BeyondTrust

최적의(JIT) 특권 액세스 관리(PAM) 가이드

정의, 필요한 이유 및
구현 방법

목차

소개

새로운 차원의 “적절한 수준” 액세스

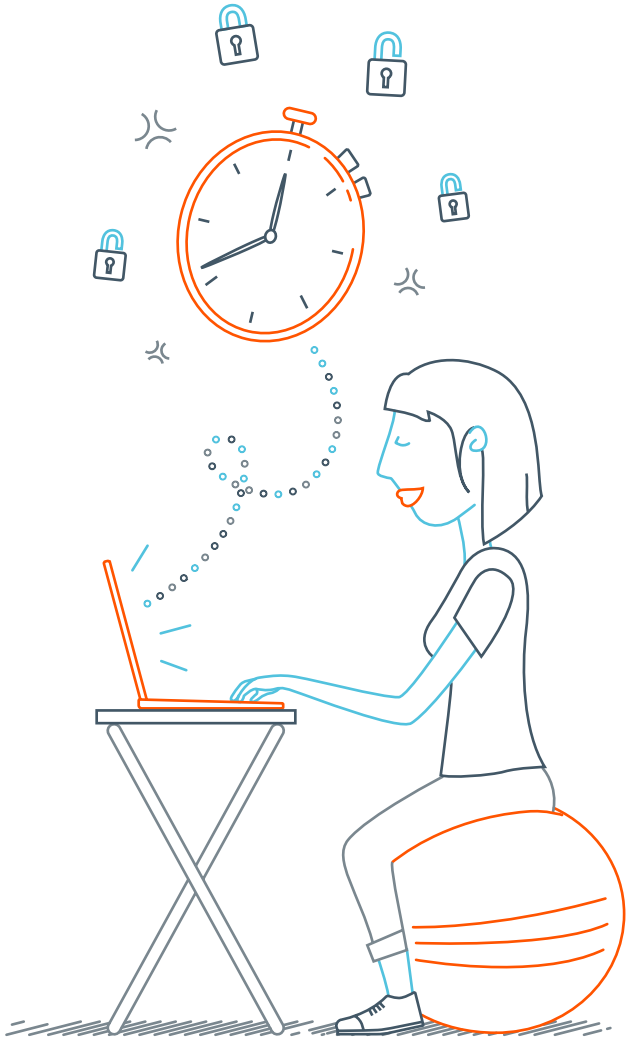
진정한 최소 권한 보안 모델에서는 사용자, 프로세스, 애플리케이션 및 시스템이 작업을 수행하기 위해 필요한 동안에만 “적절한 수준”의 권한 및 액세스를 가져야 합니다.

점점 더 많은 조직들이 특권 액세스 관리(PAM) 솔루션을 사용하는 “적절한 수준”의 액세스 기능을 효과적으로 적용하고 있지만, 대체로 특권 사용자 계정의 시간 제한적인 부분과 지속적인 위험 측면은 간과해 왔습니다.

지난 40년간, “상시” 특권 계정은 관리자 액세스의 기본 모드로 적용되었으며 엔터프라이즈 전반에 확산되어 방대한 위험 경로를 초래했습니다. 상시 활성화 모드에 있는 특권 액세스, 권한 및 사용 권한은 적법한 활동은 물론 불법적인 활동에 대해서도 언제든지 실행할 수 있도록 준비되어 있습니다. 그리고 이러한 위험 경로는 가상, 클라우드 및 DevOps 환경, 사물 인터넷(IoT) 디바이스는 물론 로보틱 프로세스 자동화(RPA)와 같은 새로운 분야가 확대되면서 급격히 확장되었습니다.

이러한 배경을 고려하면, 권한의 남용 및/또는 오용이 오늘날 거의 모든 사이버 보안 침해 인시던트에서 한몫을 한다는 점이 놀라운 일은 아닙니다. 공격자가 특권 액세스를 손에 넣으면 결국 악의적인 내부자가 되며, 이는 IT 전문가는 물론 최고 경영진 및 이사회에서까지 걱정하는 시나리오입니다.

특권 계정은 이제 조직 전반의 어디든 액세스할 수 있지만, 전통적으로 경계 기반 보안 기술은 해당 조직의 경계 내에 있는 특권 계정만 보호할 수 있습니다. 최적의(JIT) 특권 액세스 관리(PAM)는 특권 위협 경로를 대폭 축소하고 엔터프라이즈 전반의 위험을 줄일 수 있습니다. JIT PAM을 구현하면 필요한 경우에 한해 최소한의 시간 동안만 적절한 권한이 ID에 부여됩니다. 이 프로세스는 완전히 자동화되어 원활하게 처리되며 최종 사용자에게 영향을 미치지 않습니다.



점점 더 많은 조직들이 특권 접근 관리(PAM) 솔루션을 사용하는 “적절한 수준”의 액세스 기능을 효과적으로 적용하고 있지만, 대체로 특권 사용자 계정의 시간 제한적인 부분과 지속적인 위험 측면은 간과해 왔습니다.

JIT PAM 개요

최적의 특권 액세스 관리의 정의

최적의(JIT) 특권 액세스 관리(PAM)는 특권 계정을 사용하기 위한 실시간 요청을 확인, 워크플로우 및 적절한 액세스 정책에 바로 연결하는 전략입니다. 기업은 이 전략을 사용하면 행동 및 컨텍스트 매개 변수를 근거로 시간 기반 제한을 적용하여 지속적인 상시 액세스의 결함으로부터 특권 계정을 보호할 수 있습니다.

