

CLOUDSEC 2023

ENVISION IT

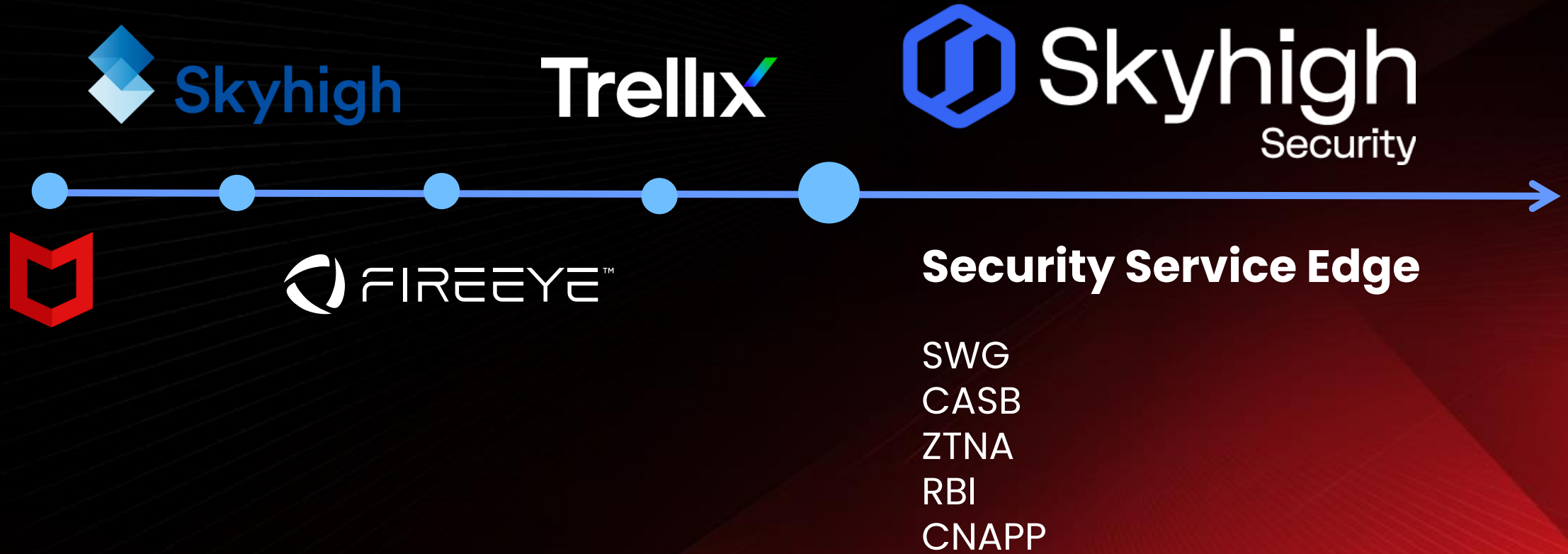
Generative AI(ChatGPT)와 같은 Shadow IT 가시성 확보 및 제어 방안

스카이하이 시큐리티 / 황민주

Hosted by



Skyhigh Security Evolution





Shadow IT 관리 및 하이브리드 보안을 위한,

Skyhigh Security

SSE (Security Service Edge)





3세대 디지털 환경의 시대

- Internet
- Mobile
- ChatGPT
(생성형 AI)

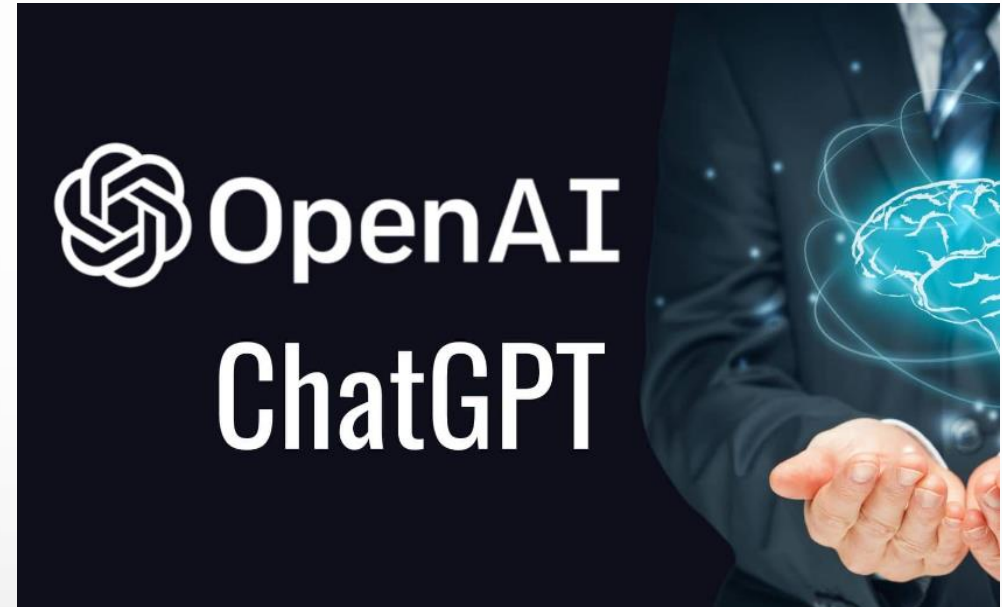






사용자 수가 100만에 이른 시간

- 인스타그램 : 2.5 months
- 스포티파이 : 5
- 페이스북 : 10
- 넷플릭스 : 3년 6개월



5일

전 세계 기업들 중 75%가 ChatGPT (혹은 그에 준하는 생성형 인공지능 알고리즘)을 도입하든 금지시키든 할 계획

- BlackBerry 보안 업체 조사 결과



빌 게이츠, "ChatGPT와 같은 생성 인공지능은 우리의 세상을 바꿀 것!"



