cisco

cisco zero Trust

팬데믹 시대의 새로운 기준

인성정보

2021 4

Defense

Zero Trust Model

FORRESTER

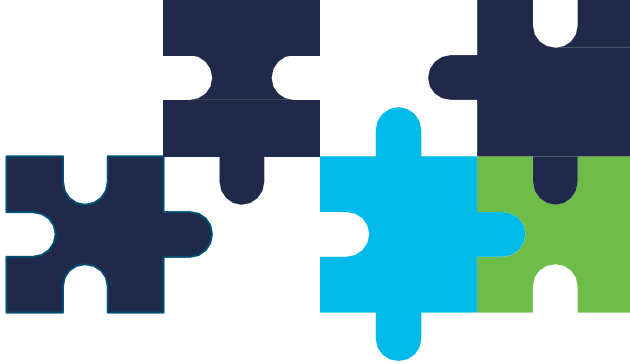
Revolutionize Your Security With Forrester's Zero Trust Model

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.

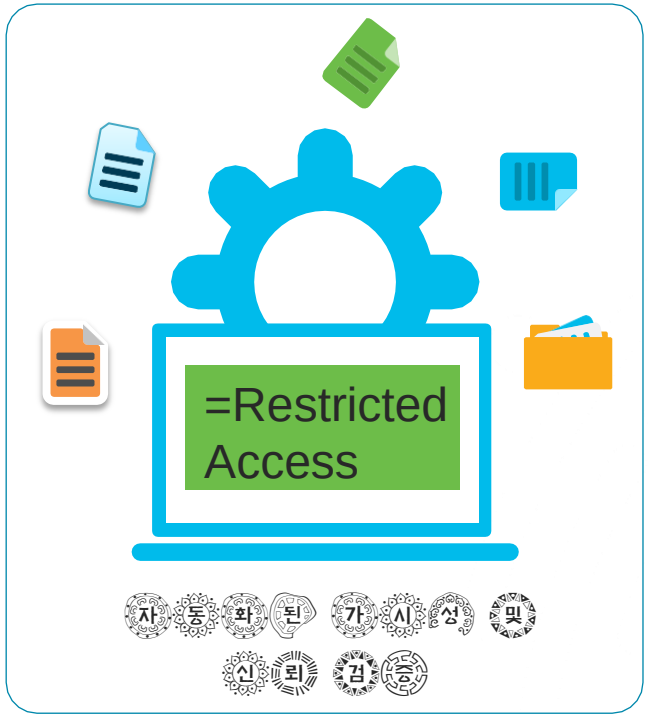
Zero Trust : 다른 방법으로 입증될 때까지 악의적인 것으로 가정

