백서 • 2017년 9월

가장 중요한 서버의 데이터 침해 위험 감소: CA 솔루션의 문제 해결 방식

목차

개요

과제

오늘날 기업은 조직 내의 중요한 데이터를 보호하기 위해 보안 침해의 위험을 줄여야 합니다. 동시에 IT 감사자는 갈수록 엄격해지는 비즈니스 요구 사항을 더욱 많이 시행하고 있습니다. 결론적으로 특권 계정 및 특권 액세스는 해커의 새로운 공격 영역이 되고 있으며 감사자는 이에 초점을 맞추어 특권 계정에 대한 한층 강력한 제어를 요구하고 있습니다.

기회

알맞은 특권 액세스 관리 솔루션은 운영 체제 수준의 액세스 및 권한 있는 사용자 작업에 강력하고 세밀한 제어 기능을 사용하여 사용자의 미션 크리티컬 서버를 포괄적으로 보호합니다. 이 시스템 수준의 호스트 기반 특권 액세스 관리 솔루션은 UNIX® 및 Linux® 루트 및 Microsoft® Windows® 관리자와 같은 강력한 기본 슈퍼 유저 계정의 액세스를 제어할 수 있어, 권한 있는 사용자의 작업을 제어, 모니터링 및 감사하여 보안을 개선하고 감사 및 규정 준수를 간소화합니다.

이점

CA 테크놀로지스는 통합된 자격 증명 관리, 강력한 인증, 제로 트러스트 액세스 제어, 능동적인 명령어 필터링, 세션 모니터링 및 기록, 고부가가치 서버에 대한 세밀한 제어 기능을 갖추었으며 배포가 쉽고 포괄적인 특권 액세스 관리 솔루션을 제공합니다. CA Privileged Access Management는 공격자가 공격의 주요 단계를 수행하지 못하도록 적극적으로 차단하는 동시에 위험을 낮추고 운영 효율을 높여주는 다양한 기능과 제어 수단을 제공합니다. 위험 감소, 책임감 향상, 감사 및 규정 준수 개선, 복잡성 감소 등의 이점을 누릴 수 있습니다.

서론

오늘날 기업은 조직 내의 중요한 데이터를 보호하기 위해 보안 침해의 위험을 줄여야 합니다. 동시에 IT 감사자는 갈수록 엄격해지는 비즈니스 요구 사항을 더욱 많이 시행하고 있습니다. 결론적으로 특권 계정 및 특권 액세스는 해커의 새로운 공격 영역이 되고 있으며 감사자는 이에 초점을 맞추어 특권 계정에 대한 한층 강력한 제어를 요구하고 있습니다.

안타까운 사실은 공격의 출처에 관계없이 모든 지능형 공격에서 공격자들의 성공 여부는 전적으로 특권 계정의 절취 및 악용 가능성에 달려 있다는 점입니다. 이러한 계정에는 직원, 제3자 협력업체, IT 인프라에 존재하는 특권 자격 증명(종종 하드 코딩되어 불특정 다수가 볼 수 있음)이 포함된 무수한 애플리케이션 및 스크립트와 같은 권한 있는 사용자, 계정 및 자격 증명이 포함됩니다.

또한 UNIX, Linux 및 Windows와 같은 운영 체제는 시스템 보안 제어의 대부분 또는 모두를 우회할 수 있는 '슈퍼 유저' 개념을 기반으로 합니다. 이처럼 고도의 권한을 가진 계정은 관리자가 합법적인 용도로 사용하지만, 악의적인 내부자 또는 외부 공격자에 의해 악용될 소지 또한 있습니다.

이러한 사용자 및 자격 증명을 보호하는 것은 공격 방지의 핵심 요소이며, 특권 액세스 관리는 비즈니스 보호를 위한 심층 전략에서 방화벽 및 바이러스 백신 못지않게 중요한 새로운 필수 구성 요소가 되었습니다. 알맞은 특권 액세스 관리 솔루션은 운영 체제 수준의 액세스 및 권한 있는 사용자 작업에 강력하고 세밀한 제어 기능을 사용하여 사용자의 미션 크리티컬 서버를 포괄적으로 보호합니다. 이 시스템 수준의 호스트 기반 특권 액세스 관리 솔루션은 UNIX 및 Linux 루트 및 Windows 관리자와 같은 강력한 기본 슈퍼 유저 계정의 액세스를 제어할 수 있어, 권한 있는 사용자의 작업을 제어, 모니터링 및 감사하여 보안을 개선하고 감사 및 규정 준수를 간소화합니다.

