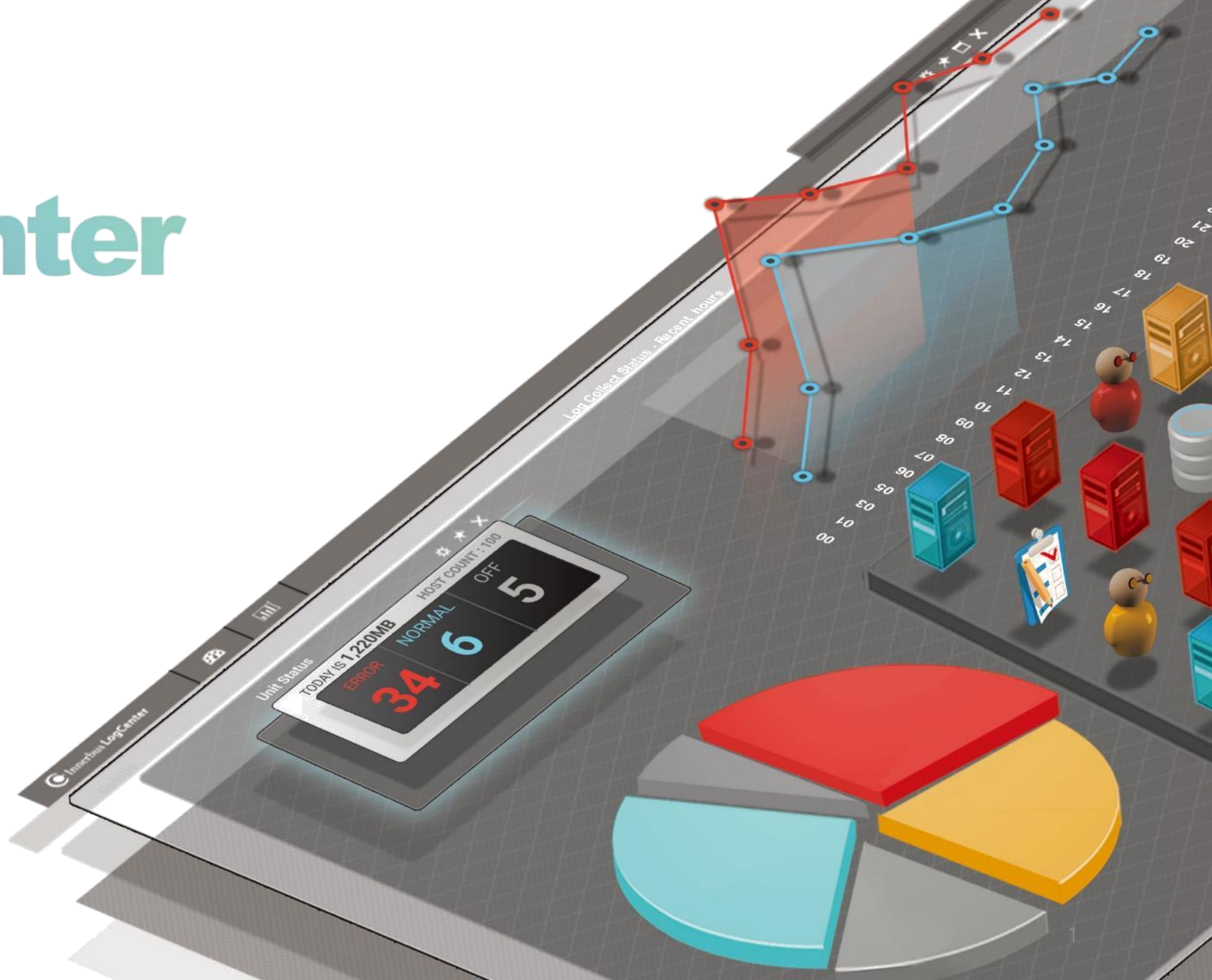
간편하고 직관적인 로그관리

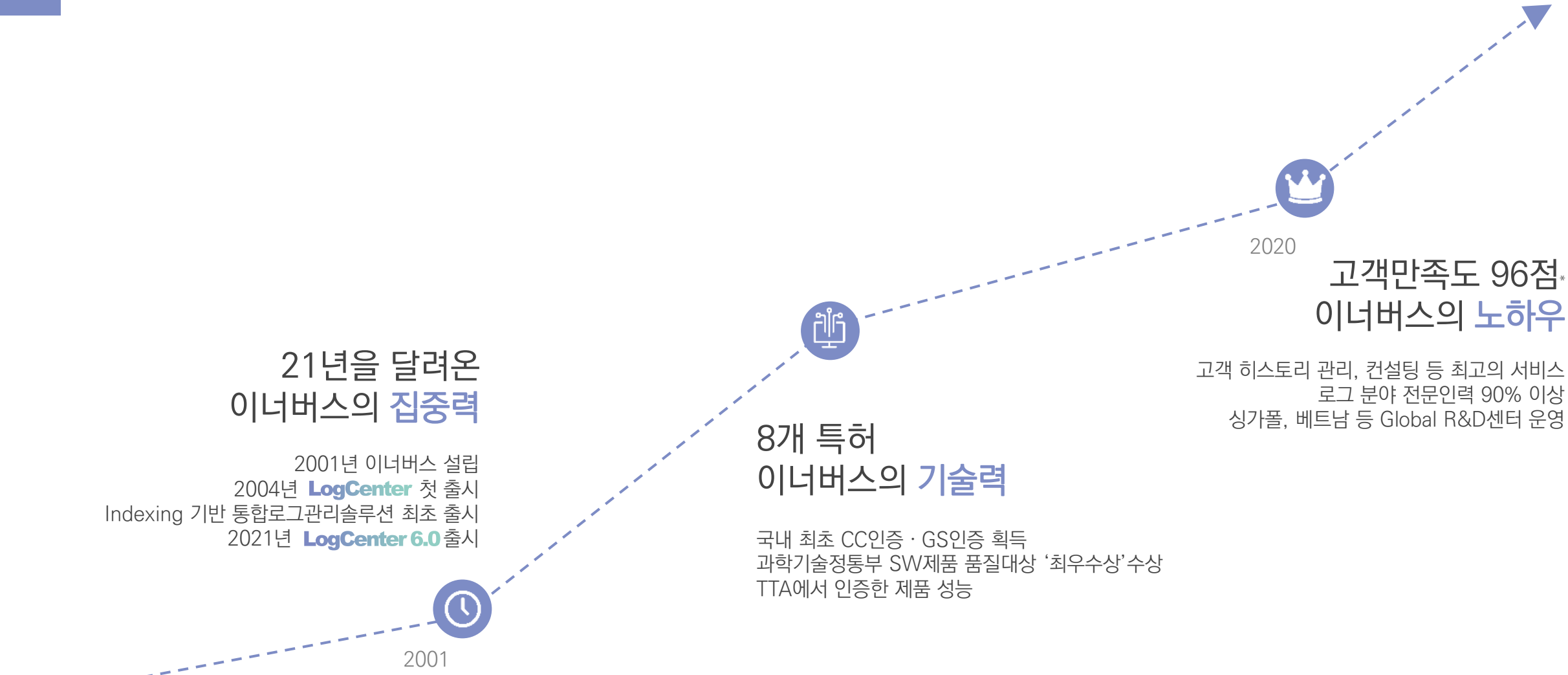
LogCenter



INDEX

01 | 이너버스 이야기

안녕하세요. 21년 넘게 로그만을 연구, 개발하고 있는 R&D 기업 이너버스 입니다.



21년을 달려온 이너버스의 집중력

2001년 이너버스 설립
2004년 LogCenter 첫 출시
Indexing 기반 통합로그관리솔루션 최초 출시
2021년 LogCenter 6.0 출시

2001

8개 특허 이너버스의 기술력

국내 최초 CC인증 · GS인증 획득
과학기술정통부 SW제품 품질대상 '최우수상'수상
TTA에서 인증한 제품 성능

2020

고객만족도 96점* 이너버스의 노하우

고객 히스토리 관리, 컨설팅 등 최고의 서비스
로그 분야 전문인력 90% 이상
싱가폴, 베트남 등 Global R&D센터 운영

*2020년 해피메일 고객만족도 설문 결과

01 | 이너버스 이야기

이너버스는 지금 시장을 리드합니다. 그리고 앞으로도 리드할 겁니다.

조달시장에서 믿고 선택하는

1위

9년 연속 1위 제품

'13~'21년 9년 연속

** 조달청 나라장터 품명:시스템관리소프트웨어 통합로그관리 부문 기준*

조달시장의 약 ⅔ 차지
2위와 격차 3배

59%

압도적인 시장 점유율

'13~'21년 조달 평균점유율

** 조달청 나라장터 품명:시스템관리소프트웨어 통합로그관리 부문 기준*

공공, 기업 등 다양한 시장에서

700+

국내 최다 레퍼런스

이너버스의 최고의 고객들

02 | 그리고 여러분의 고민들

쌓아두기만 했던 로그를 LogCenter로 관리해 봅시다
