주요 효과:

지속적인 능동적 보호

- **제로데이 공격 자동 차단** 첨단 머신 러닝을 통해 PT AF가 제로데이를 비롯하여 알려진 공격과 알려지지 않은 공격을 능동적이고 정확하게 탐지합니다. 아울러, 고도의 자동화 기능을 제공합니다.
- **주요 위협의 신속한 식별** 지능적인 상관관계 분석기술이 오탐률을 크게 낮춰주므로 가장 중요한 인시던트에 집중할 수 있습니다. 상세 공격 체인 지표를 기반으로 더욱 효율적인 포렌식 조사가 이뤄집니다.
- **즉각적인 대상 보안.** PT AF 고유의 빌트인 소스 코드 분석 모듈(P-Code)이 취약점을 탐지하고, 즉각적인 '가상 패치'를 생성합니다. 이를 통해 코드에 존재하는 특정 오류의 익스플로잇 시도를 차단할 수 있습니다. 또한, PT AF는 애플리케이션 보안 테스트(AST) 툴인 PT Application InspectorTM(SSDL 에디션 포함)와 연동하여 개발 프로세스 보안을 강화합니다.
- **첨단 L7 DDoS 차단.** 세 가지 애플리케이션 스트레스 지표(RPS, 응답 시간, 오류율)를 기반으로, PT AF의 지속적 행동 프로파일링 기능이 L7 DDoS 공격을 탐지할 뿐만 아니라 예측합니다. 조기 경고 기능을 통해 보안팀이 비즈니스 중단을 능동적으로 예방할 수 있습니다.
- **PCI DSS 준수에 필수적인 도움 제공** 기타 국제, 국내, 기업 표준 준수 지원

쉽고 빠른 시작

- **클릭 몇 번만으로 구축 및 설정 완료.** PT AF는 신속하게 몇 가지 모드로 구축이 가능합니다(L2 Bridge, Transparent 프록시 등). 아울러, 표준 WSC 마법사, 사전 정의된 보안 템플릿, 보호 대상 앱의 자동 탐지, 직관적 인터페이스를 통해 이용 가능한 기타 자동 기능들 등으로 구축 시간이 단축됐습니다.
- **기존 시스템과의 사전** PT AF는 안티바이러스, DLP, 안티 DDoS, SIEM, IPS 등 다양한 시장 주요 솔루션과 PT Application Inspector™, PT MultiScanner™, PT SIEM™ 등 Positive Technologies의 첨단 솔루션에 플러그 앤 플레이를 지원합니다. 서드 파티 연동 대상에는 CheckPoint Security Gateway, Arbor Peakflow, Qrator, Array Networks, HP ArcSight, IBM QRadar, Zecurion Zgate와 요청에 따른 기타 장비가 포함됩니다.
- **기존 인프라에 자동 연동** Cisco ACI 지원이 가능한 PT AF™는 어떤 규모의 네트워크에도 신속하게 추가될 수 있습니다.

PT APPLICATION FIREWALL™:
비즈니스 애플리케이션의 능동적 보호

시장 문제점 및 도전과제

금융, 공업, 통신, IT , 언론, 정부 등 모든 기관에서 인터넷의 비즈니스 침투는 그 어느 때보다도 심화되고 있습니다. 많은 시간이 소요됐던 과거의 작업들이 웹사이트, 온라인 쇼핑, 문서 관리 시스템, 재고, 인터넷 뱅킹, 워크플로우를 간소화하는 기타 애플리케이션들을 통해 자동화되었습니다. 그러나, 이러한 기술들은 동시에 사이버 범죄의 새로운 기회가 되고 있습니다.

2016년, Positive Technologies가 실시한 연구조사 결과, 테스트 대상 애플리케이션 전체에서 최소 심각도 '보통'의 취약점이 발견됐습니다. 테스트 대상 애플리케이션들 가운데 70%는 심각도가 더 높은 취약점을 한 개 이상 포함하고 있었고, 그같은 심각도의 웹 애플리케이션 비율은 최근 3년간 지속적으로 상승했습니다.

