aruba
a Hewlett Packard Enterprise company

LANOASIS

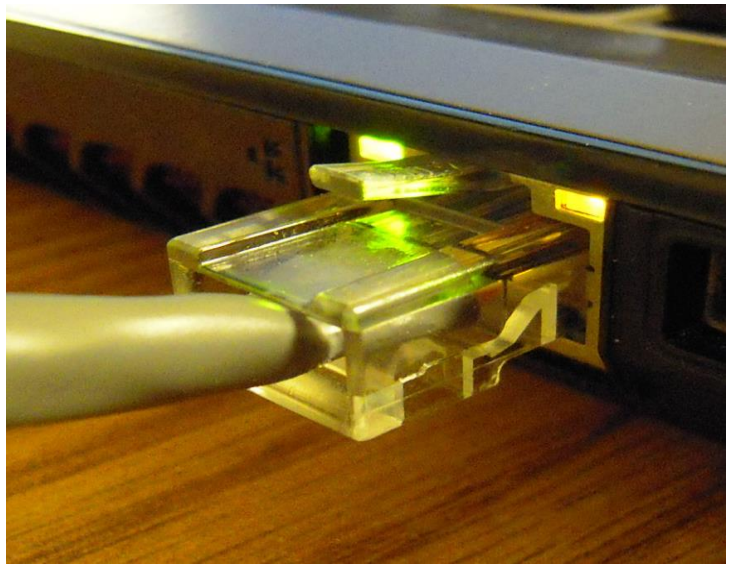
# New Normal 시대에 HPE Aruba ClearPass를 통한 네트워크 액세스 보호 솔루션을 소개합니다

2020년 8월 11일 오후 4시

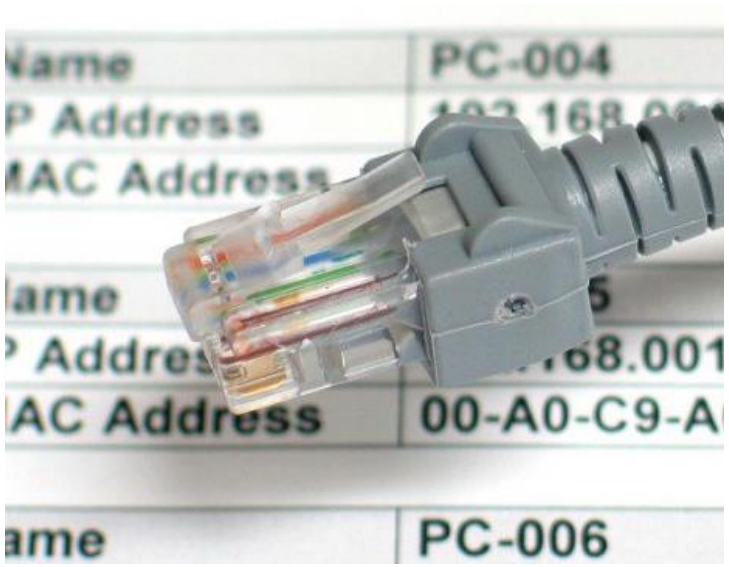

이동현 부장
정준호 과장

랜오아시스 - **HPE Aruba** 조달 총판사

# 기존 네트워크 환경



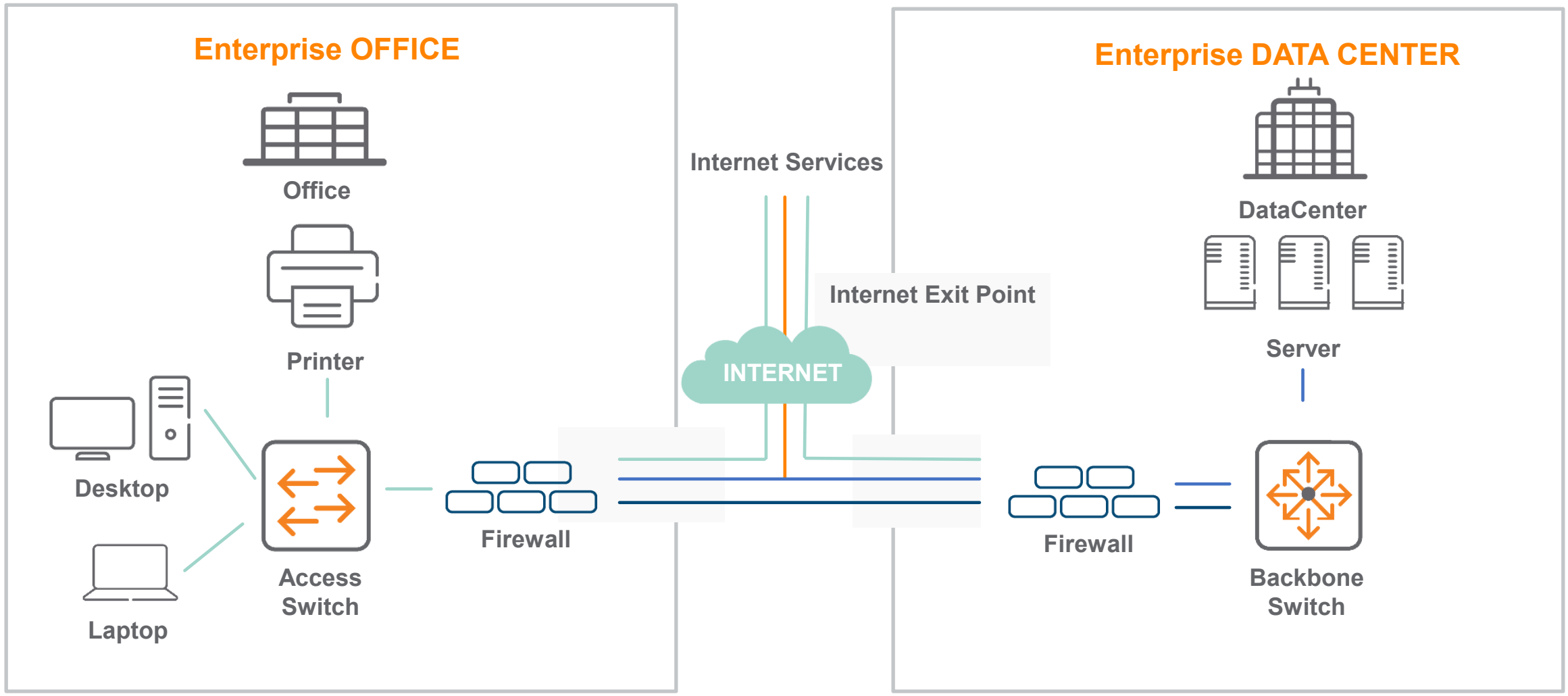
- **유선 네트워크 환경**
  - 유선 위주의 업무망
  - 데스크톱 위주 업무환경