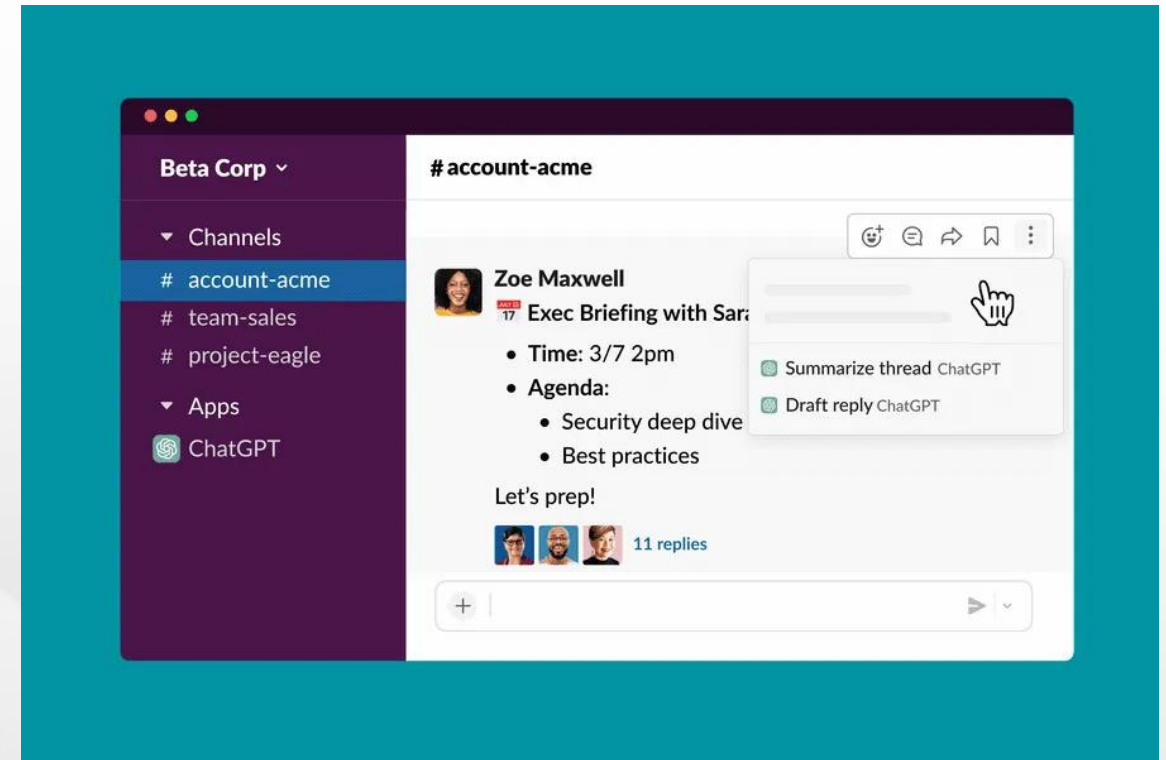
ChatGPT is the most 'revolutionary' tech in 40 years

Bill Gates says A.I. like ChatGPT is 'every bit as important as the PC, as the internet'

생성형 AI 사용 분야



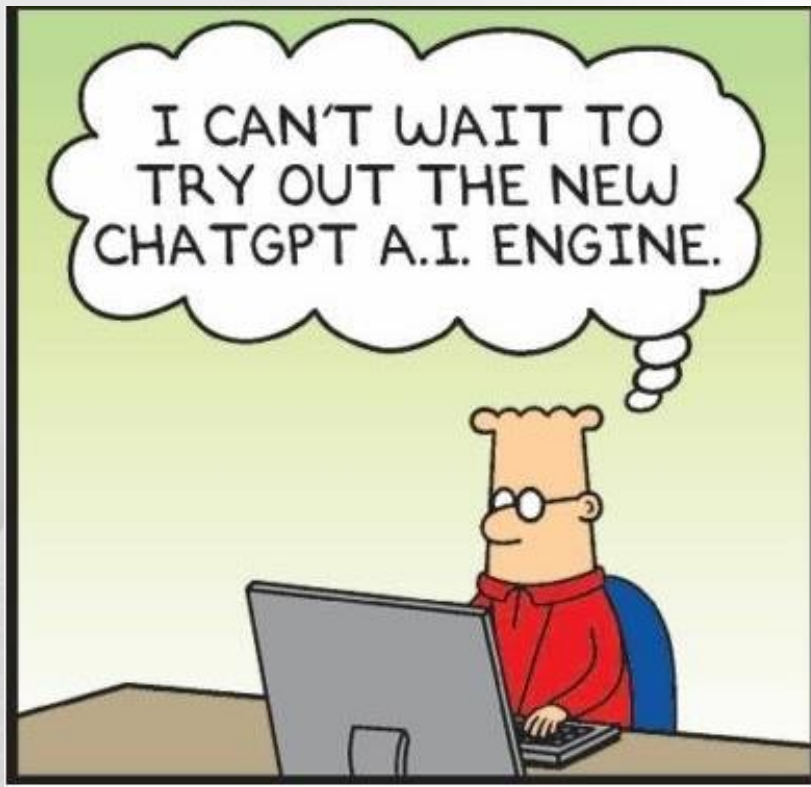
Application 과 ChatGPT : Slack 사례



보안과 ChatGPT



2023년도에 80%의 보안 전문가들이 ChatGPT를 사용합니다.



대부분의 보안 공급업체는 2023년에 AI 공동 초기 제품을 출시할 예정이며 고객에게 해당 SKU에 대해 50% 더 지불하도록 요청할 것입니다.



해커들이 사이버 보안을 위해 AI를 사용하여 약 2천만 달러의 상금을 놓고 경쟁할 것이라고 Biden 행정부가 발표

게시일: 2023년 8월 9일 수요일·오후 1시(EDT)



로렌 페이너
@LAUREN_FEINER

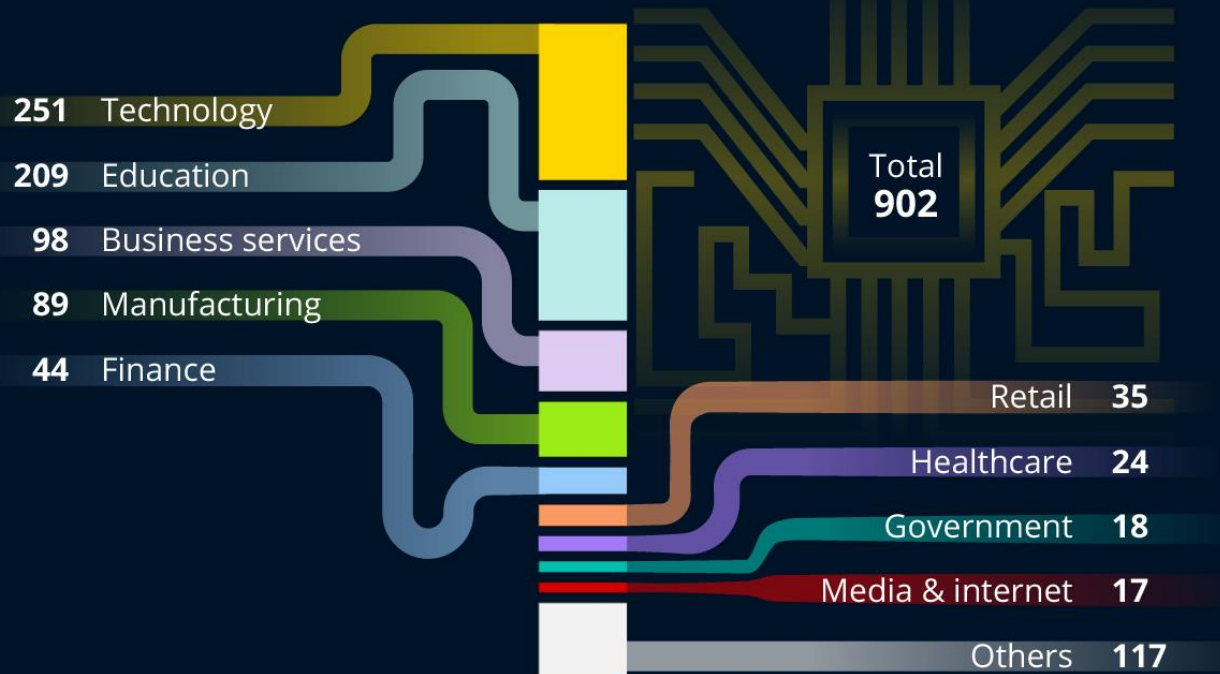
공유하다    

- 키 포인트**
- Biden 행정부는 AI를 사용하여 중요한 미국 인프라를 사이버 보안 위험으로부터 보호하는 새로운 해킹 과제를 발표했습니다.
 - AI 사이버 챌린지는 약 2,000만 달러의 상금을 수여할 예정이며, 대회에 자신의 기술을 제공할 선도적인 AI 기업인 Anthropic, Google, Microsoft 및 OpenAI의 협력이 포함됩니다.
 - 정부는 AI의 약속이 미국의 중요한 시스템을 더욱 안전하게 보호하는 데 도움이 되기를 바라고 있습니다.



