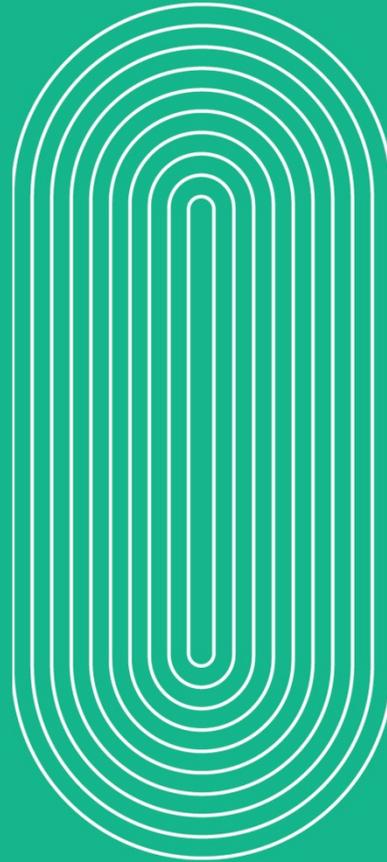


안전하고 효율적인  
패치관리 솔루션  
알약 패치관리(PMS) 2.1



알약 패치관리(PMS) 2.1

# INDEX

안전하고 효율적인  
패치관리 솔루션

## 01 제안배경

- 제로데이 공격의 증가
- 랜섬웨어 피해의 급증
- 보안패치 중요성 대두

## 02 제품소개

- PMS2.1 소개
- 도입효과
- 주요기능

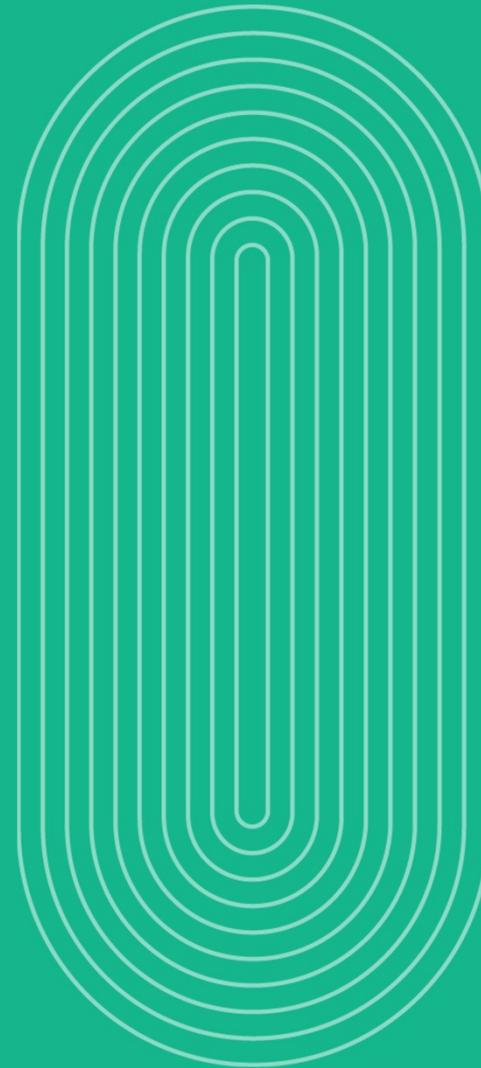
## 03 고객지원

- 이스트시큐리티 대응센터
- 고객지원 서비스
- 구성 및 운용

01

# 제안 배경

- 제로데이 공격의 증가
- 랜섬웨어 피해의 급증
- 보안패치 중요성 대두



# 제로데이 취약점 공격 증가

## 고도화되는 엔드포인트 취약점 공격

최근 발생하는 각종 침해 공격의 대부분은 시스템 및 애플리케이션의 취약점을 이용하고 있으며, 특히 해당 취약점에 대한 **패치가 나오지 않은 시점에서 이루어지는 제로 데이 공격**이 급증하고 있다.



### 제로데이 취약점

- 제로데이 취약점 공격 사상 최대 기록
- 시스템 및 애플리케이션의 취약점 악용



### 지능/조직화된 APT 공격

- 새로운 공격 기법 접목시켜 응용화
- 다양한 유입 경로를 통한 공격



### 수동 보안/관리의 한계

- 비 표준화된 다수 시스템 대응 한계
- 한정된 담당 인력으로 관리 홀 발생

# 공격 사례 - 제로데이

[연도별 공격 사례]

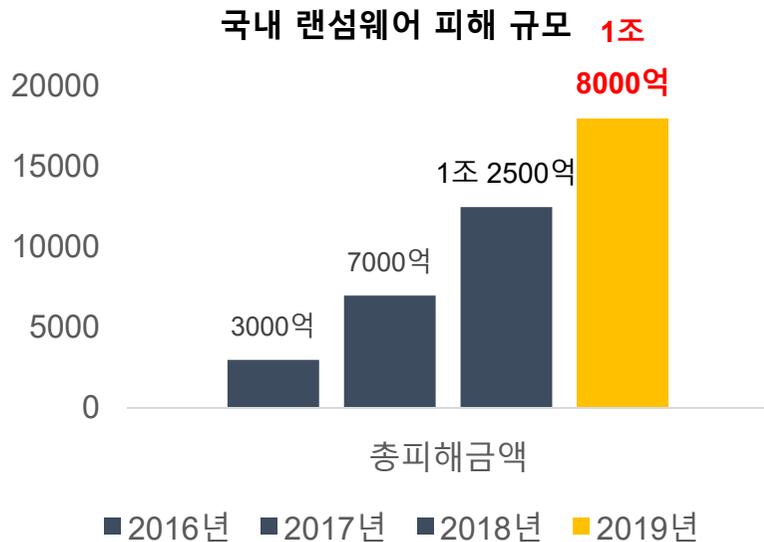
2022년	안드로이드 사용자에게도 크롬 브라우저 엔진의 코드 실행 취약점을 샌드박스 탈출 및 특권 승격과 결합한, 비슷한 익스플로잇 체인이 배포되어 혼동 취약점(CVE-2022-3723) 악용
	삼성 디바이스를 대상으로 하는 스파이웨어 익스플로잇 체인을 ARM이 2022년 1월에 수정한 ARM 말리 GPU 커널 드라이버의 특권 승격 취약점(CVE-2022-22706) 악용
2021년	애플이 2021년 10월 iOS 15.1에서 패치한 GPU 드라이버 구성요소인 AGX액셀러레이터(AGXAccelerator)의 샌드박스 탈출 및 특권 승격 결함(CVE-2021-30900)과 결합
2020년	7개사 백신프로그램 임의파일 삭제 취약점(CVE-2020-25043)을 악용
2019년	해킹 그룹 핀6(FIN6)은 금전을 목적으로 윈도우 서버 2019 UAF(Use-After-Free) 취약점(CVE-2019-0859)을 악용
2018년	중국 기반 공격 그룹 다수가 마이크로소프트 오피스 취약점(CVE-2018-0802)을 이용해 유럽, 러시아, 동남아시아, 대만에 위치한 여러 업계를 대상으로 공격 캠페인을 실행(샘플의 최소 절반 이상이 취약성 패치 배포 이전에 진행)
2017년	러시아 그룹 APT28 및 털라(Turla)는 마이크로소프트 오피스 제품 내 여러 제로데이 취약점을 활용해 공격
	북한 사이버공격그룹 APT37은 어도비 플래시 제로데이 취약점(CVE-2018-4878)을 활용한 캠페인을 수행. 위 그룹은 취약점이 공개된 후 빠른 시간 안에 공격할 수 있는 역량을 입증

출처 : 데일리시큐, itworld

# 랜섬웨어 피해 급증

## 한정된 인력으로 효율적 관리를 위한 통합 시스템 필요

- 취약점을 노린 제로데이 공격 중 랜섬웨어가 보편적인 공격 수단으로 이용
- 국내에는 Drive by Download 방식을 이용하여 사용자PC에 설치된 SW나 OS의 취약점을 악용해 랜섬웨어를 대량 유포
- 최근 업무 담당자를 타깃으로 이력서나 경고장 등 문서파일 위장 및 보안 업데이트가 미흡한 사용자를 노려 PC환경을 분석해 각종 취약점을 악용하는 랜섬웨어 유포 사례에 관한 피해 급증
- 랜섬웨어의 유포, 암호화, 우회 방식 등이 고도화되며 이로 인한 피해가 증가하는 상황