- **고정 IP주소 환경**
  - MAC기반의 고정IP주소
  - IP주소 관리의 불편함
  - IP기반의 정책 관리

- **1인 – 1 Device**
  - 사용자당 1 디바이스
  - 접속 단말수의 제한

# 네트워크 가시성 확보 어려움



# 네트워크 인프라 환경 변화

**무선인프라 확대**

- 무선 업무환경으로 전환
- 무선 성능에 대한 Needs


**BYOD 환경**

- 개인 소유 단말 증가
- 접속 단말의 수 증가

**DHCP 환경**

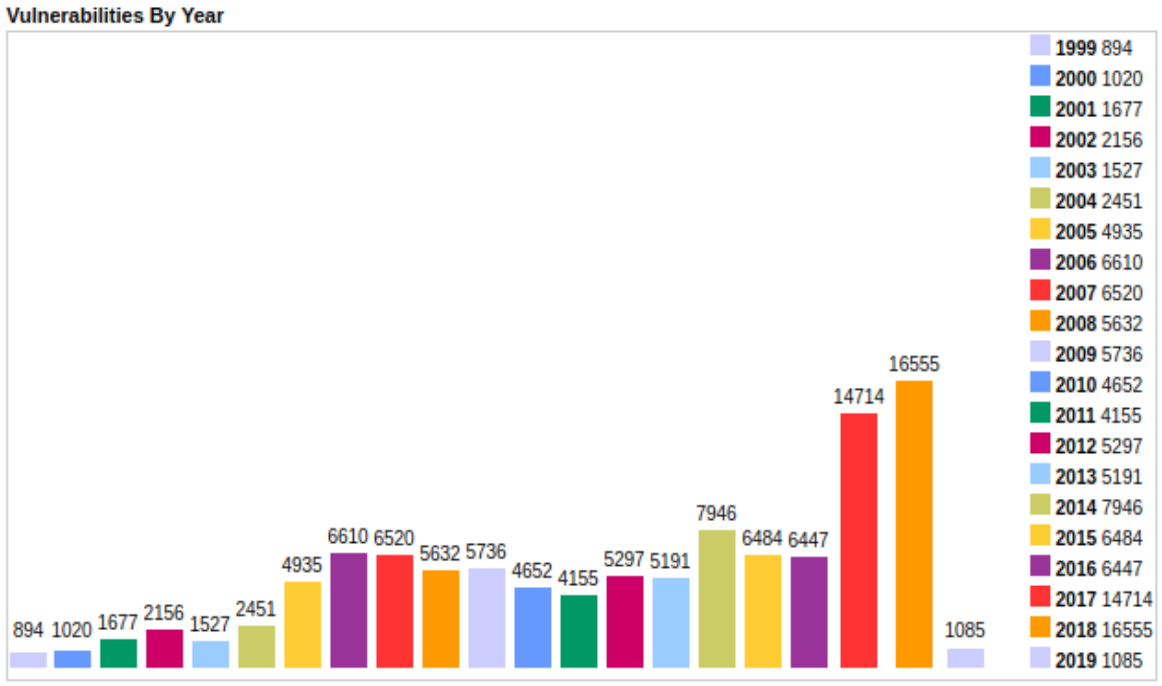
- IP 식별 어려움
- IP 기반 통제 어려움

**네트워크 복잡도 향상**

- 가시성 확보 어려움
- 휴먼 에러 위험

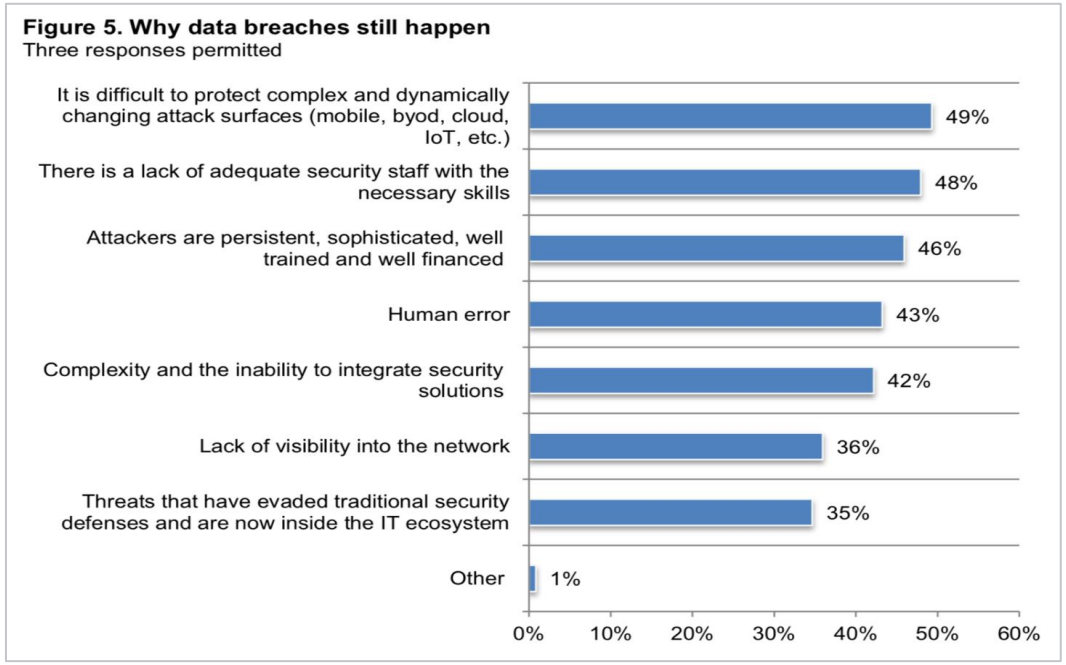
# IOT EXPANDING THE ATTACK SURFACE

## 연간 확인된 취약성




Source: MITRE CVE
Note: 2019 only small subset of total year

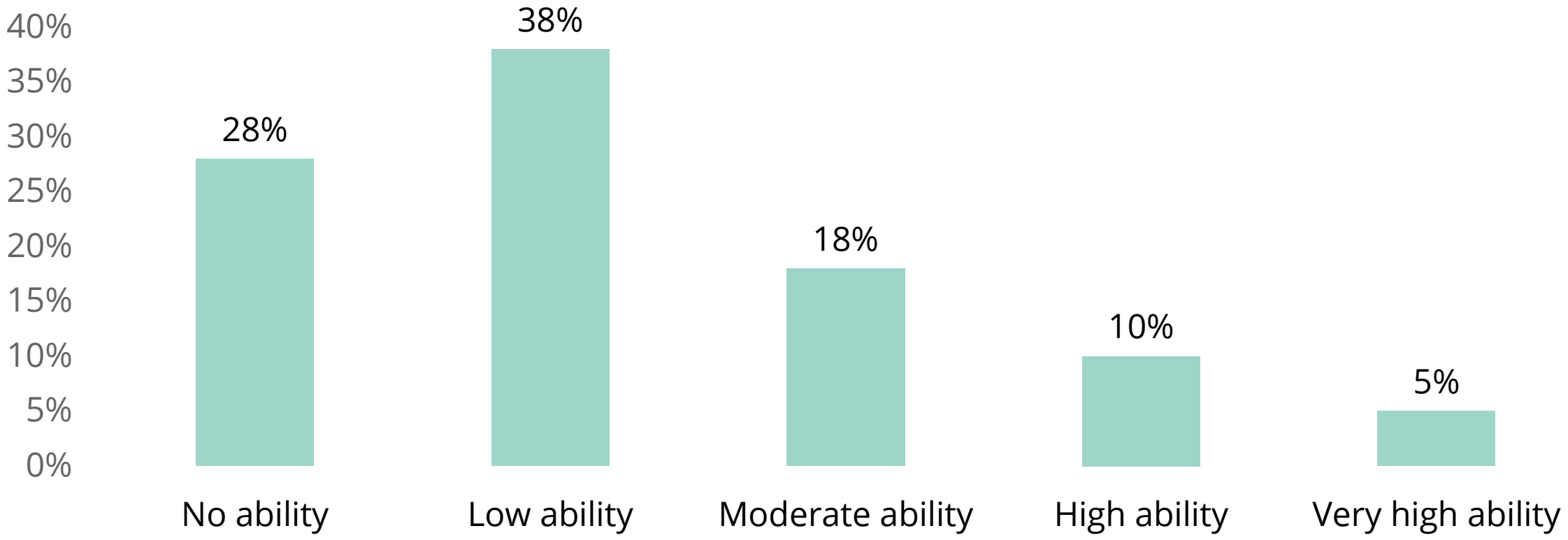
## 기업이 따라잡기 위해 고군분투



# 엔터프라이즈의 절반이 IOT 보안에 어려움을 나타냄

**Figure 1 The ability to secure IoT devices and apps**

1 = no ability, 5 = very high ability




Source: Ponemon Institute

# CIO의 고민: 모빌리티 vs 보안

## User Mobility

- 무선랜 환경
- 모바일 단말
- 원격 접속


## Enterprise Security

- 접근 제어
- 데이터 보호
- 규제 요구

# 관리자의 당면과제 - 보안

특정 타켓에 대한
고도화된
공격방식 (APT)

