IDG
STRATEGIC
MARKETING SERVICES

IBM

IDG Summary

# “패스워드는 죽었다”

## 진화하는 디지털 인증과 계정 관리 환경

디지털 인증 환경이 빠르게 진화하고 있다. 사용자 경험이 중요해지면서 인증 과정은 더 간편하면서도 보안은 오히려 강화하는 새로운 기술과 제품이 쏟아지고 있다. ‘패스워드는 죽었다’는 파격적인 주장까지 나온다. 차세대 디지털 트러스트를 둘러싼 최신 트렌드와 핵심 기술을 살펴본다. 최근 기업 IT 인프라의 가장 큰 흐름인 클라우드 환경을 중심으로 기존 보안 체계의 한계와 보완 방법도 알아본다. 또한, 주요 은행 등의 실제 사례를 통해 기업을 위한 차세대 디지털 트러스트 구축 방안을 제시한다.

# "패스워드는 죽었다"
# 진화하는 디지털 인증과 계정 관리 환경

**박형근 · 조가원** 실장 | 한국IBM 보안사업부

여기 천재적인 해커가 있다. 다크 웹에서 얻은 정보와 최신 해킹 기술, 다양한 소셜 엔지니어링 공격까지 총동원해 거액이 들어 있는 산탄데르 은행 계좌의 아이디와 비밀번호를 빼내는 데 성공하고, RAT 원격 제어를 통해 SMS 토큰 탈취도 성공했다. 스푸핑을 통해 사용자로 위장하고 은행 웹사이트에 접속해 아이디와 패스워드를 입력해 로그인 완료. 이후 모바일 OTP SMS 토큰 인증을 통해 돈을 송금한다. 이 해커는 과연 원하는 것을 얻을 수 있을까?

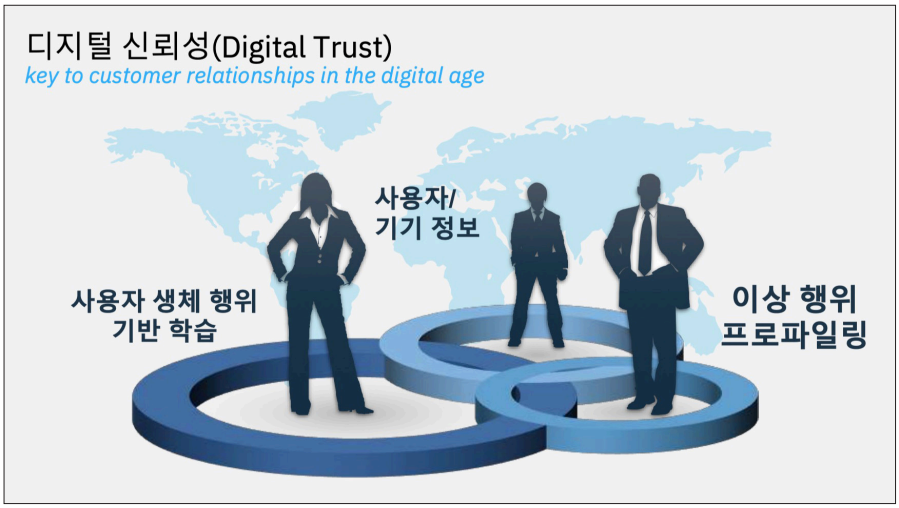
결론부터 말하면 실패할 가능성이 크다. 산탄데르 은행은 사용자의 생체 행위를 학습해 정상 패턴, 이상 패턴, 해커 패턴 등으로 구분해 대응하는 지능적인 보안 시스템을 운영하고 있기 때문이다. 키보드를 입력하는 속도, 마우스를 조작하는 방식 등 사용자의 사용 패턴을 지속적으로 학습해 정상 사용자인지 자동으로 판단한다. 로그인 화면에서 해커는 기존 사용자의 생체 패턴과 일치하지 않고, 정상 사용자와 다르게 원격 제어 등의 이상 트랜잭션을 발생시킨다. 시스템은 이러한 이상 징후를 파악해 다른 유형의 추가 인증 혹은 접속을 제한하는 보호조치를 취하게 된다.