출처: 한국 랜섬웨어 침해 대응센터

## 최근 랜섬웨어 해커의 공격시간이 크게 단축

원격 근무의 증가로 랜섬웨어 공격을 수행하는 해킹 그룹의 활동이 특히 활발해지고 있는 상황

일부 사례의 경우 데이터 복호화 비용을 받아내는 데까지의

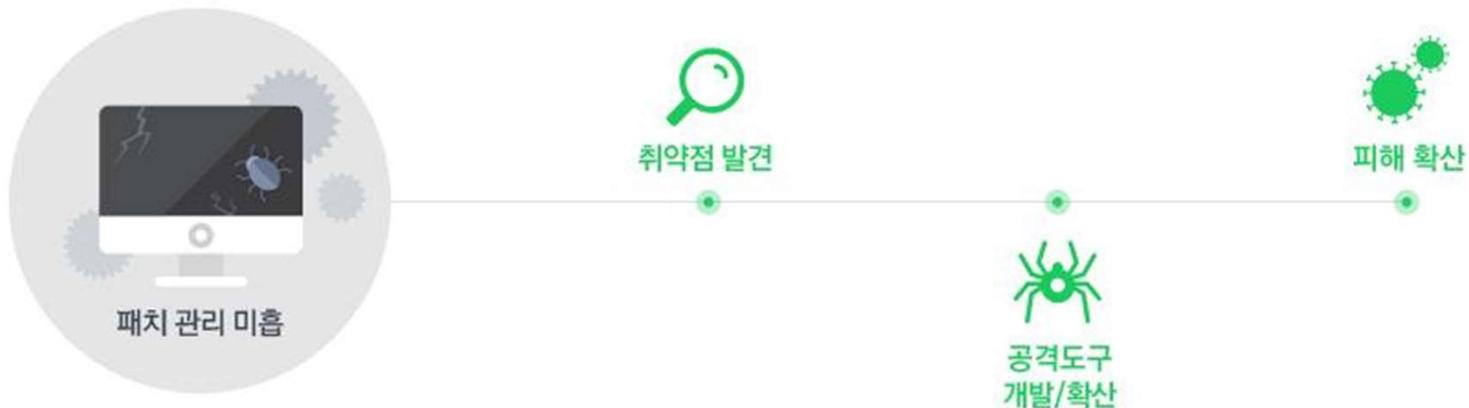
**소요시간은 단 45분**

출처: MS 시큐리티 인텔리전스

# 보안패치의 중요성 대두

## 패치 적용만으로 많은 보안 위협 감소

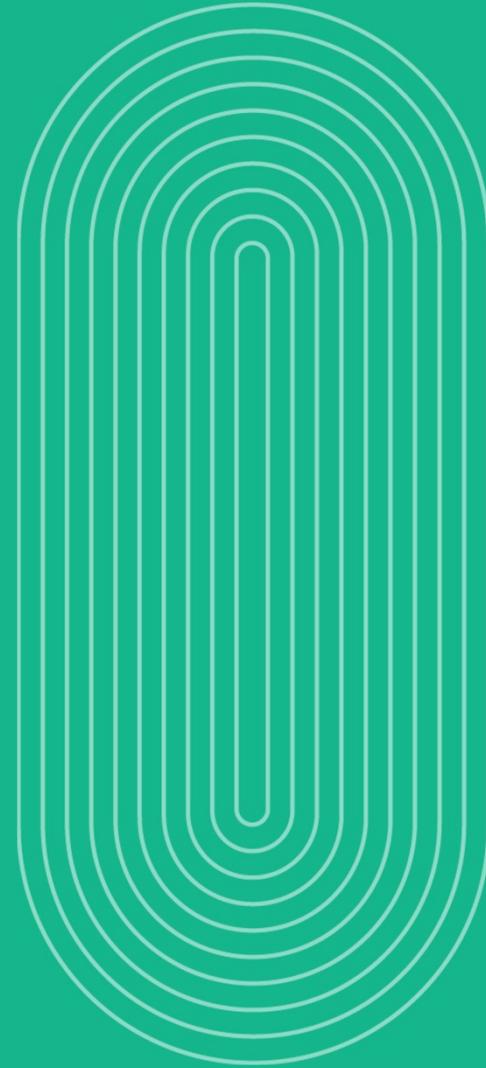
- 취약점은 제로데이(패치 미발표)와 원데이(최신 패치 존재)로 구분되며, 제로데이 공격과 함께 이미 패치가 발표된 상태의 공격 또한 쉽게 일어나는 만큼 **패치 적용만으로 많은 위협을 줄일 수 있음**
- 사내 모든 PC 및 관리 시스템에 대한 일괄적인 패치 설치 및 관리의 어려움으로 중앙화 관리가 가능한 패치 솔루션 도입이 권장 됨
- 특히 은행과 같은 폐쇄망 환경에서는 인터넷을 통한 패치 설치 및 업데이트가 불가능하기 때문에, 전문 패치 솔루션 도입을 통해 더욱 고도화된 패치 관리가 필요함



02

# 제안 배경

- PMS2.1 소개
- 도입 효과
- 주요 기능



## 알약 패치관리(PMS)

알약 패치관리(PMS)는 관리자가 기업 내 PC의 윈도우 업데이트나 주요 소프트웨어의 패치 설치 현황을 실시간으로 확인하고, 신속하고 간편하게 패치 파일을 배포하여 관리할 수 있는 **패치 관리 솔루션**입니다.

높은  
안전성

- 자체 검증 및 테스트 후 패치 파일 배포
- PC 환경 및 상태 별 패치 자동 설치
- 배포 트래픽 자동 분산 처리를 통한 배포 안정성 확보
- 자가보호 기능으로 외부의 공격으로부터 스스로를 보호

고도화된  
효율성

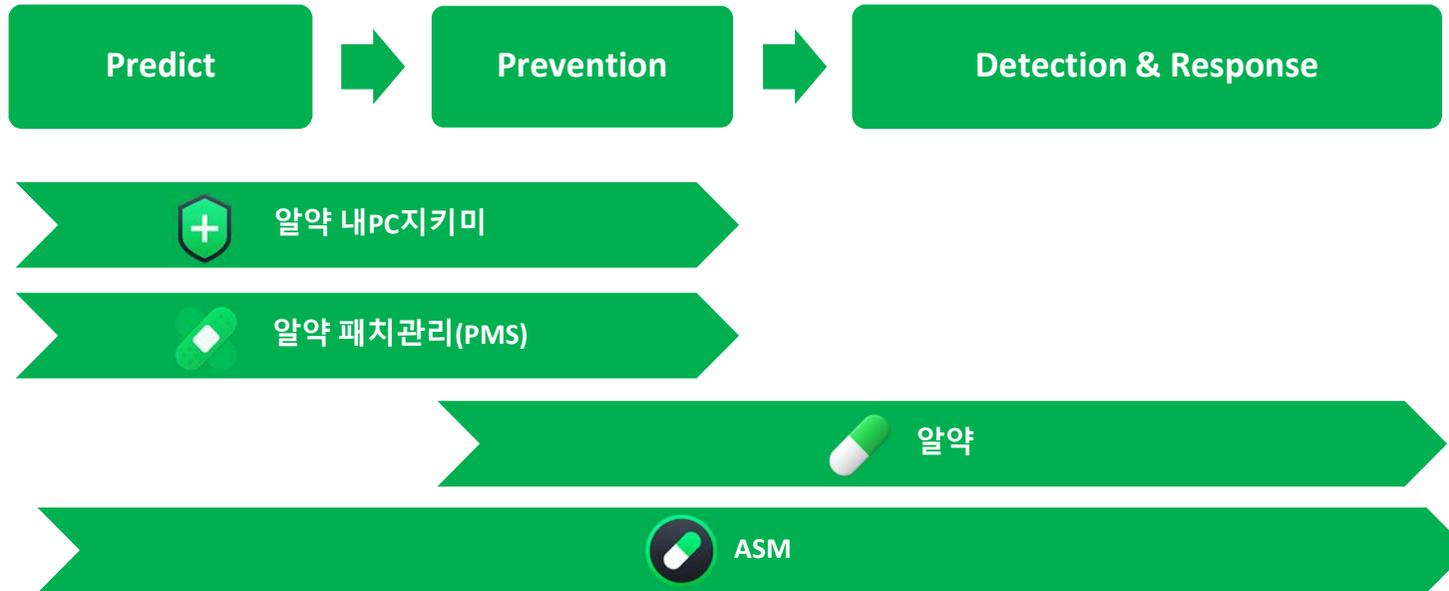
- 알약 제품군 도입 시 별도 서버 구축 없이 라이선스 구매만으로 사용 가능한 시스템 구축 편의성
- ASM4 연동을 통해 백신, 자산, 취약점 등 보안 기능 통합 관리
- 패치 금지 시간, 롤백, 대기일, 용량 제한 등 다양한 패치 스케줄 및 설치 옵션 제공

