합니다.
- + 원격 접근을 간소화하기 위해 보안 메커니즘이 약화될 수 있습니다.
- + 비즈니스 애플리케이션 개발자는 보안보다 기능에 집중하는 경향이 있습니다.
- + 시스템에는 정기적인 수정이 필요합니다.
- + 1년 365일 24시간 운영으로 인해 취약점 해결책 개발과 구축의 여지가 거의 없습니다.

PT AF 솔루션:

- + 포털 SAP 솔루션에 사전 학습된 모듈 적용
- + XML 관련 공격 차단
- + 가상 패치

4. HOW IT WORKS: MODULES AND ENGINES



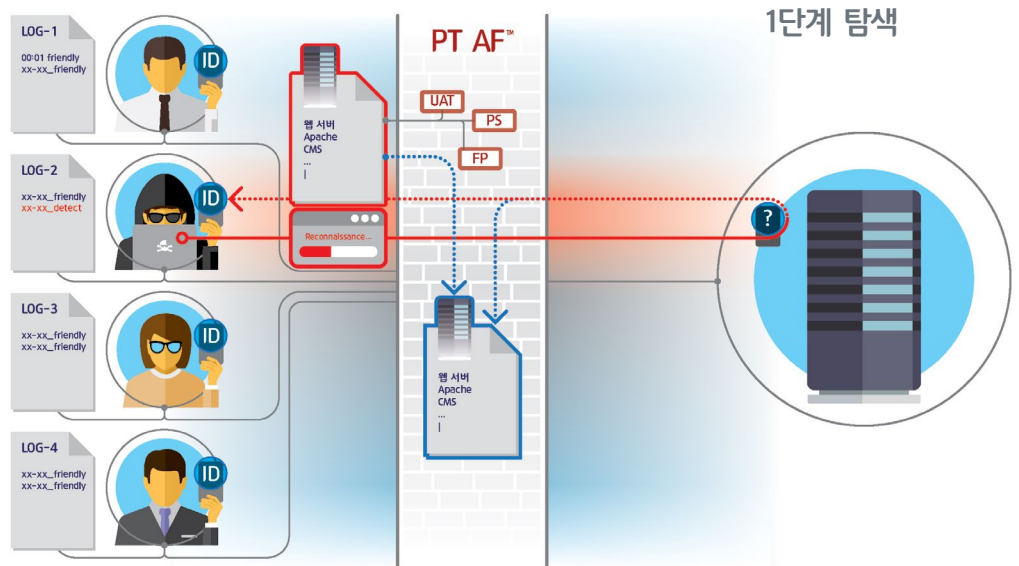
웹, 모바일, ERP 애플리케이션의 정확하고 침투 불가능한 보호를 위해 PT Application Firewall™은 다양한 전문 모듈이 포함된 다계층 방어 스킴을 사용합니다.