## 디지털 인증 환경이 진화한다

이 사례는 빠르게 발전하고 있는 디지털 인증 환경의 현주소를 잘 보여준다. 디지털 시대의 도래와 더불어 사용자 경험의 중요성이 부각되고 있고, 이를 위해 간편 인증을 비롯해 추가 인증을 최소화하는 위험 기반 차등 인증을 도입하는 기업이 늘어나고 있다. 산탄데르 은행은 사용자 계정이 도용되는 경우에도 고객의 자산을 안전하게 지킬 수 있는 지능화된 인증 보안을 통해 특히나 사용자 경험이 중요해지고 있는 모바일 뱅킹을 비롯한 옴니 채널에 대한 디지털 혁신을 가져올 수 있었다.

디지털 인증 혁신을 통한 사용자 편의성 개선은 오늘날 사용자가 가장 원하는 것이다. iSMG의 〈2018 Digital Identity Trust Survey〉 결과를 보면, 기업 온라인 서비스를 이용하는 '사용자 여정' 중에 로그인(29%), 추가 인증(23%), 회원 가입(19%) 등 대표적인 인증 절차에서 고객이 이탈하는 것으로 확인됐다. 사이트별로 갈수록 복잡하고 긴 비밀번호를 기억하고, 별도의 OTP(One Time Password) 기기를 가지고 다녀야 하며, 번번이 지문이나 홍채 같은 추가 정보를 제공하는 방식은 더는 고객의 환영을 받지 못한다는 사실을 보여준다.

고객 관리의 핵심 요소로 부상하는 디지털 트러스트




'마찰 없는(frictionless)' 사용자 경험 개선을 위한 투자 계획을 수립하는 기업이 96%에 이를 만큼 이미 사용자 경험은 기업의 핵심 과제가 되고 있다.

디지털 인증 혁신에 기반한 사용자 신뢰성 확보는 기업 보안 관점에서도 매우 중요하다. 인증 관리에 실패했을 때 기업이 감수해야 할 피해가 눈덩이처럼 커지고 있기 때문이다. RSA의 〈2018 Fraud Report〉 등에 따르면, 계정 도용으로 인한 피해는 사고 건당 6,600만 달러, 신용카드 사기 피해 금액은 5,700만 달러에 달한다. 악성코드와 바이러스의 피해도 건당 500만 달러로 집계됐다. 결국 기업이 디지털 인증에 대한 신뢰 기반을 갖추지 못하면 고객을 잃는 것은 물론 막대한 금전적 피해까지 볼 수 있다.

## 클라우드 도입으로 인한 인증의 '대혼란'

디지털 인증 혁신은 고객 서비스뿐만 아니라 IT 인프라의 거대한 흐름인 클라우드 전략에 있어서도 의미가 크다. 현재 거의 모든 기업이 클라우드를 도입하거나 도입을 준비 중이다. 초기 단계에서는 비용 절감이 주된 요인으로 거론됐지만, 본격적으로 대두되는 더 중요한 요인은 애자일(agile)이다. 고객의 변화에 맞춰 빠르게 제품과 서비스를 개발하고, 이를 기반으로 유연하고 민첩하게 시장에 반응하기 위해 많은 기업이 클라우드를 도입하고 있다.

클라우드 도입을 위해서는 다양한 영역의 고려사항이 필요하고, 보안 관점에서도 인증을 비롯하여 여러 가지 문제가 발생한다. 기업은 기본적으로 클라우드 서비스 업체가 제공하는 계정관리 기능으로 인증 문제가 해결될 것이라고 기대한다. 그러나 여전히 존재하는 기업 레거시 시스템의 계정을 클라우드 혹은 SaaS 애플리케이션과 연동하고, 직무별 접근 권한을 관리해야 하는 이슈가 발생한다. 인증을 둘러싼 기업 현장의 고민은 단순히 로그인 계정을 관리하는 수준을 넘어선다. 일부 기업과 대학, 공공기관에서 내부 사용자가 업무용 서버를 이용해 비트코인을 채굴하다가 적발된 사례를 보면, SaaS 애플리케이션 혹은 클라우드 리소스가 본 목적에 맞게 사용되고 있는지 검증할 수 있는 가시성의

확보가 필수적이다.

클라우드에서 개인 사용자 계정이 도용되는 것도 물론 위험하지만, 오픈 환경으로 전환된 시스템에서의 관리자 및 임직원 계정이 도용되는 경우 심각한 침해가 발생할 수 있다. 앞서 살펴본 디지털 인증 관리, 즉 디지털 트러스트(Digital Trust) 문제가 점점 중요해지는 것도 이 지점이다. 그렇다고 2중, 3중 인증을 적용하는 것도 무리다. 결국 기업은 계정 권한 관리와 접근 제어 등에서 사용자 경험을 고려한 전략이 필요하다는 것을 깨닫게 되고, 편의성과 신뢰를 동시에 확보하는 방안을 고민하게 된다.