본 백서에서는 미션 크리티컬 서버 보호라는 과제와 오늘날 사용 가능한 접근법을 다루는 한편, 미션 크리티컬 서버 보호에 가장 성숙하며 강력한 검증된 솔루션을 제공하는 CA Privileged Access Manager Server Control을 소개합니다. CA Privileged Access Manager Server Control은 검증된 메인프레임 보안 모델을 기반으로 하므로 슈퍼 유저를 대상으로도 매우 효과적인 능동적인 액세스 제어 및 뛰어난 감사를 적용할 수 있게 합니다.

미션 크리티컬 서버 보안에 대한 오늘날의 과제

악의적인 내부자 및 외부 해커는 미션 크리티컬 서버의 권한 있는 사용자 계정을 빼앗아 악용하려 합니다. 단 한 번의 침해로 조직이 평판 및 재정 손해를 광범위하게 입을 수 있습니다. IT 부서는 표적 공격을 막고 내부자 위협을 완화하는 동시에 규정 준수 요구 사항을 달성하고 유지하기 위해 업계 보안 요구 사항 및 표준을 따라야 한다는 엄청난 압박을 받고 있습니다. IT 부서는 갈수록 복잡해지는 하이브리드 인프라를 관리 및 보호하는 동시에 자동화 및 확장성을 통해 운영 효율성을 달성해야 합니다. 책임의 범위가 상당합니다.

일반적으로 위험은 서버에 저장된 내용이 미션 크리티컬한지에 따라 허용 가능한 수준으로 줄어듭니다. 일부 서버는 신용카드 정보, 주민등록번호, 개인 식별 정보, 의료 기록, 이메일 주소 또는 계획, 재무 결과 및 내부자 정보와 같은 지적 재산 정보로 인해 다른 서버보다 가치가 높습니다. 특권 액세스 관리가 위험을 줄여주지만, 대부분의 미션 크리티컬 서버를 보호하려면 추가 조치가 필요합니다. 이러한 접근법 중 몇 가지를 살펴보겠습니다.

주요 접근법 중요 시스템의 보호에는 기본적인 '강화' 이외의 대책이 필요함

IT의 가장 큰 과제 중 하나는 고객 데이터, 금융 기록 및 지적 재산과 같은 회사의 민감한 전자 자산을 호스트하는 서버의 보안을 보장하는 것입니다. 이러한 자산은 여러 조직의 대동맥이나 마찬가지며 침해될 경우 돌이킬 수 없는 피해를 입게 됩니다.

일반적인 '서버 강화'로 다음과 같은 조치를 시행할 수 있습니다.

- 네트워크에 연결하기 전에 모든 패치 설치
- 불필요한 서비스 제거
- 사용하지 않는 소프트웨어 및 샘플 파일 삭제
- 바이러스 백신 및 스파이웨어/피싱 차단 소프트웨어 설치
- 민감한 드라이브 암호화
- 강력한 암호 사용
- 소수의 핵심 관리자만 슈퍼 유저 암호를 공유

이러한 지침 대부분은 좋은 조언이며 일반적으로 수용되는 보안 원칙을 따른 것이지만, 마지막 지침은 관리 시스템 계정을 효과적으로 제어하기가 불가능하다는 근본적으로 잘못된 가정에서 출발한 것입니다. 이 지침처럼 하면 악의적 내부 사용자뿐만 아니라 외부 공격자까지도 악용할 수 있는 커다란 서버 보안 허점이 생깁니다. 공격의 출처에 상관없이 특권 ID를 사용한 공격은 가장 큰 피해를 입힙니다. 본질적으로 특권 ID 계정에는 시스템, 애플리케이션 또는 데이터베이스에 중요한 영향을 미칠 수 있는 변경 권한이 있습니다. 이러한 계정을 사용하는 작업은 큰 피해를 줄 가능성이 있으므로 면밀한 모니터링이 필요합니다.

운영 체제가 제공하는 기본 보안 기능

운영 체제의 기본 제어 기능에서 보안 과제의 핵심은 기본적으로 슈퍼 유저라는 개념에 기반한다는 사실입니다. 슈퍼 유저는 서버의 모든 보안 제어를 기본으로 우회 및 무효화할 수 있는 특권 계층입니다. 슈퍼 유저의 가장 흔한 예는 Linux/UNIX '루트' 계정과 Windows '관리자' 계정입니다.

