

# ivanti

## 보안 제품 소개자료

Insung Digital

2022/04

# Agenda

What is Ivanti

Ivanti Connect Secure

Ivanti Neuron for ZTA

Ivanti Neuron for Secure Access

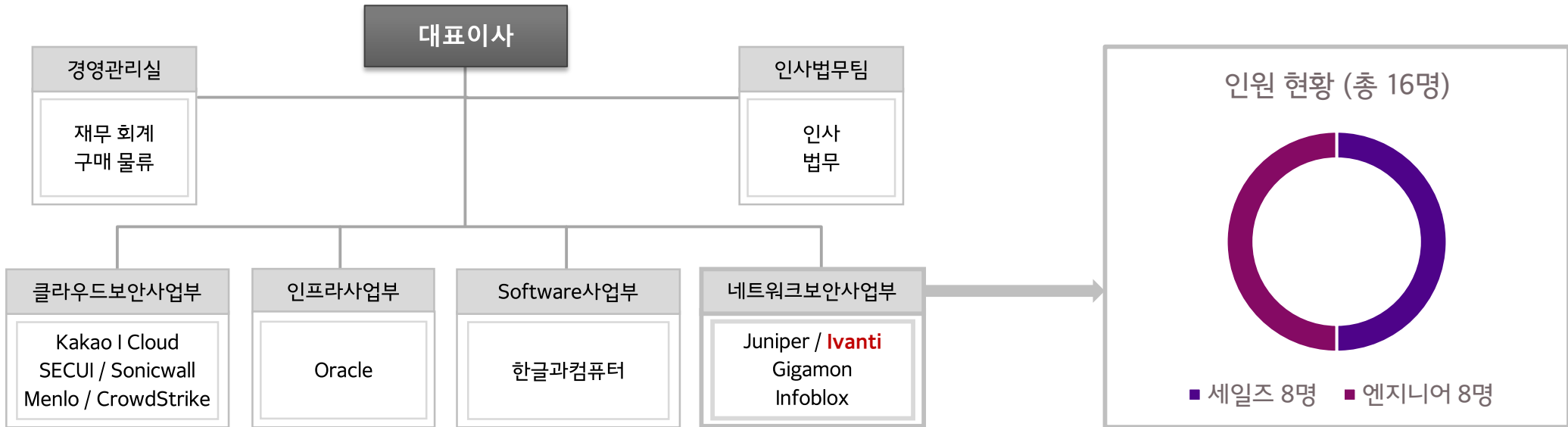
# What is Ivanti

Ivanti Connect Secure

Ivanti Neuron for ZTA

Ivanti Neuron for Secure Access

회사명	인성디지털	대표자	이인영
사업 분야	네트워크 솔루션 및 보안 솔루션, 기업용 Software, Cloud 서비스 등 IT Total 솔루션 600+의 채널 파트너 인프라를 통한 총판 영업		
주소	본사 : 서울 송파구 위례성대로 22길 28 (오금동, S2F빌딩) 3, 4층		
전화번호	전화번호 : 02- 2105-4500 팩스번호 : 02-2105-4670		
회사 설립년도	1998년 7월		
해당부문 종사기간	1998년 7월 ~ 현재 (23년 7개월)		



# IVANTI PRODUCT

## 사용자

- Zero Sign-On
- Anti-Phishing (MTD)
- Secure Productivity Apps
- Privilege Management

## 액세스

- Ivanti Neurons for Zero Trust Access
- Ivanti Neurons for Secure Access
- VPN
- NAC

## 디바이스

- Ivanti Neurons for (Risk-Based) Patch Intelligence
- Ivanti Neurons for (Risk-Based) Vulnerability Management
- Mobile Threat Protection
- Endpoint Threat Protection
- Device Control

## 애플리케이션

- Application Control
- Application Security & Correlation for Vulnerability Management

## 관찰 / 행동

- Neurons for Discovery
- Neurons for Edge Intelligence
- Neurons for Healing

**ivanti**

+



**mobileiron**

+



**Pulse Secure**

+



**cherwell**

+

**RISKSENSE**  
Acquired by Ivanti

**What is Ivanti**

**Ivanti Connect Secure**

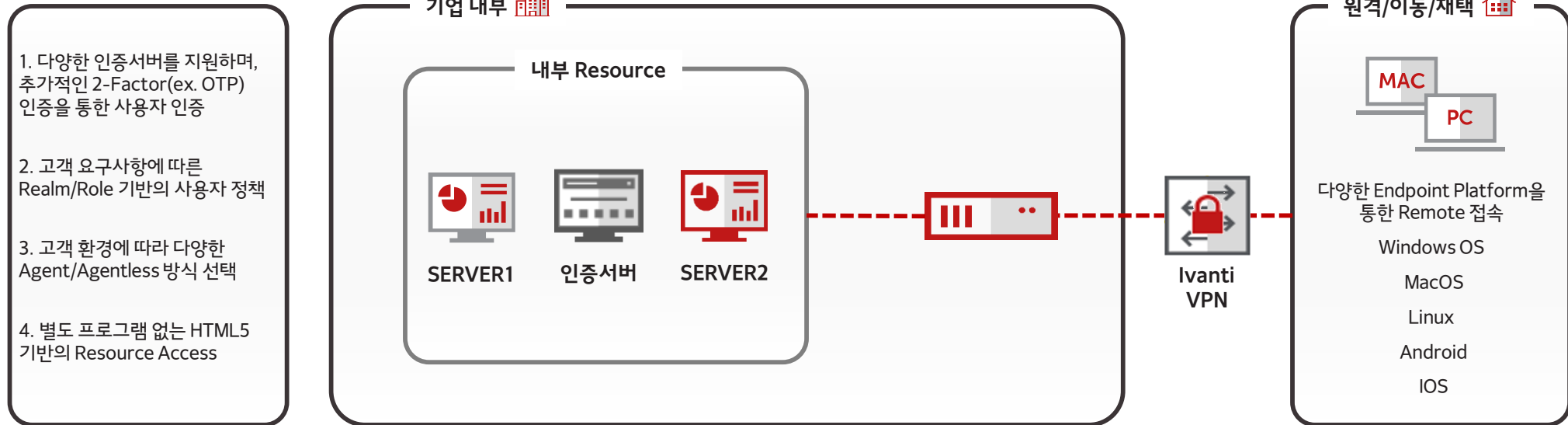
**Ivanti Neuron for ZTA**

**Ivanti Neuron for Secure Access**

# IVANTI CONNECT SECURE

## On-premise 및 Cloud 환경에 대하여 언제 어디서나 외부에서 안전하게 Access

- 네트워크(HTTPS)을 통하여 안전한 내부 자원 Access
- 다양한 Mobile 기기를 사용하여 언제 어디서나 SSLVPN 접속
- 보안 기능을 통하여 Endpoint Device의 보안 준수 여부 체크



# WHY SSLVPN

## 하이브리드 근무 환경으로의 전환

HOME > 뉴스 > 경제/교육

### “직원 업무 우선순위 변화...근무 방법·장소·시간도

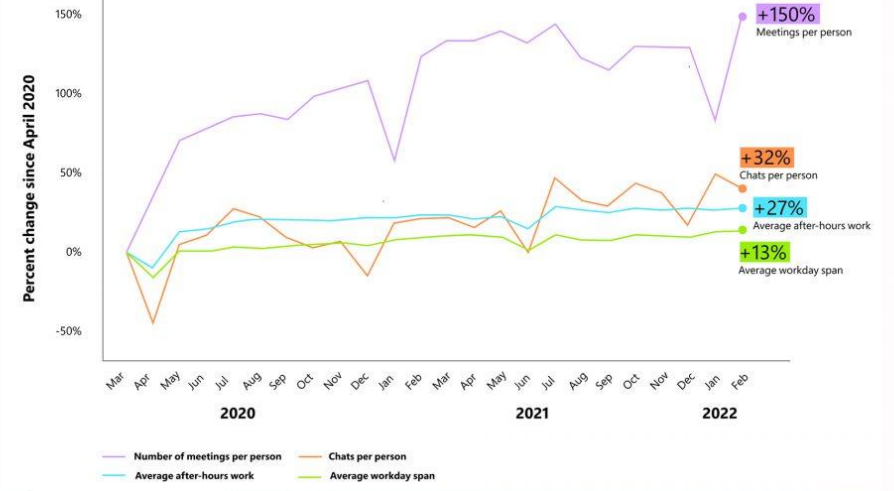
윤현기 기자 | 승인 2022.03.18 10:32 | 댓글 0

MS, 글로벌 업무 트렌드 반영한 '2022 업무동향지표' 발표  
팀 화합 위해 관리자에 많은 권한 부여해야...근무 시간 기준 설정 필요성도 피력

[데이터넷] 직원들의 업무 우선순위가 달라지고 있다. 개인의 목표와 워라밸을 더욱 중시함에 따라 근무 방법, 장소, 시간 등도 달라져야 한다는 분석이다.

18일 마이크로소프트는 이 같은 내용을 담은 '2022 업무동향지표(Work Trend Index)'를 발표하고 하이브리드 업무 활성화를 위한 새로운 로드맵을 공유했다.

[ 2022 업무동향지표 (Microsoft 발표) ]





# WHY SSLVPN

## 공공 및 금융권의 재택 근무 확대

HOME > 뉴스 > 소프트웨어

### 공공까지 넓어지는 원격근무,

윤현기 기자 | 승인 2022.03.12 11:18 | 댓글 0

재택근무 솔루션으로 급부상...초기 구축 부딪

[데이터넷] 코로나 팬데믹 이후 사무실뿐만 아  
우가 늘어나면서 이를 지원하기 위한 방안으로  
우드를 활용하기에 인터넷만 연결되면 언제 (단  
말이나 운영체제에 상관없이 서비스를 이용  
다.

HOME > 뉴스 > 보안

### [주목 2021] 코로나19가 바꾼 망분리... 공공·금융 재택/원격근무

김선애 기자 | 승인 2021.01.08 10:30 | 댓글 0

VPN 사용 원격 접속 가능 ... VDI-중계서버 이용-직접 접속 가능

[데이터넷] 코로나19는 공공·금융기관의 망분리 환경까지 변화시켰다. 공공·금융기관의 업무망은 외부에서 접속하지 못하도록 폐쇄된 환경을 유지해야 해 재택근무나 원격근무가 불가능했다.

코로나19로 공공·금융기관 임직원이 긴급하게 재택근무를 해야 하는 상황에 놓이자 일시적으로 재택근무를 가능하게 예외조치를 취했으며, 금융기관은 전자금융감독규정 시행세칙 개정에 따라 2021년 1월부터 모든 임직원이 상시 재택근무가 가능하게 했다. 단 전산센터 시스템 개발과 운영은 원격접속이 불가능하다.

# WHY SSLVPN

## 기업의 급격한 인프라 운영 환경의 변화로 인한 보안 이슈

HOME > 뉴스 > 보안

### “코로나기간 국내 기업 데이터 유출로 41억 손실”

김선애 기자 | 승인 2021.08.02 10:32 | 댓글 0

IBM “인증정보 도용·이메일 침해·사회공학 해킹·피싱으로 인한 피해 많아”  
사고 인지·대응 시간 287일로 늘어...클라우드 성숙도 낮을수록 피해 커  
AI·보안 자동화제로 트러스트 도입 기업 피해 낮아

[데이터넷] 코로나19 기간동안 우리나라 기업이 데이터 유출사고로 평균 41억1000만원의 손실을 입었으며, 데이터 유출 피해 건 당 피해 금액이 가장 큰 산업은 금융, 서비스, IT 였던 것으로 나타났다.