보안사고나 장애를 파악하고, 원인을 규명하고, 또 필요한 근거 데이터를 뽑아내는 데 로그를 활용할 수 있습니다.

"로그는 저장만 하면 된다?"

"로그는 사고나 장애 원인을 파악하고 예방할 수 있는 근거 데이터다."

LogCenter 는 로그를 활용 가치가 높은 정보자산으로 만듭니다.

01
컴플라이언스 준수

"로그 컴플라이언스를 준수하려면
어디서부터 어디까지 관리해야 하는 지 막막합니다."

02
빅데이터 로그 처리

"로그 데이터가 워낙 많다보니
필요한 로그를 찾는 데만 너무 오래 걸립니다"

03
로그 분석과 모니터링

"로그를 제대로 활용해보고 싶은데
전문 지식이나 교육 없이는 분석이 어렵고 복잡해요."

02 | 그리고 여러분의 고민들

쌓아두기만 했던 로그를 LogCenter로 관리해 봅시다
보안사고나 장애를 파악하고, 원인을 규명하고, 또 필요한 근거 데이터를 뽑아내는 데 로그를 활용할 수 있습니다.

1 저장 방법

접속기록이 **위변조 및 도난, 분실되지 않도록** 안전하게 보관하여야 한다.

2 보존 기간

개인정보처리 시스템에 접속한 기록을 **1년 이상 보관** 및 관리하여야 한다.

3 점검 기간

월 1회 이상 점검하여야 한다.

개인정보 보호법

[행정안전부 법률 제16930호]
개인정보보호법 시행령, 안전성 확보조치 기준, 표준 개인정보보호지침 등

개인정보의 안전성 확보조치 기준 제8조

개인정보처리시스템에 접속한 기록을 **1년 이상 보관** 및 관리하여야 한다.
(*5만명 이상의 정보주체의 경우 혹은 고유식별정보 등 민감정보 포함 시, **2년 이상**)

월 1회 이상 점검하여야 한다.

접속기록이 **위조·변조 및 도난, 분실되지 않도록** 안전하게 보관하여야 한다.