운영 체제는 이러한 계정의 무제한적인 성격을 전제로 설계됩니다. 이러한 이유로 슈퍼 유저 계정은 공격자의 먹음직스러운 공격 대상이 됩니다. 침입자가 슈퍼 유저 계정을 손에 넣게 되면 익명으로 서버의 아무 곳에나 사실상 무제한 액세스할 수 있게 되는데, 이는 계정이 특정 개인과 관련이 없기 때문입니다. 따라서 대부분의 상용 서버 기반 솔루션은 사용자의 능력을 제어 및 제한하려고 시도하며 슈퍼 유저 계정을 사용하게끔 합니다. ***이러한 접근법의 결점은 이미 슈퍼 유저 권한을 악용하고 있는 사용자로부터 서버를 방어할 수 없다는 것입니다***. 보안 제어 자체도 의욕적으로 공격하는 숙련된 공격자에게 뚫릴 수 있습니다. 또한 보안 제어는 대개 솔루션이 제어하려고 시도해야 하는 그룹 중 하나인 시스템 관리자가 관리하고 유지합니다. 이는 고양이에게 생선을 맡긴 것과 다름없습니다.

위와 같은 이유로, 운영 체제의 기본 제어 기능은 실수나 고의에 의한 공격을 충분히 방어하지 못할 뿐만 아니라 전체 서버 환경을 신뢰성 있게 감사할 수 없으므로 고객 데이터베이스, 병원 환자 기록 또는 독점 정보 같은 조직의 가장 민감한 전자 자산을 보호하는 데 어려움이 따릅니다. 외부 고객용 호스팅 시스템에 기밀 데이터 및 중요 애플리케이션이 포함되어 있거나, 중요 시스템 또는 정보가 협력업체에 노출되거나 서비스 공급자를 통해 호스팅되는 경우에는 문제가 더욱 심각해집니다.

운영 체제 액세스 제어는 **알려진 제어**이기 때문에 또한 분석 및 차단될 위험이 따릅니다. 악의적인 공격자가 특권 계정에 대한 액세스 권한을 확보한 경우(외부자의 무단 액세스 또는 내부자의 액세스) 공통적으로 수행할 첫 단계는 보안 설정을 조사하는 것입니다. 운영 체제 권한을 살펴보고 악의적으로 이용될 수 있는 제어 취약성을 찾는 과정이 여기에 포함됩니다. 또한 악의적인 사용자는 자신의 흔적을 숨기기 위해 운영 체제 로그를 수정하려고도 합니다. 액세스 제어가 엄격하게 시행되는 시스템이라 해도 잘 훈련된 공격자들은 경고를 발생시키고 감지당할 만한 행동을 쉽사리 하지 않습니다. ***슈퍼 유저조차도 규제 대상일 정도로*** 완전하게 외부화된 보안 시스템만이 **예측 불가능하고 파악 불가능한** 보안 요소를 보안 시스템에 구현하는 한편, 시스템을 완전히 보호하기 위해 요구되는 액세스 제어 및 사용자 활동 로그를 제공할 수 있습니다.

운영 체제는 또한 본질적으로 자체 제어의 무결성을 보장하지 못합니다. 모든 시스템에는 해당 시스템의 보안 제어를 변경하거나 우회할 수 있는 특권 계정이 존재합니다. 적절한 액세스 권한을 가진 사용자는 무단으로 작업을 수행하기 위해 필수 제어를 해제할 수 있으며 그러한 활동 기록을 지우기 위해 시스템 로그 파일을 수정할 수 있습니다.

운영 체제 보안 제어에 의존할 경우 따르는 또 다른 문제는 이들 보안 제어의 **통일성 부재**입니다.

플랫폼에 따라 보안 제어의 제공 여부와 그 성능에 상당한 차이가 있을 수 있습니다(예: UNIX 파일/디렉터리 제어는 Windows의 제어와 크게 다름). 이는 다음과 같은 실질적인 보안 문제로 이어질 수 있습니다.

- 비즈니스 니즈를 충족하는 보안 정책이 아닌 시스템 한계에 맞춘 보안 정책이 생성됩니다.
- 보안 관리의 복잡성이 증가하여 오류 및 누락이 발생합니다.

