암호전환과 Zero Trust를 위한 필수역량

Crypto Agility

부제: Advance Towards SW-Defined Cryptography

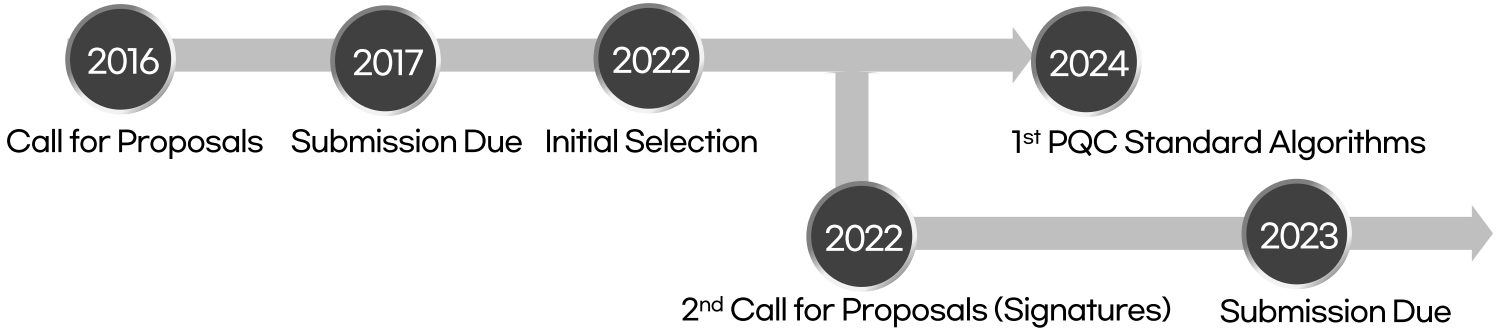
조지훈 마스터 (VP in Technology)
삼성SDS

양자내성암호 (Post Quantum Crypto, PQC)

기존 컴퓨터 및 양자컴퓨팅 환경에서도 안전한 암호 알고리즘

- 美 NIST*에서는 PQC알고리즘 표준화를 시작
- '24年 4종의 PQC 알고리즘 1차 표준화 완료
- PQC 알고리즘 추가 선정 진행

* NIST: National Institute of Standards and Technology



NIST Crypto standards

Public key based

- Signatures (FIPS 186)
- Key Establishment (SP 800-56 A/B/C)

Tools

- RNG (SP 800-90 A/B/C)
- KDF (SP 800-108/135)

Symmetric key based

- AES (FIPS 197)
- Modes of operation (SP 800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- Randomized hash (SP 800-106)
- HMAC derived functions (SP 185)

Guidelines

- Hash usage/security (SP 800-107)
- Key generation (SP 800-57)
- Transition (SP 800-133)

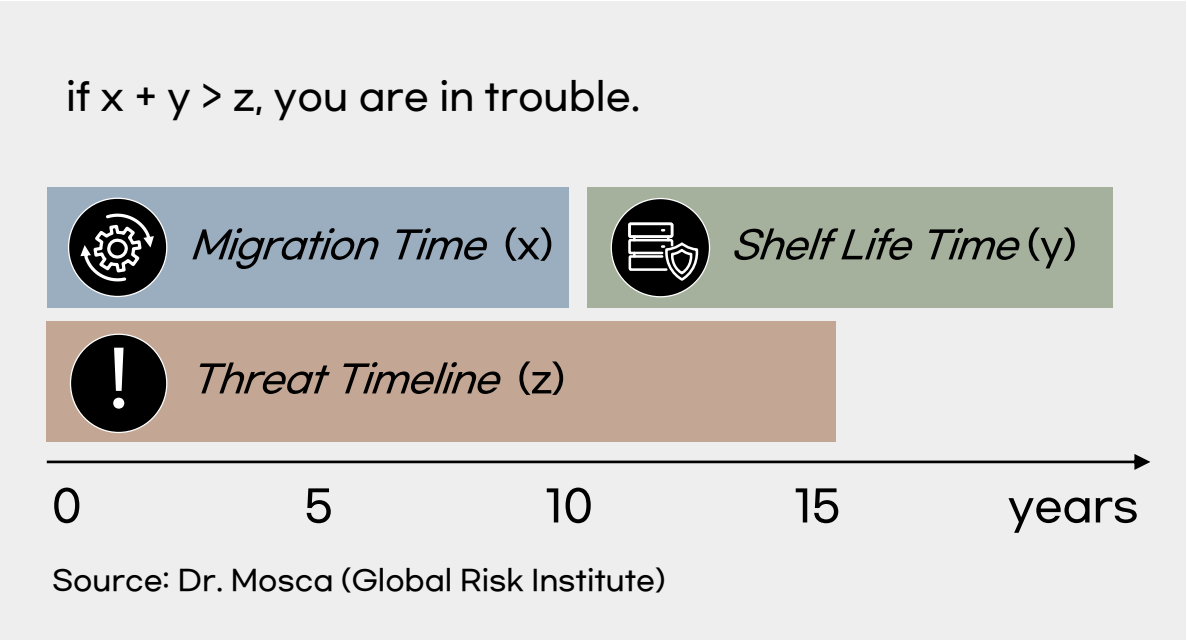
양자내성암호(PQC) 알고리즘으로 전환 必

양자내성암호 전환 고려사항

❶ Threat Timeline
언제 암호가 Break될 것인가?

❷ Shelf-life Time
데이터가 보호되어야 하는 기간은?

❸ Migration Time
양자내성암호 전환에 걸리는 시간은?



양자내성암호 전환 고려사항 2.　데이터가 보호되어야 하는 기간

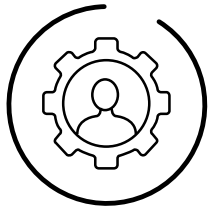
장기간 보호되어야 하는 데이터나 사용되어야 하는 기기는
양자컴퓨팅 기반 공격시점 이전에 보호방안이 적용되어야 함.

Harvest Now & Decrypt Later 공격:
장기간 보호가 필요한 데이터에 대해 공격자가 지금 암호화된 데이터를 백업, 이후 양자컴퓨터 성능이 일정수준이 이르면 해킹

* CRQC: Cryptographic Relevant Quantum Computer

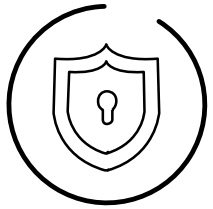
양자내성암호 전환 고려사항 3. 양자내성암호 전환에 필요한 기간

미국의 경우 연방정부기관의 IT시스템의 양자내성암호 전환에 **10년 이상의 기간 예상**
향후 암호 전환은 지속적으로 일어날 것으로 예측



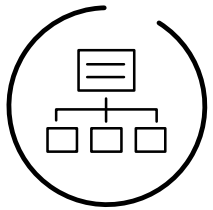
Difficulties of Crypto Migration

비교적 간단한 대칭키 암호의 경우도 **10년 이상 소요**



Complexity of PQC

성능 및 사이즈 측면에서 **다양한 양자내성암호**



Complexity of Targets

IT 시스템의 **복잡성 증가** (vs. Y2K?)

