백서

2020년 11월

Zero Trust 시작하기

아무 것도 믿지 말고 항상 확인하라

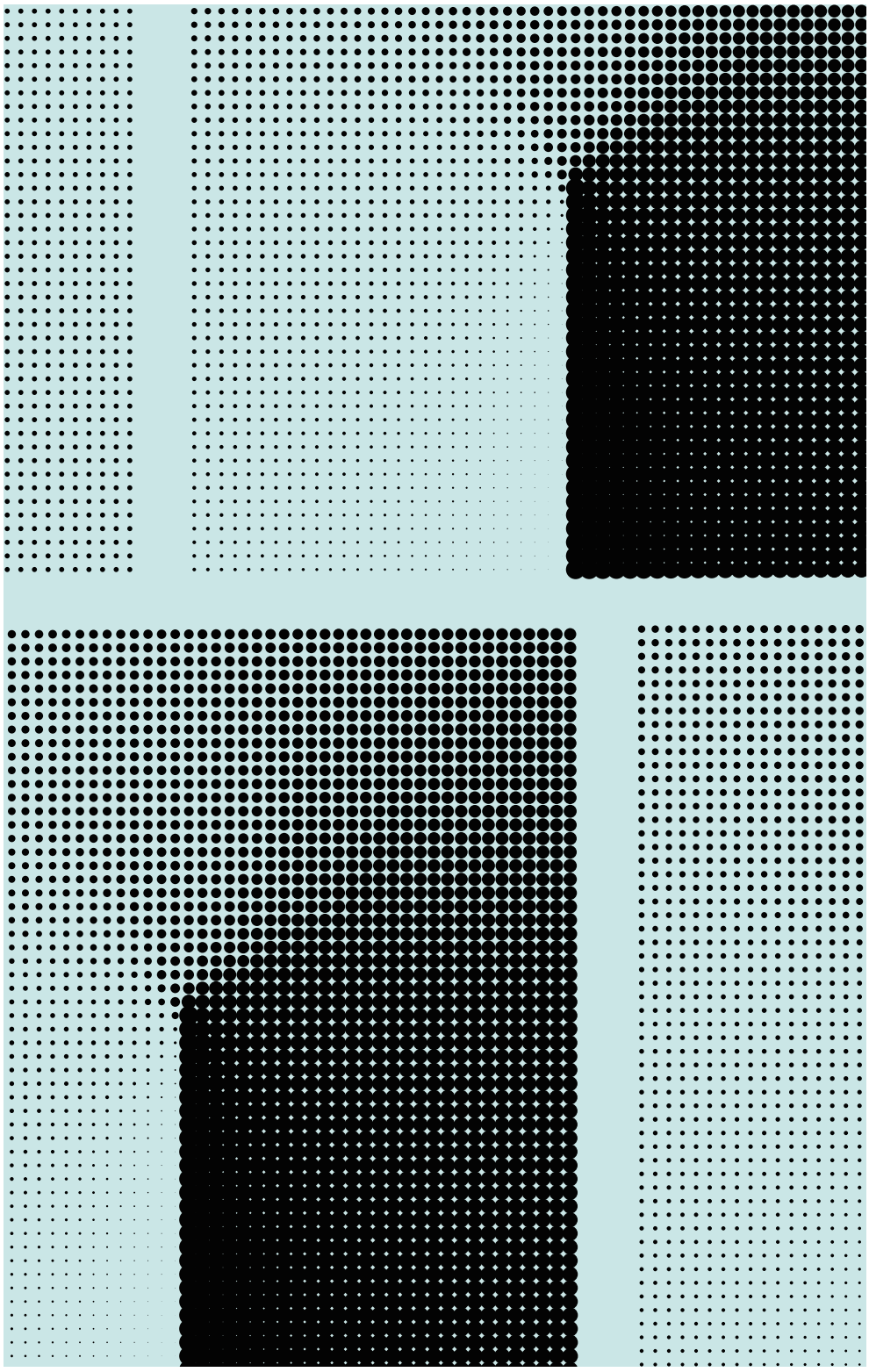
Okta Inc.