셸 래퍼

운영 체제 제어 기능을 사용하여 권한 있는 사용자를 제어하는 일반적 방법은, 특정 개인이 특정 명령에 액세스하는 것을 허용하거나 거부하도록 구성 가능한 셸 래퍼를 사용하는 것입니다. 셸 래퍼는 운영 체제의 사용자 모드에서 실행되므로 명령이 커널(운영 체제의 하위 수준 구성 요소)에 의해 실행됩니다.

셸 래퍼에는 다음과 같이 많은 취약성이 있습니다.

- 셸 래퍼는 슈퍼 유저 계정 자체를 차단하지는 못합니다. 루트 계정에 대한 액세스 권한이 있는 사용자와 IT 지식이 풍부한 다른 사용자는 항상 다음과 같은 방법으로 셸 래퍼를 우회할 수 있습니다.
  - 루트 사용자가 설정된 셸 래퍼를 무효화하고, 커널이 래퍼 제한이 없는 새로운 셸을 만듭니다.
  - 사용자가 대상 시스템에 스크립트를 업로드하고 파일을 실행합니다. 그러면 모든 명령이 셸 래퍼를 우회하여 운영 체제 커널에 의해 실행됩니다. 이 스크립트는 셸 래퍼의 감시나 제어를 전혀 받지 않고 중요한 데이터를 수정, 삭제하거나 시스템 외부로 전송할 수 있습니다.
- 셸 래퍼는 셸에 입력된 명령만 보호할 수 있습니다. 시스템의 다른 애플리케이션(예: Oracle)에 보안 구멍이 생겨 악성 명령을 실행하는 데 이용될 수 있습니다. 이러한 상황은 셸 래퍼에 의해 감지, 제어되거나 기록되지 않습니다.
- 키 로거 역시 눌러진 키만 캡처할 뿐, 실행되는 명령은 캡처하지 않기 때문에 셸 래퍼의 일부일 경우 효과가 없습니다. 악의적인 사용자(또는 관리자 등)가 여러 작업을 수행하는 스크립트를 업로드할 수 있습니다. 그러면 키 로거는 스크립트가 실행되었다는 것만 기록하고 실제 수행된 작업은 기록하지 않습니다. 이로 인해 책임 소재가 불분명해지며 키 로거의 원래 목적이 의미를 상실합니다.
- 셸 래퍼를 옹호하는 공급업체에서는 루트 암호를 사용하거나 공유하지 말라고 권장하는 경우가 많습니다. 하지만 이는 현실적으로 어렵습니다. 설치 또는 실행을 위해서는 루트 암호가 필요한 애플리케이션도 많기 때문입니다.

sudo

sudo('superuser do'의 줄임말)는 시스템 관리자가 특정 사용자(또는 사용자 그룹)에게 일부(또는 전체) 명령을 루트로 실행할 수 있는 권한을 주고 사용된 모든 명령을 기록할 수 있는 프리웨어 프로그램입니다. sudo는 대부분의 UNIX/Linux 환경에서 운영 담당자가 루트 셸에 액세스할 필요는 없지만 프로세스 시작/중지, 특정 구성 파일 업데이트, 서버 재부팅 등과 같은 특정 명령을 루트로 실행해야 할 필요가 있을 때 많이 사용됩니다. sudo는 중요한 기능(특권 작업 위임)을 제공하지만, 그 자체는 부적절한 제어입니다.

sudo에는 다음과 같이 많은 취약성이 있습니다.

