

# Search **A** 통합 모니터링 솔루션 제안서

변함없는 마음자세로 고객과 함께 하겠습니다.

(주)에이원네트웍스



# Contents

SearchA 통합 모니터링 솔루션 제안서

- I 회사 소개
- II 제안 배경
- III SearchA 소개
- IV 제품의 특징점
- V 기대 효과



# 회사소개 - 일반현황



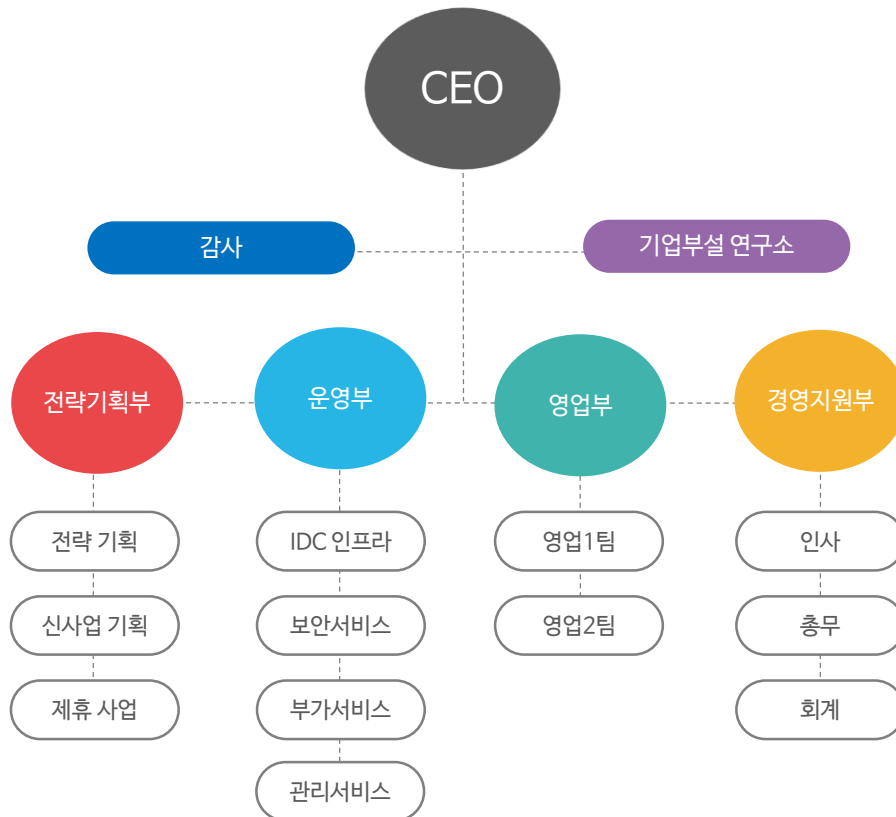
회사명	(주)에이원네트웍스 [ Aone Networks ]
대표자	민효홍
설립일	2004년 7월 2일
주요사업	VIDC 서비스 (코로케이션, 서버호스팅) / IT 아웃소싱 서비스 솔루션 구축 (하드웨어, 솔루션) / 정보보안
주요현황	기업부설연구소   정보보호안전진단필   메인비즈 인증 소프트웨어사업자   부가통신사업자 정보시스템유지관리서비스   정보시스템개발서비스   운영위탁서비스 특허 등록 (네트워크 가상화 시스템 및 방법) 특허 등록 (클라이언트/서버간 온라인 성능 테스트 방법 및 장치)

## 인증서



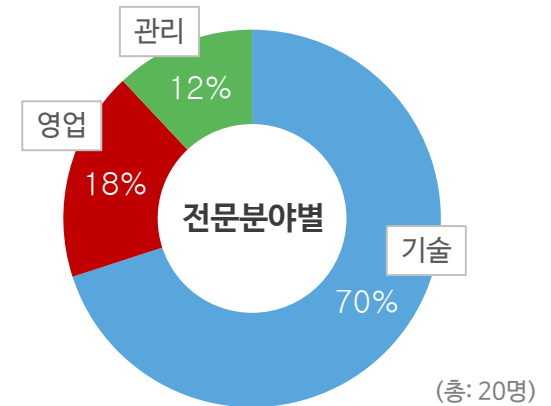
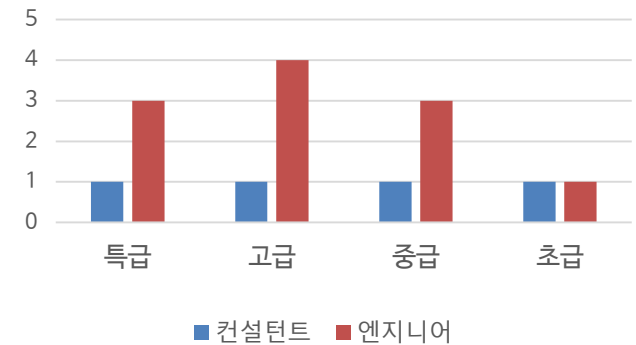
# 회사소개 - 일반현황

## 조직도



## 인력현황

### 기술인력현황



## 회사소개 - 연혁

### History

#### 2013~ 도약기

- 2016년 11월 환경정화시설 모니터링 시스템 '라온누리' 출시
- 2016년 11월 민간전자입찰시스템 'e-아파트 bid' 구축
- 2016년 06월 소프트웨어사업자 등록 (한국소프트웨어산업협회)
- 2016년 02월 아이씨비(주)/티케이온(주) 등 5개사 PG시스템 구축
- 2015년 09월 MAKEUS 인도네시아 서비스 구축 및 운영
- 2015년 06월 특허기술 등록 (네트워크 가상화 시스템 및 방법)
- 2015년 06월 특허기술 등록 (클라이언트/서버간 온라인 성능 테스트 방법)
- 2015년 02월 보건복지부 '콜센터 DB 이관 사업' 구축 및 운영
- 2015년 02월 직접생산확인증명서 추가 발급 (운영위탁서비스)
- 2015년 01월 통합모니터링시스템 'Search A' 출시
- 2014년 12월 에스원(주)와 정보보안 관련 업무협약 체결
- 2014년 12월 직접생산확인증명서 발급 (정보시스템 유지관리/개발서비스)
- 2014년 05월 이투데이(주) Site 및 기사송출시스템 개발 및 유지보수 계약 체결
- 2014년 05월 GS네오텍(주)와 CDN 서비스 업무협약 체결
- 2013년 07월 경영혁신형 중소기업 (MAIN-BIZ) 선정 (중소기업청)
- 2013년 05월 펜타시큐리티(주)와 업무협약 체결
- 2013년 05월 윈스텍넷(주)와 업무협약 체결
- 2013년 01월 미국 호스팅서비스 개시

