

Orangelabs

Convenience Up!

기업 전산관리의 편의성을 향상시켜주는

The Client

왜 Why The Client ? The Client인가?

기업들의 전산장애로 인한 경제적 손실과 관리 부담감 증대

韓 금융권 IT투자금, 美의 1/6...올해 전산장애 27%↑

ㅣ [금융IT 안전성 점검③] "단순 점검으로는 금융 전산 사고 해결책 안 돼"

인터넷 | 입력 : 2023/11/01 11:06 수정: 2023/11/01 20:32



백봉삼 기자 | ✉ 기자 페이지 구독 | 📄 기자의 다른기사 보기



[이벤트] 한국지멘스 디지털 인더스트리 초성 퀴즈 응모 시 스타벅스 아메리카노 기프티콘 증정!

중소형 증권사, 전산장애 '취약'...운용비 증액 시급

조영지 기자 | © 알약 2023.08.03 17:02 | 댓글 0



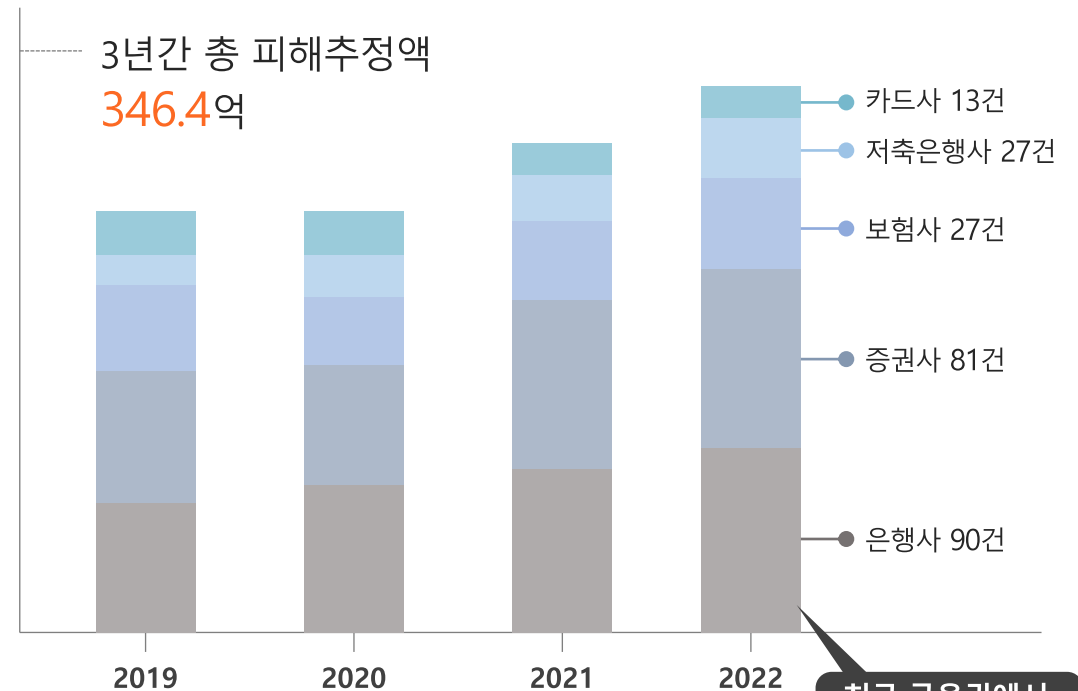
전산실, 사진=제타데이터뱅크

증권업계 '고질병'인 전산장애 민원이 올해도 끊이지 않고 있다. 공모주 청약 과정에서 집중적으로 발생하는 가운데 대형 증권사보다는 자기자본 3조원 미만인 중소형 증권사가 전산장애에 취약한 것으로 드러났다.

증권사들은 전산운용비 확보를 통해 시스템 보안에 집중할 계획이다.

금융권 전산장애 발생 추이

3년간 총 피해추정액
346.4억

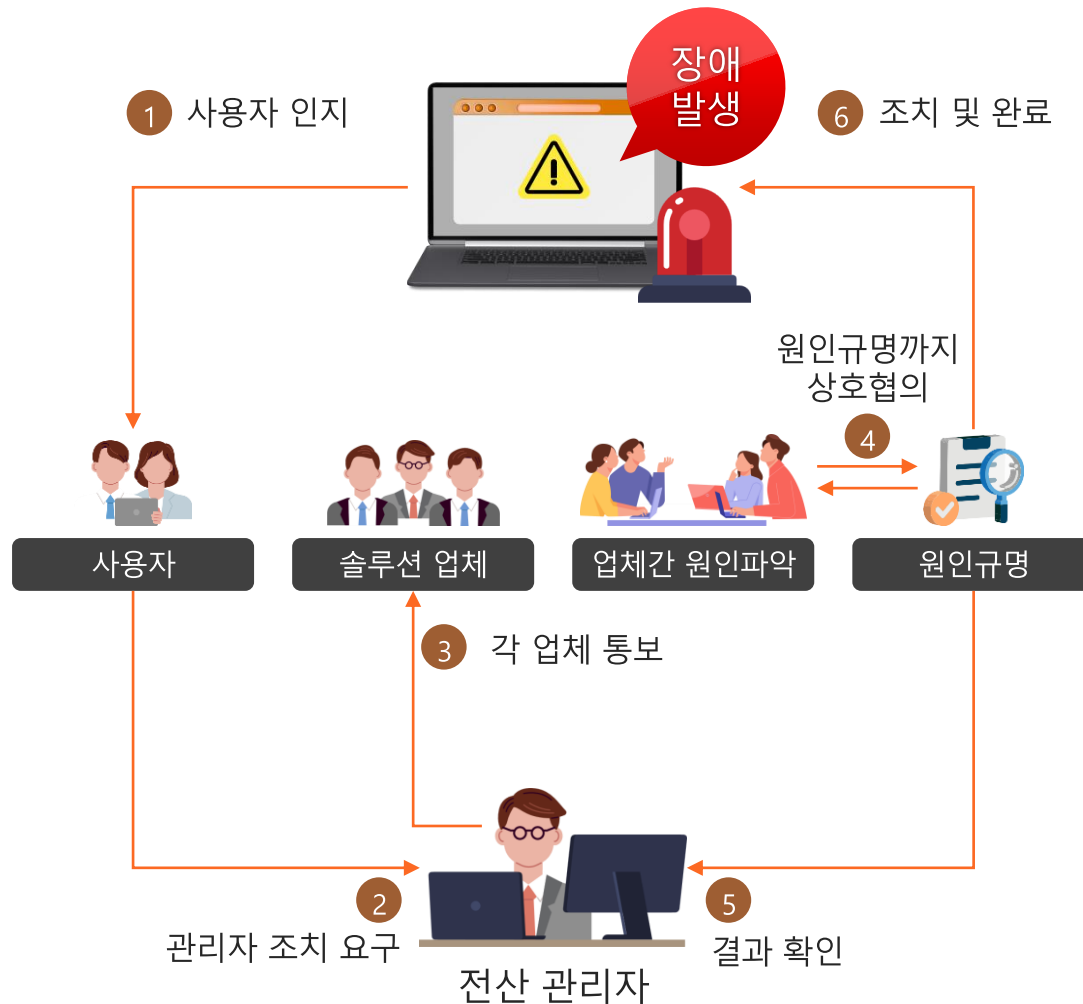


출처: 금융감독원 『국내 금융업권 전산장애 현황(2022)』

최근 금융권에서
전산사고 지속 증가

전산 문제의 원인 파악을 위한 복잡한 과정 및 장시간 소요

01. PC장애 인지의 어려움



✓ 기업의 IT 관리자는 개인 PC 사용자의 요청으로 처음 장애 인지

✓ 관리자가 정확한 원인 파악이 어렵기 때문에 1차 보안 솔루션 업체 분석 의뢰

✓ 미해결 시, 현재 사용 중인 솔루션 업체 모두 확인(2차 조치)

✓ 신규 솔루션 도입, OS 업데이트, 기존 솔루션 업데이트 시 비교 판단 데이터 부재로 업체가 상호협의를 통해 원인 규명

장애 처리 지연

수작업 방식의 성능 장애 분석 프로세스로 전산관리 효율성 저하



02. 수작업 방식의 원인파악

- ✓ 생산성 향상과 동시에 보안도 중요한 이슈로 부각되어 환경에 맞는 프로그램 추가 설치 및 수시 업데이트
- ✓ 설치된 프로그램의 증가로 PC 성능 저하 및 프로그램간 충돌로 장애 발생 빈도 상승
- ✓ 원인 해결을 위한 프로세스는 수작업으로 진행

03. 인력 및 시간 소요

- ✓ PC 성능 분석 및 해결을 위해 내부 관리자부터 담당 프로그램 외부 개발업체까지 접근하여 해결
- ✓ 새로운 프로그램의 설치 전/후 비교 데이터가 전무하여 정확한 비교 판단 불가
- ✓ 똑같은 문제가 발생하여도 기존 프로세스 반복
- ✓ 이로 인해 시간과 인력이 많이 투입되고 비용 발생

원인 파악을 위한 각 종 테스트 및 업체간 충돌로 장시간 소요

Convenience Up!