- + **User Tracking** 은 보호 대상 애플리케이션 이용 시 사용되는 사용자 계정의 지오로케이션을 비롯한 세션 데이터를 관리자가 분석할 수 있도록 하는 기능입니다. 이 기능을 통해 PT AF 관리자는 사용자 및/또는 사용자 그룹별로 차단 규칙을 추가하고, 접근 제어 목록을 통해 접근을 관리할 수 있습니다. 또한 의심되는 활동이 발생하는 경우에 보안 인시던트를 식별하여 웹 사기를 예방할 수 있습니다. 아울러, PT AF™는 다수의 로그인 시도 실패를 탐지하고, 그러한 인시던트들을 연결시켜 신속하게 브루트포스 공격을 식별하고 차단합니다.
- + **Web Engine**은 내장형 Dynamic Application Security Testing(DAST) 모듈로서 애플리케이션 구성요소(CMS, 프레임워크, 라이브러리)의 능동적 핑거프린팅, 자체 학습 엔진의 훈련, 애플리케이션 취약점의 탐지 등에 사용됩니다. 웹 엔진은 공격자가 탐지한 취약점을 신속하게 검증하는 데 사용될 수 있습니다.
- + **Passive Scan**은 애플리케이션 구성요소(CMS, 프레임워크, 라이브러리 등)를 소극적으로 핑거프린팅하고, 알려진 취약점(CVE 기반) 및 데이터 유출을 탐지합니다.
- + **Normalization**은 HPP, HPC, 기타 데이터 조작 공격 등에 의한 보안 우회를 예방하기 위해 백엔드 웹 애플리케이션 핑거프린트(웹 서버, 언어, 프레임워크)에 따라 HTTP 데이터와 헤더를 재구성합니다.
- + **서드 파티 연동** PT AF는 내장형 AV 엔진과 민감한 데이터 탐지 규칙을 사용하지만 외부 안티바이러스 및 DLP 솔루션과도 연동이 가능합니다. 대규모 DDoS 공격을 차단하기 위해 PT AF는 봇의 IP 주소를 Arbor와 같은 외부 안티 DDoS 솔루션에 보고할 수 있습니다.
- + **Rule engine**은 알려진 CVE 취약점 전체를 비롯하여 취약점에 대한 사용자 정의 규칙을 생성합니다. 추가적인 지오로케이션 튜닝이 특정 지오로케이션을 바탕으로 하는 차단 규칙 및 제외의 생성을 지원하므로 특정 지역에서 비롯되는 공격을 표적으로 차단할 수 있습니다.
- + **WAF.js** 는 보호 대상 페이지가 열릴 때마다 사용자 브라우저에서 실행되는 클라이언트 사이드 공격(XSS, DOM, XSS, CSRF, Clickjacking)을 차단하는 JavaScript 모듈입니다.
- + **휴리스틱스** 자체 학습 인공 지능 알고리즘을 기반으로 PT AF는 요청 속성을 지속적으로 추적하여 알려지거나 알려지지 않은(제로데이) 공격을 탐지합니다.
- + **Correlation**은 경고 횟수를 줄여주고, 애플리케이션 핑거프린트, 취약점, 사용자 추적, 공격 히스토리 등을 기반으로 중요한 인시던트를 강조합니다. 또한, 공격 체인 지표를 구성하여 포렌식을 간소화합니다.
- + **Data masking** 은 결제 카드 번호, 여권 데이터, 보험 정보 등 최종 사용자 정보의 기밀성을 보장하며, 웹 애플리케이션 내에 탐지된 사소한 결점이 수정 완료될 때까지 웹 애플리케이션이 계속 정상 작동하도록 지원합니다.

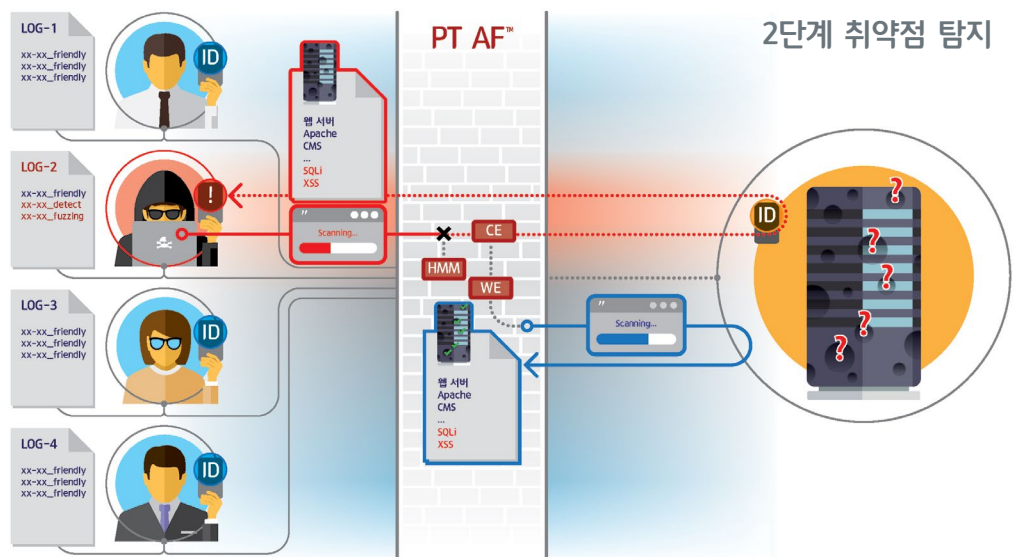
고유의 P-Code Module이 애플리케이션의 즉각적인 보호를 위해 소스 코드 취약점을 탐지하고, 차단 규칙(가상 패치)을 자동 생성합니다. 따라서, 개발자가 취약한 코드를 수정할 시간을 확보할 수 있습니다.