NIST 양자내성암호 전환 프로젝트 (2022-2026)

NIST에서는 양자내성암호 알고리즘의 표준공모 외,
별도의 **양자내성암호 전환 프로젝트를 진행** 중이며,

'22년 10여개 기업의 참여로 시작해, 현재 30여개 기업, 기관(NSA, CISA 등) 참여 중

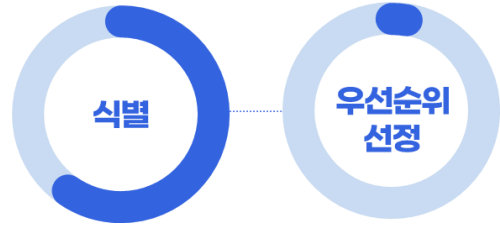
목표

"Initiating the **development of practices to ease migration** from the current set of public-key cryptographic algorithms **to replacement algorithms (PQC)** that are resistant to quantum computer-based attacks"

Project Consortium Participants

- Amazon Web Services, Inc. (AWS)
- Cisco Systems, Inc.
- Cybersecurity and Infrastructure Security Agency (CISA)
- Cloudflare, Inc.
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Dell Technologies
- DigiCert
- Entrust
- HP, Inc.
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Keyfactor
- Kudelski IoT
- Microsoft
- National Security Agency (NSA)
- Palo Alto Networks
- PQShield
- QuantumXchange
- SafeLogic, Inc.
- Samsung SDS Co., Ltd.
- SandboxAQ
- Santander
- SSH Communications Security Corp
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- Utimaco
- Verizon
- VMware, Inc.
- wolfSSL

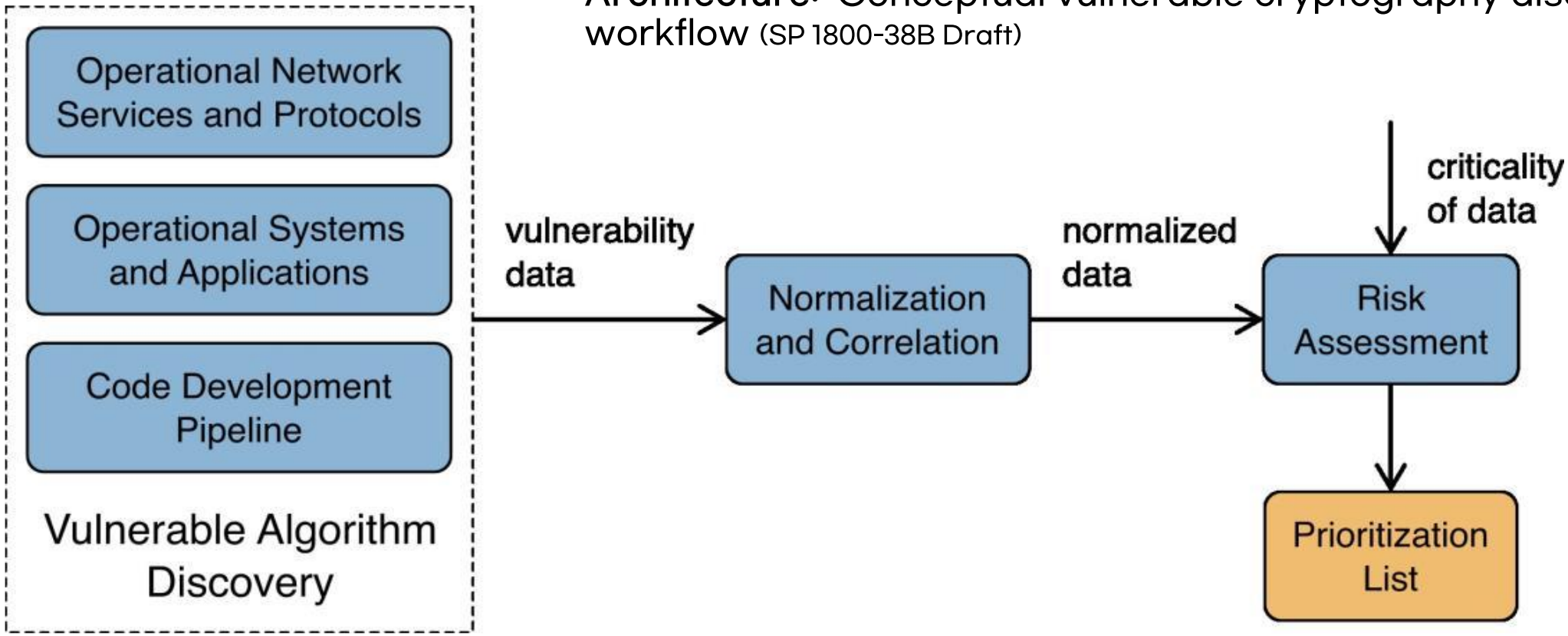
SP 1800-38B: Cryptographic Discovery



삼성SDS는 자체 툴(S-CAPE*)을 확보하고, NIST Lab에서 테스트 진행

* S-CAPE: Samsung SDS Crypto Agility Platform for Enterprise

Architecture: Conceptual vulnerable cryptography discovery workflow (SP 1800-38B Draft)



+ Source: NIST SP 1800-38B (Preliminary Draft)

SP 1800-38C: Interoperability & Performance

PQC(KEM, Digital Signature) 구현물에 대한 성능 및 상호호환 테스트를 진행
삼성SDS는 자체 모듈(s-pqc-tls)을 확보하고, TLS 프로토콜 테스트 참여

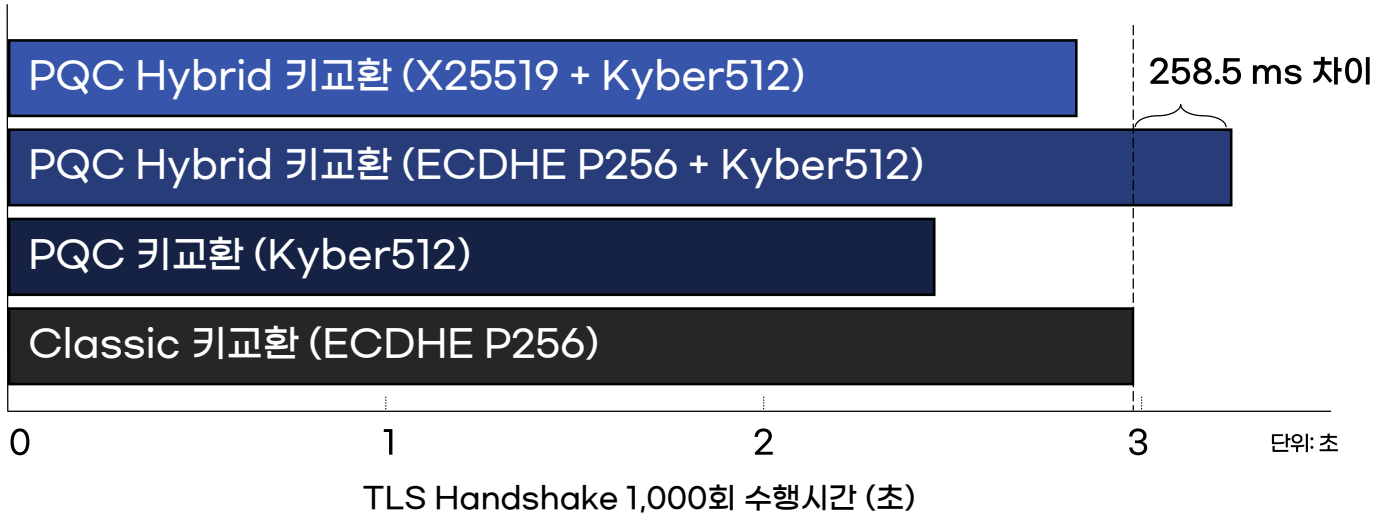
테스트 대상 PQC 알고리즘

키교환 (KEM)
Kyber-512(L1), 768(L3), 1024(L5)
P256+Kyber-512, P384+Kyber-768,
P521+Kyber-1024

전자서명
Dilithium-2, 3, 5
Falcon-512(L1)/1024(L5)
SPHINCS+(w/ SHAKE, SHA2)
LMS/HSS, XMSS/XMSSMT(w/ SHA2)

테스트 프로토콜, 표준, Use-Case
SSH, TLS, X.509, HSM

키교환 방식별 TLS 암호화 통신 성능 비교*



* NIST NCCoE Lab에서 테스트:
Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-72-generic x86_64), Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz (2 Core) 32GiB RAM

NIST 양자내성암호 프로젝트 향후 계획

현재 우선순위 선정을 위한 향후 진행방안 논의 중,
최종적으로, **Crypto Agility**을 위한 Best Practice 및 Tool 제공 필요

THE WHITE HOUSE

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

Central to this migration effort will be an emphasis on **cryptographic agility**, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards. This effort is an imperative across all sectors of the United States economy, from government to critical infrastructure, commercial services to cloud providers, and everywhere else that vulnerable public-key cryptography is used.

the term "**cryptographic agility**" means a **design feature** that enables future **updates to cryptographic algorithms** and **standards without** the need to **modify or replace** the surrounding infrastructure;

Design Feature of Crypto Agility in Enterprise?