Which Sectors Are Working With OpenAI?

Number of companies/organizations using Open AI in their business processes worldwide, by sector* (as of Jan. 2023)



* OpenAI is an artificial intelligence research and deployment company (e.g. ChatGPT)
Source: Enterprise Apps Today



statista

출처: 세계경제포럼

ChatGPT 리스크





ChatGPT

Risks for Corporate Data

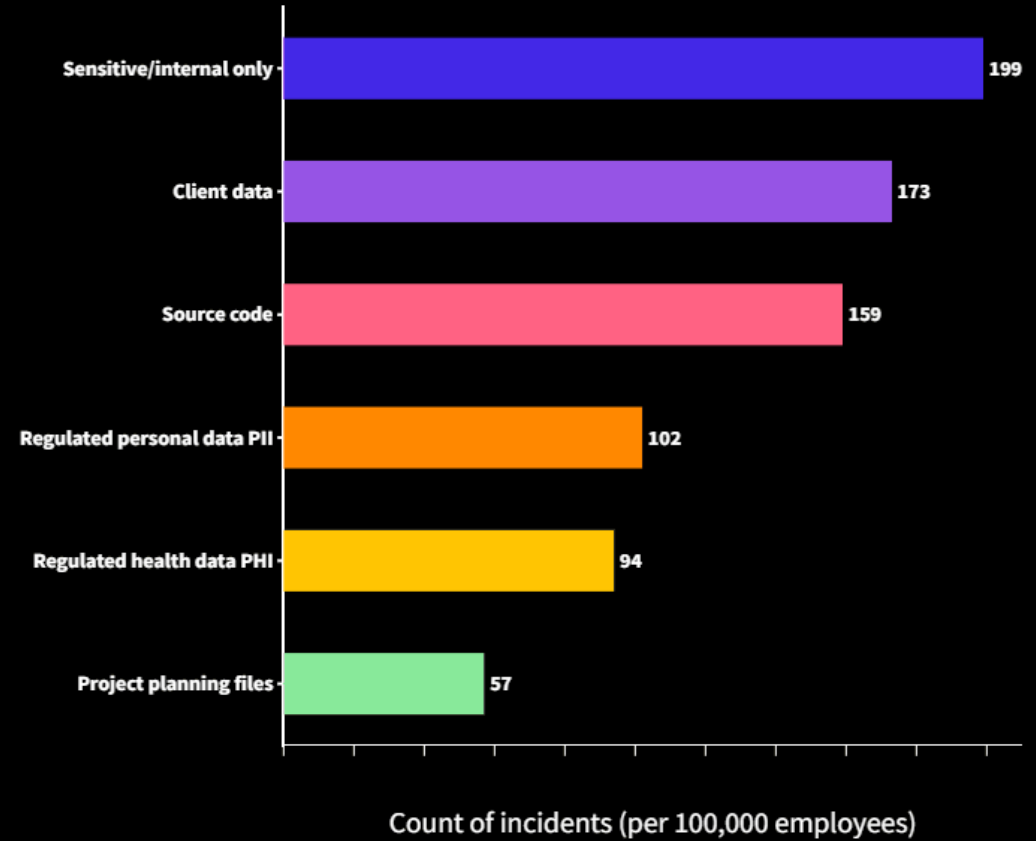
Cyberhaven은 직원의 4.9% 이상이 회사의 민감한 데이터를 ChatGPT에 붙여넣는 것을 발견했습니다



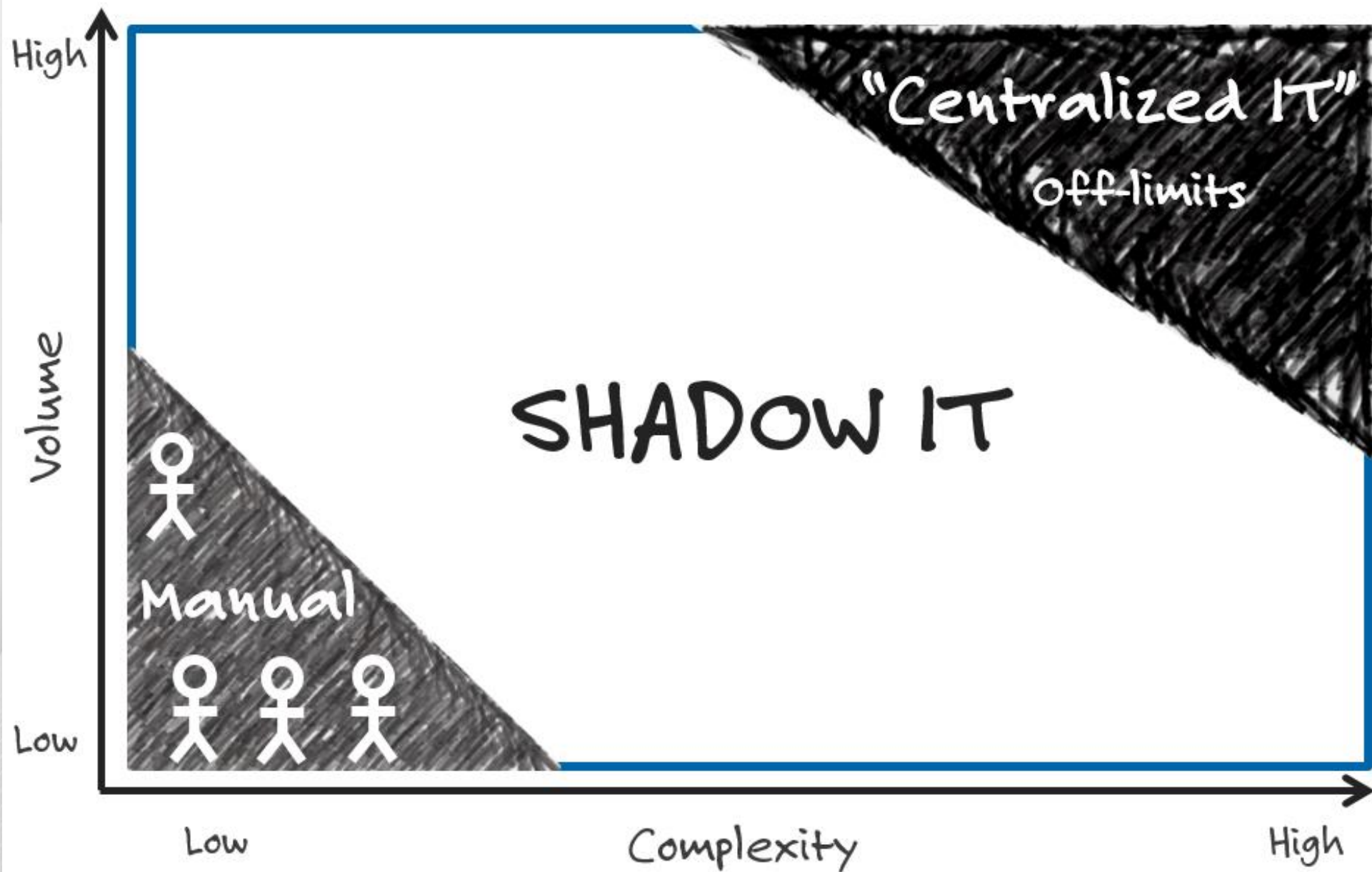
How much sensitive data goes to ChatGPT

(Incidents per 100,000 employees the week of February 26 - March 4)