서울 강남구 테헤란로 152

강남파이낸스센터 41층

support.okta.com

050-6626-1877



okta

목차

개요

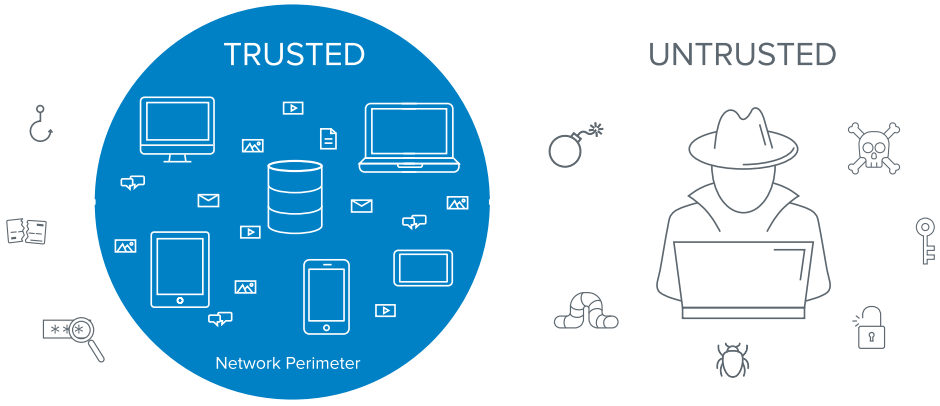
Zero Trust 보안은 내부 네트워크는 “신뢰할 수 있고”, 외부 네트워크는 “신뢰할 수 없다”는 개념을 타파합니다. 모바일과 클라우드가 도입되면서 이제는 보안을 네트워크 경계의 중심에서 생각할 수 없게 되었습니다. 오히려 위치나 디바이스 또는 네트워크와 관계없이 다양한 사용자(직원, 파트너, 계약자 등)가 안전하게 액세스할 수 있는 환경이 필요합니다. Zero Trust 보안 아키텍처를 쉽게 구축할 수 있는 묘책은 없지만 기업이 Zero Trust 여정을 시작하는 데 IAM(Identity and Access Management)이 핵심 테크놀로지인 것만은 틀림없습니다.

본 백서에서는 Zero Trust 개발로 이어지는 보안 환경의 변화와 오늘날 ZTX(Zero Trust Extended Ecosystem) 프레임워크의 모습, 그리고 기업이 현재는 물론이고 미래에도 Okta를 Zero Trust 프로그램의 성공을 위한 토대로 활용하는 방법에 대해 알아봅니다.

과제: 데이터를 보호하는 방화벽이 사라진다면

종래의 보안 아키텍처는 조직 내에서 무엇이든 액세스할 수 있는 신뢰할 수 있는 개인과 그렇지 않은 개인의 두 가지 집단을 염두에 두고 설계되었습니다. 보안 팀과 IT 팀은 두 그룹 사이에 방화벽을 설치하여 네트워크 경계를 안전하게 보호하는 방어 시스템에 투자했습니다. 잠재적 위협을 차단하는 방화벽을 설치하여 기업의 에코시스템을 안전하게 보호하는 데는 성공했지만 이렇게 완전한 신뢰 모델에도 문제는 있습니다. 보안 경계가 뚫리면 공격자가 기업 내부에서 권한이 있는 인트라넷을 통해 비교적 쉽게 어디든지 액세스할 수 있기 때문입니다. 악의를 가진 내부자가 보안 경계를 침입하지 않고도 막대한 피해를 입히는 것은 말할 것도 없습니다.

“성과 해자(Castle and Moat)” 방식의 기업 보호 접근법



오늘날 모바일 및 클라우드 테크놀로지 도입의 확산으로 안전한 기업 네트워크가 아닌 외부에서 업무를 처리하는 경우가 많아지면서 네트워크 경계를 적용하기가 갈수록 어려워지고 있습니다. 이러한 환경에서는 기업의 중요한 자산을 보호하는 방화벽은 존재하지 않습니다. 직원부터 계약자, 파트너, 공급업체에 이르기까지 모두가 종래의 경계를 벗어나서 데이터에 액세스하기 때문입니다.

클라우드 및 모바일 환경에서는 많은 사람들이 그 어느 때보다 다양한 장소에서 각종 디바이스를 사용해 갖가지 리소스와 데이터에 액세스합니다. 하지만 전체 에코시스템에 피해를 입히는 사람은 악의적 행위자, 단 한 명입니다. 결과적으로 기업은 IT 스택을 구성하는 어느 요소에서도 더 이상 신뢰를 단정하지 못합니다.

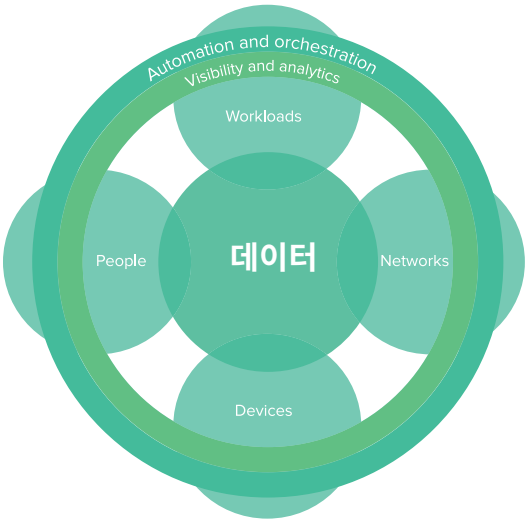
차세대 프론티어: 진화하는 Zero Trust

이러한 보안 환경의 변화는 결국 Zero Trust의 개발로 이어지고 있습니다. Zero Trust는 Forrester Research 애널리스트인 존 킨더박(John Kindervag)이 2009년에 개발한 보안 프레임워크로, 내부 네트워크는 신뢰할 수 있고 외부 네트워크는 신뢰할 수 없다는 개념을 타파합니다. 킨더박은 모든 네트워크 트래픽을 신뢰할 수 없는 것으로 간주해야 한다고 주장했습니다. 초기 프레임워크에서 네트워크 경계 개편에 초점을 맞춰 기업이 네트워크 세그먼테이션 게이트웨이를 통해 모든 네트워크 트래픽을 실시간으로 검사해야 한다고 권장했습니다. 특히 Zero Trust를 구성하는 세 가지 주요 원칙은 이렇습니다. 1) 모든 리소스는 위치에 관계없이 안전한 액세스가 보장되어야 합니다. 2) 액세스 제어는 알 필요에 따라 엄격하게 적용됩니다. 3) 기업은 모든 트래픽을 검사하고 기록하여 사용자가 적법한 일을 하고 있는지 확인해야 합니다.