특권 계정은 표준 사용자 권한 이상의 특권 및 권한이 부여된 계정으로 정의되며, 여기에는 다음 권한이 포함됩니다.

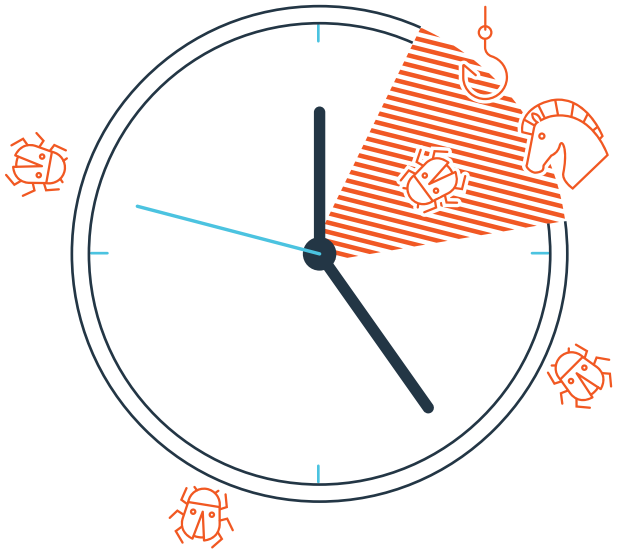
- 관리자(Windows 환경) 또는 루트(Unix/Linux 환경)와 같은 광범위한 특권을 가진 슈퍼 사용자
- 슈퍼 사용자 및 표준 사용자 계정 사이의 특권을 가진 고급 사용자(비특권 또는 최소 권한 사용자 계정이라고도 불림)

JIT PAM은 계정이 향상된 계정 권한 및 접근 권한을 보유하는 기간을 엄격히 제한하여, 위협 요소가 계정 특권을 남용할 수 있는 취약성 시간을 급격히 줄여줍니다. JIT는 최소 권한 원칙을 실행하여 특권 작업이 허용 가능한 사용 정책에 맞게 수행되도록 하는 동시에 적절한 컨텍스트에 포함되지 않는 특권 활동을 금지합니다.

권한을 요청하면 확인되기 전에 필수 컨텍스트 매개 변수를 충족해야 하며, 계정에서 권한을 소유할 수 없습니다. 이를 통해 특권 접근 관리 배포 환경 외부에서 잠재적으로 활용될 경우 오용 위험을 완화할 수 있습니다. 따라서 특권 계정이 더 이상 본질적으로 남용의 대상이 되지 않습니다.

예를 들어, 일주일에 168시간 동안 "권한 활성화 상태"인 전형적인 상시 특권 계정을 생각해 보십시오. JIT PAM 접근 방식으로 전환하면 권한 활성화 상태를 168시간에서 불과 몇십 분 수준으로 축소시킬 수 있습니다. 이 효과를 조직의 모든 특권 사용자 계정 전반으로 증대시키면 진정으로 강력한 위험 감소 효과를 얻게 됩니다.

JIT를 권한 관리 방식의 일환으로 채택하면 진정한 최소 권한 모델을 전사적으로 구현할 수 있습니다. 그리고 노출은 단순히 시간에만 기반을 두지 않습니다. 리소스 전반에서 활용할 "상시" 특권 계정이 없기 때문에 측면 이동과 같은 기술을 활용하는 공격 벡터 또한 완화됩니다.



기업은 이 전략을 사용하면 행동 및 컨텍스트 매개 변수를 근거로 시간 기반 제한을 적용하여 지속적인 상시 접근의 결함으로부터 특권 계정을 보호할 수 있습니다.

JIT PAM 자동화

JIT 방법

권한 관리에 대한 JIT 접근 방법을 위해서는 조직이 최적의 특권 액세스에 대한 기준을 수립하고 이 정책에 포함되는 계정이 잠재적으로 브레이크 글래스 시나리오 외부에서 사용되지 않는다는 점을 수락해야 합니다.

JIT에 대해 확립된 유사 개념이 제조와 같은 기타 활용 사례 전반에 존재하긴 하지만, 이 모델을 보안 및 운영 솔루션에 대해 적용하면 구현 과정에서 일부 고유한 기술 고려 사항이 제기됩니다.

JIT 특권 계정의 목표는 승인된 작업 또는 임무에 기반하여 필요한 권한을 "즉시" 자동으로 할당한 다음 작업이 완료되거나 승인된 액세스에 대한 시간 또는 컨텍스트가 만료되면 이를 제거하는 것입니다.

표준 사용자 계정에 적절한 권한을 적용하기 위해 필요한 모델링은 다음과 같은 6가지 JIT 방법 중 하나를 사용하여 구현할 수 있습니다.

1 JIT 권한

임무를 수행하기 위해 모든 기준을 충족하는 경우 제한된 기간 동안만 계정에 개별 특권, 사용 권한 또는 권한 유형을 추가하는 방법입니다. 이러한 권한은 임무를 완료하고 나면 철회되어야 하며 다른 권한이 부적절하게 변경되지 않았다는 인증을 포함해야 합니다.

2 JIT 계정 생성 및 삭제

임무 목표를 달성하기 위해 적절한 특권 계정을 생성 및 삭제하는 방법입니다. 이 계정은 요청 ID 또는 로깅 및 포렌식 운영을 수행하는 서비스로 다시 연결되는 특성을 가져야 합니다.