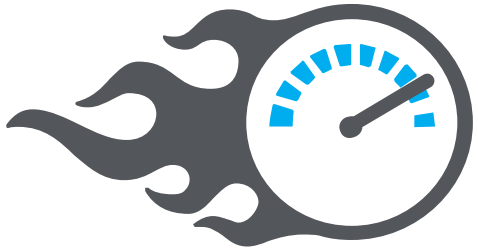
Network와
End-Point에 대한
**가시성 및 위협**
**탐지 어려움**

여러 보안
솔루션으로 인한
**복잡성 증가** 및
보안 IT담당자의
**업무 부담**

# 네트워크 보안 제품의 요구사항

위치, 시간, 장소에
관계없이 네트워크에
대한 접근 제어

실시간 정보
공유를 통한
정확한 정책 적용



3rd Party 보안제품과
통합된 Workflow

# ISMS 인증 의무대상자

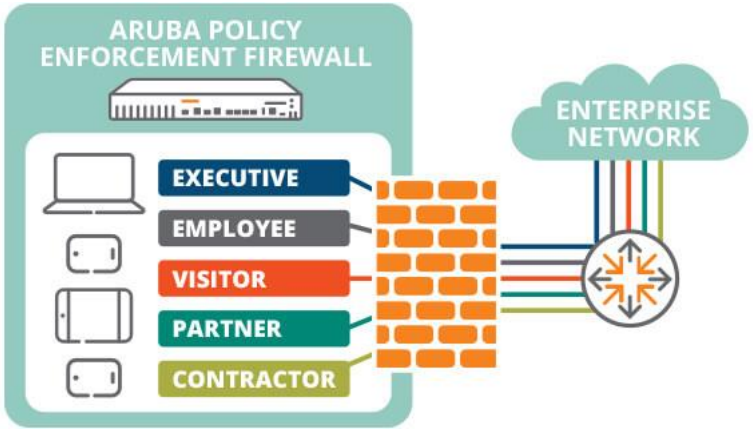
## 정보통신망법 제 47조 2항

| 구분 | 의무대상자 기준 |
|---|---|
| **ISP** (Internet Service Provider) | – [전기통신사업법] 제6조제1항에 따른 허가 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자 |
| **IDC** (Internet Data Center) | – [정보통신망법] 제46조에 따른 집적정보통신시설 사업자 |
| 연간 매출액 또는 세입이 **1,500억원 이상인 자 중**에서 다음에 해당하는 경우 | – [의료법] 제3조의4에 따른 **상급종합병원**<br>– 직전연도 12월31일 기준으로 재학생 수가 **1만명 이상인 대학교*** |
| **정보통신서비스** (인터넷 쇼핑몰, 게임, 포털 등) | – 전년도 매출액 100억원 이상<br>– 전년도 직전 3개월간 일일 평균 이용자 100만명 이상 |

* [고등교육법] 제2조에 따른 학교

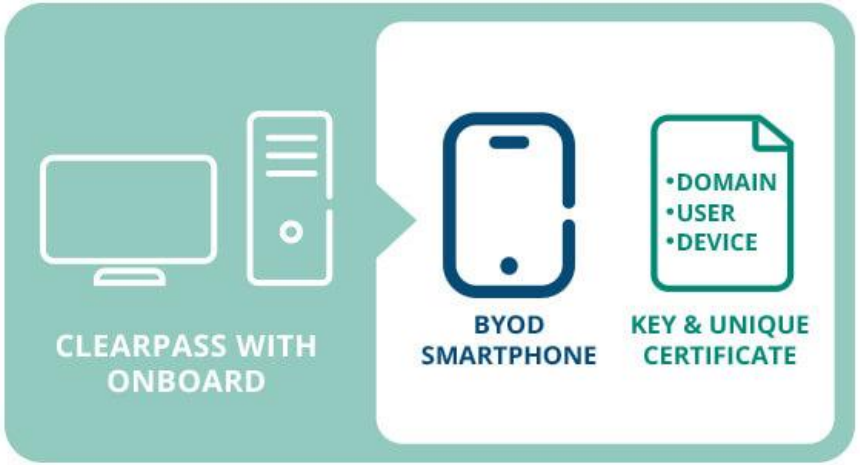
# 접근통제 - 유선 네트워크 접근

| 항 목 | 2.6.1 네트워크 접근 |
|---|---|
| 인증기준 | 네트워크에 대한 비인가 접근을 통제하기 위하여 **IP관리, 단말인증** 등 관리 절차를 수립 이행하고, 업무목적 및 중요도에 따라 네트워크 분리 (DMZ, 서버팜, DB존, 개발존 등)와 **접근통제를 적용**하여야 한다. |
| 주요 확인 사항 | • 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부 네트워크는 **인가된 사용자**만이 접근할 수 있도록 통제하고 있는가? |
| | • 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 **분리**하고 각 영역간 접근통제를 적용하고 있는가? |
| | • 네트워크 대역별 IP주소 부여 기준을 마련하고, DB서버 등 외부 연결이 필요하지 않은 경우 사설 IP로 할당하는 등의 대책을 적용하고 있는가? |
| | • 물리적으로 떨어진 IDC, 지사, 대리점 등과의 네트워크 연결 시 전송구간 보호대책을 마련하고 있는가? |



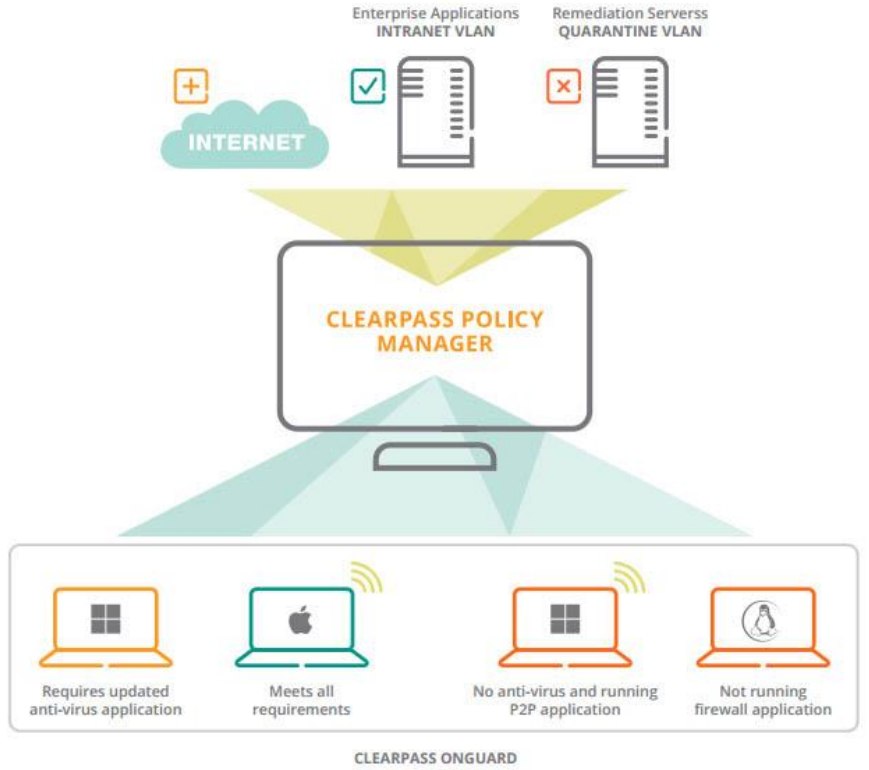
# 접근통제 - 무선 네트워크 접근

| 항 목 | 2.6.1 무선 네트워크 접근 |
|---|---|
| 인증기준 | 무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 **무선 네트워크 보호대책**을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립 이행하여야 한다. |
| 주요 확인 사항 | • 무선네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위해 인증, 송수신 데이터 암호화 등 보호대책을 수립 이행하고 있는가? |
| | • 인가된 임직원만이 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립 이행하고 있는가? |
| | • AD Hoc 접속 및 조직내 허가 받지 않은 무선 AP 탐지 차단 등 비인가된 무선 네트워크에 대한 보호대책을 수립 이행하고 있는가? |