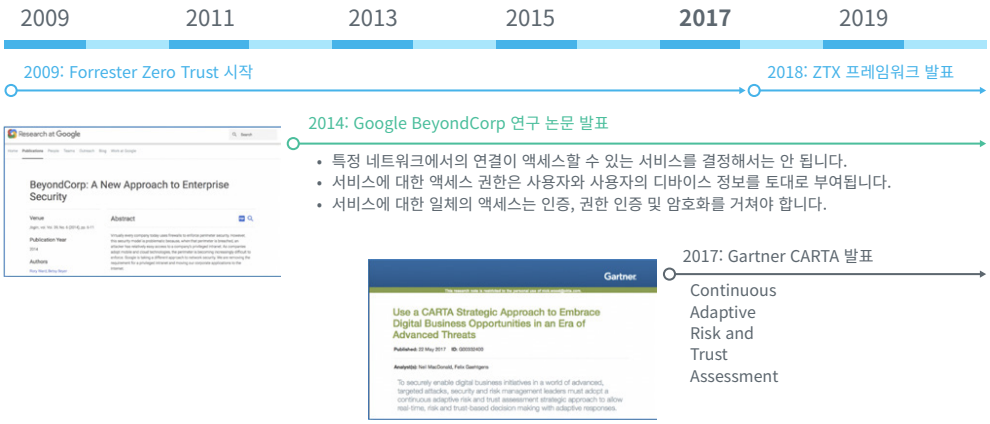
2009년 이후 클라우드와 모바일의 확산으로 킨더박이 창안한 Zero Trust 모델은 빠른 발전을 이루었습니다. Gartner는 2017 CARTA 프레임워크[1]에서 잠재적 위협까지 식별하려면 게이트웨이는 물론이고 사용자 환경 곳곳에서 적응형 위험 기반 평가를 통한 인증 및 액세스 권한 인증이 끊임없이 필요함을 거듭 강조하여 킨더박의 Zero Trust 프레임워크를 상기시켰습니다. Google이 2014년에 발표한 BeyondCorp 연구 논문[2]은 오늘날 대규모로 구현된 Zero Trust의 본보기가 되고 있습니다.

또한 Forrester의 애널리스트인 체이스 컨닝햄(Chase Cunningham)이 주도하여 발전시킨 Zero Trust 프레임워크인 ZTX(Zero Trust Extended Ecosystem)도 이러한 네트워크 분할을 넘어서는 변화를 강조하고 있습니다. 이러한 발전 과정에서 Zero Trust는 '차세대 방화벽'를 넘어서 '차세대 액세스'로 바뀌면서 보안 모델에서 인적 요소의 중요성을 강조하여 네트워크와 데이터에 액세스하는 사람에 대한 명령과 제어를 성공의 열쇠로 주목하고 있습니다. Forrester 팀은 SSO(Single Sign-On)와 같은 테크놀로지를 중요한 기능으로 꼽으면서 다중 요소 인증(MFA) 테크놀로지가 "액세스 위협을 크게 줄일 것"이라고 강조했습니다.[3]

[1] Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, Gartner, Inc., 2017년 5월 22일
[2] BeyondCorp: A New Approach to Enterprise Security, Google, 2014
[3] The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc., 2018년 1월 19일



보안 모델이 발전하는 과정에서도 이러한 Zero Trust의 핵심 개념은 바뀌지 않았습니다. 다시 말해서 오늘날 보안 환경에서 중요한 것은 네트워크가 아니라 시스템에 액세스하는 사람이며, 이들의 액세스를 제어하는 것입니다. 바로 여기에서 아이덴티티와 Okta가 적용됩니다.