3 JIT 위장

이 계정은 기존에 존재하는 관리자 계정에 연결되며, 특정 애플리케이션 또는 작업을 수행할 때 이러한 크리덴셜을 사용하여 기능이 상승됩니다. 이는 일반적으로 자동화를 사용하거나 Windows "RunAs" 또는 *Nix SuDo를 활용한 스크립팅을 사용하여 수행됩니다. 일반적으로, 최종 사용자는 이 작업 유형에 대한 위장 계정을 인식하지 못하며, 프로세스는 상시 특권 계정 위임과 겹칠 수 있습니다.

4 JIT 토큰화

애플리케이션 또는 리소스의 특권 토큰을 수정하여 운영 체제 커널에 주입하는 방법입니다. 이 최소 권한 양식은 일반적으로 엔드포인트에서 최종 사용자의 권한 상승 없이 애플리케이션 우선 순위 및 권한을 높일 때 사용됩니다.

5 JIT 그룹 멤버십

임무 기간 동안 특권 관리자 그룹에 계정을 자동 추가 및 제거하는 방법입니다. 이 계정은 해당하는 기준을 충족하는 경우에만 상승된 그룹에 추가해야 합니다. 그룹 멤버십은 임무 완료 시 즉시 철회되어야 합니다.

6 JIT 비활성화 관리 계정

비활성화된 관리자 계정은 모든 사용 권한, 특권 및 권한 유형과 함께 시스템 내에 존재하며 기능을 수행합니다. 이 계정은 특정 임무를 수행하기 위해 활성화되며 운영 기준이 충족되고 나면 다시 비활성화됩니다. 이 개념은 상시 관리자 계정을 가지는 것과 다르지 않지만, 기본 구현 기능을 활용하여 JIT 액세스를 제어한다는 점이 예외입니다.

JIT 트리거

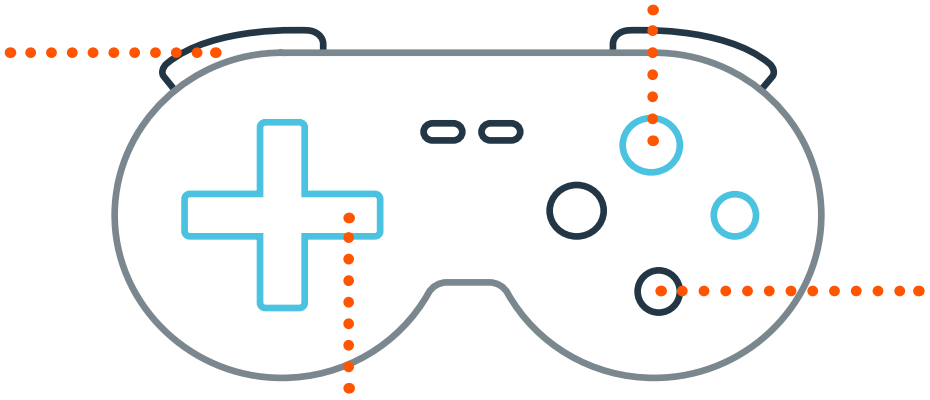
이러한 특권 계정 상승 방법을 최적의 특권 액세스 관리 원칙에 따라 적용하려면, 다음 기준을 트리거로 *고려해야 합니다*. 또한 이러한 변경 제어 기간에 대한 시간과 날짜 같은 변수는 물론, 보안 침해 표시기가 감지되는 경우 일시 중단 또는 종료 기준을 포함해야 합니다.

2단계(2FA) 또는 다단계 인증(MFA)

상시 또는 JIT 특권 계정에 특권 접근 권한을 부여하는 일반적인 방법은 2FA 또는 MFA입니다. 이 방법은 두 가지의 접근 기술을 구별하지 않지만, 특권 계정에 대한 적절한 접근을 가진 ID를 검증하여 추가 위험 완화 기능을 제공합니다. 그러나 이러한 인증 방법은 위에 나열된 기술 중 하나를 사용하는 계정에 대한 JIT 트리거로 사용할 수 있습니다.

워크플로우

워크플로우 승인 개념은 일반적으로 콜 센터, 헬프 데스크 및 다른 IT 서비스 관리(ITSM) 솔루션과 연관됩니다. 접근을 위한 요청을 제출하면, 승인자의 정의된 워크플로우를 사용하여 접근이 부여되거나 거부됩니다. 일단 워크플로우가 승인되면, JIT 계정을 활성화할 수 있습니다. 이는 일반적으로 사용자, 자산, 애플리케이션, 시간/날짜, 그리고 변경 제어 또는 헬프 데스크 솔루션 내의 관련 티켓에 해당합니다. 이 시나리오에서는 일반적으로 특권 세션 모니터링이 PAM 솔루션에 의해 활성화되어 해당하는 모든 동작이 적절한지를 확인합니다.



컨텍스트 인식

컨텍스트 인식 접근은 소스 IT 주소, 지리적 위치, 그룹 멤버십, 호스트 운영 체제, 메모리 내에서 설치되거나 운영되는 애플리케이션, 문서화된 취약성 등의 기준에 기반합니다. 이러한 특성 중 임의의 논리적 조합을 기반으로 JIT 계정 접근을 부여하거나 철회하여 비즈니스 요구 사항을 충족하고 위험을 완화할 수 있습니다.

권한 유형

특권 접근 관리가 ID 및 접근 관리(IAM) 솔루션과 통합될 때 솔루션 간 권한 유형을 특권 접근에 대해 동기화할 수 있습니다. 이를 위해 JIT 접근은 PAM 솔루션을 통해, 또는 프로그래밍 방식으로 IAM 권한 유형을 통해 직접 할당할 수 있습니다. 전형적인 IAM 권한 유형 워크플로우는 더 이상 동기화 프로세스가 아니며 실시간으로 수행되지 않을 수 있지만, 권한 기반의 계정 인증을 위한 수단을 제공합니다. 이는 IAM을 PAM 솔루션에 연결하여 접근을 제어할 때 무효화될 수 있습니다.

