

CLOUDSEC 2023

ENVISION IT

제로 트러스트를 통한 보안 환경 지속성

단계별 제로 트러스트 적용 모델 가이드

Hosted by



복잡한 IT 환경에서의 주요 보안 취약점

오른 소스
취약점

구 버전, 패치
되지 않은 OS

제재되지 않은
SaaS apps

네트워크
취약점

클라우드 서비스
잘못된 구성

애플리케이션
취약점

엔드포인트
취약점

취약한 OT
디바이스

Warning



공격자는 확장된 공격 대상 영역을 악용



취약성의 이용 속도가 빨라짐

많은 제로데이 취약성이 이용되어
검출하기 어려운 복잡한 공격이
발생됨





하지만.....

실제로 진행되지 않는 위험 관리

왜 위험을 파악하고 관리하는 것이 그렇게 어렵습니까?

모든 곳에 존재하는 사용자와 애플리케이션

제한된 가시성, 데이터 사일로화

대량의 도구와 공급업체

대량의 경고

컴플라이언스 대응

리소스 및 기술 부족



서버리스



코드 리포지트리



컨테이너



파일 스토리지



워크로드



클라우드 네트워크



엔드포인트 & 서버



내부 네트워크



모바일



ICS/OT



메일



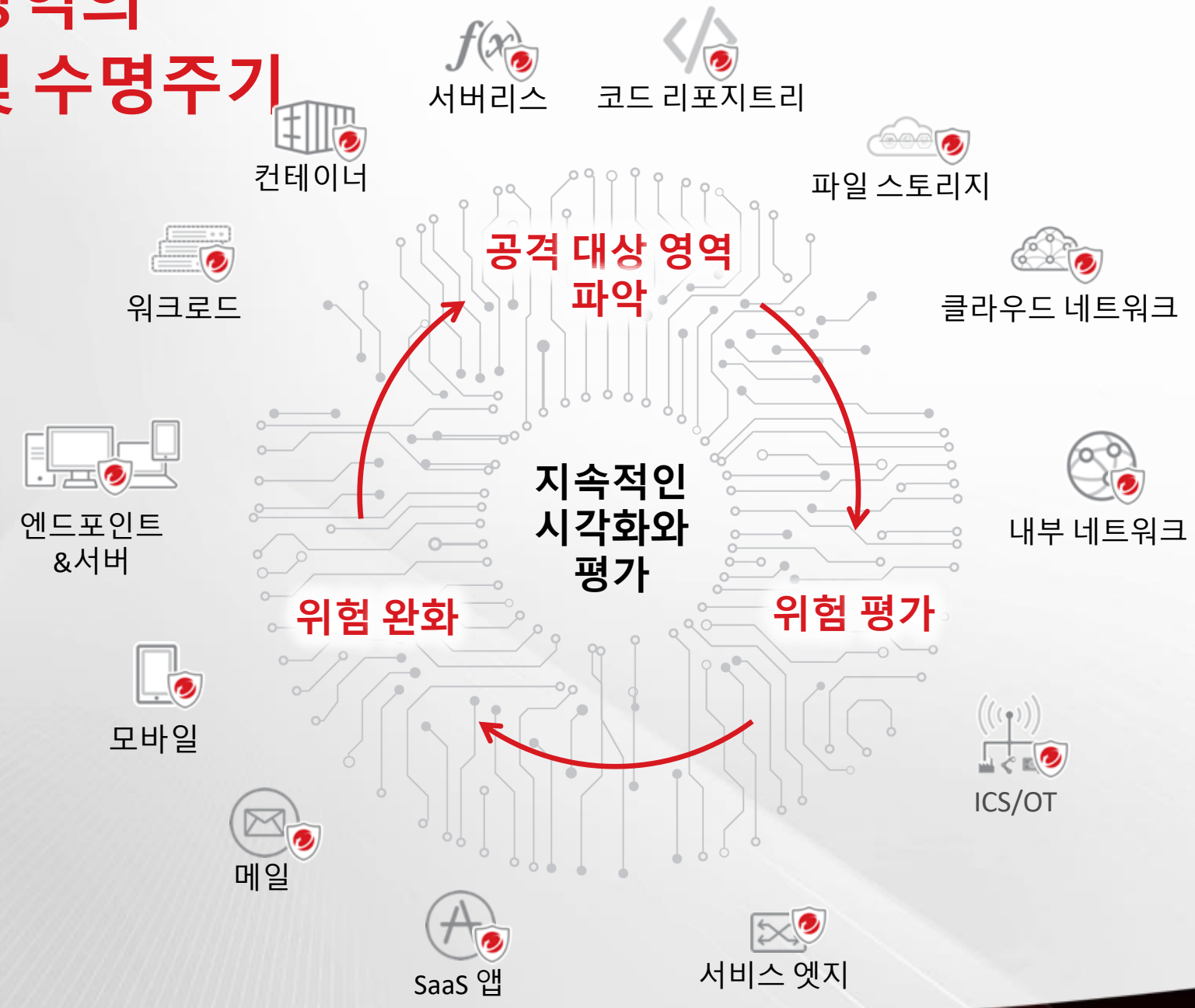
SaaS 앱



서비스 엣지

사이버 위험 관리 구현

공격 대상 영역의 위험 관리 및 수명주기



제로 트러스트에 대한 접근법

제로 트러스트는
진화하는 **위협**에 대하여
어떤 **환경**을 만들어야 하는지를
제시한 **사고방식**

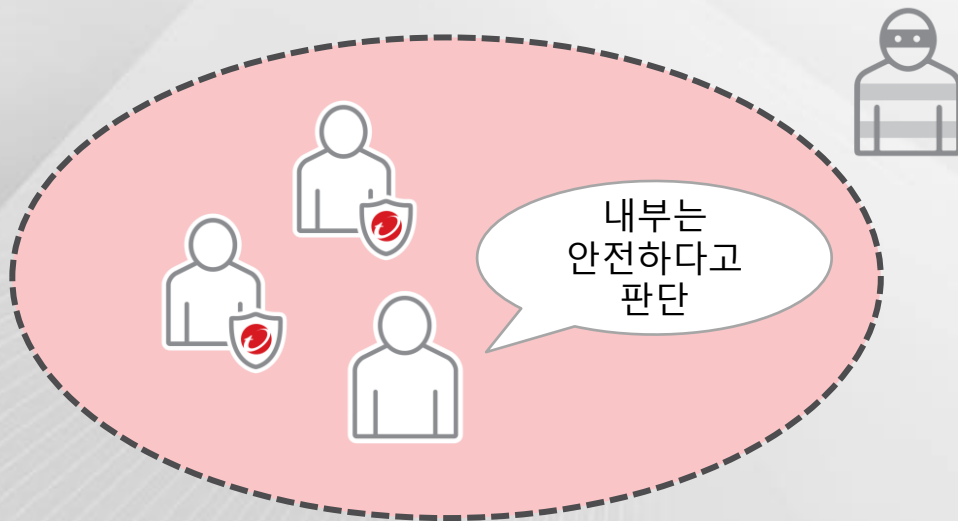
제로 트러스트 아키텍처(ZTA) 란?

"방화벽이나 VPN으로 대표되는 기존형태의 보안(경계 방어 모델)보다 모든 트래픽을 신뢰하지 않는 것을 전제로 검증함으로써 위협을 막는다는 접근법"

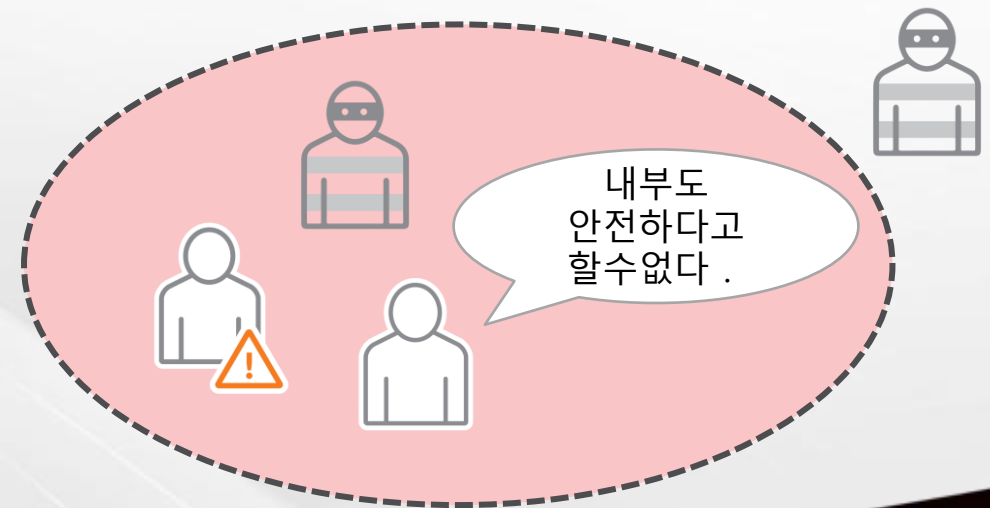
<Gilman & Barth, 2019>

경계 방어 모델과는 기본 전제가 전혀 다르다는 점이 특징

경계 방어 모델의 기본 형태



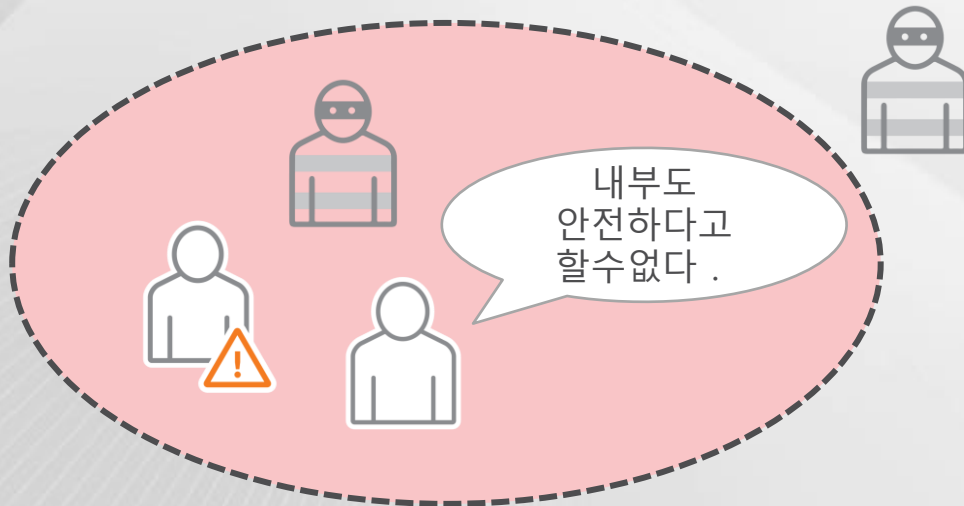
제로 트러스트 모델의 기본 형태



ZTA의 기본이 되는 사고방식이란?

- 제로 트러스트 네트워크의 5가지 원칙
 1. 네트워크는 항상 안전하지 않다고 간주된다.
 2. 네트워크상에는 외부 및 내부 위협이 항상 존재한다.
 3. 네트워크를 신용할 수 있다고 판단하기에는 로컬 네트워크로는 불충분하다.
 4. 장치 사용자 네트워크 흐름은 하나뿐 아니라 인증되고 승인됩니다.
 5. 정책은 동적이며 가능한 한 많은 출처를 기반으로 만들어져야 한다.