# 시스템 및 서비스 보안관리 - 업무용 단말기기 보안

| 항 목 | 2.10.6 업무용 단말기기 보안 |
|---|---|
| 인증기준 | PC, 모바일 기기 등 단말기기를 업무목적으로 사용하는 경우 **기기 인증 및 승인, 접근 범위, 기기 보안설정** 등의 접근 통제 대책을 수립하고 주기적으로 점검하여야 한다. |
| 주요 확인 사항 | • PC, 노트북 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안설정 등의 **보안 통제 정책**을 수립 이행하고 있는가? |
| | • 업무용 단말기를 통해 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료공유프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립 이행하고 있는가? |
| | • 업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유노출을 방지하기 위하여 보안대책을 적용하고 있는가? |
| | • 업무용 단말기기에 대한 접근통제에 대책의 적절성에 대해 주기적으로 점검하고 있는가? |

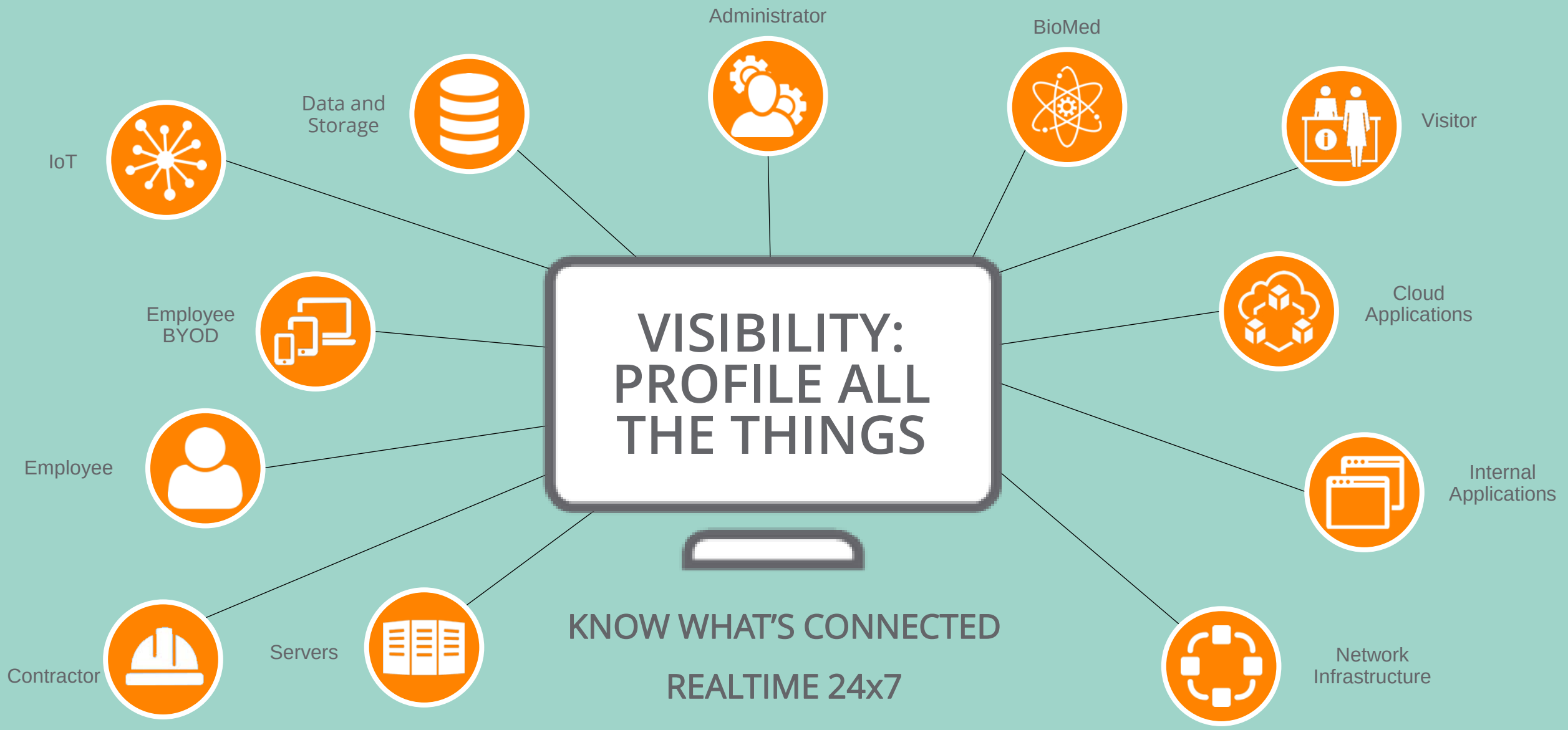


# CLEARPASS: COMPLETE POLICY MANAGEMENT IN A SINGLE SOLUTION

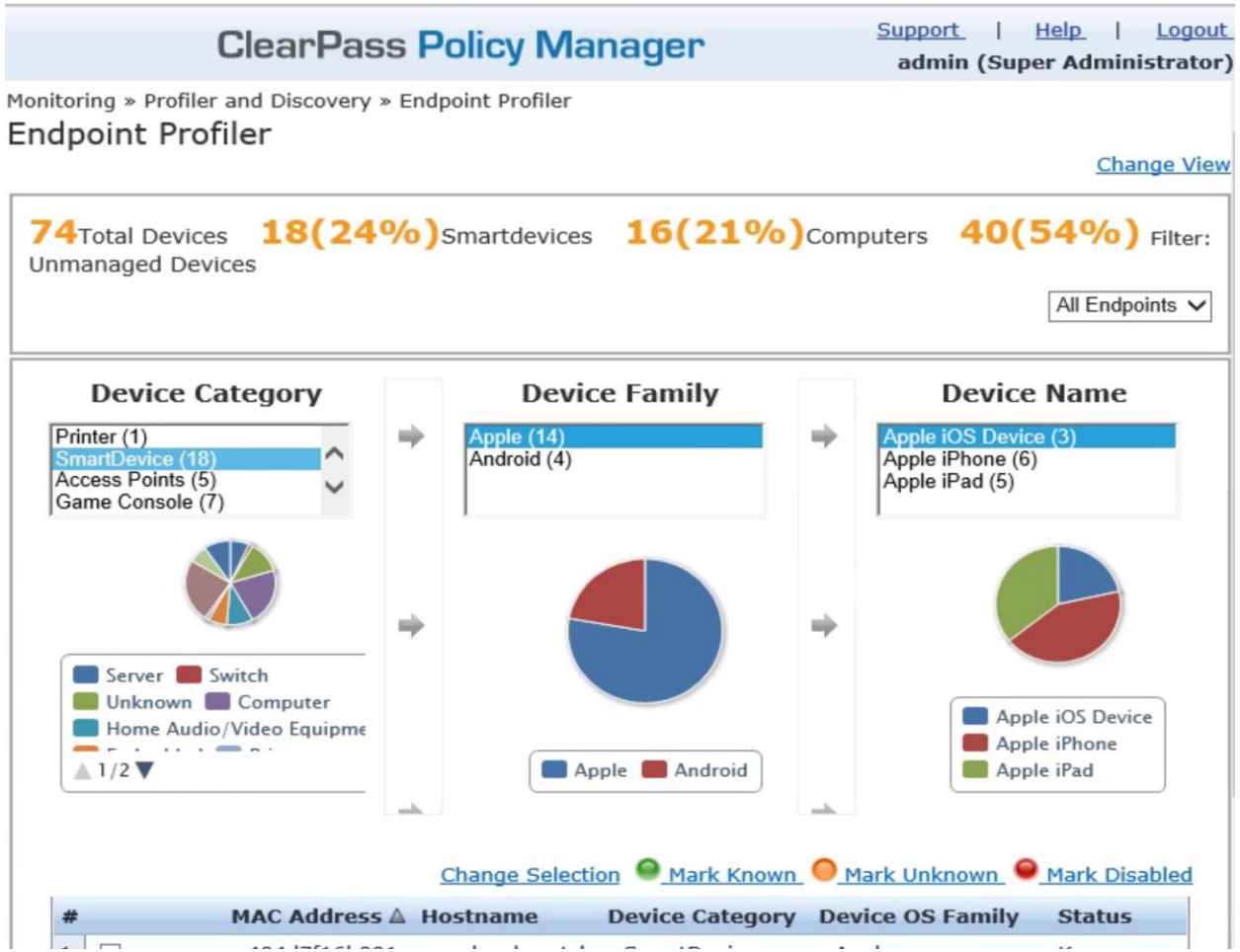

| Guest | Policy Engine | Flexible Enforcement | 3rd Party Integrations | Reporting | Network Device Admin |
|---|---|---|---|---|---|

