비밀번호가 없는 인증 방식의 도입 가속화

EMA 연구 보고서 “비밀번호가 없는 인증 - 마찰이 적은 ID 관리와 보안 수준이 높은 ID 관리 간의 격차 해소”의 결과 활용

ENTERPRISE MANAGEMENT ASSOCIATES®(EMA™) 백서

의뢰 고객: IBM

Steve Brasen

2019년 7월

EMA

IT 및 데이터 관리

연구 | 산업 분석 | 컨설팅

비밀번호가 없는 인증에 대한 이해

엔터프라이즈 IT 보안의 주요 목적은 적합한 사용자에게 정상적인 조건에서 올바른 IT 리소스에 액세스할 수 있는 적절한 권한을 부여하는 것입니다. 따라서 보안 정책의 적용은 액세스 권한을 요청하는 사용자를 올바르게 식별하는 데 크게 좌우되며, 이로 인해 ID 관리가 엔터프라이즈 보안의 1차 방어선이 됩니다. 그러나 기존의 비밀번호 기반 인증 솔루션은 일반적으로 '마찰이 많은(high-friction)' 방식으로 간주되므로 사용자가 적시에 대응하는 데 어려움이 있으며 시간이 많이 소모됩니다. 기업은 이제 사용자 생산성을 향상시키는 동시에 책임감 있게 보안 인증을 달성할 수 있는 비밀번호가 없는 인증(Passwordless Authentication) 방식을 광범위하게 고려하고 있습니다.

비밀번호가 없는 인증 기술은 일반적으로 세 가지 범주 중 하나에 해당합니다. 첫 번째는 신체적 특성 (예: 지문, 얼굴, 음성 또는 행동 인식)으로 사용자를 식별하는 생체 인식이고, 두 번째는 하드웨어 및 소프트웨어 키 등의 암호화된 토큰이며, 세 번째는 승인된 기기에서의 사용자 액세스를 허용하는 기기 인증입니다. 하지만 무엇을 사용하든 한 가지 범주의 인증만으로는 최적으로 안전하고 사용자 친화적인 결과를 얻을 수 없다는 사실을 인식하고 있어야 하며, 그렇기 때문에 대부분의 조직은 복수의 접근 방식을 채택합니다. 이러한 점에서 기존의 비밀번호 제어에서 저마찰(low-friction) 솔루션으로의 전환은 하룻밤 사이에 이뤄지지 않으며 장기화되는 경향이 있습니다. 비밀번호가 없는 인증 및 ID 관리 솔루션(싱글 사인온(SSO) 및 비밀번호 볼팅)은 전략적으로 도입해야 비밀번호에 대한 의존도를 체계적으로 줄이는 동시에 최 종 사용자가 겪는 마찰을 최소화할 수 있습니다.

연구 결과에서는 비밀번호가 없는 인증 기술의 도입 절차를 간소화하는 동시에 보안 효율성을 개선하고 관리 노력 및 관련 비용을 절감하는 방법을 명확하게 보여줍니다.

불행히도 보안 인증을 달성하면서 비밀번호가 없는 인증을 활성화하는 최적의 경로를 찾는 것은 IT 및 보안 관리자에게 혼란을 초래하거나 시간이 많이 드는 노력을 요구합니다. 이 의사결정 프로세스를 명확히 파악하기 위해 EMA (Enterprise Management Associates)는 요구사항, 과제 및 가장 효과적인 인증 접근 방식에 대한 1차 설문조사 기반의 연구를 실시했습니다.[1] 연구 결과에서는 비밀번호가 없는 인증 기술의 도입 절차를 간소화하는 동시에 보안 효율성을 개선하고 관리 노력 및 관련 비용을 절감하는 방법을 명확하게 보여줍니다.

1 비밀번호가 없는 인증: 마찰이 적은 ID 관리와 보안 수준이 높은 ID 관리 간의 격차 해소(Passwordless Authentication: Bridging the Gap Between Low-Friction and High-Security Identity Management)

EMA 연구 보고서 개요

조사 방법

EMA는 조직에서 ID 및 액세스 관리 서비스의 관리와 사용에 대해 잘 알고 있는 IT 전문가를 대상으로 1차 설문조사를 실시했습니다. 신뢰도를 보장하기 위해 모든 응답자들은 면밀한 조사를 거쳤으며, 통계 결과는 오차 범위 5% 이내로 계산되었습니다.