#### 2008~2012 성장기

- 2012년 12월 클라우드 서비스 'Clouda.KR' 오픈
- 2011년 10월 목동 IDC 개통 멀티센터 기반 확보
- 2011년 10월 ETRI '서비스 융합플랫폼' 사업자문 지정
- 2010년 12월 Oracle 골드파트너 등록
- 2010년 06월 영우디지털 HP, CISCO 파트너 협약 체결
- 2009년 11월 기업부설연구소 등록 (한국산업기술진흥협회)
- 2008년 09월 벤처기업인증 획득 (기술보증기금)
- 2008년 04월 한국사회복지사협회 '온라인보수교육시스템구축' 선정

#### 2003~2007 태동기

- 2007년 06월 인텔넷(주)에서 에이원네트웍스(주)로 상호 변경
- 2007년 02월 본사 서울이전 (구로디지털단지)
- 2007년 02월 자본증자(자본금: 5천만원 ->) 3억원)
- 2006년 12월 부가통신사업자 등록 (서울전파관리소)
- 2006년 07월 중앙선거관리위원회 재보궐선거 시스템 구축 및 운영 대행(3년)
- 2004년 04월 버디버디 미니홈피 배경음 서비스 네트워크 구축
- 2003년 10월 주식회사 인텔넷 설립

## 회사소개 - 사업영역/핵심경쟁력

IDC 서비스 기반의 IT 전문인력과 축적된 업무 노하우를 바탕으로 고객의 비즈니스 환경과 요구사항에 부합한 최상의 서비스 컨설팅을 제공합니다. 고객이 비즈니스에만 전념하실 수 있도록 시스템 통합관리 코디네이터가 되겠습니다.

### ■ 사업영역

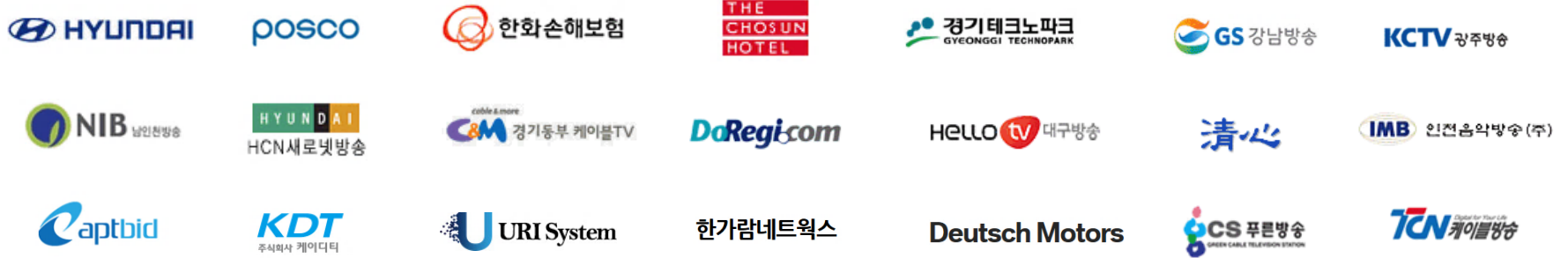
VDC 서비스	ITO 서비스	정보보안	솔루션 구축
서버호스팅, 코로케이션, 클라우드, 부가서비스	모니터링, IT운영/관리, 시스템컨설팅, SI/유지보수	보안 서비스, 보안 컨설팅	하드웨어 및 솔루션 구축

### ■ 핵심 경쟁력



# 회사소개 - 주요 고객사

## SearchA 주요 고객사



## VIDC 주요 고객사



## 제안배경: 네트워크 환경의 변화

다양한 비즈니스 패턴의 변화에 대해 너무도 많은 대응의 문제점이 발생하고 있습니다.  
금전적, 관리적, 기술적인 대응을 어떻게 하고 계십니까?



### 인터넷 기반의 네트워크의 확장

- 매년 50 ~ 100% 씩 네트워크 사용량 증가
- 점점 빨라지는 사용자 Device와 Application들은 높은 신뢰성과 안정성을 필요로 함
- 무선 시장의 급속한 변화

### 업무환경에서 지속적 변화 요구

- 높은 품질의 가용성 보장 요구
- 더 많은 대역에 대한 지원 요구
- 대용량 트래픽의 증가
- 다양한 비즈니스 패턴의 변화 요구

### 관리적 문제점 발생

- 장애 발생 시 대응 방법 부재
- 이기종 환경에서 관리 어려움
- 성능 관리의 현실적 어려움
- 투자의 고비용 구조

### 네트워크의 안정성 및 확장성 요구

- 네트워크 단절은 곧 업무의 단절
- 높은 안정성 및 트래픽의 확장 지속적 요구
- 기업의 생산성을 높이는 절대 가치로 발전
- 다양한 접점에서 성능 저하 발생



## 제안배경: 기존 관리 솔루션의 문제점

- 기업에서 운영하고 있는 모든 IT Infra는 생산성 및 업무의 효율화를 위해 존재하며, 그 모든 기반은 End User에게 제공되는 서비스를 위해 유지됩니다.
- 가용성을 위해 다양한 관리 방법이 존재하지만 단편적인 정보 관리의 한계를 보이며, 서비스 관점에서는 효율성이 매우 떨어지는 형태로 진행되고 있습니다.