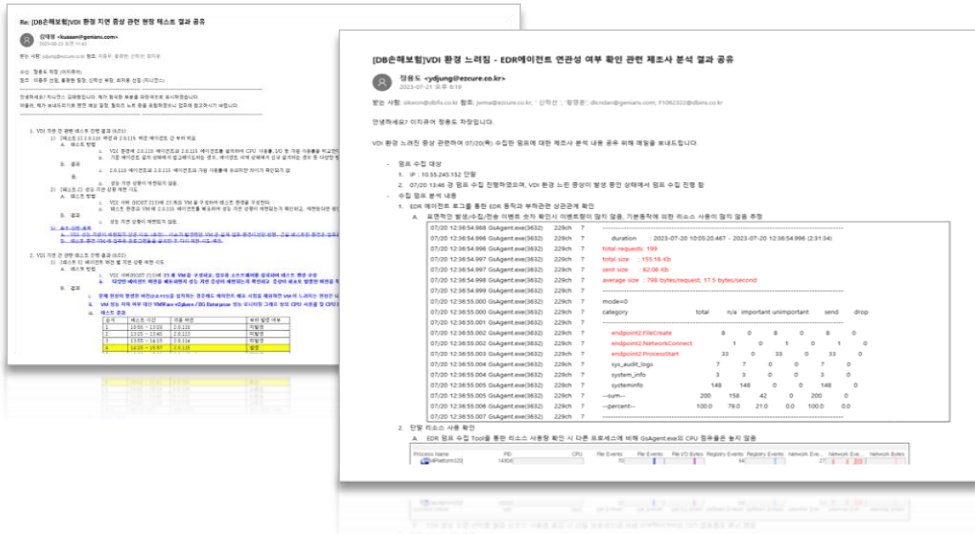
기업 전산관리의
편의성을 향상시켜주는

The Client

개발 배경 기업의 전산관리 Needs

기업 전산 관리자의 성능 장애 분석에 대한 필요성 급증

00 손해보험 보안 SW 기업 '이지**'의 해결 요청 메일



00시 보안관제팀 PM

"00시에서는 부수적으로 중단 단말의 운영 가용성 증진에 도움을 받기를 희망합니다.
행정업무 PC의 경우 다수의 공공기관 전용 프로그램을 사용하고 있으며 때때로 상호간 또는 윈도우 패치의 영향으로 서비스 장애를 겪는 사례가 많습니다. EDR에서 수집된 정보로 원인의 인과관계 파악에 도움을 받을 수 있다면 매우 효과가 클 것으로 기대합니다.
하지만 현재 수집정보(Process, File, Module, Network, Registry)로는 부족함이 있다고 생각되며 이에 대한 개선이 진행된다면 현장의 운영팀에서는 서비스 가용성 강화 측면에서도 상당한 도움이 될 것으로 기대됩니다"

00 손해보험 보안 SW 기업 '이지**'의 해결 요청 메일

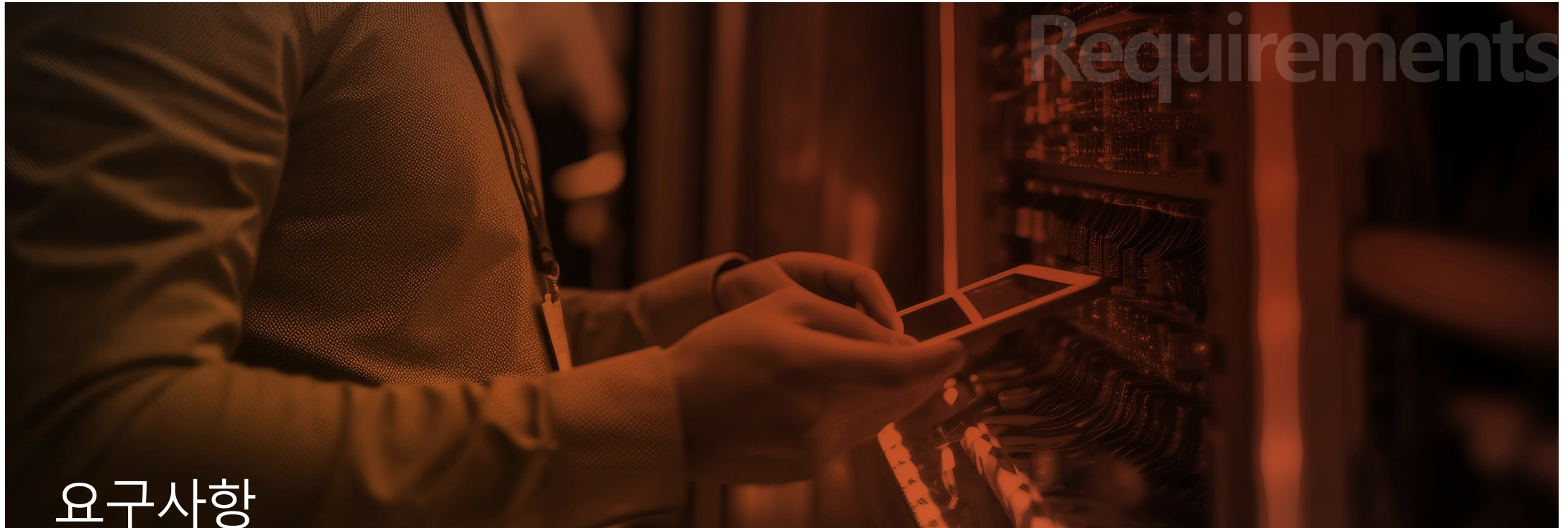


대다수 고객사
IT 담당자
VOC 결과

PC 성능 저하, 장애 발생으로 인해 원인 분석에 대한 문의는 많지만 해결방안은 전무함

전산 문제를 실시간으로 탐지하고 원인을 자동으로 분석하는 솔루션 필요

다수의 PC관리 및 보안을 위한 효율적인 단말 관리솔루션 필요



요구사항

PC 성능저하 관리

- ✔ PC관리, 보안을 위해 PC에 설치된 여러 소프트웨어로 인한 PC 성능저하
- 사용자 민원 증가에 따른 정확한 원인 분석 필요

PC 장애발생 관리

- ✔ 새로 도입한 솔루션, 기존 솔루션의 업데이트, OS업데이트 설치 후 사용자 PC가 느려지거나 상호간 충돌 등으로 인한 장애 발생으로 설치 전과 후의 명확한 검토 자료 요구

실시간 중앙관리

- ✔ 전사 PC의 성능, 사용율, 장애증상 등의 실시간 확인을 통한 관제 기능 필요



국내 최초 전산 문제를 실시간으로 탐지하고
원인을 자동으로 분석 하는

The Client 개발

Convenience Up!

기업 전산관리의
편의성을 향상시켜주는

The Client

The Client 소개

특화된 기능을 통하여 기업의 안정적인 전산 운영 환경 실현



Orange Labs's
The Client

Speedy Up

신속한 장애탐지

- 어플리케이션 장애 탐지
- 커널 장애 탐지
- 탐지 대상 정의

Efficiency Up

효율적인 성능진단

- 어플리케이션 성능 모니터링
- 커널 성능 모니터링
- 탐지 및 저장

Support Up

실시간 통합관리 및 안정화지원

- 실시간 저장 시스템
- 실시간 1:1, 1:N 원격명령
- PC와 언제나 연결 및 접근 가능한 구조



Orangelabs

여기서 잠깐, Why Orange labs ?

왜 오렌지랩스인가?