5. 공격 및 방어 시나리오

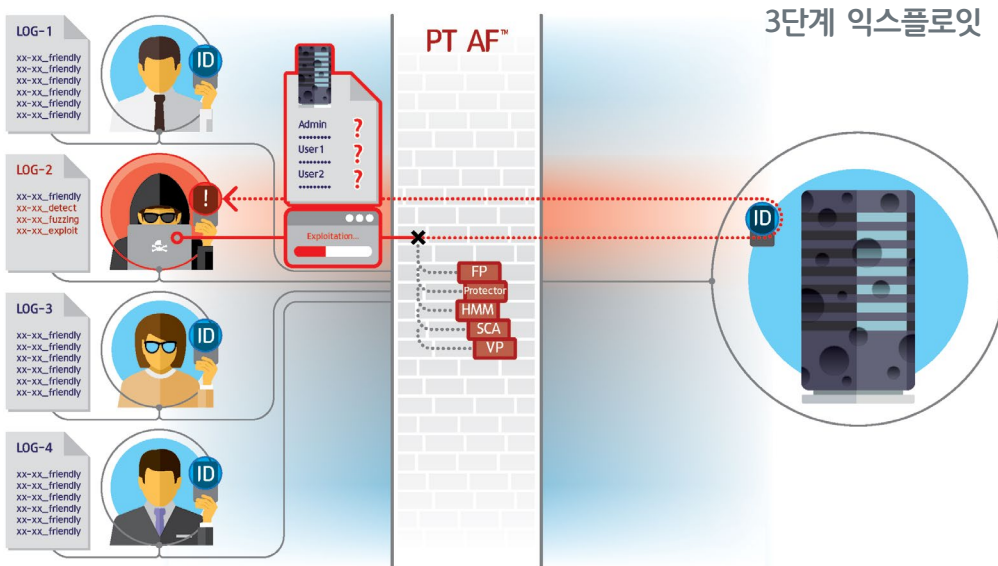
일반적인 공격은 몇 개의 단계로 이뤄집니다. PT Application Firewall이 애플리케이션을 실시간으로 보호하기 위해 공격자 활동의 각 요소에 반응하는 방법을 확인해 보겠습니다.



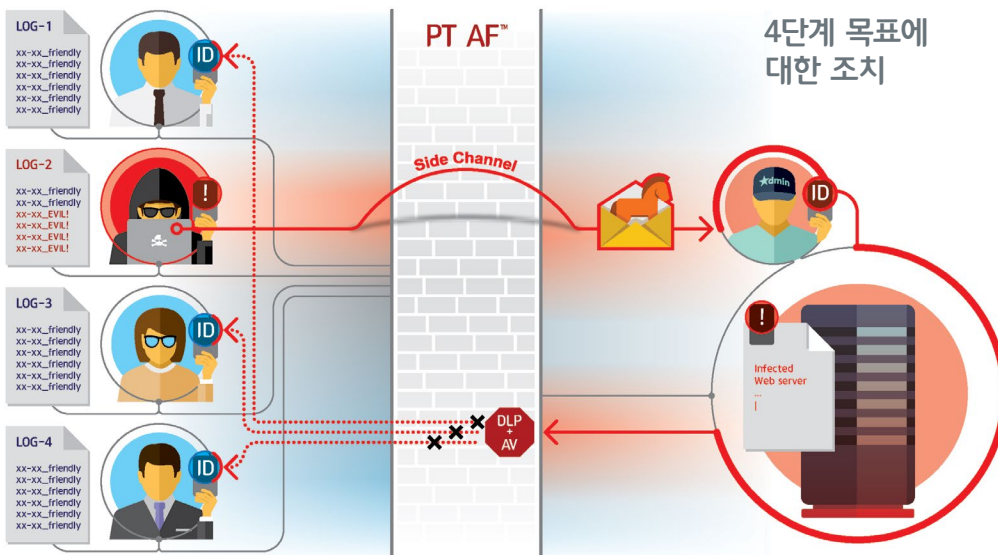
1단계 탐색. 공격자는 애플리케이션의 논리와 아키텍처를 연구하고, 사용되는 서비스, 소프트웨어 구성요소, 프레임워크를 파악합니다. PT Application Firewall Normalization and Protection 엔진은 보호 대상 애플리케이션의 특정 행동에 따라 설정 가능합니다. 이를 통해 PT AF는 탐지율을 최대화하고, 잠재적 우회를 예방합니다.