Source: Cyberhaven.com



CYBERHAVEN





Shadow IT 에 대한 보안이 필요한 이유? by ChatGPT

- **데이터 보호:**
- Shadow IT는 보안 프로토콜을 거치지 않고 사용되는 경우가 많습니다. 조직 내부나 외부에서 민감한 데이터가 노출될 수 있으며, 이로 인해 개인정보 유출, 지적재산권 침해 등의 문제가 발생할 수 있습니다.
- **규정 준수:**
- 다양한 규정과 법률에 따라 조직은 데이터 보호와 관련된 기준을 준수해야 합니다. Shadow IT는 이러한 규정을 준수하는 것을 어렵게 만들 수 있습니다.
- **악성 소프트웨어 및 사이버 위협:**
- 공식적인 IT 부서가 감시하지 않는 IT 자원은 악성 소프트웨어나 해킹 등의 사이버 위협에 노출될 수 있습니다.
- **네트워크 및 시스템 호환성:**
- Shadow IT는 조직 전체 시스템과 호환되지 않을 수 있습니다. 이로 인해 네트워크에 문제가 발생하거나 서로 다른 시스템 간의 데이터 통합이 어려워질 수 있습니다.
- **관리와 모니터링의 어려움:**
Shadow IT는 공식적인 프로세스를 거치지 않기 때문에 관리와 모니터링이 어려울 수 있습니다. 이로 인해 문제 발생 시 대응이 늦어질 수 있습니다.
- **비용 증가:**
각 부서나 직원이 독자적으로 IT 자원을 구매하고 유지보수하면, 중복 구매와 유지보수 비용이 증가할 수 있습니다.



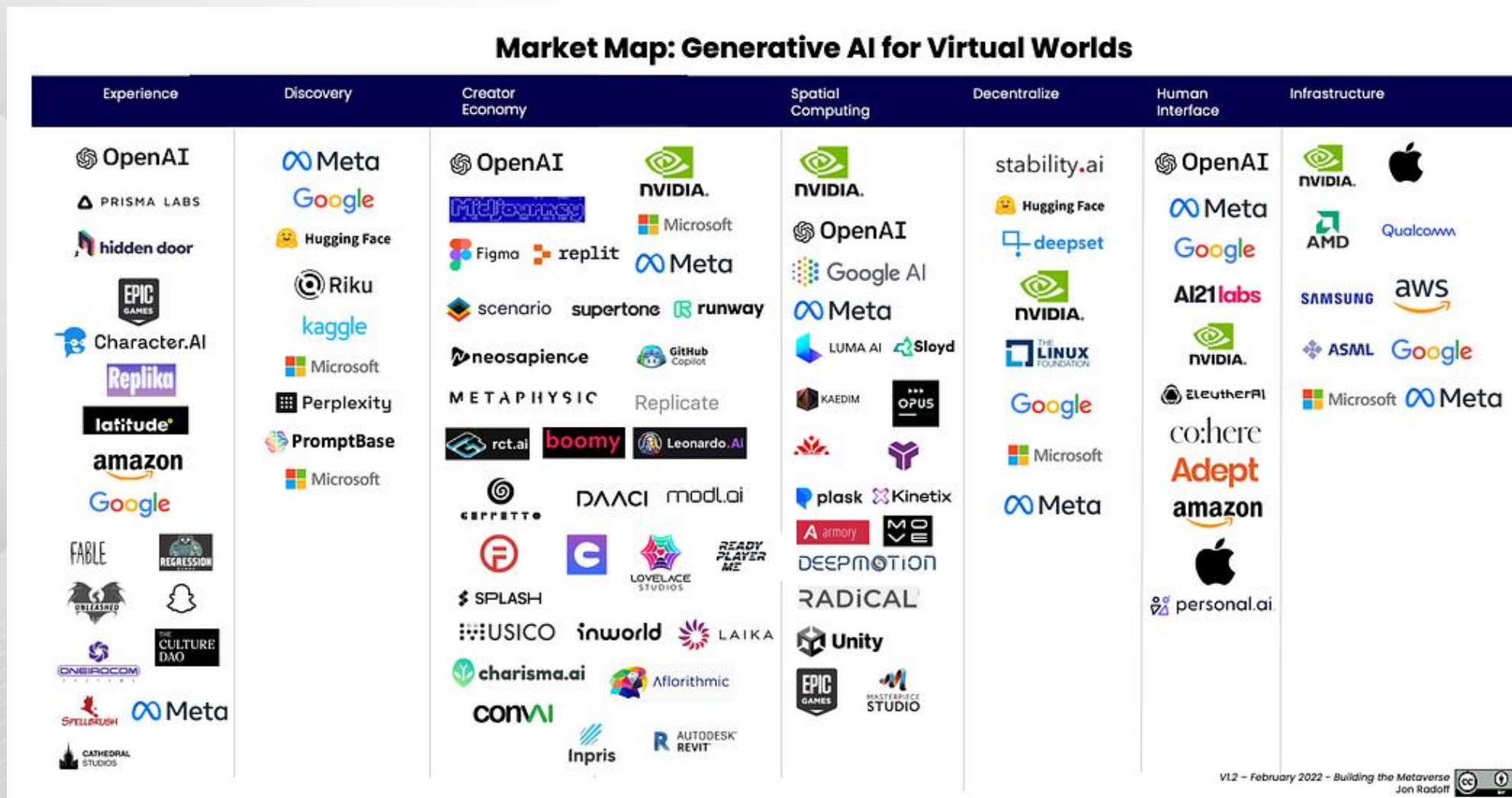
Visibility & Control

Shadow IT 관리 방안





우리 회사는 얼마나 많은 생성형 AI 를 사용하고 있을까?