EDR개발 노하우와 수년간의 현장 경험이 축적된 S/W 개발

대표

김 범 진

- ✓ 국내 최고 EDR 개발자로서 SW보안 분야에서 레드스톤 소프트 공동창업 및 팀스 선정
- ✓ 코스닥 상장사인 '지니언스'에 M&A, 이후 EDR 사업부를 총괄하며 인수 후 3년간 국내 EDR 점유율 80% 기록
- ✓ EDR 사업 등 영업을 통한 고객사들의 보안 및 단말시장의 고객사 Needs를 기반으로 '오렌지랩스' 창설

주요경력_직책 및 주요 성과

지니언스 | EDR 개발팀장 / 레드스톤소프트 M&A 이후 사업부 총괄
 "국내 시장 점유율 80% 이상 달성"
 주요 고객사 : SK하이닉스(45,000대), KB은행(40,000대) 등

레드스톤소프트 | 국내최초 EDR 개발 / 공동창업, CTO, 개발총괄
 "팀스 과제 통한 국내 최초 EDR시스템 개발, 지니언스 M&A"

피플웨어 | 창업자 / 대표이사
 "위치 기반/증강현실/커뮤니티/PC연동 모바일 앱,
 RemoteX, AirMovie 개발, 국내 앱스토어 유료앱 판매 1위 "

안랩 | 기업용PC 보안관리 시스템 개발리더
 "기업PC보안 관리 시스템 개발, 패치관리 시스템 개발"

삼성SDS | DMS(Desktop Management System) 개발리더
 "기업 PC관리 시스템 개발, 행정망 프로그램 자동 업데이트 시스템 개발"

연혁

2017.01 | 레드스톤소프트 창업 (김범진 대표 공동창업자)

2017.07 | 팀스프로그램 선정

2018.07 | 지니언스, 레드스톤소프트 인수 및 EDR 사업부 런칭 및 고객사 영업

실시간 모니터링	진단/분석	대응	데이터분석
- 어플리케이션/커널 성능 - 전체 사용자의 단말 사용률 및 on/off 상태, 발생 증상	- 어플리케이션/커널 장애 - 단말기의 기능 장애 - 프로그램 간의 충돌 원인제공자 분석	- 선 제 적 대 처 방 안 수립 - 장애 프로그램 종료 - 부하지수, CPI/메모리/IO 사용량 분석/고지 - 분석된 장애 대응	- 가시화된 분석화면 - 수치화 데이터 제공 - 웹 연동 방식

전산 문제를 실시간으로 탐지하고 원인을 자동으로 분석하는 솔루션 개발

The Client의 기능 및 장점

장점 01.

Efficiency Up

효율적인 성능진단

장점 02.

Speedy Up

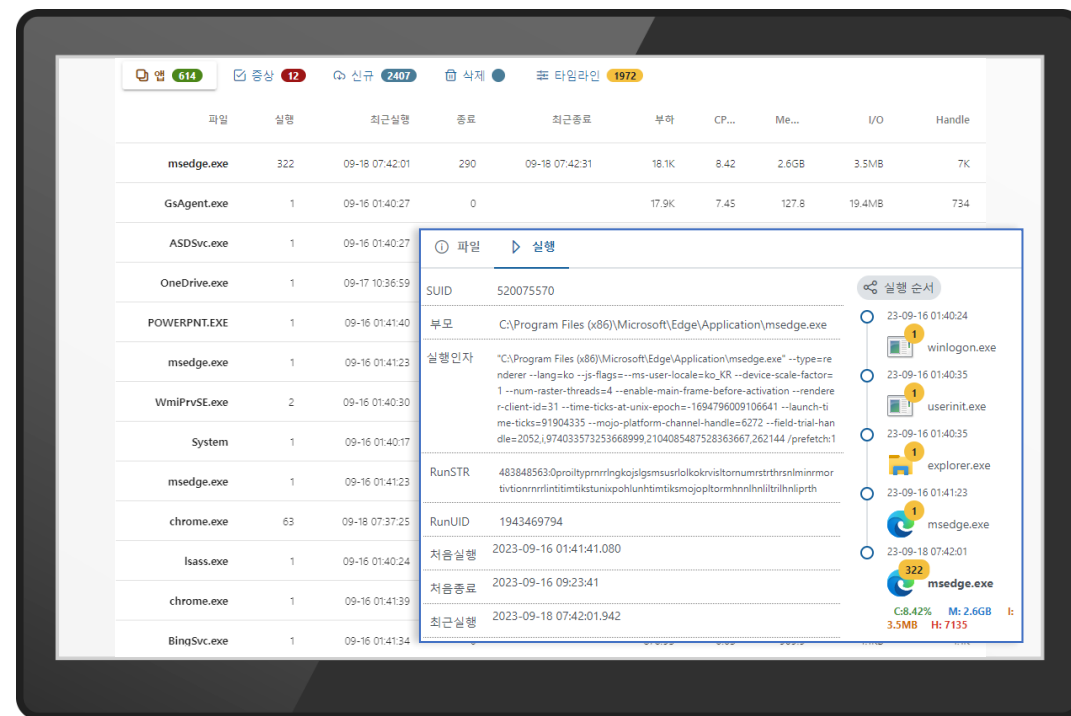
신속한 장애 탐지

장점 03.

Support Up

실시간 통합관리 및 안정화
지원

PC 성능을 수치화 된 데이터로 나타내어 알아보기 쉽게 제시



01. 다양한 증상



- ✔ 프로세스 동작 방식,
시스템 상태, 윈도우
이벤트 등 다양한 문제
증상 탐지

02. 솔루션간 영향도



- 2개의 서로 다른 솔루션 간 충돌, 장애, 성능 데이터를 통한 상호 관계 분석
- 관리자는 솔루션 간 서로 미치는 영향도 파악

03. 외부환경 요소



- 외부 네트워크 장비,
서버 문제 등

Convenience Up!

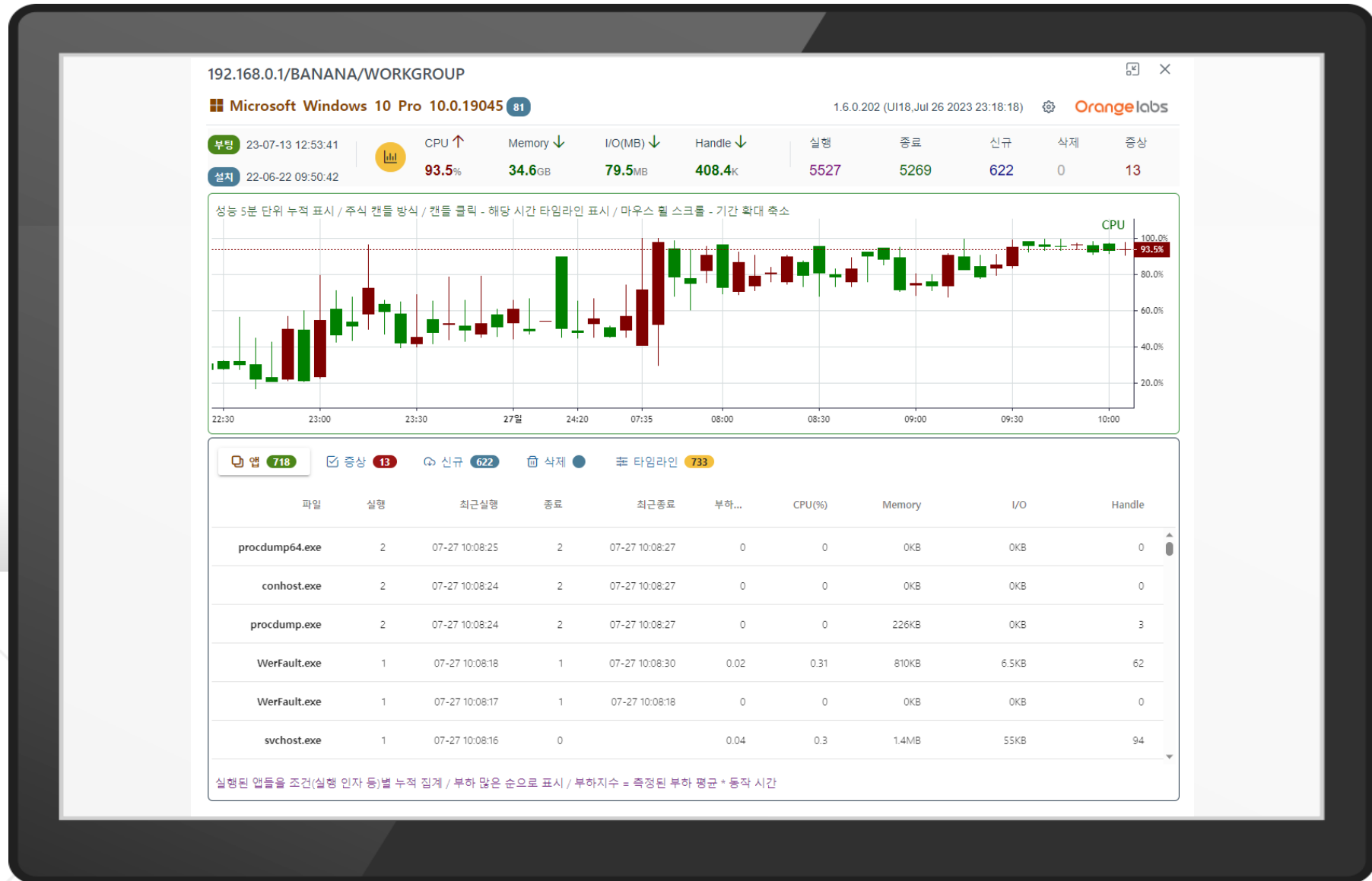
기업 전산관리의
편의성을 향상시켜주는

The Client

The Client의 기능

Efficiency Up 효율적인 성능진단

직관적인 관리화면을 통한 전산관리자의 업무 효율성 향상



Convenience Up!