Design Feature of Cybersecurity in Enterprise?

THE WHITE HOUSE

MAY 12, 2021

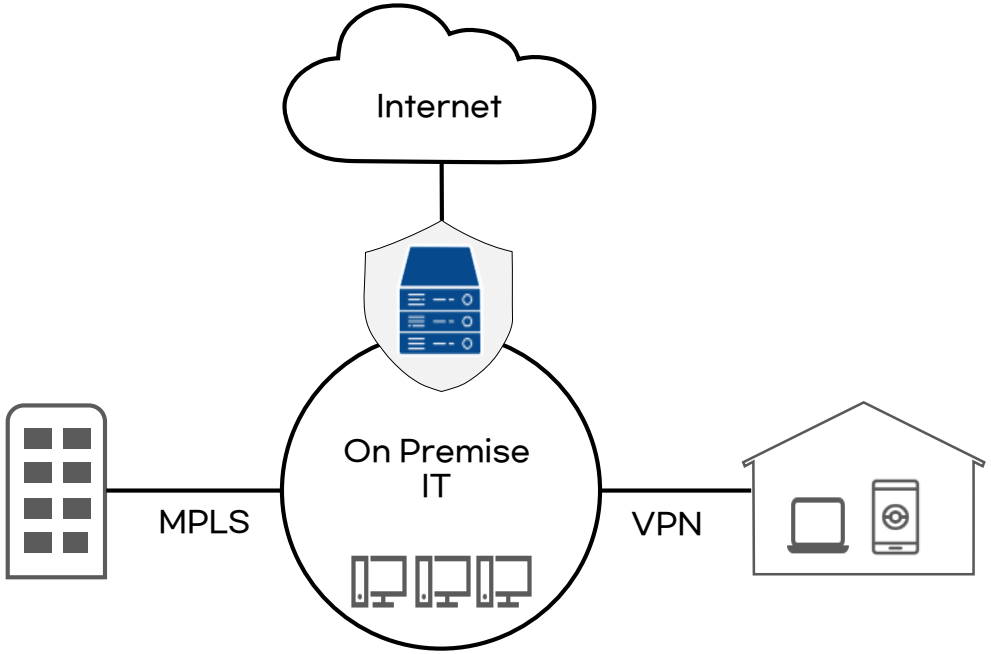
Executive Order on Improving the Nation's Cybersecurity

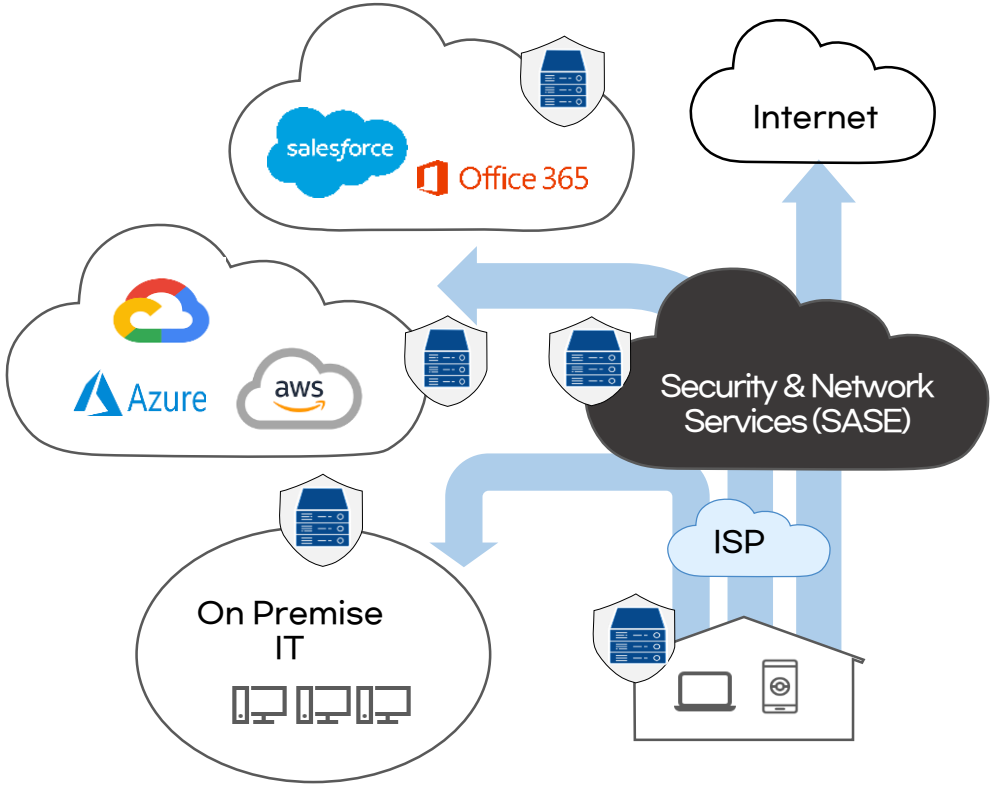
Sec. 3. **Modernizing Federal Government Cybersecurity**.

(a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government **must adopt security best practices; advance toward Zero Trust Architecture**; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

WHY Perimeter-based Security to Zero Trust?