[ 2021 Report (IBM Security 발표) ]



20,000

Active Customers

80%

Fortune 50개 기업 중 40개

14

미 정부 주요 15개 기관 중 14개

20M

2천만 이상의 Endpoints

80%

Fortune 500개 기업 중 400개

200

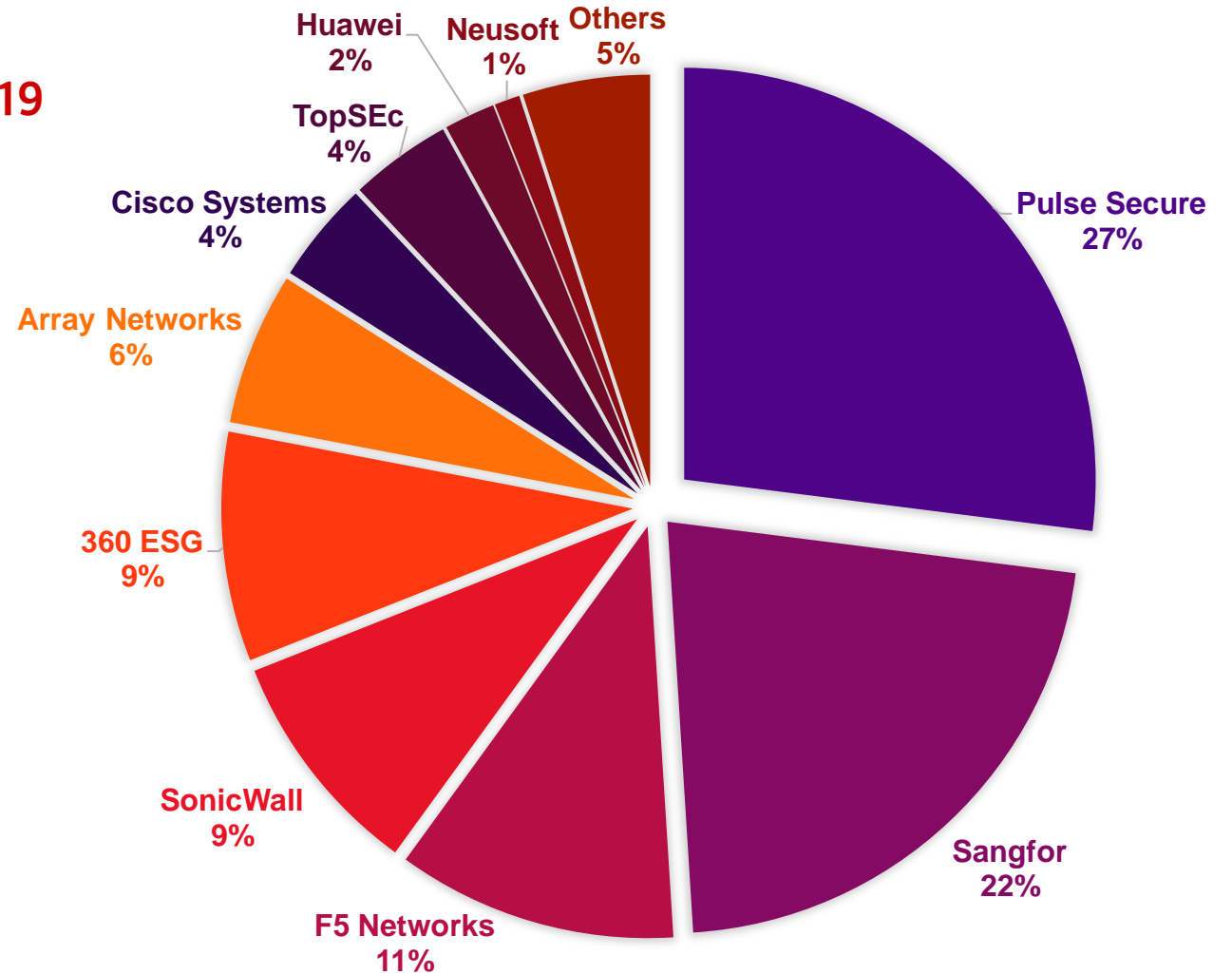
특허 출원

# IVANTI CONNECT SECURE

## 업계 1위의 SSLVPN 제품

### SSLVPN : Market Share by Revenue, APAC, 2019

- pulse secure strengthened its leadership position and increased its market share to 27%.
- The vendor continued to see strong adoption of its Pulse Access suites that provide secure access spanning multiple entry points - be it network, data center, cloud or application.
- Its has achieved good success in India, China, China and Hong Kong.



# IVANTI CONNECT SECURE



## Pulse Secure (acquired by Ivanti) Lauded by Frost & Sullivan for Leading the Secure Remote Access Market with Its Pulse Access Suite

USA - English

NEWS PROVIDED BY  
[Frost & Sullivan](#) →  
18 Dec, 2020, 15:40 IST

SHARE THIS ARTICLE



*The deep network visibility and Zero Trust secure access offered by Pulse Secure's (acquired by Ivanti) solutions have established the company as a valuable security partner in the era of remote working*

SINGAPORE, Dec. 18, 2020 /PRNewswire/ -- Based on its recent analysis of the Asia-Pacific secure remote access market, Frost & Sullivan recognizes [Pulse Secure®](#) (acquired by Ivanti) with the 2020 Asia-Pacific Secure Remote Access Company of the Year Award. Pulse Secure (acquired by Ivanti) demonstrated an impressive year-on-year growth of 29.2% in 2019, which was much higher than the industry average of 5.8%. This growth was mainly because of the healthy adoption of the company's Pulse Access Suite and the continual innovation of its flagship network access control solution.

# PSA SERIES

## Pulse Security Appliance Series



### PSA300 / PSA3000

- Max Concurrent SSL Users 200
- Max ESP Tunnel Throughput 200Mbps
- Max SSL Tunnel Throughput 100Mbps
- Login Late(Users/Sec) 20
- Interface 2 X 1GbE
- MGMT Interface -



### PSA5000

- Max Concurrent SSL Users 2,500
- Max ESP Tunnel Throughput 1Gbps
- Max SSL Tunnel Throughput 550Mbps
- Login Late(Users/Sec) 50
- Interface 2 X 1GbE
- MGMT Interface 1 X 1GbE



### PSA7000C/F

- Max Concurrent SSL Users 25,000
- Max ESP Tunnel Throughput 4.2Gbps
- Max SSL Tunnel Throughput 2.8Gbps
- Login Late(Users/Sec) 115
- Interface 4 X 1/10GbE
- MGMT Interface 1 X 1GbE

# ISA SERIES

## Ivanti Security Appliance Series



### Virtual (Cloud)

- Virtual Platform
  - VMware
- Cloud Platform
  - AWS
  - Microsoft Azure
  - Google Cloud Platform (예정)

Oct 2021



### ISA6000

- 컴팩트 사이즈 (1U)
- 기존 장비 대비 향상된 성능(2배 이상)
- 강화된 보안
- 성능 대비 전력 효율 강화
- 전반적인 HW 업그레이드

Q1 2022



### ISA8000

- 컴팩트 사이즈 (1U)
- 기존 장비 대비 향상된 성능(2배 이상)
- 강화된 보안
- 성능 대비 전력 효율 강화
- 전반적인 HW 업그레이드

Q2 2022

# IVANTI SECURITY APPLIANCE

## ISA6000 (PSA300/PSA3000/PSA5000 대응 모델)

Hardware / Performance Specifications	
Form Factor	1U
Supported Software	21.x version or above
Memory	16GB DDR4
Network Interfaces	Intel X550 NIC (2 x 10G BASE-T) / Intel I210A (2 x 1G BASE-T)
Storage	480GB SSD
Power Supply Unit	200W
Max Concurrent Users	2,500
Max Throughput (ESP Mode)	3.5 Gbps

**ISA6000**

- OS 및 SW 무결성을 위한 TPM Chip
- 보안 강화를 위한 최신 커널
- 사용자 경험을 위한 최신 REACT 프레임 워크



# IVANTI SECURITY APPLIANCE

## ISA8000 (PSA7000 대응 모델)

Hardware / Performance Specifications	
Form Factor	1U
Supported Software	21.x version or above
Memory	64GB DDR4
Network Interfaces	Intel XL710 NIC (4 x 10GE)
Storage	480GB SSD / 2 X 2TB HDD (RAID)
Power Supply Unit	400W
Max Concurrent Users	25,000
Max Throughput (ESP Mode)	N/A (Q2 2022 예정)

**ISA8000**

- OS 및 SW 무결성을 위한 TPM Chip
- 보안 강화를 위한 최신 커널
- 사용자 경험을 위한 최신 REACT 프레임 워크

# IVANTI SECURITY APPLIANCE

## 성능 비교 (ISA6000 vs PSA5000)

구분	ISA6000 (Hardware)	ISA6000-V (VMware)	PSA5000 (Hardware)	PSA5000 (VMware)
MAX Concurrent Users	2,500	2,500	2,500	2,500
MAX Tunnel Throughput (ESP Mode)	3.5Gbps	3.5Gbps	1Gbps	514Mbps
RAM	16GB	16GB (Recommended)	8GB	8GB (Recommended)
Interface	2 X 1/10GbE + 1 X 1GbE	Configurable on host	3 X 1GbE	Configurable on host



# IVANTI CONNECT SECURE

## 주요 기능

### API를 통한 Manage

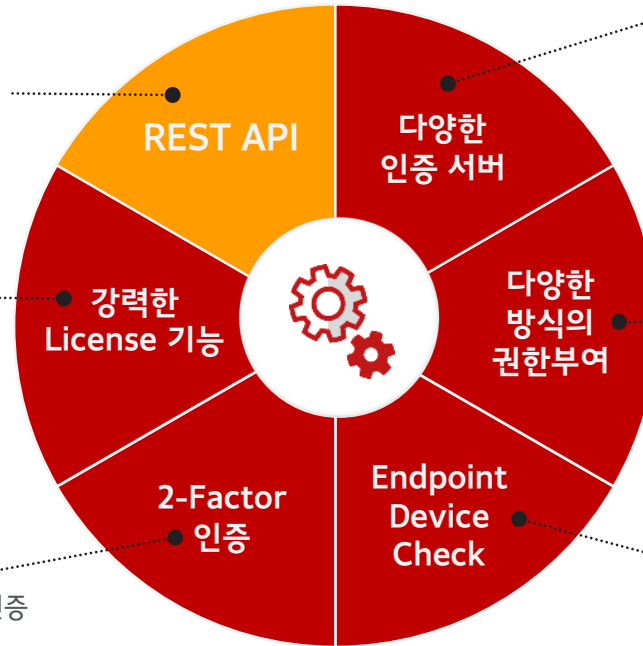
- REST API를 통한 관리의 효율성 증대
- Monitoring/Configuration 등 다양한 메뉴에 대한 Method URL 지원

### License를 통한 추가 기능

- 별도의 License Server를 통한 User License 관리
- 예외적인 상황을 대비한 Emergency License
- Agentless 기반의 HTML5 방식과 같은 기능 License

### 2-Factor 인증

- 3rd party 솔루션 연동을 통하여 OTP / SMS / Mail 등의 추가 인증
- 별도의 솔루션 연동 없이, Google OTP App을 이용한 OTP 추가 인증



### 다양한 type의 인증서버 연동을 통한 사용자 인증 보안

- On-premise type (Local / AD / LDAP / RADIUS 등)
- SAML type (Azure AD , Octa 등)
- MDM type (MS Intune, Air watch, Mobile iron)
- TOTP type (Google OTP)

### Realm & Role 기반의 세분화된 정책 설정

- Sign-page / 인증 절차 / 정책 설정 등을 Group별 분리
- Split tunneling / 다양한 Session option 지원