- sudo는 하나 이상의 sudoers 파일을 사용해야 하는데, sudoers 파일을 관리하는 데는 시간과 리소스가 많이 소요되고 오류가 발생할 확률이 큽니다. 더군다나 sudoers 파일과 그 관리가 다름 아닌 보안 침해 위험을 안고 있는 특권 ID에 의해 수행되므로 적절한 보안 기능을 제공하기 힘듭니다.
- sudo는 엔터프라이즈급 로깅 기능을 제공하지 않습니다. sudo는 루트 사용자의 무단 개조에 취약한 UNIX syslog를 사용합니다. sudo는 각 sudo 작업에 대한 책임 소재를 명확하게 보여 주지 않습니다. sudo를 통해 실행되는 명령 중에는 로깅이 되지 않아 원래 사용자를 추적하지 못하는 것도 있습니다. 이 경우 PCI 및 SOX의 요구 사항 충족이 어렵습니다.
- sudo는 사용자가 셸로 침입할 때조차 "vi"를 호출하는 원래 사용자 ID를 기반으로 작업을 감사하고 추적하지 않습니다. 사용자가 sudo를 사용하여 루트로 "vi"를 호출하면, "vi"에서 벗어나 루트 권한으로 셸 명령을 실행할 가능성이 있습니다. CA Privileged Identity Suite sudo를 사용하면 실행되는 이러한 모든 셸 명령이 sudo를 호출한 원래 사용자까지 추적됩니다.
- sudo에는 중요한 기능 제한이 있습니다. sudo는 사용자 관련 파일/폴더 또는 명령 액세스 권한을 할당하거나 제한하지 못합니다.
- 사용자가 권한을 승격하면 sudo는 실패합니다. OS 취약성을 악용하여 '루트' 액세스 권한을 획득한 일반 사용자는 모든 sudo 제한을 우회합니다.
- 또한 운영 체제의 기본 제어 기능을 사용하면 서버 및 플랫폼 전반에서 보안 정책이 일관되지 않게 적용되기도 합니다. 플랫폼 차이를 중화하려면 여러 플랫폼 간에 적용 가능한 하나의 강력한 액세스 제어 집합이 필요합니다.

프록시 제어

액세스 제어를 구현하는 또 다른 방법은 프록시입니다. 이 방법을 사용하면 모든 명령이 중앙 '관문'을 통과하므로 규칙 집합으로 지정된 모든 명령을 필터링(거부)할 수 있습니다. 이 방법은 특정 작업 수행에 필요한 명령을 인식하고 차단하여 권한 있는 사용자가 셸을 '중지(kill)'하는 것을 방지할 수 있습니다.

프록시에는 다음과 같이 많은 취약성이 있습니다.

- 프록시는 애플리케이션을 사용하여 피할 수 있습니다. 사용자는 텍스트 편집기(예: vi)를 사용하여 실행 파일을 생성하고 이를 제한된 명령으로 채울 수 있습니다. 프록시는 애플리케이션 내에서 사용자가 수행 중인 작업을 파악할 수 없습니다. 프록시는 '자동 완성'되거나 서로 나누어진 명령을 감지할 수 없습니다.
- 프록시는 외부 다운로드를 사용하여 피할 수 있습니다. 셸 래퍼와 마찬가지로 사용자는 FTP, SSH, 물리적 USB 드라이브 등의 여러 가지 방법을 사용하는 대상 시스템에 제한된 명령이 포함된 파일을 다운로드하여 프록시를 완전히 우회할 수 있습니다. 이러한 파일 전송 유틸리티는 일반적인 관리 및 시스템 작업이 필요한 경우가 많기 때문에 이 유틸리티에 대한 액세스를 거부하는 것이 불가능할 때가 있습니다.
- 보안이 적용되지 않는 단일 명령이 프록시 제어를 우회하는 백도어로 사용될 수 있습니다.
- 프록시는 소프트웨어 취약성을 보호하는 데는 효과적이지 않을 수 있습니다. 프록시 기반 제어는 제로 데이 공격처럼 취약한 소프트웨어를 대상으로 하는 공격에는 전혀 효과가 없습니다.

액세스 제어/호스트 보안

앞서 언급했듯 공유된 슈퍼 유저 계정을 사용하면 권한 있는 사용자가 중요한 시스템과 데이터에 불필요하게 액세스할 수 있습니다. 이는 '최소 권한'과 '직무 분리'라는 보안 원칙을 위반하는 것입니다. 운영 체제에는 공유 계정을 사용하는 여러 사용자의 작업 및 액세스를 제한할 수 있는 기능이 없습니다. 세부 액세스 제어는 OS 보안을 넘어 ***사용자의 원래 아이덴티티를 확인하여 작업을 허용 또는 거부할지 결정합니다***. 이는 진정한 최소 권한 액세스를 가능하게 합니다.