정보통신 망법

[방송통신위원회 법률 제17358호]
정보통신망법 시행령, ISMS, 개인정보의 기술적·관리적 보호조치 기준 등

개인정보의 기술적·관리적 보호조치 기준 제5조

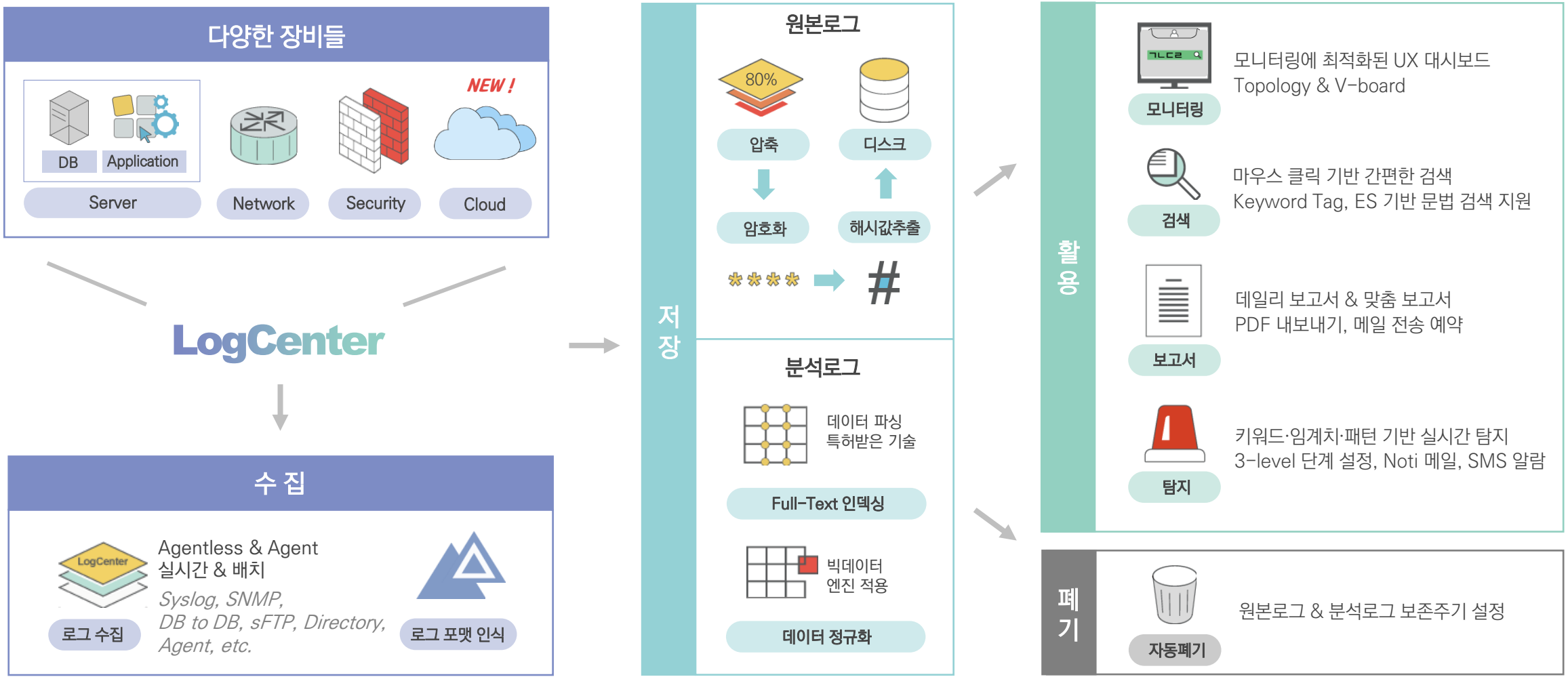
개인정보처리시스템에 접속한 기록을 **월 1회 이상 확인·감독**하여야 한다.

최소 **1년 이상** 접속기록을 보존·관리하여야 한다.
(*기간통신사업자의 경우 최소 **2년 이상**)

접속기록이 **위·변조되지 않도록** 별도의 물리적인 저장 장치에 보관하여야 한다.

03 | LogCenter 를 소개합니다

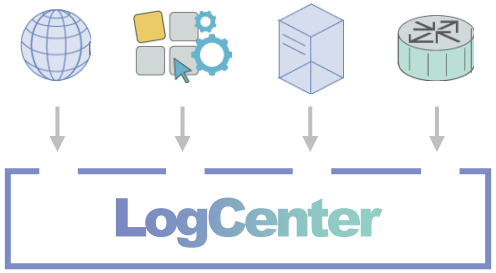
다양한 이기종 장비에서 발생하는 로그를 LogCenter로 수집하고, 저장, 분석, 폐기 합니다.



03 | LogCenter 를 소개합니다

이너버스의 Hyper Full-text Indexing 특허기술이 Bigdata Engine과 만나 더 강력해졌습니다.
안정적인 수집 성능과 탄탄한 분석 엔진, 독보적인 기술력 모두를 경험해 보세요.

안정적인 수집 성능



TTA 시험항목

"4대의 수집대상 서버에서 로그를 전송하여
수집 성능이 200,000EPS 이상인지 확인"

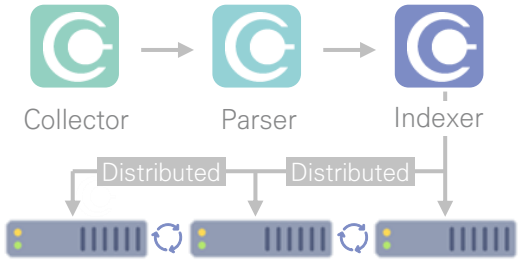
목표치: 200,000EPS 이상

측정치: 평균 258,296EPS

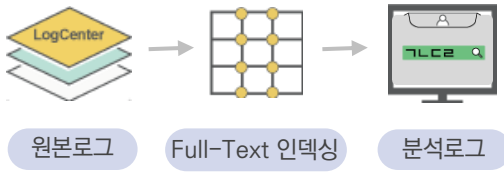
**TTA 성능인증, 2017*

탄탄한 분석 엔진

Bigdata Engine으로 분산처리도 가볍게



원본로그 수집 시 실시간 Full-Text 인덱싱



독보적인 기술력

"로그관련 특허 8종 中 로그데이터
파싱기술 관련 특허 3종 보유"

특허 제 10-0817562호

발명의 명칭 : **대용량 로그 파일의 인덱싱 방법**

… 인덱싱로그파일의 인덱싱 방법, 이를 내장한 컴퓨터가 판독 가능한 기록매체 및 이를 수행하기 위한 인덱싱 시스템이 개시 된다. 이에 따라, 대용량의 로그파일에서 특정 문자열이 포함된 로그라인을 검색하여 집계하는 로그분석 통계에서 발견된 로그라인들에 대응하는 발견 파일의 크기를 줄일 수 있다. …

03 | LogCenter 를 소개합니다

LogCenter의 손쉬운 사용성이 또 한 번 강화되었습니다.
더 보기 편안한 화면, 더 심플한 메뉴, 그리고 더 편리해진 컨텐츠들로 대시보드를 자유롭게 구성해 보세요.

심플한 메뉴

Topology, 대시보드, 검색, 보고서, 알람 등
아이콘 클릭으로 한 번에 접속

보기 편한 화면

깨끗하고 깔끔한 화이트White 모드,
눈의 피로도를 줄여주는 다크Dark 모드 설정

편리한 컨텐츠

V-board 위젯, 보고서 위젯, 그리고 탐지패턴까지
모든 컨텐츠를 Drag & Drop

03 | LogCenter 를 소개합니다

LogCenter의 손쉬운 사용성이 또 한 번 강화되었습니다.
더 빠르고 쉬워진 검색, 더 간편해진 분석 기능으로 어렵기만 했던 로그를 이제 쉽게 분석해보세요.