### Host Checker 기능을 통한 Device 보안 요구사항 Check

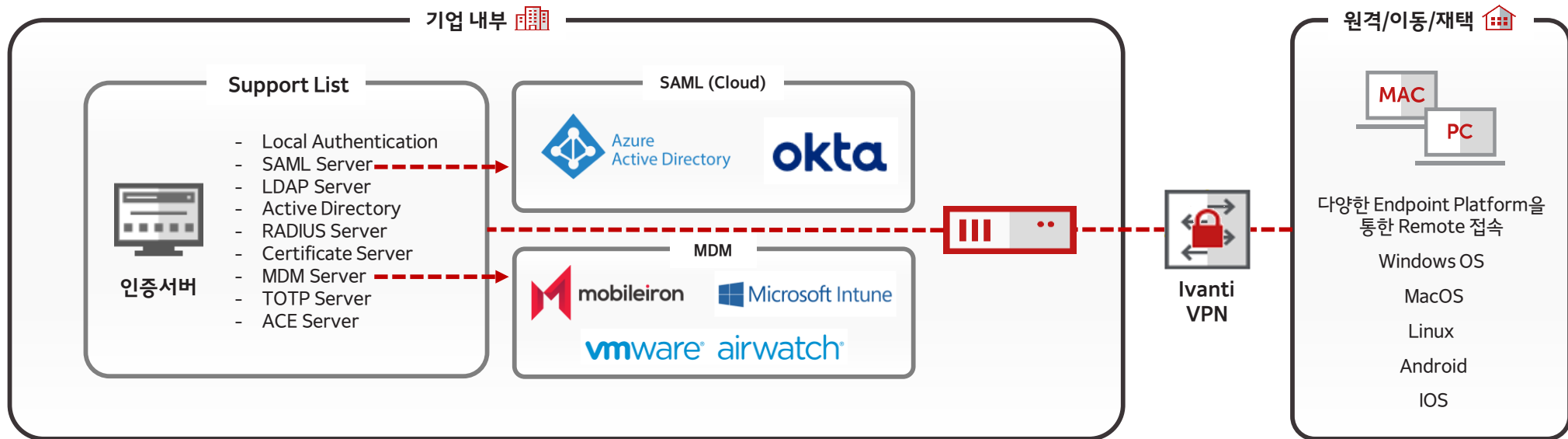
- AV / Firewall / OS / Process / File 등의 항목을 통한 보안 Check
- MAC Address / Register Key 등을 통하여 특정 Device만 허용

Leading SSL VPN Solution for Enterprises

# IVANTI CONNECT SECURE

## On-premise 및 Cloud 기반의 다양한 인증 서버 지원

- 다양한 On-premise 인증 서버 지원
- 다양한 MDM Solution 연동을 통하여 Mobile 기기에 특화된 단말 보안 지원
- Cloud 인증서버를 통한 SAML2.0 지원



# IVANTI CONNECT SECURE

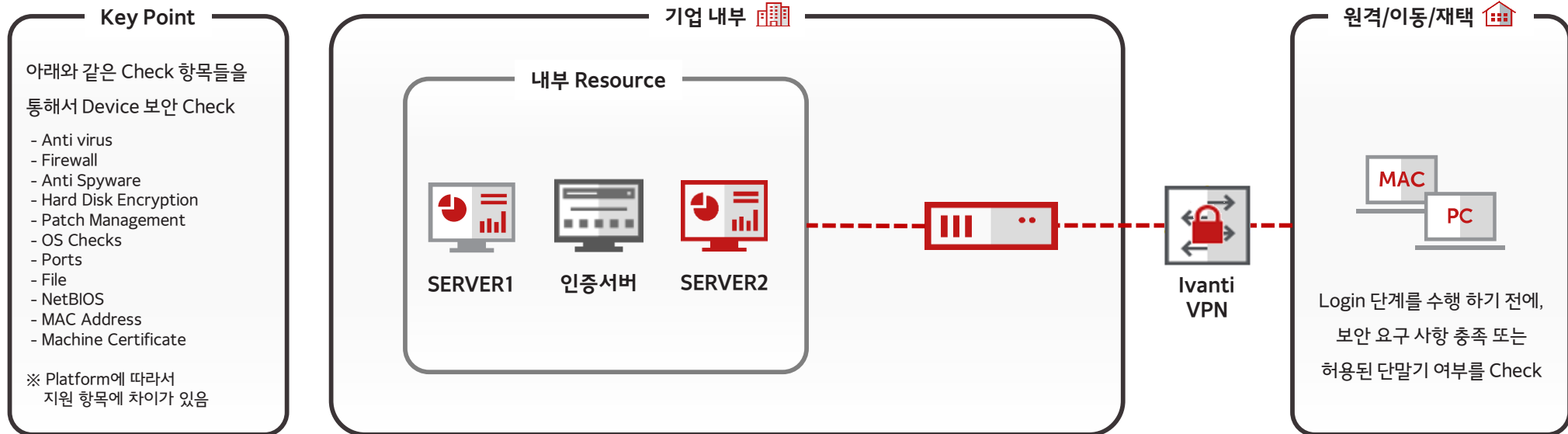
Realm / Role 기반의 사용자 Group별로 Login URL / 인증 방법 / 사용자별 권한 등을 각각 부여

구분	A 사용자 Group		B 사용자 Group		C 사용자 Group
Sign-in URL					
사용 대상	협력사		직원		기타
사용 대상	1차 협력사	2차 협력사	임원	사원	고객
인증 방식	Local Auth	Local Auth	AD + OTP	AD	Certificate
접근 권한	ERP / 파일서버	ERP	ALL	Web 서버 Mail 서버 ERP / 파일서버	고객 Web 서버

# IVANTI CONNECT SECURE

## Host Checker (Endpoint Device 검사를 통하여 추가 보안)

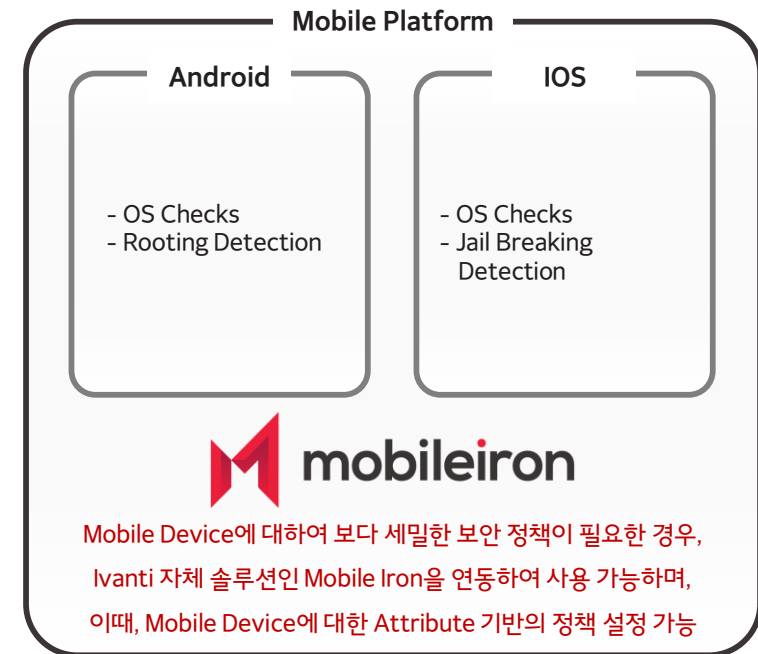
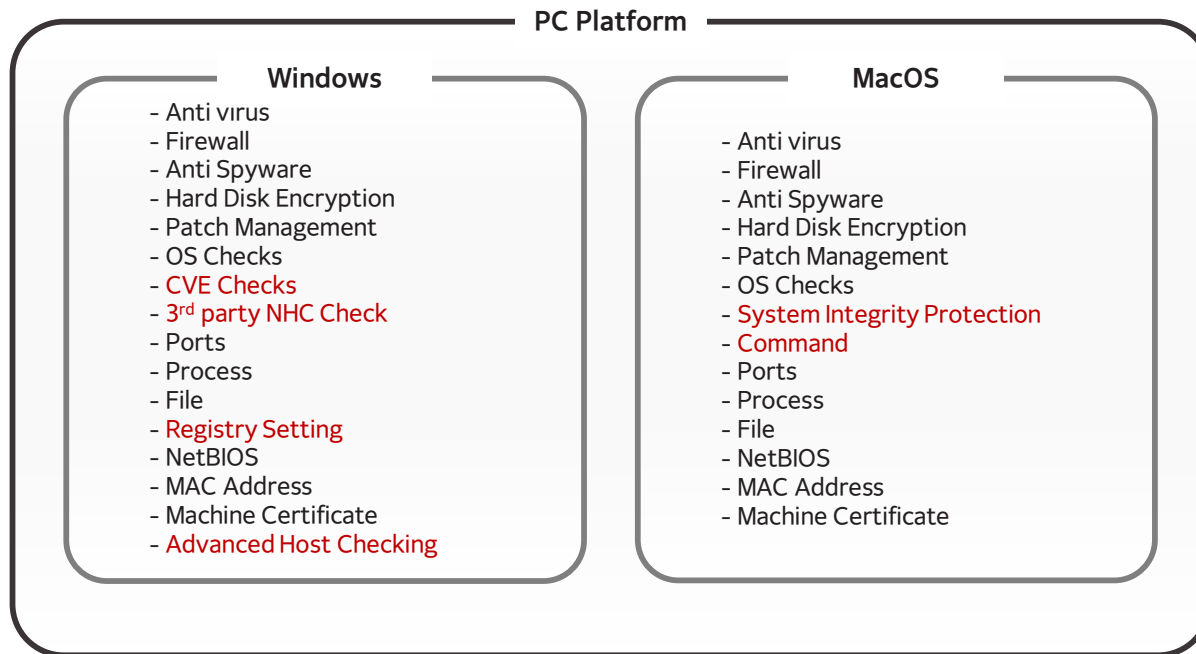
- Login 단계를 수행하기 전에 접속을 시도하는 단말기에 대하여 추가 보안 Check
- 다양한 Check 항목을 통하여, 보다 세부적인 보안 Check가 가능
- 보안 Check 결과에 대한 상세 로그 출력 / 안내 페이지 커스터마이징 지원



# IVANTI CONNECT SECURE

## Endpoint Device 검사 항목 List

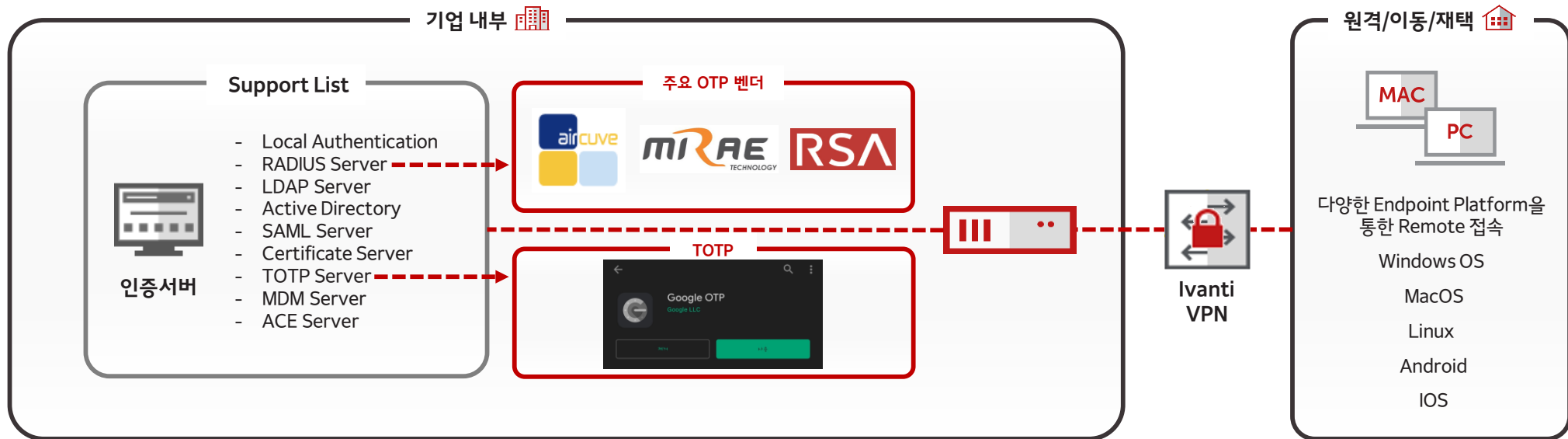
- Login 단계를 수행하기 전에 접속을 시도하는 단말기에 대하여 추가 보안 Check
- 다양한 Check 항목을 통하여, 보다 세부적인 보안 Check가 가능
- 보안 Check 결과에 대한 상세 로그 출력 / 안내 페이지 커스터마이징 지원



# IVANTI CONNECT SECURE

## 2-Factor 인증 (ex. OTP)

- ICS에서 연동 가능한 인증 서버들은 대부분 2차 인증 서버로도 사용 가능
- 이 외에, 추가적으로 OTP, SMS, Mail 기반의 2-Factor 사용 가능 (로그인 페이지 커스터마이징 필요)
- OTP의 경우, 별도의 3rd Party 솔루션 없이 Google OTP 어플을 이용한 2-Factor 구성 가능