차별화된  
사용성

- 2017년 5월 GS 인증 1등급, 2020년 5월 CC 인증 획득
- 패치 현황에 대해 빠른 파악이 가능한 시각화된 대시보드와 통계 보고서
- 용도 및 목적에 따라 대시보드 커스터마이징 가능
- 조직도 상시 노출 등 직관적인 작업 및 정책 명령 프로세스 지원
- 추가 보안 제품 구축에 대한 확장성이 고려된 관리 콘솔 UI

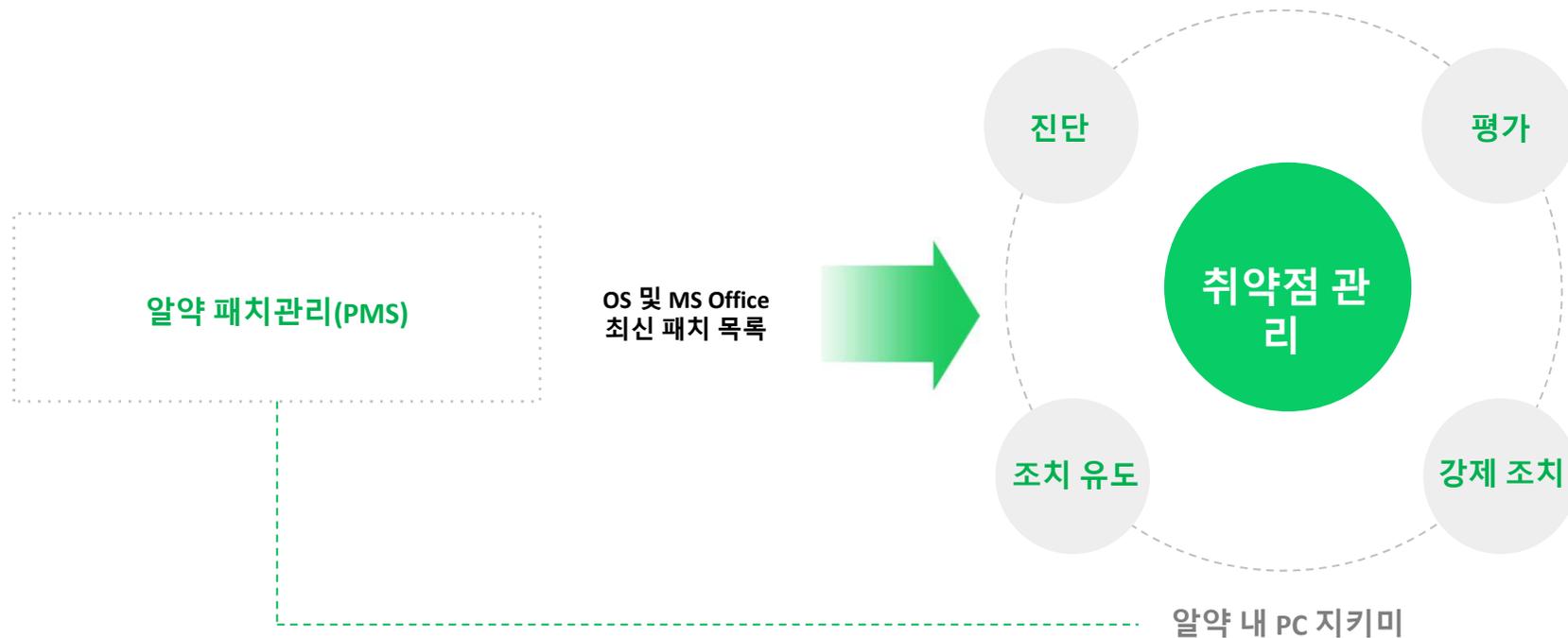
## 도입 효과

지능화되는 사이버 공격에 대응하기 위해서 각 영역별 연계된 방어가 중요해지고 있습니다. 알약 패치관리(PMS)는 최신 보안 패치를 통해서 초기 단계의 취약점을 이용한 공격을 차단합니다. 또한, ASM 통합 플랫폼과 연동되어 Prevention 영역에서 다른 보안 제품과 연계되어 통합 보안 솔루션을 구축합니다.



## 도입 효과

취약점 관리 솔루션인 알약 내PC지키미와 함께 도입 시, 사용자 PC의 모든 취약점 진단에서 조치까지 통합 관리할 수 있어 PC의 취약점으로 인해 발생할 수 있는 모든 위협에 효과적으로 대응할 수 있습니다. 알약 내PC지키미와 연동된 알약 패치관리(PMS)는 패치 관리 시스템을 통해 OS 및 MS office 의 최신 보안 패치 목록을 제공하여 취약점 점검 시, 빠르고 안정적인 패치 설치를 지원합니다.



## 도입 효과

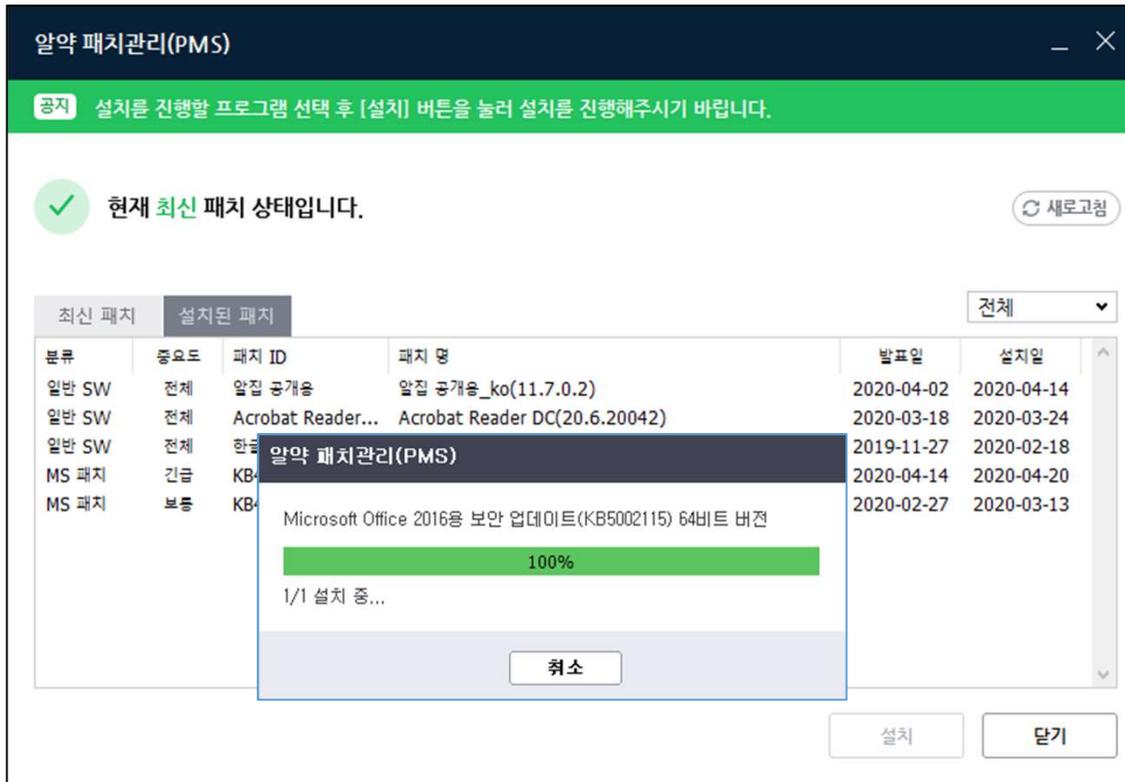
알약 패치관리(PMS) 도입 시 안전하고 효율적인 패치 관리를 통해 고도화되는 위협을 사전 예방할 수 있으며, 최소화된 운영 리소스와 비용으로 알약 및 다양한 솔루션과 연계된 통합 보안 시스템을 구축하여 기업의 보안 수준을 향상시킬 수 있습니다.