기업 전산관리의
편의성을 향상시켜주는

The Client

The Client의 기능

Efficiency Up 효율적인 성능진단

직관적인 관리화면을 통한 전산관리자의 업무 효율성 향상



Convenience Up!

기업 전산관리의
편의성을 향상시켜주는

The Client

The Client의 기능

Efficiency Up 효율적인 성능진단

직관적인 관리화면을 통한 전산관리자의 업무 효율성 향상

2

증상 중 1명의 이름, 부서, IP, 부팅일, H/W정보, OS 종류 등 확인

The Client

전체 35 온라인 17 오프라인 18

2023-7-26



172.16.77.150/CHOIT/WORKUP	
사용자	최민재
부서	보안파트
PC명	CHOIT
도메인명	WORKUP
로그온ID	choit
IP(내부)	127.0.0.1
IP(외부)	172.16.77.150
부팅	2023-07-26 15:54:23
부팅ID	196
설치	2022-08-25 15:54:24.000
VM여부	false

1

의 사용자 클릭 후 증상 발생자 확인(IP, PC명 등)

사용자 35 증상 57 타임라인 118

유형	발생	방안	1	↓ 사용자	등록 사용자 중 발생 수량
파일시스템	I/O지연	System	2	3	2023-07-26 17:47:00
부팅성능	성능저하	msedge.exe	2	3	2023-07-26 13:56:29
부팅성능	성능저하	svchost.exe	2	2	2023-07-26 17:46:35
프로세스	RuntimeBroker.exe	svchost.exe	1	1	2023-07-26 17:56:15
프로세스	LenovoVantage-(Vantage	Lenovo.VantageService.InstallerHelper.e	1	1	2023-07-26 17:51:45
부팅성능	성능저하	services.exe	1	1	2023-07-26 17:47:15

처음발생

설명

I/O를 완료하는데 30초 이상 걸림. 하드디스크 성능 저하 또는 보안 프로그램 문제일 수 있음.

증상설명

Convenience Up!

기업 전산관리의
편의성을 향상시켜주는

The Client

The Client의 기능

Efficiency Up 효율적인 성능진단

직관적인 관리화면을 통한 전산관리자의 업무 효율성 향상

[FileInfo] Antimalware Service Executable 4.18.23050.9 (18bf1f2590bbc7e0256a02153591e722bb971707)

1 클릭 후 증상에 대한 분석 확인

① 파일 분석 <> JSON

I/O를 완료하는데 30초 이상 걸림. 하드디스크 성능 저하 또는 보안 프로그램 문제일 수 있음.

```
{
  "DocType": "Event",
  "Event": {
    "EventTime": "2023-07-26 06:46:45.988837300",
    "File": {
      "PID": 63900,
      "Process": {
        "RunId": "FileSystemDegradation",
        "SUID": 2537485307,
        "time": 1690321500
      }
    }
  }
}
```

SUID 105391514

증상원인 및 이력 시점 확인

수집 시점 및 유형

- 2023-07-26 06:46:45.988837300 MsMpEng.exe
- 2023-07-19 05:12:31.3451663Z MsMpEng.exe
- 2023-07-18 06:06:26.3788557Z MsMpEng.exe
- 2023-07-18 06:06:26.3788557Z MsMpEng.exe
- 2023-07-13 17:09:42.0000329Z MsMpEng.exe

증상별 최대 5건 수집.

사용자 35 증상 57 타임라인 119

유형	발생	원인	↓ 사용자	횟수	최근발생	처음발생	설명
프로세스	GsAgent.exe	xfliterctr164.dll	1	6	2023-07-26 11:38:23	2023-07-26 10:35:53	1개 이상의 CPU 코어를 일정 시간 이상 점유함.
프로세스	pennyroyal.exe	svchost.exe	1	1	2023-07-26 10:37:54	2023-07-26 10:37:54	프로그램 강제 종료됨
프로세스	Widgets.exe	svchost.exe	1	2	2023-07-26 18:04:31	2023-07-26 09:21:00	프로그램 강제 종료됨
프로세스	backgroundTaskHost.exe	svchost.exe	1	1	2023-07-26 08:52:23	2023-07-26 08:52:23	프로그램 강제 종료됨
프로세스	MsMpEng.exe	ntdll.dll	1	1	2023-07-26 08:27:37	2023-07-26 08:27:37	1개 이상의 CPU 코어를 일정 시간 이상 점유함.
파일시스템	I/O지연			1	2023-07-26 15:46:50	2023-07-26 15:46:50	I/O를 완료하는데 30초 이상 걸림. 하드디스크 성능 저하 또는 보안 프로그램 문제일 수 있음.

1 I/O지연 발생 원인 확인 위한 클릭

Convenience Up!

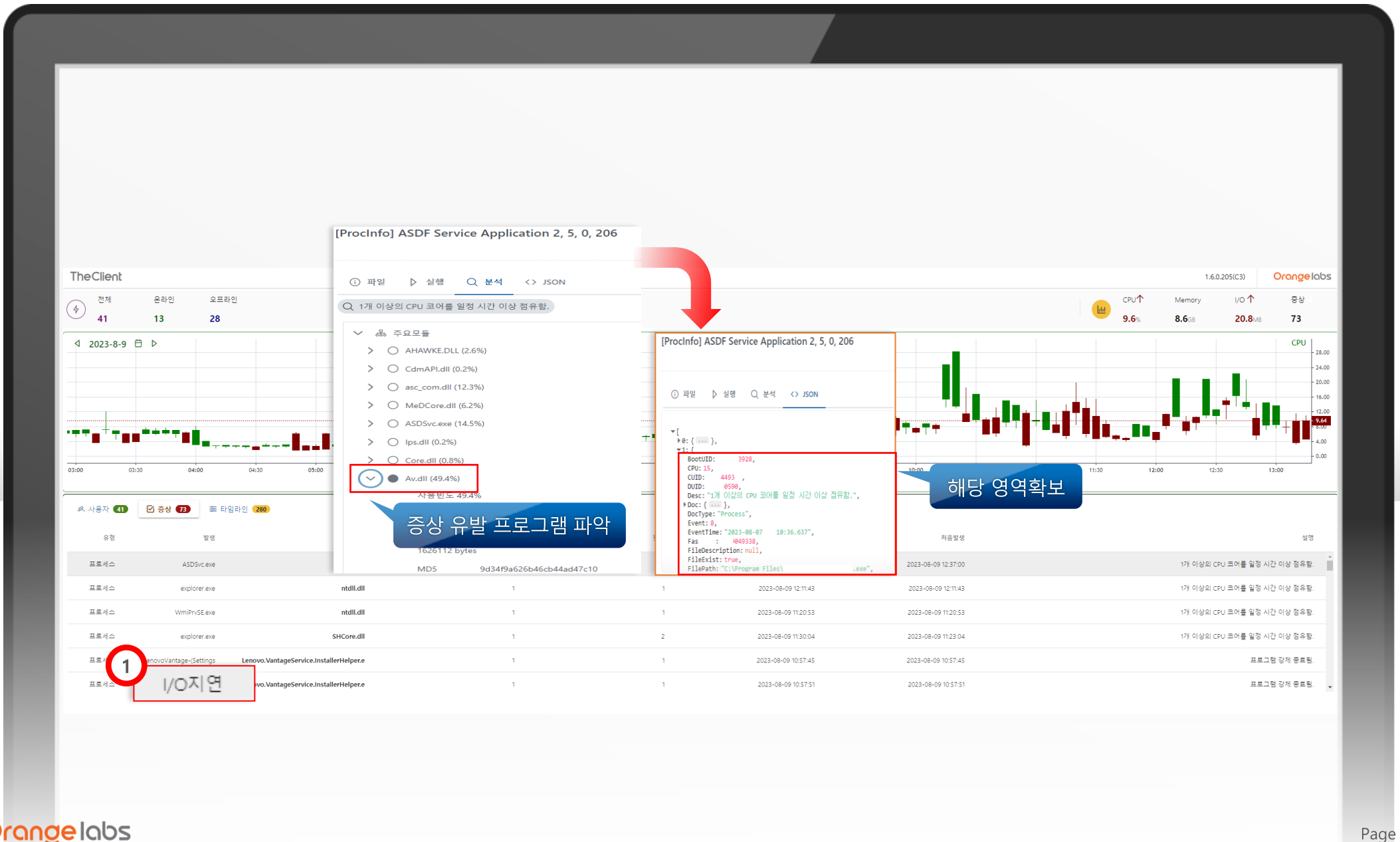
기업 전산관리의
편의성을 향상시켜주는

The Client

The Client의 기능

Efficiency Up 효율적인 성능진단

직관적인 관리화면을 통한 전산관리자의 업무 효율성 향상



The Client의 기능 및 장점

장점 01.