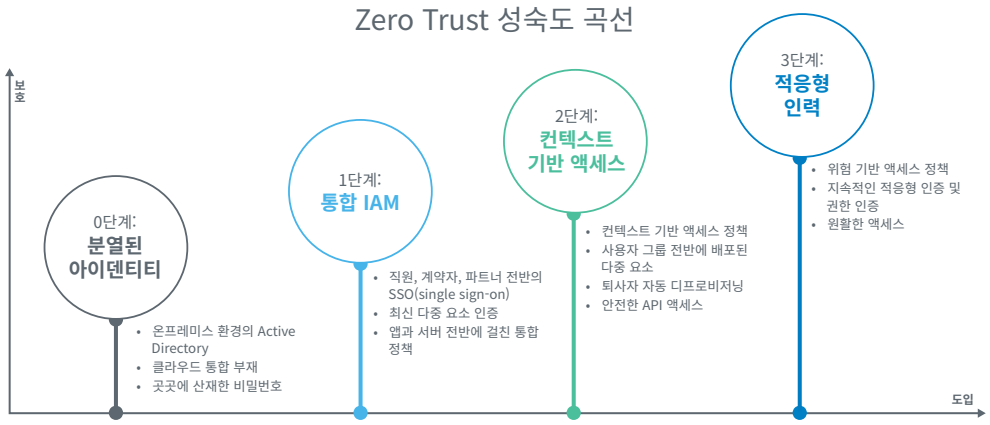


Forrester 역시 최근에 새로운 Zero Trust 연구 보고서[4]를 발표하여 액세스 권한의 중요성을 강조하면서 Okta를 Zero Trust 보안 시장의 선두 기업으로 선정했습니다. The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018이라는 제목의 이 보고서에서는 다수의 벤더를 평가하고 있는데, 여기서 Okta는 "사람/인력 보안", "ZTX 비전 및 전략", "시장 접근 방식"의 세 가지 평가 항목에서 최고점을 받았습니다. Forrest는 보고서에서 다음과 같이 논평합니다. "'시스템'과 '인프라'에 대한 기존 개념이 모두 사라지면서 유형을 막론하고 아이덴티티의 중요성이 그 어느 때보다 커졌습니다." Forrester는 이러한 아이덴티티의 중요성을 고려하여 아이덴티티를 "Zero Trust의 핵심 영역"으로 평가하고 있습니다.[5]

[4] Future-Proof Your Digital Business With Zero Trust Security, Forrester Research Inc., 2018년 3월 28일
[5] The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

Zero Trust의 토대를 이루는 아이덴티티

짧게 얘기하자면 Zero Trust의 핵심 원칙은 “아무 것도 믿지 말고 항상 확인하라”입니다. 다시 말해서 적합한 사용자가 적정 수준의 권한을 갖고 해당 컨텍스트에서 필요한 리소스에 액세스할 수 있어야 하며, 이러한 액세스가 지속적으로 평가되어야 합니다. 또한 이러한 과정에서 사용자에게 불편이 가중되어서는 안 됩니다. 이러한 Zero Trust 구현은 하룻밤 만에 이루어지지 않습니다. 기업이 Zero Trust 아키텍처를 구현할 때 다음과 같이 몇 개의 인프라 성숙도 단계를 거치게 됩니다.



0단계: 분열된 아이덴티티

기업들은 다양한 온프레미스 및 클라우드 애플리케이션으로 Zero Trust 여정을 시작하려고 하지만 이러한 애플리케이션은 Active Directory와 같은 온프레미스 디렉터리에 통합되지 않은 경우가 대부분입니다. 결과적으로 IT 팀은 다수의 시스템에서, 그리고 IT 팀도 모르게 사용되는 여러 애플리케이션과 서비스에서 서로 다른 아이덴티티를 관리할 수밖에 없습니다. 사용자 입장에서는 비밀번호가 너무 많아져서 위험성이 높아지는 셈입니다. 이렇게 분열된 아이덴티티에 대한 가시성과 소유권의 부재로 IT 팀과 보안 팀은 공격자가 개별 시스템에 액세스할 수 있는 잠재적 위험을 안게 됩니다.

1단계: 통합 IAM(Identity and Access Management)

분열된 아이덴티티로 인해 발생하는 보안 공백을 해결하려면 먼저 온프레미스 환경과 클라우드 환경에서 단일 IAM 시스템으로 통합해야 합니다. SSO(Single Sign-On)을 통한 1단계 통합은 액세스 관리에 반드시 필요한 것으로, 그 대상을 고객으로 한정해서는 안 되며 오히려 직원, 계약자, 파트너 등 완전히 확장된 형태의 기업을 포함해 서비스에 액세스해야 하는 모든 사용자에게 적용해야 합니다. 2차 인증 요소를 중앙의 아이덴티티 액세스 포인트까지 계층화하면 자격증명을 겨냥한 공격을 완화하는 데 도움이 됩니다. 또한 애플리케이션을 비롯해 IT 인프라의 핵심인 서버까지 액세스 정책을 통합하는 것은 IAM을 안전하고 관리가 가능한 IT 환경으로 단일화하는 데 매우 중요합니다.

현재 수천 개의 기업들이 Okta SSO를 사용해 사용자 아이덴티티를 통합하고 있습니다. Okta Universal Directory와 Okta SSO를 함께 사용하는 경우도 많습니다. Okta Universal Directory는 클라우드 기반의 디렉터리 서비스로, IT 팀이 신뢰할 수 있는 단일 데이터 소스 역할을 할 뿐만 아니라 다수의 AD 및 기타 온프레미스 디렉터리 서비스에 대한 통합 지점의 역할을 합니다. Okta SSO는 IT 팀이 손쉽게 확장 기업을 관리 및 보호할 수 있도록 지원하는 동시에 비밀번호가 늘어나 사용자에게 불편을 초래하는 상황을 방지합니다. IT 팀은 Okta Advanced Server Access를 통해 동일한 액세스 제어를 서버 계층으로 확장하여 관리가 필요한 온프레미스 및 클라우드 리소스까지 액세스를 안전하게 관리할 수 있습니다.