## 암호 대신 신뢰성, 차세대 디지털 트러스트의 조건

그동안 디지털 트러스트 전략은 단계적으로 발전해 왔다. 1990년대 중반 계정 및 비밀번호 관리 등 보안 관점의 인증은 2000년대 들어서 중앙 정책 관리, 권한 카탈로그 관리 등 규제 관점으로 확장됐다. 그리고 이제 사용자 분석을 기반으로 사용자 경험을 해치지 않으면서 안전한 디지털 트러스트를 구축하는 위험 기반 인증 체계로 진화하고 있다.

그렇다면 기업은 클라우드 가속화와 더불어 어떻게 차세대 디지털 트러스트를 구현할 수 있는지 살펴보자. 가장 중요한 핵심은 사용자 경험과 애자일이다. 보안성과 편의성을 동시에 제공하기 위해 사용자에게 더 어려운 패스워드를 강요하는 대신 신뢰성을 검증할 수 있는 인증 프로세스가 필요하다. 자동으로 사용자 정보를 수집하고, 지능적으로 분석해 정교한 통찰력을 확보하도록 지원하는 차세대 디지털 트러스트 플랫폼을 통해 신뢰 인증 프로세스가 가능해진다. 그리고 이러한 인증 프로세스가 클라우드 상에서 유연하게, 빠르게 제공되는 것이 관건이다. 차세대 디지털 트러스트 플랫폼은 크게 3가지 영역에서 기존의 인증 시스템과 차별화된다. 기업의 디지털 인증 담당자가 클라우드 프로젝트를 진행할 때 반드시 고려해야 할 부분이기도 하다.

## 계정 관리, '레거시-클라우드' 하이브리드 구성이 핵심

첫 번째로 계정 관리를 살펴보자. 많은 기업은 일차적으로 레거시의 계정 관리 경험을 SaaS와 클라우드에 적용하고자 한다. 물론 구성 형태에 따라 기존의 계정 관리 방법으로 가능한 경우도 있다. 일부 SaaS 애플리케이션의 경우 표준 기술 기반으로 사용자 정보를 인식하기도 한다. 그러나 AWS를 비롯한 대부분 클라우드와 SaaS 애플리케이션은 계정 권한 관리(IAM-Identity and Access Management) 영역에 대해 사용자가 직접 관리해야 한다. 클라우드의 계정 역시 생성 요청에서부터 관리자 승인에 의한 권한 부여 및 만료 계정 삭제 정책에 이르기까지 기업 계정 관리 프로세스에 의해 이루어져야 한다. 또한 거버넌스 측면에서 관리자가 기업 프로세스에 맞게 사용자를 추가하는지, 개인 목적으로 추가하는지 검증이 안 되는 문제도 해결해야 한다. 기존 레거시 계정 관리 체계를 통해 클라우드 계정을 관리하는 것이 이상적이지만 실제적으로 구현하는 것은 만만한 작업이 아니다.

현재 기업들은 기존 레거시 시스템과 클라우드를 혼용하는 하이브리드 클라우드 전략을 가져가고 있다. 이를 위해서는 기존 환경과 클라우드, SaaS 환경을 동시에 관리할 수 있고, 다양한 배치 옵션을 지원하며 빠르게 적용 가능한 시스템이 필요하다. 현재 시장에 나온 제품 대부분은 레거시 혹은 클라우드 중심으로 집중되어 있는 경우가 많고 SaaS 특화 솔루션의 경우 레거시를 아예 지원하지 않는 제품도 있다. 다양한 형태를 각각 지원하는 것은 물론 필요에 따라 하이브리드 방식으로 사용자를 관리할 수 있는 솔루션을 찾아야 한다. 운영 효율화를 위해 SaaS 방식으로 도입하는 것도 대안이 될 수 있다.