Efficiency Up

효율적인 성능진단

장점 02.

Speedy Up

신속한 장애 탐지

장점 03.

Support Up

실시간 통합관리 및 안정화
지원

Convenience Up!

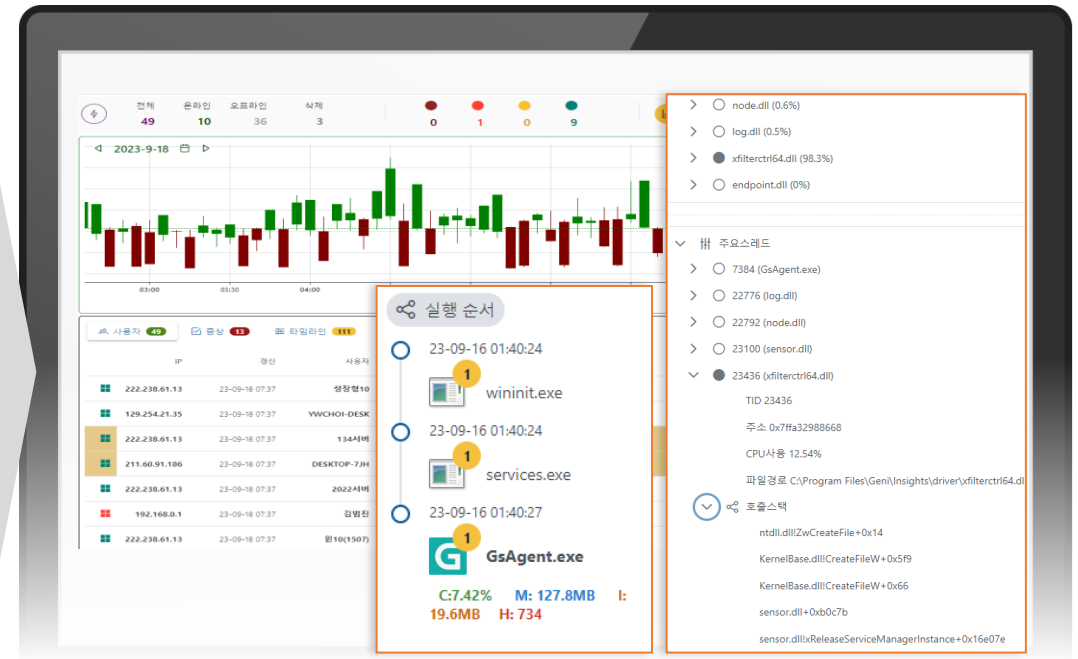
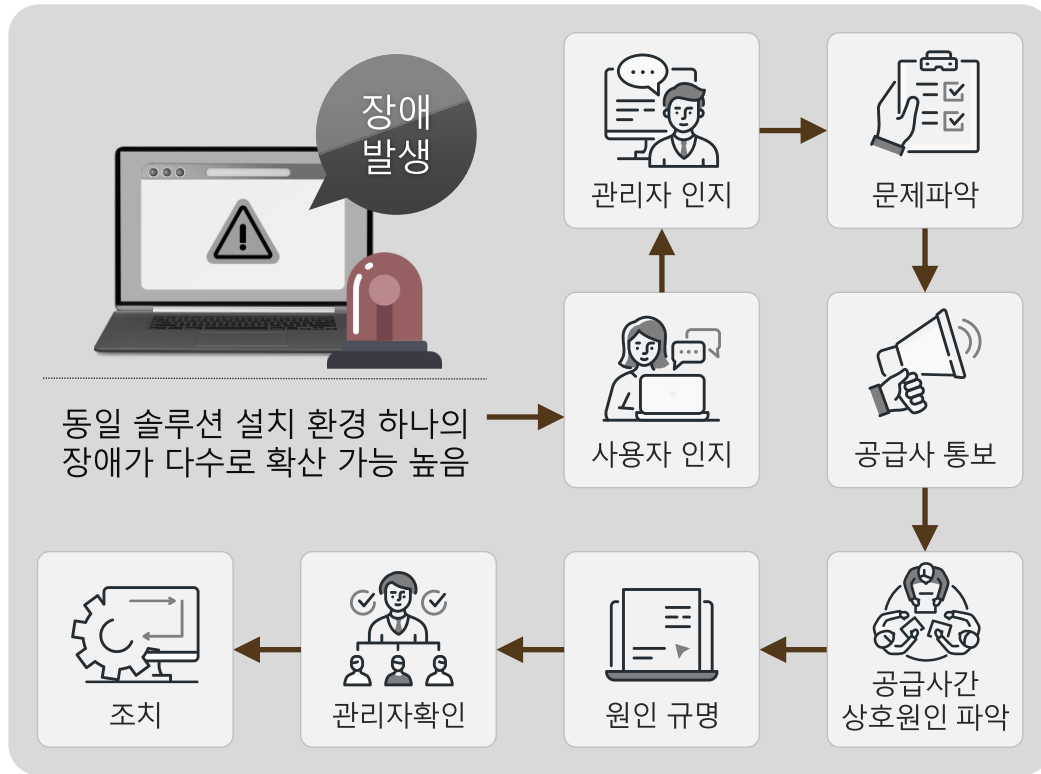
기업 전산관리의
편의성을 향상시켜주는

The Client

The Client의 기능

Speedy Up 신속한 장애탐지

실시간 모니터링을 통한 장애원인 파악으로 신속한 조치 가능



다양한 개발 경험을 통해 다수의 문제발생 장애탐지 기술 확보

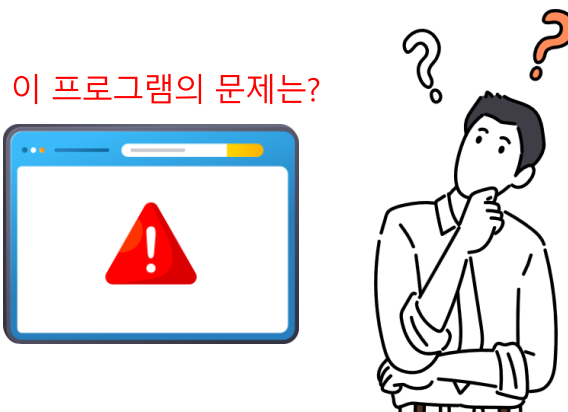
장애유형

프로그램 설치 실패



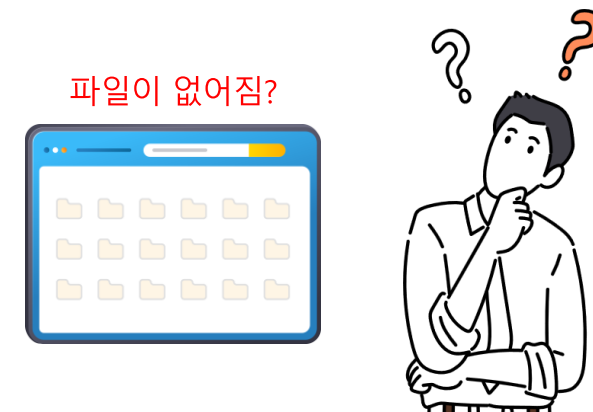
프로그램 설치 과정에서 계속 실패 메시지 표시됨

새로 도입한 프로그램의 잦은 종료



새로 설치한 프로그램의 잦은 종료
해당 프로그램 제작사에서도 파악 안됨

필수 프로그램 자동 삭제



사내 필수 프로그램의 실행 파일이 사라짐
다시 설치해도 또 사라짐



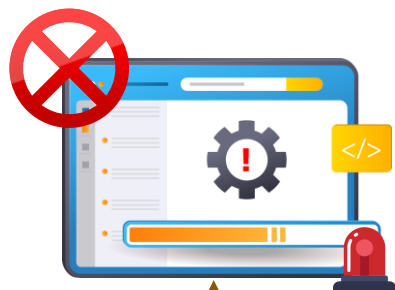
여러가지 문제들로 얽힌 복잡한 장애 발생 탐지가능

CPU 사용률, 메모리 사용량과 같은 일반적인 성능 지표로는
절대 풀 수 없는 문제도 탐지가능

다양한 장애 증상 탐지로 가벼운 장애 요인 사전 차단

솔루션

프로그램 설치 실패



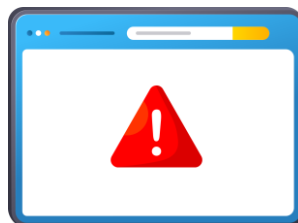
문제를 발생시킨
솔루션 특정



보안 솔루션의 신규 파일 분석 ▶ 파일 선점
이로 인한 설치본 설치 과정의 방해 발생

새로 도입한 프로그램의 잦은 종료

이 프로그램의 문제는?