2단계: 컨텍스트 기반 액세스

IT 팀이 IAM을 통합했다면 이제 Zero Trust 보안의 다음 단계로, 컨텍스트 기반의 액세스 정책을 계층화해야 합니다. 컨텍스트 기반이란 사용자의 컨텍스트(사용자가 누구인가? 사용자가 위험군에 속하는가?), 애플리케이션 컨텍스트(사용자가 어떤 애플리케이션에 액세스하려고 하는가?), 디바이스 컨텍스트, 위치 및 네트워크에 대한 여러 가지 신호를 수집한 후 해당 정보에 따라 액세스 정책을 적용하는 것을 말합니다. 예를 들어 기업 네트워크에서 로그인하는 관리형 디바이스에는 원활한 액세스를 허용하고, 새로운 위치에서 로그인하는 비관리형 디바이스에는 MFA를 요구하도록 정책을 설정할 수 있습니다. 또한 인증 시도 횟수에 따라 사용자 그룹에 다중 요소를 적용하여 인증을 강화할 수도 있습니다. 그 밖에 스마트폰이 없는 저위험 사용자에게는 일회용 비밀번호를 제공하거나, 혹은 고위험 공격 대상은 암호화된 핸드쉐이크를 사용하는 하드 토큰으로 안전하게 인증하여 서비스를 이용하도록 설정할 수도 있습니다. 나아가 사용자가 퇴사하거나 업무를 변경할 경우 자동 프로비저닝을 통해 해당 업무에 필요한 툴에만 액세스할 수 있도록 제한하는 것도 가능합니다(혹은 퇴사 시 모든 액세스를 자동으로 취소하여 퇴사 후 사용자가 없는 계정이나 휴면 계정의 위험을 줄일 수 있습니다) 마지막으로 이러한 다각적 액세스 제어는 기업 인력이 사용하는 모든 테크놀로지로 확장되어야 합니다. 예를 들어 최신 애플리케이션의 빌딩 블록이지만 중요한 데이터를 웹에 노출시킬 수 있는 API에 대한 액세스도 보호할 수 있어야 합니다.

오늘날 다수의 기업들이 Okea Adaptive MFA에서 컨텍스트 기반의 액세스 관리 기능 세트를 이미 이용하고 있습니다. Okta 정책 프레임워크는 사용자, 디바이스, 위치, 네트워크, 그리고 리소스에 액세스하는 애플리케이션이나 브라우저에 대한 컨텍스트 기반의 다양한 인사이트를 처리하여 컨텍스트에 기반한 응답을 제공할 수 있습니다. 이러한 응답은 기업의 위험 허용 한도를 바탕으로 기업을 안전하게 보호하는 첫 번째 방어선으로 작용합니다. 예를 들어 사용자가 기업 네트워크에서 일반 기업 노트북을 사용해 인증을 시도할 경우 기업은 사용자에게 비밀번호 입력만 요구하는 정책을 설정할 수 있습니다. 하지만 외국에서 기업 노트북을 사용해 공용 와이파이 네트워크로 인증을 시도한다면 비밀번호와 2차 인증 요소를 모두 요구할 수도 있습니다. 이러한 컨텍스트 기반 액세스는 위험에 노출될 수 있는 인증 시도에 한해 2차 인증 요소를 요구하기 때문에 사용자는 물론이고 IT/보안 팀에게도 유용합니다.

컨텍스트 기반 액세스 관리

3단계: 적응형 인력

Zero Trust 구현을 위한 마지막 단계는 인증 및 액세스 권한 인증의 확대 적용입니다. 인증은 이제 게이트웨이에서만 수행되는 것이 아닙니다. 잠재적 위협을 식별하기 위해 사용자 경험 곳곳에서 적응형 위험 기반 평가를 통해 끊임없이 수행되고 있습니다. 3단계는 지능형 위험 기반 엔진을 2단계의 컨텍스트 기반 응답에 추가하는 것처럼 보이지만 이전 단계에서 설정한 여러 가지 정책을 능가합니다. 이제 IT 팀은 위험 허용 한도를 설정한 후 컨텍스트 기반 신호에 따라 위험 수준을 점수로 평가하여 특정 인증 이벤트에 대한 위험도를 측정하고 해당 인사이트를 근거로 2차 인증 요소를 요구할 수 있습니다. 하지만 이러한 신뢰도 절대적이지 않기 때문에 적응형 인증을 지속적으로 모니터링하여 신호가 바뀌었는지 확인하고, 사용자 컨텍스트 요소가 하나라도 바뀌었다면 인증 및 권한 인증을 다시 요구해야 합니다. 마지막으로 지능형 위험 기반 액세스 제어를 통해 보안이 강화되는 반면 최종 사용자 경험은 궁극적으로 간소화됩니다. 중단 없는 액세스 외에도 IT 팀이 정책을 설정하는 경우에 한해 비밀번호가 필요 없는 인증도 가능하기 때문입니다.