JIT 자동화 트리거는 계정에 특권 접근 상태를 부여하기 위한 조건입니다.

JIT PAM 자동화

JIT 정책

팀을 위해 고려해야 할 두 가지 핵심 질문은 *"적절한 특권 액세스에 대한 JIT 계정을 관리하는 정책은 무엇인가?"*, 그리고 *"이를 철회하기 위해 충족해야 하는 조건은 무엇인가?"*입니다.

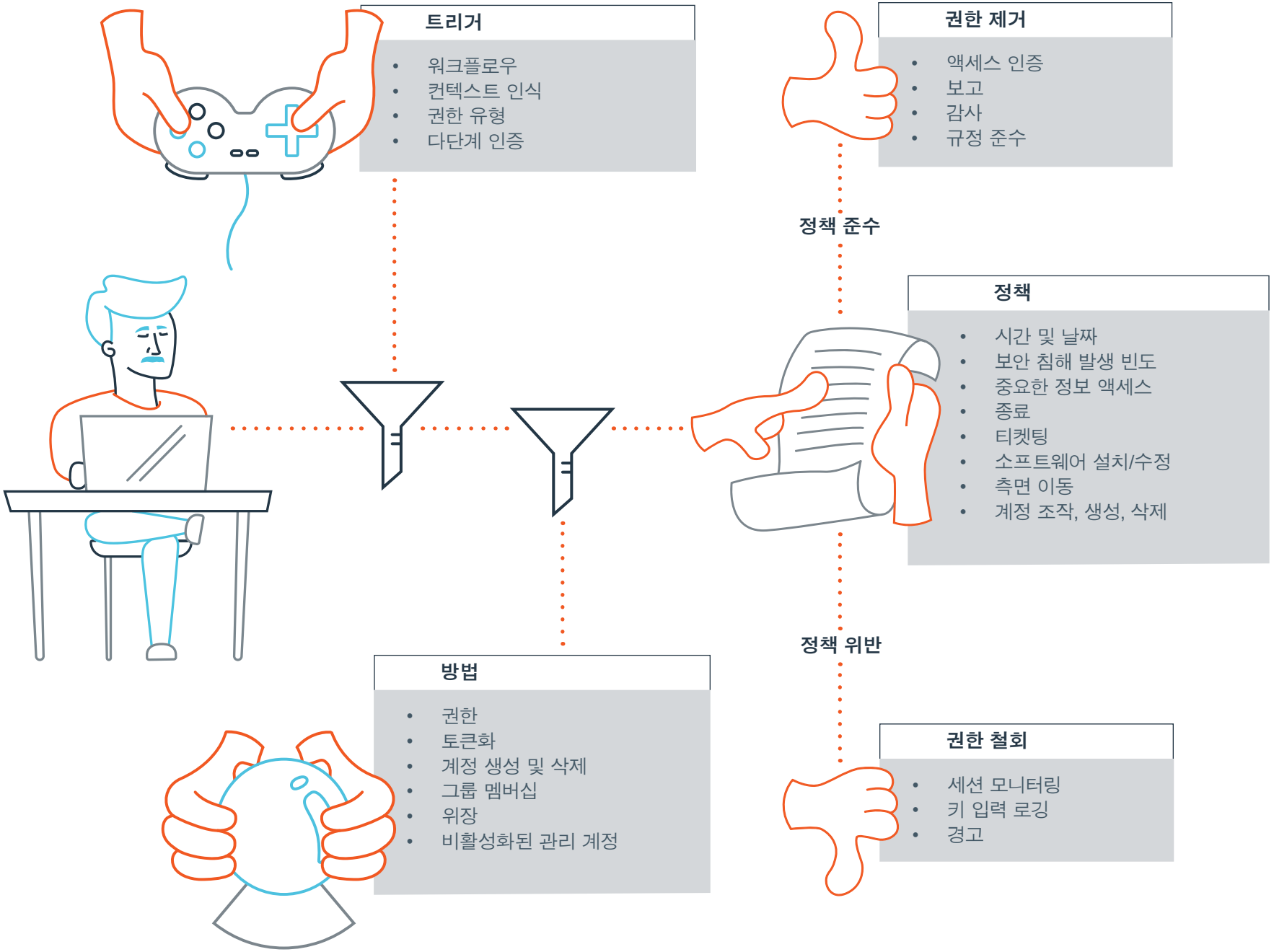
이러한 정책은 다음을 포함할 수 있습니다.

1. 접근 및 변경 제어를 위한 **시간 및 날짜 기간**
2. **명령 또는 애플리케이션**: 보안 침해 표시기일 수 있음
3. 중요한 정보에 대한 **접근 감지**
4. 기본 세션 **종료**
5. **해당하는 참고 자료 존재**: 티켓팅 솔루션 내
6. 소프트웨어 설치 또는 파일 수정 등 리소스에 대한 **부적절한 수정**
7. 측면 이동 시 **부적절한 시도**
8. 사용자 계정 또는 데이터 세트 **조작, 생성 또는 삭제**

이는 모든 정책 변수의 전체 목록은 아니지만, 해당하는 트리거에 따라 JIT 계정을 제공하거나 종료하기 위한 기준을 필터링하는 데 도움이 될 수 있습니다.