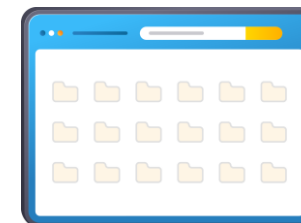
문제를 발생시킨
솔루션 특정



보안 솔루션이 오동작 또는 오설정으로
강제 종료 시킴

필수 프로그램 자동 삭제

파일이 없어짐?



문제를 발생시킨
솔루션 특정



보안 솔루션이 오동작 또는 오설정으로
파일 강제 삭제됨

EDR 개발 및 다수의 기업 운영 노하우 적용

- ✓ EDR 개발 및 시스템 설계 모든 분야에 참여한 엔지니어의 솔루션
- ✓ 많은 보안 솔루션 + 일반 제품의 다양한 행동 방식 분석 경험
- ✓ 다양한 Endpoint 행위 정보 수집 기술 + 정보 간 연결 + 인과
관계에 대한 깊은 이해와 특정 행위로 발생하는 다양한 영향 및
결과 분석 경험



여러 가지 문제들로 얽힌
복잡한 장애 발생 탐지가능

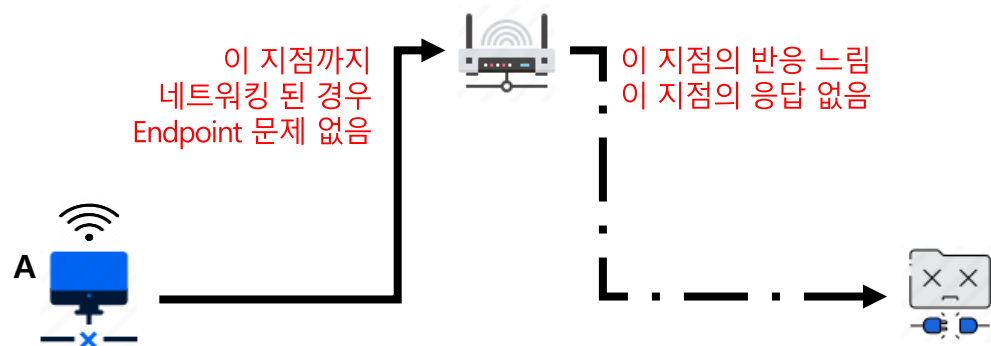
CPU 사용률, 메모리 사용량과 같은
일반적인 성능 지표로는 절대 풀 수
없는 문제도 탐지가능

다양한 증상 탐지 및 원인파악으로 신속한 장애 대처 가능

다차원 장애 증상 탐지로 복잡한 장애 요인에 대한 조치가능

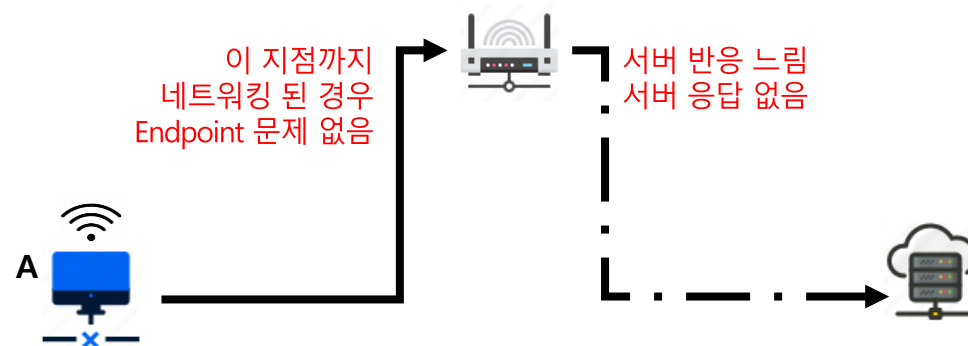
문제 원인 ▶

Endpoint 아님 외부 네트워크 장비



문제 원인 ▶

Endpoint 아님 외부 서버



관리자 정의 Endpoint 내부 증상 탐지

- ✓ 기업마다 장애의 조건 정의가 다를 수 있어 관리자 정의 탐지 제공
- ✓ Endpoint에서 수집 가능한 항목들의 조합으로 새로운 증상 정의
- ✓ 2개 이상의 증상 조합으로 복합 증상 정의와 탐지
예 : 각 Process별 동작에 문제가 없지만 시스템 전체 CPU 사용율이 80% 이상일 때 가장 사용량이 많은 Process 탐지

Endpoint 외부 증상 탐지

- ✓ Endpoint 내부는 문제 없지만 외부 네트워크 장비로 인한 증상 탐지
- ✓ 방화벽 설정 오류로 루프 지연 발생 증상 탐지
- ✓ Endpoint 외부 서버의 느린 응답 또는 응답 없음으로 문제가 발생한 경우
- ✓ Endpoint + 네트워크 장비 or 서버 와 같이 여러 차원에 걸친 문제 증상 탐지

1개 Device내 다수 행위들의 조건부 탐지와 2개 이상의 Device간
정보 연관성 분석으로 장애탐지 및 조치확인

The Client의 기능 및 장점

장점 01.

Efficiency Up

효율적인 성능진단

장점 02.

Speedy Up

신속한 장애 탐지

장점 03.

Support Up

실시간 통합관리 및 안정화
지원

Convenience Up!