<b>알약 패치관리 (PMS)</b>	<b>안전한 보안 환경 구축</b>	<ul style="list-style-type: none"> <li>• 완벽한 일괄 패치로 취약점을 이용한 악성코드 감염 예방</li> <li>• 실시간 모니터링을 통한 신속 대응 가능</li> </ul>
	<b>TCO 절감</b>	<ul style="list-style-type: none"> <li>• ASM 연동을 통한 시스템 구축 및 관리 비용 최소화</li> <li>• 보안 사고 방지를 통한 기업 손실 감소 및 업무 연속성 유지</li> </ul>
	<b>효율적인 보안 솔루션 통합 관리</b>	<ul style="list-style-type: none"> <li>• 통합 에이전트와 서버를 통해 다양한 보안 기능 사용</li> <li>• 일관된 보안 정책 유지 가능</li> </ul>

# 주요 기능

## 사용자 > 클라이언트 UI

- 알약 통합 에이전트를 통해 최신 패치 목록을 확인하고 선택적으로 수동 설치할 수 있습니다.



## 패치 관리 클라이언트

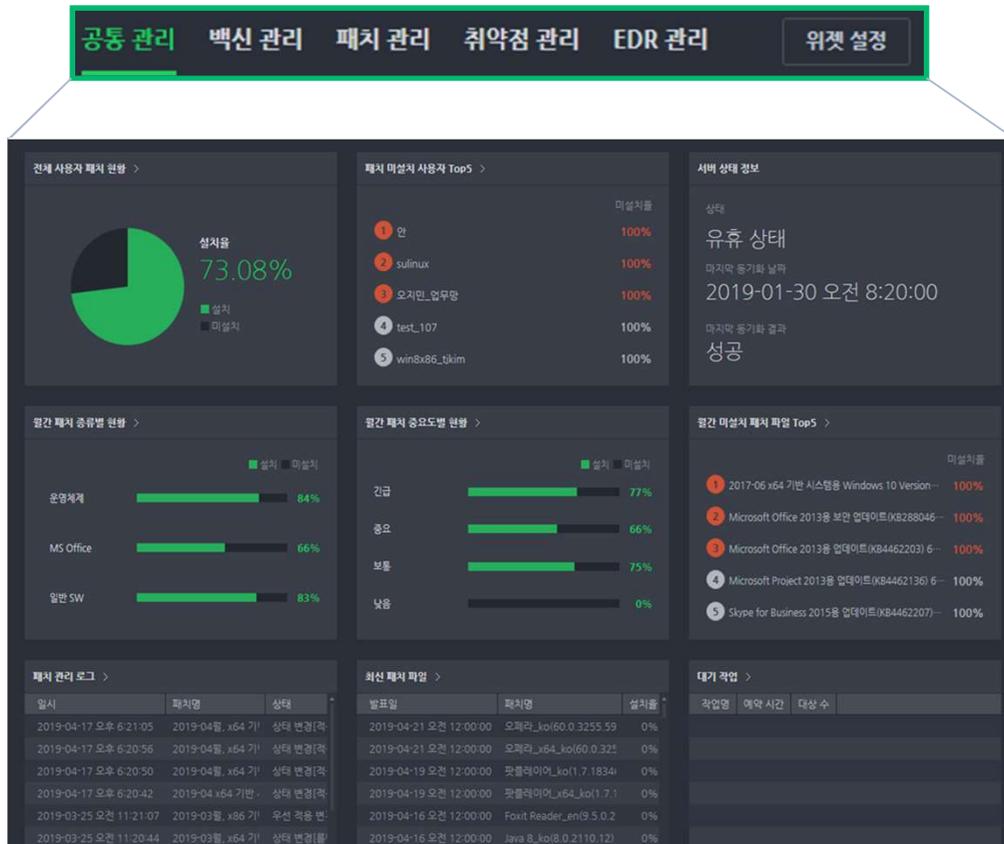
알약 백신 에이전트와 통합 운용

- 최신 패치 목록 표시
- 설치된 패치 목록 표시
- 관리자에 의해 설정된 [공지] 확인

# 주요 기능

## 관리자 > 직관적인 대시보드

- 이미지와 그래프를 통해 전체 패치 운용 현황을 한 눈에 파악 할 수 있도록 대시보드를 제공합니다.



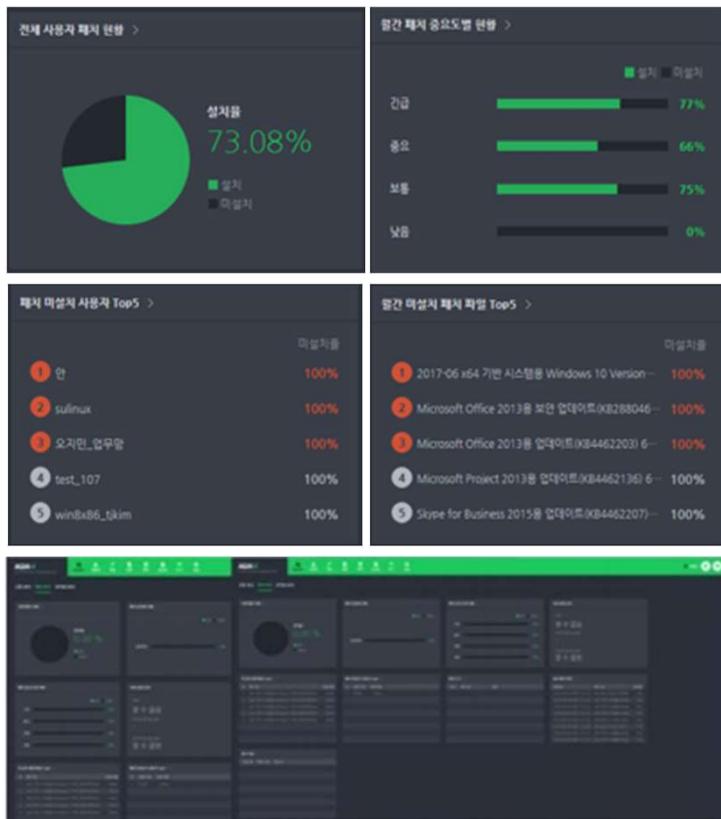
## 패치 관리

- 전체 사용자 패치 현황
- 패치 미설치 사용자 Top5
- 서버 상태 정보
- 월간 패치 종류별 현황
- 월간 패치 중요도별 현황
- 월간 미설치 패치 파일 Top5
- 패치 관리 로그
- 최신 패치 파일
- 대기 작업

# 주요 기능

## 관리자 > 직관적인 대시보드

- 이미지와 그래프를 통해 전체 패치 운용 현황을 한 눈에 파악 할 수 있도록 대시보드를 제공합니다.



### 01

#### 패치 운용 현황 확인하기

전체 사용자 패치 현황과 1 달내 발표된 패치들의 패치 종류 / 중요도별 설치 현황을 확인할 수 있습니다.

### 02

#### 패치 미설치 순위 확인하기

패치 미설치율이 높은 사용자와 1 달내 발표된 패치 파일의 미설치율 순위를 확인하여 조치할 수 있습니다.

### 03

#### 위젯 설정하기

전체 사이즈 변경에 맞추어 위젯의 정렬이 자동 변경되며, 위젯 항목을 설정할 수 있습니다.

# 주요 기능

## 관리자 > 사용자 별 패치 현황

- 전체 사용자의 기본 정보 및 패치 종류 별로 설치 현황 확인이 가능합니다.