웹 애플리케이션에서 발견되는 대부분의 취약점은 개발자 실수에서 비롯됩니다. 기존 스캐너, IDS/IPS, 방화벽 등으로는 그러한 취약점을 항상 탐지할 수 없습니다. 그 이유는 다음과 같습니다.

- 공격자는 주로 제로 데이 취약점을 익스플로잇하므로 기존 시그니쳐 기반 분석 방식은 으로는 효과를 거둘 수 없습니다.
- 표준 IDS와 IPS가 의심되는 이벤트에 대하여 생성하는 수천 개의 경고는 실제 위협 식별을 위해 수작업으로 처리되어야 합니다.
- 여러 기업 사이트와 온라인 서비스는 서드 파티 모듈을 비롯하여 맞춤화된 솔루션을 이용하는데 여기에는 고유의 취약점들이 존재합니다. 이러한 애플리케이션을 보호하려면 애플리케이션 구조, 사용자 상호작용 모델, 이용 맥락 등을 철저히 분석할 수 있는 첨단 기술이 필요합니다.
- 잘 알려진 취약점마저도 즉각적인 수정이 불가능합니다. 코드 패치 시 시간과 비용이 소요되고, 중요한 비즈니스 프로세스를 중단시키는 경우도 발생합니다. 해커는 이러한 취약점을 이용할 수 있습니다.
- 중요한 애플리케이션을 보호하고, 일반 동작에서 실제 공격을 구별하려면, 애플리케이션의 비즈니스 로직도 고려되어야 합니다.

PT Application Firewall을 소개합니다

Positive Technologies Application Firewall™(PT AF™)은 웹 포털, ERP 시스템, 모바일 앱 등의 변화하는 보안 과제에 대한 최신의 대응 방안입니다. 강력한 기술과 혁신적 방식을 기반으로 PT AF는 OWASP Top 10 클라이언트 사이드 공격 및 스크레이핑 등과 같은 자동화 공격 등을 비롯한 알려져 있는 공격과 알려져 있지 않은 공격 또는 신규 공격(제로데이) 등으로부터 애플리케이션을 지속적, 능동적으로 보호합니다.

PT AF는 지속적인 애플리케이션 보안 연구결과를 토대로 지속적으로 업데이트되므로 최고의 보안성, 유용성, 상호운용성 등을 유지할 수 있습니다.

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

자세한 내용은 당사 웹 사이트 ptsecurity.com을 방문하십시오.

PT APPLICATION FIREWALL™:
비즈니스 애플리케이션의 능동적 보호

기타 기능

+ **다계층 보호 지원** PT AF는 네트워크 계층 보안 시스템(Check Point, Arbor)과의 심층적 연동을 통해 네트워크 및 웹 공격에 대하여 기업의 전체 인프라를 종합적으로 보호합니다.

+ **관리 효율성 증대** PT AF의 자동화 기능이 설치 및 정기적 관리에 따른 시간과 비용을 절약합니다. 클릭 한 번으로 구축 모드를 변경하고, 저장과 재사용이 가능한 보안 정책을 상세히 관리하는 등 효율성이 증가합니다.

+ **비즈니스 로직 활용을 통한 공격 식별.** PT AF는 XML, JSON 등 공통 애플리케이션 데이터 프로토콜을 분석합니다. 그런 다음, 애플리케이션의 비즈니스 로직을 바탕으로 데이터에 대한 해석 및 새너티 체크(sanity-checks)를 실시하여 공격을 일반 동작과 구별합니다.