**Onboard**
Device provisioning and privileges

**OnGuard**
Device posture assessment


Administrator
BioMed
Data and Storage
IoT
Visitor
Employee BYOD
Cloud Applications
VISIBILITY: PROFILE ALL THE THINGS
Employee
Internal Applications
Contractor
Servers
Network Infrastructure
KNOW WHAT'S CONNECTED
REALTIME 24x7
AGENTLESS

# ClearPass Profiler




## 식별 및 추적

- Headless 및 IoT 단말은 스스로 네트워크 인증을 할 수가 없습니다. ClearPass Profiler는 부족한 정보를 충분히 채워 넣을 만큼 지능적입니다.
- 일반적인 단말뿐만 아니라 커스텀 단말 유형도 식별
- 단말 유형 변경사항 추적
- DHCP 및 HTTP User-Agent 문자열을 통해 단말 핑거프린트 정보를 수동적으로 수집
- OnGuard, WMI, SNMP, NMAP 등과 같은 에이전트 방식으로 단말 핑거프린트 정보를 능동적으로 수집

## 유선 및 무선 단말의 가시성 획득

- 유선 스위치 포트에 연결된 단말을 찾기 위해 네트워크 스캔을 수행

# ROLE-BASED (역할 기반) 접근 제어

## AUTHENTICATION(인증) & AUTHORIZATION(인가)

사용자별 접근 가능 여부를 사전에 정의

ClearPass는 정책들을 적용


Defines **WHO** and **WHAT DEVICES** can connect to:

Any **연결방식**

Any **제조사**

Any **단말**

Any **리소스**

# ClearPass Authorization


## Context 인지 기반 정책

액세스 방식, 사용자, 단말 및 위치 등 Context 기반의 정책 적용 가능

## 포괄적인 기능 Set

하나의 단일 플랫폼에서 모든 보안 서비스의 사용 및 관리

## 세분화된 방식

로그인 / 암호, 인증서 또는 End-point 유형에 따라 모든 사용사례에 맞게 여러 ID 저장소 및 인증방법 활용

# ClearPass Authorization

## Context 기반의 Adaptive Trust

**Enterprise Laptop**
**Internet and Intranet**

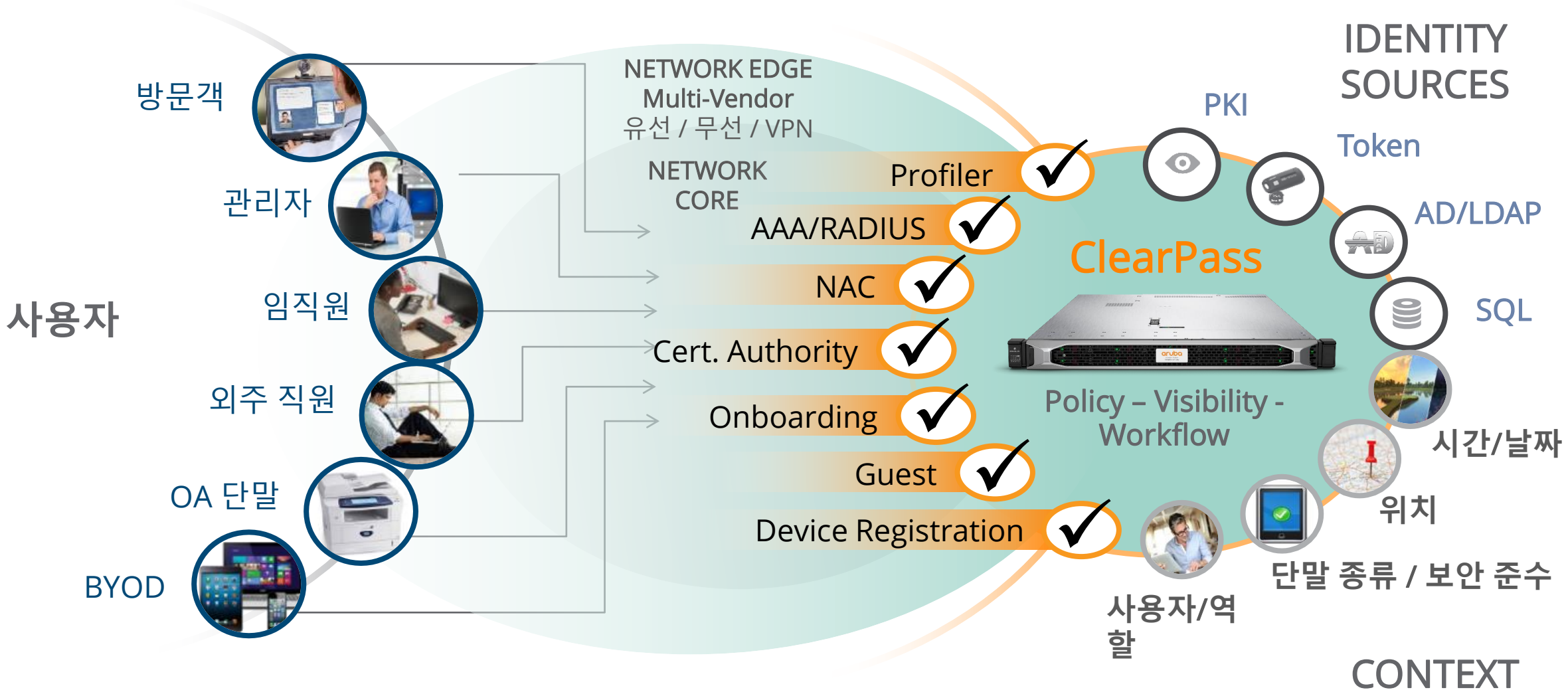
| 인증 방식 | EAP-TLS |
|---|---|
| SSID | CORP-SECURE |

**BYOD Phone**
**Internet Only**

| 인증 방식 | EAP-PEAP |
|---|---|
| SSID | CORP-SECURE |

SAP ORACLE Exchange box

# ClearPass 핵심 기능



# Role 이란?

보안 준수

평일 야간 시간

회사 업무용

임직원

회사 자산

MacBook

인사팀

# Example of “Role”

Who: **Bob**
Group: **학부생**
Device: **개인 iPad**
MDM: **Airwatch**
Location: **104호**
Time: 오전 **9시, 월요일**
Compliance: **보안 준수**
Mac Address: X
IP Address: Y
Airgroup **사용 가능**


ClearPass

*Service Chaining*

AD/LDAP — WHO

EMM/MDM — WHO, WHAT, WHERE, WHEN

Update Enforcement Device (LAN/WAN/VPN)

Update Firewall

Update Web Proxy / Filter

Logon to Applications (SSO)

Update EMM/MDM

# ClearPass Platform

Guest


Onboard

OnGuard

Expansion Applications

Hardware
(C2000, C3000)
or
VM Appliances
(Cx000V)