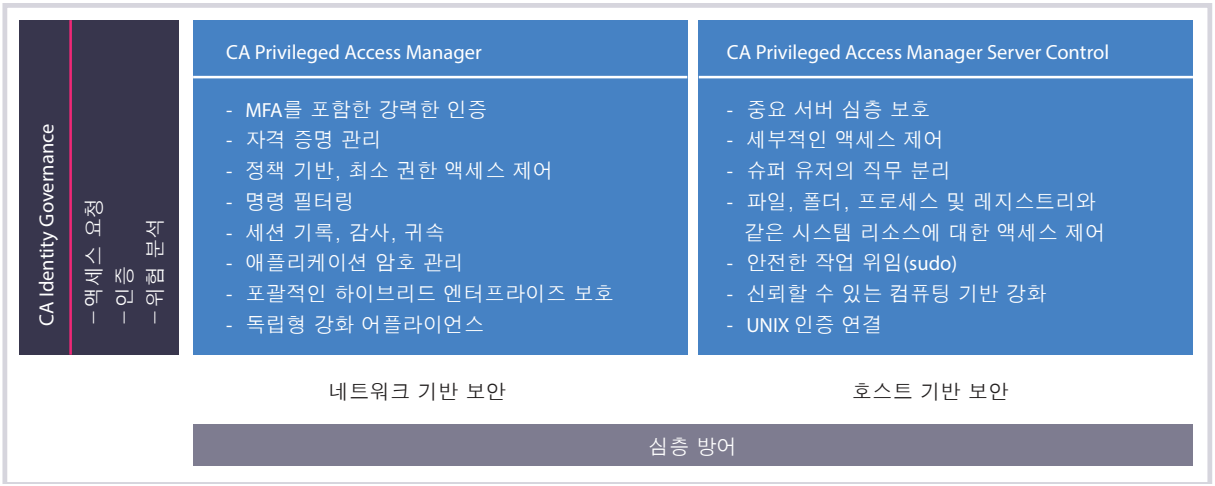
아래의 기능들은 관리자에게 맡은 작업을 수행하는 데 필요한 권한만 제공할 때 사용됩니다.

CA 솔루션의 문제 해결 방식

CA 테크놀로지스는 통합된 자격 증명 관리, 강력한 인증, 제로 트러스트 액세스 제어, 능동적인 명령어 필터링, 세션 모니터링 및 기록, 고부가가치 서버에 대한 세밀한 제어 기능을 갖추었으며 배포가 쉽고 포괄적인 특권 액세스 관리 솔루션을 제공합니다. 이 솔루션에는 보안 및 규정 준수 위험을 최소화하는 두 가지 배포 옵션이 있습니다. 다양한 보안 니즈에 적절한 수준의 방어를 제공하고 특권 계정을 심층적으로 방어하는 것입니다.

- **CA Privileged Access Manager**는 데이터 센터, 소프트웨어 정의 가상 데이터 센터와 네트워크, 퍼블릭/프라이빗 클라우드를 비롯하여 가장 광범위하고 심층적인 인프라 범위 전반을 보호하여 침해를 방지하고 규정을 준수하고 운영 효율성을 향상하는 데 필요한 포괄적인 기능을 제공합니다.
- **CA Privileged Access Manager Server Control**은 운영 체제 수준의 액세스 및 권한 있는 사용자 작업에 대한 강력한 제어 기능을 통해 주요 서버의 권한 있는 사용자 활동을 제어, 모니터링 및 감사함으로써 보안을 강화하고 감사 및 규정 준수를 간소화합니다.
- **CA Threat Analytics for PAM**은 강력한 사용자 행동 분석 및 머신러닝 알고리즘을 제공하므로 비즈니스에 영향을 미치려는 침해 시도를 사전에 탐지하고 대처할 수 있습니다.