분석된 654개 AI

DB

Skyhigh Security Dashboards Governance Analytics Incidents Policy Reports Custom Apps

Activities > > Cloud Registry

Filters Views Service Category: Artificial Intelligence Save View

Service Category

- Project Management 656
- Artificial Intelligence 654
 - Artificial Intelli... 654
- e-Commerce 563
- CRM 528
- Cloud Storage 511
- Networking 451
- Legal 445
- Service Desk and Su... 384

Risk Type

- High Risk

Cloud Services

Risk	Service Name	Category	Subcategory	Service Group(s)	Used	Enterprise Ready™
<input type="checkbox"/> 6	1Law	Artificial Intelligence	Artificial Intelligence	Artificial Intelligen	No	--
<input type="checkbox"/> 7	4DAGE	Artificial Intelligence	Artificial Intelligence	KAKAO, High Risk	No	--
<input type="checkbox"/> 5	[24]7.ai	Artificial Intelligence	Artificial Intelligence	Artificial Intelligen	No	--
<input type="checkbox"/> 5	Aavenir	Artificial Intelligence	Artificial Intelligence	Artificial Intelligen	No	--
<input type="checkbox"/> 5	Abe AI	Artificial Intelligence	Artificial Intelligence	Artificial Intelligen	No	--
<input type="checkbox"/> 5	Abi	Artificial Intelligence	Artificial Intelligence	Artificial Intelligen	No	--
<input type="checkbox"/> 4	Accenture - Artificial Intelligence	Artificial Intelligence	Artificial Intelligence	Artificial Intelligen	No	--
<input type="checkbox"/> 6	Acrotrend	Artificial Intelligence	Artificial Intelligence	Artificial Intelligen	No	--



Skyhigh Security는 어떻게 AI 서비스로부터 데이터를 보호하는가?

a. Which AI apps are available today

Cloud Registry

Filters Views Service Category: Artificial Intelligence Save View

Service Category

- Media 695
- Project Management 657
- Artificial Intelligence 651
 - Artificial Intelli... 651
- e-Commerce 564
- CRM 528
- Cloud Storage 512
- Networking 451

Risk Type

- High Risk
- Low Risk
- Medium Risk

Cloud Services

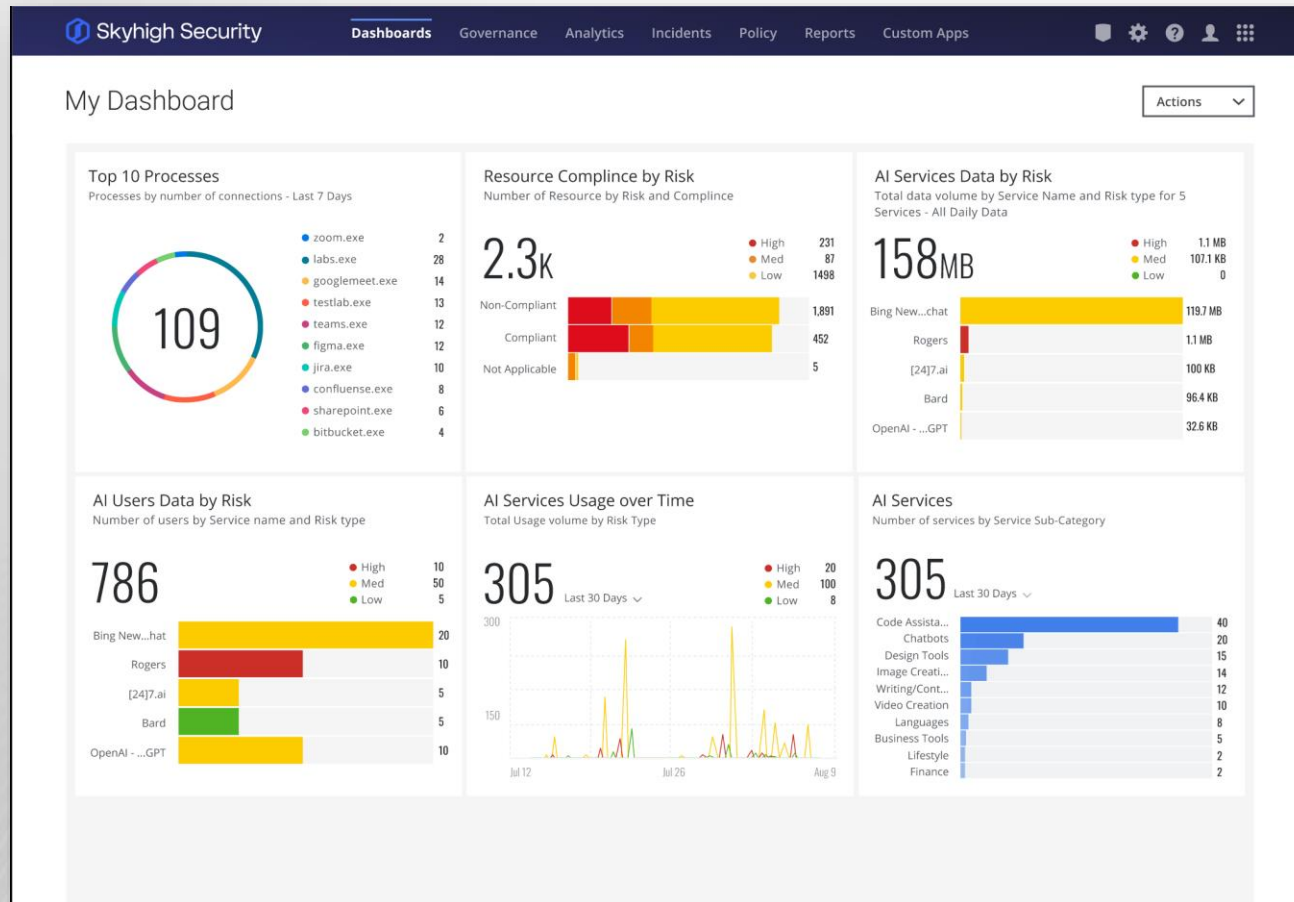
Actions

<input type="checkbox"/>	Risk	Service Name	Category	Subcategory	Service Group(s)	Used ↓	Enterprise Ready™
<input type="checkbox"/>	5	[24]7.ai	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	Yes	--
<input type="checkbox"/>	4	LivePerson AI	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	Yes	--
<input type="checkbox"/>	6	OpenAI - ChatGPT	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	Yes	--
<input type="checkbox"/>	6	Bing New (Bing Chat)	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	Yes	--
<input type="checkbox"/>	4	Vidado (Formerly Captricity)	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	No	--
<input type="checkbox"/>	7	Brevity AI	Artificial Intelligence	Artificial Intelligence	High Risk Services, C	No	--
<input type="checkbox"/>	4	Lionbridge	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	No	--
<input type="checkbox"/>	4	PROS	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	No	--
<input type="checkbox"/>	6	iFLYTEK Open Platform	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	No	--
<input type="checkbox"/>	6	New Interact	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU GI	No	--



Skyhigh Security는 어떻게 AI 서비스로부터 데이터를 보호하는가?

- Which AI apps are available today
- Discover which AI Apps are being used by **which users**





Skyhigh Security는 어떻게 AI 서비스로부터 데이터를 보호하는가?