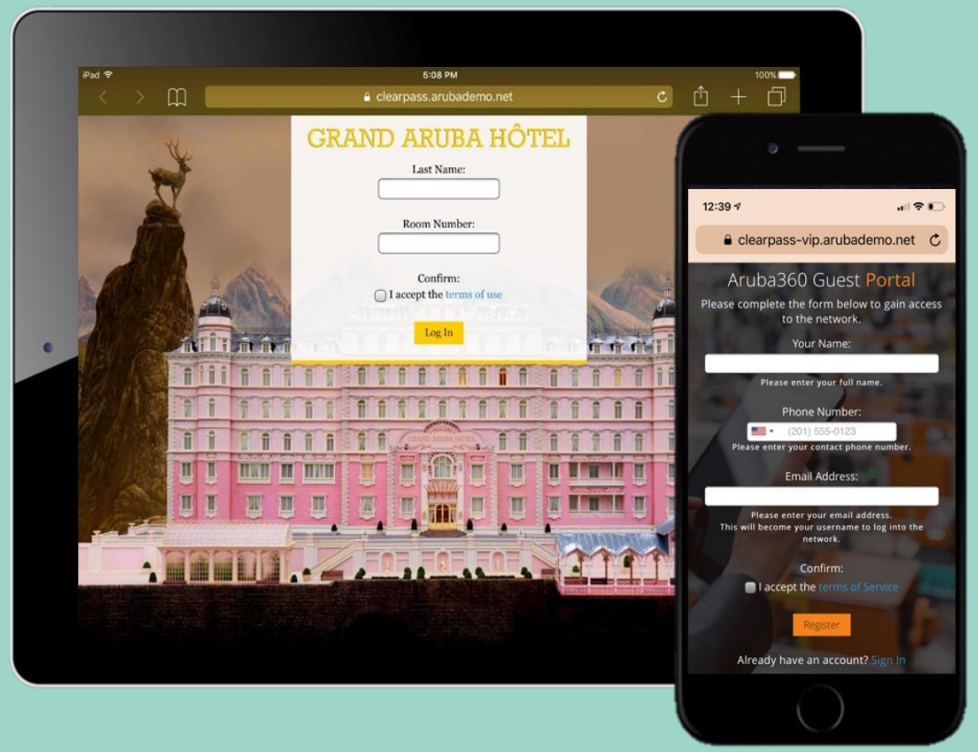
REMOTE LOCATION

ClearPass Policy Manager

# ClearPass Guest Access

- **브랜드 이미지** 및 컬러 적용
- **빌링**, 주요 **자산 관리** 및 **방문객 관리 시스템** 등과 연동 가능
- 고객에게 접근하고, **중요한 엔드 유저 정보**를 획득 가능한 플랫폼을 제공

## HOTEL GUEST PORTAL



# ClearPass Onboard

## Bring Your Own Device (BYOD)

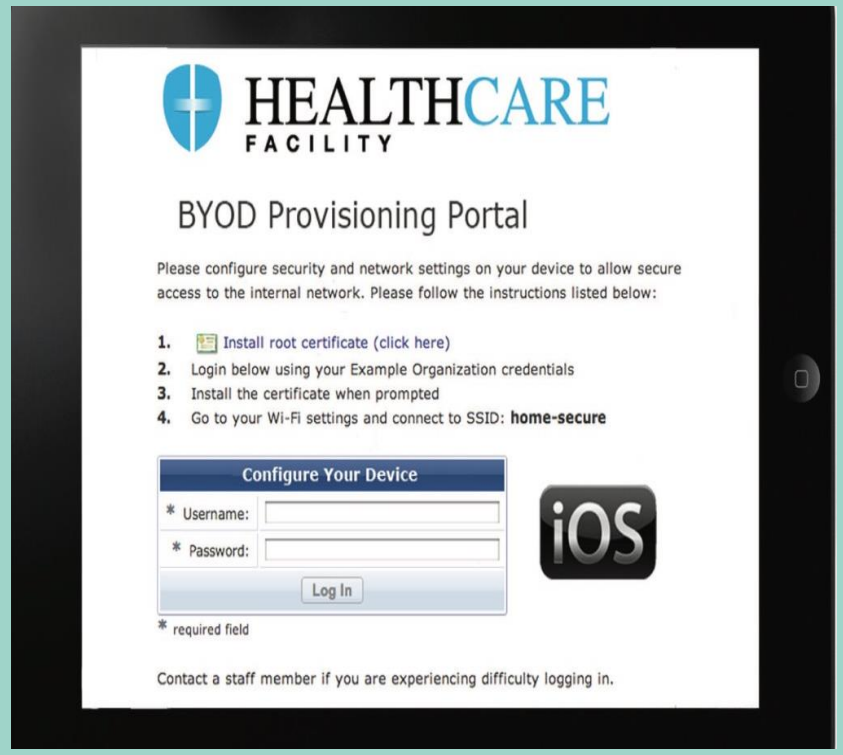
- 안전하게 네트워크 접속하도록 단말을 설정하는 것은 어려울 필요가 없음
- 네트워크 접속을 위한 단말 프로비저닝 때문에 발생되는 헬프데스크 티켓 수 감소
- Windows, MacOS, iOS, Android, Chromebook 및 Ubuntu 등 지원

## ID 라이프 사이클 관리

- 단밀 인증서를 생성하고 배포와 만료를 관리

## 단말의 기본 기능 설정

- iOS,: ActiveSync, 이메일, 캘린더, 장치 제한 등
- Windows: OnGuard 및 VIA와 같은 응용프로그램 설치




HOSPITAL PROVISIONING PORTAL

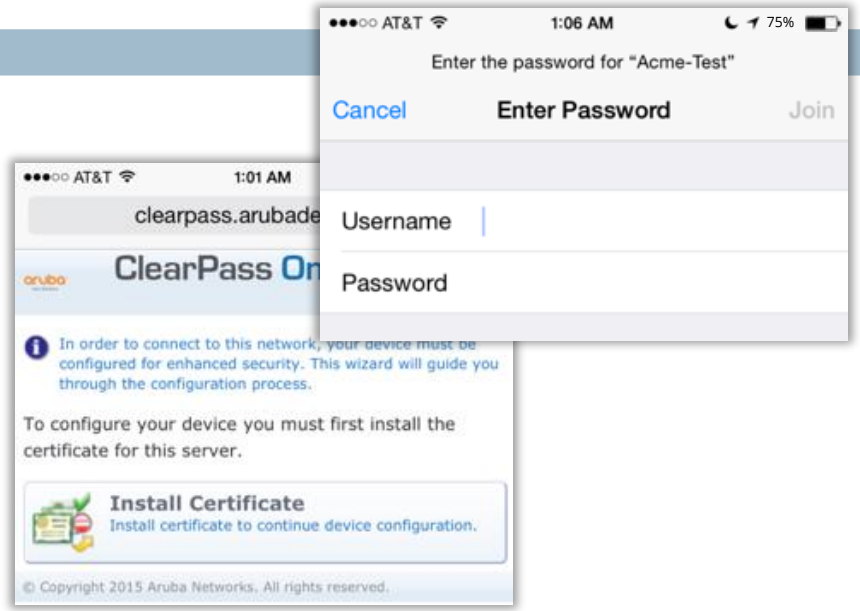
# BYOD 단말에 인증서 배포를 통한 인증

EASY — SECURE — NO PASSWORDS

1 사용자 단말을 포털로 리다이렉션

2 사용자는 단말 온보딩을 위해 계정 정보를 입력

3 자동으로 사용자를 적절한 네트워크 세그먼트로 이동



# BYOD 단말에 인증서 배포를 통한 인증

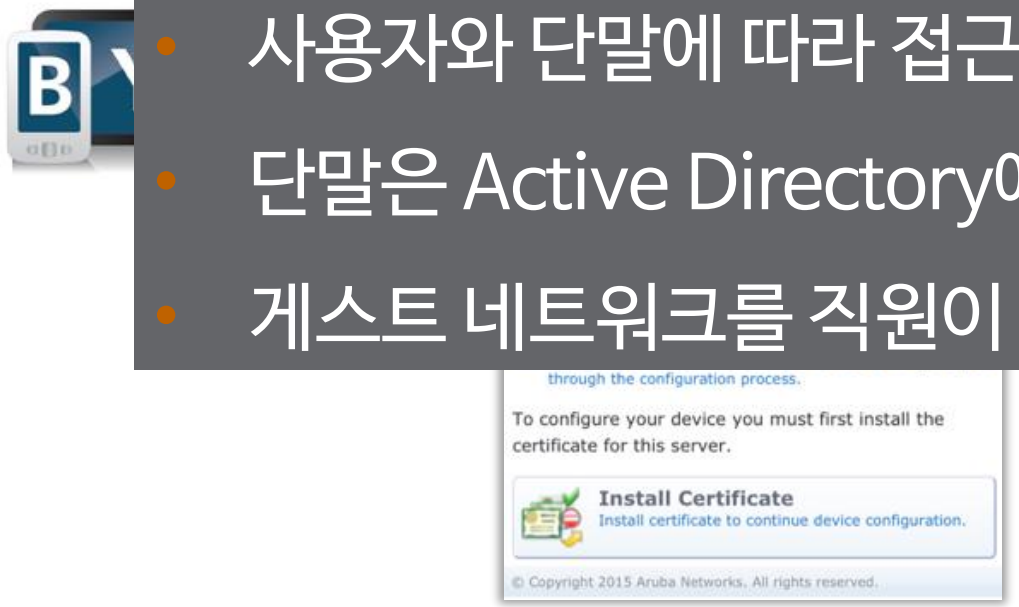
EASY | SECURE | NO PASSWORDS

1 사[illegible] 포[illegible]