Device

User

Data

N/W



Compliant BYoD iPad

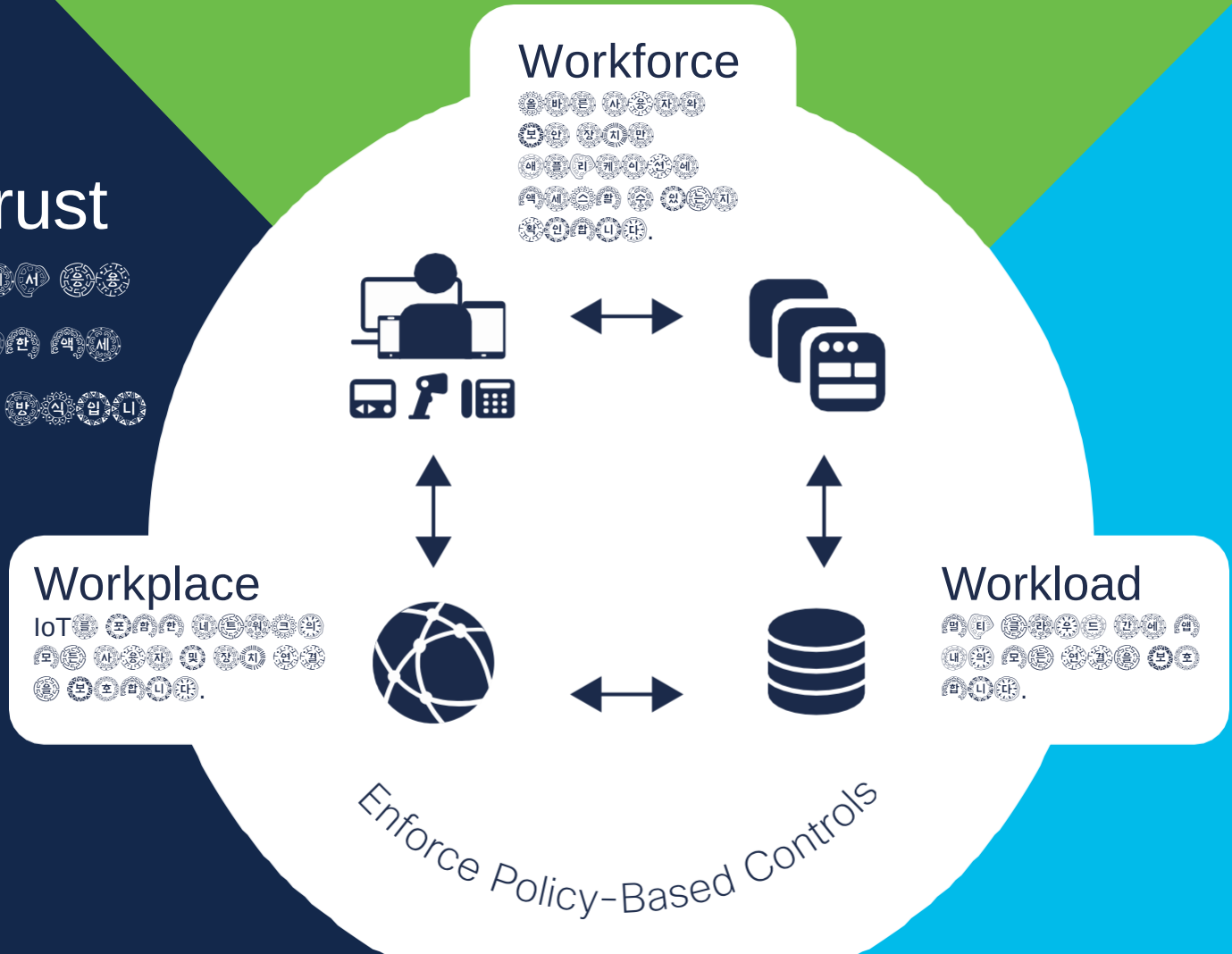
MFA=Bob Group= IT

Clean PDF

Encrypted TLS 1.3

Cisco Zero Trust

모든 사용자, 장치 및 위치에서 응용 프로그램 및 환경 전체에 대한 액세스를 보호하는 무신뢰 접근 방식입니다.



Cisco Zero Trust

직원, 워크로드 및 작업 장소에 대한 액세스를 안전하게 보호하는 포괄적인 접근 방식입니다.

Shift in IT landscape

Users, devices and apps are everywhere

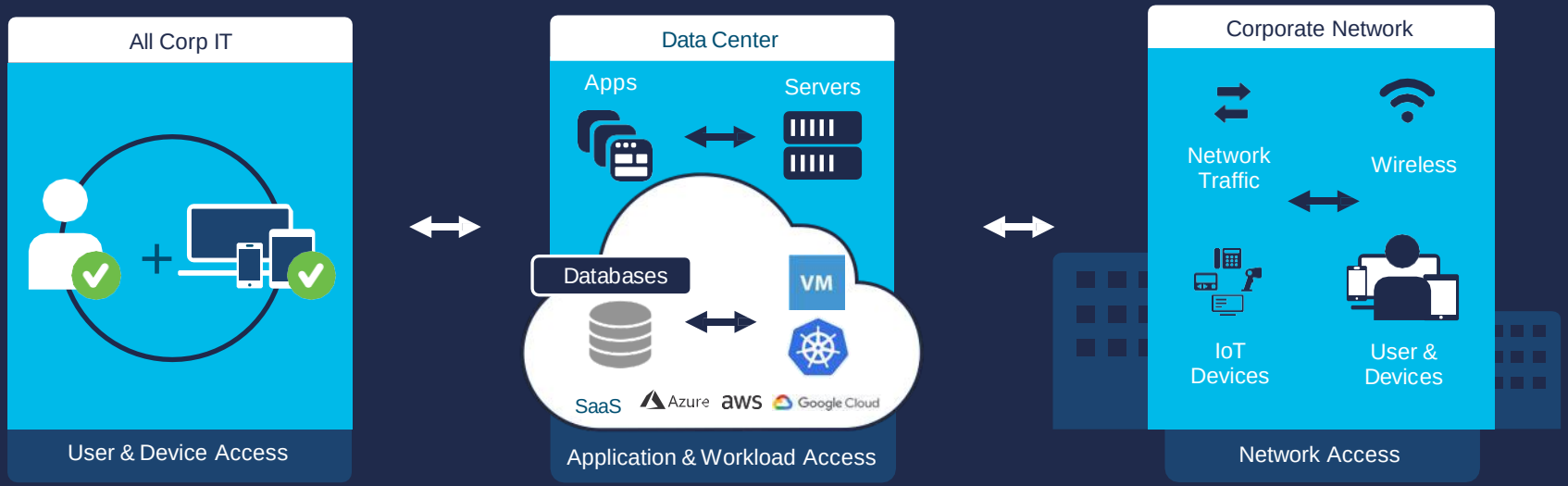
Securing Access

가시성을 확보하고 안전한 액세스를 보장하는 방법은 무엇입니까?