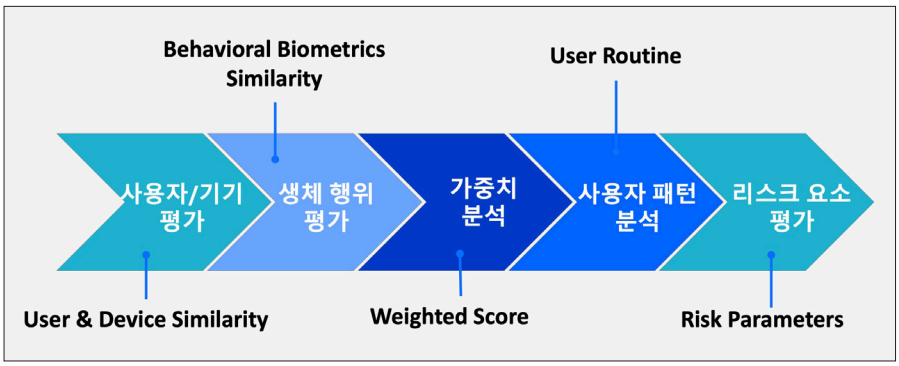
## 사용자 인증, 다양한 신기술과 방법론 기반으로 활발하게 발전 중

두 번째는 사용자 인증이다. 이제 인터넷 공간에서 ID와 패스워드를 사용하는 것 자체가 위험한 일이 돼 버렸다. 마이크로소프트 같은 기업은 '패스워드는 죽었다'고 선언하기도 했다. 그렇다면 해법은 무엇일까. 많은 기업이 다중 인증 체계를 도입하고 있고, 대표적으로 OTP가 현재 범용적으로 사용되고 있다. 사용성도 크게 개선돼 이제는 모바일로 발급 가능하고, 많은 기업이 고객 및 임직원 2차 인증 수단으로 활용하고 있다.

더 미래지향적인 방식으로 확산되고 있는 기술은 위험 기반 인증이다. 사용자 경험을 최대한 보장하는 오픈 시큐리티(Open Security) 관점에서 접근하는 위험 기반 인증은 최근 시장에서 기업 경쟁력 강화를 위해 주목받고 있는 기술이기도 하다. 기본적으로 일반적인 정보성 시스템은 손쉽게 접근할 수 있도록 인증을 최소화하고, 핵심 거래 시 리스크 요소 평가를 통해 위험 수준에 따른 차등 인증을 요구하는 방식이다.

사용자 중심의 위험 기반 인증을 위해서는 산탄데르 은행 사례와 같이 키보드 마우스 등의 입력 패턴 등 고유한 사용자 행위를 학습해 사용자 인증을 수행하는 핵심 기술을 기반으로 다양한 사용자 패턴을 분석해 통합적인 위험 평가를 수행한다. 앞서 언급된 2차 인증에 대해서도 평가된 위험 수준에 따라 메일, 혹은 SMS 형태 등 다른 종류의 2차 인증이 제시되는 지능적인 차등 인증 전략이 필요하다. 예를 들어, 원격 제어 툴에 감염된 모바일 사용자에게 SMS 인증 전송은 아무런 효력이 없다. 이와 같이 위험 기반 인증은 사용자의 편의성을 극대화

위험 기반 인증(Risk Based Authentication) 개념도



하면서 동시에 보안을 강화하는 차세대 디지털 트러스트 구현의 중요 요소이다.

## 싱글사인온, 다양한 구성 지원을 통한 애자일

클라우드의 디지털 트러스트를 고민할 때 살펴봐야 할 마지막 세 번째는 인증 단일화, 싱글사인온(Single Sign On)이다. 싱글사인온은 다양한 시스템을 사용하는 기업 전사 환경 관리에서 필수적인 요건이며, 클라우드와 다양한 SaaS 애플리케이션이 확장하면서 사용자 편의성 측면에서 중요성이 더욱 커지고 있다.

클라우드 상에서 싱글사인온을 구현하는 데 있어 이슈는 2가지다. 먼저 다양한 클라우드 SaaS 환경에 대한 민첩한 지원이다. 현재 많은 기업이 하이브리드 클라우드 전략과 더불어 가용성 등의 이슈로 멀티 클라우드 전략을 고려하고 있다. 또한 기업이 선택과 집중을 통한 더 빠른 시장 전략을 위해 오피스는 물론, CRM, 급여 등 다양한 전문 SaaS 애플리케이션을 지속적으로 도입하고 있다. 그러나 많게는 수십 개에 달하는 SaaS 애플리케이션을 연동하고, 해당 애플리케이션이 업데이트될 때마다 수정하는 것은 IT 인력이 충분한 대기업이라고 해도 쉽지 않다. 싱글사인온에서 얼마나 다양한 애플리케이션 커넥터를 제공하느냐가 클라우드 도입을 위한 전체 구축 일정에 큰 영향을 미치게 된다.