- Which AI apps are available today
- Discover which AI Apps are being used by which users
- Know about the **amount of data** being uploaded to each app

Services

Filters Views Service Group: AI Warning Save View

Service Group: AI Warning 4 Services

Service Group	Risk	Service Name	Category	Subcategory	Service Group(s)	Users	Upload Data	Inbound Data	Outbound Data	Allowed Requests	Denied Requests	Service First Used	
<input type="checkbox"/> HighRiskCloudStorage...													
<input type="checkbox"/> Legal Risk													
<input type="checkbox"/> Breached-services													
<input type="checkbox"/> Sanctioned-services													
<input type="checkbox"/> Blocked-services													
<input type="checkbox"/> Permitted-services													
<input checked="" type="checkbox"/> AI Warning													
	<input type="checkbox"/>	6	OpenAI - ChatGPT	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	2	15.7 KB	3.8 KB	17.7 KB	4	3	May 31, 2023 UTC
	<input type="checkbox"/>	4	Rogers	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	4	2.1 MB	25.6 MB	7.3 MB	341	0	May 26, 2023 UTC
	<input type="checkbox"/>	6	Bing New (Bing Chat)	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	784	7.2 MB	94.9 MB	25.7 MB	26.5 K	0	Apr 28, 2023 UTC
	<input type="checkbox"/>	5	[24]7.ai	Artificial Intelligence	Artificial Intelligence	Medium Risk - EU	2	60.8 KB	132 KB	90 KB	31	0	Nov 01, 2017 UTC



Skyhigh Security는 어떻게 AI 서비스로부터 데이터를 보호하는가?

- Which AI apps are available today
- Discover which AI Apps are being used by which users
- Know about the amount of data being uploaded to each app
- Block risky AI Apps**
- Block **some activities (login, upload)** in specific AI chatbots

The screenshot displays the Skyhigh Security console interface. On the left, the 'Web Policy' sidebar is visible, with 'Application Control' and 'Activity Control New 1' highlighted with red boxes. The main content area shows the configuration for 'Activity Control New 1', which is set to 'Block services based on Service Groups or Service Categories'. Under the 'Service Groups (1)' section, the 'AI Warning: Select Activities to Block' checkbox is checked and highlighted with a red box. Under the 'Service Category (3)' section, three categories are listed with their respective activities: 'Content Sharing (All): Upload', 'IaaS Admin Console (All): Login', and 'Development (1/7): Login'. Under the 'Individual Services (1)' section, 'Bebo: Photo share Post' is listed with a checked checkbox.



Skyhigh Security는 어떻게 AI 서비스로부터 데이터를 보호하는가?

- Which AI apps are available today
- Discover which AI Apps are being used by which users
- Know about the amount of data being uploaded to each app
- Block risky AI Apps
- Block some activities (login, upload) in specific AI chatbots
- Coach users** on the risks of using AI chatbots

The screenshot displays the configuration interface for Web Filtering Coach URLs. On the left, a table lists coaching rules with columns for Name, Criteria, Operator, and Value. The first rule is 'Category & Domain Coaching' with criteria 'IF All Traffic'. Below this, a 'Preset Rules' section includes options to set a coaching session timeout (30 Min) and to coach & allow access to categories and domains. On the right, the 'Web Filtering Coach URLs' panel allows adding a description, selecting actions, and listing URLs for smart matching, such as 'https://openai.com/' and 'https://openai.com/blog/chatgpt'.

Name	Criteria	Operator	Value
Category & Domain Coaching	IF All Traffic	-	-

Web Filtering Coach URLs

Add description

Actions ▾

Smart Match	Comment
https://openai.com/	
https://openai.com/blog/chatgpt	



Skyhigh Security는 어떻게 AI 서비스로부터 데이터를 보호하는가?

- Which AI Apps are available today
- Discover which AI Apps are being used by which users
- Know about the amount of data being uploaded to each app
- Block risky AI Apps
- Block some activities (login, upload) in specific AI Apps
- Coach users on the risks of using AI Apps
- Apply DLP policies to allowed AI Apps**

Web DLP

This rule set blocks the transfer of sensitive information outside your organization's network based on DLP Classifications that McAfee maintains and that you can configure.

! Scope DLP Policies individually.

Global Downselection Settings

- File types to exclude from Web DLP evaluation
- Limit processing the files less than MB

DLP Policies

<input type="checkbox"/>	Source Code	keven_how...	Jan 31, 2022 UTC
<input checked="" type="checkbox"/>	AIP	keven_how...	Aug 12, 2021 UTC
<input checked="" type="checkbox"/>	SSN_PII Governance Policy	keven_how...	May 3, 2022 UTC
<input checked="" type="checkbox"/>	PCI	keven_how...	Feb 24, 2022 UTC
<input checked="" type="checkbox"/>	HIPAA	keven_how...	Mar 3, 2021 UTC
<input checked="" type="checkbox"/>	Confidential Governance Policy	keven_how...	May 18, 2021 UTC
<input checked="" type="checkbox"/>	Block sensitive data from IP ownership sites	keven_how...	Dec 16, 2020 UTC



3. 클라우드와 PC의 데이터 동기화

Auto Sync SaaS Count

Number of services by Service Name for 78 Services - All Daily Data

Data
78



Auto Sync client and Cloud

Total data volume by Service Name for 78 Services - All Daily Data

Data
42.5GB



4. AI Chatbot 서비스 사용현황:

AI Chatbot Services count

Number of services by Service Name for 3 Services - All Daily Data

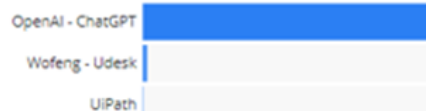
Data
3



AI Chatbot Service

Total data volume by Service Name for 3 Services - All Daily Data

Data
27.6MB



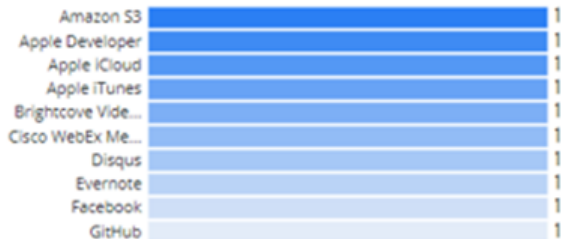
751.8 MB
730.5 MB
716.5 MB
608 MB
297.9 MB

5. File Sharing 서비스 사용현황:

File Sharing SaaS count

Number of services by Service Name for 115 Services - All Daily Data

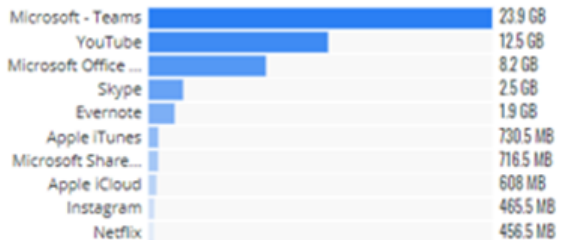
Data
115



File Sharing SaaS

Total data volume by Service Name for 115 Services - All Daily Data

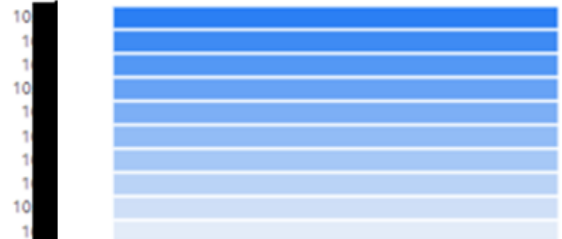
Data
55GB




File Sharing Support SaaS Users

Number of users by User for 423 Users - All Daily Data

Data
423



Shadow IT 관리 방안 - 진단 서비스 활용



Shadow IT 언제까지 손놓고 있을래?