설문조사 인구통계

- 응답자 총 200명
- 응답자 중 56.4%는 조직 내 임원급 직책을 맡고 있음
- 응답자는 다양한 업종에 포진해 있으며, 이 중 81%는 하이테크, 제조, 전문 서비스, 의료, 금융, 소매, 교육 부문에 종사하고 있음
- 응답자들은 다양한 규모의 기업에 소속됨
  - ▶ 37.5% - 1,000명 미만의 직원을 보유한 소규모 기업
  - ▶ 39.5% - 1,000~7,500명의 직원을 보유한 중간규모 기업
  - ▶ 23% - 7,500명 이상의 직원을 보유한 대규모 기업
- 응답자 중 96.5%는 북미 지역에 거주함

주요 조사 결과

- 저마찰 인증 솔루션 사용 시 보안 효율성이 개선됩니다.
- 저마찰 인증 솔루션 사용 시 관리 작업 및 관련 비용이 줄어듭니다.
- 대부분의 경우 비밀번호가 없는 인증 기술이 사용자가 겪는 마찰을 최소화하는 것으로 인정받고 있습니다.
- 비밀번호가 없는 인증 기술을 도입하는 데 가장 큰 장애물은 배포 문제인 것으로 확인되었습니다.
- FIDO 및 SAML 같은 ID 표준을 사용하고 고급 ID 관리 기술을 통합하면 배포 문제가 크게 줄어듭니다.

비밀번호 기반 제어의 지속 불가능성

저마찰 인증 솔루션을 도입하는 데 가장 적합한 접근 방식을 결정하기 전에, 기존의 비밀번호 제어 방식에 의존할 때의 가장 큰 문제점과 이 방식이 오늘날의 역동적인 비즈니스 환경에 적합하지 않은 이유를 살펴보는 것이 중요합니다. EMA의 설문조사 결과에 따르면 **조직의 64%는 사용자 식별의 기본 방식으로 계속 비밀번호를 사용하고 있습니다.** 역설적으로 들릴지 모르지만 비밀번호는 실제로 사용자를 식별하는 것이 아니라, 비즈니스 IT 리소스에 액세스할 수 있는 권한을 부여받았는지 여부와 관계없이 특정 문자열을 알고 있는 모든 사용자에게 액세스 권한을 부여합니다. 즉, 악의적인 공격자들이 액세스 권한을 얻기 위한 목적으로 비밀번호를 획득하기 위해 의심스러운 방법을 사용할 기회가 활짝 열려 있다는 의미입니다(예: 무차별 대입 공격, 키스트로크 로깅 및 피싱 사기). 또한 응답자들은 비밀번호에 의존하는 경우 중대한 보안 문제를 초래한다고 답했습니다. **전체적으로 EMA 설문조사 응답자 중 90% 이상이 조직에서 지난 12개월 동안 사용자들이 초래한 중대한 비밀번호 정책 위반을 경험했다고 답했습니다.** 보고 빈도가 높은 항목은 여러 계정에 동일한 비밀번호를 사용하는 경우였습니다(그림 1).