2 [illegible]

3 [illegible]를 적절한 [illegible]트로 이동

- 관리자는 어느 단말이 onboarding 할 수 있을지 결정
- 사용자와 단말에 따라 접근 가능한 범위 부여
- 단말은 Active Directory에 조인되지 않음
- 게스트 네트워크를 직원이 사용할 필요 없음




# ClearPass OnGuard

## 인가 및 프로파일을 위한 추가적인 Context 제공

- 높은 보안의 네트워크 접근을 통제하기 위해 풍부하고 세분화된 정책을 활성화

## Device Posture 체크

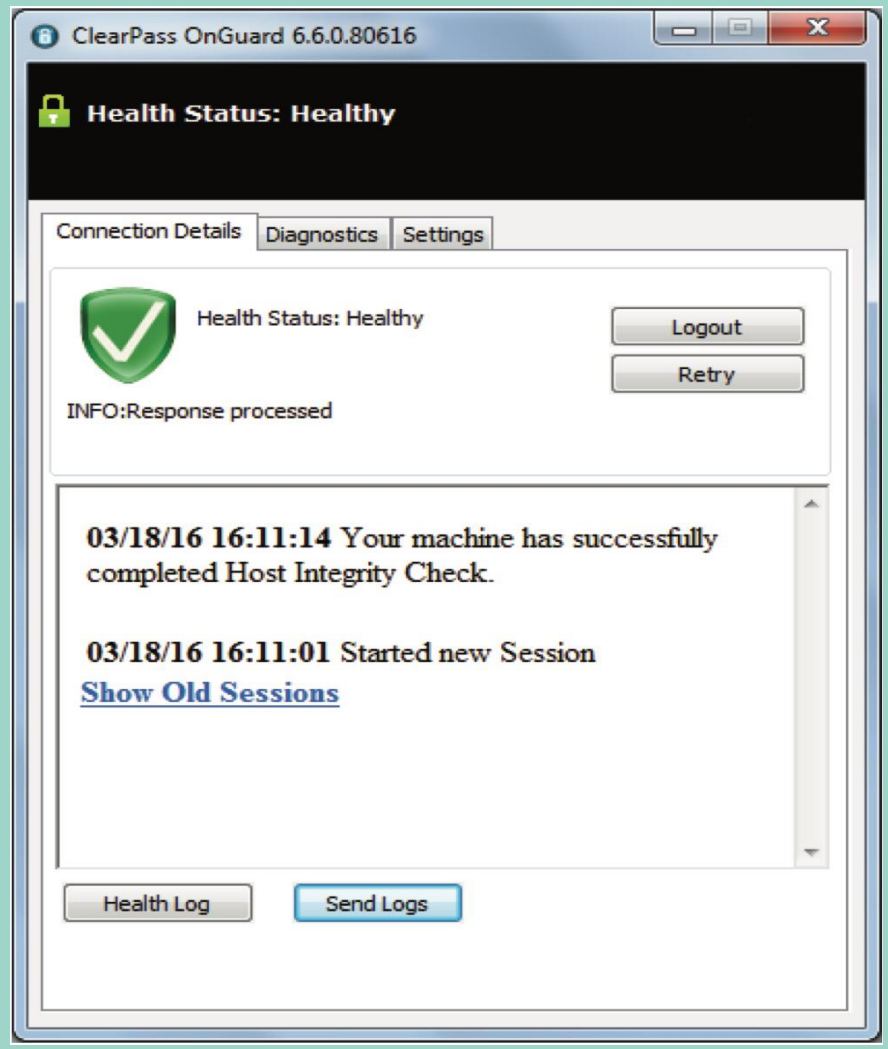
- Device Posture는 설치된 애플리케이션, 실행 중인 애플리케이션, 시스템 설정, 연결된 하드웨어 등의 디테일한 내용을 말함

## 에이전트 기반 (Persistent 또는 Dissolvable)

- Persistent 에이전트는 컴퓨터를 지속적으로 모니터링하고 ClearPass Policy Manager로 리포팅
- Dissolvable 에이전트는 네트워크에 연결될 때 즉시 실행되고 ClearPass Policy Manager의 웹 UI 로 로딩

## 관리 / 교정

- 단말이 보안 컴플라이언스를 위반했을 때 자동 또는 수동으로 보안지침을 준수하도록 선택



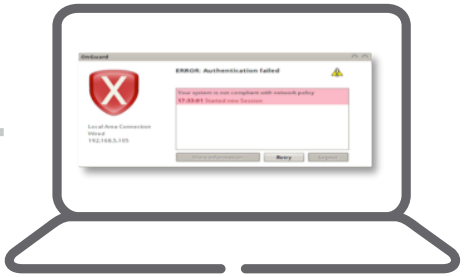

HEALTH STATUS

# 사용자 단말의 상태에 따른 정책 부여

네트워크 접근

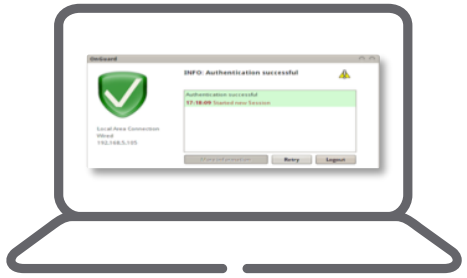
ClearPass OnGuard


컴플라이언스 위반 단말 탐지



유선, 무선 및 원격
네트워크에 대한 접속 차단

자동으로 단말 보안
위협 제거



네트워크의 위협 최소화
사용자 셀프서비스 허용

# Sample of 150+ Integrations including OT Visibility

## SECURITY

Attivo Networks
Carbon Black.
Check Point Software Technologies Ltd.
BlackBerry Cylance
FireEye
Fortinet
Juniper Networks
tenable
McAfee
paloalto Networks
Symantec
tenable
BIGFIX

## AUTH

Auth0
Azure Active Directory
Duo
Envoy
Cloud Identity
ImageWare Systems, Inc. Securing The Future
okta
Ping Identity
sine
team by wework
zoom