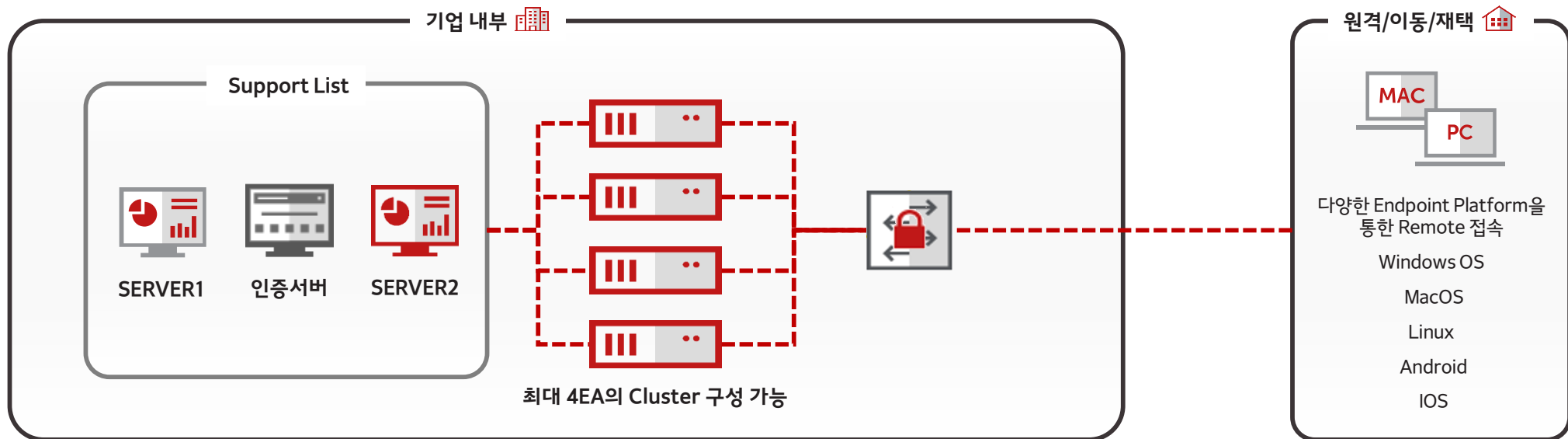




# IVANTI CONNECT SECURE

## Cluster

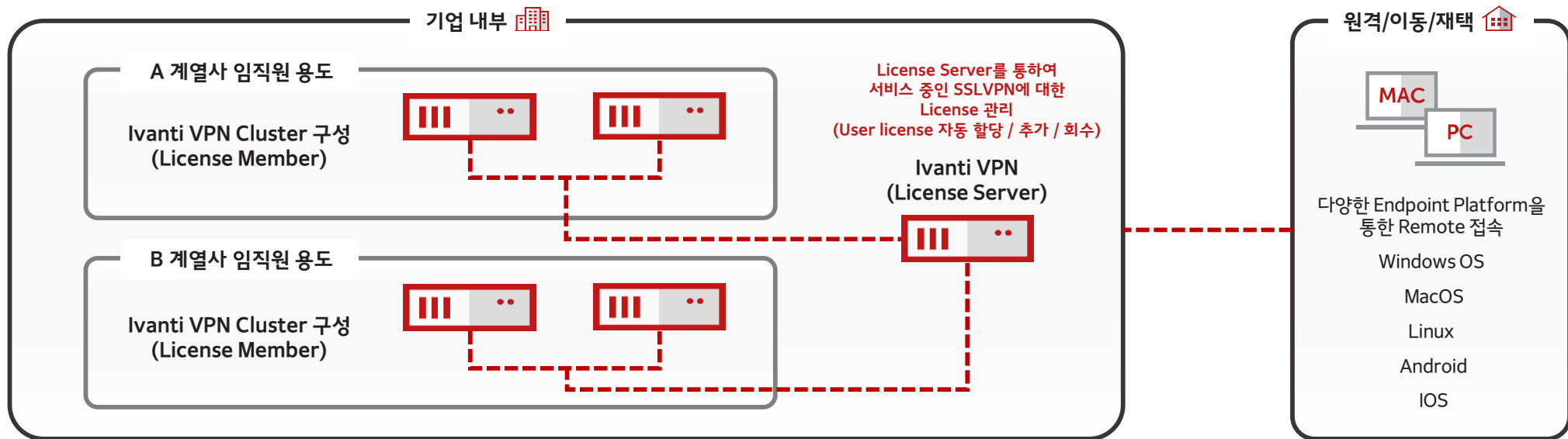
- 별도의 이중화 기술을 사용하여 Cluster 구성이 가능
- Cluster 구성 시, 각각의 Node에 User License 등록이 필요하며, 구성(A/A or A/S)에 상관없이 모든 Node의 User 라이선스를 사용 가능
- Endpoint Device(PC or Mobile)종류에 관계 없이, 단일 User License 사용
- 특정 Node에 문제가 발생 시, Grace Period 동작에 의하여 사용 가능한 전체 User License가 적용 됨



# IVANTI CONNECT SECURE

## License Server

- 별도의 License Server를 통해서 전체 User License를 통합 관리
- 상황에 따라 필요한 만큼 관리자가 직접 User License 조절 가능(ex. License 증설 / 축소)
- 그 외에, 설정에 따라 License Server에서 자동으로 License 할당 / 회수 가능



# IVANTI CONNECT SECURE

## Emergency(In Case of Emergency : ICE) License

- 예측 불가능한 상황에서 신속한 License 추가를 위한 Emergency License
- Emergency License 활성화 시, 즉시 Full User License를 사용 가능
- Activation 방식의 License

### IN CASE OF EMERGENCY LICENSE

#### "IN CASE OF EMERGENCY" (ICE) LICENSE OPTION

Enabling Business Continuity with Remote Access



#### Product Overview

Pulse Secure ICE license option provides a quick resolution when the unexpected happens, delivering the ability to handle extreme peak demands and to support continued business operations. The ICE license option is applied to the Pulse Secure PSA Series appliances.

#### Product Description

SSL VPNs can help keep organizations and businesses functional by connecting people — even during the most unpredictable circumstances. When hurricanes, terrorist attacks, transportation strikes, pandemics, virus outbreaks or other potentially catastrophic events occur, they can result in the quarantine or isolation of entire regions or groups of people for an extended period of time. Through the ICE license option, organizations can instantly address a dramatic peak in demand for remote access in cases of emergency by supporting additional users on physical and virtual Pulse Secure PSA Series appliances.

It allows using the maximum capacity of the underlying hardware for a temporary period.

### Key Point

- ◆ 아래와 같은 긴급한 상황 발생 시, 한꺼번에 많은 사용자를 커버할 수 있도록 필요한 기간 동안만 활성화 하여 사용
  - Pandemic (ex. COVID-19)
  - Natural disaster
- ◆ ICE License는 최대 8주이며, 5분 단위로 Count 됨
- ◆ 구성(ex. Cluster)이나 제품 모델, 기존에 등록된 Permanent License에 대한 제약 없이 사용 가능
- ※ EVAL(데모) License가 활성화된 장비에서는 ICE 사용 불가능

# IVANTI CONNECT SECURE

## REST API

- Configuration을 위한 GET/PUT 등의 Method URL 제공
- ICS의 XML Configuration과 유사한 JSON 형식의 설정
- Admin 계정 단위의 REST API Access 제어

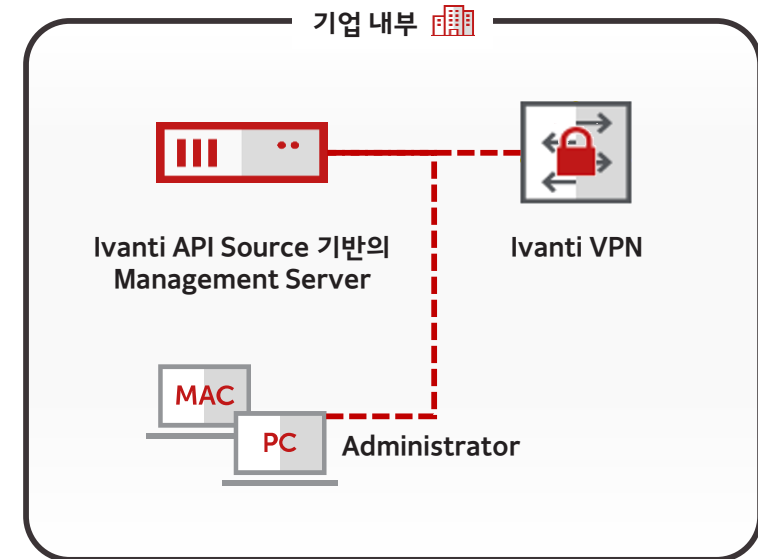
각 OS 버전에 대한 공식적인 API 연동 Guide 제공

```
Request
Fetch default number of active sessions (default=200)
curl -X -u <api-key>: https://<pcs-ip>/api/v1/system/active-users

Example:
curl -X -u K727xS4kNv1++kcViamCCiUzEBqMSF+sHKar4EcKY=: https://10.209.125.4/api/v1/system/active-users
Fetch specified number of active sessions
curl -X -u <api-key>: https://<pcs-ip>/api/v1/system/active-users?number=<number>

Example:
curl -X -u K727xS4kNv1++kcViamCCiUzEBqMSF+sHKar4EcKY=: https://10.209.125.4/api/v1/system/active-users?number=250

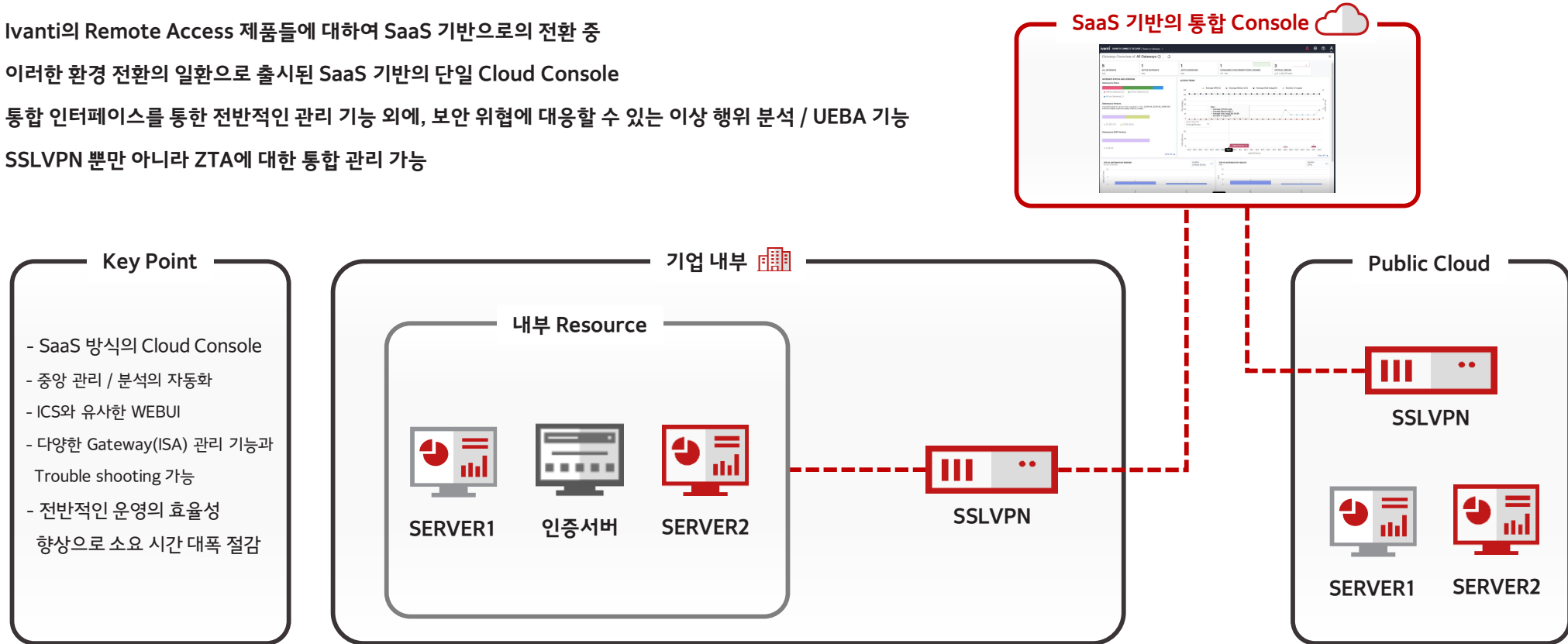
Response
Content-Type: application/json
{
  "active-users": {
    "active-user-records": {
```