SaaS 애플리케이션 위험 관리의 시작은 가시성 확보에서부터!

Shadow IT, 왜 관리해야 할까?

- ☑ 회사의 직원이 실제로 사용하고 있는 SaaS의 수와 종류에 대해서 인지하지 못하고 있다.
- ☑ SaaS를 통해 유입되고 유출되는 정보에 대한 가시성이 없다.
- ☑ 위의 상황을 제어할 수 있는 방안이나 발행되는 문제점에 대한 대안이 전혀 없다.

우리 회사가 지금 이렇다면,
스카이하이시큐리티 컨설팅
한 번 받아보시는게
어떠세요?!

01 컨설팅 신청하기

02 SaaS 사용 현황 파악

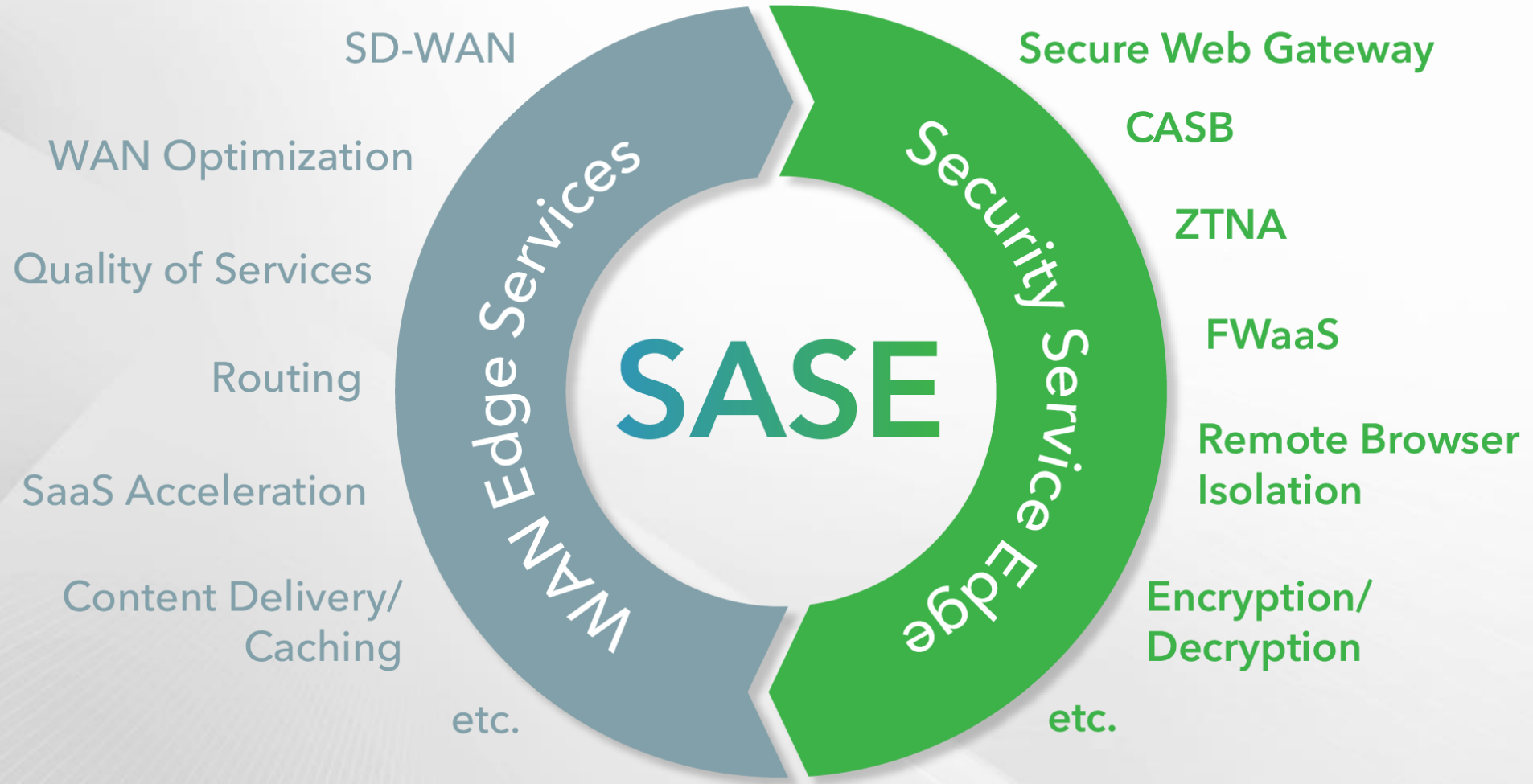
03 진단 상황에 따른 방안 제시

컨설팅 신청하기



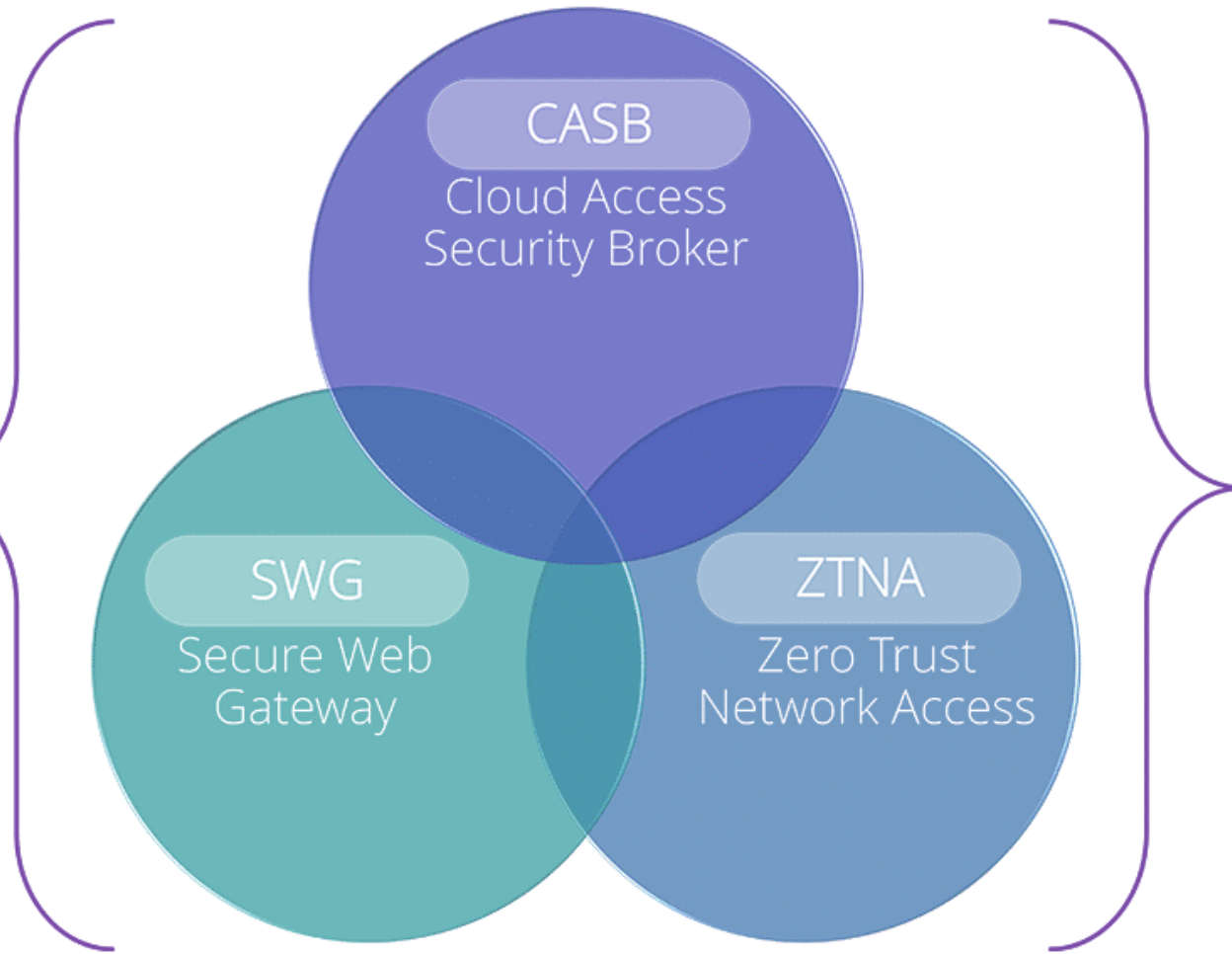


Shadow IT를 위한 보안 : SSE(security service Edge)





Data Protection
“Data awareness” is a
core embedded
function



Threat Protection
“Single Pass”
inspection is a
requirement

Shadow IT 관리 방안 with Skyhigh SSE



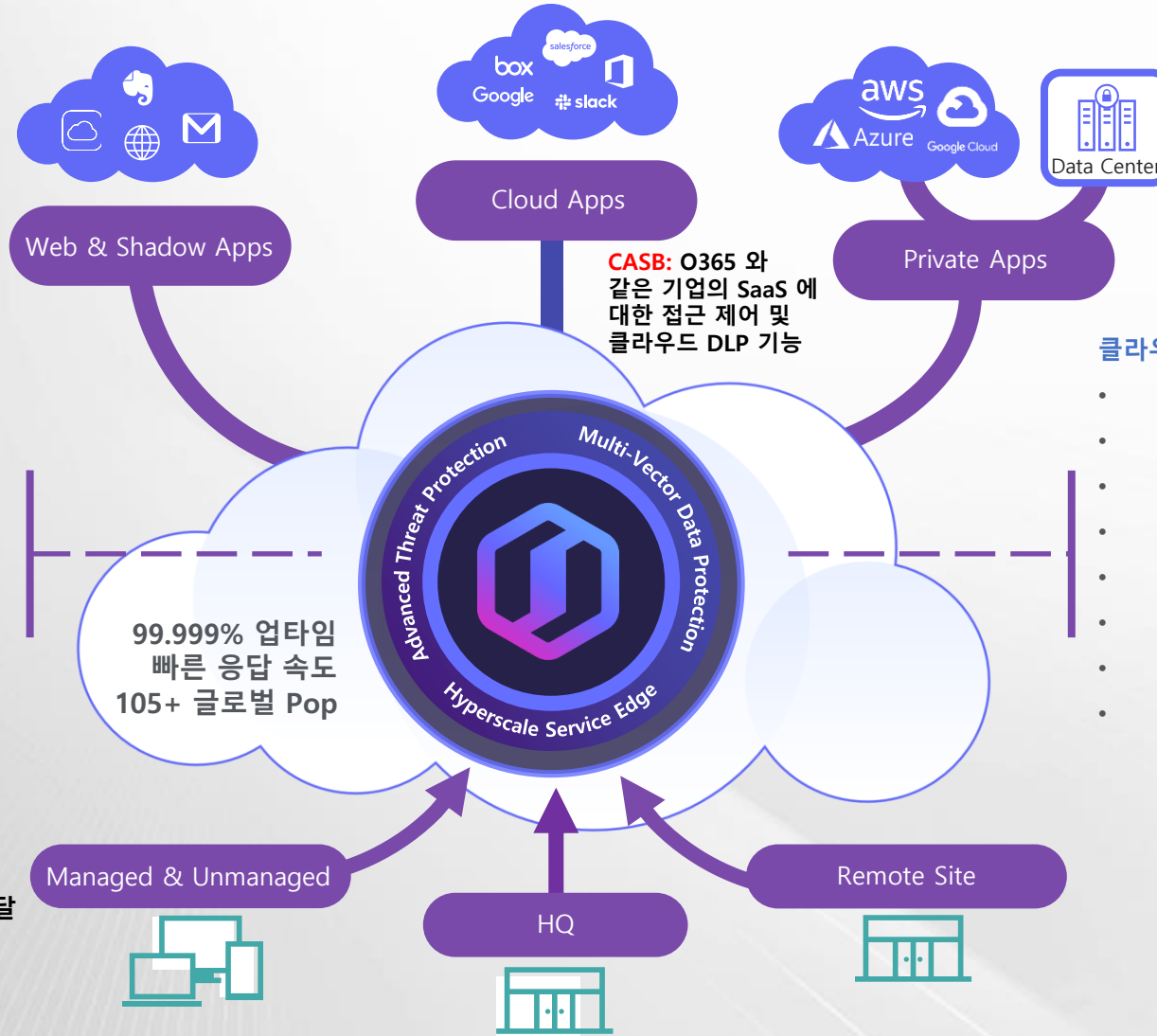
SWG(Proixy): 인터넷 사용 시 유해 사이트 차단, 위협 침투 방지, 클라우드 Shadow IT 제어, 웹격리, DLP, OCR 기능으로 안전한 인터넷 사용을 보장