## 제안배경: 새로운 대안의 필요성

- IT 자산 및 서비스에 대한 일원화된 통합 관리로 종합적인 자원 상황 감시 및 대처가 가능하며, 서비스 가용성 및 운영의 효율성이 증대되어 안정적 IT 서비스를 제공합니다.



## 제품소개: Search A

- 인프라의 장애와 서비스의 수준을 통합하여 관리하는 차세대 통합 모니터링 솔루션입니다.

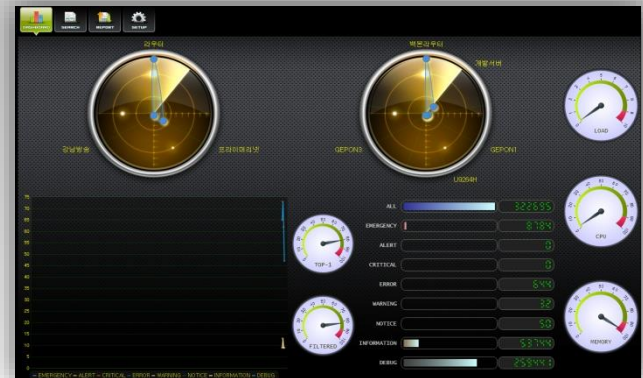


# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - 장애 관리
  - 성능 관리
  - 구성 관리
- 서비스 관제
  - 보안 관리
  - 트래픽 관리
  - 로그 관리
- 통계 관리

- 서비스 관제를 목적으로 하는 다양한 구성
- 장애/성능 분석을 위한 통합 도구로 활용
- 혁신적인 UI기술의 빠르고 안정적 엔진

- 관리시스템의 직관적인 모니터링 기능 구현
- 손쉬운 Customizing기능을 이용한 다양한 응용
- 다양한 Browser 지원

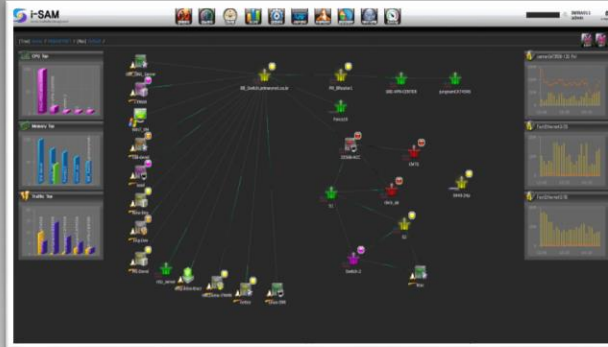


# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - 장애 관리
  - 성능 관리
  - 구성 관리
- 서비스 관제
  - 보안 관리
  - 트래픽 관리
  - 로그 관리
- 통계 관리

- Topology Map 적용
- 관리자별 권한 설정의 Easy Access 지원
- 장애/성능/트래픽 관리의 최적화 구성

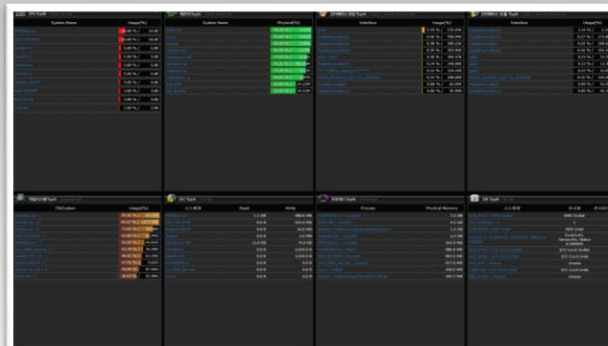
- 통계 데이터 분석을 위한 최적화된 Data 가공
- Database Accelerator를 이용한 빠른 통계 관리
- 서비스관점에서 운영평가 관리



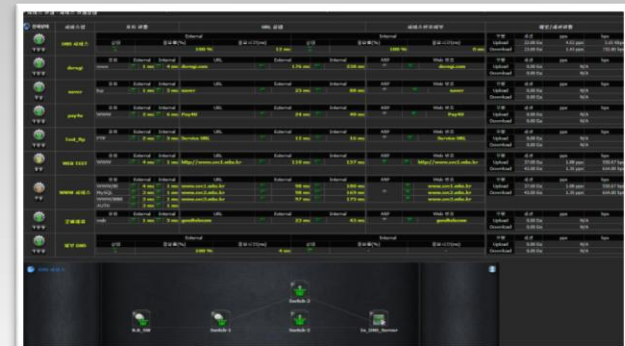
[장비맵 Topology]



[장애관리 종합상황판]



[성능관리 종합상황판]



[서비스관리 서비스현황]

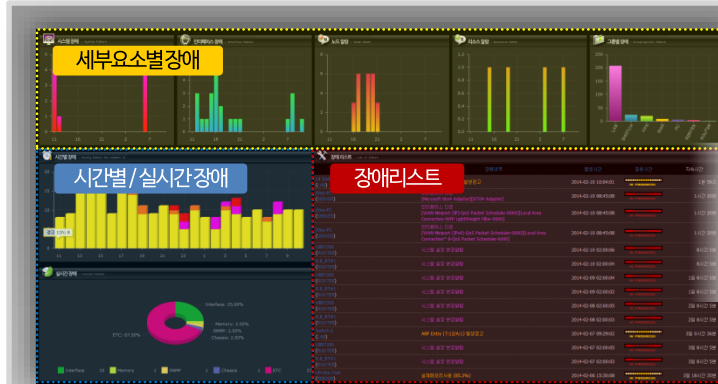


# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - 장애 관리
  - 성능 관리
  - 구성 관리
- 서비스 관제
  - 보안 관리
  - 트래픽 관리
  - 로그 관리
- 통계 관리

