

IBM Security Verify : 인공지능과 위협 분석 기반 차세대 계정 및 접근 관리

다양한 아이덴티티 공격에 선제적으로 탐지, 대응 및 관리하세요.

제로 트러스트 아키텍처의 핵심은 바로 아이덴티티에 대한 체계적인 관리와 함께, 디지털 아이덴티티의 신뢰성을 확보하고, 다양한 아이덴티티 위협 기반 공격에 대해 탐지 및 대응하는 것(ITDR)입니다.

ITDR(Identity Threat Detection and Response)이란?

숙련된 기술을 가진 악의적인 공격자는 ID 및 접근 관리(IAM) 인프라에 대해 적극적으로 공격 대상으로 삼고 있으며, 이제 자격 증명 오용이 주요 공격 방법으로 대두되었습니다. 가트너는 ID 시스템을 방어하기 위한 방법을 설명하기 위해 "Identity Threat Detection and Response(ITDR)"이란 용어를 도입했습니다. 기업은 IAM 기능을 개선하는 데 상당한 노력을 기울였지만 그중

상당 부분은 사이버 보안 인프라 강화 측면이 아니라, 사용자 인증을 개선하는 기술에 집중되어 실제로는 공격 표면을 증가시켰습니다. ITDR은 인증 시스템을 보호하고, 공격받았을 때 이를 탐지하고 효과적으로 대응할 수 있습니다.

- Gartner Identifies Top Security and Risk Management Trends for 2022
(March 7, 2022)

아이덴티티 위협 탐지 및 대응이 필요한 이유

99%

분석된 클라우드 보안사고 사례
99%가 클라우드 ID에 과도한 권한 부여

출처: 2022 IBM Security X-Force Cloud Threat Landscape Report

↑ 200%

다크 웹에서 판매한다는
클라우드 계정의 증가

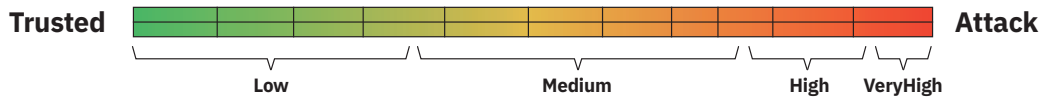
91%

E커머스 로그인 중 평균
Credential Stuffing 공격 숫자

출처: SOCRadar E-Commerce Threat Landscape Report

IBM Security Verify

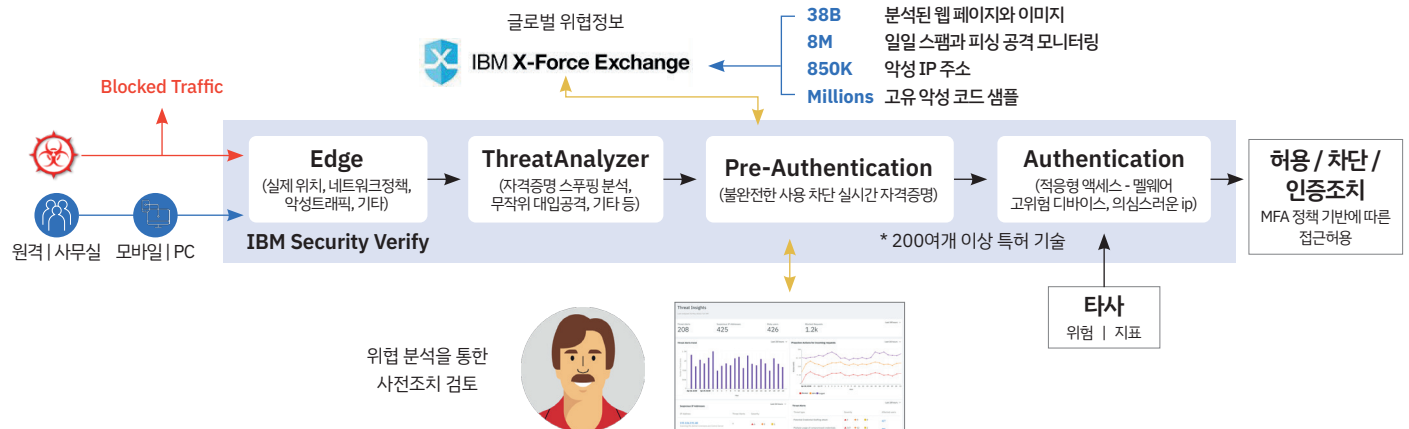
IBM Security Verify는 25년 이상 계정 및 권한 관리 분야에 대한 IBM의 투자와 기술 혁신이 결집된 최첨단 솔루션입니다. IBM의 성숙된 계정 및 권한 관리 기술을 바탕으로 인공지능을 적용하여 아이덴티티 공격을 탐지하고, 사용자의 행위 패턴을 포함하여 디바이스 및 네트워크 정보 등 다각도로 사용자의 신뢰도를 분석함으로써 현재 로그인을 시도하는 디지털 아이덴티티에 대한 위험 정도를 결정하고 트랜잭션 추이에 따라 자동으로 위험도를 조정합니다.



자동 조정된 위험도와 미리 설정된 정책에 따라 능동적으로 대응하며, 접근 요청에 대한 허용과 차단, 그리고 다양한 다중 요소 인증(MFA)을 통해 요청한 사용자임을 확인 및 인증 후라도 재확인합니다. 이때 다중 요소 인증(MFA)으로는 iOS와 안드로이드용으로 제공되는 모바일 Verify 앱을 통한 모바일 OTP, 생체인증, QR인증과 FIDO 등을 기본 제공합니다.