비밀번호가 없는 인증 방식의 도입 가속화

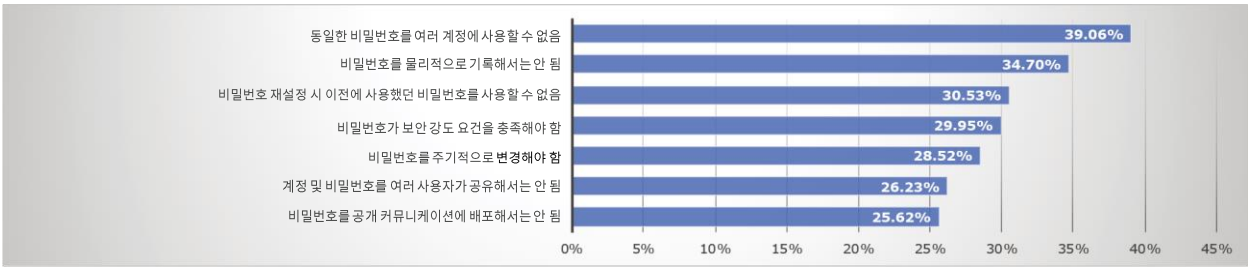


그림 1: 지난 1년 동안 조직에서 발생한 비밀번호 정책 위반에 따른 설문조사 응답자의 비율

비밀번호 관련 정책 위반의 빈도가 높으면 비즈니스와 사용자에게 실질적으로 심각한 결과를 초래합니다. 전체적으로 설문조사 응답자 중 71%는 직원 해고, 멀웨어 감염, 데이터 유출, 규제 준수 불이행, 고객 수의 감소 및 수익 창출에의 직접적인 영향 등의 구체적인 불이익과 액세스 정책 위반을 직접 연관시킬 수 있었습니다(그림 2). 또한 비밀번호에 과도하게 의존하면 관리자의 업무 효율이 저하되고 운영 비용은 증가합니다. EMA는 관리자의 주의가 필요한 것으로 사용자가 보고한 문제의 수가 최종 사용자 측의 마찰 증가와 정비례한다고 판단했습니다. 평균적으로 관리자는 100명당 사용자 액세스 문제를 해결하는 데 매년 약 27시간을 사용합니다. 이러한 관점에서 볼 때 7,500명의 사용자를 지원하는 조직은 일상적인 사용자 액세스 문제 해결을 전담하는 정규직 직원 1명에 상응하는 인력을 고용해야 합니다.

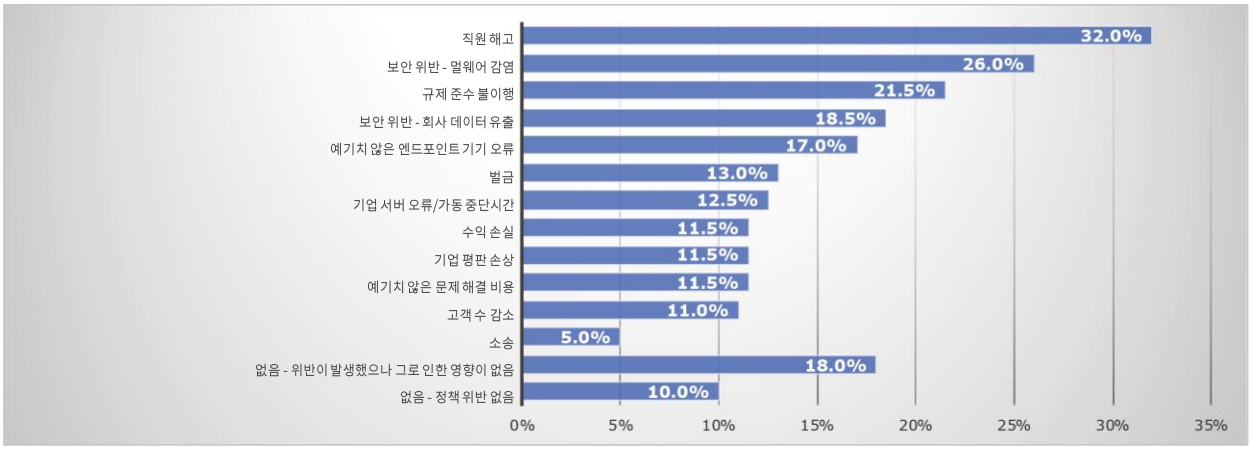


그림 2: 액세스 관리 정책 위반으로 인해 조직에서 발생한 결과에 따른 응답자의 비율

비밀번호가 없는 인증의 주요 이점

EMA의 조사 결과에 따르면 IT 및 보안 전문가들은 비밀번호가 없는 인증을 활용하는 데 따른 이점을 인식하고 있으며, 이들 중 대다수는 비밀번호가 없는 인증이 비밀번호보다 본질적으로 더 안전한 인증 방식으로 인식하고 있습니다(그림 3).