JIT PAM 자동화

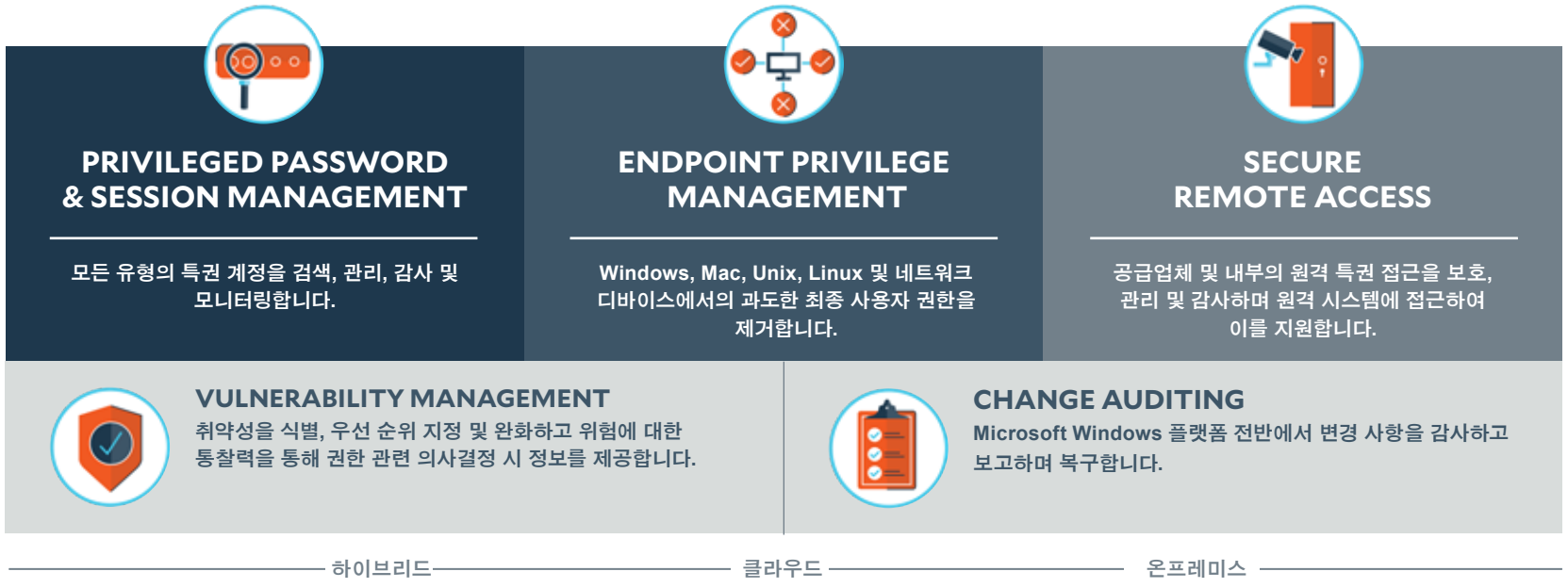
JIT PAM의 실제



BeyondTrust 솔루션으로 최적의 특권 액세스 관리를 활성화하는 방법

BeyondTrust 특권 액세스 관리 플랫폼은 조직 환경에 JIT PAM 보안 모델을 실현할 수 있으며, 또한 특권 계정 검색 및 관리, 최소 권한, 크리덴셜 관리, 권한 분리 및 작업 분리, 권한 감사, 그리고 권한 부여에 따른 위협 분석 등과 같이 특권 계정 IAM/PAM 전략의 다른 중요한 측면을 실행하여 보안을 향상시킬 수 있습니다.

BeyondTrust는 엔드포인트(데스크톱, 서버 등) 전반의 특권 크리덴셜 및 세션, 권한 상승/위임, 그리고 광범위한 트리거를 포함하는 원격 접근(직원, 공급업체 등)을 중앙 집중식으로 관리하여 JIT 모델을 지원합니다. BeyondTrust PAM 플랫폼은 다양한 통합 솔루션을 포함합니다.



BeyondTrust는 엔드포인트(데스크톱, 서버 등) 전반의 특권 크리덴셜 및 세션, 권한 상승/위임, 그리고 광범위한 트리거를 포함하는 원격 접근(직원, 공급업체 등)을 중앙 집중식으로 관리하여 JIT 모델을 지원합니다.