Okta는 관리자가 다양한 정책을 사용하여 최종 사용자 인증 경험을 개선할 수 있도록 지원하고 있습니다. 여기에는 인증 흐름에서 비밀번호를 완전히 배제하는 정책도 포함됩니다. 비밀번호를 기본 인증 요소로서 다른 요소(Okta Verify, YubiKey 등)로 대체하여 IT 관리자에게 선택의 폭을 넓혀줄 수 있습니다. 또한 위험 기반 인증 정책을 설정하여 다양한 입력 신호를 중심으로 위험 허용 한도에 따라 단계별 인증을 요구할 수도 있습니다. 그 밖에 사용자 신원을 확신할 수 있는 경우에는 비밀번호가 아닌 다른 1차 요소만 요구합니다.

Okta는 컨텍스트 기반 신호 데이터를 통합하여 강력한 정책 기반 접근 방식을 따르는 동시에 앞으로도 정책 엔진 인텔리전스를 끊임없이 개선하여 실천하는 기업의 모습을 보여줄 것입니다. 오늘날 대부분의 기업들이 Zero Trust 성숙도 곡선의 초기 단계에 머물러 있습니다. 하지만 기업이 아무 것도 믿지 않고 항상 확인하는 접근 방식을 IT 보안 환경에 계속 도입함에 따라, Okta는 보다 강력하고 손쉬운 액세스 관리 기능을 추가로 지원하고 있습니다.

더욱 광범위한 보안 에코시스템을 향한 Zero Trust 확장

Okta는 아이덴티티를 Zero Trust의 토대로 제공하는 것을 넘어 다양한 보안 솔루션에 긴밀히 통합하여 Zero Trust에 대한 접근 방식을 단일화합니다. Okta Integration Network를 통해 심층 통합에 투자하여 다음과 같이 확장된 Zero Trust 에코시스템의 모든 구성요소에서 심층 통합을 유지하고 있습니다.

netskope	McAfee Together is power.	데이터 보안에 적합
paloalto NETWORKS	cisco	네트워크 보안에 적합
vmware	Carbon Black.	디바이스 보안에 적합
CYBERARK	BOMGAR	워크로드 보안에 적합
splunk>	IBM Radar	분석에 적합
servicenow	splunk>	오케스트레이션에 적합

위에 보이는 것처럼 광범위한 통합 카테고리를 바탕으로 Okta Identity Cloud의 특징이라고 할 수 있는 동급 최고의 벤더 중립 접근 방식을 지원합니다.

기업 리소스에 대한 액세스를 지능적으로 제어하여 행동학적 모니터링의 발판으로 삼는다고 해도 특히 무엇이 아닌 누가와 관련된 문제라면 근본 원인을 규명하기 어렵습니다. Okta는 보안 분석 및 SIEM 통합을 통해 기업이 Okta의 풍부한 아이덴티티 컨텍스트와 사용자 활동을 활용하는 동시에 문제가 발생한 계정에 대한 복구 조치를 이행할 수 있도록 지원합니다. 또한 Netskope나 McAfee와 같은 CASB와 통합하여 기업에게 상세한 가시성을 제공하고, 인증 세션에서 위험한 이벤트가 발견되면 지속적으로 검사하도록 경고합니다. Okta는 SIEM 파트너들과 마찬가지로 비정상 이벤트를 효과적으로 탐지할 수 있도록 귀중한 인증 데이터를 제공하고 CASB 서비스에서 응답 메시지를 다시 수신합니다. 이렇게 수신되는 응답 메시지를 근거로 아이덴티티 계층에서 액세스를 취소할 수 있습니다. Okta Integration Network는 이 외에도 다양한 방식으로 기업에게 Zero Trust를 구현하고 있습니다.

사례 연구: 21st Century Fox

케이블, 방송, 영화, 유료 TV, 위성 자산 등에서 세계 최고의 포트폴리오를 자랑하는 21st Century Fox에게 보안은 늘 큰 고민거리였습니다. 매일 약 50개 언어로 18억 명 이상의 구독자에게 콘텐츠를 제공하고 있는 21st Century Fox는 영화 및 TV 제작 스튜디오를 포함해 케이블/방송 네트워크 및 자산으로 이루어진 전 세계 포트폴리오의 본고장입니다. 이 회사는 몇 년 전 또 다른 주요 스튜디오에서 보안 공격을 당하면서 보안 목적을 강화하기 위한 작업에 돌입했습니다.

1단계: Zero Trust 시작하기

21st Century Fox는 방화벽에서부터 안티바이러스 소프트웨어에 이르기까지 일반적으로 사용되는 경계 기반 보안 솔루션을 모두 갖추고 있었습니다. 21st Century Fox의 CISO인 멜로디 힐데브란트(Melody Hildebrandt)가 IT 팀에게 처음으로 맡긴 프로젝트 중 하나는 내부 Fox 사용자를 모두 동일한 환경으로 통합하는 것이었습니다. 여기에는 인증을 강화하고, 어떤 사용자가 어떤 애플리케이션에 대한 액세스를 요청하고 있는지 더욱 쉽게 파악하며, 아이덴티티 관리 프로세스를 간소화하는 작업이 포함되었습니다. 힐더브란트는 중요한 아이덴티티 및 액세스 인프라를 통합한 후 새로운 Zero Trust 아키텍처를 설계하기 시작했습니다. 이 아키텍처는 오늘날 헤드라인을 장식하는 여러 데이터 유출 사고의 원인인 자격증명 도용과 피싱 공격을 막는 데 큰 역할을 했습니다. 이 과정에서 Fox 네트워크를 지원하는 직원과 계약자 및 파트너들의 사용자 경험은 아무런 영향도 받지 않았습니다.