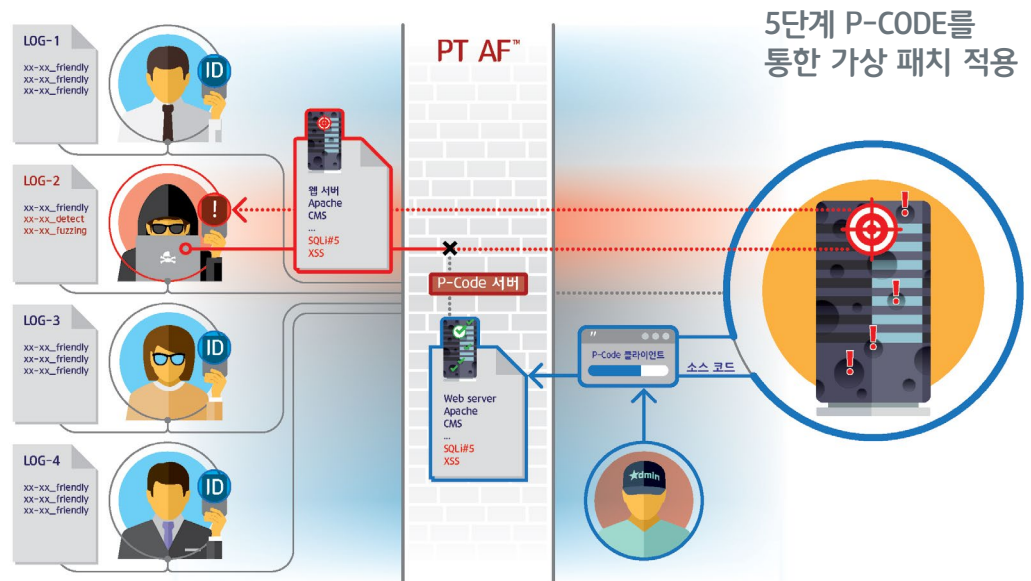
2단계 취약점 탐지 공격자가 취약점을 적극적으로 탐지하려고 하는 동안 PT AF는 내장형 DAST Web Engine을 이용하여 공격 대상 취약점의 존재를 확인합니다. 자체 학습 은닉 마르코프 모델(HMM) 모듈은 초기 단계의 공격도 경고(또는 선택에 따라 차단)할 수 있습니다.



3단계 익스플로잇. 공격자가 애플리케이션에서 취약점을 식별하면, 시스템 고장을 일으키거나 민감한 데이터에 대한 접근권한을 얻기 위해 취약점의 익스플로잇을 시도합니다. PT Application Firewall이 데이터 구조의 이상을 탐지할 수 있는 머신 러닝 알고리즘을 기반으로 공격을 차단합니다.



4단계 목표에 대한 조치. 시스템이 사이드 채널(트로이 공격, 내부자, 물리적 침입 등)을 통해 보안 침해를 입으면, 정보 유출(도난)을 위해 감염된 서버를 이용하거나 악성코드를 확산하는 공격이 PT AF에 의해 탐지되고 차단됩니다. PT AF의 내장형 Anti-Malware 및 Data Control 엔진은 PT AF의 유연한 통합 API를 통해 기업의 기존 외부 안티바이러스 또는 DLP 솔루션으로 보완이 가능합니다.