- 노드, 그룹별 맵을 이용한 관리
- 다양한 장애 탐지 루틴 적용

- 이벤트 제공으로 신속한 장애 대처
- 최적화된 웹기술로 빠른 속도 제공



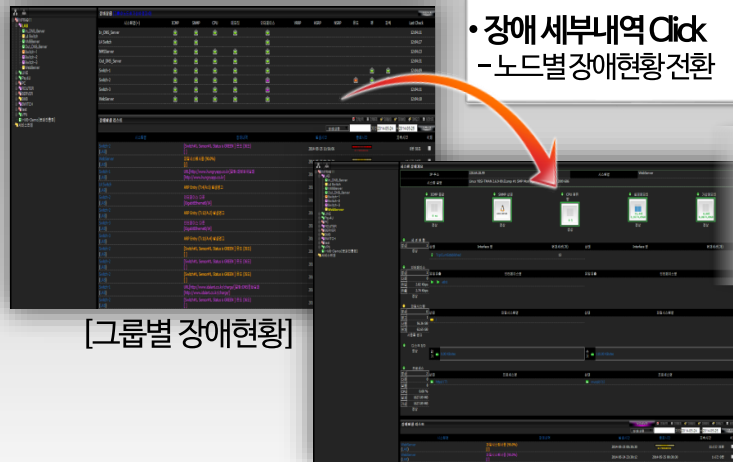
[종합상황판]

**세부요소별 장애**

- 시스템장애 / 인터페이스장애 / 그룹별장애
- 노드알람 / 리소스알람

**장애리스트**

- 시스템별장애내역
- 장애발생시간 / 종료시간 / 지속시간



[그룹별 장애현황]

[노드별 장애현황]

• 장애 세부내역 Click  
- 노드별 장애현황 전환

**그룹별 장애현황**

- 3단계 루틴 탐지로 (ICMP, SNMP, Rshell) 무결성 확보

**노드별 장애현황**

- ICMP 및 SNMP 상태
- CPU 및 메모리 현황
- 인터페이스, 파일시스템, 세션 및 프로세스의 현황

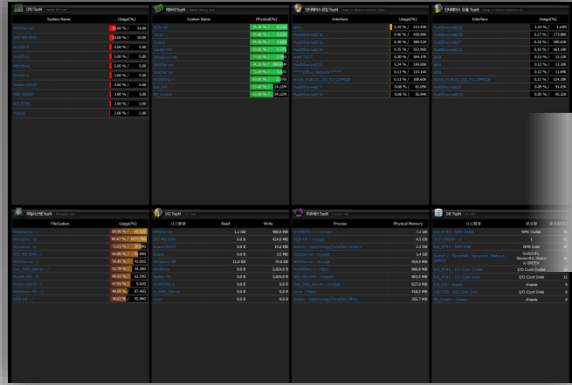
# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - 장애키 관리
  - 성능 관리
  - 구성 관리
- 서비스 관제
  - 보안 관리
  - 트래픽 관리
  - 로그 관리
- 통계 관리

- 장비별 자원성능정보
- Routing Protocol 성능관리

- 모듈 정보관리
- Interface 무결성 검증

- L4/VPN/보안장비/QoS 성능분석
- Traffic 성능분석 및 관리



[종합상황판]



[장비별 성능현황]

TopN

- CPU 및 Memory의 사용률 (% 및 M/Gbit)
- 인터페이스의 유입 / 유출 (% 및 K/Mbps)
- 파일시스템 사용률 (% 및 Gbyte)
- 디스크 I/O의 Read / Write 사용률 (K/M/Gbyte)
- 기타 센서의 DB 값 (온도, chassis, Power 등)

네트워크 인프라

- 시스템 개요
- CPU 및 Memory 사용률
- 온도 센서 현황
- FAN 및 Power 현황
- 인터페이스 및 모듈 현황

서버 인프라

- 시스템 개요
- CPU 및 (가상) Memory 사용률
- Session 현황
- 인터페이스 현황
- 파일시스템 및 디스크 I/O 현황
- 프로세스 현황

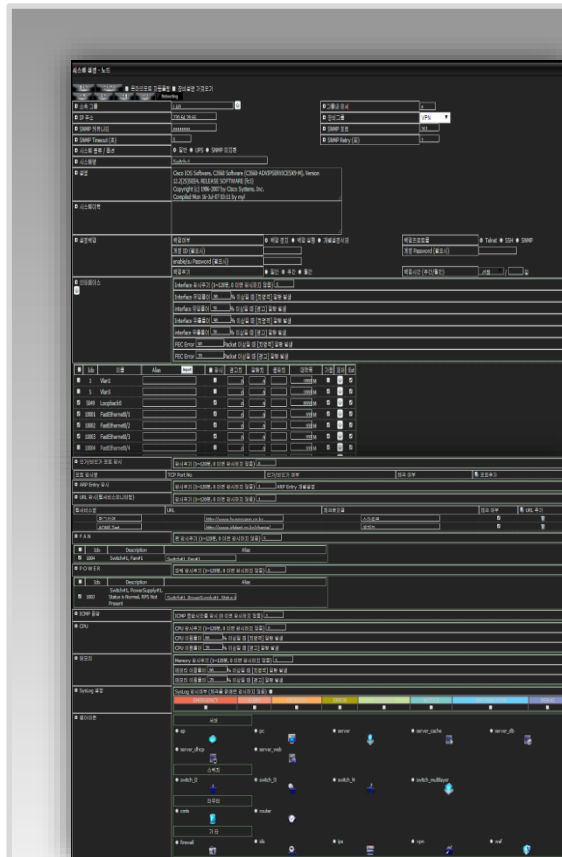
# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - 장애키 관리
  - 성능 관리
  - 구성 관리
- 서비스 관제
  - 보안 관리
  - 트래픽 관리
  - 로그 관리
- 통계 관리