ALYac Security Manager

ASM 5  
ALYAC SECURITY MANAGER

공통 관리  
사용자 현황  
백신 관리  
탐지 현황  
매체 사용 현황  
패치 관리  
위악점 관리  
위악점 현황

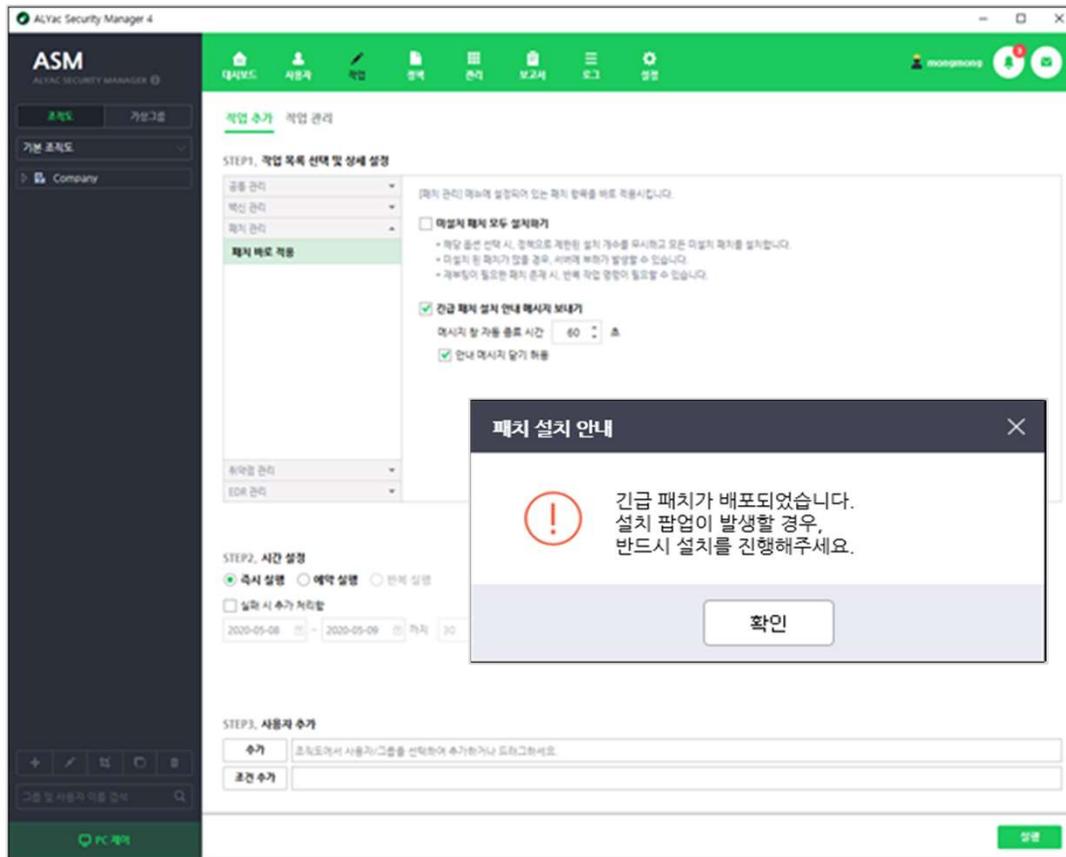
사용자 목록 3명

사용자명	부서명	패치 설치율	운영체제 설치율	MS Office 설치율	일반 SW 설치율	OS	최근 접속 일시	IP
<input type="checkbox"/>	이규원	EP컨설팅팀: 78%	33%	79%	100%	Windows 10 Enterprise 21H2	2022-04-11 오후 1:06:51	172.19.112.1
<input type="checkbox"/>	이원준	EP컨설팅팀: 79%	33%	79%	100%	Windows 10 Enterprise 21H2	2022-04-13 오후 5:26:31	172.21.240.1
<input type="checkbox"/>	최찬혁	EP기술지원팀: 0%	0%	100%	100%	Windows 10 Pro 1803	2022-04-11 오후 1:39:14	172.19.123.248

# 주요 기능

## 관리자 > 패치 적용/파일 배포

- 사용자/그룹에게 긴급 패치 및 패치 셋에 포함되지 않은 개별 파일의 배포가 가능합니다.



- 패치 바로 적용 선택한 사용자나 그룹에게 패치 적용 명령 가능

\*[미설치 패치 모두 설치] 체크시, 설치 갯수 제한없이 모든 미설치 패치 설치 가능

\*[긴급 패치 설치 안내 메시지 보내기] 가능  
(안내 메시지 닫기 허용 on/off)

- 파일 배포(공통 관리 기능) 선택한 파일이나 프로그램을 원하는 그룹/사용자에게 전송가능

# 주요 기능

## 관리자 > 패치 적용/파일 배포

- 사용자/그룹에게 긴급 패치 및 패치 셋에 포함되지 않은 개별 파일의 배포가 가능합니다.

### 01. 패치 즉시 적용하기

패치 적용이 실행될 시간 선택 후 조직도에서 명령을 내릴 사용자나 그룹을 추가하여 명령할 수 있으며, 조직도 우클릭 메뉴를 통한 즉시 명령도 가능합니다.

STEP1. 작업 목록 선택 및 상세 설정

공통 관리	[패치 관리] 메뉴에 설정되어 있는 패치 항목을 바로 적용시킵니다.
패치 관리	
<b>패치 바로 적용</b>	

STEP2. 시간 설정

즉시 실행    예약 실행    반복 실행

실패 시 추가 처리할

2016-05-12 - 2016-05-12 까지 30 분 간격으로 추가 실행

STEP3. 사용자 추가

추가	김준섭 x 조직도에서 사용자/그룹을 선택하여 추가하거나 드래그하세요.
조건 추가	

김준섭

- 업데이트
- 정책 바로 적용
- 원격 지원
- 메시지 전송
- 사용자 정보 가져오기
- 프로그램 배포
- 패치 관리** > **패치 바로 적용**
- 취약점 관리
- 수정
- 잘라내기
- 삭제

# 주요 기능

## 관리자 > 패치 적용/파일 배포

- 사용자/그룹에게 긴급 패치 및 패치 셋에 포함되지 않은 개별 파일의 배포가 가능합니다.

### 02. 작업 명령 결과 확인하기

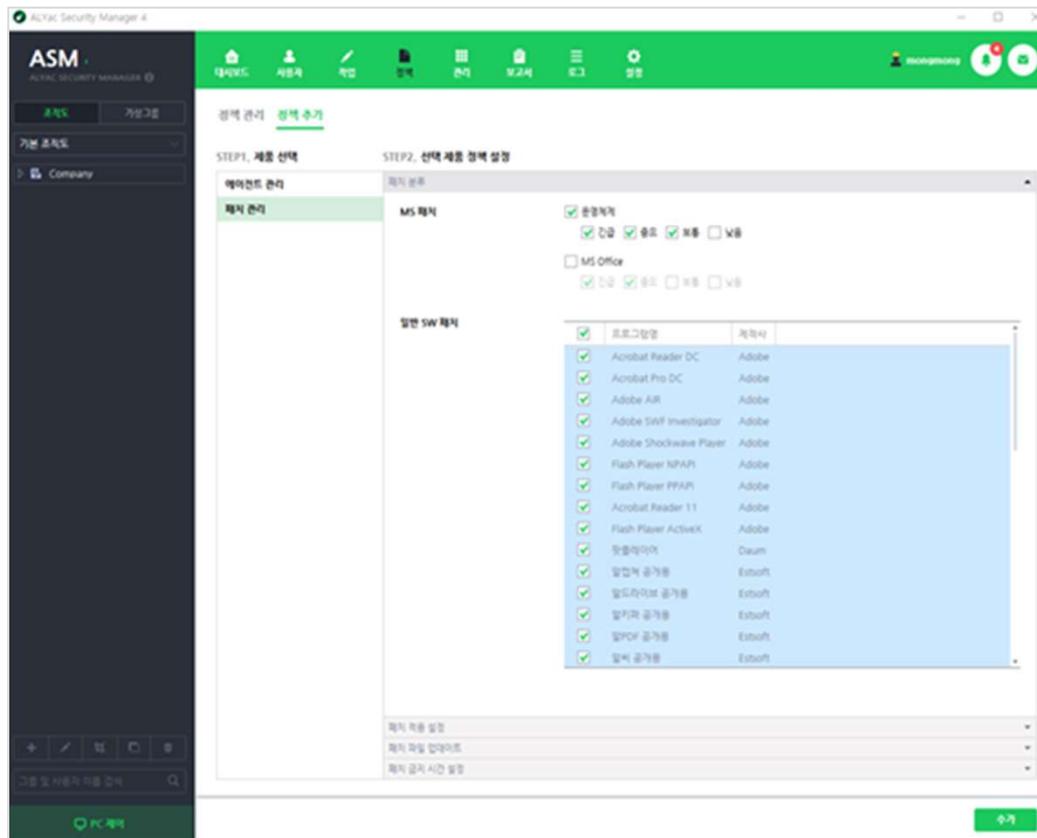
[작업 관리] 메뉴에서 명령한 작업의 진행 상황을 확인할 수 있습니다.