특징:

- 웹정책
- Shadow IT 차단
- 웹격리
- 위협 차단
- 공유/협업 제어
- 비정상행위탐지

엔드포인트 에이전트 역할:

- CASB는 Agent 불필요
- 인터넷 트래픽을 근거리 POP으로 전달
- Endpoint DLP Addon (필요 시)



CASB: O365 와 같은 기업의 SaaS 에 대한 접근 제어 및 클라우드 DLP 기능

ZTNA: AWS, Azure, GCP, vCenter 등에서 운영되는 내부 서비스에 대한 접근 제어/DLP/디바이스 제어 기능을 제공

클라우드 POP 제공 기능

- SWG (Proxy)
- AV
- CASB
- DLP
- OCR
- 웹격리
- ZTNA
- FWAAS/IDS (Q4 2022)



Summary

- 생성형 AI 서비스는 보안에 있어서 큰 취약점이다
- 누가 어떤 AI 서비스에 얼마의 데이터를 올리는지 아는 것이 보안의 취약성을 줄일 수 있는 길이다
- 생성형 AI 서비스 사용 결정에 있어 제일 우선시 해야 할 것은,
Shadow IT 에 대한 가시성 확보
- Shadow IT 진단 서비스를 통해서 현황 파악이 필요





Shadow IT 관리 및 하이브리드 보안을 위한,

Skyhigh Security

SSE (Security Service Edge)



감사합니다