- 노드/그룹 관리
- 이력관리

- 사용자관리
- 시스템관리

- 이벤트관리



[노드별 구성관리]

## 노드별 구성관리

- 소속그룹 및 장비그룹
- SNMP 및 장비유형 선정
- 백업 설정
- 인터페이스 임계치 설정
- 인가/비인가 포트 감시, ARP Entry 감시, URL 감시 설정
- FAN 및 Power 설정
- ICMP 응답, CPU 및 Memory 감시 설정
- SysLog 설정
- 웹 아이콘 설정

## 그룹별 구성관리

- 소속그룹 및 장비그룹
- SNMP 및 장비유형 선정
- 인가/비인가 포트 감시, URL 감시 설정
- 웹 아이콘 설정
- 그룹내 장비현황/노드 순서
- 그룹별 임계치 설정



# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - ▶ 장애 관리
  - ▶ 성능 관리
  - ▶ 구성 관리
- 서비스 관제
  - ▶ 보안 관리
  - ▶ 트래픽 관리
  - ▶ 로그 관리
- 통계 관리

• ARP 위변조 감시

• 웹페이지 변경 감시

• PORT상태 감시

• 서버 세션 감시

**ARP History**

● ● ● 그룹명 ● 시스템명      검색기간    2014-10-    2014-10-    검색

번호	그룹	시스템명	장바번호	MAC	내역	일자	이전MAC
1			222.122.52.212	101F743B7CA4	Delete	2014-10-17 19:39:06	101F743B7CA4
2	한시스먼터넷	Server_218.153.6.242	218.153.6.242	79E38518198C	Delete	2014-10-17 19:00:02	79E38518198C
3			222.122.52.222	101F743B7CA4	Delete	2014-10-17 15:46:06	101F743B7CA4
4			222.122.47.106	001878075154	Delete	2014-10-16 23:33:06	001878075154
5	한국사회복지발전연구원	Server_222.122.47.10	222.122.47.10	001878075154	Add	2014-10-16 22:18:05	
6	송암원격영상교육원	Server_218.153.6.211	218.153.6.211	9848E17F2068	Delete	2014-10-16 20:47:02	9848E17F2068
7			222.122.52.132	001E076465AC	Delete	2014-10-16 20:34:04	001E076465AC
8			222.122.52.152	001E0749F760	Delete	2014-10-16 20:23:05	001E0749F760
9			222.122.52.150	000C2984E88E	Delete	2014-10-16 18:09:04	000C2984E88E
10			222.122.52.153	000C2930520F	Delete	2014-10-16 16:54:06	000C2930520F

[ARP 위변조내역 분석/조회서비스]



[URL 웹페이지, PORT, 세션감시 서비스]

## ARP 위변조에 대한 감시

- ARP 위변조 트래킹 감시
- ARP 위변조로 인한 서비스 중단 방지
- ARP 변조의 이력 추적 기능
- 서비스 가용성 증대

## URL 웹페이지에 대한 감시

- URL 웹페이지 관제
- 웹페이지 변조 여부 감시
- 해킹 공격에 대한 피해 방지
- 서비스 안정성 증대

관제대상

ARP  
변조

URL  
감시

PORT  
감시

세션  
감시

- 서비스별 활성 포트 감시
- 서버별 비활성 포트 감시
- 서비스 상태 감시
- 해킹 위협에 대한 피해 방지
- 서비스 안정성 증대

- 서버별 세션 상태 감시
- 서비스의 적정성 감시
- 세션 과다에 따른 접속 지연 체크
- 서비스 안정성 증대

## PORT 상태에 대한 감시

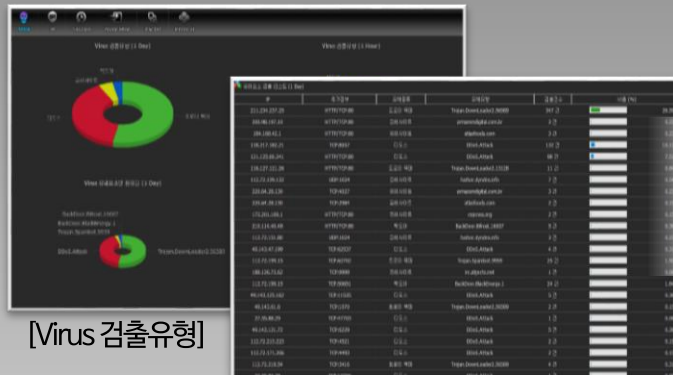
## 세션 상태에 대한 감시

# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - 장애 관리
  - 성능 관리
  - 구성 관리
- 서비스 관제
  - 보안 관리
  - 트래픽 관리
  - 로그 관리
- 통계 관리

- 월 1회 DDoS 및 Virus에 관한 업데이트
- Flow 기반의 트래픽 관리

- DDoS / Virus / Worm 등의 탐지
- 트래픽 관련 통계 보고서




[Virus 검출유형]

[Virus 검출리스트]

### 유해트래픽 관리

- Virus 유해요소별 점유율
- Virus 유해요소 검출리스트
- 유해사이트, 트로이목마, 디도스, 백도어, 애드웨어 등 검출




[Application별 분석]

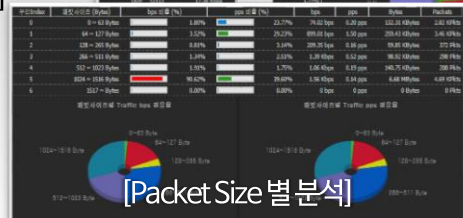
### Flow기반 트래픽 관리

- Netflow 수집을 통해 IP, Session, Application, Packet 및 Protocol 기반 분석
- Packet Analyzing 기능
- ARP Spoofing 탐지
- Traffic Storming 탐지
- 비정상 세션의 탐지
- 트래픽 관련 통계보고서 제공



[IP별 분석]