제로 트러스트 네트워크의 전제



NW는 항상 안전하지 않다.

외부 및 내부 위협 존재

로컬 네트워크 만으로는 불충분

모두 인증 및 승인

많은 출처를 기반의 동적 정책

제로 트러스트 기본 원칙

사용자에게 반드시 필요한 접근 이외에는 어떤 접근도 허용하지 않는다.
(기본 신뢰 없음, 항상 검증하고 위협일 수 있다고 가정.)

기본 원칙을 넘어서:

사용자 계정 또는 디바이스의 위험에
기반한 지속적인 동적 접근 제어.



제로 트러스트(Zero Trust) 운영 원칙



Define your attack surface



Assess your risk



Implement multi-factor authentication



Segment your network



Monitor and detect



Continuously assess and adjust



Secure remote access

제로 트러스트: 지속적인 리스크 변화를 확인하여 접근을 제어



- 인증 : IdP(Azure, Openldap, Okta)와의 SSO로 사용자 인증
- 인가: 인증된 사용자의 접근을 인가(누가/언제/어디서/어디로) ⇒ 허가·로깅·차단)
- **위험: 'IT 자산'의 위험 상태를 지속적으로 모니터링**

위험(Risk)도 높은 사용자, 디바이스에 대해서는 내부/외부 접근 제한, 로그인 규제(사용자 계정 비활성화, 강제 로그 아웃, 비밀번호 변경)

Zero Trust 적용방안

1. 제로 트러스트의
사고방식 가지기
(제품부터 시작하지 말 것)

2. 사용자나 디바이스로부터의
정보를 바탕으로 **리스크를
가시화**하고 우선순위 적용

Risk Insights

3. 가시화된 리스크를 바탕으로
동적인 액세스 제어를 실행

Zero Trust Secure Access

Trend Micro Vision One

- Zero Trust Secure Access

Earlier detection. Faster response. Reduced Risk.

Attack Surface Risk Management
Discover Attack Surface • Assess Risk • Mitigate Risk

Zero Trust Architecture

Extended Detection and Response (XDR)



User and Identity



Endpoints and Servers



Email



Cloud Infra



Applications



Code Repo



Data



Network



5G



ICS/OT

Email Security

Endpoint Security

Cloud Security

Network Security

OT Security

Orchestration and Automation

Global Threat Intelligence

Attack Surface Intelligence | Zero Day Initiative | Threat Research | AI/ML | Big Data Analytics

Platform Foundations

Multi-Tenancy | Role-Based Access Control | Single Sign-On | Policy Decision Point

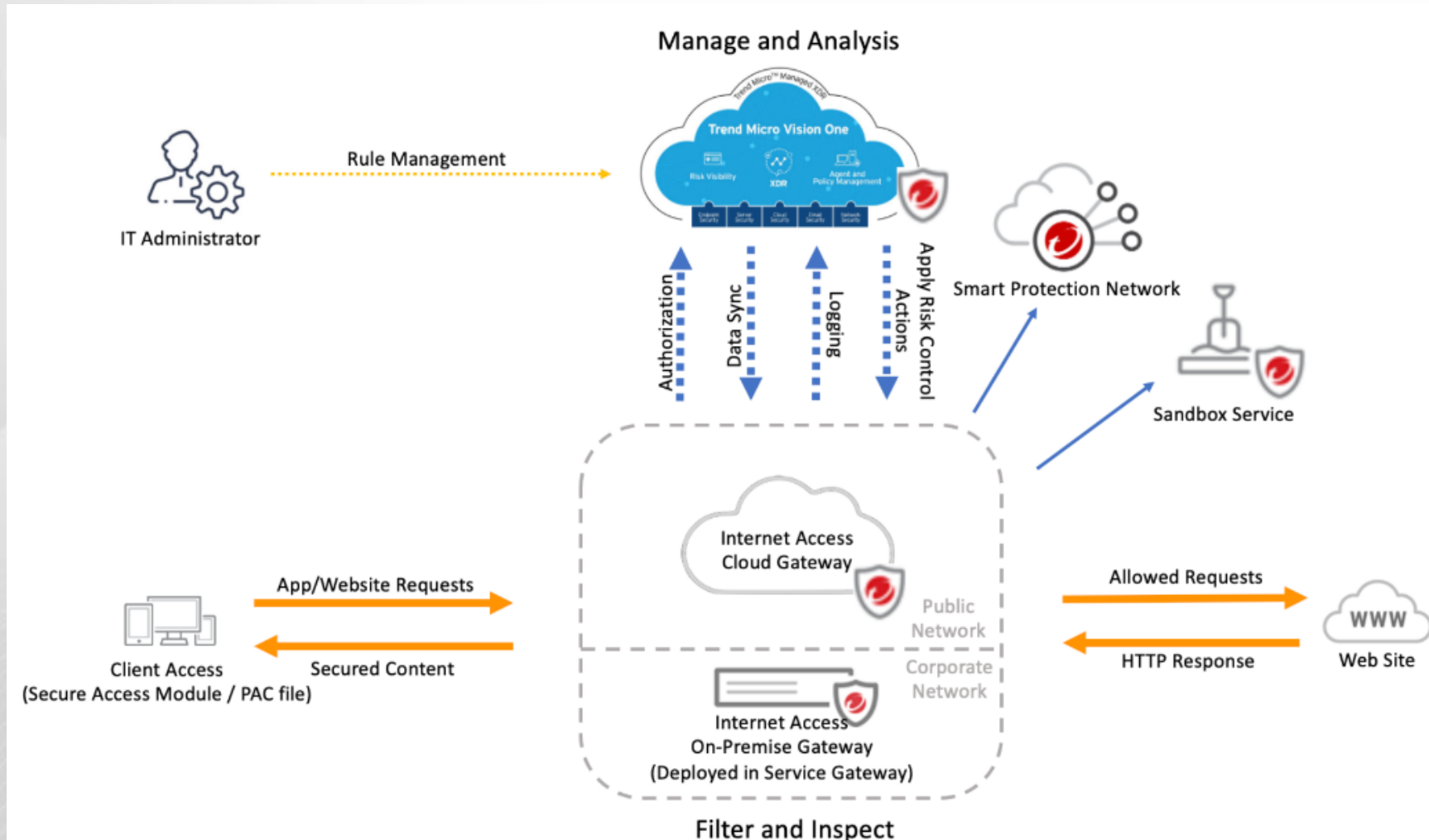
Managed Services

Ecosystem Integration

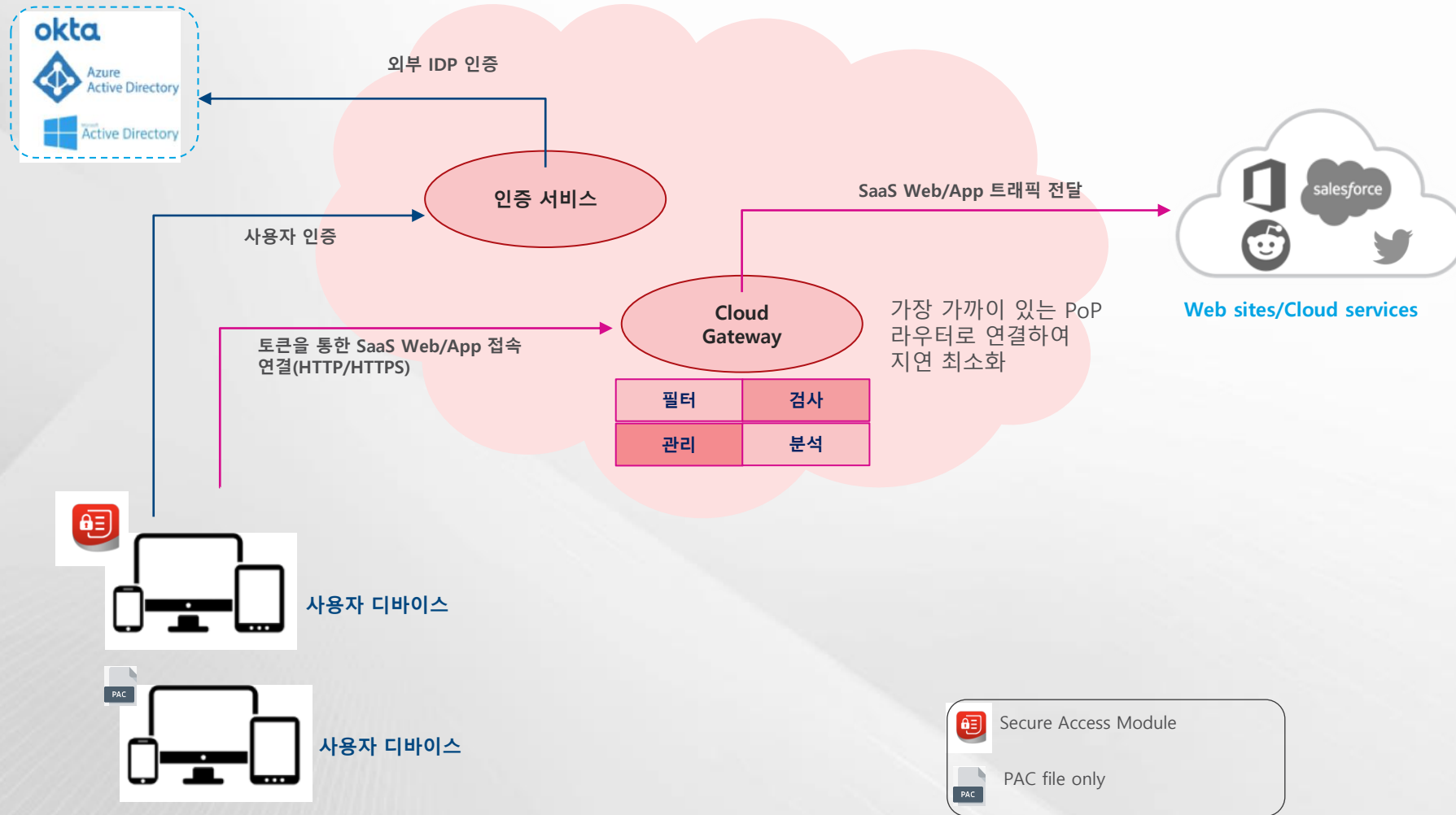
Zero Trust Secure Access

- SaaS 웹 / 앱 접근 제어

SaaS Web/Applications 접근 제어 기본 구조



SaaS Web/Applications 접근 제어 Gateway 동작 방식



SaaS Web/Applications 접근 제어 정책



제한된 / 제한되지 않은
클라우드 앱 접근 제어



HTTPS 검사



웹 콘텐츠 필터



위협으로부터 보호

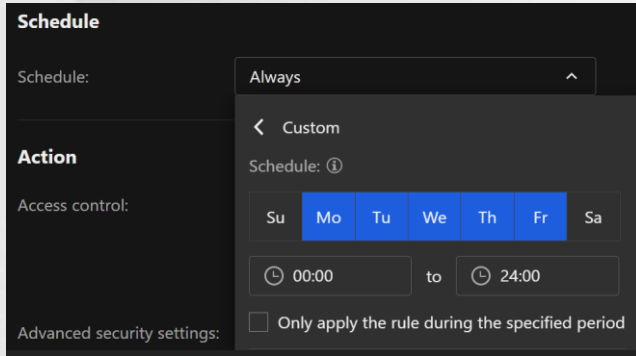


데이터 유출 방지

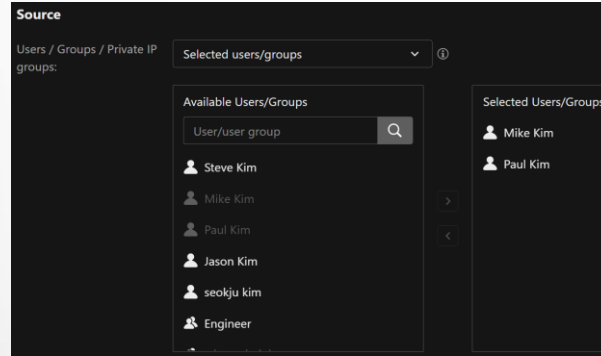
Zero Trust Secure Access

- 관리 콘솔 데모(접근 제어 정책)