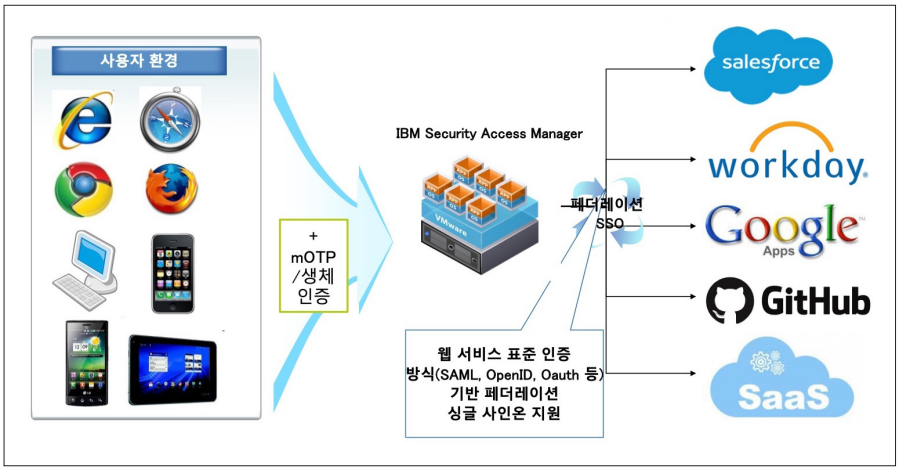
싱글사인온을 둘러싼 또 다른 이슈는 다양한 이해 관계자를 동시에 지원할 수 있는지다. 일반적으로 기업의 인증 시스템은 다양한 관점으로 기능 요건이 다르게 정의되는 경우가 많다. 사용자 유형의 관점에서 볼 때 임직원, 협력사, 고객 등으로 구분될 수 있다. 예를 들어 고객은 소셜 로그인 등을 이용해 기업이 ID 정보를 관리하지 않고 연동 처리하는 경우가 있지만, 임직원 계정은 기업 인사 DB를 통해 직접 관리해야 한다. 또한 부서, 혹은 그룹사의 구분에 따라서 별도의 구분된 관리체계 구성이 필요한 경우도 많다. 이렇듯 다양한 구성과 멀티 테넌시 요건을 지원해야 별도 구축에 소요되는 비용 낭비를 막고, 기업 거버넌스를 충족할 수 있다.

## IBM 솔루션, 레거시 전문성과 클라우드의 결합

IBM은 기업이 사용자 경험을 해치지 않으면서 레거시와 클라우드를 포괄하는 강력한 인증 체계를 구축할 수 있도록 IBM Cloud Identity, Security Access Manager, Trusteer 솔루션 등을 기반으로 한 차세대 디지털 트러스트 플랫폼을 공급하고 있다. 번거롭고 도용 가능한 인증 수단을 넘어서 신뢰할 수 있는 프로세스와 플랫폼을 제공하는 데 초점을 맞추고 있다.

IBM의 가장 큰 장점은 다양한 클라우드, SaaS 업체와의 파트너십이다. 기업이 기존 레거시 경쟁력을 유지하면서도 다양한 클라우드 솔루션을 함께 사용할 수 있도록 지원한다. 실제로 마이크로소프트의 오피스 365와 쉐어포인트 온라인, 야머, 세일즈포스, 워크데이, 깃허브, 젠데스크 등 360여 개 SaaS 애플리케이션에 대해 커넥터를 미리 개발해 지원한다. 특히 IBM은 전통적인 인프라를 비롯해 클라우드 서비스에 이르기까지 다양한 기업 IT 환경을 지원하는 파트너로서 클라우드에서 어떻게 기업 솔루션을 구축, 배포할 것인지 끊임없이 고민하

IBM Security Access Manager Enterprise Edition 솔루션 개요




며 다른 업체와 차별화된 강력한 기술력과 경험을 확보하고 있다.

IBM 제품은 차세대 디지털 트러스트의 3가지 요건도 충실하게 지원하고 있다. 먼저 계정 및 권한 관리에서 사용자의 다양한 요구사항과 여건에 따라 물리 어플라이언스와 가상화, 클라우드, SaaS 등 다양한 방식으로 시스템을 구축할 수 있다. 현재 하이브리드 방식으로 사용자 계정 및 권한 관리를 지원하는 것은 IBM이 유일하다.

