



Cisco Zero Trust

판데믹 시대의 새로운 기원

인성경보

2021년 4

Defense



13

14

15

16



13

14

15

16

Zero Trust Model

FORRESTER®

Revolutionize Your Security With Forrester's Zero Trust Model

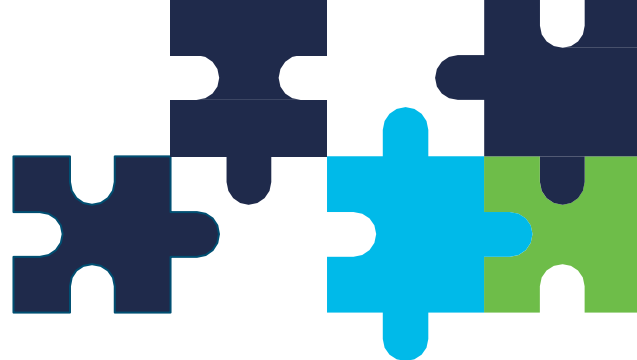
Get business buy-in and keep hackers out

We live in an era of unprecedented cyber risk, made worse by archaic systems, dissonant silos, and a dizzying array of new security tech.

The struggle is real for today's security leaders, but that's where Zero Trust comes in. It's a strategy and framework designed to consolidate costs and build protection into every single layer of your ecosystem.



제로 트러스트 접근 방식의 차이점



전통적인 접근 방식

신뢰는 액세스 요청이 수신되는 네트워크 위치를 기반으로 합니다.



공격자가 네트워크 내에서 측면으로 이동하여 왕관 보석으로 이동할 수 있습니다.

보안을 새 경계까지 확장하지 않습니다.

제로 트러스트 접근 방식 : 절대 암시적으로 신뢰하지 않음, Always Verify

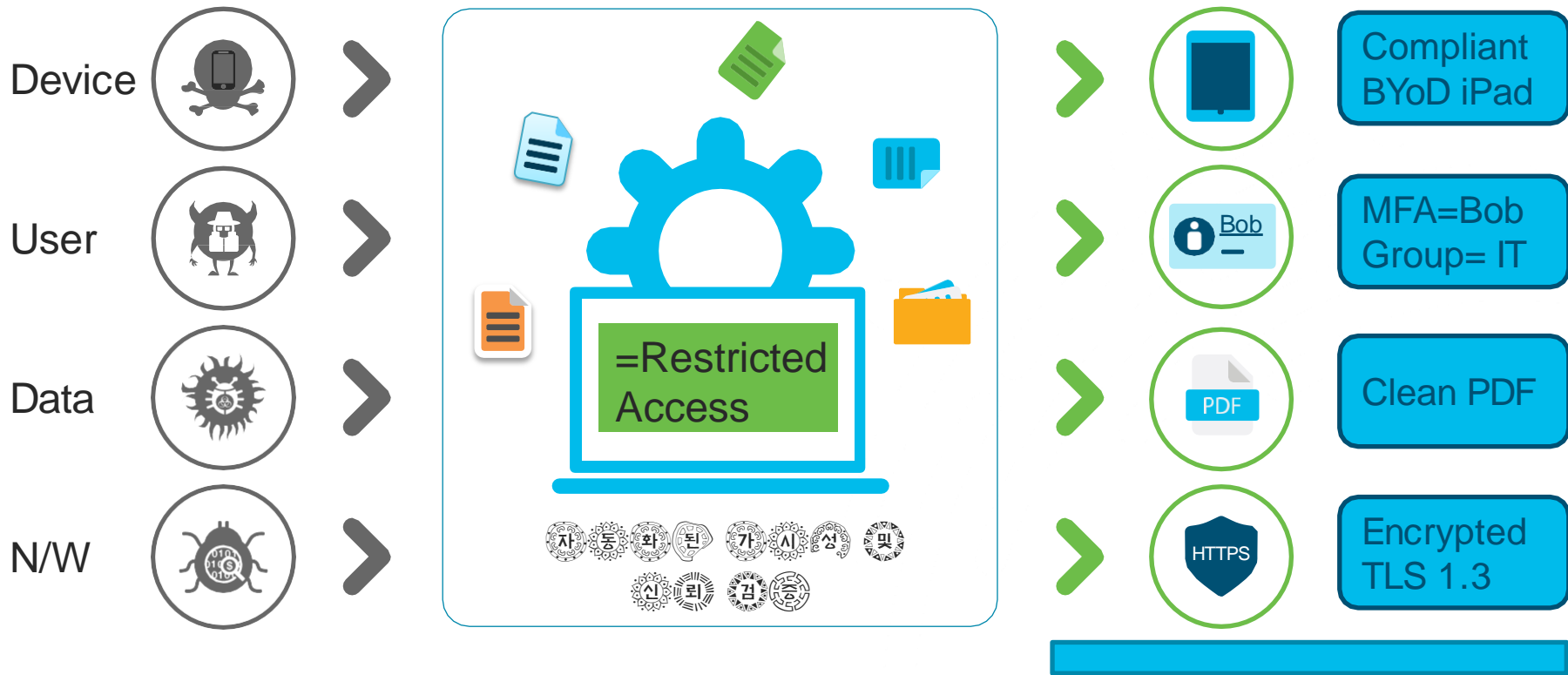
모든 액세스 요청에 대해 요청이 수신되는 위치에 관계없이 신뢰가 설정됩니다.