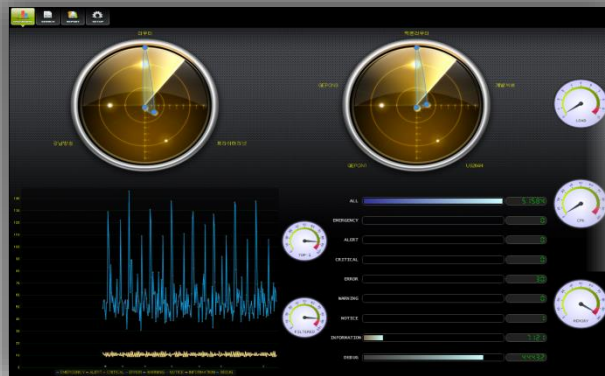
[Packet Size 별 분석]

# 제품소개: 주요기능

- 대시보드
- 인프라 관제
  - ▶ 장애 관리
  - ▶ 성능 관리
  - ▶ 구성 관리
- 서비스 관제
  - ▶ 보안 관리
  - ▶ 트래픽 관리
  - ▶ 로그 관리
- 통계 관리

- 직관적 UI의 종합상황판
- 심층분석의 Filtering 및 Searching

- 로그의 빠른 수집 및 분석
- 개인정보의 기술적, 관리적 보호 조치 기준



[SysLog 종합상황판]

## SysLog 종합상황판

- 노드 / 그룹별 로그수집 점유율 현황
- 각 로그레벨 별 수치
- 로그시스템의 CPU 및 Memory 현황



[SysLog Search]

## 심층분석을 위한 Searching 및 Filtering

- 조회기간 설정
- Priority, IP 주소, 메시지의 AND / OR / NOT 연산 제공
- 화면 갱신주기 설정

# 제품소개: 주요기능

- 유연한보고서포맷형식
- 이력관리

- 사용자관리
- 시스템관리

- 이벤트관리

- 대시보드
- 인프라 관제
  - 장애 관리
  - 성능 관리
  - 구성 관리
- 서비스 관제
  - 보안 관리
  - 트래픽 관리
  - 로그 관리
- 통계 관리



[인프라관제 보고서 옵션]

## 인프라관제 보고서 옵션

- 일간/주간/월간보고서를 생성하여 웹화면 그대로 출력하도록 설계
- 고객별로 웹 접속을 통한 자체 보고서 제공하여 개별적으로 보고서 활용 가능
- 장비별 인터페이스, 파일시스템 및 프로세스 보고서 작성
- CPU, 메모리, 파일시스템, 디스크 I/O, 세션, 프로세스 및 인터페이스별 사용현황 보고서
- 장애유형, 시스템가동률 보고서



[서비스관제 보고서 옵션]

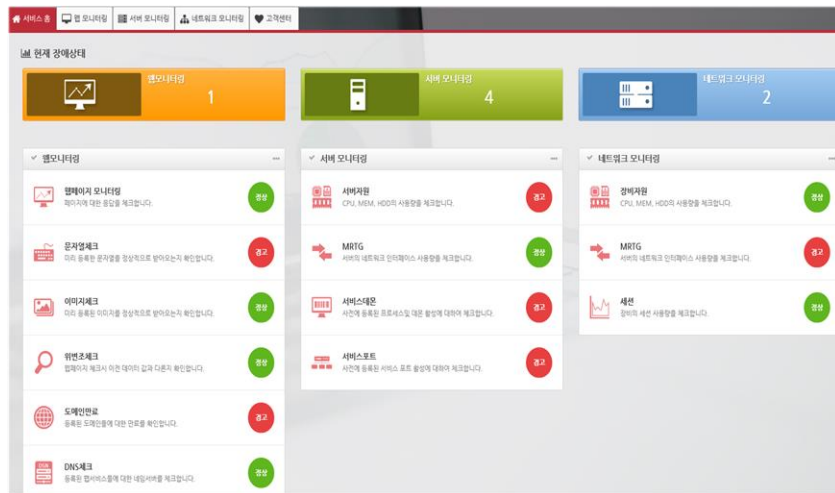
## 서비스관제 보고서 옵션

- 비물리적 장애 관련 보고서
- 서비스 Port, URL 장애 관련 보고서
- 고객별 트래픽 사용량 보고서
- 장애발생리스트 보고서

# SearchA 상품구성

## SearchA Cloud

- 특징: 별도의 설치프로그램 없이 간편한 웹사이트 회원가입을 통해 웹/서버/네트워크 모니터링 사용 가능
- 서비스 대상: 20대 이하의 소규모 시스템을 위한 ASP형 서비스로, 사용자가 쉽게 설정하여 사용 가능



[SearchA Cloud 대시보드]

## SearchA Enterprise

- 특징: 산재된 모든 네트워크 및 서버자원에 대한 구성/성능/장애 관리뿐만 아니라 서비스 품질 관리를 통합하여 관리하는 구축형 통합 모니터링 시스템
- 서비스 대상: 독립된 전산시스템 관리용으로, 대규모 유저를 관리하는 시스템 유지보수 사업자, 솔루션 ASP 사업자, 호스팅 사업자 등 내부망 관리에 특화