BeyondTrust 솔루션	JIT PAM을 지원하는 특징 및 기능					
Privileged Password & Session Management	**지속적인 자동 계정 검색 및 자동 온보딩**	**안전한 SSH 키 관리**	**애플리케이션 간 패스워드 관리**	**향상된 권한으로 세션 관리**	**적응형 접근 제어**	**권한 부여에 따른 고급 위협 분석**
모든 유형의 특권 계정을 검색, 관리, 감사 및 모니터링합니다.	분산형 네트워크 검색 엔진을 활용하여 모든 자산을 검사하고 파악하며 프로파일링합니다. 동적 범주화는 새로운 계정이 삭제될 때 효율적인 관리 및 JIT 접근을 위한 Smart Group에 대한 자동 온보딩 기능을 구현합니다.	지정된 일정에 따라 SSH 키를 자동 순환하고 세분화된 액세스 제어 및 워크플로우를 구현합니다. 프라이빗 키를 활용하여 다른 사용자에게 키를 노출하지 않으면서 전체 특권 세션 기록을 포함하여 프록시를 통해 사용자가 Unix/Linux 시스템에 안전하게 로그온하도록 합니다.	확장 및 중복이 가능한 패스워드 캐시가 무제한으로 포함된 적응형 API 인터페이스를 통해 하드 코딩되거나 내장된 애플리케이션 크리덴셜을 제거합니다. 이를 통해 모든 애플리케이션의 최신 패스워드에 대한 JIT 액세스를 구현합니다.	라이브 세션 관리를 통해 진정한 이중 제거가 가능하여 관리자는 세션을 없애거나 생산성을 저해하지 않고도 모든 JIT 작업에 기반하여 의심되는 행동을 기록하고 중단시키며 문서화할 수 있습니다.	사용자가 시스템에 대한 액세스 권한 부여를 결정하기 위해 리소스에 액세스할 때 해당 요일, 날짜, 시간 및 장소를 고려하여 적기에 컨텍스트를 평가하고 액세스 요청을 단순화합니다.	날짜별로 자산의 특성 및 사용자 행동을 측정하여 모든 변화의 범위 및 속도를 평가하며 의심되는 이상 현상에 대해 알려줍니다.
Endpoint Privilege Management	**최소 권한 적용**	**완벽한 애플리케이션 제어**	**전체 감사 및 보고**	**권한 부여에 따른 위협 분석**	**보안 협력 체계 통합**	
최소 권한을 적용하여 Windows, Mac, Unix, Linux 및 네트워크 디바이스에서의 과도한 최종 사용자 권한을 제거합니다.	세분화된 정책 기반 제어를 통해 모든 운영 체제에서 표준 사용자용 애플리케이션의 권한을 높여, 적시에 작업을 완료하기 위한 적절한 수준의 접근만을 제공합니다.	포괄적인 규칙을 수립하기 위한 유연한 정책 엔진을 통해 신뢰 기반의 애플리케이션 화이트리스트, 블랙리스트 및 그레이리스트를 제공합니다. 고급 사용자를 위한 자동화된 승인을 선택하거나 (완전한 감사 기록을 통해 보호), 문제-대응 코드를 활용하여 적시 애플리케이션 제어를 구현합니다.	포렌식을 가속화하고 규정 준수를 간소화하는 사용자의 모든 작업에 대한 단일화된 명확한 감사 내역을 제공합니다.	최고 수준의 보안 솔루션에서 얻은 자산 취약성 데이터와 보안 인텔리전스를 사용자 행동과 연계하여 최종 사용자 위험의 전반적인 상태를 알려줍니다.	헬프 데스크 애플리케이션, 취약성 관리 검사 프로그램 및 SIEM 툴 등 타사 솔루션에 대한 기본 커넥터 덕분에 조직에서 보안 투자 회수를 실현할 수 있습니다.	

BeyondTrust 솔루션		JIT PAM을 지원하는 특징 및 기능					
Secure Remote Access		**특권 접근 제어**	**세션 모니터링**	**공격 경로 감소**	**패스워드 관리와 통합**	**모바일 및 웹 콘솔**	**감사 및 규정 준수**
공급업체 및 내부의 원격 특권 접근을 보호, 관리 및 감사하며, 원격 시스템에 접근하여 이를 지원합니다.	**원격 공급업체 및 타사 액세스**	사용자에게 모든 원격 세션에 대한 적절한 접근 수준을 제공하여 최소 권한을 실현합니다.	RDP, VNC, HTTP/S 및 SSH 연결에 대한 표준 프로토콜을 사용하여 세션을 제어하고 모니터링합니다.	최적의 특권 계정에 대한 추적, 승인 및 감사를 한 곳에 통합하고 단일 접근 경로를 생성하여 위협 경로를 줄입니다.	한 번의 클릭만으로 적시에 서버 및 시스템에 크리덴셜을 직접 주입하여 사용자가 일반 텍스트 크리덴셜을 절대 보거나 알 필요가 없습니다.	모바일 애플리케이션 또는 웹 기반 콘솔을 언제 어디서나 적시에 사용하여 원격 접근 작업을 수행합니다.	상세한 세션 데이터를 실시간으로 또는 세션 후 검토를 통해 캡처하여 감사 내역, 세션 포렌식 및 기타 보고 기능을 생성하고, 증명 보고서를 제공하여 규정 준수를 검증합니다.
	원격 지원 및 헬프 데스크 담당자	**채팅 지원**	**광범위한 플랫폼 지원**	**세분화된 권한 및 역할**	**협업**	**세션 기록 및 감사 내역**	**Chrome, Firefox, IE 등 지원**
		화면 공유 및 원격 제어를 위한 적시 확장을 제공하는 클릭 투 챗(Click-to-chat)을 통해 최종 사용자와의 연락을 끊지 않고도 사용자의 웹사이트에서 라이브 지원을 구현합니다	Windows, Mac, Linux, iOS 및 Android 디바이스와 상호 지원됩니다. 또한 RDP, Telnet, SSH 및 VNC 를 사용하여 기존 디바이스를 지원합니다.	팀, 사용자, 역할 및 세션 허가 설정을 세부적으로 관리하여 최소 권한 보안 방침을 이행합니다.	지원 인시던트를 보다 빠르게 해결하고 숙련된 리소스에 대한 확장 경로를 정의하면서 적절한 팀 구성원을 적시에 포함하여 고객 만족도를 높입니다.	팀 성과를 추적하고 세션 활동을 기록하여 보안, 규정 준수 및 훈련을 위한 감사 내역으로 제공합니다.	BeyondTrust의 HTML5 웹 대표 콘솔은 다운로드할 필요 없이 모든 브라우저에서 적시에 Secure Remote Support 를 제공하므로 즉시 문제 해결을 시작할 수 있습니다.