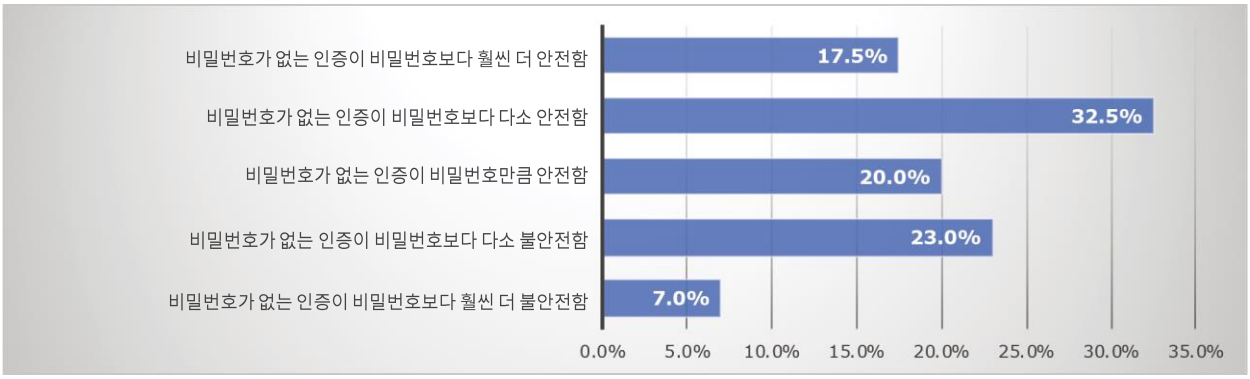


그림 3: 비밀번호가 없는 인증 방식을 통해 제공되는 보안 수준에 대한 인식과 그에 따른 응답자 비율

물론 비밀번호가 없는 인증 솔루션을 가장 쉽게 정량화할 수 있는 가치는 사용자 경험의 개선입니다. 사용자의 노력을 줄이면 직원의 생산성이 향상되고, 비즈니스 민첩성이 높아지며, 사용자의 만족도가 향상되어 소중한 직원을 유지하는 데 도움이 됩니다. 이와 유사하게 비밀번호가 없는 인증을 도입하면 관리자의 노력과 관련 비용을 줄이는 데 엄청난 영향을 미칠 수 있습니다. 전반적으로 EMA 설문조사 응답자들은 생체인식 인증과 하드웨어 토큰이 최종 사용자 생산성 증가에 엄청난 영향을 미쳤다고 답했습니다. 또한 이러한 기술은 최고 수준의 보안을 제공하는 것으로 알려져 있으며, 이는 접근 방식으로 인해 발생한 마찰의 정도와 달성한 보안 효과의 수준 간의 직접적인 상관관계를 나타냅니다.

사용자의 노력을 줄이면 직원의 생산성이 향상되고, 비즈니스 민첩성이 높아지며, 사용자의 만족도가 향상되어 소중한 직원을 유지하는 데 도움이 됩니다.

비밀번호가 없는 인증 방식의 도입 가속화

인증 유형	설명	사용자 생산성 향상	보안 효과
얼굴 인식	얼굴의 고유한 특징과 형태로 사용자를 식별하는 생체 인식 기술	매우 높음	매우 높음
지문	사용자의 엄지 손가락이나 다른 손가락의 마찰 융선을 판독하여 사용자를 식별하는 생체 인식 기술	높음	매우 높음
망막 스캔	인간의 독특한 망막 혈관 분포를 스캔하여 사용자를 식별하는 생체 인식 기술	높음	매우 높음
행동 기반 생체 인식	개인의 고유한 행동 및 버릇을 모니터링하여 사용자를 식별	매우 높음	높음
하드웨어 토큰	자동으로 생성된 암호화 키로 기존의 비밀번호를 대체하는 물리적 기기(예: 전자 열쇠, USB 키 또는 스마트카드)	보통	높음
기기 인증	PC 또는 휴대용 기기와 같은 개인 기기에서 분명하게 식별된 사용자는 재인증 없이 승인된 IT 서비스에 액세스할 수 있도록 허용	낮음(*)	보통(*)
성문	미리 지정한 단어나 구를 말할 때의 고유한 음성 패턴을 분석하여 사용자를 식별하는 생체인식 기술	낮음	보통
일회용 비밀번호	확인된 사용자의 기기 또는 이메일 주소로 단일 로그인 세션에서만 유효한 암호를 제공하여 사용자를 확인	낮음	보통
개인식별번호(PIN)	사용자가 기억하고 있는 짧은 일련 번호(일반적으로 4~6자)로, 프롬프트가 표시되면 입력해야 액세스 가능	낮음	낮음
비밀번호	문자, 숫자, 기호로 구성된 문자열로, 프롬프트가 표시되면 입력해야 액세스 가능	매우 낮음	낮음

** 참고: 기기 인증 방식의 경우, 사용자 생산성 향상 및 보안 효과의 수준은 개인 기기에서 사용자를 처음 인증하는 데 사용되는 솔루션의 유형에 따라 달라집니다. 여기에 제시된 내용은 설문조사 응답자의 평균 결과입니다.*

비밀번호가 없는 인증으로의 여정 탐색

저마찰 인증의 가치에 대한 인식은 높아지고 있지만, 솔루션 배포의 복잡성에 대한 우려가 비밀번호가 없는 인증 방식의 도입을 방해하는 주요 요인으로 고려되고 있습니다. 다시 말해, 많은 조직이 비밀번호가 없는 인증 솔루션을 배포하기가 쉽지 않고 이로 인해 비즈니스 운영에 지장을 줄 것이라고 판단하면서 이를 도입하기를 주저하고 있습니다. 가장 효과적인 솔루션에는 다음과 같은 4가지 원칙을 지원하는 기능이 포함되어 있습니다.