기업 전산관리의
편의성을 향상시켜주는

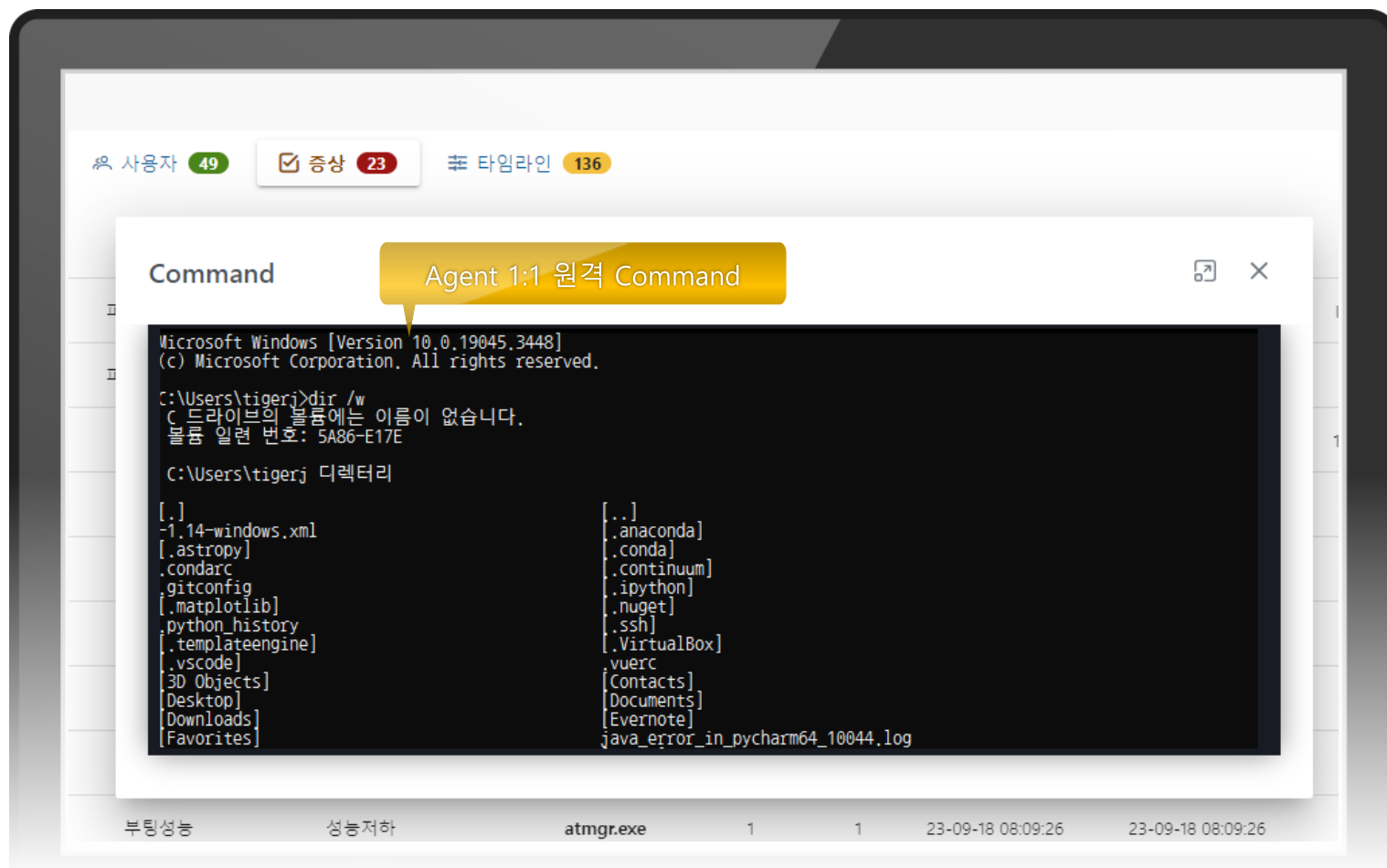
The Client

The Client의 기능

Support Up 실시간 통합관리 및 안정화지원

자동화 데이터 집계 및 실시간 처리구조를 통한 운영 연속성 확보

- ✓ 기업 전체 현황부터 개인별 세부 사항까지 실시간으로 파악
- ✓ 기업 전체 PC들을 대상으로 1:N 명령 하달 및 정보 집계
- ✓ 특정 PC 1대를 대상으로 명령 하달, 원격 커맨드, 정보 집계 및 에이전트 상세 정보 스트리밍



Live Response

- 윈도우 CMD(도스창)를 원격으로 구현
- 1:1 명령 처리 및 실시간 처리 결과 확인

Live Command

- 전사 모든 PC를 대상으로 1:N 명령 수행
- 처리된 명령 결과의 실시간 확인 및 취합

Live Search

- 전사 모든 PC를 대상으로 1:N 정보 수집
- 처리된 수집 결과의 실시간 확인 및 취합
- 파일 해시, WMI 등의 정보 수집 명령어 제공

Convenience Up!

기업 전산관리의
편의성을 향상시켜주는

The Client

The Client의 기능

Support Up 실시간 통합관리 및 안정화지원

실시간 통합관리를 통해 실시간 사용자 PC 관리로 안정성 확보

- ☑ 관리자 UI에서 Push Notification 처리 기술을 통해 실시간 화면 표출
- ☑ 관리자 UI - 매니저, Agent - 매니저간 실시간 네트워킹 처리 기술로 실시간 PC관리



Convenience Up!

기업 전산관리의
편의성을 향상시켜주는

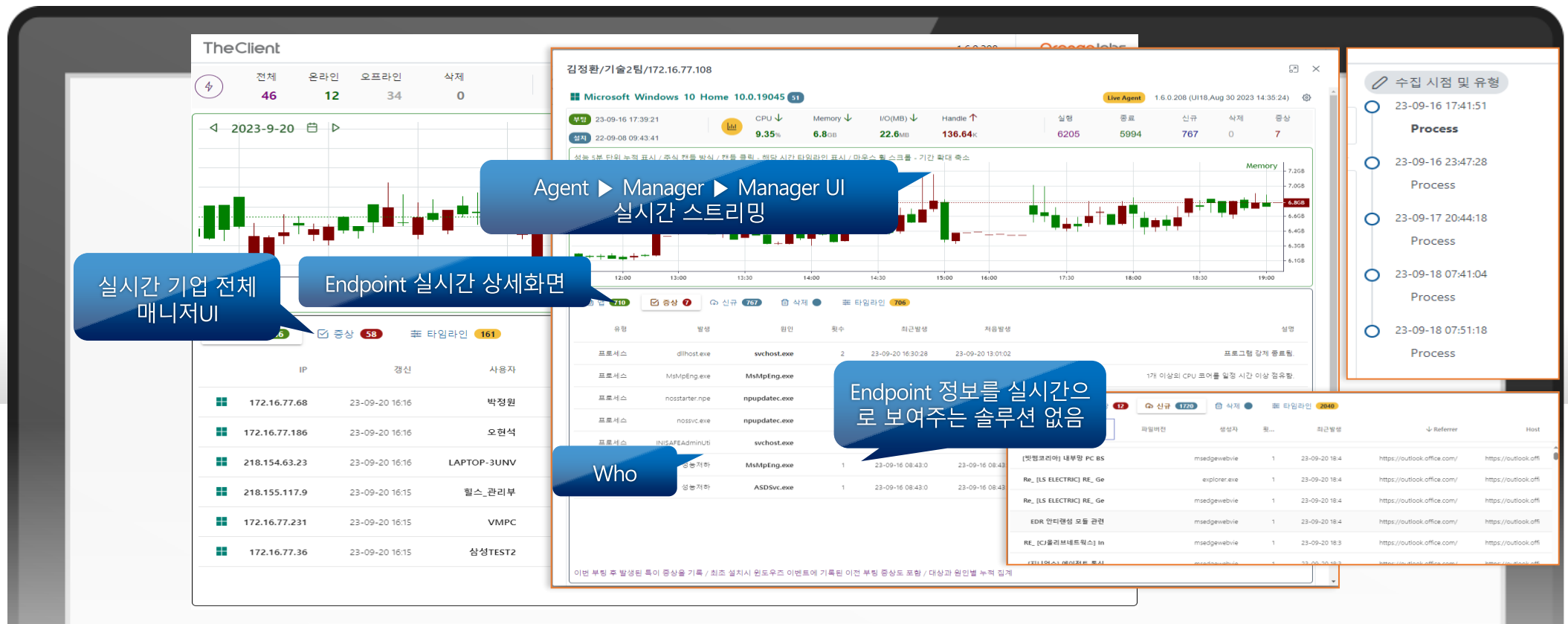
The Client

The Client의 기능

Support Up 실시간 통합관리 및 안정화지원

실시간 통합관리 및 지속적 지원을 통한 안정적인 운영환경 실현

- ✓ 관리자 UI – Endpoint 간 실시간 네트워킹 기술
- ✓ NAT와 같은 다양한 네트워킹 환경에서의 처리 기술



다양한 네트워크 실시간 통합관리 기술을 통해 사용자 PC실시간 관리가능

머신 러닝 예측 시스템 개발 등 지속적인 업그레이드로 안정성 지원 보장(개발 예정)

- ✓ 머신러닝 학습에 필요한 다양한 행위 정보 수집 기술 개발예정
- ✓ 행위 정보 별 연관성 분석 기술 개발예정

특정 PC CPU 과다 사용 ▶

다른 PC 발생 가능성 예측

동작방식(SUID)이 동일한 솔루션 설치
영향도 있는 추가 솔루션 설치
동일 솔루션 서버와 비슷한 패턴의 네트워크 통신
윈도우 특정 레지스트리 설정 동일 여부
▶ 비슷한 조건의 다른 PC에도 발생 가능성 높음

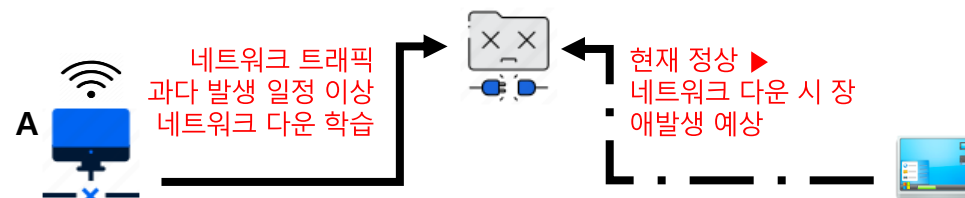


장애 사전 예측

- ✓ 현재 기 구현된 Endpoint 기술과 기능은 case by case 코드 구현
- ✓ 성능 지표가 임계치 초과 or 크래시 / 파일 선점 / 파일 삭제와 같은 명확한 증상 탐지
- ✓ 기업 IT인프라 환경 복잡성 증대 ▶ 학습을 통한 추가 탐지와 예측 필요