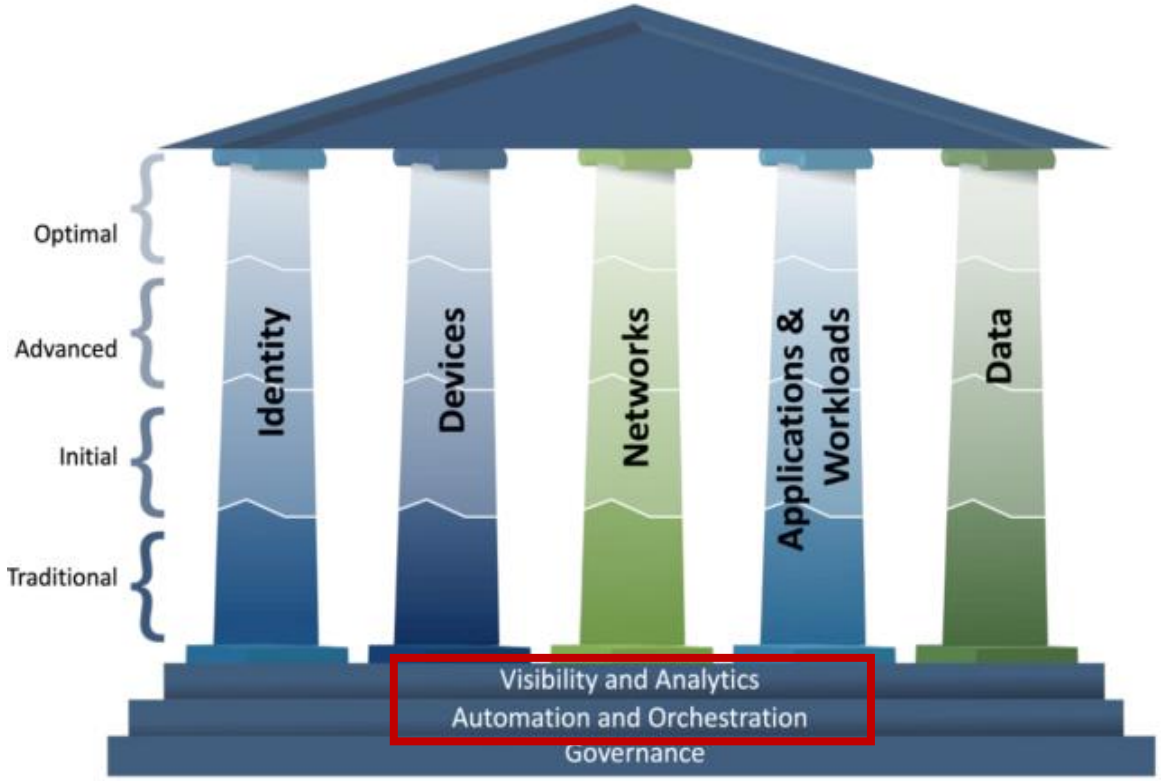
기존 → 현재 → 미래





How Zero Trust?
(Never Trust, Always Verify)

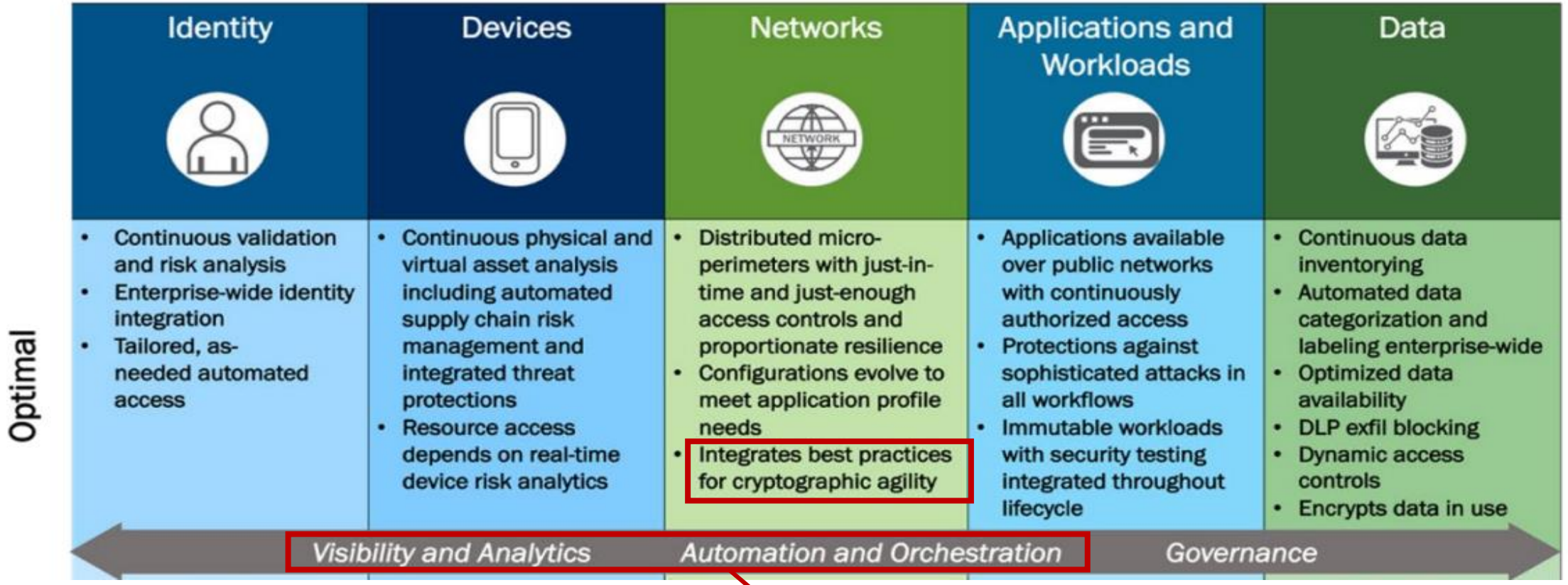
Visibility & Automation



+ Source: Zero Trust Maturity Model 2.0 (CISA)

Zero Trust Maturity & Crypto Agility

Networks 영역에서 Optimal(최고성숙도)단계를 달성하기 위해
"Best Practices for Cryptographic Agility"가 필요



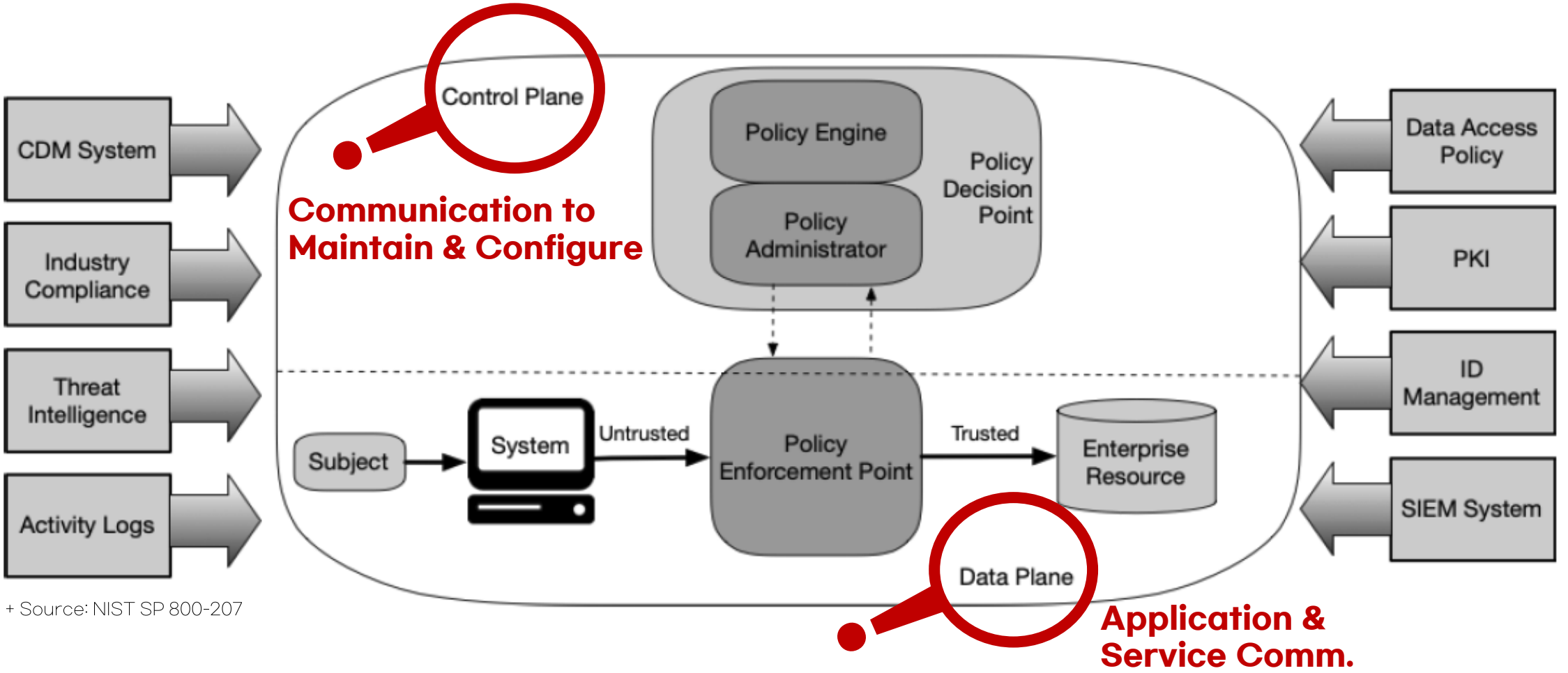
+ Source: Zero Trust Maturity Model 2.0 (CISA)

암호운영에 있어 **가시성**과 **자동화**를 어떻게 확보?