빠르고 쉬운 검색

마우스 클릭 몇 번으로 빠르게 검색하기
컬럼 태그 기능으로 검색조건도 간단하게 설정

간편한 분석

분석하고 싶은 데이터가 있다면 통계 버튼을 클릭
컬럼 체크만 하면 즉시 분석 완료

풀 텍스트 인덱싱

로그의 모든 값을 인덱싱하면
무엇이든 키워드로 활용

LogCenter 를 이렇게 사용하세요

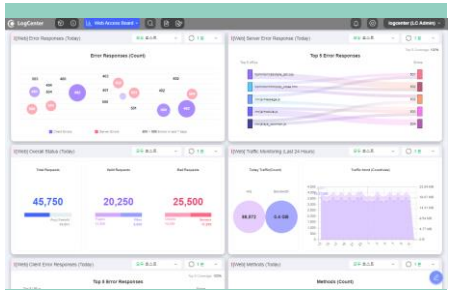
로그 수집, 저장, 분석, 검색 그리고 관리까지. LogCenter의 대표 기능들을 소개합니다.

Topology

50+ 호스트 아이콘, 연동로그 설정, 리소스 임계치 체크 후 3단계 자동 컬러링(심각/정상/중지)

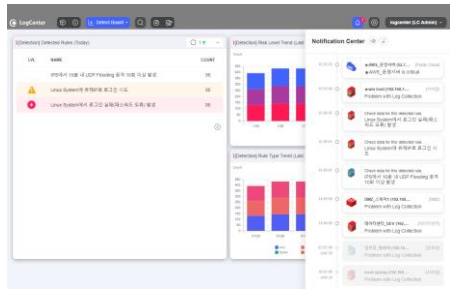
Host Info

CPU/MEM/DISK 리소스 정보, 네트워크 사용량 정보, 호스트별 타임라인(히스토리) 이벤트 관리



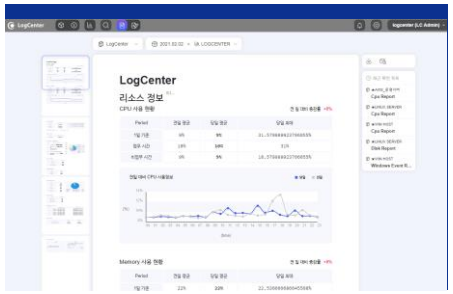
V-board

실시간 UX대시보드, 완성형 컨텐츠 위젯 & 사용자 위젯, 자유로운 구성, 위젯 클릭 시 상세 로그데이터 뷰



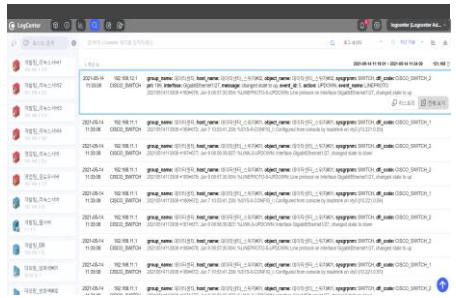
Detection

9-type 탐지유형, 3단계 위험도 설정, 룰/시나리오 컨텐츠, Noti Push 및 메일, SMS 알람



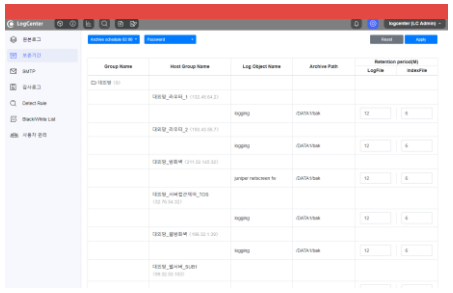
Report