작업 관리					
대기 작업					
진행 중인 작업					
완료 작업					
<input type="checkbox"/>	작업 명	대상 수	성공	실패	작업 시간
<input type="checkbox"/>	업데이트	26	17	9	2016-05-03 9

# 주요 기능

## 관리자 > 배포 정책 설정

- 선택된 사용자나 그룹에게 적용될 패치 배포 정책을 설정하고 적용합니다.



## 패치 관리

- 적용 패치 분류 선택
- 패치 자동 적용 여부 설정
- 패치 파일 크기 제한
- 패치 대기일 적용
- 패치 재시도, 진행 개수 설정
- 업데이트 대기 시간 설정
- 패치 실행 최소 용량 설정
- 패치 금지 시간 설정

# 주요 기능

## 관리자 > 배포 정책 설정

- 선택된 사용자나 그룹에게 적용될 패치 배포 정책을 설정하고 적용합니다.

### 01. 정책 추가하기

정책 내용을 간편하게 추가하고 수정할 수 있으며, [상속 정책] 기능을 통해 기존 정책을 활용한 정책을 생성할 수 있습니다.

The image shows two parts of a software configuration interface. On the left is a form for creating a policy, and on the right is a detailed view of the product selection step.

**Left Panel (Policy Creation Form):**

- 정책명:** Policy Name input field.
- 설명:** Description input field.
- 상속 정책:** Inheritance Policy section with radio buttons for '사용 안함' (Not used) and '사용' (Used), and a dropdown menu.
- 정책 제품 선택:** Policy Product Selection section with checkboxes for '알약 패치 관리(PMS)' and '알약 내PC자키미'.

**Right Panel (STEP2. 선택 제품 정책 설정):**

- 패치 분류:** Patch Classification section with checkboxes for '운영체제' (OS) and 'MS Office'.
- 일반 SW 패치:** General Software Patch section with a table of software products.

일반 SW 패치	제품명	제조사
<input checked="" type="checkbox"/>	프로그램명	제조사
<input checked="" type="checkbox"/>	Acrobat Reader DC	Adobe
<input checked="" type="checkbox"/>	Adobe AIR	Adobe
<input checked="" type="checkbox"/>	Adobe Shockwave Player	Adobe
<input checked="" type="checkbox"/>	Acrobat Pro DC	Adobe
<input checked="" type="checkbox"/>	Adobe SWF Investigator	Adobe
<input checked="" type="checkbox"/>	Flash Player NPAPI	Adobe
<input checked="" type="checkbox"/>	Flash Player PPAPI	Adobe
<input checked="" type="checkbox"/>	Acrobat Reader 11	Adobe
<input checked="" type="checkbox"/>	Flash Player ActiveX	Adobe
<input checked="" type="checkbox"/>	팟플레이어	Daum
<input checked="" type="checkbox"/>	알집치 공개용	Estsoft
<input checked="" type="checkbox"/>	알드라이브 공개용	Estsoft
<input checked="" type="checkbox"/>	알키미 공개용	Estsoft
<input checked="" type="checkbox"/>	알PDF 공개용	Estsoft
<input checked="" type="checkbox"/>	알씨 공개용	Estsoft

# 주요 기능

## 관리자 > 배포 정책 설정

- 선택된 사용자나 그룹에게 적용될 패치 배포 정책을 설정하고 적용합니다.

### 02. 정책 적용하기

정책 추가 후 사용자나 그룹을 선택하여 간편하게 정책을 적용시킬 수 있으며 조직도 우클릭을 통한 정책 적용도 가능합니다.



# 주요 기능

## 관리자 > 패치 관리

- MS 패치(운영체제 및 MS-Office 패치)와 일반 SW 패치의 목록과 상태를 관리합니다.

### ※ MS 패치 목록

자산 관리 운영체제 관리 하드웨어 관리 소프트웨어 관리  백신 관리 수집 파일 관리 악성코드 관리 신고 내역 관리  패치 관리 <b>MS 패치 관리</b> 일반 SW 패치 관리	패치 파일 검색						
	분류 <input type="text"/> 운영체제 <input type="text"/>		검색 <input type="text"/>				
	패치 파일 목록						
	<input checked="" type="radio"/> 전체 <input type="radio"/> 적용 <input type="radio"/> 대기 <input type="radio"/> 롤백						
	<input type="checkbox"/>		분류	중요도	패치 대상/ID	패치명	우선 ?
	<input type="checkbox"/>	+	운영체제	긴급	KB4549947	2020-04x64 기반 시스템용 Windows 10 Version 1809에 대한 서비스 스택 업데이트(KB4549947)	일반
	<input type="checkbox"/>	+	운영체제	긴급	KB4549949	2020-04 x64 기반 시스템용 Windows 10 Version 1809에 대한 누적 업데이트(KB4549949)	일반
	<input type="checkbox"/>	+	운영체제	긴급	KB4549951	2020-04 x64 기반 시스템용 Windows 10 Version 1903에 대한 누적 업데이트(KB4549951)	일반
	<input type="checkbox"/>	+	운영체제	긴급	KB4549951	2020-04 x64 기반 시스템용 Windows 10 Version 1909에 대한 누적 업데이트(KB4549951)	일반
	<input type="checkbox"/>	+	MS Office	중요	KB4484258	Microsoft Office 2016용 보안 업데이트(KB4484258) 64비트 버전	일반
<input type="checkbox"/>	+	MS Office	중요	KB4464544	Microsoft Visio 2013용 보안 업데이트(KB4464544) 64비트 버전	일반	

### ※ 일반 SW 패치 목록

백신 관리 수집 파일 관리 악성코드 관리 신고 내역 관리  패치 관리 MS 패치 관리 <b>일반 SW 패치 관리</b>	패치 파일 목록						
	<input checked="" type="radio"/> 전체 <input type="radio"/> 적용 <input type="radio"/> 대기						
	<input type="checkbox"/>	패치 대상/ID	패치명	상태 ?	대기일	설치율	발표일
	<input type="checkbox"/>	Chrome	Chrome_x64_ko(80.0.3987.163)	적용 <input type="text"/>	3	100%	2020-04-02
	<input type="checkbox"/>	알집 공개용	알집 공개용_ko(11.7.0.2)	적용 <input type="text"/>	3	100%	2020-04-02
	<input type="checkbox"/>	Acrobat Reader DC	Acrobat Reader DC(20.6.20042)	적용 <input type="text"/>	3	100%	2020-03-18
	<input type="checkbox"/>	Flash Player PPAPI	Flash Player PPAPI_ko(32.0.0.344)	적용 <input type="text"/>	3	100%	2020-03-12
	<input type="checkbox"/>	알송 공개용	알송 공개용_ko(3.47.0.6)	적용 <input type="text"/>	3	100%	2020-03-05

# 주요 기능

## 관리자 > 패치 관리

- MS 패치(운영체제 및 MS-Office 패치)와 일반 SW 패치의 목록과 상태를 관리합니다.

### 패치 설치율 확인하기

패치 파일별 설치율을 확인할 수 있으며, 항목 클릭 시 해당 패치가 적용된 사용자나 그룹의 상세 설치 현황을 확인할 수 있습니다.

분류	중요도	패치 번호	패치 명	상태	대기일	설치율	재부팅
+ 운영체제	중요	2487367	Windows XP, Windows Server 2003, Wind	적용	3	0%	필요
+ 운영체제	중요	2737083	Windows 7, Windows Vista 및 Windows Sr	적용	3	0%	필요
+ 운영체제	보통	2719033	Windows 7용 보안 업데이트(KB2719033)	적용	3	0%	필요

ASM4

2018-06 x64 기반 시스템용 Windows 10 Version 1803에 대한 누적 업데이트(KB4284835)

사용자명: [ ]

사용자명	부서명	IP	설치 여부
+ 7 86 jmk	ESTsecurity:Endpoint개발부문:알약개발팀:	192.168.190.198	설치
+ 각지훈	ESTsecurity:Endpoint개발부문:PMS개발팀:	192.168.190.99	미설치
+ 구기석	ESTsecurity:Endpoint개발부문:플랫폼개발팀:	192.168.190.10	설치
+ 김명선2	ESTsecurity:	192.168.190.86	설치
+ 김선숙	ESTsecurity:코어개발팀:	192.168.190.28	설치
+ 박종혁	ESTsecurity:Endpoint개발부문:플랫폼개발팀:	192.168.190.100	설치

### 패치 상태 변경하기

패치의 상태와 대기일 설정을 간단하게 변경할 수 있습니다. (대기일은 패치 상태가 [대기] 일때만 변경 가능합니다.)