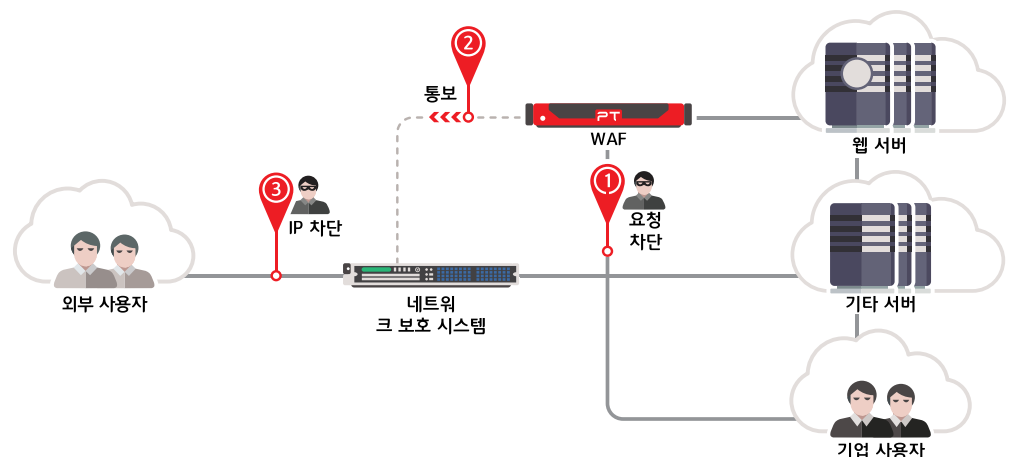
5단계 P-Code 기술을 통한 가상 패치 적용. 최신 WAF 솔루션은 사용자 정의 차단 규칙을 할당하여 패치가 까다롭거나 불가능한 취약한 코드를 보호합니다. 그러나 대부분의 WAF는 수작업에 의한 패치 적용과 애플리케이션 분석을 요구합니다. 서드 파티의 능동적 스캐너 이용 시, 소스 코드 분석이 부족하기 때문에 제한된 수의 취약점만 탐지가 가능합니다.

그러나 PT Application Firewall을 사용하는 고객은 정적, 동적, 양방향 코드 분석(SAST, DAST, IAST)의 장점들을 결합하여 가상 패치 적용을 자동화하는 P-Code 모듈을 활성화할 수 있습니다. 취약점이 탐지될 때마다 P-Code는 취약한 특정 파라미터와 그 값(익스플로잇)을 산출하고 차단 규칙을 자동 생성하여 수작업의 필요성을 줄여줍니다.

6. 다계층 보호 시나리오

PT AF는 네트워크 통신 계층 보호가 목표인 기타 Positive Technologies 및 서드 파티 시스템들(예: Check Point, Arbor)과 연동이 가능합니다. 이러한 연동의 결과가 모든 시스템의 보안 인시던트들의 완전한 동기화와 상관관계를 바탕으로 공격을 정확히 탐지할 수 있는 결합형 보호 메커니즘으로, 가장 일반적인 네트워크 및 웹 공격으로부터 포괄적으로 보호해줍니다.

PT AF는 의심되는 요청을 탐지, 차단하고, 네트워크 보호 시스템에게 의심되는 IP 주소를 즉시 통보합니다. 네트워크 보호 시스템은 전사적으로 위협의 출처를 즉시 차단합니다.



7. 구축 옵션

PT Application Firewall은 가상 장치, 하드웨어 장치, 또는 SaaS 등으로서 구축이 가능하며, 퍼블릭 클라우드(Microsoft Azure)에서 이용 가능합니다.

PT Application Firewall는 다음 중 한 가지 모드로 구축이 가능합니다.