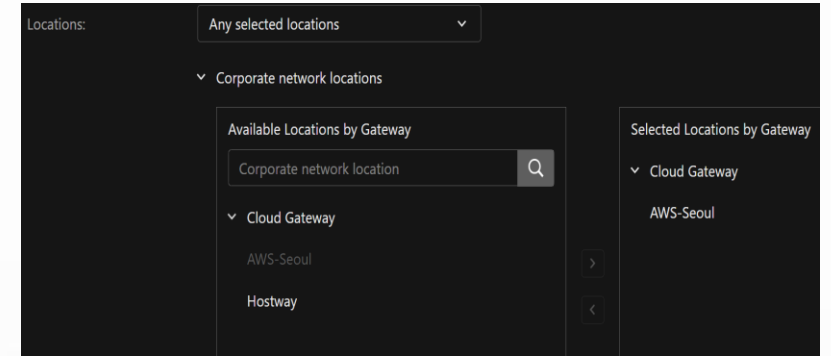
접속 권한 정책 예제



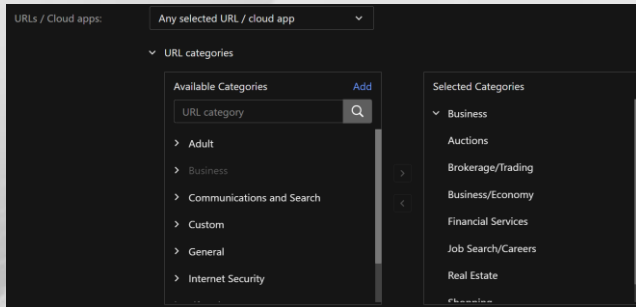
< 정책 적용 스케줄 지정 >



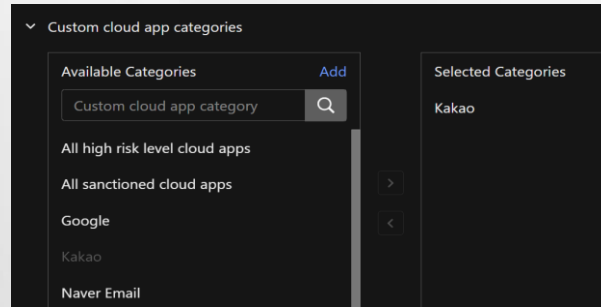
< 사용자/그룹 지정 >



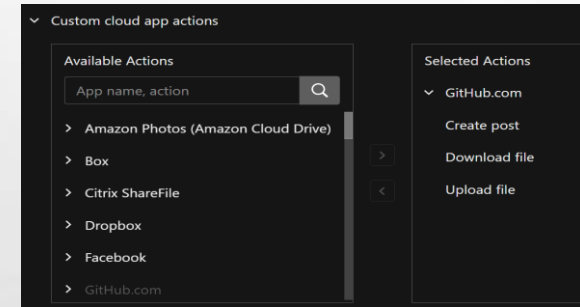
< 정책 적용 위치 지정 >



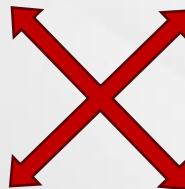
< SaaS Web/App URL 지정 >



< Cloud App 지정 >



< Cloud App Action 지정 >



접속 제어 정책

Device Posture Profiles	File Profiles	Threat Protection	Data Loss Prevention	Custom URL Categories	Custom Cloud App Categories	IP Address Groups	Tenancy Restrictions	HTTP/HTTPS Request Filters
+ Add	Profile name							
Profile name	Description	Operating systems	Ass...					
All Android device...	Default profile that identifies all Android devices in your organization	Android	0					
All iOS/iPadOS de...	Default profile that identifies all iOS/iPadOS devices in your organization	iOS/iPadOS	0					
All macOS devices...	Default profile that identifies all macOS devices in your organization	macOS	0					
All Windows devic...	Default profile that identifies all Windows devices in your organization	Windows	0					

< 디바이스 상태에 따른 제어 설정 >

Name	Description	Type	Last modified		
All File Extension (Test)	-	Customized	2023-08-17 14:45:44		
Adult	Words commonly associated with the adult entertai...	Predefined	2023-06-12 15:29:57		
Albania: IBAN (International Bank Account N...	An international standard for identifying bank acco...	Predefined	2023-06-12 15:29:57		
All File Extension	All File Extension	Predefined	2023-06-12 15:29:57		
All Personally Identifiable Information (English)	Information that can be used singly or with other s...	Predefined	2023-06-12 15:29:57		
All: Credit Card Number	Credit card numbers	Predefined	2023-06-12 15:29:57		
All: IBAN (International Bank Account Number)	An international standard for identifying bank acco...	Predefined	2023-06-12 15:29:57		
All: IIN (Issuer Identifier Number)	Also known as BIN (bank identification number) an...	Predefined	2023-06-12 15:29:57		
All: IMEI (International Mobile Equipment Ide...	An international standard for uniquely identifying ...	Predefined	2023-06-12 15:29:57		
All: Names from US Census Bureau	Names from the US Census Bureau (up to the year ...	Predefined	2023-06-12 15:29:57		

Web Reputation | File Scanning | Advanced Scanning

Enable Web Reputation

Security level:

High
Blocks pages that are:

- Dangerous: Verified to be fraudulent or known sources of threats
- Highly suspicious: Suspected to be fraudulent or possible sources of threats
- Suspicious: Associated with spam or possibly compromised

Medium (default)
Blocks pages that are:

- Dangerous: Verified to be fraudulent or known sources of threats
- Highly suspicious: Suspected to be fraudulent or possible sources of threats

Low
Blocks pages that are:

- Dangerous: Verified to be fraudulent or known source of threats

Web Reputation | File Scanning | Advanced Scanning

Action to take upon detection of botnets:

Block

Enable Predictive Machine Learning

Action to take upon detection of Suspicious Objects:

To configure default actions, go to Suspicious Object Management.

- Suspicious IP address
Use default actions
- Suspicious URL
Use default actions
- Suspicious domain
Use default actions
- Suspicious File SHA-1
Use default actions

< 웹 평판, 악성코드 검사 설정 >

Expressions | File Attributes | Keyword Lists

An expression is data that has a certain structure. You can use predefined and customized expressions.

+ Add Type: All Name, Description Import Export All

Name	Description	Type	Last modified		
South Korea: Resident Registration Number (1)	Used to identify residents in transactions with priva...	Customized	2023-08-08 16:52:11		
Albania: IBAN (International Bank Account N...	An international standard for identifying bank acco...	Predefined	2023-06-12 15:29:08		
All: Credit Card Number	Credit card numbers	Predefined	2023-06-12 15:29:08		
All: Email Address	Email addresses	Predefined	2023-06-12 15:29:08		
All: IBAN (International Bank Account Number)	An international standard for identifying bank acco...	Predefined	2023-06-12 15:29:08		
All: IIN (Issuer Identifier Number)	Also known as BIN (bank identification number) an...	Predefined	2023-06-12 15:29:08		
All: IMEI (International Mobile Equipment Ide...	An international standard for uniquely identifying ...	Predefined	2023-06-12 15:29:08		
All: Names from US Census Bureau	Names from the US Census Bureau (up to the year ...	Predefined	2023-06-12 15:29:08		
All: SWIFT BIC (SWIFT Business Identifier Code)	Also known as ISO 9362, BIC code, SWIFT ID, and S...	Predefined	2023-06-12 15:29:08		
All: Time zone offset	An amount of time added to or subtracted from th...	Predefined	2023-06-12 15:29:08		

< 기본 DLP 템플릿 및 Custom DLP 규칙 생성 >

Media Types | File Names | True File Types

Available Media Types

Search for...

- Images
- Video
- Audio
- Other

Selected Media Types

No data to display

< 제어 정책에 적용할 파일 속성 설정 >

접속 제어 정책

Tenancy Restriction Rule

Cloud app:
Microsoft Office 365
Microsoft Office 365
Google Workspace
Dropbox
Other cloud app

Applicable domains:
login.microsoftonline.com,login.microsoft.com,login.windows.net

Set action on header

Header	Operation	Value
Restrict-Access-To-Tenants	Add	Permitted tenants (domains or directory IDs)
Restrict-Access-Context	Add	Single directory ID

< Cloud App Tenancy 제어 정책 >

Cloud Gateway

Specify the externally-facing IP addresses of your organization's internet gateways
Note: By default, all endpoints configured to send traffic to the Internet Access Cloud Gateway.

Add Corporate Location

< Cloud Gateway for SaaS 웹/앱 접속 제어 >

On-Premises Gateways

View your deployed on-premises gateways and indicate the corporate locations managed by your organization.
Note: To forward traffic to on-premises gateways, add the FQDNs or IP addresses of the gateways.

Deploy New On-Premises Gateway

Location, IP address

< On-Premise Gateway for SaaS 웹/앱 접속 제어 >

Private Access Connectors Internal Applications Global Settings

+ Add Private Access Connector Group

< Private ZTNA Gateway for 내부 웹/앱 접속 제어 >

HTTP/HTTPS Request Filter Settings

Request method:
 Any selected request method
GET, POST, PUT, HEAD, DELETE

Request URLs:
 Any specified URL host name or IP address
Example: www.example.com, www.example.c?, *.example.com

Use commas (,) to separate multiple values. Wildcards supported.

Any specified URL path (do not start the path with the '/' or include the '?' of the query)
Example: example.com/news.htm, example.com/news?.htm, *news*

Use commas (,) to separate multiple values. Wildcards supported.

Header fields:

< HTTP/HTTPS Request 제어 정책 >

Customization Settings

Zero Trust Secure Access supports customization of web pages and module notifications. You can change the appearance of the user portal and restricted access pages.