분류	중요도	패치 번호	패치 명	상태	대기일	설치율	재부팅	발표일
+ 운영체제	중요	2487367	Windows XP, Windows Server 2003, Wind	적용	3	0%	필요	20160429
+ 운영체제	중요	2737083	Windows 7, Windows Vista 및 Windows Sr	적용	3	0%	필요	20160429
+ 운영체제	보통	2719033	Windows 7용 보안 업데이트(KB2719033)	대기	3	0%	필요	20160429
+ 운영체제	중요	2736422	x64 기반 시스템용 Windows 7 및 Windows	대기	3	0%	필요	20160429

# 주요 기능

## 관리자 > 패치 관리

- MS 패치(운영체제 및 MS-Office 패치)와 일반 SW 패치의 목록과 상태를 관리합니다.

### 패치 우선 순위 설정하기

패치 파일별 우선순위를 설정할 수 있으며, 우선 적용 칼럼에서 [우선] 선택 시, 일반 패치보다 우선적으로 설치됩니다.

	우선 적용	상태 ?	대기일	설치율	재부팅	발표일
용 Windows 10 Version 1809의 Adobe Flash Player 보안 업데이트(KB4493478)	일반 <input checked="" type="checkbox"/>	적용 <input type="checkbox"/>	3 <input type="checkbox"/>	50%	필요	2019-04-09
용 Windows 10 Version 1803의 Adobe Flash Player 보안 업데이트(KB4493478)	일반 <input type="checkbox"/>	적용 <input type="checkbox"/>	3 <input type="checkbox"/>	75%	필요	2019-04-09
용 Windows 7용 Internet Explorer 11 누적 보안 업데이트(KB4493435)	우선 <input type="checkbox"/>	적용 <input type="checkbox"/>	3 <input type="checkbox"/>	50%	필요	2019-04-09
용 Windows 10 Version 1803에 대한 누적 업데이트(KB4493464)	일반 <input type="checkbox"/>	적용 <input type="checkbox"/>	3 <input type="checkbox"/>	50%	필요	2019-04-09
용 Windows 10 Version 1809에 대한 누적 업데이트(KB4493509)	일반 <input type="checkbox"/>	적용 <input type="checkbox"/>	3 <input type="checkbox"/>	100%	필요	2019-04-09

# 주요 기능

## 관리자 > 보고서

- 에이전트 별, 패치 종류별로 다양한 형태의 통계 보고서를 제작 합니다.

### 패치 통계 확인하기

에이전트 별 또는 패치 별로 통계 보고서를 제작하고 엑셀 파일로 생성합니다.

자산 관리

운영체제 통계

소프트웨어 통계

제품별 미설치자 통계

백신 관리

백신 설치 통계

악성코드 탐지 통계

악성코드 종류별 탐지 통계

악성코드 Top 10

악성코드 탐지자 Top 10

패치 관리

에이전트별 패치 통계

패치 종류별 통계

위약점 관리

위약점 진단 통계

위약점 종류별 통계

에이전트별 위약점 통계

기간별 위약점 통계

기간 내 발표된 패치 종류별로 적용 현황을 확인할 수 있습니다.

**기간 설정**

기간 설정 사용 안 함

1주  1개월  3개월  6개월  1년  직접 지정

2019-03-29 ~ 2019-04-29

**표시 단위**

일

**옵션 설정**

패치 분류:  전체  
 운영체제  MS Office  
 일반 SW

패치 중요도:  긴급  중요  보통  낮음  
\* 일반SW는 중요도를 구분하지 않습니다.

설치율: 60%  이상  이하

**보고서 저장하기**

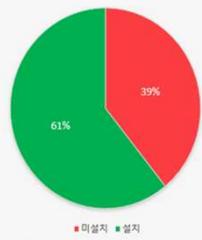
Excel

**에이전트 패치 통계**

에이전트 별로 적용된 패치 현황과 결과를 확인할 수 있습니다.

\* 기간 : 전체      생성 일시 : 2019-04-24 16:45

\* 대상/전체 : Company (24/25개)



사용자 명	연류타	부서 명	설치
안	DESKTOP-NAH1M7B		-
김희선_PC2	DESKTOP-KFAHMIDA	ESTsecurityEndpoint개발부문.실약개발과목,	6
이병찬	LEEC-PC	ESTsecurityEndpoint개발부문.품질개발팀.리눅스개발과목,	59

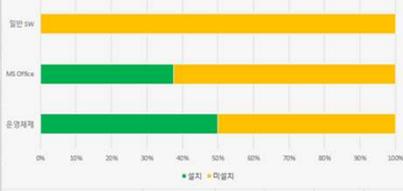
**패치 종류별 통계**

기간 내 발표된 패치 종류별로 패치 적용 현황을 확인할 수 있습니다.

\* 기간 : 2019-03-24 ~ 2019-04-24      생성 일시 : 2019-04-24 16:45

\* 대상/전체 : Company (24/25개)

\* 패치 수 : 127



패치명	종류	중요도	설치	미설치	설치율
2019-04-23 16:41:12 [24] Windows 7 Internet Explorer 11 누적 보안 업데이트 (KB4495472)	운영체제	긴급	1	1	50%
2019-04-23 16:41:12 [24] Windows 7에 대한 보안 취약점 공지 (MS19-047)에 대한 보안 패치 (KB4495472)	운영체제	긴급	1	1	50%
2019-04-23 16:41:12 [24] Windows 7에 대한 보안 취약점 공지 (MS19-047)에 대한 보안 패치 (KB4495472)	운영체제	긴급	1	1	50%

# 주요 기능

## 관리자 > 패치 상태 로그

- 패치의 상태 변경, 에이전트 별로 설치된 내역 등에 대한 로그를 확인합니다.

### 패치 상태 로그 확인

패치 별로 상태가 변경된 내역을 표시하고 분류에 따라 특정 로그를 검색-조회 합니다.

공통 관리 서버 로그 관리자 로그 수행 로그 파일 유효성 에이전트 로그  백신 관리 탐지 로그 검사 로그 랜섬웨어 차단 로그 행위 차단 로그 매체 사용 로그  패치 관리 패치 상태 로그 패치 설치 로그	분류	전체	2020-04-08	~	2020-05-08	검색
	일시	패치명	분류	패치 대상/ID	상태	
	2020-05-08 오후 12:59:46	2020-04 x64 기반 시스템용 Windows 10 Version 1909에 대한 누적 업데이트	운영체제	KB4549951	우선 적용 변경[일반]	
	2020-05-08 오후 12:59:42	Microsoft Office 2013용 보안 업데이트(KB4484229) 64비트 버전	MS Office	KB4484229	우선 적용 변경[일반]	
	2020-05-08 오후 12:59:35	Microsoft Office 2013용 보안 업데이트(KB4484229) 64비트 버전	MS Office	KB4484229	우선 적용 변경[우선]	
	2020-05-08 오후 12:59:25	2020-04 x64 기반 시스템용 Windows 10 Version 1909에 대한 누적 업데이트	운영체제	KB4549951	우선 적용 변경[우선]	

# 주요 기능

## 관리자 > 패치 설치 로그

- 패치의 상태 변경, 에이전트 별로 설치된 내역 등에 대한 로그를 확인합니다.