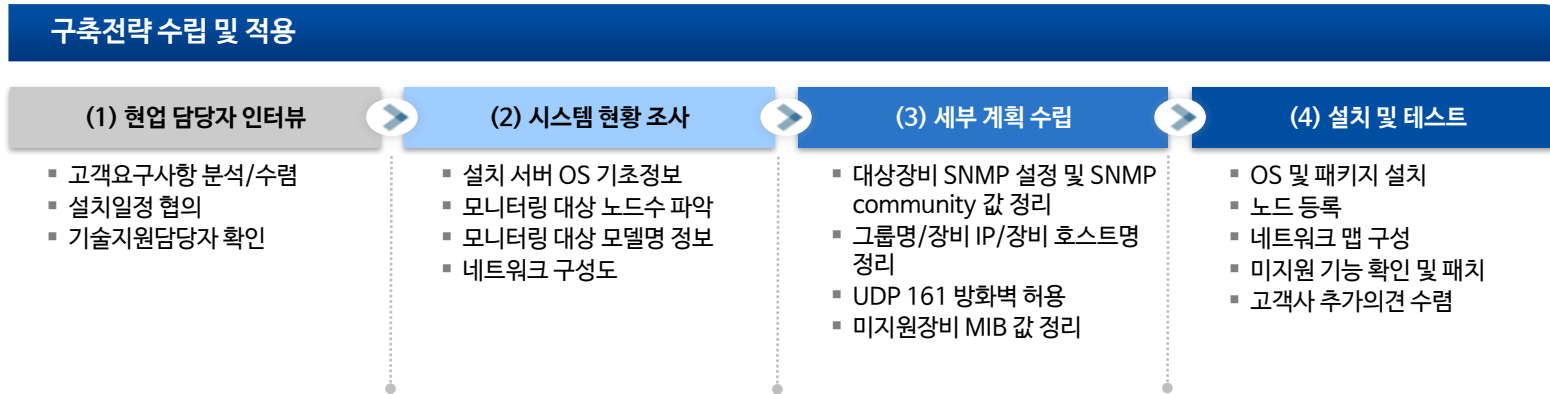
[SearchA Enterprise 대시보드]

# SearchA 주요기능

제품명	분류		주요 특징	기본형	고급형	
SearchA Cloud	웹 모니터링		• 웹페이지 모니터링/문자열 체크/이미지 체크/위변조 체크/도메인 만료/DNS 체크	○		
	서버 모니터링		• 서버자원/MRTG/서비스 데몬/서비스 포트 체크	○		
	네트워크 모니터링		• 네트워크 장비자원/MRTG/세션 체크	○		
SearchA Enterprise	기본형	종합 상황판	• 종합 현황, 알람 설정 • 개별 장애페이지, 장애발생 리스트	○	○	
		성능 관리	서버 인프라	• 시스템 개요 • CPU/HDD/Memory 사용률 • 인터페이스 유출입 현황	○	○
			네트워크 인프라	• 파일시스템 및 디스크 I/O 사용률 • 기타 센서의 DB값(온도/Fan/Power)	○	○
		장애 관리	• 시스템/인터페이스/그룹별 장애 이력 조회 • 노드별/그룹별 장애 현황: 통계 리포팅	○	○	
		설정 관리	• 노드관리/그룹관리/사용자관리 • 노드이력관리/시스템관리	○	○	
		보고서	• 자원 사용현황/프로세스별 사용현황 • 장애유형 보고서 • 일/주/월/년간 보고서	○	○	
		기술지원	• 고객사 담당자에게 Email로 장애통보	○	○	
			• 고객사 담당자에게 SMS로 장애통보 (추가 협의사항) • 전화상담: 24시간/365일 (추가 협의사항)	○	○	
	고급형 (optional)	보안 관리	• ARP 위변조 감시 • 웹페이지 변경 감시 • PORT 상태 감시 • 서버 세션 감시	X	○	
		트래픽 관리	• 유해트래픽 관리: DDoS/Virus/Worm 탐지 • Flow 기반 트래픽 관리	X	○	
로그 관리		• 노드/그룹별 로그수집 점유율 현황 • 각 로그 레벨별 수치 • 로그시스템의 CPU 및 Memory 현황 • 심층분석을 위한 Searching 및 Filtering	X	○		

# SearchA Enterprise 구축 방안

- 고객별 IT 자산 및 서비스 현황을 분석하여 최적의 모니터링 솔루션 구축전략을 수립 및 적용합니다.



참고 사항		
NMS 서버	상세내용	비고
H/W 권장사양	<ul style="list-style-type: none"> <li>CPU Intel 6C Xeon E5-2630 2.6Hz</li> <li>Memory 8G / DISK 300G (Raid 1구성)</li> </ul>	100노드 기준, 1년간의 데이터 보관 가능한 수준
OS 구성	<ul style="list-style-type: none"> <li>Cent OS 6.8 (64Bit) / Maria DB</li> </ul>	
파티션 정책	<ul style="list-style-type: none"> <li>/boot : 부트 파티션 정책</li> <li>Swap 메모리 : 물리적 메모리의 2배 설정</li> <li>/ : 나머지 전체를 /로 적용</li> </ul>	
지원가능 대상장비 OS	<ul style="list-style-type: none"> <li>Windows NT 및 Linux 계열의 경우, 대부분 지원 가능</li> <li>Unix 계열의 경우, 일부 지원 불가</li> </ul>	
설치 패키지	<ul style="list-style-type: none"> <li>Base System : 모두 선택</li> <li>Servers : FTP만 선택</li> <li>Web Services/Virtualization/Desktops/Applications : 선택하지 않음</li> <li>System Management : SNMP, system management 선택</li> <li>Development : 모두 선택 / Languages : Korean support 선택</li> </ul>	