그림 A.
CA의 심층 방어 보안 접근법의 핵심 요소



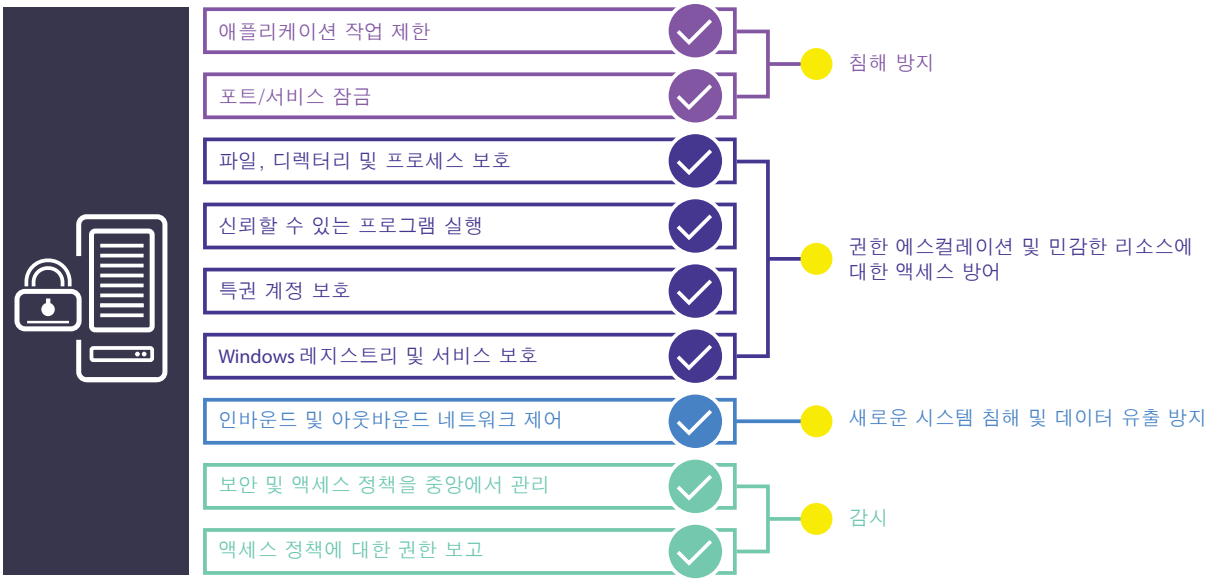
CA Privileged Access Manager Server Control 자세히 살펴보기

비즈니스 크리티컬 자산을 호스팅하는 고가치 서버를 위한 추가 보안 요구 사항이 있는 조직에서는 CA Privileged Access Manager Server Control을 통해 운영 시스템 수준의 액세스와 애플리케이션 수준의 액세스를 로컬화된 방식으로 세부적으로 제어 및 보호할 수 있습니다. 또한 특정 호스트에 대한 정책 및/또는 세부 제어를 기반으로 에이전트를 활용하여 커널 수준에서 개별 파일, 폴더 및 특정 명령을 보호할 수 있습니다.

CA Privileged Access Manager Server Control은 미션 크리티컬 서버의 결함 있는 슈퍼 유저 기반 보안 모델에 내재된 보안 결함을 독창적이고 정확하게 처리합니다. CA Privileged Access Manager Server Control은 다음을 제공합니다.

- 슈퍼 유저 계정이 사용 중인 경우에도 원 사용자 ID 추적 기능을 사용하여 SoD(직무 분리) 및 책임성을 추적합니다. 이 방법은 슈퍼 유저 기반 보안 모델을 근본적으로 바꾸어 줍니다. 예를 들어, Linux 루트 계정을 사용하는 사용자 A는 Linux 루트 계정을 사용하는 사용자 B와는 다른 권한을 가집니다. 또한 변조 방지 감사 로그로 모든 슈퍼 유저 작업을 수행하는 사용자의 실제 ID를 식별할 수 있습니다.
- 파일, 디렉터리 및 시스템 프로세스 리소스에 대한 세분화된 액세스 제어
- 사용자 ID 및 로그인 실행 보호
- UNIX/Linux에 커널 모듈 로드/언로드
- Windows 레지스트리 보호.
- 들어오고 나가는 TCP/IP 보호
- UNIX/Linux 및 Windows를 위한 작업 위임(보안 sudo 대체)
- 루트 암호 숨기기 기능
- 파일 및 프로그램 무결성 모니터링
- 우회 또는 종료에 대한 자체 보호

그림 B.
CA Privileged Access Manager Server Control 자세히 살펴보기



솔루션 이점

CA Privileged Access Manager는 공격자가 공격의 주요 단계를 수행하지 못하도록 적극적으로 차단하는 동시에 위험을 낮추고 운영 효율을 높여주는 다양한 기능과 제어 수단을 제공합니다. 구체적으로 조직에서는 CA Privileged Access Manager로 다음을 실현할 수 있습니다.