General Layout

Page Banner

Private Access User Portal

Sign In Page

User Portal

Restricted Access Pages

Risk Control Rule Block Page

Private Access Rule Block

Internet Access Rule Block Page

Device Posture Check Block Page

Threat Protection Block Page

Data Loss Prevention Block Page

Blocked URL Page

HTTPS Certificate Verification Block Page

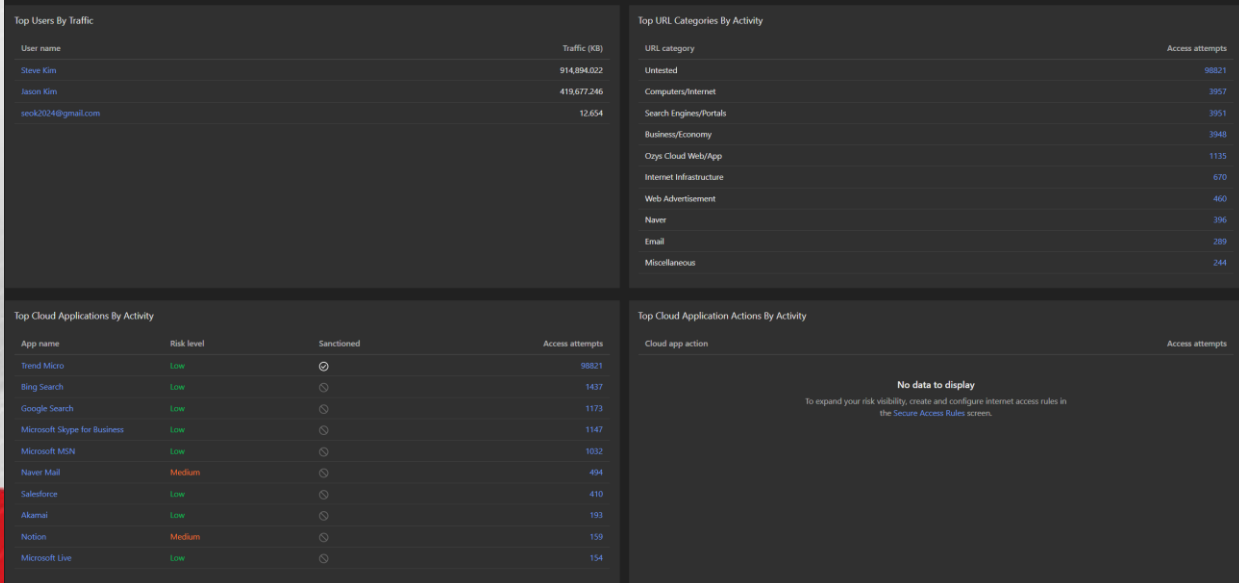
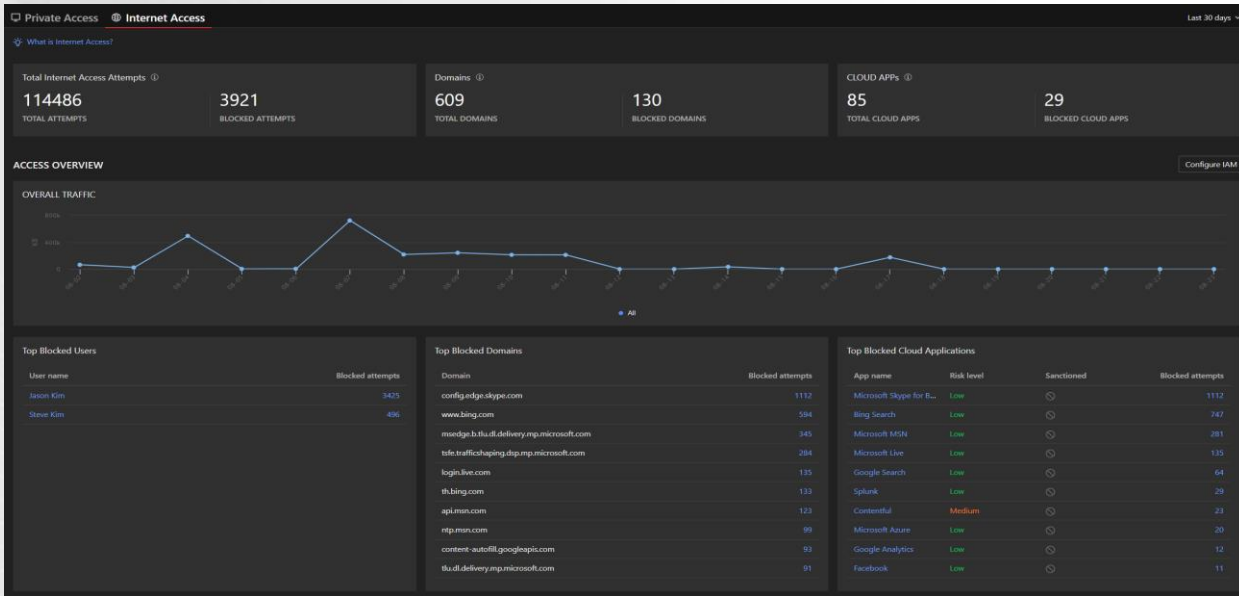
HTTPS Certificate Verification Warning Page

Secure Access Module Notification

Customize Cancel

< 사용자 웹 UI Customizing >

접속 권한 정책 예제



Trend Vision One™ Secure Access History (2023-08-23 14:43)

User Activity Logs | Remediation Logs

Filters: Last 30 days | Triggered by: All | Activity status: Monitored / Blocked | User location: All

Search: User name [] Search by: User name [Apply] Switch to Advanced

User name	Device name	Activity status	Triggered by	App	User location	Device IP address	Device operating system
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Microsoft Sky...	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Microsoft Sky...	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Microsoft Sky...	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Bing Search	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Google Search	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Google Search	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
> Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348

Total: 7254 | 20 per page | 3 / 363

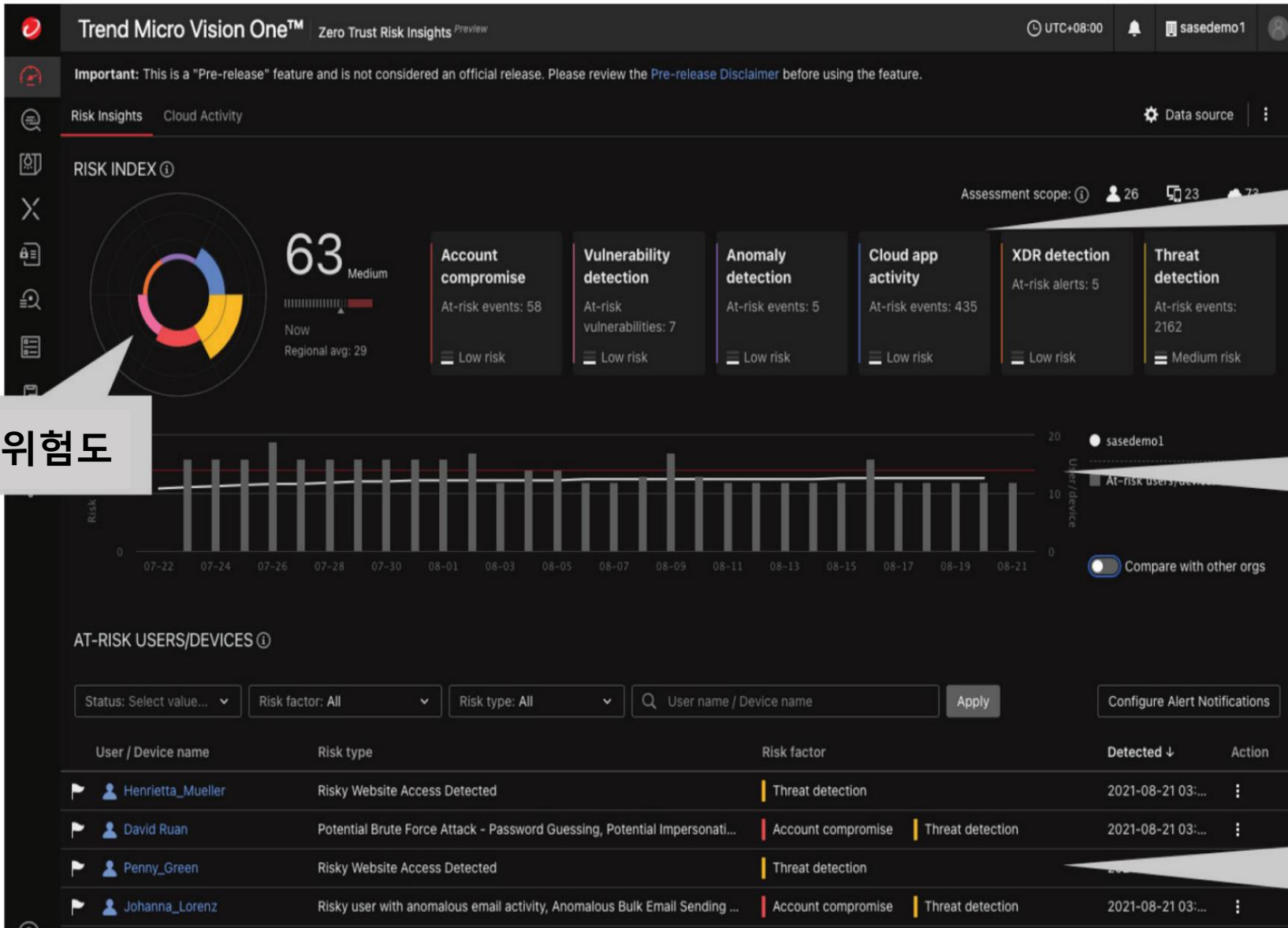
Secure Access History:

- 다양한 옵션에 따른 탐지/차단 로그 조회
- 허용된 내부/SaaS 앱 접근 현황 조회
- 조치된 로그 현황 조회

Secure Access Overview:

- 전체 접근/차단 시도 통계
- App/Domain별 접근/차단 통계
- 사용자별 빈도, 시간별 접근 트래픽

보안 이벤트 및 위험 상태 시각화



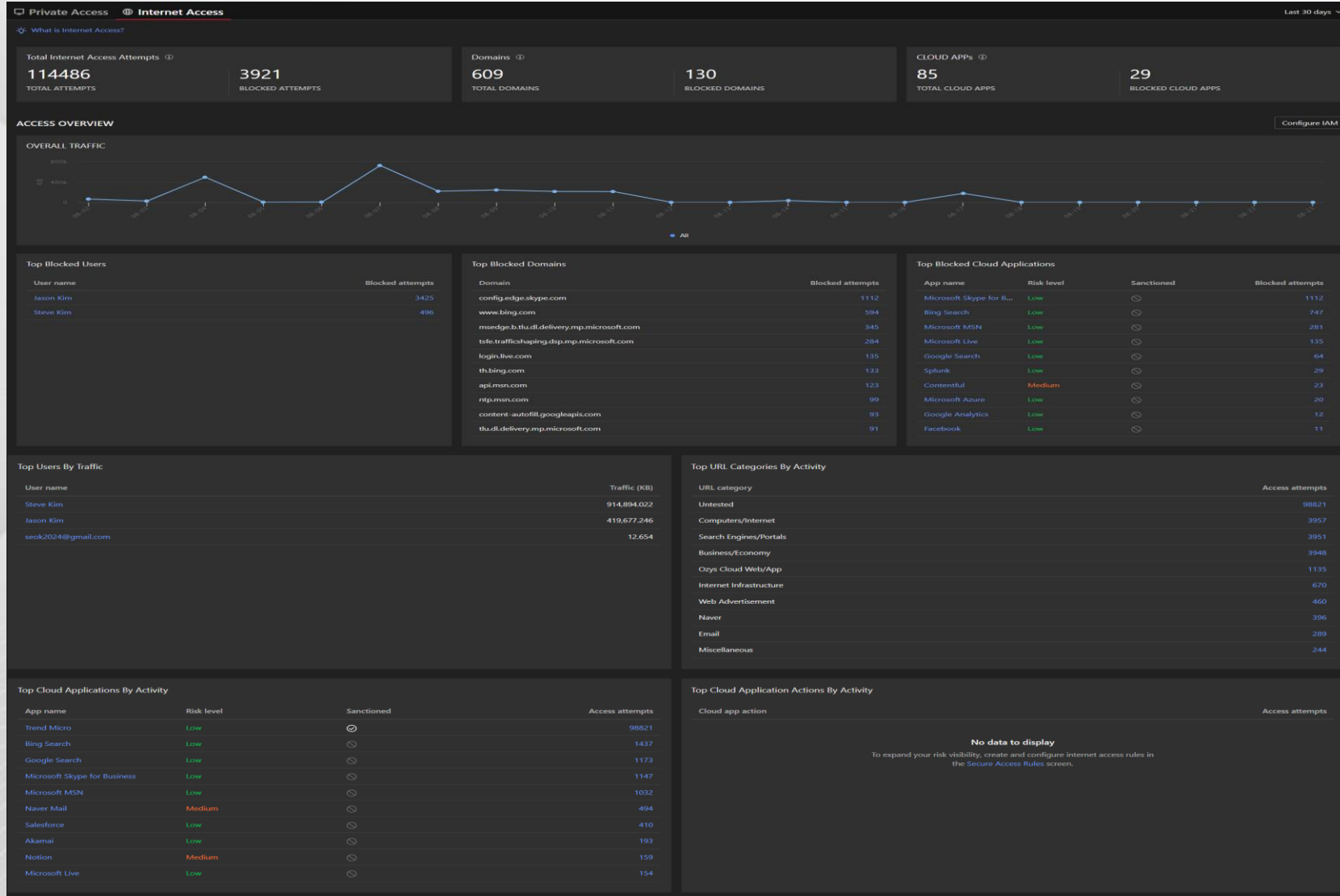
전체 위험도

위험 요소와 점수

기간별 위험도 변화와 조직간 비교

사용자 / 디바이스 위험 우선순위

보안 이벤트 및 위험 상태 시각화



Secure Access Overview:

- 전체 접근/차단 시도 통계
- App/Domain별 접근/차단 통계
- 사용자별 빈도, 기간별 접근 트래픽등

보안 이벤트 및 위험 상태 시각화

The screenshot displays the Trend Vision One Secure Access History interface. At the top, there are navigation tabs for 'User Activity Logs' and 'Remediation Logs'. Below these are filters for 'Last 30 days', 'Triggered by: All', 'Activity status: Monitored / Blocked', and 'User location: All'. A search bar is present with the text 'User name' and a search button. The main area contains a table with the following columns: User name, Device name, Activity status, Triggered by, App, User location, Device IP address, and Device operating system. The table lists multiple entries for 'Steve Kim' with various device names and activity statuses. At the bottom, there is a note: 'Only 50000 log entries displayed. To view more Secure Access activity data, go to the Search app.' and a pagination bar showing 'Total: 7254', '20 per page', and '3 / 363'.

User name	Device name	Activity status	Triggered by	App	User location	Device IP address	Device operating system
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Microsoft Sky...	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Microsoft Sky...	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Microsoft Sky...	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Bing Search	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Google Search	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	Google Search	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348
Steve Kim	EC2AMAZ-A6...	Public cloud app / URL access monitored	Internet access control rule: default	-	Korea	15.165.20.209 / 10.1.1.7	windows 10.0.20348

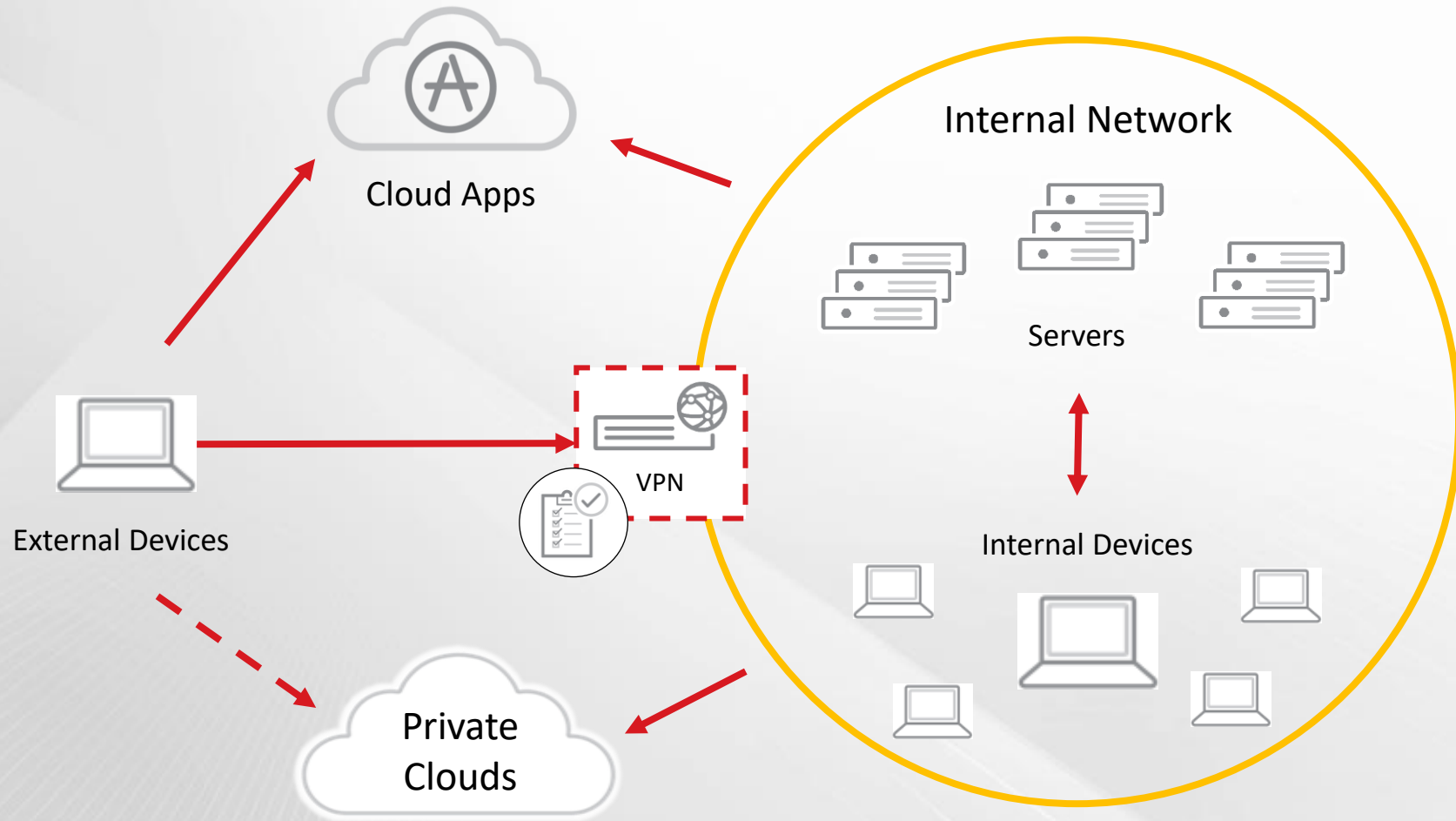
Secure Access History:

- 다양한 옵션에 따른 탐지/차단 로그 조회
- 허용된 내부/SaaS 앱 접근 현황 조회
- 조치된 로그 현황 조회 등

Zero Trust Secure Access

- 내부 웹 / 앱 접근 제어

원격 업무의 전통적인 접근 방법



전통적인 보안 모델로부터 제로 트러스트 방법 모델로의 전환



네트워크 연결된 모든 접근 신뢰



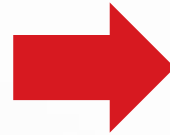
허가된 사용자(신원)으로 가정



사용자 책임 신뢰



공격자 행위 기반 탐지



기본적으로 모든 접근 신뢰하지 않음



모든 항목 검증 (사용자 & 디바이스 증명과 보안 상태)