JIT 방법 및 트리거 매핑

다음 매트릭스는 각 BeyondTrust 솔루션에 JIT PAM 트리거 및 방법을 매핑합니다.

	Privileged Password & Session Management	Endpoint Privileged Management	Secure Remote Access
트리거			
권한 유형	●		●
워크플로우	●	●	●
컨텍스트 인식	●	●	●
다단계	●	●	●
방법			
계정 생성 및 삭제	●		
그룹 멤버십 권한	●		
위장	●	●	●
비활성화된 관리 계정		●	
토큰화		●	

BEYONDTRUST와 JIT PAM

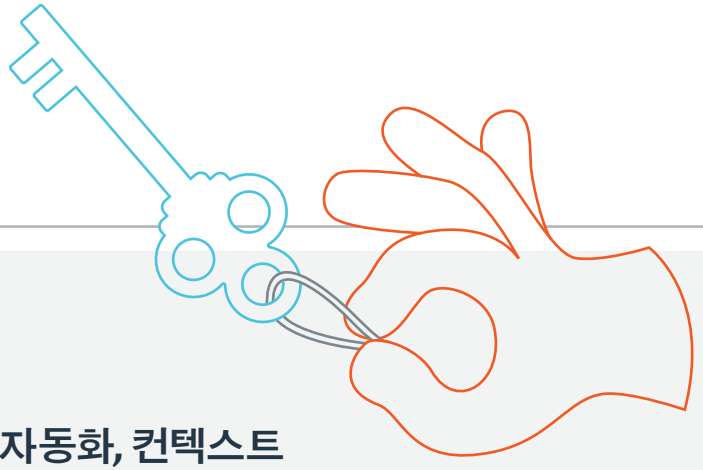
JIT PAM 구현을 통한 사이버 위험 감소

많은 조직에서 적절한 수준의 접근 모델과 동시에 JIT 전략을 구현하는 것은 소중한 IT 자산을 보호하기 위해 다음으로 취할 수 있는 가장 효과적인 단계입니다.

JIT 권한 관리는 진정한 최소 권한 전략의 필수 구성 요소로 간주되어야 합니다. 인증된 후 항상 계정을 활성화하는 대신, 계정을 사용하기 위한 적절한 비즈니스 기준을 충족할 때까지 모든 특권 작업을 거부하도록 보안 모델을 확장하여 사용할 수 있는 시기와 방법에 대한 추가적인 제어를 행사하십시오. 이를 통해 계정 접근 뿐만 아니라 계정이 실시간으로 사용할 수 있는 실제 권한, 사용 권한 및 권한 유형을 제한할 수 있습니다.

컨텍스트 트리거에 사용하는 최적의 특권 접근 관리를 활성화하고 실시간 정책에 기반하여 특권 계정의 사용자 행동이 적절한지 확인함으로써, JIT PAM은 상시 계정으로 인한 상당한 전사적인 위험을 동적으로 해결합니다. 이는 특권 접근 관리의 자연스러운 발전은 물론 IT 위험 관리 부문의 상당한 진보를 의미합니다.

BeyondTrust 특권 접근 관리는 조직에서 최종 사용자의 생산성과 보안을 유지하면서 점점 더 복잡해지는 이기종 IT 환경 전반에 퍼져 있는 상시 특권 계정의 과제 및 위험을 해결하도록 지원합니다.



JIT PAM의 주요 이점

1. **권한의 중앙 집중식, 자동화, 컨텍스트 인식 및 시간 기반 프로비저닝/프로비저닝 해제를 통해 권한이 잠재적으로 악용될 수 있는 취약성 시간을 상당히 줄여줍니다.**

2. **진정한 최소 권한 적용은 보다 적은 권한이 부여된 사용자 및 세션과 동일한 효과를 제공하며, 보안을 개선하고 감사 및 규정 준수 이니셔티브를 간소화할 수 있습니다.**

3. **최종 사용자에게 영향을 미치지 않고 원활하게 작동하여 워크플로우 중단 없이 생산성을 지원합니다.**

4. **상시 특권 계정 및 이에 연결된 공격 벡터가 제거됩니다.**

관련 개념 및 용어

권한: 권한은 특정 보안 제약을 재정의하거나 우회할 수 있는 권한을 부여하며, 시스템 종료, 디바이스 드라이버 로딩, 네트워크 또는 시스템 구성, 계정 및 클라우드 인스턴스의 프로비저닝 및 구성과 같은 동작을 수행할 수 있는 권한을 포함할 수 있습니다.

브레이크 글래스: 컴퓨팅 컨텍스트에서 브레이크 글래스란 일반적으로 다른 액세스 방법이 실패하거나 접근할 수 없는 중요한 응급 상황에서 정상적인 접근 제어 절차를 우회하기 위한 시스템 계정 패스워드 확인을 의미합니다. 브레이크 글래스는 사용자에게 일반적으로 접근이 승인되지 않을 수 있는 계정에 대해 즉각적이지만 일반적으로 시간이 제한된 접근을 제공합니다.