1



In-line Mode

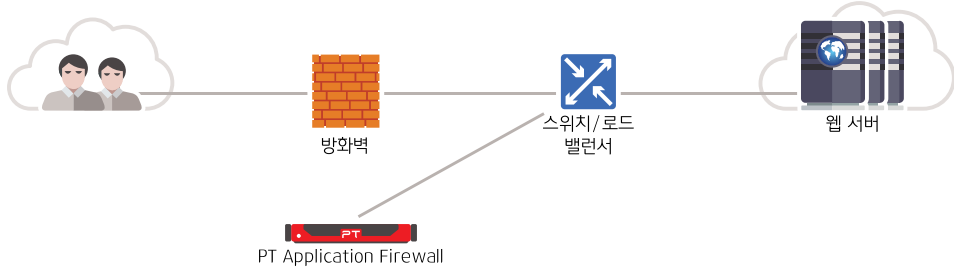
세 가지 구축 스킴이 가능합니다:

- + Reverse-Proxy
- + Transparent Proxy
- + L2 Bridge(탐지 모드에 한함)

트래픽은 공격을 능동적으로 탐지, 차단하는 PT Application Firewall을 통해 라우팅됩니다.

관리자는 PT AF 웹 인터페이스를 통해 Transparent Proxy와 L2 Bridge 사이를 쉽고 빠르게 이동할 수 있습니다.

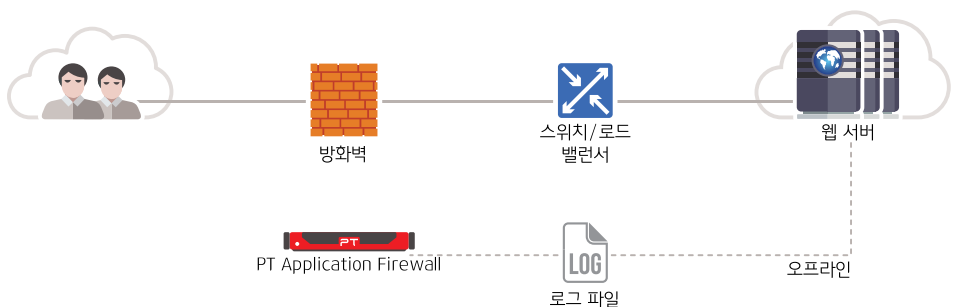
2



Mirror Mode

라우터가 PT Application Firewall로 트래픽을 미러링하면, PT Application Firewall이 잠재적 위협을 탐지하여 기존 보안 시스템에 경고합니다.

3



Off-line Mode

PT Application Firewall이 포렌식 분석을 위해 이전 공격들의 증거 로그를 검사합니다.

8. 설치 및 설정

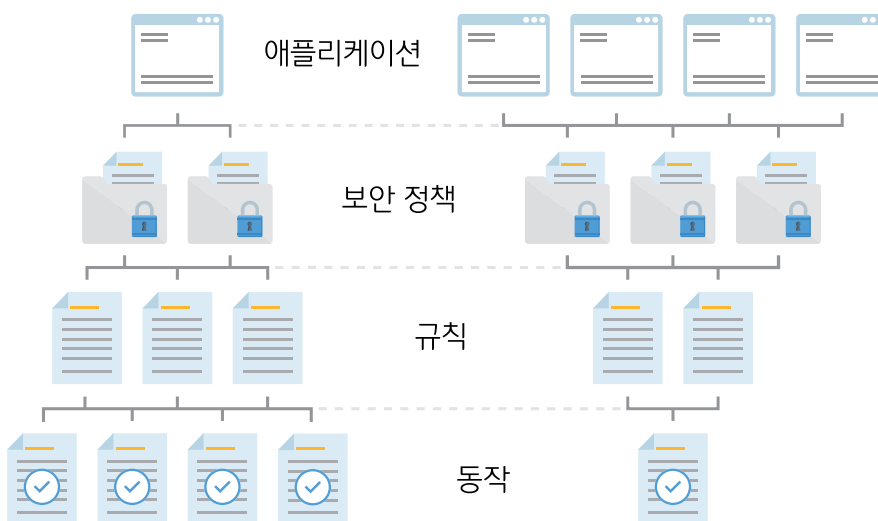
PT AF는 아래와 같은 기능을 통해 설치 시간을 획기적으로 줄였습니다.