## NEW OT/ICS

Claroty
Indegy
CyberX
Nozomi Networks

## LOGGING

ArcSight
splunk>
IBM QRadar
solarwinds loggly

## HOTSPOT

Authorize.Net
PayPal
worldpay from FIS

## MESSAGING

Microsoft Teams
pagerduty
Twilio SendGrid
servicenow
slack
twilio

## PROPERTY

Agilysys
Oracle Micros
Opera
protel hotel software
Silverbyte

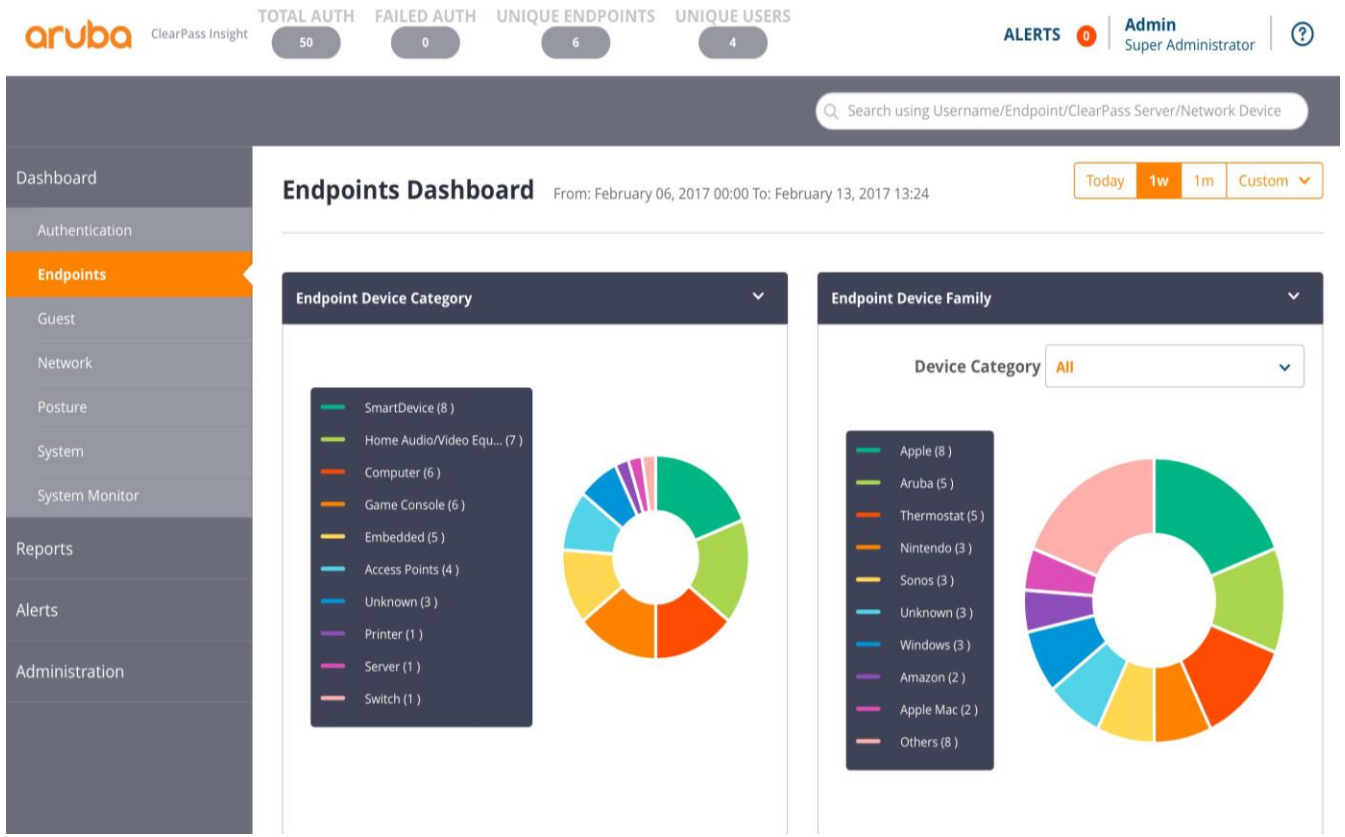
## EMM

BlackBerry
Citrix
G Suite
IBM MaaS360
Intune
jamf
mobileiron
SAP
SOTI
Workspace ONE

## SOCIAL

amazon
facebook
GitHub
Google
Instagram
LinkedIn
salesforce
twitter

# ClearPass Insight



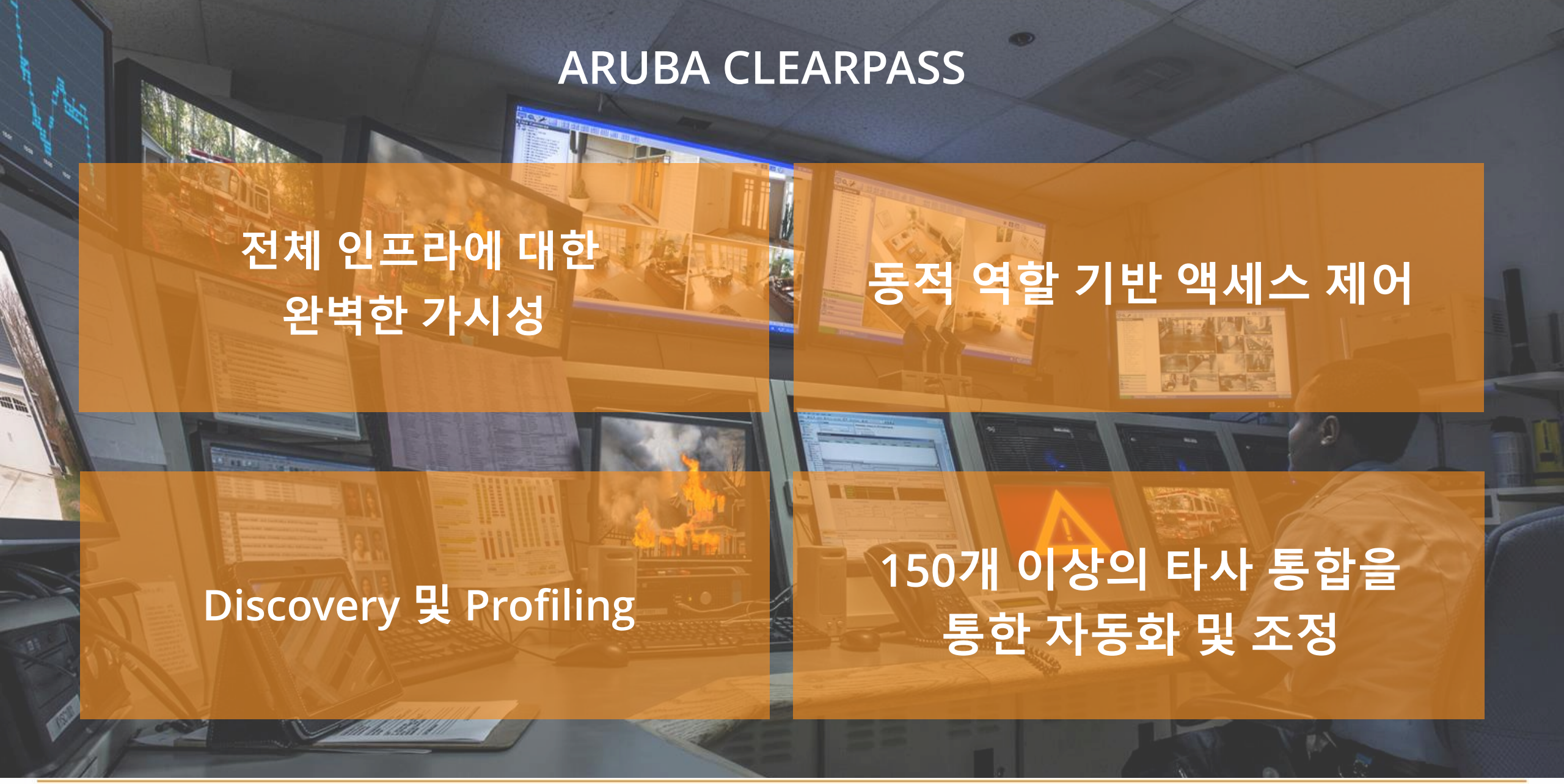

## 대시보드

- 인증 트렌드 식별
- 네트워크상의 단말 유형별 **시각화 제공**
- 네트워크의 게스트 접속 추적
- ClearPass 시스템 레벨의 **상태 모니터링**

## 유선 및 무선 네트워크 단말의 가시성 획득

- 유선 스위치 포트에 연결된 단말 확인을 위한 네트워크 **탐색** 수행

# ARUBA CLEARPASS



전체 인프라에 대한
완벽한 가시성

동적 역할 기반 액세스 제어

Discovery 및 Profiling

150개 이상의 타사 통합을
통한 자동화 및 조정

New Normal 시대에 HPE Aruba ClearPass를 통한
네트워크 액세스 보호 솔루션을 소개합니다

# Thank You

aruba
a Hewlett Packard Enterprise company

LANOASIS