# IVANTI CONNECT SECURE

## Neurons for Secure Access 연동

- Ivanti의 Remote Access 제품들에 대하여 SaaS 기반으로의 전환 중
- 이러한 환경 전환의 일환으로 출시된 SaaS 기반의 단일 Cloud Console
- 통합 인터페이스를 통한 전반적인 관리 기능 외에, 보안 위협에 대응할 수 있는 이상 행위 분석 / UEBA 기능
- SSLVPN 뿐만 아니라 ZTA에 대한 통합 관리 가능



# IVANTI SECURITY APPLIANCE

## 다양한 Endpoint Platform을 지원 - PC

### Qualified Platform

Platform	Operating System
Windows	Windows 11 Version 21H2 Windows 10 Version 21H1 Windows 10 Version 20H2 Windows 8.1 Enterprise, 64 bit
Mac OS X	macOS Monterey 12.0.1 macOS Big Sur 11.4 macOS Big Sur 11.1 Apple Silicon 11.1 macOS Catalina 10.15.6
Linux	Ubuntu 20.04.1 Fedora 32 Debian 10.6 RHEL 7 RHEL 8 CentOS 8.2.2004

### Compatible Platform

Platform	Operating System
Windows	Windows 10 Version 2004 Windows 10 Version 21H2 Windows 10 Version 1903 Windows 10 Redstone 5 Version Windows 10 Redstone 4 Version 1803 Windows 10 Version 1909 Windows 10 32 and 64 bit Windows 8.1 non-Enterprise, 32 and 64 bit
Mac OS X	macOS Big Sur 11.6 macOS Big Sur 11.5 macOS Big Sur 11.3.1 macOS Big Sur 11.2 Apple Silicon 11.2 macOS 10.15.3, 64 bit macOS 10.15.2, 64 bit macOS 10.13, 64 bit
Linux	Ubuntu 18.04 LTS Fedora 30 Debian 10.X RHEL 8.X CentOS 8.X

# IVANTI SECURITY APPLIANCE

## 다양한 Endpoint Platform을 지원 - Mobile

OS Type	Qualified Version	Qualified Devices	Compatible Version	Compatible Devices
iOS	15.0.2, 15, 14.7.1, 13.2, 12.5.4	iPhone11, iPhone Xs, iPhone X, iPhone SE, iPhone 6S, iPhone 6S+, iPhone 6+, iPad Pro	12.x, 13.x, 14.x, 15.x	Various
Android	8.0, 8.1, 9.0,10.0, 11.0, 12.0	Google Pixel 4A, Google Pixel 5, Galaxy s21, Samsung Galaxy S10 Note, Samsung Galaxy S20, S7, S8, S9, S10, OnePlus 6, Google Nexus 6P, Google Pixel 2, Google Pixel 3 XL	8.0, 8.1, 9.0,10.0,11.0, 12.0	Various

# IVANTI CONNECT SECURE

## 레퍼런스

### 그룹사



### 제조 / 건설 / 공공



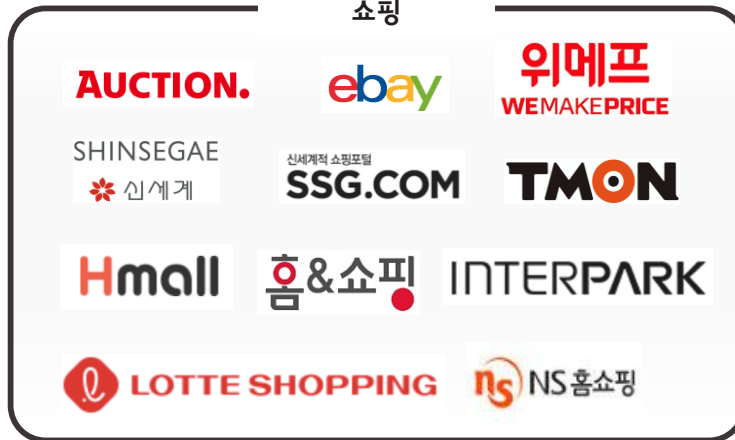
### 금융



### 포털 / 게임



### 쇼핑



### 통신 / 교육





# IVANTI CONNECT SECURE

## 벤더 기능 비교자료

Feature		Ivanti	F5	Ctrix	SecuWiz
보안	SSL / ESP 방식의 Layer3 SSL VPN 지원	O	O	X	X
	네트워크 Access 권한이 부여되기 전에 Endpoint 장치의 보안 정책 요구 사항을 충족하는지 검사 지원 (Desktop)	O	O	O (Windows, Mac)	O
	네트워크 Access 권한이 부여되기 전에 Endpoint 장치의 보안 정책 요구 사항을 충족하는지 검사 지원 (Mobile)	O	O	X	O
	Two-Factor 인증 지원	O	O	O	O
	터널 연결 후 ACL 기능으로 허용된 자원만 접속 지원	O	O	O	X
사용자 제어	Endpoint 장치가 네트워크 연결 시 항상 터널 활성화 기능 (Always-on VPN)	O	O	O	X
	Multiple URL 기능	O	O	O	O
	세분화된 감사 및 로깅 기능 지원	O	O	O	O
	장비 이중화 구성 시 클러스터내의 유저 라이선스 공유 사용	O	X	X	X
범용성	Android OS / IOS 단말 지원	O	O	O	O
	Windows / Mac / Linux OS 지원	O	O	O	O
	Cloud 환경에서 서비스 지원 (AWS, Azure, GCP)	O	O	O	X
	가상 어플라이언스 플랫폼 지원	O	O	O	X
	Google OTP 연동 지원	O	O	O	O

# IVANTI CONNECT SECURE

## 벤더 기능 비교자료

	Feature	Ivanti	F5	Ctrix	SecuWiz
편의성	벤더 자체 MDM 솔루션 보유 및 통합 연동 지원	O	X	X	X
	Single-Sign On(SSO) 연동 지원	O	O	O	O
	유저 ID별 다중 VPN session 지원	O	O	O	O
	FQDN 기반 Split Tunneling	O	O	O	X
	Clientless HTML5 Access 지원 (Citrix XenApp, VMware View Blast)	O	O	O	X
	Clientless RDP/Telnet/SSH Session using HTML5 Browsers 지원	O	X	X	X
	모바일 전용 APP 지원	O	O	O	O
	긴급 라이선스 지원 (In Case of Emergency (ICE) license)	O	X	X	X
	License Server를 통한 장비 별 유저 라이선스 재 할당 기능 지원	O	X	X	X
	RESP API 지원	O	O	O	X
	공지 팝업창 기능 지원	O		O (개발 필요)	

What is Ivanti

Ivanti Connect Secure

**Ivanti Neuron for ZTA**

Ivanti Neuron for Secure Access

# IVANTI NEURON FOR ZTA

## Zero Trust의 구성 요소



**ID**  
강력한 인증을 사용하여 보안을 확보



**Device**  
Device의 가시성 확보, 규정 준수 및 상태 확인



**Application**  
적절한 App 허용 및 실시간 분석, 모니터링 및 제어



**데이터**  
경계 기반의 데이터 보호에서 데이터 기반의 보호로 전환



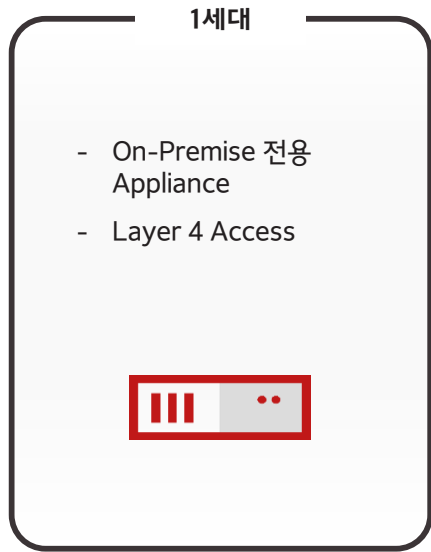
**인프라**  
공격 및 변칙을 감지하고 자동으로 위험 행동을 차단



**네트워크**  
사용자의 위치(내/외부)에 상관없이 모든 통신을 암호화

# IVANTI NEURON FOR ZTA

## 원격 접속에서 Zero Trust 기반 접속으로 전환



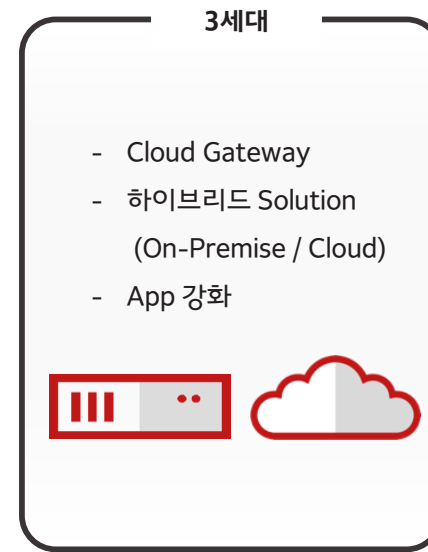
2010년 이전

NEOTERIS / NETSCREEN



2010- 2015

JUNIPER NETWORKS



2015 - 2020

PULSE SECURE



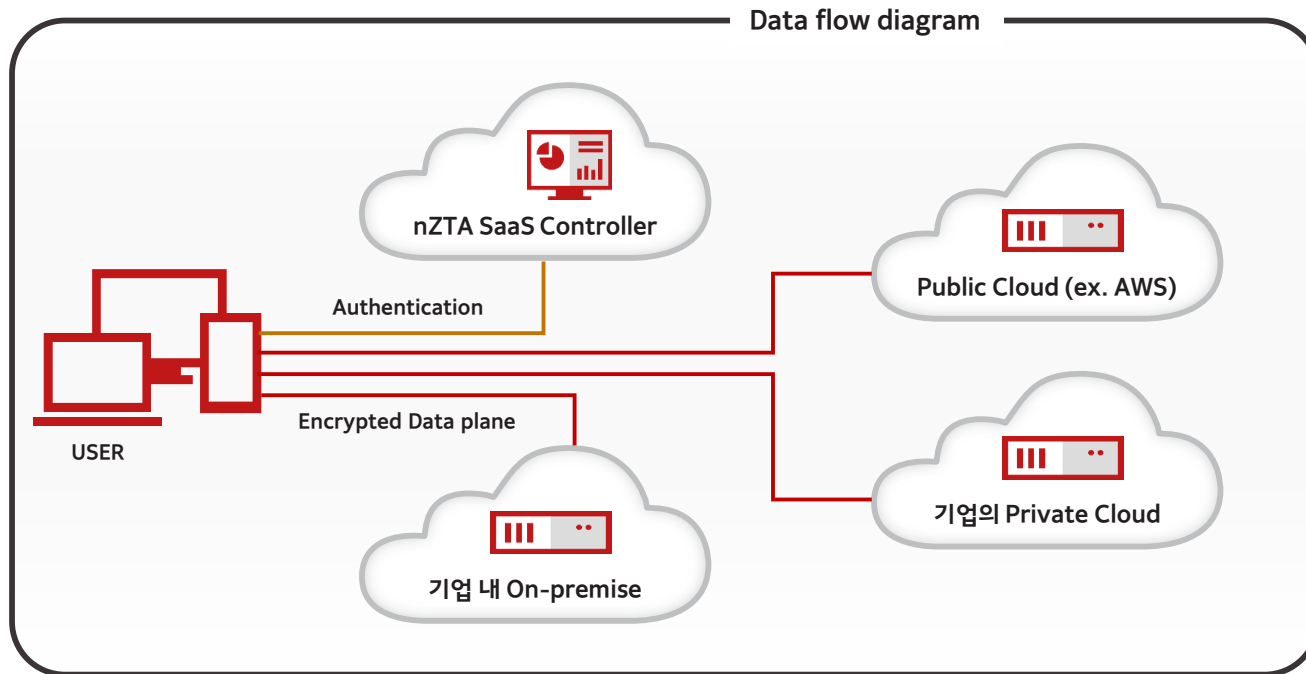
현재

IVANTI

# IVANTI NEURON FOR ZTA

## Flow for communication

- Client는 ZTA SaaS Controller를 통한 사용자 인증
- 각 지점(HQ, Private / Public Cloud)의 Gateway와 ZTA SaaS Controller 간의 제어 통신
- Client는 로그인 후, 각 지점의 모든 Gateway와 암호화 통신 가능