호스트별 데일리 보고서, 리소스 현황 등 보고서 전용 컨텐츠, PDF 내보내기, 메일 예약 전송



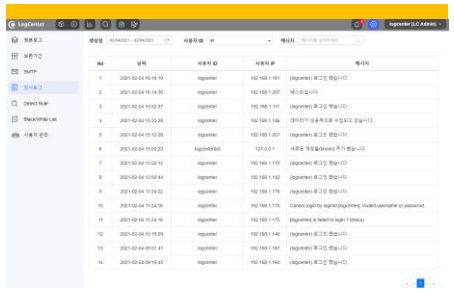
Search

검색어 키워드 검색, 문법 검색, 검색어 태그 기능, 최근 검색이력, 컬럼 통계



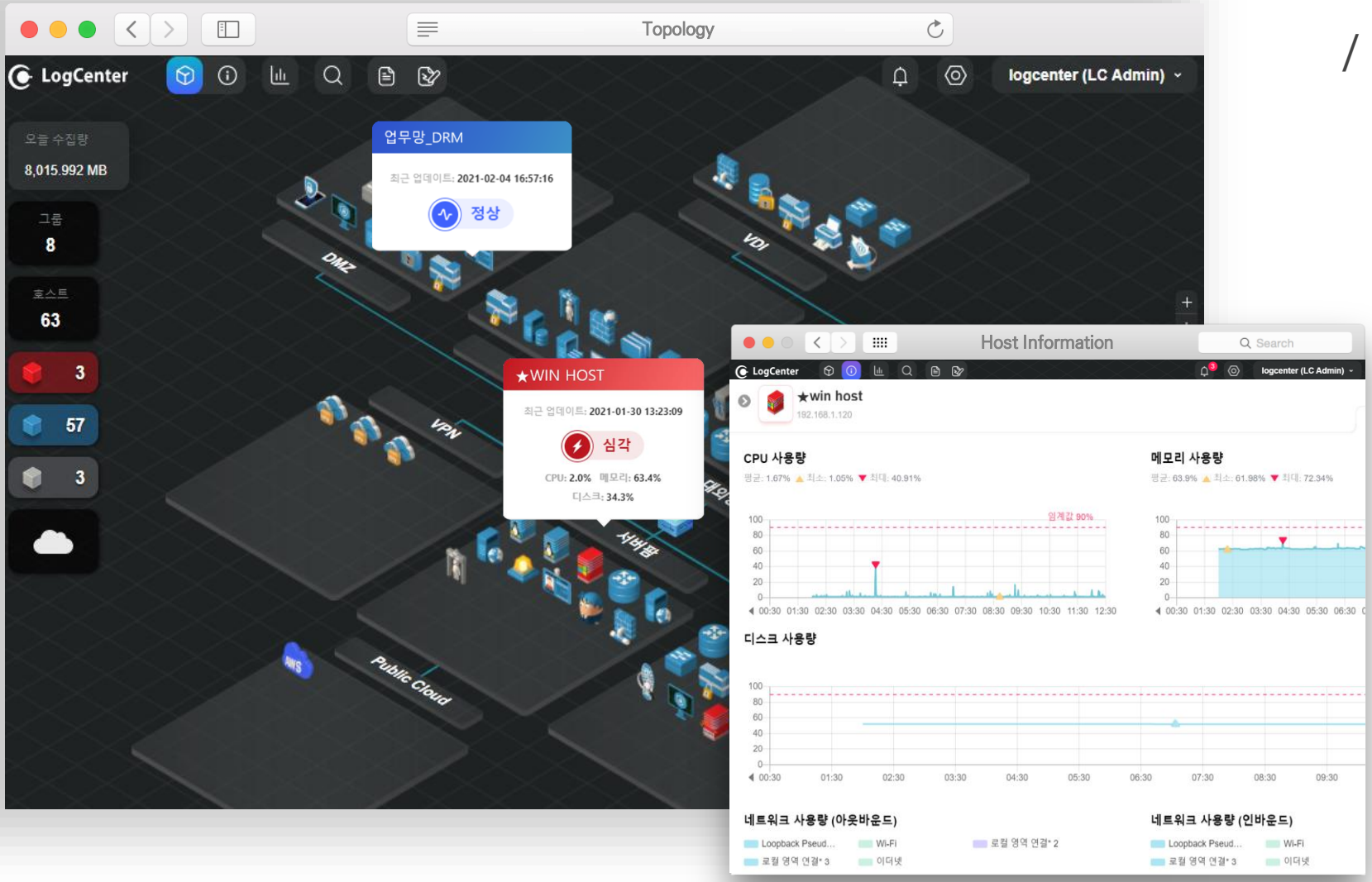
Data Integrity

AES-256 암호화, SHA-256 해시 값 추출, 무결성 체크, 보존주기 설정, 원본로그 데이터 다운로드



Management

사용자 권한 관리, 시스템 감사로그, BlackList & WhiteList 설정, SMTP 설정



/ 리소스를 모니터링 할 수 있습니다.

핵심능력

리소스(CPU/MEM/DISK) Trend 제공
빨간색/파란색/회색 컬러링으로 호스트 상태 자동 표시
호스트별 타임라인과 히스토리 관리

사용방법

1. LogCenter 에 연동한 호스트들을 한눈에 파악할 수 있도록 맵으로 표현합니다.
2. 리소스 상태가 정상인 호스트들 모두 파란색 정상 으로 운영되고 있습니다.
3. 서버팜 그룹의 호스트 하나가 빨간색 심각으로 변했습니다.
4. Host Info를 확인해보니, 현재 메모리 사용량이 임계치를 초과했네요.
5. LogCenter Bot이 전달해준 체크리스트를 참고하여 문제를 해결합니다.

innerbus

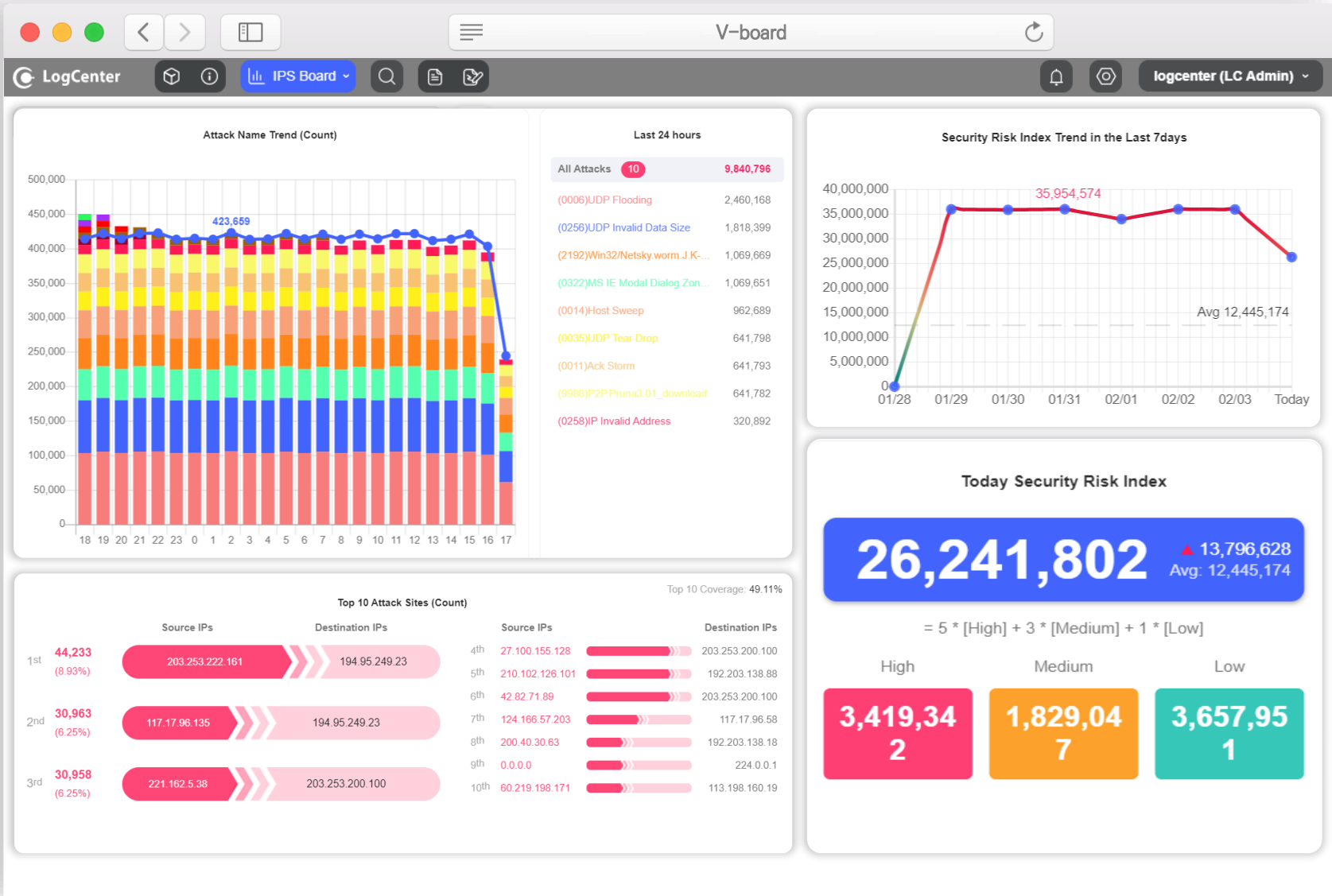
/ 위험도 높은 IP를 추적할 수 있습니다.