슈퍼 사용자 계정: 슈퍼 사용자 계정은 특권이 높은 계정으로 주로 전문 IT 담당자의 관리 작업에 사용되며, 명령을 실행하고 시스템 변경을 수행하기 위해 실질적으로 제한 없는 능력을 제공합니다. 슈퍼 사용자 계정은 일반적으로 Unix/Linux 환경에서 “루트” 또는 Windows 시스템에서 “관리자”를 의미합니다. 슈퍼 사용자 권한은 파일, 디렉토리 및 리소스에 대해 전체 읽기/쓰기/실행 권한을 포함하는 제한 없는 접근을 제공할 수 있습니다. 슈퍼 사용자 계정은 또한 파일 또는 소프트웨어 생성 또는 설치, 파일 및 설정 수정, 사용자 및 데이터 삭제 같은 네트워크 전반의 시스템 변경을 렌더링할 수 있습니다. 슈퍼 사용자는 다른 사용자에 대한 접근 및 권한을 프로비저닝/프로비저닝 해제할 수도 있습니다.

최적의(JIT) 특권 접근 관리: JIT 권한 관리의 목표는 승인된 작업 또는 임무에 기반하여 필요한 권한을 “즉시” 할당한 다음 작업이 완료되거나 승인된 접근에 대한 시간 또는 컨텍스트가 만료되면 이를 제거하는 것입니다. JIT 권한 관리를 사용하면 조직은 행동 및 컨텍스트 매개 변수를 근거로 제한을 적용하여 지속적인 상시 접근으로부터 특권 계정을 보호할 수 있습니다.

최소 권한: 최소 권한이란 사용자, 계정 및 컴퓨팅 프로세스에 대한 접근 권한을 일상적인 승인된 작업을 수행하기 위해 절대적으로 필요한 리소스로만 제한하는 개념 및 사례를 의미합니다. 최소 권한 보안 모델은 사용자가 역할을 수행하도록 허용하는 최소 수준의 사용자 권한 또는 가장 낮은 보안 인가 등급을 적용합니다. 최소 권한은 또한 프로세스, 애플리케이션, 시스템 및 디바이스(예: IoT)에도 적용되며, 이 경우 각 권한은 승인된 작업을 수행하기 위해 필요한 권한만 보유할 수 있습니다.

특권 계정: 특권 계정이란 비특권 계정 이상의 접근 및 권한을 제공하는 모든 계정으로 간주됩니다(예: 표준 계정 및 게스트 사용자 계정). 특권 사용자는 현재 특권 계정 등을 통해 특권 접근을 활용하는 모든 사용자를 의미합니다. 이러한 향상된 기능 및 접근으로 인해 특권 사용자/특권 계정은 비특권 계정/비특권 사용자보다 상당히 큰 위험을 야기합니다.

특권 세션: 특권 세션이란 일반적으로 표준 사용자의 권한 이상의 특권을 필요로 하는 작업 실행에 연관된 컴퓨팅 세션을 의미합니다. 특권 세션은 사용자, 시스템, 애플리케이션 또는 서비스에 의해 시작될 수 있습니다.

특권 세션 관리(PSM): 특권 세션 관리(PSM)는 향상된 접근 및 권한과 연관된 사용자, 시스템, 애플리케이션 및 서비스에 대한 모든 세션의 모니터링 및 관리를 수반합니다. PSM은 내부 위협 또는 잠재적인 외부 공격으로부터 보다 효과적으로 환경을 보호하는 데 사용될 수 있는 고급 감독 및 제어를 구현하는 동시에 점점 더 많은 규제 및 규정 요건 준수를 위해 필요한 중요 포렌식 정보를 유지합니다.

특권 접근 관리(PAM): 특권 계정 관리, 특권 ID 관리(PIM) 또는 간단하게 권한 관리라고도 부르는 PAM은 특권 계정을 관리하고 보호하며 사용자, 애플리케이션, 서비스, 프로세스, 작업 등에 대한 권한 위임 및 확장 작업을 제어하는 솔루션 및 전략을 의미합니다. PAM 솔루션을 활용하여 조직은 (서버 및 데스크톱 전체의) 사용자로부터 관리자 권한을 제거하는 대신, 필요에 따라 승인된 애플리케이션 또는 작업에 대한 권한을 높일 수 있습니다.

표준 사용자 계정: 표준 사용자 계정은 때때로 최소 권한 사용자 계정(LUA) 또는 비특권 계정으로 불리며 제한된 권한 세트를 보유합니다. 최소 권한 환경에서 이러한 계정은 대부분의 사용자가 90% 이상의 비율로 운영하는 계정 유형입니다. 표준 사용자는 컴퓨팅 환경(Windows, Mac, Unix 등)에서 기본 접근 권한을 가지는 비특권 사용자입니다. 이러한 계정/사용자 유형은 광범위한 관리 권한 및 특권 접근을 가진 특권 사용자 또는 슈퍼 사용자 계정(루트 또는 관리자)과 달리 리소스 및 설정에 대해 제한된 접근을 가집니다.

BeyondTrust 소개

BeyondTrust는 특권 접근 관리 분야의 세계적 선도업체로서 크리덴셜 유출, 권한 오용 및 원격 액세스 손상과 관련된 데이터 보안 침해를 방지하기 위한 가장 완벽한 접근 방식을 제공합니다. 엔드포인트, 서버, 클라우드, DevOps 및 네트워크 디바이스 환경 전반으로 위협이 번지는 상황에서 조직은 확장성 플랫폼을 통해 손쉽게 권한 보안 조치를 확대할 수 있습니다. BeyondTrust는 위험 완화, 규정 준수 목표 달성 및 운영 성과 향상을 위해 조직에 필요한 가시성과 제어 능력을 제공합니다. Fortune지 선정 100대 기업 중 절반 이상 및 글로벌 파트너 네트워크를 포함하여 20,000여 고객의 신뢰를 받고 있습니다.

beyondtrust.com/ko

V2019_07_KOR