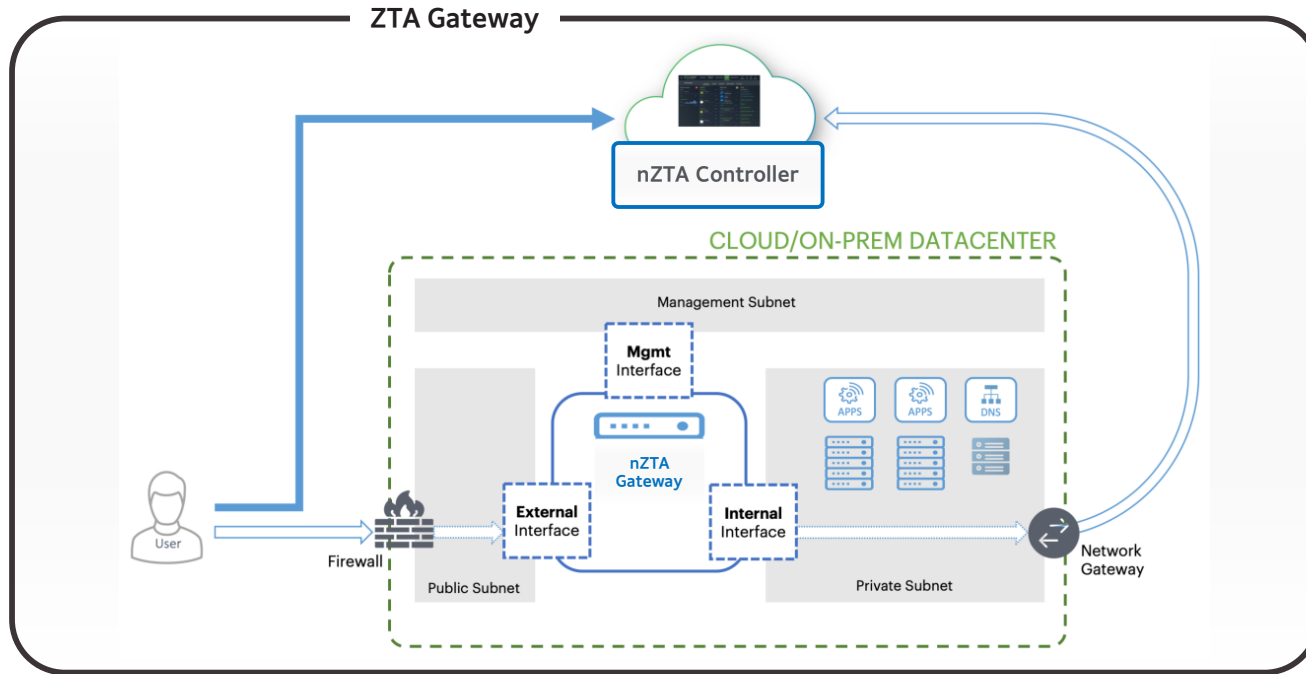
## Key Point

- ◇ ZTA SaaS Controller를 통해서 사용자 인증을 거치기 때문에, 각 GW별로 접속할 필요 없이, 모든 GW에 대한 Tunnel 통신이 가능
- ◇ 접속을 시도하는 모든 Device에 대하여 예외 없이 등록 과정을 거치며 관리 됨

# IVANTI NEURON FOR ZTA

## ZTA Gateway 구성도

- ZTA Gateway는 Appliance type이 아닌 Software type으로 Virtual OS / Public Cloud 등에 설치하여 사용
- Interface 구성 및 기본적인 Communication Flow는 아래와 같음
- SSLVPN의 구성과 유사하나, External/Internal interface의 경우 방향에 따라서 외부와 통신이 가능해야 한다



### Key Point

- ◇ VMware 기준 권장 사양
  - 4 vCPU's & 8 GB memory
  - 8 vCPU's & 32GB memory
- ◇ External 인터페이스는 외부에서 Access가 가능해야 함 (공인 IP 필요)
- ◇ Internal 인터페이스는 ZTA SaaS Controller와 통신이 가능 해야 함
- ◇ 그 외 windows NTP 서버와 통신이 가능 해야 함

# IVANTI NEURON FOR ZTA

## 주요 기능 - 인증 서버

- 사용자 인증 자체를 SaaS Controller에서 수행
- 사용(or 연동)가능한 인증 서버 List : Local / SAML (Azure AD) / SAML (Custom)
- SAML (Custom)의 경우, SAML 표준 프로토콜을 사용하는 모든 인증 서버와 연동 가능 (SaaS 포함)

ZTA Controller 내의 Auth Server 관리 Page

	AUTHENTICATION SERVER NAME ↑	DEFAULT ↑	AUTHENTICATION METHOD ↑	USERS
<input type="checkbox"/>	AADEnrollment		SAML (Azure AD)	N/A
<input type="checkbox"/>	Admin Auth	✓	Local	17 USERS
<input type="checkbox"/>	IM-AuthServer		Local	3 USERS
<input type="checkbox"/>	JS-ISD-IDP		SAML (Custom)	N/A
<input type="checkbox"/>	JS-ISD-IDP-enroll		SAML (Custom)	N/A
<input type="checkbox"/>	local user		Local	10 USERS
<input type="checkbox"/>	takumi-auth		Local	1 USERS

SAML 기반 인증 서버

이외에, SAML 기반의 인증 서버는 모두 연동 가능

Azure Active Directory

okta

PingIdentity®

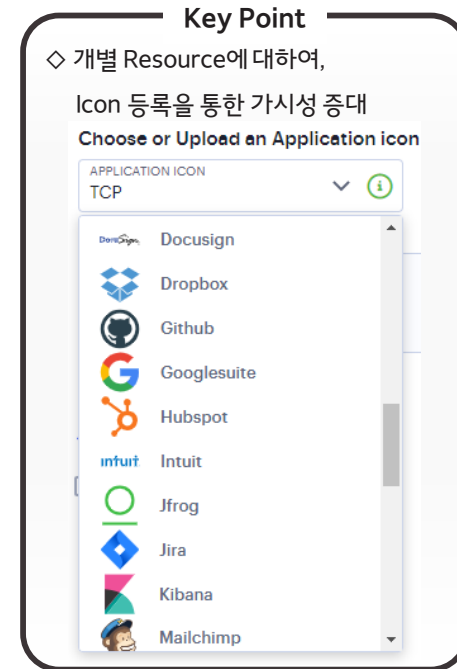
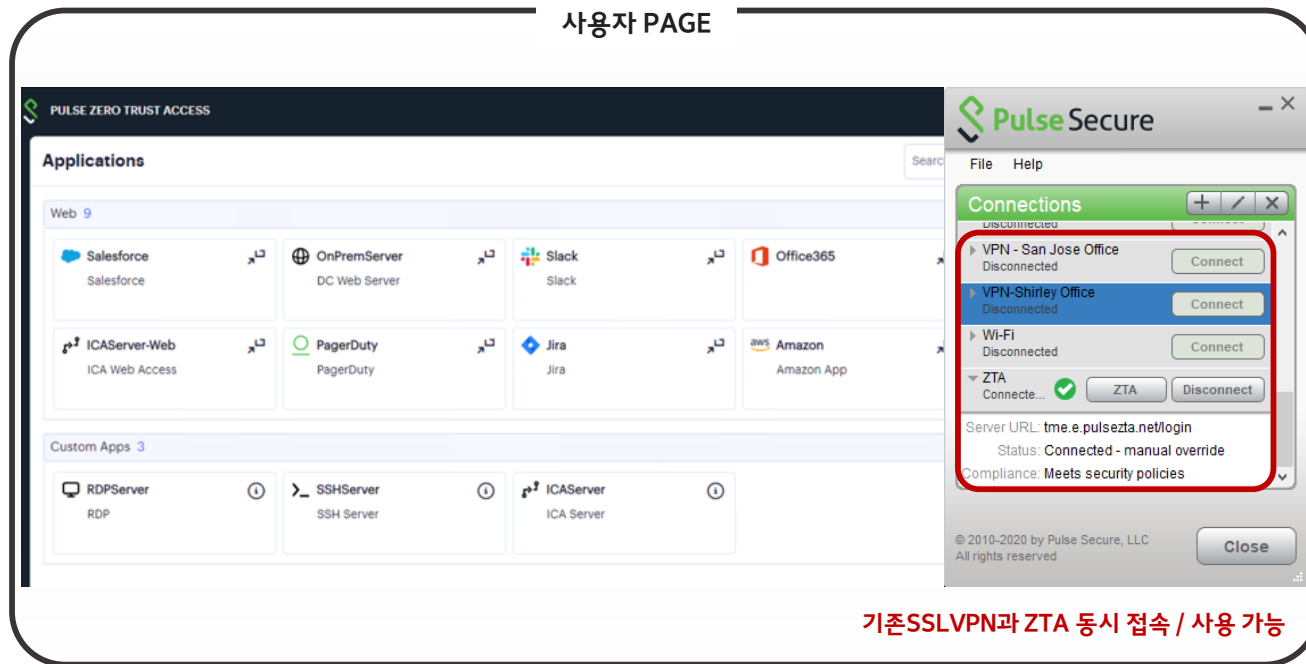
onelogin  
by OKTA IDENTITY



# IVANTI NEURON FOR ZTA

## 주요 기능 - Application 기반의 Resource Access

- 다양한 SaaS Web Application / Protocol(ex. RDP, SSH 등) 기반의 Access 기능 제공
- 이로 인하여, Application 기반의 Access 로그 및 Endpoint 정보를 이용한 관리자 가시성 증대
- 40+의 Application / Protocol 인식 (다른 서비스로 분류 됨)



# IVANTI NEURON FOR ZTA

## 주요 기능 - Device Rule (Endpoint Device 검사를 통하여 추가 보안)

- 보안 요구사항에 위배 되더라도 로그인은 가능하나, 해당 보안 요구사항이 적용된 Application은 Access 불가
- 항목에 따라서 기존 VPN의 Host Checker 보다 훨씬 세밀한 조건 설정이 가능 (Ex. Anti virus의 Enforcement Level)
- Endpoint Platform에 따라서 지원 항목에 차이가 있음

**Device Check Rule (ex. Anti-virus check)**

**Device Rules** ⓘ

**Add Device Policy Rules**

RULE TYPE: Antivirus

RULE NAME: TEST-AV ⓘ

Rule Details

RULE DESCRIPTION: V3 Check

PLATFORM: windows

Add Vendors

SELECT VENDORS: AhnLab, Inc.