핵심능력

실시간 모니터링에 최적화된 **UX 대시보드**
Line, Bar 등 **다채로운 위젯**과 화이트 & 다크 **듀얼 모드**
항상 업데이트되는 위젯 컨텐츠 Drag & Drop
위젯 차트 클릭 시 상세 로그데이터 뷰

사용방법

1. LogCenter 에 새로 업데이트된 컨텐츠 중 '보안 관제' 위젯들을 다운로드합니다.
2. 다운로드 받은 위젯들을 우선순위나 유형에 따라 보기 편하게 구성하여 보안 관제용 대시보드를 만듭니다.
3. 실시간으로 분석된 위험도 높은 공격 리스트를 확인합니다.
4. 위험도 높은 공격을 유발한 IP 리스트도 같이 확인합니다.
5. 위젯 차트를 클릭하여 해당 IP들이 접속한 시스템 정보 등 상세 데이터를 조회하고, 사내 보안 조치 근거 자료로 사용합니다.



04 | LogCenter 를 이렇게 사용하세요

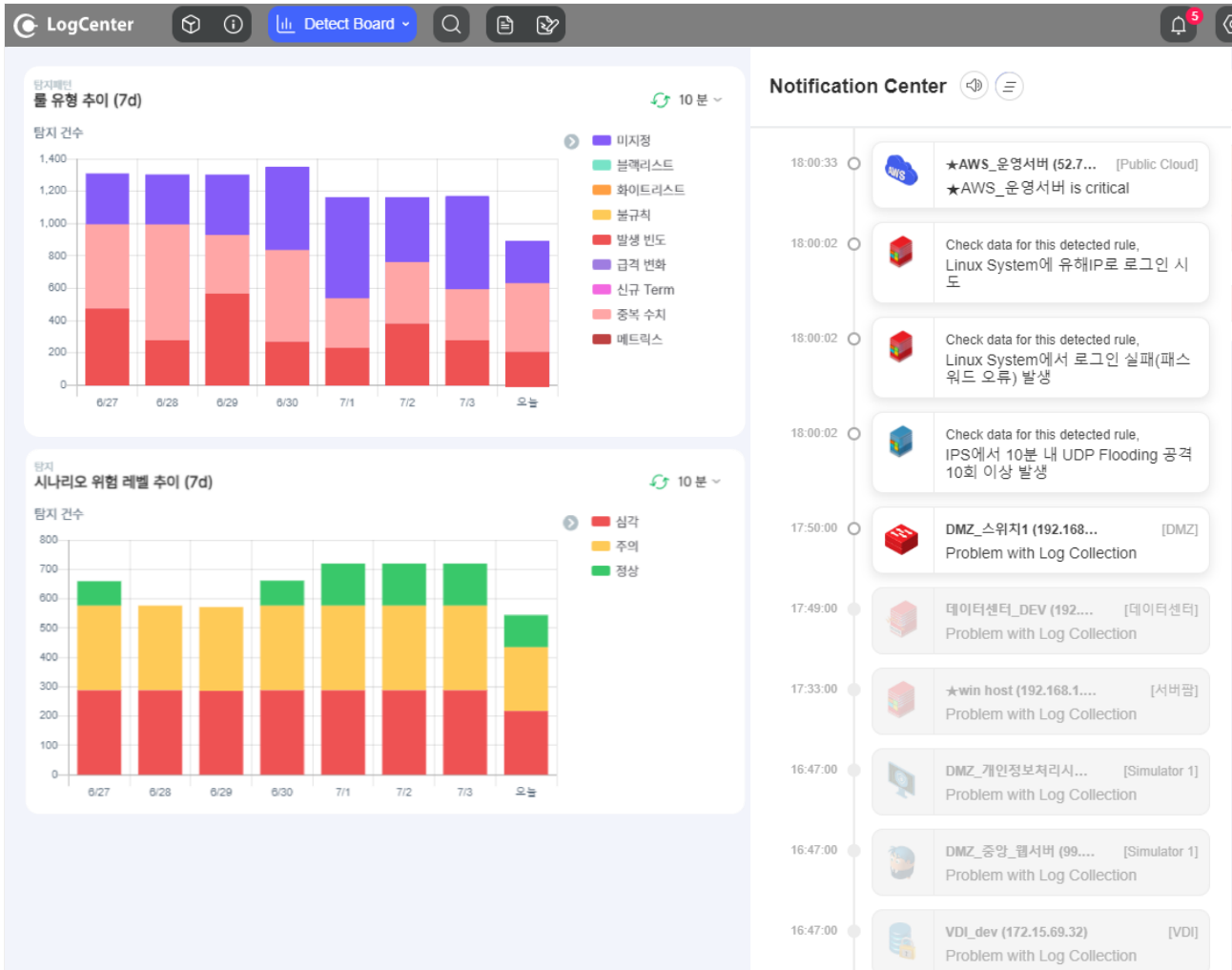
/ *시스템 이상 접근자를 탐지할 수 있습니다.*

핵심능력

9-type **실시간 탐지** 및 **시나리오와** Notification Push
담당자 메일, SMS 연동으로 실시간성 극대화
이너버스의 21년 노하우가 녹아 있는 **270+ 탐지패턴 컨텐츠**

사용방법

1. 실시간 대응이 필요한 이슈는 **탐지패턴과 시나리오를** 걸어둡니다.
2. 서버 로그인 실패 건수가 과다하게 발생하면 **즉시 Notification**을 푸쉬합니다.
3. 연동해둔 알람 메일을 확인하고, LogCenter 에 접속해서 탐지 내역을 확인합니다.
4. 로그인 실패가 계속 발생하고 있으며, 원인은 패스워드 오류로 확인되었습니다.
5. 상세 로그데이터를 조회하여 로그인 실패를 발생시킨 계정 정보를 확인하고 서버 담당자에게 전달합니다.



innerbus

Daily Report

192.168.1.121

메모리 보고서

시간대별 사용률 당일 메모리 사용률 추이와 각 상태별 랩타임을 확인할 수 있습니다.