2단계: 21st Century Fox의 확장 기업 범위에 대한 컨텍스트 기반의 동적 액세스 도입

21st Century Fox는 Okta Identity Cloud를 사용해 자사의 직원에게는 Okta의 인력 아이덴티티 제품을, 파트너와 계약자 에코시스템에게는 Okta API 제품을 지원하는 등 다양한 인력에게 Zero Trust 접근 방식을 적용했습니다. 회사는 이미 Okta SSO, Universal Directory, Lifecycle Management를 사용하고 있었지만 여기에 더해 Adaptive MFA와 API Access Management까지 추가하기로 결정했습니다.

힐데브란트의 팀은 핵심 인프라를 구축한 후 동적 액세스 모델로 전환하게 되었고, 이러한 이유로 Okta Lifecycle Management와 Universal Directory를 구현했습니다. 이제 Fox의 HR 시스템인 Workday에서 사용자의 상태가 바뀌면 UD가 사용자의 속성을 확인하여 해당하는 그룹으로 분류합니다. 그런 다음 Lifecycle Management가 사용자의 업무에 필요한 툴과 액세스 수준을 프로비저닝합니다.

결과적으로 사용자가 1일차부터 필요한 모든 것을 얻을 수 있으며, 누군가가 제한된 정보에 우발적으로 액세스하게 될 위험이 없습니다. 나아가 자격증명이 도용되더라도 다른 사람이 중요한 데이터나 콘텐츠에 액세스 할 위험이 줄어들게 됩니다. 즉, 21st Century Fox 직원이 퇴사하거나 파트너와 계약이 종료되면 디프로비저닝 절차가 거의 동시에 이루어지는 것입니다. Universal Directory에서 해당 계정이 디프로비저닝되는 즉시 액세스가 취소되므로 “사용자가 없는 계정”이 발생할 일이 없기 때문입니다. 또한 회사는 Adaptive MFA를 통해 사용자 신원, 사용하는 디바이스의 유형, 업무 장소, 액세스를 요청하는 애플리케이션 등 다양한 요인을 토대로 스마트 인증을 결정할 수 있습니다. 따라서 인증 절차 과정에서 직원들이 불필요한 단계를 거치지 않고 높은 수준의 보안을 유지할 수 있습니다. 21st Century Fox는

> Okta는 Zero Trust 모델의 성숙도를 높일 수 있는 초석이 되어주었습니다. 아이덴티티 수준에서 도움을 받은 덕분에 우리는 사용자 신원을 확인하는 데 필요했던 대부분의 제어 기능을 도입할 수 있었습니다. 결과적으로 Zero Trust에 대한 계획을 앞당기는 계기가 되었습니다.
>
> 멜로디 힐더브란트(Melody Hildebrandt),
> 21st Century Fox의 CISO

Adaptive MFA를 배포한 후 직원과 파트너의 피드백에 귀를 귀울였고, Okta Verify, YubiKey, Okta Verify with Push, Voice, SMS, U2F USB 토큰 등 최대한 많은 인증 요소 옵션을 제공했습니다.

21st Century Fox의 Zero Trust 구현: 보안 + 사용 용이성

21st Century Fox가 소비자에게 쉽고 안전하게 콘텐츠를 제공할 수 있다는 것만으로도 궁극적인 성공 여부를 알 수 있습니다. 대표적인 예로, 이 회사가 인도 소비자에게 제공하고 있는 모바일 애플리케이션인 Hot Star를 들 수 있습니다. 이 애플리케이션은 최근 실시간 동시 시청자 수가 700만 명을 넘어섰습니다. 힐더브란트는 “DDoS 또는 잠재적 자격증명 스터핑 공격으로부터 보호하면서 인도의 모바일 사용자들에게 최초로 크리켓 콘텐츠를 전송하는 등 2년도 채 되지 않아 시청자 수를 이 정도로 늘린 것은 정말 엄청난 성과입니다.”라고 강조했습니다.

21st Century Fox 직원들과 파트너는 이제 Okta 덕분에 외부 위협에 대한 걱정 없이 자신이 가장 잘 하는 일, 즉 재미 있는 콘텐츠를 자사의 고객에게 전송하는 데 집중할 수 있게 되었습니다. 이제 근본적으로 커다란 보안 격차를 줄이는 동시에 사용자와 IT 팀에게 미치는 복잡성까지 최소화할 수 있게 되었습니다. 이로써 Fox 시청자들은 앞으로 많은 것을 기대해도 좋을 것입니다. 콘텐츠가 나날이 좋아질 것이기 때문이죠.