- + **표준 WSC 마법사 및 편리한 인터페이스.** 관리자는 표준 CLI 시나리오와 PT AF의 직관적 웹 인터페이스를 사용하여 구축 환경설정을 신속하게 완료할 수 있습니다.
- + **보호 대상 리소스의 자동 탐지** Transparent Proxy, Bridge, Mirror 구축 모드 활용 시, 모든 보호 대상 리소스가 자동 탐지되므로 관리자가 기억하지 않아도 됩니다. 사전 제품 설치가 완료되면 UI에 전체 보호 대상 애플리케이션에 대한 정보가 표시됩니다. 필터링, 정렬, 추가, 제거 등 유연한 관리 옵션이 다양하게 지원됩니다.
- + **유연한 보안 정책.** PT AF는 사전 정의된 보안 템플릿을 제공합니다. 따라서, 관리자가 정의가 필요한 보안 정책을 다음과 같은 기준에 따라 신속하게 수립할 수 있습니다.
 - + **보안성 수준**(높음, 보통, 낮음)
 - + **계층**(예: 여러 애플리케이션에 적용되는 일반 정책 또는 앱별로 적용되는 개별 정책)
 - + **기능**(서로 다른 정책들이 공용 영역 요소, 개인 계정, 관리자 인터페이스 등과 같은 애플리케이션의 각각의 부분에 적용)
- + **보안 정책 내의 유연한 환경설정** PT AF에는 모든 보안 정책에 자동 적용되는 통합형 규칙 기반이 포함됩니다. 따라서, 각 보안 정책마다 별도의 규칙을 생성할 필요가 없습니다. 또한, 관리자는 보호 대상 애플리케이션의 중요도에 따라 각 규칙의 차단 또는 로깅 등과 같은 다양한 시스템 동작을 적용할 수 있습니다. 이 경우, 보안 정책에 변경사항이 적용될 필요가 없습니다. 즉, 관리자는 PT AF 보호 수준을 세부적으로 제어할 수 있고, 그러한 세부적 제어에 따른 시간과 노력은 크게 줄어듭니다. 이러한 기능은 여러 개의 애플리케이션으로 작업할 때 특히 중요합니다.

기타 기능:

- + **시스템 설정의 자동 복구**
시스템 설정에 실패하는 경우, 최근 저장된 환경설정이 자동 복구됩니다. 따라서, 수작업의 필요성이 감소하므로 PT AF 장치와 원격으로 작업하는 관리자에게 특히 유용합니다.
- + **저장되는 데이터 길이 지정 기능** 특정 파라미터가 장기적 가치가 없는 경우, 모든 데이터를 저장할 필요가 없습니다. 관리자는 길이가 긴 데이터(Request POST Data, Matched 인수 값, Request/Response 헤더 등)의 어느 부분이 저장되어야 하는지를 지정할 수 있습니다. 따라서, 데이터베이스 과부하의 위험성이 감소하고, 저장된 데이터 세트의 크기가 줄어들므로 검색 속도가 향상됩니다.

PT AF 설정 유연성



PT AF는 다양한 보안 계층의 요구사항을 만족시키기 위해 아래와 같은 세부적인 제어기능을 제공합니다.