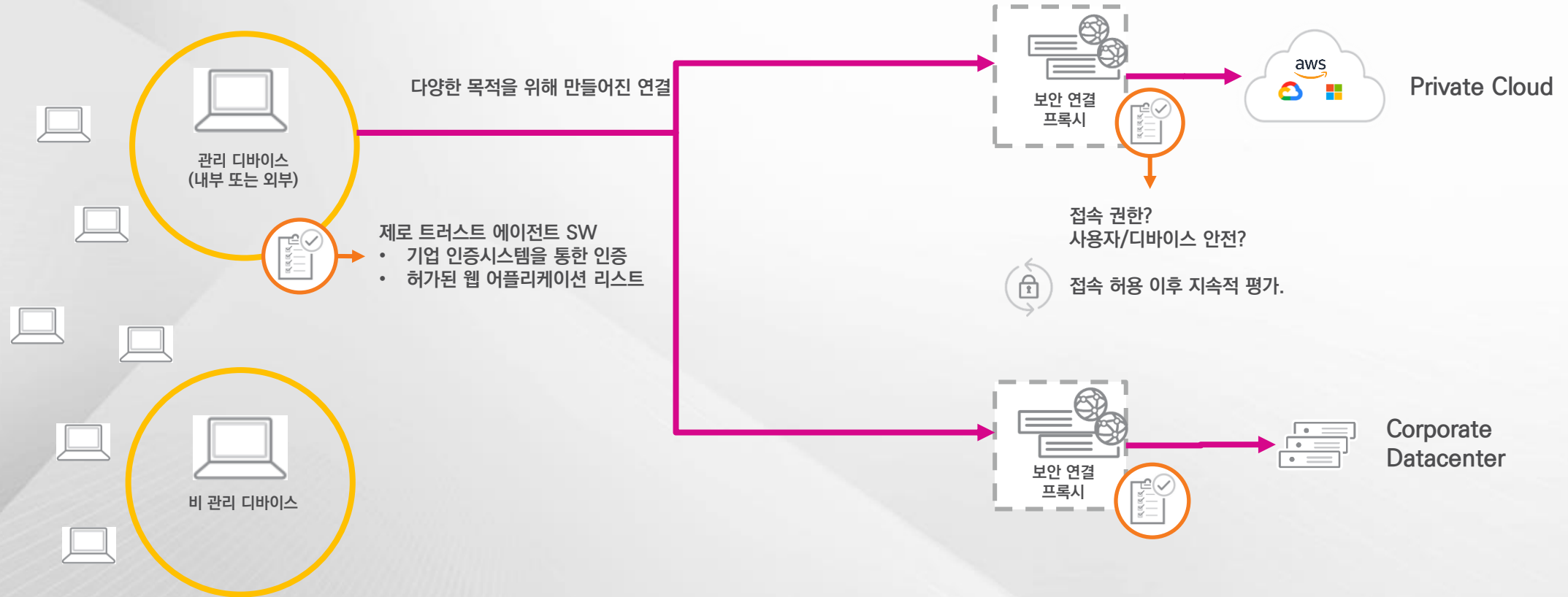
선택적으로 특정 네트워크와 앱 접근 허용



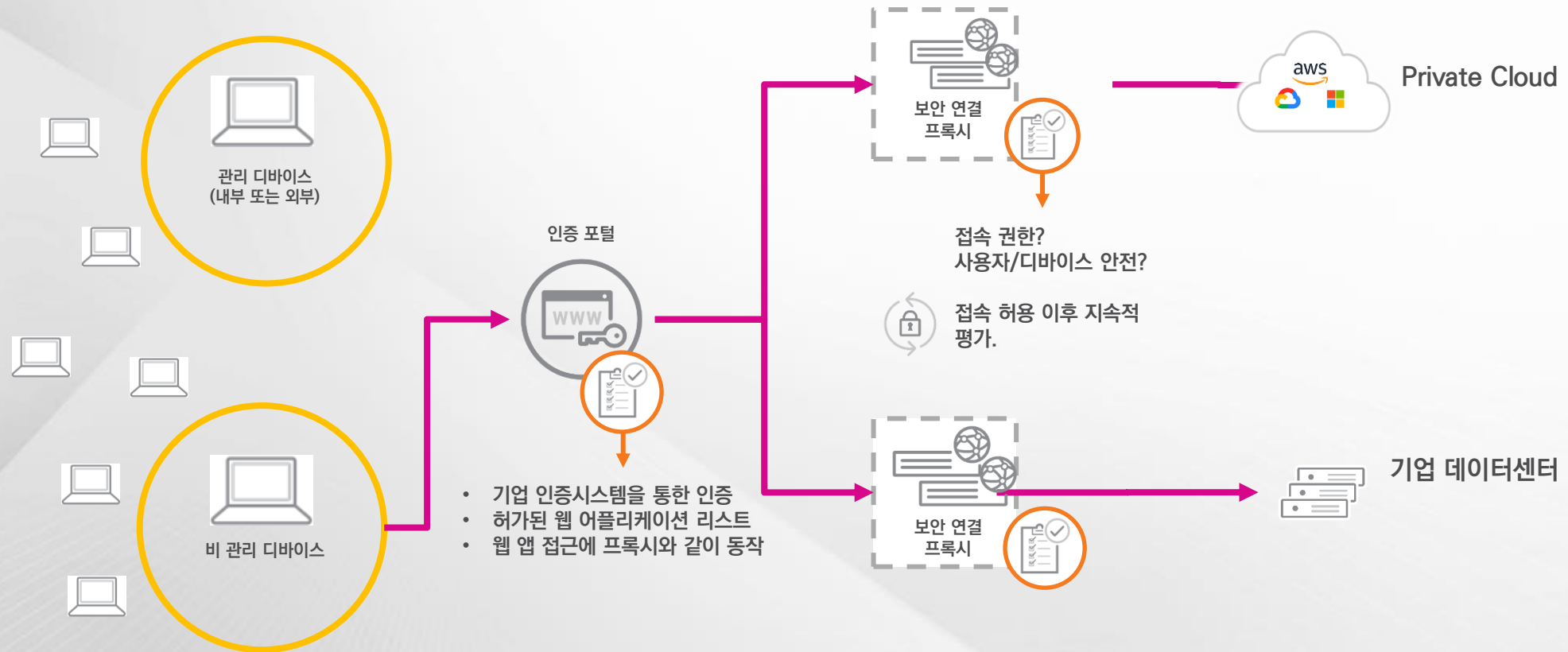
공격자의 접근을 지속적으로 어렵게 함



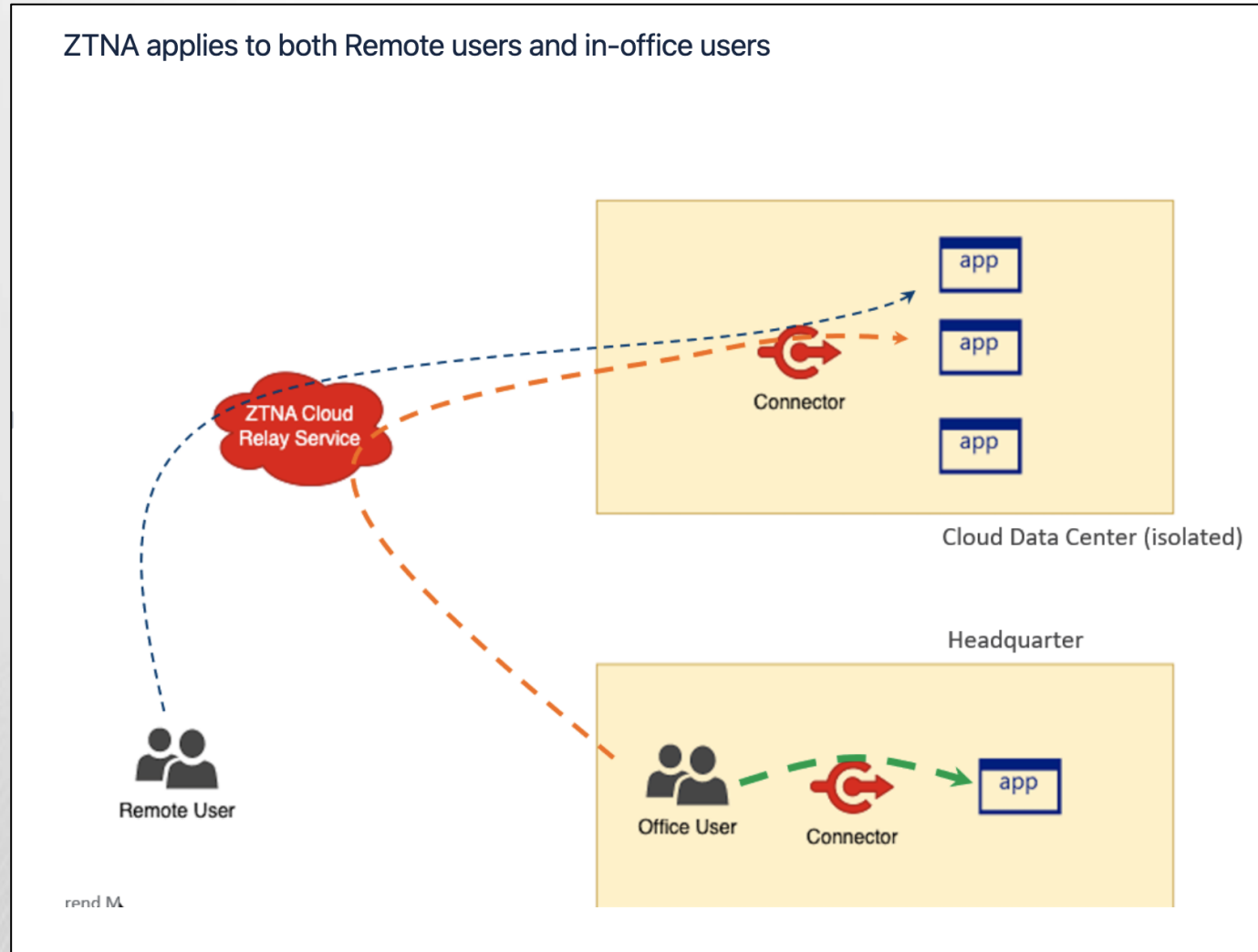
Datacenter or Private Cloud 접근 제어 : 기본 구조



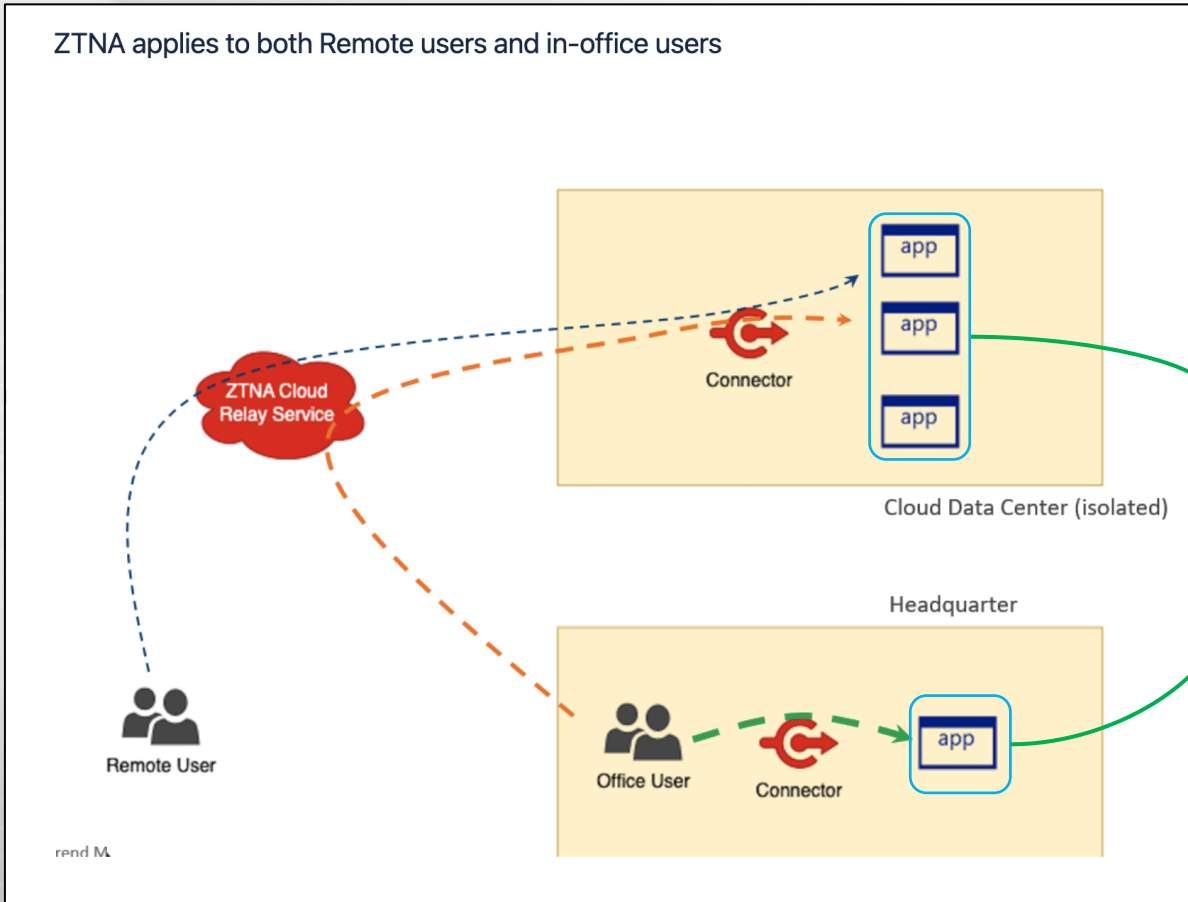
Datacenter or Private Cloud 접근 제어 : 기본 구조



Datacenter or Private Cloud 접근 제어 : Gateway 동작 방식



접근 통제 대상 내부 애플리케이션 설정



Add Internal Application

Connector group:

App group tag:

Client Access: **Browser Access**

Allow users to access via a user portal provided by Trend Micro
Browser Access is only available on Connectors starting with version 2.0.