Zero Trust Architecture (Design Feature of Cybersecurity)

"… The **data plane** and **control plane** are logically separate"

3.4.1 Network Requirement to Support ZTA (NIST SP 800-207)



+ Source: NIST SP 800-207

Software-defined Network & Control/Data Plane

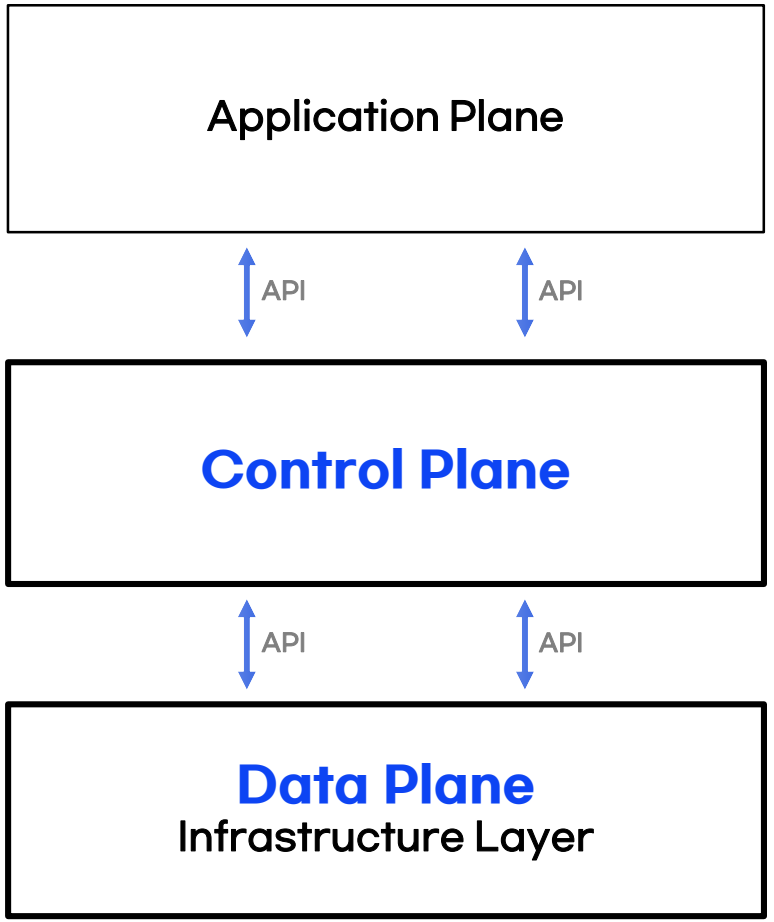
Software-Defined Networking (SDN): Layers and Architecture Terminology (RFC 7426)

Data Plane과 **Control Plane**간의 Interface를 정의,
Application Plane에서
SW 프로그래밍(SW-Defined)을 통해

"**전체** 네트워크를 **동적**으로 통제"

① 전체 Network에 대한 **가시성** 확보
② 각 Network 장비에 대한 설정배포 **자동화**

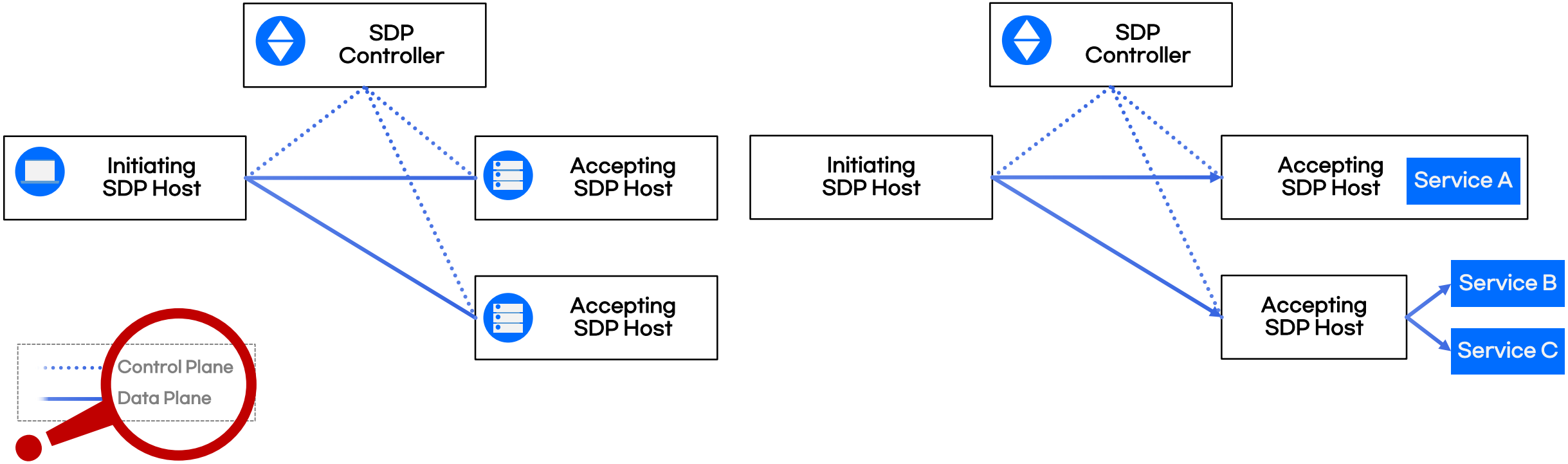
Simplified SDN Architecture



+ Source: RFC 7426

SDN to SDP (Software-defined Perimeter)

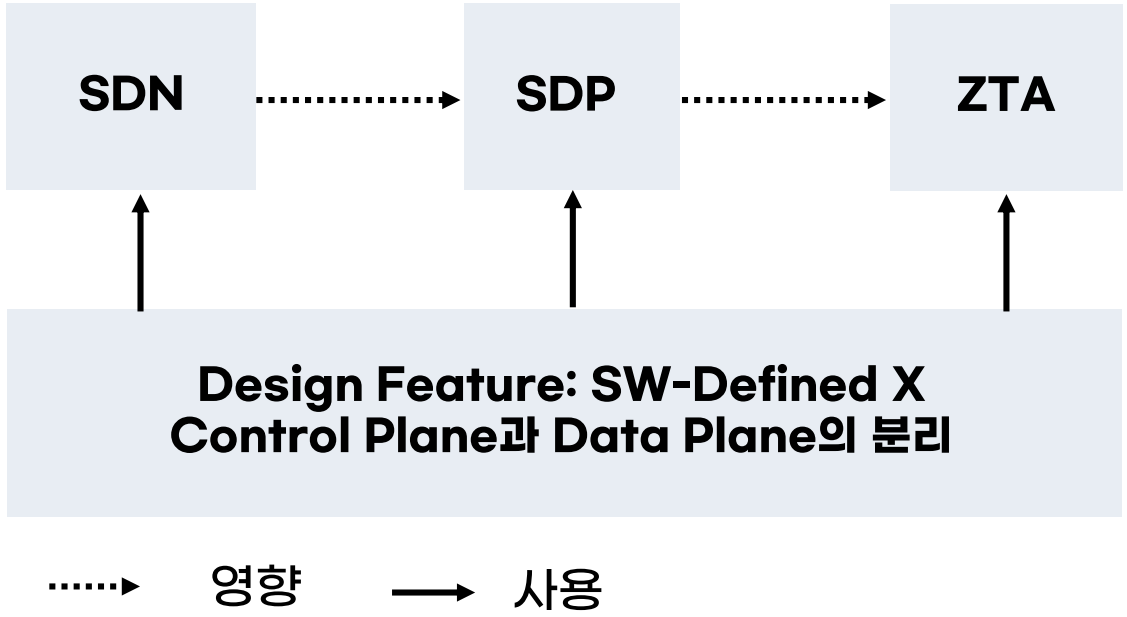
SDP focuses on protecting the critical organizational resources instead of the organizational perimeter, and **replaces perimeter-based and (often, physical) appliances with logical components** that operate under the control of the application owner.