(%) 평균: 54.35% 최소: 44.36% 최대: 73.88%

상태	정상	주의	심각
랩 타임	13시간	11시간	-

메모리 고사용 프로세스 Top 10 메모리 사용률이 높은 프로세스를 확인할 수 있습니다.

#	프로세스명	PID	최대 사용률	일평균
1	YourPhone.exe	10388	1.5% (-)	1.5%
2	TextInputHost.exe	10628	1.0% (-)	1.0%
3	dllhost.exe	10948	0.3% (-)	0.3%
4	fontdrvhost.exe	940	0.2% (-)	0.2%
5	SecurityHealthSystray.exe	11404	0.3% (-)	0.3%
합계			3.3%	3.3%

#	프로세스명	PID	최대 사용률	일평균
6	svchost.exe	1088	0.2% (-)	0.2%
7	svchost.exe	1280	0.2% (-)	0.2%
8	TUCTLSystem.exe	5616	0.2% (-)	0.2%
9	winlogon.exe	728	0.3% (-)	0.3%
10	WUDFHost.exe	956	0.3% (-)	0.3%
합계			1.2%	1.2%

프로세스 위험 분석 LogCenter의 분석 엔진으로 고위험 프로세스를 식별합니다.

데이터가 없습니다.

/ 보고서로 활용할 수 있습니다.

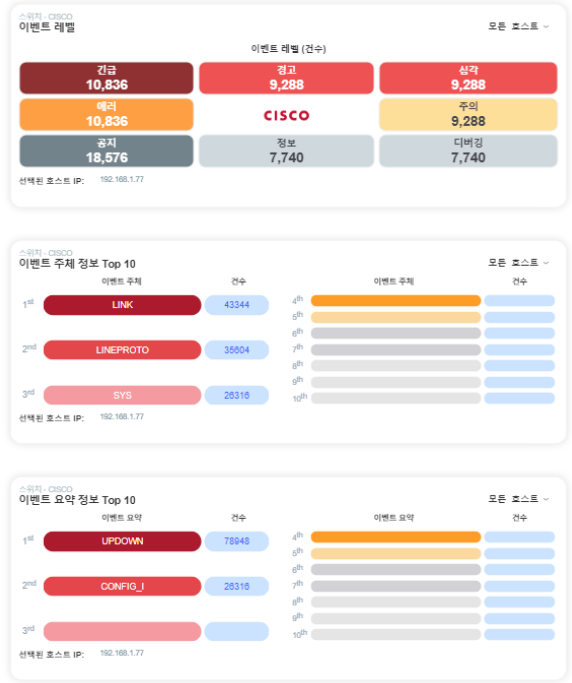
핵심능력

데일리 보고서 & 맞춤 보고서 자동 생성
리소스 현황, 이벤트 현황 등 다양한 컨텐츠
PDF다운로드, 예약 메일 전송해서 보고 자료로 활용

사용방법

1. LogCenter 에 연동한 호스트를 한눈에 볼 수 있는 Topology에서 자주 위험도가 심각(빨간색)으로 뜨는 서버들이 발견됩니다.
2. 대부분 모바일 서비스 구간의 서버들인데 위험 원인이 MEM 임계치 초과입니다.
3. 모바일 서비스를 오픈하고 난 후 접속량 폭증으로 부하가 오는 듯 합니다.
4. 심각 서버들의 리소스 데일리 보고서를 확인합니다.
5. 최근 일주일치 보고서를 PDF 다운로드하고, 보고 자료로 제출합니다.

Custom Report



innerbus

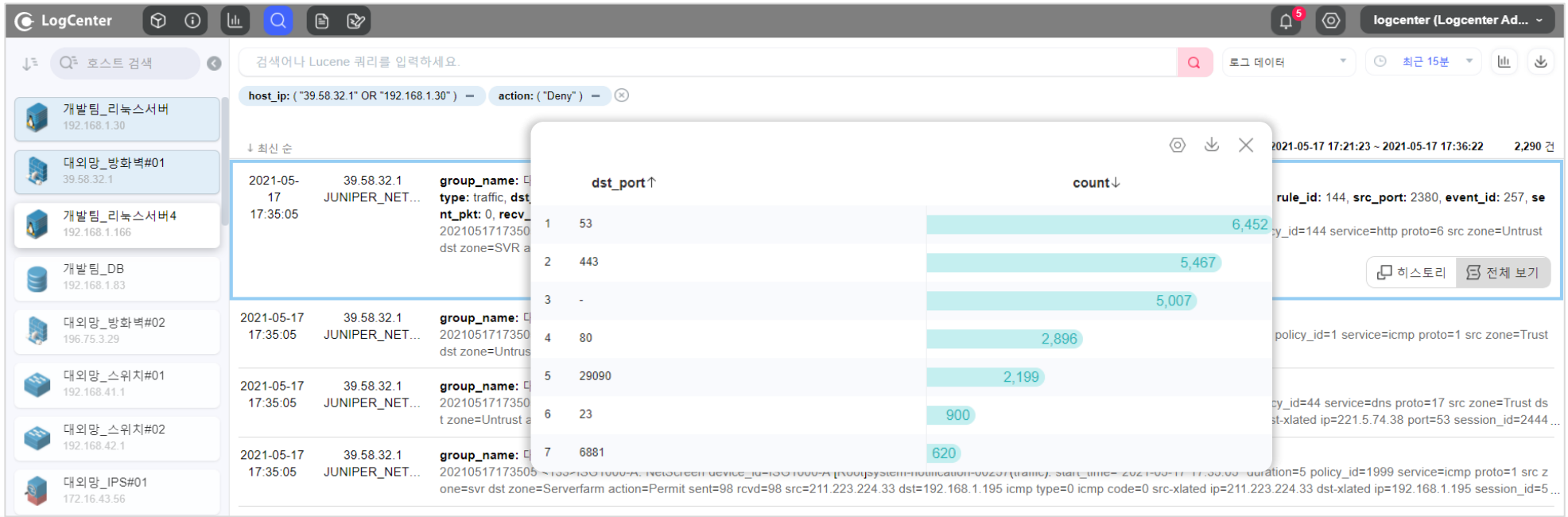
/ 빠르고 간편하게 **검색**할 수 있습니다.