응용프로그램 및 네트워크에서 액세스를 보호합니다. 올바른 사용자 및 장치만 액세스할 수 있도록 보장합니다.

BYOD, 클라우드 애플리케이션, 하이브리드 환경 등을 통해 현대 기업을 지원하기 위한 신뢰도를 높입니다.

Zero Trust : 다 른 방 법 스 루 트 입 장 일 때 까 지 악 의 적 인 것 스 루 트 가 정



Cisco Zero Trust

모든 사용자, 장치 및 위치에 서
프로그램 및 환경 진척에 대한 액세스
스스로 보호하는 부신뢰 접근 방식입니다.

Workforce

올바른 사용자와
보안 장치만
애플리케이션에
액세스할 수 있는지
확인합니다.



Workplace

IoT를 포함한 네트워크의
모든 사용자 및 장치에
올바른 접근을
확인합니다.



Enforce Policy-Based Controls

Cisco Zero Trust

신원, 워크로드 및 작업상에 대한 액세스를 모호하게 포괄적인 접근 방식을 입니다.

Shift in IT landscape

Users, devices and apps are everywhere



Remote users,
contractors and
third-parties



Personal and
mobile devices



IoT Devices



Evolving
perimeter



Cloud appli
cations



Hybrid infra
structure



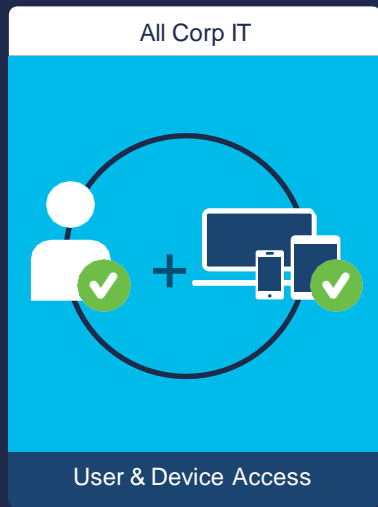
Cloud infras
tructure



Securing Access

가 시 성 을 확 보 하 고 인 전 한 액 세 스 를 보 장 하 는 방 법 은 무 엇 입 니 까 ?

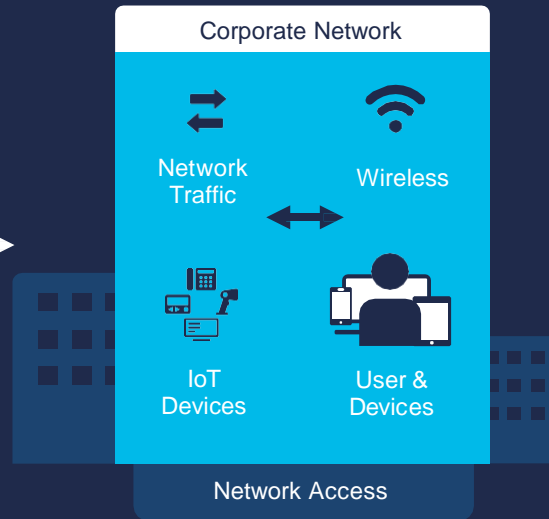
Workforce



Workload



Workplace



Workforce – DUO



Multi-Factor Authentication (MFA)



How it works:



A user logs in using primary authentication (**something they know** = username + password).