Protocol:

Some web apps require that you configure access to other internal apps to function.
To find associated apps, install the [Trend Micro Web App Discovery Chrome extension](#).

Home page:

Internal URL:

Note: The path field is optional. Do not use a filename. Paths can have multiple elements separated by a slash (/).

External URL:

Canonical name (CNAME): [tmk-anthony.edge.sg.ztna.trendmicro.com](#)
Add the CNAME to your public DNS and verify that the domain for the application resolves to the record.

Certificate:

The default certificate is a self-signed certificate provided by Trend Micro. Using the default certificate, web browsers display a certificate warning when end users access the application.

End user access: Make the app visible for end user access

Reachability check: Check if the application is reachable by the selected Private Access Connector group

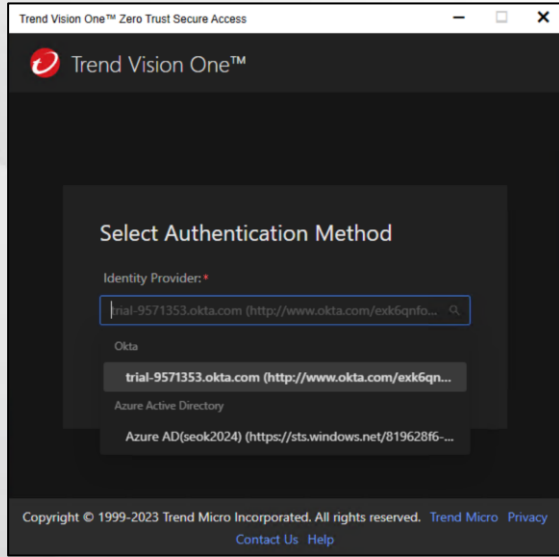
TCP:

Scheduled check: Off

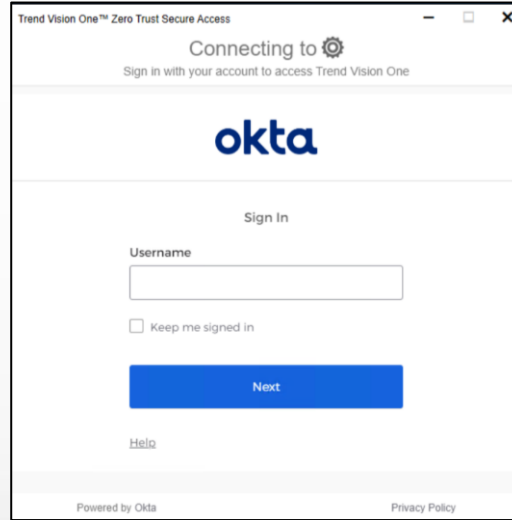
The Private Access Connector automatically checks the application reachability every five minutes.

< 내부 애플리케이션 접근 제어 정책 설정 >

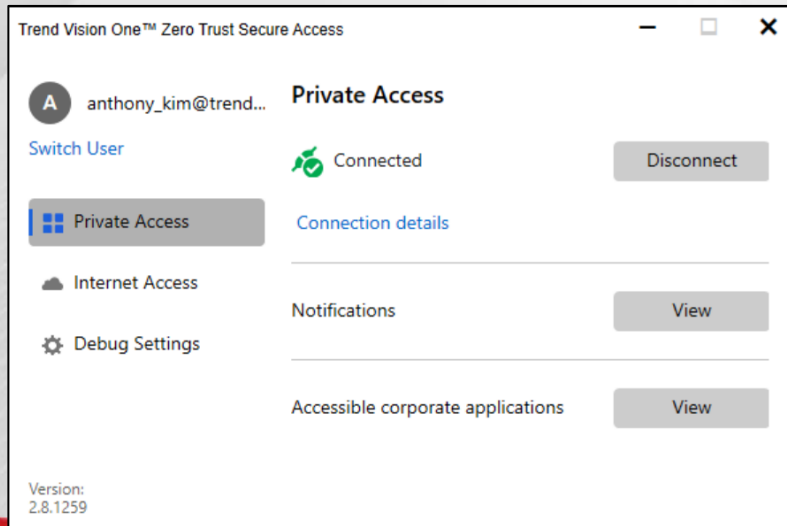
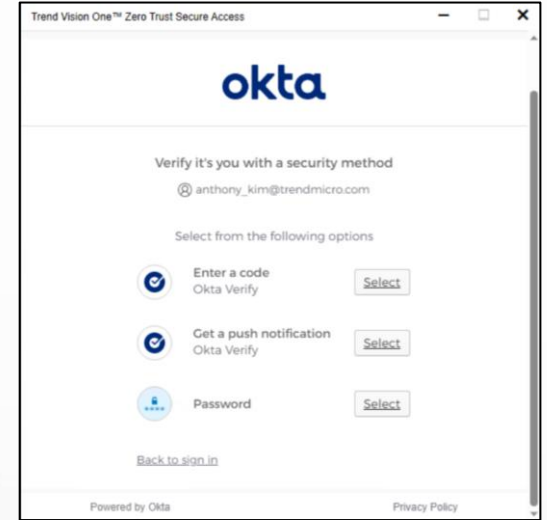
사용자 환경 : 인증 & 접근 허용 앱



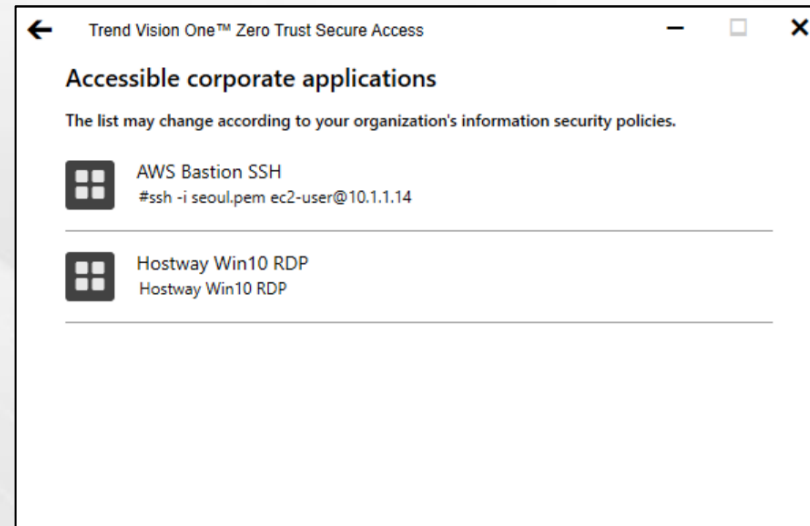
< 인증 수단 선택 >



< 사용자 인증 >



< 접근 허용 앱 리스트 >



접속 권한 정책 예제



위험 정책 확장



모든 제한사항이 요구되지는 않는다. 선택적 상세 설정 가능

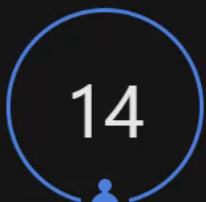




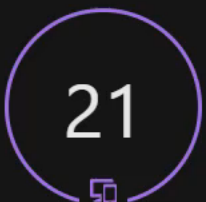
Important: This is a "Pre-release" feature and is not considered an official release. Please review the [Pre-release Disclaimer](#) before using the feature.

SECURE ACCESS CONTROL HIGHLIGHTS TO INVESTIGATE

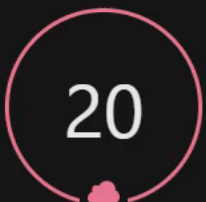
Last 30 days ▾



USERS



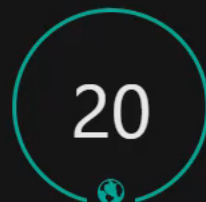
DEVICES



CLOUD APPS



INTERNAL APPS



IP ADDRESSES



URLS

TOP 10 SECURE ACCESS RULES WITH MOST DETECTIONS

Last 30 days ▾

Rule name	Description	Rule type	Matched entities	Affected activity ▾
Control access to Wiki	Control access to Wiki	Permission Control	17 13	534
Monitor access to Jira	Monitor access to Jira	Permission Control	16 12	295
Users with a persistent high risk score	A user has maintained a high risk score range over a period of time in the past.	Risk Control	6	240
Default rule for internal app access	Block access to all configured internal applications. The default rule is not editable.	Permission Control	15 12	149
Block access to Github	Block access to Github	Permission Control	14 13	148
Monitor access to Jenkins	Monitor access to Jenkins	Permission Control	11 11	97
Monitor Adfs	Allow or block access to specified internal apps based on users, devices, time, and location.	Permission Control	6 2	80
Internal app -	Allow or block access to specified internal apps based on users, devices, time, and location.	Permission Control	2 1	56
demo for access wiki	Demo when using account ztsa_demo	Permission Control	1 1	39
for demo	Allow or block access to specified internal apps based on users, devices, time, and location.	Permission Control	1 1	23

[View all enforced rules](#)

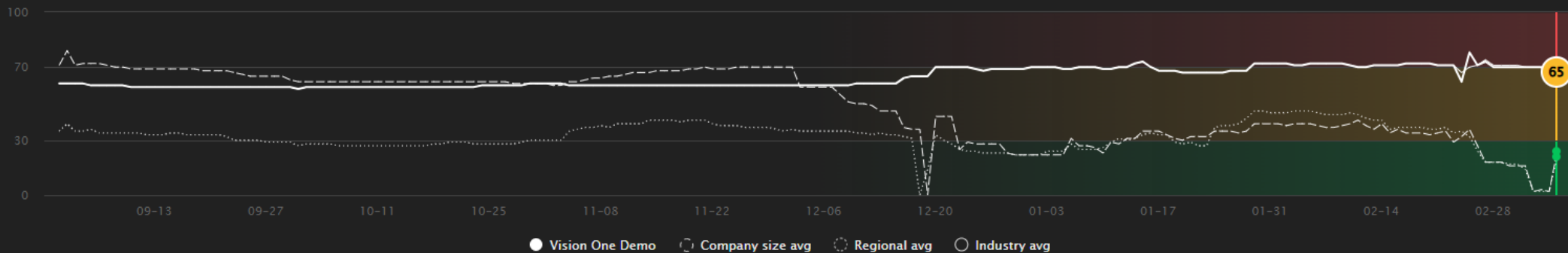
Attack Surface Risk Management (공격 표면 위험 관리)

RISK INDEX [What is Risk Index?](#)

65 /100
Medium risk

The risk score is a comprehensive results correlated by different factors:

- Exposure >
- Attack Overview >
- Security Configuration >



Attack Surface - Devices [What is the Attack Surface?](#)

Current

Device Estimate 246 [Update Estimate](#)

Determines your device count based off of network discovery and administrative estimates

Total devices: Discoverable devices: 100% (246) Additional devices (from estimate) (0)

Discoverable devices 246 out of 246 [Extend Visibility](#)