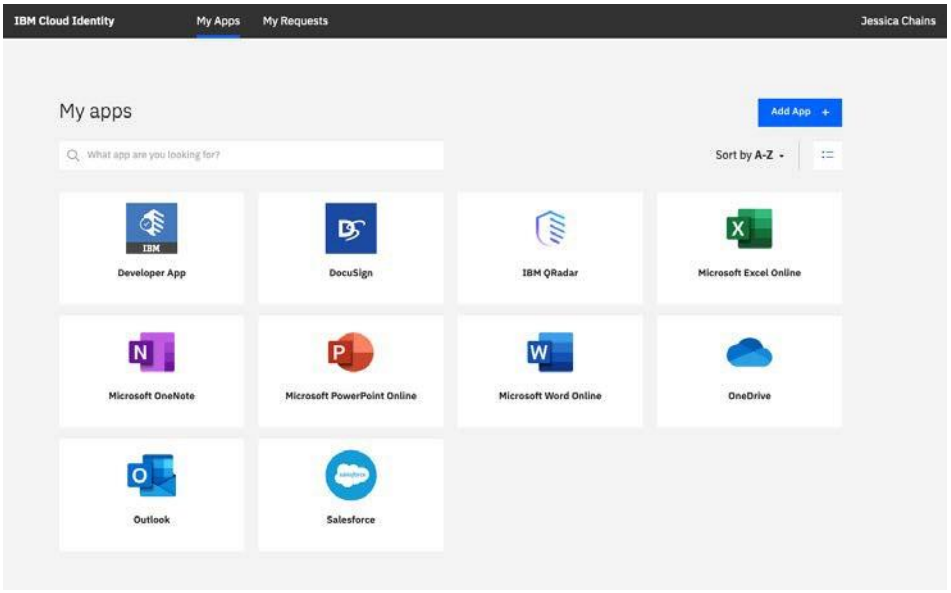
- **직관적** – 솔루션은 도입 절차가 간단하고, 최종 사용자 교육이 거의 또는 전혀 필요하지 않으며, 관리자의 지원 없이도 간편하게 관리할 수 있어야 합니다.

- **정보 제공** – ID 지원 환경 전반에 걸친 가시성을 통해 사용자, 기기, 네트워크 및 호스팅된 서비스의 상황별 데이터를 수집할 수 있어야 합니다. 정보 보고서는 사용자 경험에 대한 잠재적 위험 또는 문제를 쉽게 식별할 수 있도록 이해가 쉽게 작성되어야 합니다.

- **지능적** – 인텔리전스 기술(예: 분석, 머신러닝 및 언어 처리)을 통해 수집된 ID 데이터를 활용하여 액세스 허용과 관련된 위험 수준을 판단해야 합니다. 사용자에게 제공된 인증 요소의 수는 식별된 위험 수준에 따라 동적으로 결정되어야 합니다.

- **통합형** – 솔루션은 FIDO, SAML 및 Open ID Connect 등의 업계 표준을 활용하여 인증 기술과 호스팅 서비스를 통합할 수 있어야 합니다. 서비스, 시스템 및 보안 관리 플랫폼과의 직접적인 통합은 관리 업무를 한층 더 간소화하므로 액세스 정책 관리를 통합하는 데 도움이 됩니다.

비밀번호가 없는 저마찰 인증 기술의 도입 절차를 간소화하도록 설계된 솔루션의 대표적인 예시는 IBM Cloud Identity 플랫폼입니다. 기존의 온프레미스 ID 및 액세스 관리 투자를 활용하도록 설계된 IBM Cloud Identity를 사용하면 모든 엔드포인트 기기와 모든 호스팅된 IT 서비스 간의 액세스를 중앙 집중식으로 관리할 수 있습니다. 이 솔루션은 FIDO 및 SAML 등의 주요 ID 표준과 연동하여 온프레미스 및 클라우드에서 호스팅되는 IT 서비스에 대한 액세스 제어를 쉽게 통합할 수 있습니다. 플랫폼에는 수천 개의 사전 구축된 커넥터가 포함되어 있기 때문에 조직은 가장 효과적인 인증 방법으로 가장 많이 사용되는 SaaS 애플리케이션에 빠르고 쉽게 액세스할 수 있습니다. 이 솔루션은 통합형 엔드포인트 관리 플랫폼인 IBM MaaS360과 직접 통합되어 최종 사용자에게 완벽한 디지털 워크스페이스 경험을 제공하도록 설계되었습니다. IBM Cloud Identity에서 제공하는 단순하고 광범위한 지원을 통해 조직은 사용자의 생산성을 높이고 보안 효율성을 향상시키는 비밀번호가 없는 인증 기술을 책임감 있게 도입할 수 있습니다.