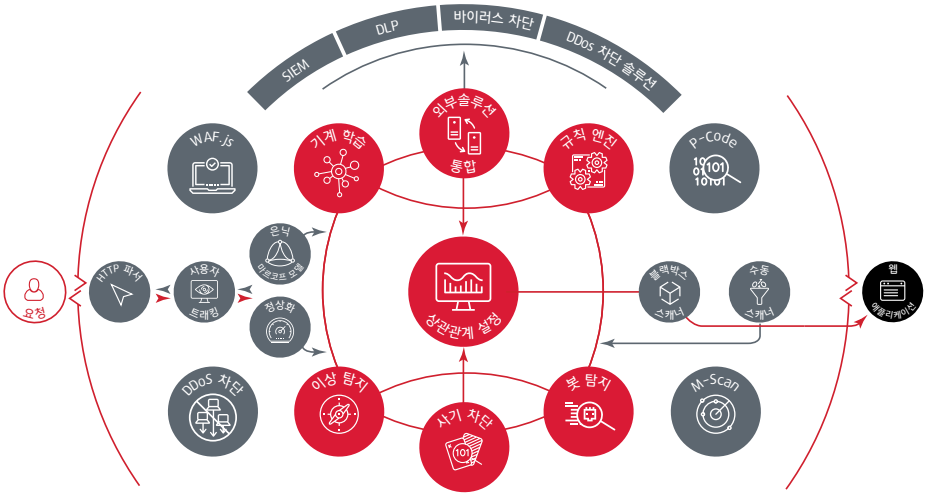
+ **최종 사용자 데이터의 기밀성 극대화.** PT AF는 서드 파티 및 PT AF 관리자 등의 결제카드 번호, 여권 정보, 보험 정보 등 개인 정보를 식별하고 숨길 수 있습니다(마스킹).

+ **위치에 상관없는 가용성.** PT AF 는 기업의 IT 정책에 따라 하드웨어 장비 또는 가상 장비에 구축이 가능합니다.. 100% 클라우드 이용 가능하며(SaaS, VAS, MSS) 애플리케이션 호스팅 보안을 위한 훌륭한 선택입니다. PT AF는 퍼블릭 클라우드(Microsoft Azure)에서도 사용 가능합니다.

작동 방식 모듈 및 메커니즘

PT Application Firewall은 다양한 전문 모듈 및 메커니즘을 통해 종합적인 360º 보안을 제공합니다.

+ **Hidden Markov Model(HMM):** 자체 학습 모듈로서 제로데이 공격을 차단하고, 첨단 자동화를 보장합니다.
+ **WAF.js:** 클라이언트 사이드 공격(XSS, DOM, XSS, CSRF, Clickjacking)으로부터 JavaScript 모듈을 감시합니다. 보호 대상 페이지가 열릴 때마다 사용자 브라우저에서 실행됩니다.
+ **P-Code module:** 애플리케이션 소스 코드에 존재하는 취약점을 식별하고, 해당 취약점을 바탕으로 공격을 차단하는 규칙(가상 패치)을 자동 생성합니다.
+ **Bot Mitigation:** 시그니쳐 기반분석과 휴리스틱 분석 간 결합을 기반으로 첨단 봇 탐지 기능을 제공합니다. 악의적이지 않은 봇의 활동에 영향을 미치지 않고 봇 공격을 차단합니다.
+ **M-Scan module:** 안티 바이러스 엔진을 이용하여 사용자가 업로드하고 다운로드한 파일을 자동 스캔합니다.
+ **Passive Scanner:** 애플리케이션 구성요소(CMS, 프레임워크, 라이브러리)를 수동적으로 식별하여 정상화 모듈을 설정하고, 데이터 유출 및 알려진 CVE 취약점을 탐지합니다.
+ **BlackBox Scanner:** 능동적 애플리케이션 보안 테스트(DAST)를 실행하고, 애플리케이션 구성요소를 식별하며, 자체 학습 엔진을 지원하고, 애플리케이션 취약점을 탐지합니다.
+ **Rule Engine:** 알려진 모든 CVE 취약점들을 비롯하여 취약점에 대한 사용자 정의 규칙이 생성됩니다.
+ **SOA Firewall:** XML 분석 모듈이 배포된 웹 서비스에 대한 공격을 차단합니다. 정상화 메커니즘이 서버 컨텍스트를 고려하여 HTTP 요청 데이터와 헤더를 살균합니다. 이를 통해 대부분의 방화벽 우회 방법(HPC, HPP, Verb Tampering 등)을 차단할 수 있습니다.



지금 바로 PT APPLICATION FIREWALL™를 무료 체험해 보십시오.

조직 내 PT Application Firewall 무료 체험을 원하신다면 af.ptsecurity.com으로 문의해 주십시오.

포지티브 테크놀로지스

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

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com