The level of Trend Micro access to devices based on discovery by Trend Micro services, product telemetry logs, or third-party services

Visibility: Full (42) Partial (3) Limited (201)

Device Exposure Assessment 246 out of 246 [Extend Risk Assessment Scope](#)

Assesses device risk levels based on unpatched vulnerabilities, system configurations, and internet accessibility (does not factor in Trend Micro security configurations)

Exposure level: Low risk (219) Medium risk (10) High risk (17) Unable to assess (0)

Devices with Managed Agents 42 out of 246 [Improve Security](#)

The level of security applied to agents managed by Trend Micro

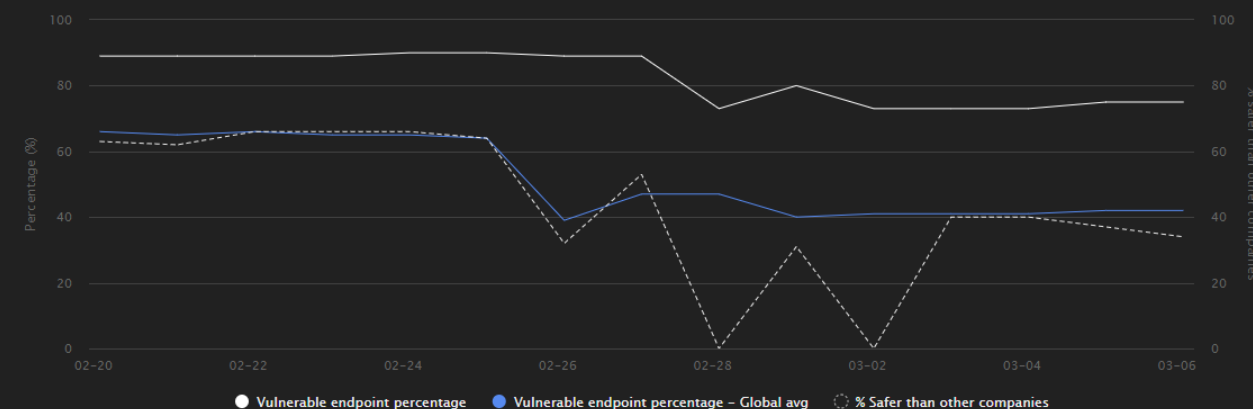
Security configuration: High security (16) Medium security (3) Low security (0) XDR only (23) No Trend Micro agent (204)

Risk Summary



VULNERABLE ENDPOINT PERCENTAGE ⓘ [View details](#)

75 % of your endpoints contain highly-exploitable CVEs. Your company is safer than **34** % of companies worldwide.



< Back

SASE-PC1

RISK ASSESSMENT

91
Current risk score

desktop
Windows Server 2016 : 93
2022-05-21 05:06:12

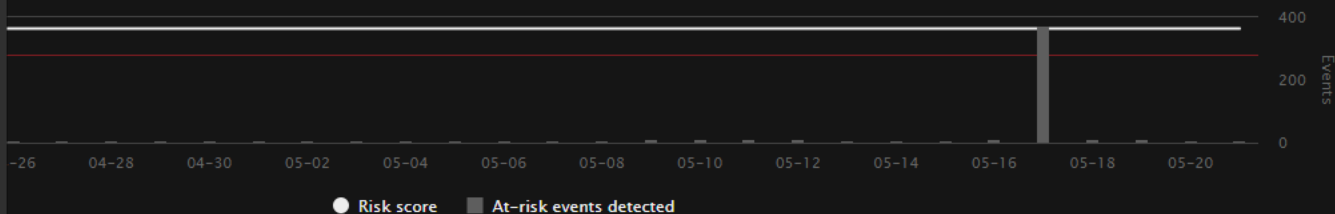
ZERO TRUST SECURE ACCESS

- Unblock Internal App Access
- Isolate Endpoint
- Assign Secure Access Rule
- View Zero Trust Action History

Significant Profile Tags

- Server
- Windows
- Publicly shared
- Normal activity
- Any time
- Fixed location
- Regular access
- Highly active
- Development tools, Business software, Communication, Sales
- Windows

[Check all assigned profile tags](#)



RISK INDICATORS

Risk factor	Risk event	Data source / processor	Risk level	Detected ↓
> Threat detection	Risky Website Access Detected	Apex One as a Service	High	2022-05-21 08:38:07
> XDR detection	Potential Targeted Attack	Connected Endpoint Product Agent	High	2022-05-21 03:06:06
▼ Threat detection	TippingPoint - Security Risk Detection	TippingPoint	High	2022-05-21 03:05:28
TippingPoint rule triggered: 16460: HTTP: BrutPOS Malware Communication Attempt Remediation: Use the detection rule to check the risk details.				
<pre> destinationIp: 10.0.0.1 destinationPort: 80 sourcePort: 1027 sourceIp: 10.204.167.113 rule_name: 16460: HTTP: BrutPOS Malware Communication Attempt </pre>				
> Threat detection	Risky Website Access Detected	Apex One as a Service	High	2022-05-21 00:20:19
> Threat detection	TippingPoint - Security Risk Detection	TippingPoint	High	2022-05-20 19:08:36
> XDR detection	Potential Targeted Attack	Connected Endpoint Product Agent	High	2022-05-20 19:08:00
> XDR detection	Anomalous Autostart Registry Entry	Endpoint Sensor	High	2022-05-20 17:07:53

< Back

Yvonne Zhang

Risk Asse

100

Current risk score

Attack Payload Autho

Staff engineer

yvonne_zhang@trend

RD

Washington

Last seen: 2022-05-21

- ZERO TRUST SECURE ACCESS
- Disable User Account
- Force Sign Out
- Force Password Reset
- Unblock Internal App Access
- Block Cloud App Access
- Assign Secure Access Rule
- View Zero Trust Action History

Profile Tags

Low privilege

Member R&D

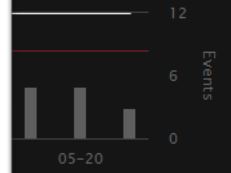
RISK II

Virtual Analyzer detected a risk in a cloud app (OneDrive) and took the configured action: Quarantine.
Remediation: Check detailed event information to verify the detection.

	Event	Data source / processor	Risk level	Detected ↓
>	Risky Website Access Detected	Apex One as a Service	High	2022-05-21 08:38:07
>	Virtual Analyzer - Cloud App Risk	Cloud App Security	High	2022-05-21 03:04:33
>	Threat detection	Risky Website Access Detected	High	2022-05-21 00:20:19
>	Threat detection	Virtual Analyzer - Cloud App Risk	High	2022-05-20 19:05:52

```

folderPath: https://tmdevorg-my.sharepoint.com/personal/admin_tmdevorg_onmicrosoft_com/Documents/trophy/
appName: OneDrive
fileUploadTime: 2022-05-20 19:00:02
action: Quarantine
userName: yvonne_zhang@trendcasdemo.onmicrosoft.com
actionResult: Fail
  
```



+
-

>>

Trend Micro Vision One – Zero Trust Secure Access

요약

공격 표면 발견



트렌드마이크로 솔루션 범위

- Endpoints
- Email
- Network

그리고 타 솔루션 연동...



접근 제어



공격과 위험 가능성에 기반.

트렌드마이크로와 타 솔루션을 통한 좀 더 완전한 평가 정책 적용

위험 감소



누가, 어떤 어플리케이션에 접속하는지에 제한하기 위해 권한 정책 적용.

기본적 신뢰 없음.
항상 검증

지속적 모니터링



많은 위험 요소들 기반한 접속 허용 이후 지속적 평가.

서비스 사용중 사용자나 디바이스가 위험 레벨 전환시 모니터링을 지속하고 접속을 제어

차별성

가시성

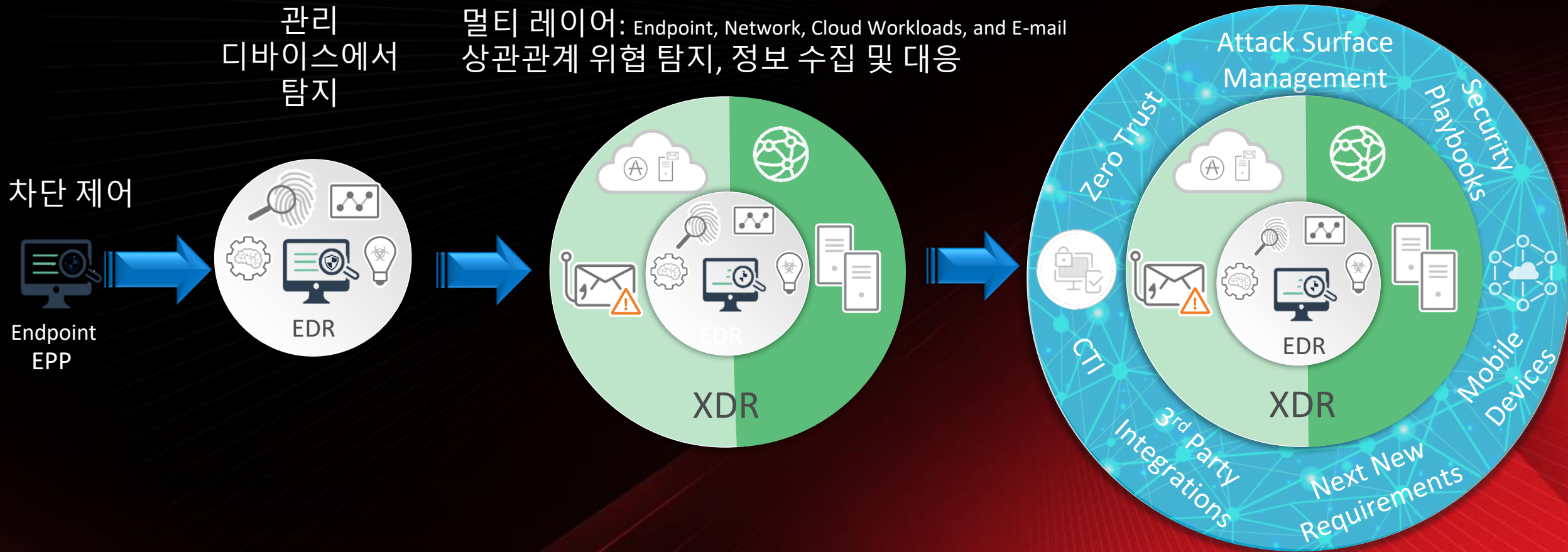
- 더 넓은 범위: endpoint, email, servers, SaaS apps, network
- Endpoint Agent를 통한 CASB 보다 더 넓은 SaaS 가시성 (특히 제한되지 않은 앱 포함)
- ZTSA Agent로 XDR까지 구성 및 기능 적용

분석 정보

- GWS 및 M365 사용에 상세한 분석 정보 제공
- 가장 광범위의 기업 서비스 종류와 시간대별 취약점 인텔리전스 제공

보안 도구에서 통합 사이버 보안 플랫폼으로 전환

Trend Micro One – 통합 사이버 보안 플랫폼
EDR, XDR, Attack Surface Management, Zero Trust, Threat intel, Assessment



새로운 사이버 보안 요구사항 & 과제



양희선 이사

luke_yang@trendmicro.com