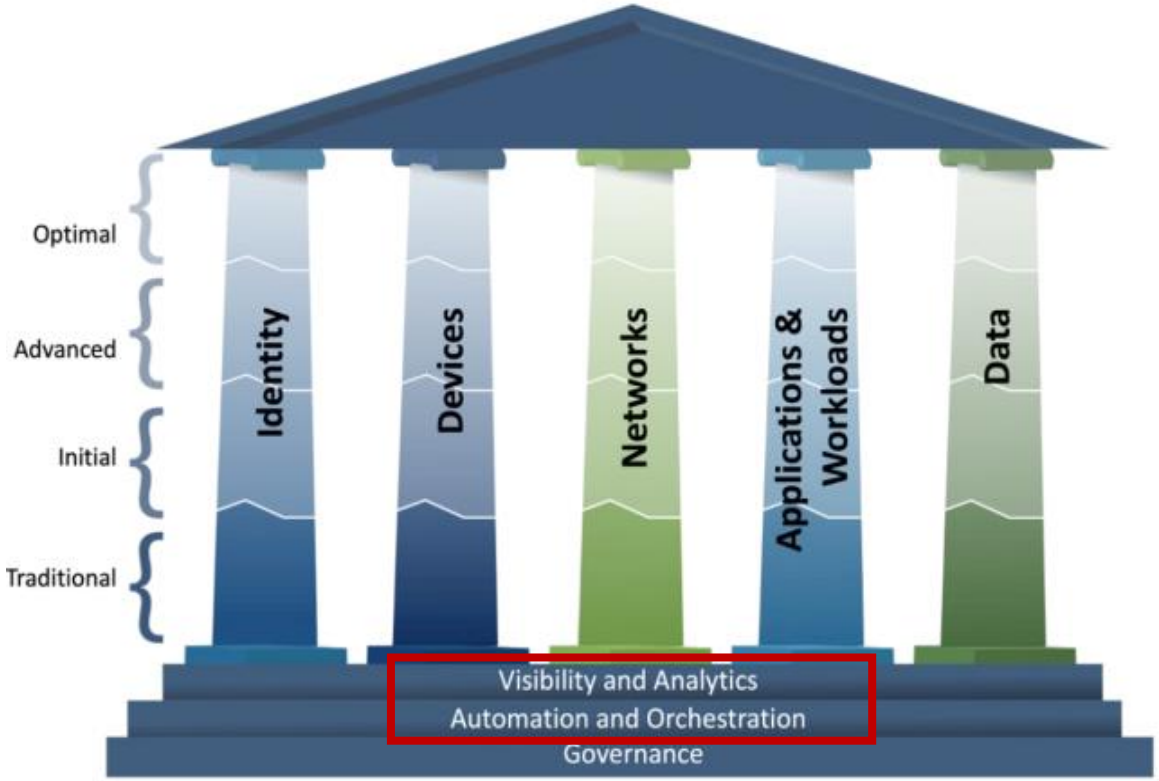


+ Source: CSA Software-Defined Perimeter (SDP) Specification 2.0 (CSA)

Towards SW-Defined Cybersecurity

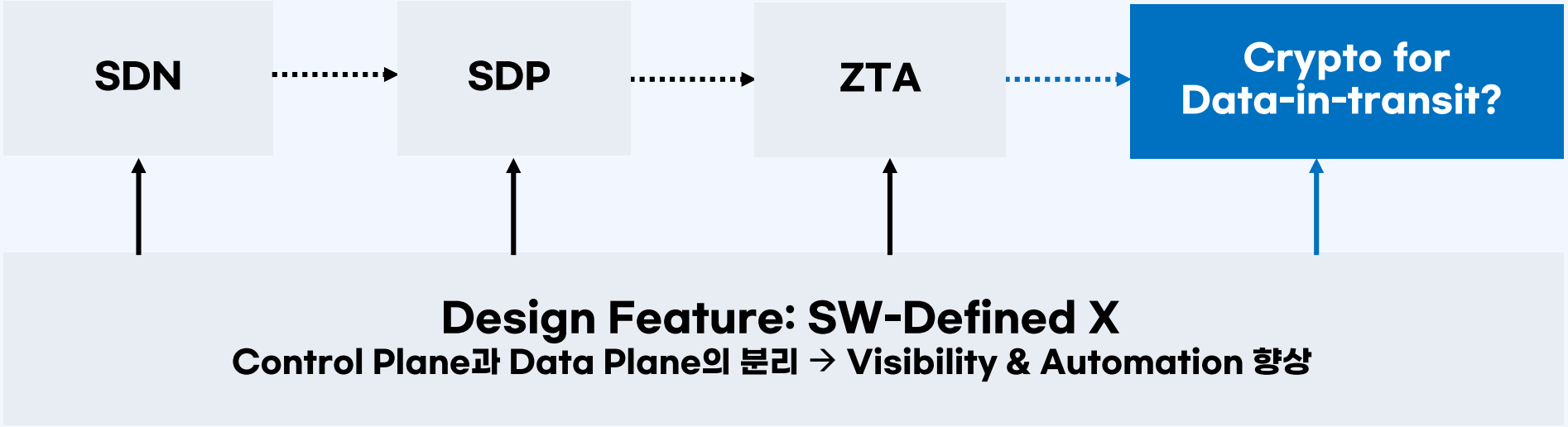
SW-Defined X의 Design Feature는 높은 수준의
Visibility(+Analytics)와 **Automation**(+Orchestration)의 역량을 제공





+ Source: Zero Trust Maturity Model 2.0 (CISA)

