A Broadcom Company
technologies

Product Brief

PAM
Privileged Access Manager

제품 특장점

- **접근 경로 단일화**
- **특권 계정 접근 관리**
- **RDP(Remote Desktop Protocol) 애플리케이션**
- **패스워드 관리 정책**
- **특권 계정 세션 레코딩 명령어 통제/경유 접속 차단**
- **AWS 특화 기능**
- **위협 분석**

차별화 요소

- **보안 위험 감소 –** 보안 위협에 대한 탐지 및 사용자 행위에 대한 다양한 뷰를 제공
- **명확한 가시성 –** 보안 위험 관리, 사고 대응, 컴플라이언스 대응을 손쉽게 함. 사용자, 이벤트, 시스템 활동 내역에 대한 상세 정보 제공
- **빠른 투자 회수 –** 솔루션 설치 즉시 직관적인 위험도 가시성을 제공함
- **빠른 설치 –** 가상 어플라이언스 형태로 쉽게 설치, 구성

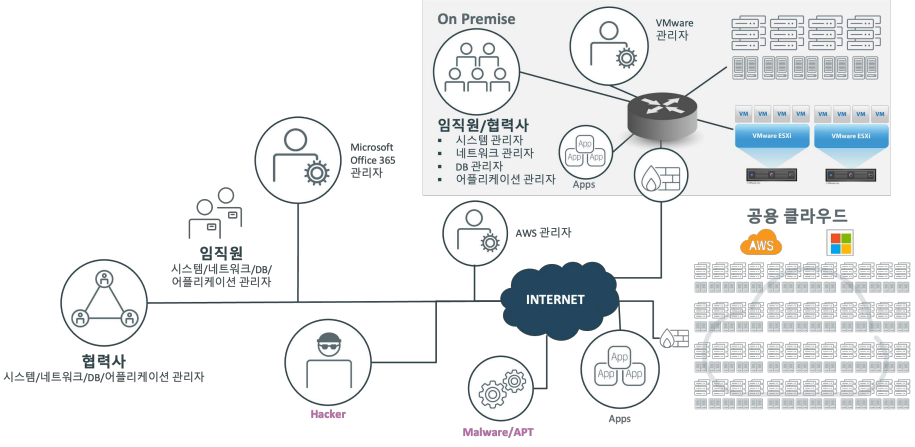
소개

Broadcom의 PAM(Privileged Access Manager)은 특권 계정의 접근을 제어하는 솔루션입니다. PAM은 전통적인 SecureOS 기반 서버 보안 기술에 최근 하이브리드 클라우드로 빠르게 변화 중인 엔터프라이즈 컴퓨팅 환경의 변화에 발맞춰 온프레미스를 넘어 IaaS, PaaS, SaaS에 대한 접근 제어 기능까지 제공합니다.

하이브리드 환경을 위한 특권 계정 관리

온프레미스 환경은 서버 접근 제어를 통해 특권 계정을 관리하는 것이 일반화되어 있습니다. 반면에 클라우드 환경에서 운영하는 게스트 운영체제, 가상 머신 인스턴스, 컨테이너 환경 등에 대한 특권 계정 접근 제어는 온프레미스와 비교해 허술한 측면이 많습니다. 이런 이유로 주요 클라우드 보안 사고를 보면 특권 계정 탈취나 오남용으로 인한 것이 많습니다.

PAM을 적용하면 온프레미스 환경과 클라우드 환경을 포괄하는 특권 계정 접근 제어를 할 수 있습니다. 이를 통해 내부 인력뿐 아니라 협력사들, 프로젝트 인력들, 개발사 관계자 모두에 대한 특권 계정 관리를 효과적으로 수행할 수 있습니다.



다양한 특권 계정 관리

PAM으로 관리할 수 있는 특권 계정은 데이터베이스 관리자, 시스템 관리자, 네트워크 엔지니어, 보안 운영자, IT 감사, 데이터센터 운영자, 애플리케이션 개발자, 클라우드 관리자 등 다양합니다.

하이브리드 환경 지원

PAM을 활용하면 모노리식 아키텍처로 구축한 전통적인 엔터프라이즈 데이터센터부터 가상 머신 및 컨테이너로 구성한 소프트웨어 정이 기반 데이터센터, 퍼블릭 클라우드와 SaaS까지 특권 계정의 접근을 제어할 수 있습니다. 이처럼 다양한 환경을 수용하기 위해 PAM은 하드웨어 어플라이언스 형태 외에도 가상 머신 환경에 배포할 수 있는 옵션을 제공합니다.

PAM의 주요 기능

접근 경로 단일화

- 다양한 배포 아키텍쳐(온프레미스, AWS)
- 다양한 대상 시스템, 애플리케이션에 대한 통합된 특권 계정 접근 관리

특권 계정 접근 관리

- 암호화 통신을 지원하지 않는 경우 공격자가 통신 패킷을 분석하여 시스템 접속에 대한 주요 정보를 탈취할 가능성이 있음
- 가상화 방식을 이용하여 사용자가 PAM에 접속하는 세션과 실제로 시스템에 접속하는 세션을 분리
- 접속자(클라이언트)에는 어떠한 에이전트 및 접속 기록이 남지 않음

RDP 애플리케이션

- Windows 환경일 경우 서버의 특정 애플리케이션을 사전에 서비스로 등록하여 해당 애플리케이션만 나타나게 함
- 접속자 권한을 해당 애플리케이션으로 제한하여 보안 강화

패스워드 관리 정책

- 지정된 규칙(복잡도) 및 주기에 따라 자동으로 시스템 패스워드 변경
- 시스템 패스워드 변경 규칙은 시스템의 종류에 따라 여러 가지 생성
- 생성된 규칙을 관리자는 각각의 시스템에 서로 다르게 적용

특권 계정 세션 레코딩

- 시스템에서 수행한 모든 내역을 동영상으로 기록하며, 위반이 발생 시 문제 발생 시점 표시하고 해당 시점으로 바로 이동할 수 있어 전체 내용을 다시 볼 필요가 없는 효율적인 검색
- Idle 타입 관리와 프로토콜 레이어 기반 녹화로 효율적인 녹화 파일 크기 제공

명령어 통제/경유 접속 차단

- Command Filter : 모든 CLI 세션에 대한 위험 명령어 정책을 디바이스별/그룹별로 설정하여 허용되지 않는 명령어 실시간 차단
- Socket Filter : 정책에 의해 허용된 리소스 이외에 임의 접속 시도 원천 차단

AWS 특화 기능

- AMI 패스워드/SSH Public Key 관리
- AMI, AWS 콘솔 활동 내역 기록
- Dynamic AWS EC2 인스턴스 통제 및 보호
- 4 AWS Access Key 관리 및 ID Federation
- AWS 환경의 통합 접근 통제

위협 분석

- 자동화된 위협 탐지, 교정 및 경고: 기존 PAM, SIEM, SOC 를 보완하는 위협 분석 기능은 특권 계정 보안 위협에 대한 지능적인 모니터링을 제공
- 능동적 사용자 행위 분석: 주로 금융 온라인 트랜젝션에서 사용하던 위협 탐지 매커니즘을 사용하여, 과거 행위 패턴에 근간한 실시간 위험 분석 기능을 제공함
- 위험도에 따른 자동 정책 적용: 세션 레코딩, 부가 인증 정책을 동적으로 적용함으로 특권 계정 위협에 대한 보호 정책 시행

BROADCOM

For more information, please visit
https://www.broadcom.com/products/cyber-security/identity/pam