Workforce

Workload

Workplace



Workforce – DUO

Multi-Factor Authentication (MFA)

How it works:

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

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

Cisco Zero Trust for the Workload

How to Establish Trust with Tetration

Visibility and behavior modeling

WITH

Application discovery and dependency maps

All Processes, cmds, files, users and network comms

Per workload, micro-segmentation policy

WITH

Automated, context-based, segmentation policy

Consistent policy:
Any workload, Anywhere

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

Workplace – SD-Access

Cisco Zero Trust for the Workplace

How to Establish Trust with SD-Access & ISE

Discover and classify devices

WITH

IoT device profiling BYOD lifecycle management
User device Posture

Context-based network access control policy for users and things

WITH

Dynamic precise policies
Group-based (SGT)

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

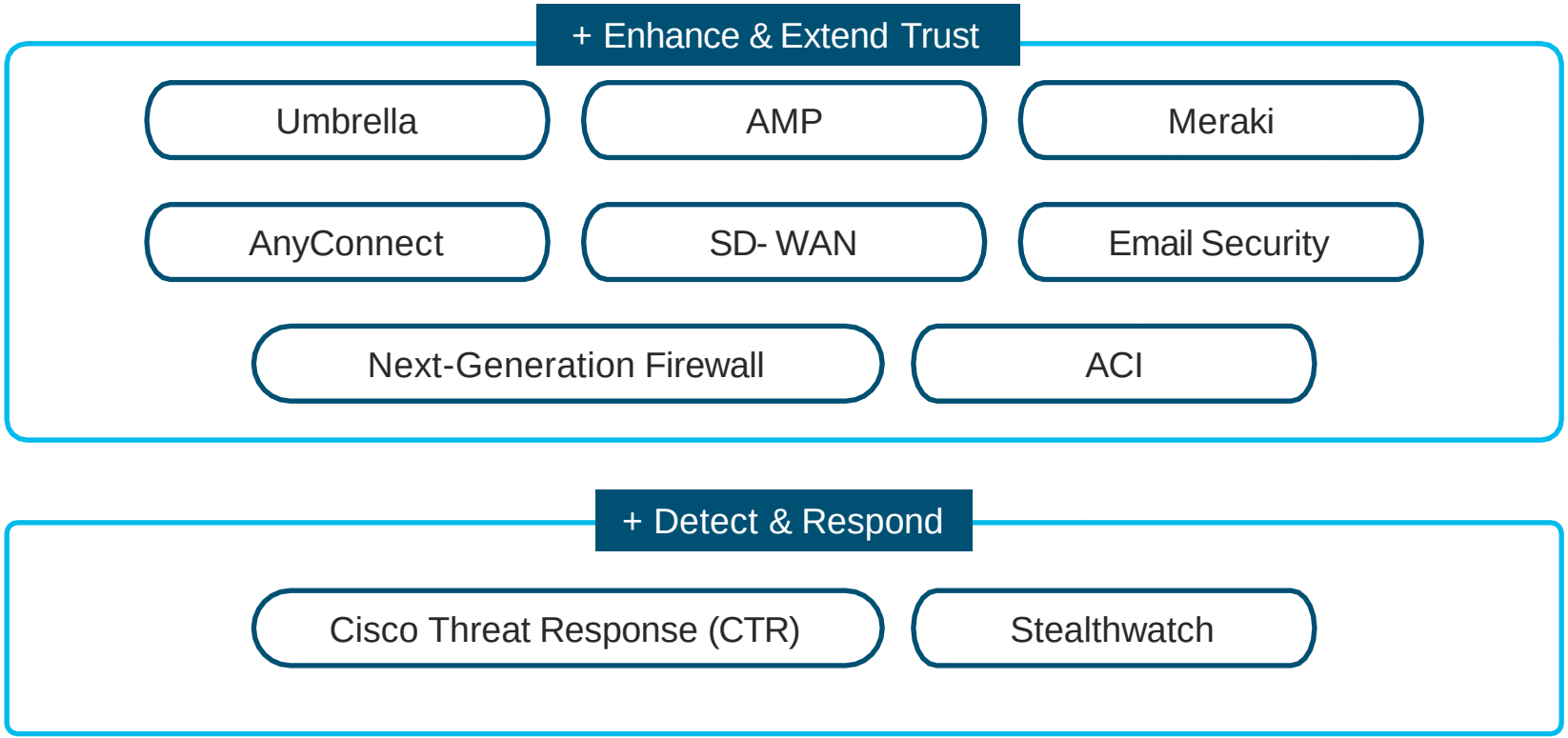
Cisco Zero Trust for the Workplace

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



감사합니다.