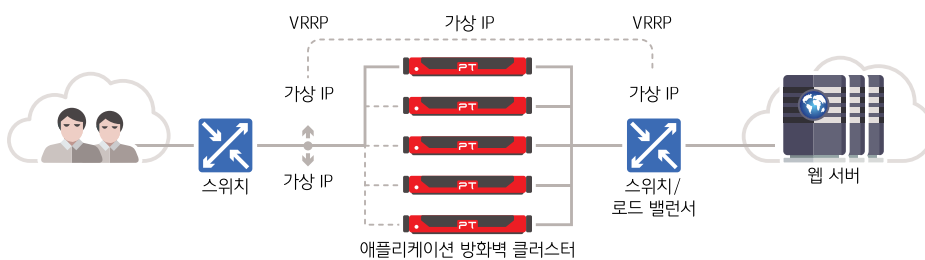
- + 각각의 애플리케이션 혹은 애플리케이션 그룹은 한 개 혹은 여러 개의 보안 정책으로 보호할 수 있습니다.
- + 각각의 보안 정책 혹은 보안 정책 그룹은 한 개 혹은 여러 개의 보안 규칙으로 보호할 수 있습니다.
- + 각각의 보안 규칙 혹은 보안 규칙 그룹에 한 개 이상의 탐지 시 대응 규칙을 지정할 수 있습니다.

한번 설정된 환경설정은 향후 재사용을 위해 템플릿 형태로 저장 가능하므로 반복적으로 설정 작업을 실행할 필요가 없습니다.

9. 고성능 및 고가용성

PT AF는 고가용성을 고려하여 설계되었습니다. PT AF는 active - active 또는 active - passive 모드에서 구축이 가능합니다. 기업은 PT AF에 내장된 커널 로드 밸런싱과 외부 로드 밸런서를 이용하여 효과를 볼 수 있습니다.

1



Active-Active 고가용성:

내장형 로드 밸런싱, 캐싱 및 Active Active 클러스터가 고성능의 안정적인 애플리케이션을 생성합니다.

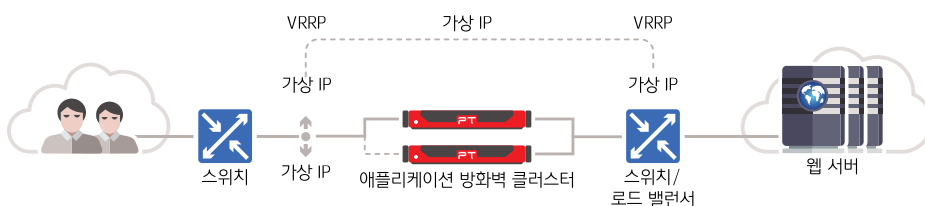
2



Active-Active 고가용성:

Active Active 클러스터는 외부 로드 밸런서와 연동이 가능합니다.

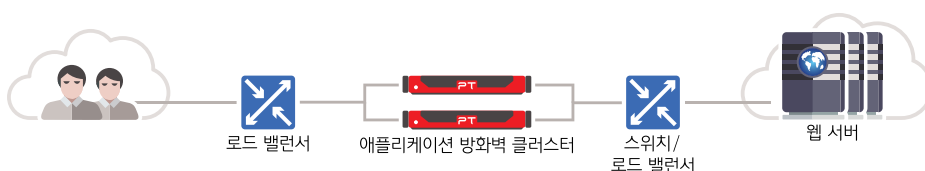
3



Active-Passive 고가용성:

Active Passive 클러스터가 내장형 로드 밸런싱을 통해 두노드 (two-node) 동작을 지원합니다.

4



Active-Passive 고가용성:

Active Passive 클러스터는 외부 로드 밸런서와 연동이 가능합니다.

포지티브 테크놀로지스

포지티브 테크놀로지스는 취약점 및 컴플라이언스 관리, 보안 사고 및 위협 분석, 애플리케이션 보호 솔루션 등 토털 기업 보안 솔루션을 제공하는 업계 선도 기업입니다. 고객과 연구에 대한 헌신적 노력을 통해 세계적 분석 기관들로부터 ICS(산업제어시스템), banking, 통신, 웹 애플리케이션, ERP 보안 분야의 선두주자라는 명성을 얻고 있습니다. 포지티브 테크놀로지스에 대한 더 자세한 정보는 ptsecurity.com에서 확인할 수 있습니다.

© 2017 Positive Technologies. Positive Technologies 및 포지티브 테크놀로지스 로고는 포지티브 테크놀로지스의 상표 또는 등록상표입니다. 본 문서에 언급된 일체의 기타 상표는 해당 소유권자의 재산입니다.