핵심능력

검색어 Tag 기능으로 쉽고 간편한 검색
검색하고 싶은 컬럼값을 클릭하면 즉시 검색어 Tag 등록
컬럼별 Count 통계 추출 & 다운로드

사용방법

1. 방화벽 정책을 변경하기 위해 사내에서 사용하는 포트 정보가 필요합니다.
2. 방화벽 호스트들을 클릭하면 사내 모든 방화벽 로그가 한 번에 검색됩니다.
3. 목적지 포트(dst_port) 컬럼을 기준으로 통계를 추출합니다.
4. 불필요한 포트 정보를 확인하고 다운로드해서, 정책 변경을 위한 근거자료로 활용합니다.



05 | 최고의 고객이 LogCenter 를 좋아합니다

B공사, 이** 과장

B공사는 **컴플라이언스 준수**가 필요했습니다.

“ 정기 보안감사를 준비할 때 마다 **로그 백업과 분석**에 대한 고민이 많았는데요. 그 고민을 LogCenter 로 해결했습니다. ”
컴플라이언스에 맞춰 로그를 안전하게 통합 관리하면서, 주요 시스템 로그는 실시간으로 분석도 하고 있습니다.

G시청은 **접속로그 위변조 방지**가 필요했습니다.

“ 시스템 접속기록을 백업하고는 있지만 위변조 방지가 되지 않아서, 보안사고가 있을 때 근거로 활용할 수 있을 지 고민되는 부분이 있었습니다. LogCenter 를 도입해서 위변조 방지를 확실히 하고 저장하니 매우 안심됩니다. ”

G시청, 김** 주무관

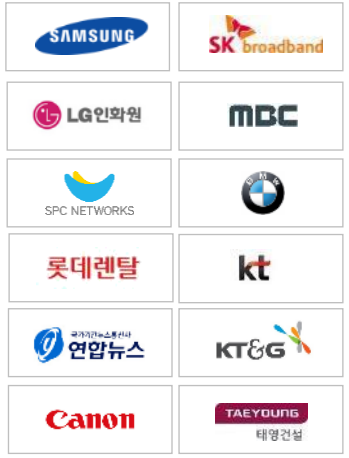
사업명	(B공사) 통합로그관리시스템 구축	(G시청) 통합로그관리시스템 구축
도입목적	컴플라이언스 준수	접속로그 위변조 방지
라이선스	1일 로그량 50G 연동대상시스템 100D	1일 로그량 10G 연동대상시스템 30D

05 | 최고의 고객이 LogCenter 를 좋아합니다

공공, 기업, 금융, 의료, 교육 등 다양한 영역에서 700+ 고객이 LogCenter를 선택했습니다.
국내 최다 수행경험과 성공 노하우를 가진 LogCenter로 최고의 로그관리를 경험하십시오.

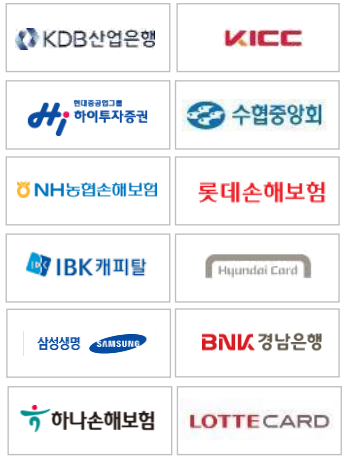
공공

기업



교육 & 의료

금융



공사 공단

최근순, ~'22.06

한국지역난방공사	서울시설공단	안동시시설관리공단	한국교통안전공단
한국승강기안전공단	한국공항공사	중소벤처기업진흥공단	여수광양항만공사
부산교통공사	인천국제공항공사	대한석탄공사	부산항만공사
공무원연금공단	제주도개발공사	한국공항공사 서울본부	KAC한국공항공사
한국환경공단	LX한국국토정보공사	한국예탁결제원	경기도시공사
부산항보안공사	성북구도시관리공단	신용보증기금	해양환경관리공단
인천도시공사	SH서울주택도시공사	인천항보안공사	대전도시철도공사
강남구도시관리공단	주택관리공단	한국수산자원관리공단	노량진수산시장
한국전기안전공사	부산교통공사	울산항만공사	한국시설안전공단

연구원 협회 재단

최근순, ~'22.06

창업진흥원	경상남도교육청 교육연구정보원	한국정보통신공사협회	경제인문사회연구회
한국사회적기업진흥원	한국보건산업진흥원	국립수산과학원	한국에너지기술평가원
의료기관평가인증원	한국원자력안전재단	소프트웨어공제조합	사회보장정보원
한국과학기술원 부설 고등과학원	한국전기공사협회	한국표준과학연구원	한국한의학연구원
국사편찬위원회	중소기업기술정보진흥원	대한의사협회 의료배상공제조합	한국항공우주연구원
국립부산과학관	한국건강증진개발원	농림식품기술기획평가원	대한체육회

별첨 | LogCenter 라인업

LogCenter는 고객의 니즈와 환경에 따라 다양한 모델을 제공합니다. 비즈니스 상황에 맞는 최적의 모델을 선택하세요.

* HW 사양은 제조사 사정으로 일부 변경 될 수 있습니다.

Model	LogCenter 1000	LogCenter 2000	LogCenter 3000	LogCenter 5000	LogCenter 10000
Max 1일 로그량	10GB	20GB	30GB	50GB	100GB
표준 연동대상시스템 수	10D	30D	50D	100D	200D
CPU	XEON 10C 2.1GHz *2	XEON 10C 2.1GHz *2	XEON 10C 2.1GHz *2	XEON 10C 2.1GHz *2	XEON 10C 2.1GHz *2
RAM	64GB	64GB	64GB	64GB	64GB
HDD 분석로그 6개월 원본로그 12개월 저장	18TB (Raid 1)	28TB (Raid 1)	36TB (Raid 1)	48TB (Raid 1)	60TB (Raid 1)

* 라이선스 정책은 1일 로그량 및 연동대상시스템 수량에 따릅니다.

** HDD의 경우 고객사의 로그 보존주기 정책에 따라 변경 가능하며, 외부 스토리지 등의 연계도 가능합니다.

THANK YOU


innerbus
THE BEST WAY FOR LOG DATA
Web page
Home www.innerbus.com
Blog blog.naver.com
/innerbus_co
Contact us
|전략사업부
E sales@innerbus.com
T 070.7500.7390