또한, IBM X-Force 연구소의 전 세계 보안 현황 분석을 통해 취합된 위협 인텔리전스 정보를 활용하여 악의적인 사용자임이 명백한 접근은 사전에 차단합니다.



또한, 사용자가 패스워드 설정 혹은 재설정 시, 다크웹 등에 노출된 유출 혹은 취약한 패스워드는 사용하지 못하도록 경고합니다.

Warning Your password was updated. Consider changing your password because it was found on a list of commonly used and/or breached passwords.

<패스워드 설정 시, IBM X-Force Intelligence 정보 확인하여 유출 패스워드 설정 경고 혹은 거부>

아울러, IBM Security Verify로부터 발생된 아이덴티티 위협 알람을 QRadar SIEM/UBA와 같은 통합 관제 플랫폼과의 연계를 통해 전사 관점의 이상 사용자 분석을 수행할 수 있습니다. 혹은 QRadar SOAR와 같은 사고 대응 플랫폼과의 연계를 통해 아이덴티티 위협 정도에 따라 Remediation Group으로 해당 ID의 그룹을 변경하거나, 세션 차단, 계정 잠금 혹은 삭제 등의 보다 적극적인 자동/수동 조치를 취할 수 있습니다. 이를 통해 XDR(Extended Detection and Response)의 보다 완성된 체계를 구축할 수 있습니다.

Permission name	Description	Application	Category
Basic access	Provides access to the application with basic authorization	AWS IAM(Custom)	Default
aws-ec2-spot-fleet-tagging-role	...	AWS IAM(Custom)	AWSIAMRoles
AWSServiceRoleForConfig	...	AWS IAM(Custom)	AWSIAMRoles
AWSServiceRoleForElasticCache	...	AWS IAM(Custom)	AWSIAMRoles
AWSServiceRoleForElasticLoadBalancing	...	AWS IAM(Custom)	AWSIAMRoles
AWSServiceRoleForOrganizations	...	AWS IAM(Custom)	AWSIAMRoles
AWSServiceRoleForRDS	...	AWS IAM(Custom)	AWSIAMRoles
Custom On Prem App	...	AWS IAM(Custom)	AWSIAMRoles
Demo 02	...	AWS IAM(Custom)	AWSIAMRoles
Demo 03	...	AWS IAM(Custom)	AWSIAMRoles
Demo App 01	...	AWS IAM(Custom)	AWSIAMRoles
Demo Native App	...	AWS IAM(Custom)	AWSIAMRoles
Dune Privacy Demo	...	AWS IAM(Custom)	AWSIAMRoles
Google Workspace	...	AWS IAM(Custom)	AWSIAMRoles
IAM_LAB_R1	...	AWS IAM(Custom)	AWSIAMRoles
ISAM_IAM_LAB_R1	...	AWS IAM(Custom)	AWSIAMRoles

<IBM 계정 관리 솔루션에서 사용자 할당 위해 AWS 역할 정보 동기화>

어플리케이션, 데이터베이스, 시스템 등 기존 레거시 인프라에 대한 계정 및 권한 관리 뿐만 아니라, 다

양한 클라우드 및 M365, Salesforce, Workday 등과 같은 SaaS에 이르기까지 전사에서 사용하는 모든 멀티 하이브리드 인프라에 대한 통합 계정 및 권한 관리를 제공합니다. 특히, 기존 레거시에 대한 싱글사인온 방식으로부터 SAML, OIDC, OAuth 등 표준 인증 프로토콜을 지원합니다. 또한, 계정 관리에 있어서도 SCIM 표준을 지원하여, 상기 표준을 지원하는 모든 클라우드와 PaaS, SaaS에 대해 폭넓은 연계를 지원합니다.

Risk Level	Risk Score	Reason	View Details
High	305	James Martin has recently gained an unusual number of entitlements.	View Details
Medium	274	James Martin's entitlements deviate from similar peers.	View Details
Low	104	JamesM account had an alert for misuse of access in last 30 days.	View Details
Very Low	19	JamesM account has no activity since 7 days.	View Details

Recommendation: **Revoke (80% confidence)**

Similar certification requests:

- User: Maria Doss Entitlement: L1 Support Risk Match: 100% Action: Revoke
- User: Olive Diggs Entitlement: L1 Support Risk Match: 100% Action: Revoke
- User: Ronald Attento Entitlement: AD_User Domain Resources Risk Match: 80% Action: Approve

Buttons: Accept, Revoke, Close

<계정/권한 승인 요청 시, IBM AI를 통한 다양한 정보 제공 및 권한 승인/거부에 대한 추천>

인공지능에 의해 사용자의 현재 보유하고 있는 계정과 접근 권한에 대한 분석을 통해 동일 업무의 다른 사용자와의 유사성을 파악하여 위험한 사용자를 식별하며, 계정 및 권한 신청에 대한 승인권자에게 보다 주의 깊게 살펴볼 수 있도록 다양한 정보를 제공하며, 요청에 대한 승인 혹은 거부에 대한 선택을 추천합니다.

IBM Security Verify는

- 기존 인프라 뿐만 아니라, 하이브리드 클라우드에 대해서도 계정/권한 및 접근 관리를 통해 엔터프라이즈 거버넌스 체계를 적용할 수 있도록 도와 줍니다.
- 다양한 인증 표준 적용을 통해 디지털 트랜스포메이션을 가속시키며, 동시에 패스워드리스 및 FIDO 등 최신 인증 기술 도입으로 사용자 경험을 향상시킵니다.
- 인공지능 기술을 통해 다양한 아이덴티티 위협에 대한 보다 적극적인 탐지와 대응을 통해 제로 트러스트를 실현합니다.