AhnLab, Inc. X

Add Products

SELECT PRODUCTS: AhnLab V3 Lite (4.X)

AhnLab V3 Lite... X

ENFORCEMENT LEVEL: high

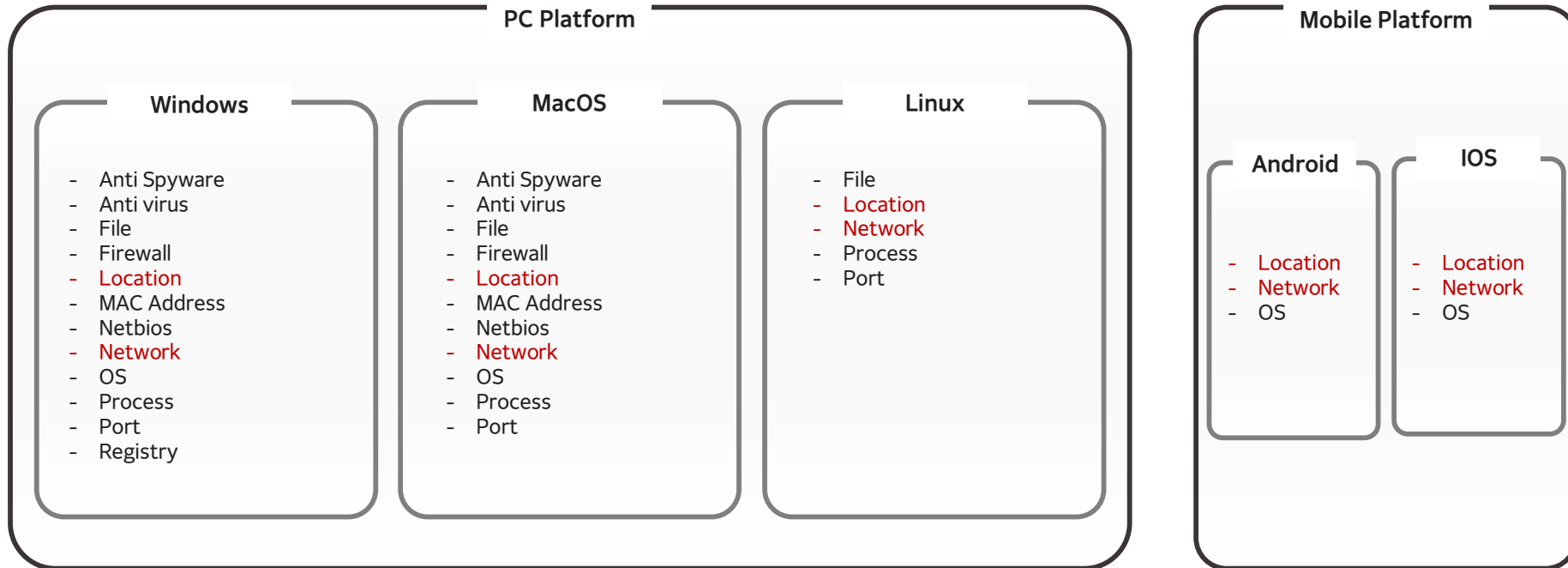
**Key Point**

- ◇ ENFORCEMENT LEVEL
  - High
  - Low
  - Moderate
- ◇ High : AV Install 및 실시간 감시 모드 활성화 Check / 최근 2일 이내 DB Update Check / Full Scan 여부 Check
- ◇ Low : AV Install 및 실시간 감시 모드 활성화 Check / 최근 10일 이내 DB Update Check / Full Scan 여부 Check
- ◇ Moderate : AV Install 및 실시간 감시 모드 활성화 Check

# IVANTI NEURON FOR ZTA

## 주요 기능 - Endpoint Device Check 항목 List

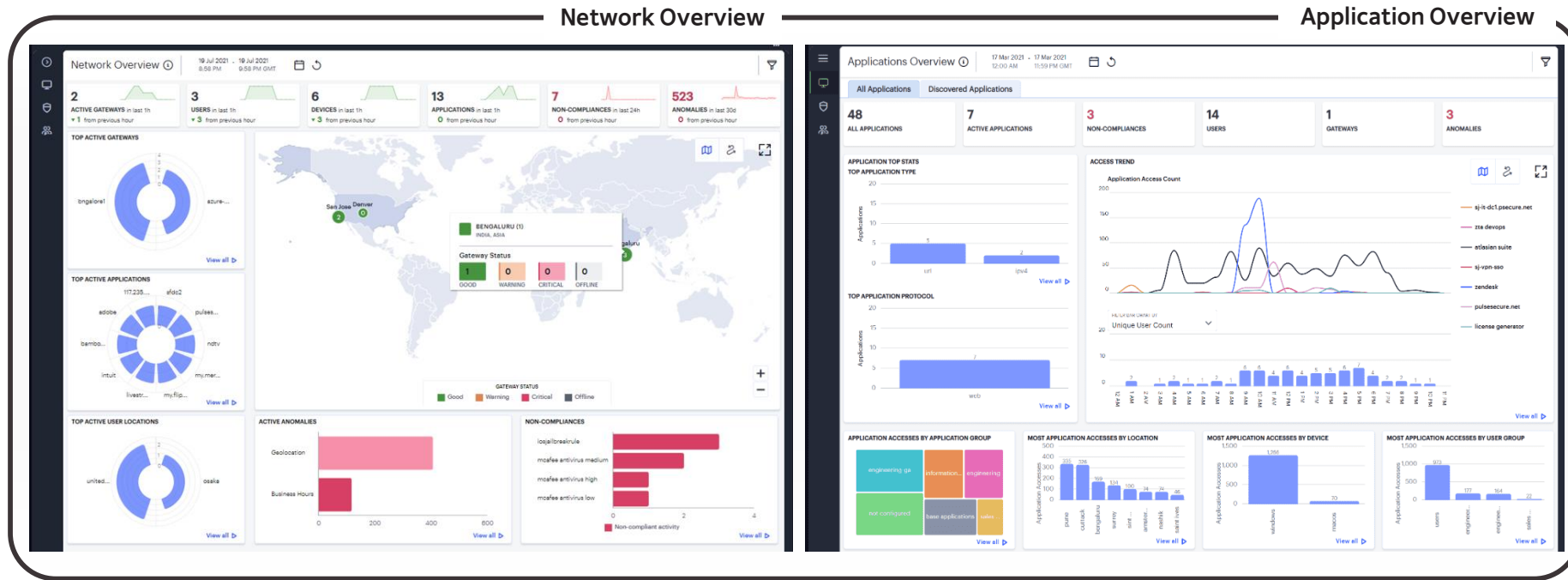
- 보안 요구사항에 위배 되더라도 로그인은 가능하나, 해당 보안 요구사항이 적용된 Application은 Access 불가
- 항목에 따라서 기존 VPN의 Host Checker 보다 훨씬 세밀한 조건 설정이 가능 (Ex. Anti virus의 Enforcement Level)
- Endpoint Platform에 따라서 지원 항목에 차이가 있음



# IVANTI NEURON FOR ZTA

## 주요 기능 - 인텔리전트 분석 및 관리

- 사용자에 대한 행동 분석(UEBA) 및 이상 탐지
- 사용자 / Application 단위의 세부적인 통계 그래프
- 각 Gateway에 대하여 다양한 Monitoring 기능



# IVANTI NEURON FOR ZTA

## 주요 기능 - Configuration Wizard

- 직관적인 단계별 Configuration
- 세분화된 Application / Device / User Policy에 대하여 Wizard 기반으로 간편한 설정

별도의 Configuration Wizard를 통하여 손쉬운 Access Policy 생성

### Select or Create Application

SELECT AN APPLICATION  
RDP - 10.10.50.5

ADD TO APPLICATION GROUP APPLICATION GROUP  
CHOIMJ TEST

NAME	TYPE	RESOURCE	DESCRIPTION
RDP - 10.10.50.5	application	rdp://10.10.50.5	RDP - 10.10.50.5
WEB - 10.10.50.5	application	http://10.10.50.5	WEB - 10.10.50.5



Back Next Cancel

### Select or Create User Rules

SELECT OR CREATE USER GROUP(S)  
Users

SELECT AN AUTHENTICATION POLICY  
User Signin

SELECT OR CREATE RULE  
CHOIMJ RULE

NAME	ATTRIBUTE	VALUE	ACTIONS
CHOIMJ RULE	username	choimj	 

CANCEL ADD USER RULE

### Configuration Wizard Step

Create Secure Access Policy

Complete all the steps below

Configuration 100%

STEPS

- Select or Create Application
- Select Device Policies
- Select or Create User Rules
- Select Gateway
- Summary >