Duo prompts the user with secondary authentication (**something they have** = push notification sent via Duo Mobile app on their smartphone).

Establish Trust

- ✓ ID 기반 공격을 방지합니다.
- ✓ 도난당하거나 손상된 암호를 사용하는 공격자를 무력화합니다.
- ✓ 애플리케이션에 대해 제로 트러스트 액세스를 제공합니다.
- ✓ 암호에만 의한 의존도를 감소.



Workload - Tetration

The background is a solid green color. Overlaid on this are several white, semi-transparent decorative elements. These include several thick, curved lines that sweep across the frame from the bottom left towards the top right. Additionally, there are several white circles of varying sizes scattered across the background, some appearing to be part of the curved lines or as separate elements.



Cisco Zero Trust for the Workload

How to Establish Trust with Tetration



Establish Trust

Visibility and
behavior modeling

WITH

Application discovery and
dependency maps

All Processes, cmds, files,
users and network comms



Enforce
Trust-Based
Access

Per workload,
micro-segmentation policy

WITH

Automated, context-based,
segmentation policy

Consistent policy:
Any workload, Anywhere



Continuous
Trust
Verification

Real-time security
health of workloads

BY

Security visibility and
health score

Vulnerability, anomaly,
forensic and threat data



Cisco Zero Trust for the Workload

Workload – Continuous Trust Verification

Use Cases

How Cisco helps:

What is the real-time security health of my workload environments?



Tetration Security Dashboard



I need to defend my workloads from attacks



Tetration Forensics rules
Automate segmentation rules based on threat/risk data



How can I leverage my other security tools to protect my workloads?



Tetration integration with SD-Access/ISE, CTR, NGFW, StealthWatch, etc.



Log and Audit Everything

The background is a solid orange color with several faint, light-orange decorative elements. These include several curved, brush-stroke-like lines that sweep across the right side of the frame, and a few small, semi-transparent circles scattered in the upper right quadrant.

Workplace – SD-Access



Cisco Zero Trust for the Workplace

How to Establish Trust with SD-Access & ISE



Establish Trust

Discover and
classify devices

WITH

IoT device profiling BYOD
lifecycle management
User device Posture



Enforce
Trust-Based
Access

Context-based network
access control policy for
users and things

WITH

Dynamic precise policies
Group-based (SGT)



Continuous
Trust
Verification

Continuous security
health monitoring of
devices

BY

Continuous Posture
Vulnerability assessments
Indications of compromise

Network Segmentation: Policy

With ISE Segmentation policy enforced the way you actually intended through dynamic Group-Based Policy.	Segmentation Policy	Internet	ERM	Ordering	DevOps
	Visitor	Permit	Deny	Deny	Deny
	Human Resources	Permit	Permit	Deny	Deny
	Sales	Permit	Deny	Permit	Deny
	R&D	Permit	Deny	Deny	Permit

With Trust-Based Access, you can:

- 장치 분류 및 액세스 요구에 따라 네트워크 권한 부여 정책 적용
- 무선, 유선 및 VPN 연결 전반에 걸쳐 분할 정책 적용
- 정책 관리자를 통해 ISE를 통한 세분화 관리
- 네트워크 장치에 동적으로 정책 배포
- 그룹 기반 정책으로 세분화 간소화



Cisco Zero Trust for the Workplace

How to Establish Trust with SD-Access & ISE

Use Cases

How Cisco helps:

What is, and has been, on my network?



SDA, ISE, DNAC, AAA, Profiling, Context visibility



How do I establish trust for users and things



Threat-Centric NAC, MDM for posture



I need to easily apply group-based access control to every user and device on my network



Network Analytics and Contextual Group-Based Policy



Log and Audit Everything



Cisco Zero Trust Portfolio Depth

+ Enhance & Extend Trust

Umbrella

AMP

Meraki

AnyConnect

SD- WAN

Email Security

Next-Generation Firewall

ACI

+ Detect & Respond

Cisco Threat Response (CTR)

Stealthwatch



감사합니다.