## 기대효과

# 정확한 장애 예방과 성능 분석을 통한 서비스 중심의 관제 시스템 구축



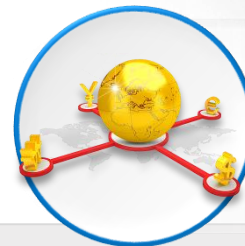
서비스 중심의 관제 시스템을  
이용한 통합 운영 관리 지원



실시간 장애 탐지를 이용한  
Down-Time 최소화



네트워크 전반의 성능 분석을  
통한 효율적인 투자 극대화

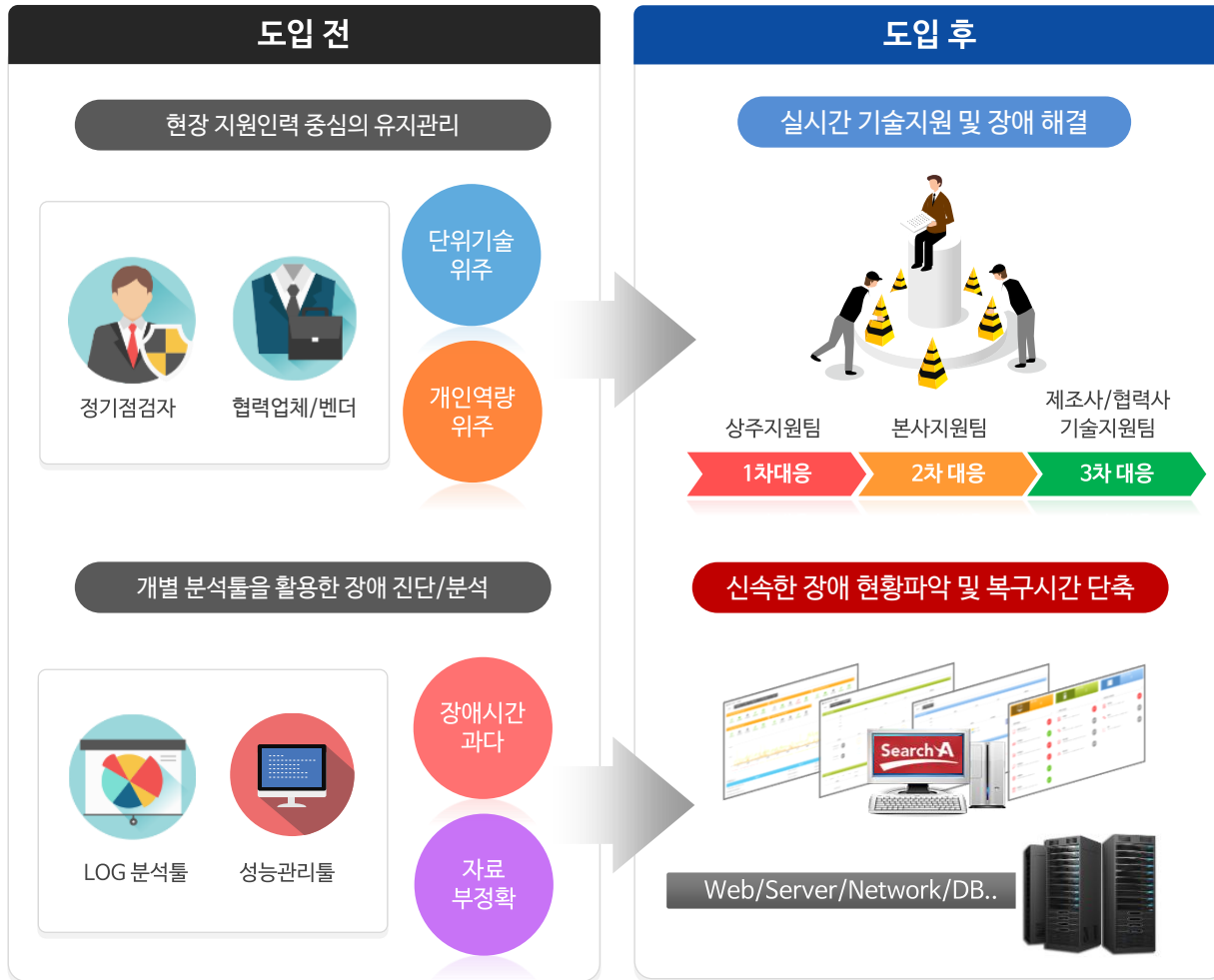


최적의 네트워크를 한눈에 보여  
주는 통합형 대시보드 제공



# 사례연구

## e아파트비드: SearchA 통합모니터링솔루션 도입 사례



**- 주요 개선사항**

- 1) 원스탑 컨설팅을 통해 최적화 된 시스템 및 솔루션 구축
- 2) 24시간 365일 운영되는 통합관제 지원센터를 통해 복잡장애에 대한 실시간 기술지원 및 장애 해결
- 3) 통합 모니터링 솔루션을 통한 신속한 장애 현황파악 및 복구시간 단축

현수준      목표수준

**20% 감소**

- 선제적 예방활동 강화
- 신속한 장애 해결

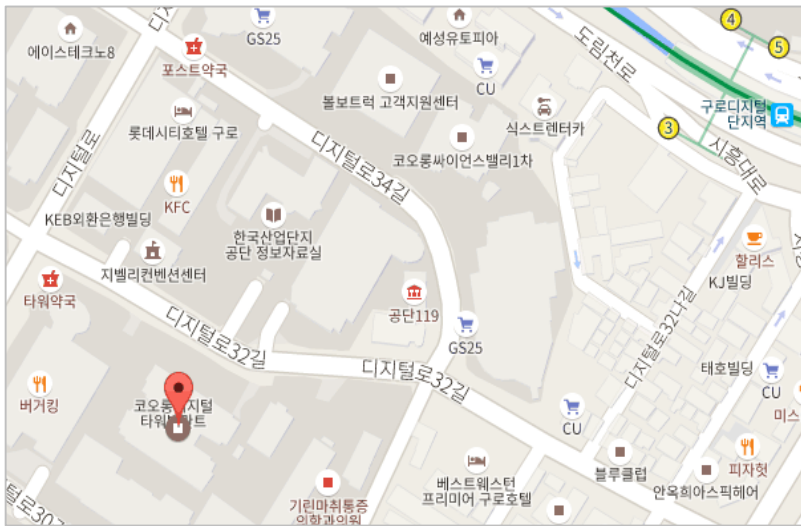
**15% 감소**

- 업무 중단 감소
- 복구시간 단축

# 연락처

서울사무실

분당사무실



서울특별시 구로구 디지털로 32길 30 코오롱디지털타워빌라트 1차 1003호

TEL : 02-853-8700

FAX : 02-853-8400



경기도 성남시 분당구 야탑동 343-2 KTICC 분당센터 B-1

TEL : 1544 - 6191

FAX : 031-706-6191



Thank You!

변함없는 마음자세로 고객과 함께 하겠습니다.