- **위험 감소.** 무단 액세스를 예방하고 네트워크 이용을 허가할 때 사전 승인된 리소스에 대한 액세스 권한을 제한할 수 있습니다. 암호 및 다른 자격 증명을 무단 도용 및 손상으로부터 보호할 수 있습니다. 사용자가 시스템에서 수행할 수 있는 작업을 제한합니다. 네트워크에서 권한이 없는 명령 및 측면 이동의 실행을 방지합니다.
- **책임감 향상.** 공유 계정을 사용할 때도 사용자 활동의 책임 소재를 완벽하게 파악할 수 있습니다. 포괄적인 로깅, 세션 기록 및 사용자 경고를 통해 활동을 파악하고 무단 행동을 억제할 수 있습니다.
- **감사 개선 및 규정 준수 촉진.** 새롭게 등장하는 인증 및 액세스 제어 요구 사항을 지원함으로써 규정 준수를 간소화하고, 네트워크를 논리적으로 구획하여 규정 준수 요구 사항의 범위를 제한할 수 있습니다.
- **복잡성 감소 및 운영자 생산성 향상.** 특권 사용자 SSO는 위험을 제한하는 데 도움이 될 뿐만 아니라 관리가 필요한 시스템 및 리소스에 개별 관리자가 더 빠르고 간편하게 액세스할 수 있게 함으로써 생산성을 높일 수 있습니다. 중앙 집중식 정책 정의 및 실행을 통해 보안 제어 조치를 간편하게 생성하고 이행할 수 있습니다. 이 솔루션은 기존의 물리적 데이터 센터(서버, 네트워킹 장치, 데이터베이스, 스위치 및 관련 리소스)와 커지는 가상 및 클라우드 플랫폼을 포괄하는 광범위한 하이브리드 IT 인프라를 보호할 수 있습니다. 이를 통해 소프트웨어 정의 데이터 센터 및 네트워크, IaaS 환경 및 SaaS 오퍼링에 배치된 기본 관리 인프라 및 리소스를 보호할 수 있습니다.

고객은 CA 솔루션은 채택이 용이하며 숨겨진 하드웨어 비용을 피할 수 있다는 사실을 발견하게 됩니다. 관리의 용이성/사용 용이성은 확장 능력뿐만 아니라 가치 실현 시간을 제공하므로 미래에 대비한 하이브리드 IT 인프라를 구축할 수 있으며 위험을 줄이고 규정 준수를 유지할 수 있습니다. 현재 CA Privileged Access Manager를 보유하고 있으며 미션 크리티컬 서버를 보호하려는 고객은 CA Privileged Access Manager Server Control로 업그레이드하는 것이 좋습니다. 심층 방어 프로그램을 사용하여 조직의 보안 상태를 개선하기 시작한 경우라면 CA Privileged Access Manager를 사용하여 내부자 위협 및 특권 계정 남용의 위험을 완화하는 것을 고려해 보십시오.

결론

스마트한 기업에서는 많은 비용이 소모되는 데이터 유출을 방지하기 위해 가장 중요한 서버에서 특권 계정에 대한 액세스를 보호하고 자동화합니다. 보안에 특권 액세스 관리를 비롯한 심층 방어 접근법을 사용하는 제로 트러스트 모델을 채택하므로 귀사의 조직은 끊임없이 진화하는 위협으로부터 최상의 보호를 받을 수 있습니다. CA Privileged Access Manager는 공격자가 공격의 주요 단계를 수행하지 못하도록 적극적으로 차단하는 동시에 위험을 낮추고 운영 효율을 높여주는 다양한 기능과 제어 수단을 제공합니다.

다음 단계

액세스를 보호하는 방법 및 데이터 침해를 방지하기 위해 기업이 할 수 있는 활동에 대한 내용은 **CA 테크놀로지스 Privileged Access Management 구매자 가이드**를 참조하십시오.

CA의 Privileged Access Management에 대한 자세한 내용은 다음을 참조하십시오.
ca.com/pam

CA 테크놀로지스에 연결

CA Technologies(NASDAQ: CA)는 고객이 비즈니스 민첩성을 개선할 수 있도록 복잡한 IT 환경의 관리와 보안을 지원하는 IT 관리 솔루션을 제공합니다. 조직은 CA 테크놀로지스 소프트웨어와 SaaS 솔루션을 활용하여 데이터 센터에서 클라우드에 이르는 모든 환경에서 혁신을 가속화하고 인프라를 전환하며 데이터와 아이덴티티를 보호할 수 있습니다. CA 테크놀로지스는 고객이 CA 기술을 사용함으로써 우수한 성과와 원하는 비즈니스 가치를 실현하도록 지원하기 위해 최선의 노력을 기울이고 있습니다. CA의 고객 성공 프로그램에 대한 자세한 내용을 보려면 ca.com/customer-success 페이지를 방문하시기 바랍니다. CA 테크놀로지스에 대한 자세한 내용은 ca.com/kr을 참조하십시오.

CS200-305094_0917