네트워크 장비 다운 예측 ▶

해당 장비를 이용하는 Endpoint 수 측정



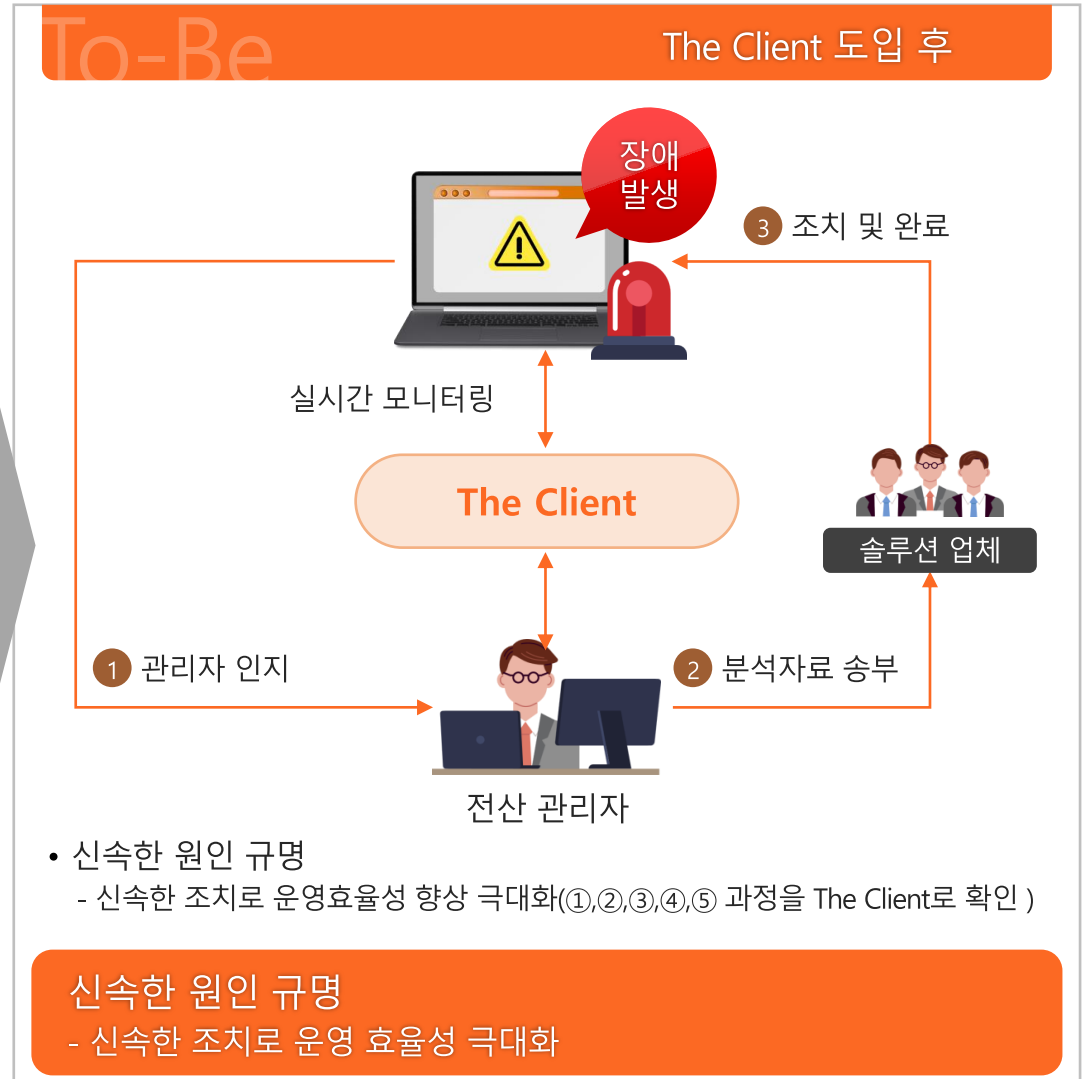
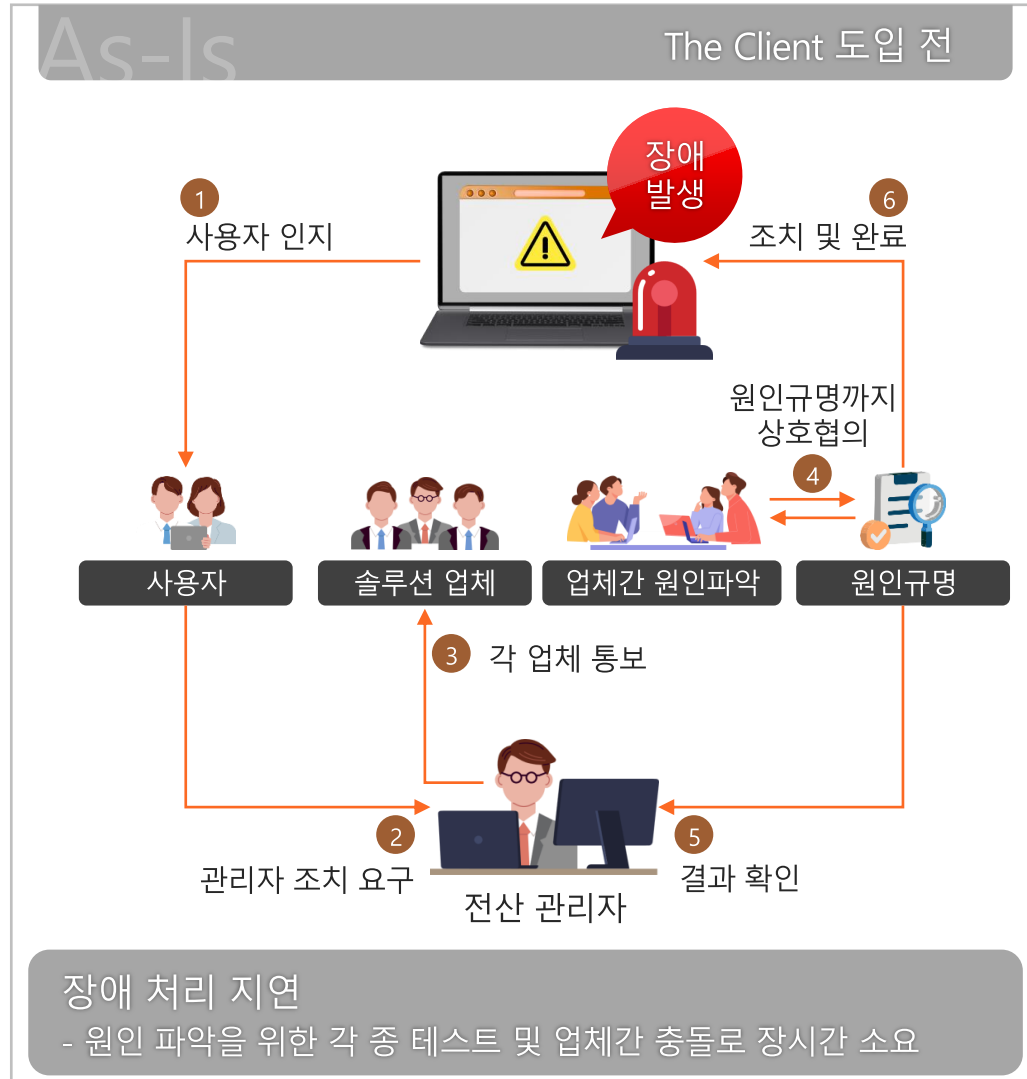
학습 자료

- ✓ 설치된 솔루션 정보 ▶ 동작방식(SUID) / 증상이 일어난 원인 모듈
- ✓ 설치된 솔루션 간의 영향도 정보
- ✓ EDR 기술로 수집 가능한 정보 ▶ 프로세스 / 파일 사용량 / 네트워크 / 주요 레지스트리(윈도우 및 주요 프로그램 설정) 변경 정보
- ✓ 라우터 경로 정보 ▶ ICMP / Broadcasting 정보

이전 나열된 모든 기술과 기능에서 추출된 정보들을 종합
기업 전체에 발생할 장애를 미리 예측

신속한 원인 규명으로 안정적인 운영환경 보장

✓ The Client도입을 통해 업그레이드된 PC관리 및 원인분석 보장



Orange labs The Client

Efficiency Up

효율적인 성능진단

Speedy Up

신속한 장애탐지

Support Up

실시간 통합관리 및
안정화지원

Convenience Up!

기업 전산관리의 편의성과 안전성 향상을 약속 드립니다.



Q n A

감사합니다.