### 패치 설치 로그

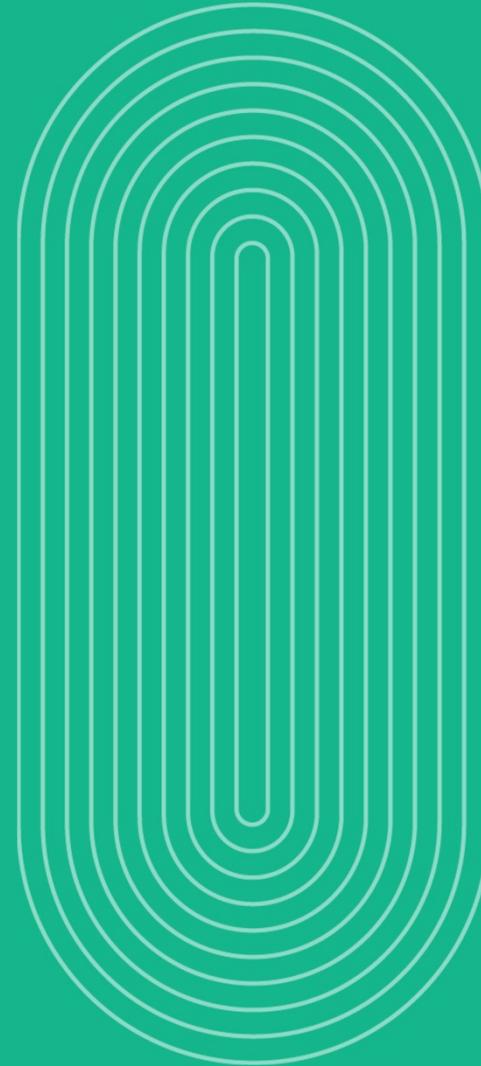
사용자 별로 패치가 설치된 내역을 로그로 확인하고 조건에 따라 조회-검색합니다.

공통 관리 서버 로그 관리자 로그 수행 로그 파일 유효성 에이전트 로그  백신 관리 탐지 로그 검사 로그 랜섬웨어 차단 로그 행위 차단 로그 매체 사용 로그  패치 관리 패치 상태 로그 패치 설치 로그	사용자명			2020-04-08	2020-05-08	검색		
	일시	사용자명	IP	제품	상태	패치 대상/ID	파일명	내용
	2020-05-07 오후	정민 1064	192.168.190.199	PMS	설치 성공	KB4537572	windows10.0-kb4537572-x64...	패치 설치 완료
	2020-05-07 오후	정민 1064	192.168.190.199	PMS	설치 성공	KB4549951	windows10.0-kb4549951-x64...	패치 설치 완료
	2020-05-07 오후	정민 1064	192.168.190.199	PMS	설치 성공	Chrome	ChromeStandaloneSetup64_8...	패치 설치 완료
	2020-04-22 오후	김순민	192.168.190.91	PMS	설치 성공	알캡처 공개용	ALCapture268.exe	패치 설치 완료
	2020-04-22 오후	김정민	192.168.190.199	PMS	설치 진행	KB4537572	windows10.0-kb4537572-x64...	패치 설치 진행 중
	2020-04-22 오후	김정민	192.168.190.199	PMS	설치 성공	KB4549951	windows10.0-kb4549951-x64...	패치 설치 완료
	2020-04-22 오후	김정민	192.168.190.199	PMS	설치 성공	Chrome	ChromeStandaloneSetup_80.0...	패치 설치 완료
	2020-04-22 오전	최근용	192.168.190.77	PMS	패치 삭제	Java 8	jre-8u241-windows-i586.exe	설치된 패치 수동 삭제
	2020-04-22 오전	김순민	192.168.190.91	PMS	설치 진행	KB4538156	windows10.0-kb4537490-x64...	패치 설치 진행 중
	2020-04-22 오전	김순민	192.168.190.91	PMS	설치 실패	알캡처 공개용	ALCapture268.exe	확인 불가 오류
	2020-04-22 오전	김순민	192.168.190.91	PMS	설치 실패	KB4538156	windows10.0-kb4537490-x64...	확인 불가 오류
	2020-04-20 오후	김순민	192.168.190.91	PMS	설치 실패	알캡처 공개용	ALCapture268.exe	확인 불가 오류
	2020-04-20 오후	김순민	192.168.190.91	PMS	설치 실패	알캡처 공개용	ALCapture268.exe	확인 불가 오류

03

# 고객 지원

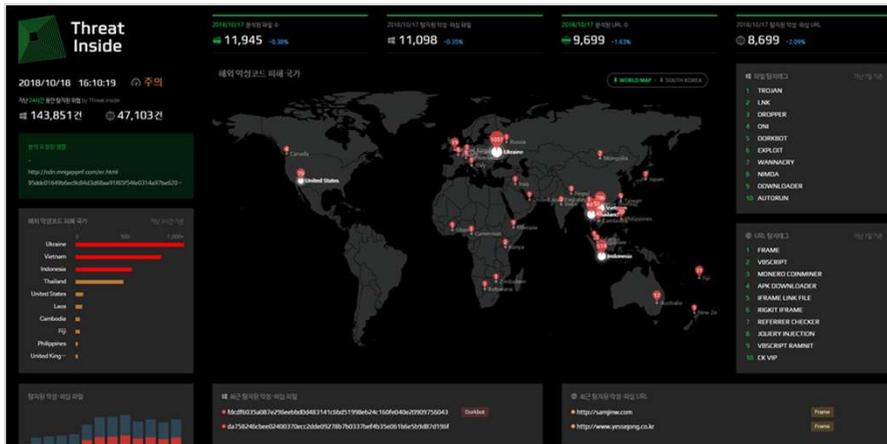
- 이스트시큐리티 대응 센터
- 고객지원 서비스
- 구성 및 운용



# ESRC

## 이스트시큐리티 대응센터 ESRC

국내 보안 사고는 주로 국내 사정을 잘 알고 있는 집단이 조직적이고 계획적으로 진행하여 이뤄졌습니다.  
 국내 최고 전문가들로 구성된 이스트시큐리티 대응센터(ESRC)는 정부 주요 기관들과 연계한 **상시 대응 체계**를 유지하여,  
**국내에 특화된** APT 공격과 랜섬웨어 등 각종 위협에 **가장 빠르게 대응**하고 있습니다.



+



+



## 고객지원 서비스

### 지원 센터

#### 시큐리티 대응센터

실시간 모니터링 체계를 구축하여 국가기관과 연계한 상시 대응 체계를 유지하고 있습니다. DDos, 해킹, 랜섬웨어 등 긴급상황 발생 시 고객사를 포함한 민간의 피해를 최소화하고자 하며, 전용 백신 개발 및 배포를 통해 위기 상황에 신속하게 대응하고 있습니다.

#### 기술 지원 센터

기업 고객들을 위한 전문 기술 지원 센터를 운영하고 있습니다. 기술지원 요청 시, 원격 지원은 물론 방문 지원 서비스 등 특화된 지원 서비스를 기업 고객들께 제공하며, 기술지원 핫라인을 24시간 운영하여 빈틈없는 보안 서비스를 제공하고 있습니다.

### 지원 시스템

#### 오류 보고 시스템

알약과 ASM은 오류 발생 시 이를 자동으로 신고하여 가장 빠르게 조치 받을 수 있는 시스템을 지원합니다. 오류 보고 시스템을 통해 관리자는 장애 상황 발생 시 신속한 선조치 및 긴급 복구 서비스를 제공받게 됩니다.

#### 장애 모니터링 시스템

전문 보안 기술 인력들이 기업용 모니터링 시스템을 통해 고객사의 알약 및 ASM 동작 상태를 24시간 체크합니다. 모니터링 시스템을 통해 관리자가 인지하기 전에 장애 조치를 제공받고 조치 결과를 안내 받을 수 있습니다.

## 고객지원 서비스

전문 기술 인력이 체계적이고 신속한 고객 지원 서비스를 제공합니다.

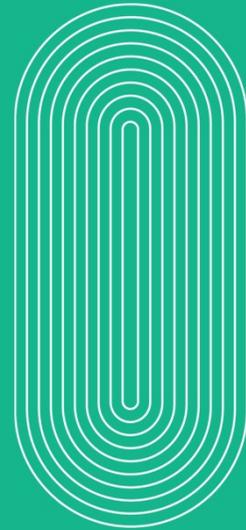
 신고하기/ e-mail 상담 (2시간 이내 회신)	 전문 기술 인력의 전화 상담	 야간 및 공휴일, 주간 핫라인 운영
 PC 원격지원 서비스	 대규모 사이트 전담 인력 배정 및 정기 방문 점검 서비스 제공	 제품 교육 서비스 제공

- 구매문의 : 02-3470-2970
- 고객센터 : 1544-9744
- 홈페이지 : <https://www.estsecurity.com/enterprise/product/alyac-enterprise>

# 구성 및 운영

## 시스템 구성





## 알약 패치관리(PMS) 2.1

**EST**SECURITY

문의처 TEL : 02-583-4616 홈페이지 : [www.estsecurity.com](http://www.estsecurity.com)