Okta와 Zero Trust의 향후 행보

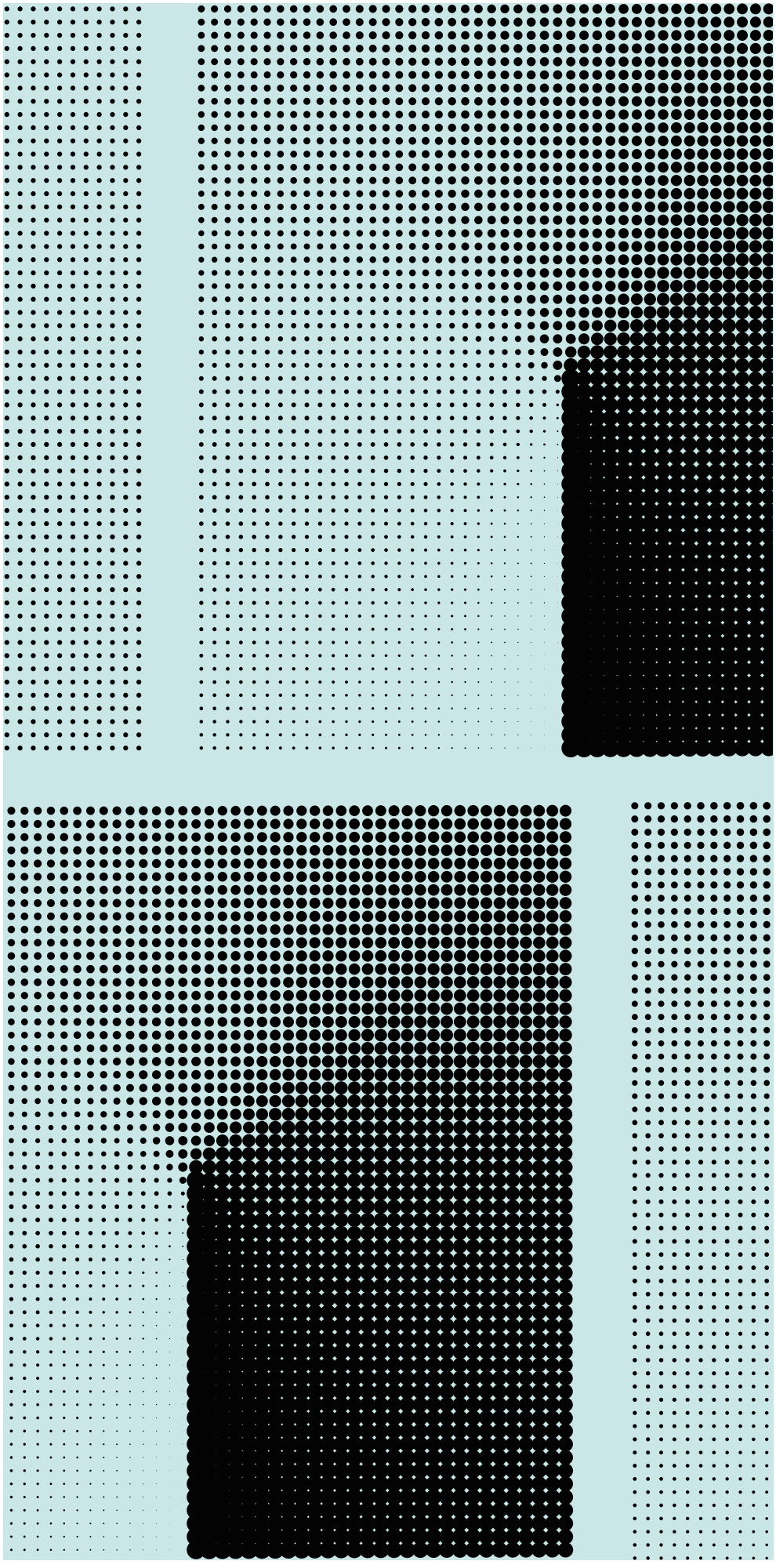
Zero Trust를 쉽게 달성할 수 있는 묘책은 없습니다. 일부 테크놀로지 벤더들은 그렇지 않다고 얘기하지만 기업들은 유연성과 생산성을 모두 높일 수 있는 최고의 테크놀로지를 원하기 마련입니다. 오늘날 기업들이 자신의 Zero Trust 여정을 시작하면서 아이덴티티와 Okta에 기대를 거는 이유도 바로 이 때문입니다. Okta Identity Cloud를 차세대 액세스 전략의 핵심으로 활용하여 해당 권한을 가진 사용자만이 원하는 정보에 적시에 액세스할 수 있도록 보장하기 때문입니다. 아무 것도 믿지 말고 항상 확인하십시오.

최신 액세스 관리

Okta는 이 여정의 모든 단계에서 기업을 지원하기 위해 지속적으로 투자하고 있습니다. 추가 업데이트가 플랫폼에 배포될 예정이므로 okta의 기업 및 보안 블로그(**okta.com/blog** 및 **www.okta.com/ security-blog/**)를 눈여겨봐 주시기 바랍니다 .

Okta 소개

Okta는 기업 아이덴티티 분야의 독자적인 선두 기업입니다. Okta Identity Cloud는 기업들이 사람과 테크놀로지를 적시에 안전하게 연결할 수 있도록 지원합니다. 6,500개 이상의 애플리케이션 통합을 바탕으로 Okta의 고객들은 자신의 비즈니스에 가장 적합한 테크놀로지를 손쉽고 안전하게 사용할 수 있습니다. 자세한 내용은 **okta.com**을 참조하십시오.



okta