SW-Defined Cryptography
for Crypto Agility



SW-Defined Cryptography:
Design Feature of Crypto Agility for Data-in-Transit

Control Plane과 Data Plane간의 분리,

중앙에서 Enterprise 네트워크 **전체**에 대한

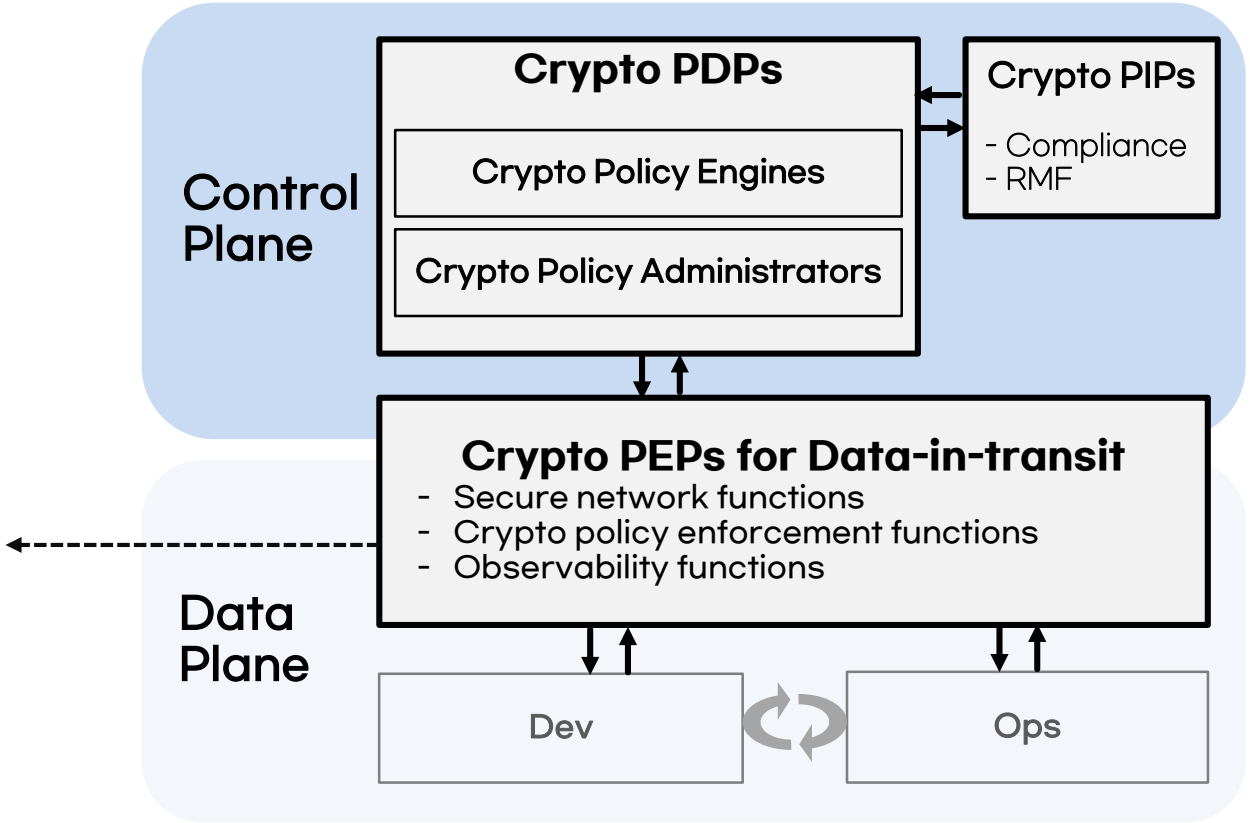
① 암호 사용실태 파악(Visibility)

② 암호정책 자동반영(Automation)

그리고,

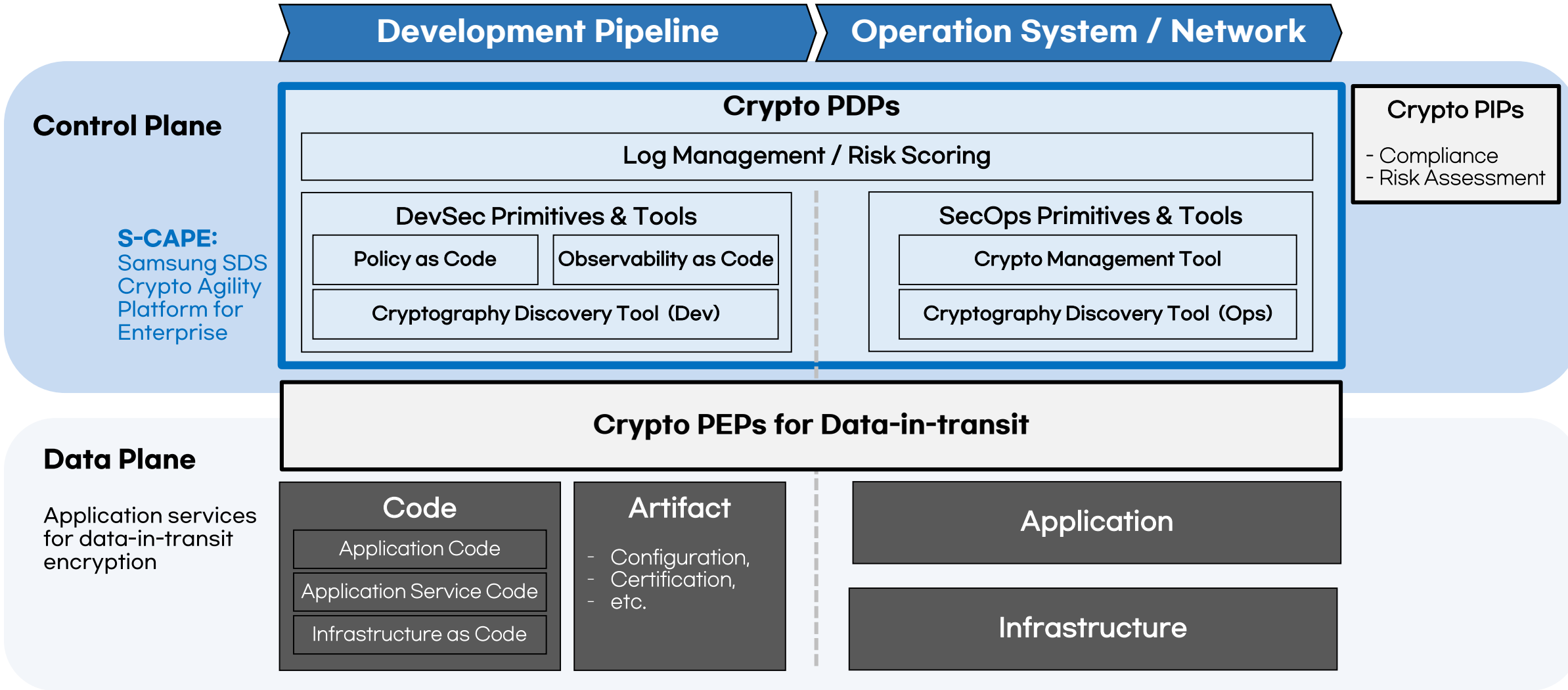
어플리케이션 수정 없이 암호정책을 적용 필요

(Separation of crypto configuration from applications)



PIPs: Policy Information Points, PDP: Policy Decision Point,
PEPs: Policy Enforcement Points

Design Feature 1. Control Plane과 Data Plane 분리 (Visibility)