IBM Cloud Identity 대시보드

EMA의 견해

많은 IT 및 보안 전문가들이 보안과 사용자 액세스 요구사항을 정반대의 요소로 간주합니다. 따라서 보안 수준이 높아지면 사용자 액세스에 더 많은 제한이 적용되고, 그 반대의 경우도 마찬가지입니다. 그러나 이러한 두 요구사항이 충돌해야 하는 이유는 없습니다. EMA의 조사 결과에 따르면 인증 프로세스로 인한 마찰의 정도가 감소하면 보안 수준이 정비례하게 증가합니다. 또한 인증 단계를 줄이면 조직에서 관리자가 수행해야 하는 업무량도 그에 비례하여 줄어듭니다. 이러한 점에서 비밀번호가 없는 저마찰 인증 방식은 사용자 및 비즈니스 요구사항을 효과적으로 조정합니다.

안타깝게도 저마찰 인증 방식을 배포하고 유지하기 위해서는 복잡한 기술 도입이 필요할 것이라고 생각하는 조직들이 많습니다. 그러나, 실제로는 기존 ID 기술 투자를 전면 교체할 필요가 없으며, 그 대신 이미 보유하고 있는 리소스를 강화할 수 있어야 합니다. 비밀번호가 없는 인증을 책임감 있게 도입하기에 가장 효과적인 솔루션은 액세스 요청과 관련된 위험 수준에 맞게 문제와 심각도의 규모를 올바르게 판단하여 인증 단계의 수를 체계적으로 줄일 수 있도록 설계된 것입니다. EMA는 보안 강화, 사용자 생산성 향상 및 관리 업무 감축을 실현할 수 있는 비밀번호 없는 인증 기술의 간편한 적용을 위해 IBM Cloud Identity와 같은 ID 관리 솔루션의 도입을 권장합니다.

IBM SECURITY 소개

IBM은 엔터프라이즈 보안 제품 및 서비스에 대한 최첨단 통합 포트폴리오를 제공합니다. 세계적으로 인정받는 IBM X-Force® 연구 팀이 지원하는 이 포트폴리오를 통해 조직은 위험을 효과적으로 관리하고 새로운 위협에 대응할 수 있습니다. IBM은 전 세계에서 가장 광범위한 보안 연구, 개발 및 제공 조직을 운영하고, 130여 개 국가에서 매일 350억 건의 보안 이벤트를 모니터링하며, 3,000개 이상의 보안 특허를 보유하고 있습니다. 자세한 내용을 보려면 www.ibm.com/kr-ko/security를 참조하거나, 트위터에서 @IBMSecurity를 팔로우하거나, IBM Security Intelligence 블로그를 방문하십시오. IBM Cloud Identity에 대해 더 자세히 알아보려면 https://ibm.co/2XOLQsx를 확인하십시오.

Enterprise Management Associates, Inc. 소개

1996년에 설립된 Enterprise Management Associates(EMA)는 모든 영역의 IT와 데이터 관리 기술에 관해 심도 깊은 인사이트를 제공하는 전문적인 분석 기업입니다. EMA 애널리스트들은 실질적인 경험, 업계 최고 사례에 대한 통찰력, 현재 또는 향후 벤더 솔루션에 대한 심도 깊은 지식을 종합적으로 갖춰 고객들의 목표 달성을 지원합니다. EMA 연구, 분석, 비즈니스 사용자, IT 전문가와 IT 벤더를 겨냥한 엔터프라이즈 라인의 컨설팅 서비스에 대한 자세한 정보는 www.enterprisemanagement.com 또는 blog.enterprisemanagement.com에서 확인할 수 있습니다. 또는 트위터, Facebook 또는 LinkedIn에서 EMA를 팔로우하여 최신 소식을 확인할 수 있습니다.

본사:
1995 North 57th Court, Suite 120
Boulder, CO 80301
전화번호: +1 303.543.9500
팩스: +1 303.543.7687
www.enterprisemanagement.com

3868.07222019