사용자 인증 관련해서는 위험 기반 인증(Risk Based Authentication)을 지원한다. 머신러닝과 인공지능 등 다양한 특허 기술을 활용해 정상 사용자와 악성 사용자의 행위를 학습해 실시간으로 안전한 인증 환경을 제공한다. 시장조사 업체 포레스터의 북미 기업 대상 리서치 결과, IBM Trusteer 도입을 통해 사기 대응 비용을 90% 절감한 것으로 나타났다. 현재 산탄데르 은행을 비롯해 600여 개 이상 기업이 IBM 솔루션을 사용하고 있다.

마지막으로 싱글사인온 영역에서도 멀티 테넌트 지원을 통해 직원부터 협력사는 물론 고객까지 다양한 요건에 대해 동시에 사용할 수 있도록 지원한다. 이를 통해 중복 투자를 줄이면서 보안 시스템을 이용하는 사용자에 맞춰 필요한 정책을 유연하게 적용할 수 있다.

## 클라우드 시대의 디지털 트러스트 구축 가이드

최근 국내에서도 클라우드 도입이 가속화되면서 디지털 트러스트에 대한 기업의 고민이 늘고 있다. 애자일한 시장 전략을 위해 6개월을 목표로 클라우드로 주요 기능을 이전하는데, 레거시와 클라우드, 신규 SaaS 애플리케이션 통합 인증 구축을 위해 1년이 걸리는 웃지 못할 상황이 벌어질 수도 있다. 이렇게 되면 더는 비용의 문제가 아니다. 애초 클라우드로 전환하려 했던 목표, 즉 민첩성이라는 근본 명제부터 흔들리게 되고, 미래 성장 잠재력까지 의심되는 난감한 상황에 이르게 된다.

기업이 이러한 위험을 최소화하려면 무엇보다 프로젝트 초기부터 보안에 대한 고려가 수반돼야 한다. 초기 클라우드 도입 계획 단계에서 많은 기업이 핵심

업무 설계에 주력하다 보면 계정 및 권한 관리를 비롯한 보안 요건에 공백이 발생할 가능성이 크다. 현업은 막연히 클라우드 업체가 모든 것을 처리해 줄 것으로 기대하지만 실제 클라우드 보안은 책임 공유 모델을 기반으로 서비스 제공자의 책임은 인프라에 한정되는 경우가 대부분이다. 이런 보안의 공백은 작게는 부서 간 불협화음, 크게는 클라우드 도입의 실패로 이어질 수 있다. 대표적으로 해외 대형 은행의 경우, 보안 요건에 대한 합의가 이루어지지 않아 1차 도입이 무산된 사례가 있다. 클라우드 서비스에서 제공되는 기능에 대한 명확한 이해를 기반으로 기업의 보안 거버넌스에 대한 매핑과 보완 전략의 수립이 필요하다.

그다음은 기업 최적화된 아키텍처와 구축 전략을 수립해야 한다. 기술적인 구현 가능성, 비용, 컴플라이언스 등의 고려사항을 기반으로 운영 아키텍처를 면밀히 검토해야 한다. 막연히 '클라우드 적용 가능합니다'가 아니라 구체적인 아키텍처와 해당 세부 구성안이 도출돼야 한다. 하이브리드 환경에서 레거시와 클라우드 중 어디에 서버를 배치하고, 어떻게 데이터 동기화하는지 등의 세부 구성에 따라 비용이 크게 차이 날 수도 있다. 실제적인 구성안 검토를 통한 최적 아키텍처를 통해 투자대비효과(ROI)를 높여야 한다.

## 사용자 경험과 인텔리전스로 완성하는 '최고의 보안' 디지털 트러스트

오늘날의 보안 환경은 과거 그 어느 때보다 정교하고 지능적인 해법을 요구하고 있다. 레거시와 클라우드라는 다양한 인프라에 걸쳐 매끄럽게 작동하는 것은 기본이고, 편리한 사용자 경험도 제공해야 한다. 또한 안전한 보안 환경을 위해 실시간으로 변화하는 위협 트렌드에 빠르게 대응할 수 있는 자동화된 인텔리전스가 핵심적으로 필요하다. 그러면서도 비용의 절감을 기대할 수 있다면 이것이 최고의 보안이 아닐까.

고객의 눈에 '보이지는 않지만'(불편하게 만들지는 않지만), '안전하게 보호받고 있음'을 느낄 수 있도록(실제로 보호) 하는 조용한 보안이야말로, 디지털 시대에 차세대 디지털 트러스트가 고객에게 제공할 수 있는 진정한 가치다.