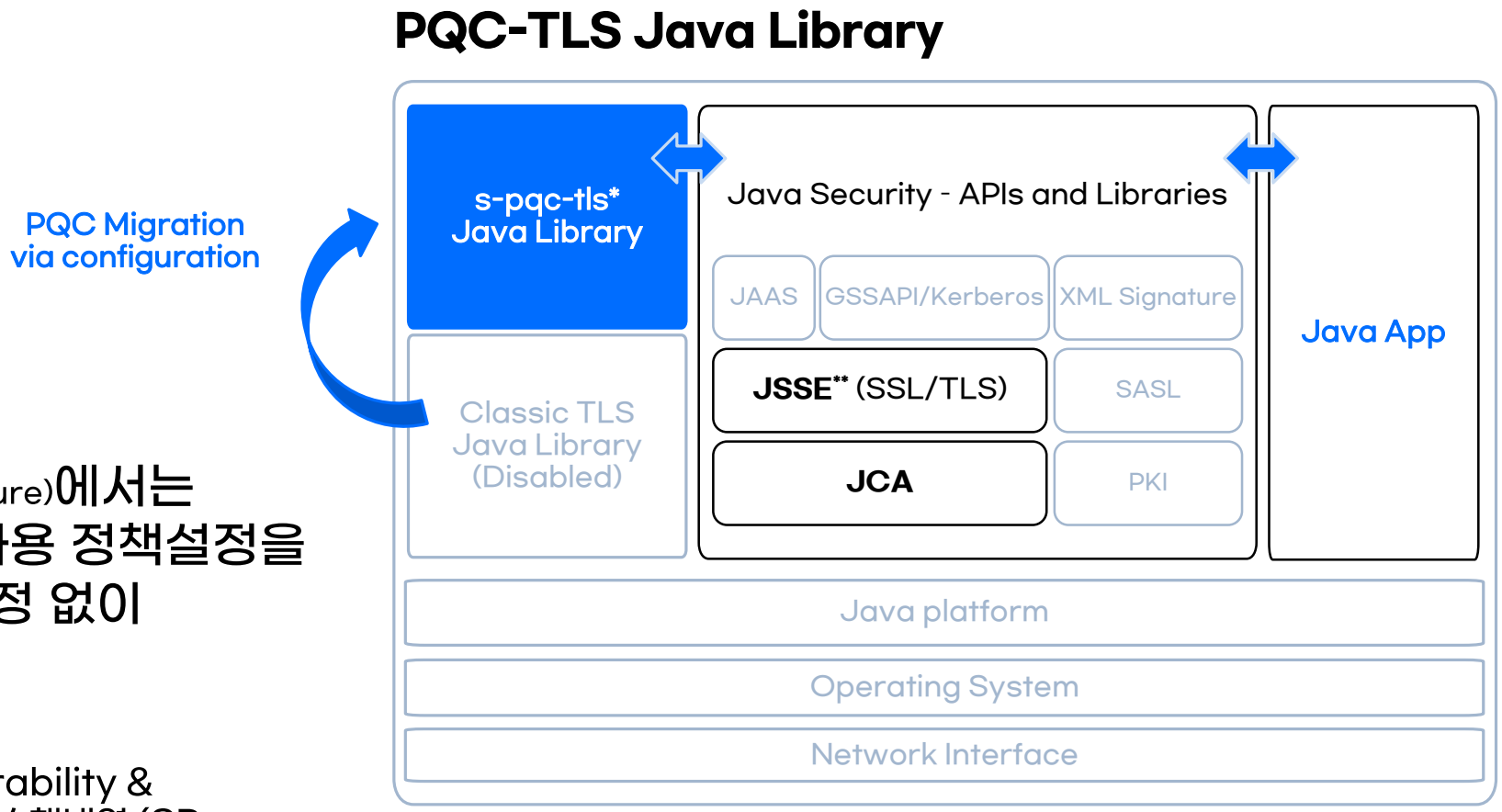


NIST Migration to PQC: Discovery Work Stream에서의 수행내역 (SP 1800-38B에 수록) 기반 확장모델

Design Feature 2. 암호사용에 대한 정책설정(configuration) 분리

JCA(Java Cryptography Architecture)에서는
어플리케이션으로부터 암호사용 정책설정을
분리하여, 어플리케이션의 수정 없이
암호(사용)정책 변경 가능

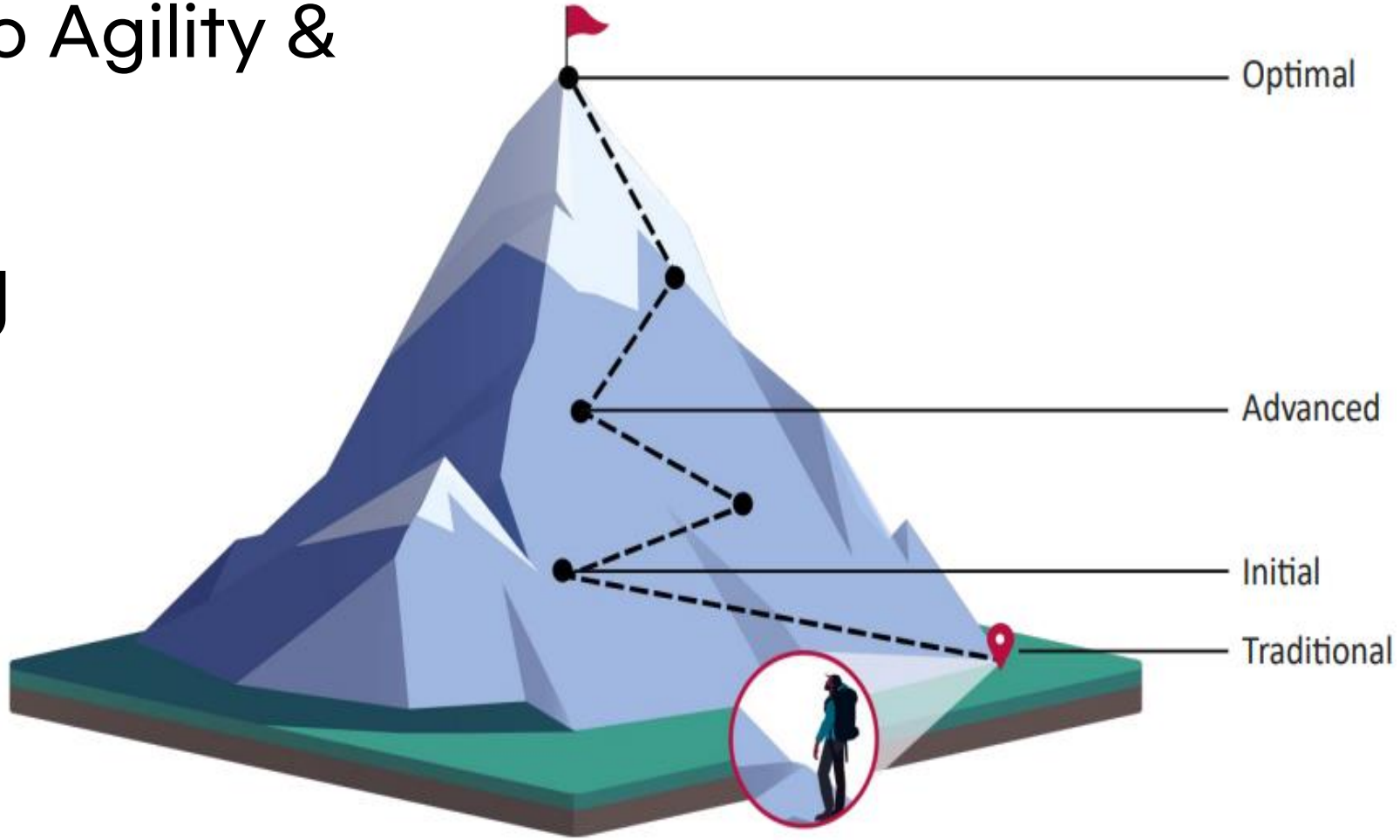
NIST 'Migration to PQC' Interoperability & Performance Work Stream에서의 수행내역 (SP 1800-38C 수록)



* s-pqc-tls: Samsung SDS PQC TLS

Achieving Crypto Agility &
Zero Trust is

a Long, Long Journey!



+ Source: Zero Trust Maturity Model 2.0 (CISA)

Crypto Agility 도입이전에,

조직의 **IT시스템과 Cybersecurity는**

SW-Defined 되어 있습니까?

SAMSUNG SDS

Seoul, Korea · New Jersey, USA · Weybridge, UK · Beijing, China · New Delhi, India · Singapore, Singapore · Hanoi, Vietnam · Sao Paulo, Brazil