What is Ivanti

Ivanti Connect Secure

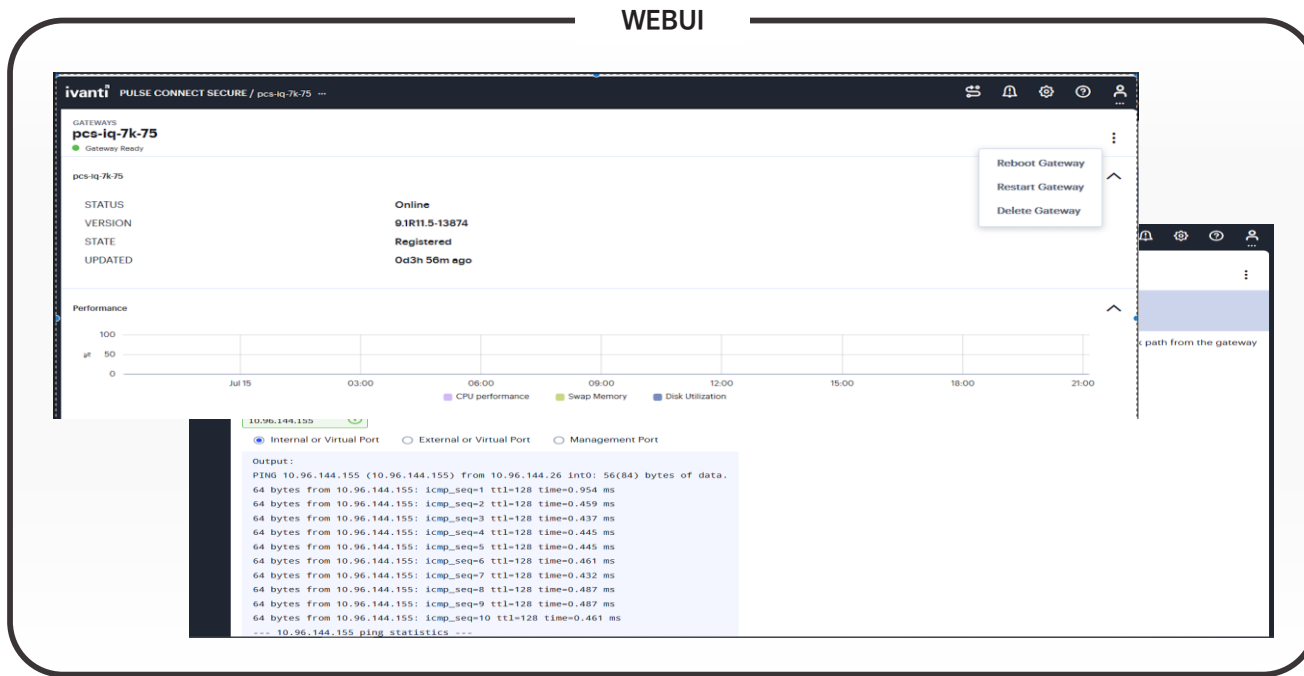
Ivanti Neuron for ZTA

**Ivanti Neuron for Secure Access**

# IVANTI NEURON FOR SECURE ACCESS

## VPN / ZTA 통합 관리 솔루션

- SaaS 기반의 VPN / ZTA Gateway 통합 관리
- VPN 관리의 경우, Configuration에 대한 부분은 향후 지원 예정



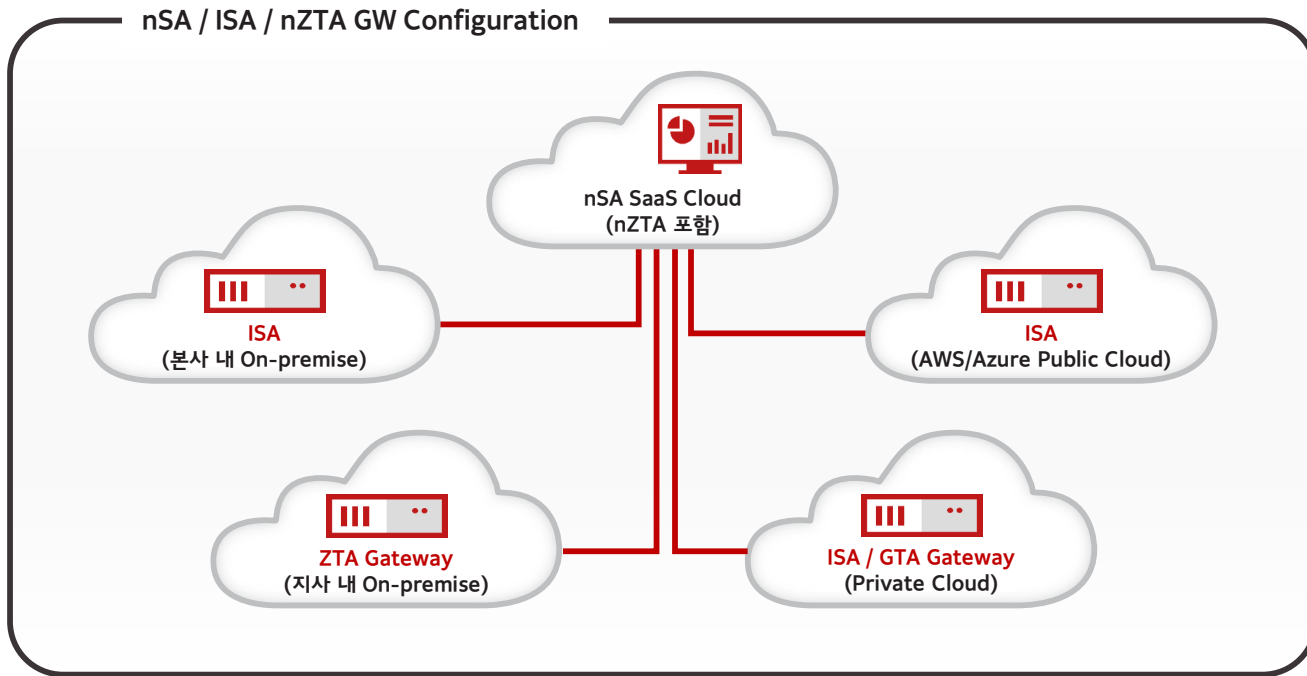
### Gateway 관리 기능

- ◇ Upgrade Gateways & clusters
- ◇ Restart Services
- ◇ Reboot Gateways
- ◇ Rollback Gateway
- ◇ Delete Gateway
- ◇ Health Monitoring
- ◇ Individual Gateway specific logs
- ◇ Trouble shooting
  - Common trouble shooting capabilities
  - System snapshot, Debug logs, Tools, TCP dump, etc

# IVANTI NEURON FOR SECURE ACCESS

## VPN / ZTA 통합 관리 솔루션

- SaaS 기반의 VPN / ZTA Gateway 통합 관리
- VPN 관리의 경우, Configuration에 대한 부분은 향후 지원 예정



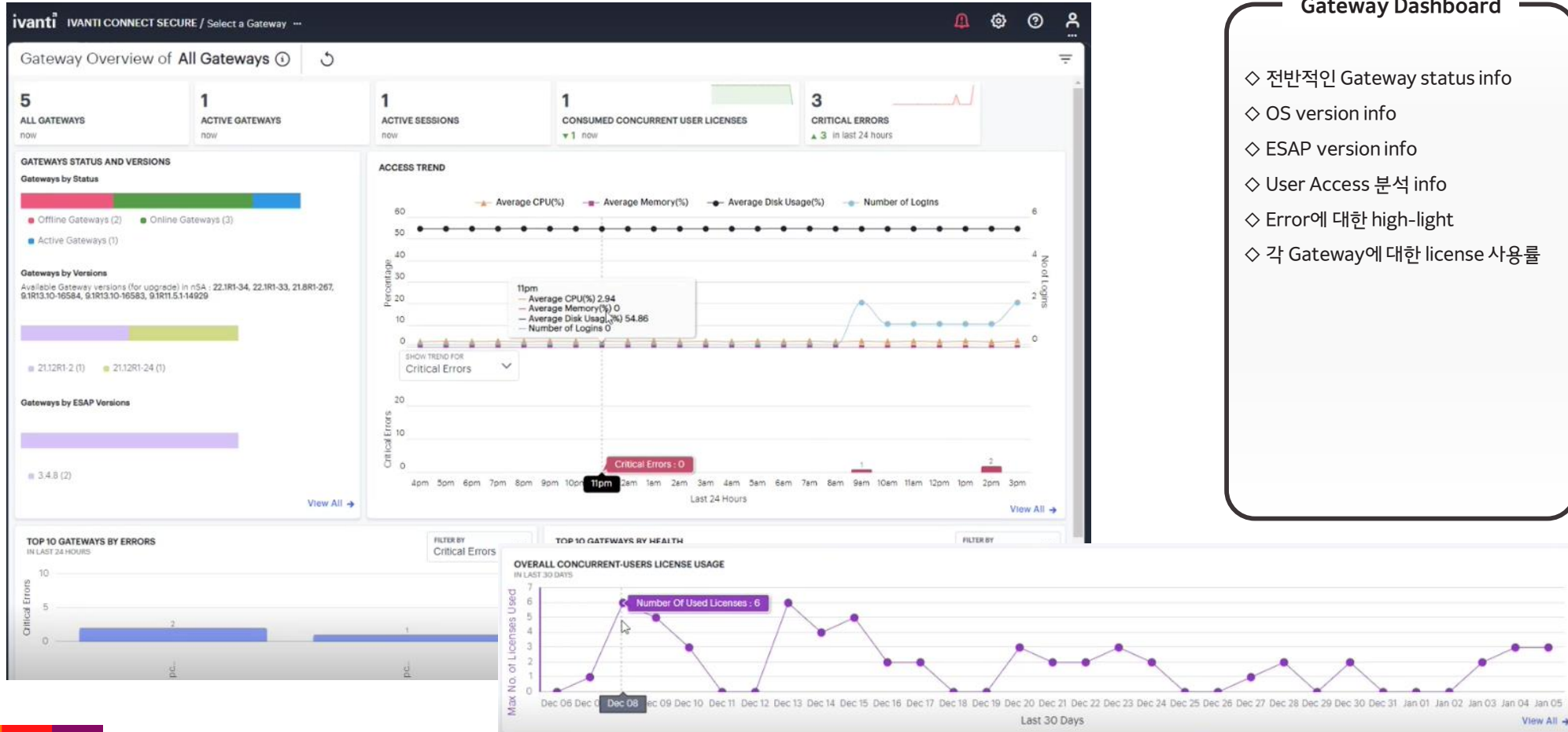
### Key Point

- ◇ 하나의 SaaS Cloud Console을 통해서, ISA / ZTA GW 통합 관리
- ◇ SSLVPN과 nGTA를 모두 사용하는 경우, 별도의 Unified License를 이용하여, 장비 구분 없이 하나의 통합된 License로 운영 가능



# IVANTI NEURON FOR SECURE ACCESS

## ICS Gateway Dashboard

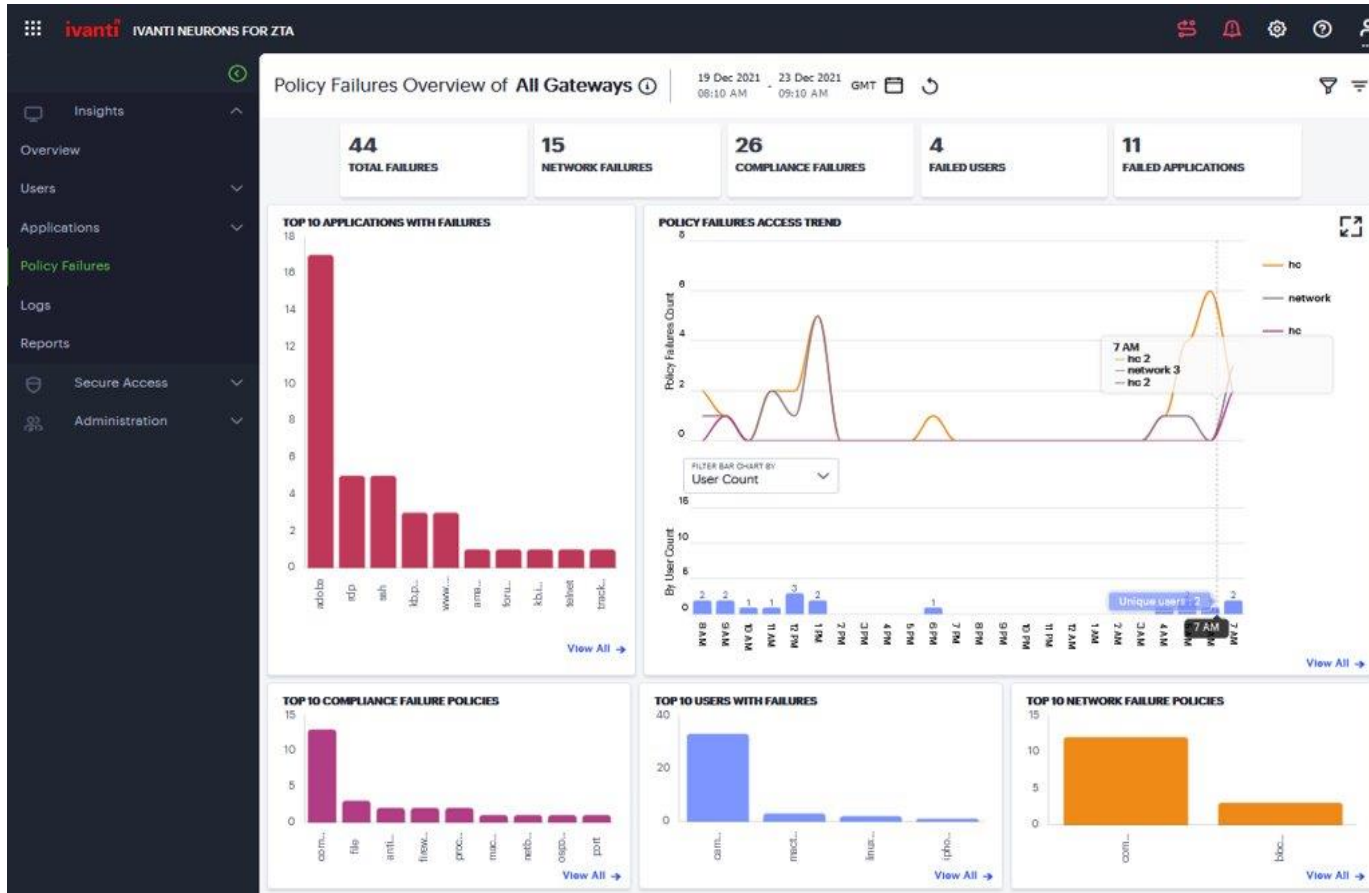


### Gateway Dashboard

- ◇ 전반적인 Gateway status info
- ◇ OS version info
- ◇ ESAP version info
- ◇ User Access 분석 info
- ◇ Error에 대한 high-light
- ◇ 각 Gateway에 대한 license 사용률

# IVANTI NEURON FOR SECURE ACCESS

## Endpoint Device Policy에 대한 Dashboard



### Endpoint Dashboard

- ◇ 네트워크 또는 Policy를 만족하지 않는 Endpoint Device 를 추적
- ◇ 2가지 유형의 내용 Display
  - 네트워크 정책 실패
  - 규정 준수 정책 실패
- ◇ 다양한 통계 그래프를 통해서 가시성이 향상되어, 이슈에 대한 동향 파악에 더욱 적은 시간이 소요됨

---

# 왜 저희 제품을 선택할까요?

---

## 전 세계 최상의 제품

- 포춘지 500대 기업의 80% 이상 사용
- 3만개 이상의 국내외 고객 레퍼런스 확보
- 최상의 제로트러스트 기반 접속 솔루션
- 기존 인프라 보안과 통합 가능한 에코시스템

## 선도적인 보안 액세스 밴더

- 뛰어난 생산성 및 가시성 제공
- 안전하고 효율적인 접근을 위한 단일 통합 클라이언트
- 기업에서 필요로 하는 다양한 인증 및 단말 장치 검사 기능 중앙 집중식 통합 정책 관리 및 통제

## 하이브리드 IT 구축

- 기존의 온프레미스 및 데이터 센터 액세스와 공존하는 멀티 클라우드에 대한 액세스 기능 제공

**ivanti**