

윈도우 수명 주기 관리를 통한 PC 보안 강화 전략



CONTENTS

- I** Windows를 완벽하게 사용하는 방법
- II** Windows 수명 주기 관리의 중요성
- III** Windows 수명 주기 관리 현황
- IV** 수명 주기에 기반한 PC보안 강화 방안
- V** 자동화를 통한 Windows 수명 주기 관리 사례

Windows를 완벽하게 사용하는 방법

1. Windows 10/11에 대해 알아야할 4가지
2. 서비스형 윈도우(WaaS)로 제공
3. Windows 버전 도입
4. 일반공급채널 서비스로 변화
5. Windows 10/11 수명 주기 정책

1 Windows 10/11에 대해 알아야할 4가지

서비스형 윈도우(WaaS)로 제공

Microsoft는 몇 년마다 새 버전의 Windows를 출시했습니다. 이 것은 새 기능의 출시를 지연시켰고 운영체제의 상당한 변경으로 인해 배포 시 상당한 문제를 야기시켰습니다. 이런 문제를 해결하고 최신 상태로의 유지를 위해 서비스 모델을 채택하였습니다.

Windows 버전 도입

Windows 10 부터는 ‘버전’ 개념을 도입하여 새로운 버전의 윈도우 출시 대신 버전 업그레이드를 지속하고 있습니다. 각 버전은 수명주기 정책에 의해 관리됩니다.

Windows 10/11에 대해 IT담당자가 알아야할 4가지

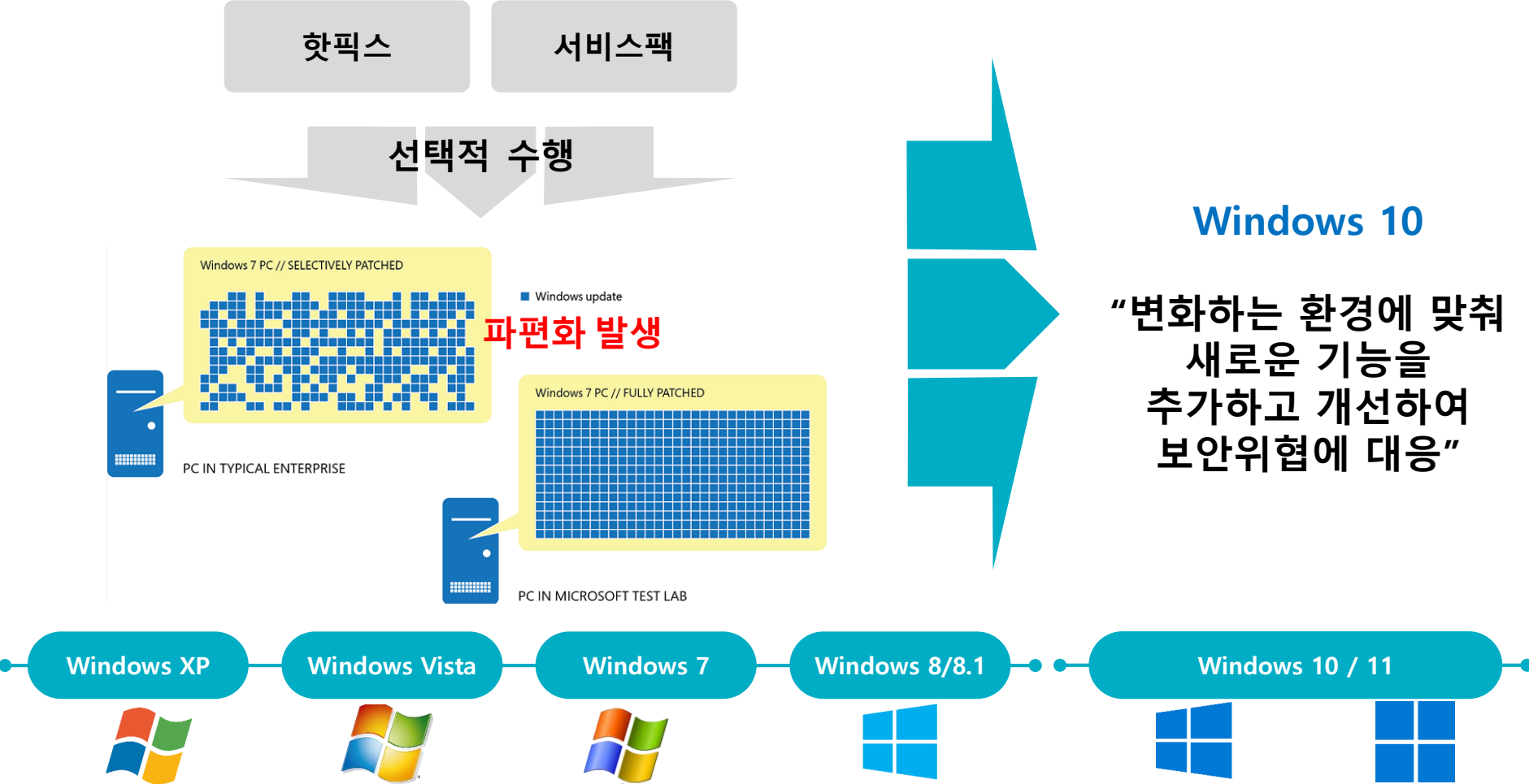
일반공급채널 서비스로 변화

Windows 10 버전 21H2부터 1년에 한번 새로운 기능 및 업데이트를 포함하는 신규 버전을 출시합니다.

Windows 10/11 수명 주기 정책

Windows 10의 수명 주기 정책은 릴리즈 날짜로부터 18개월, Windows 11의 수명 주기 정책은 릴리즈 날짜로부터 24개월 동안 매월 품질 업데이트를 제공받습니다.

2 서비스형 윈도우(WaaS)로 제공





3 Windows 버전 도입

주기적으로 Windows 10 버전을 관리하여 보안위협에 대비

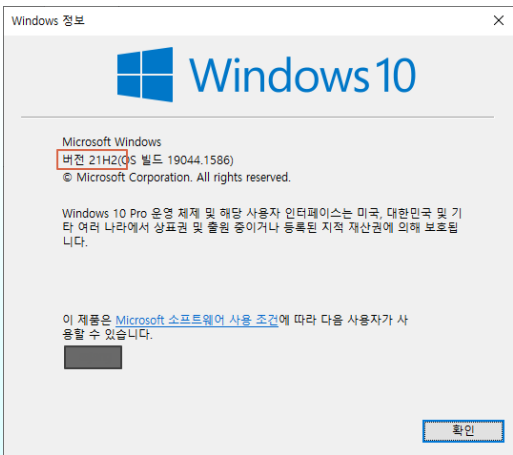
Windows 10 버전 확인 방법

- 방법
01

❶ 시작  > 설정  을 선택합니다.

❷ 설정에서 시스템 > 정보를 선택합니다.
- 방법
02

❶ 좌측 하단의 검색창에 “winver” 명령어를 입력합니다.



Windows 10 버전 표기법

[2020년 상반기까지 표기]

2004

출시년도	출시시점 (3월/9월)
버전	

[2020년 하반기부터 표기]

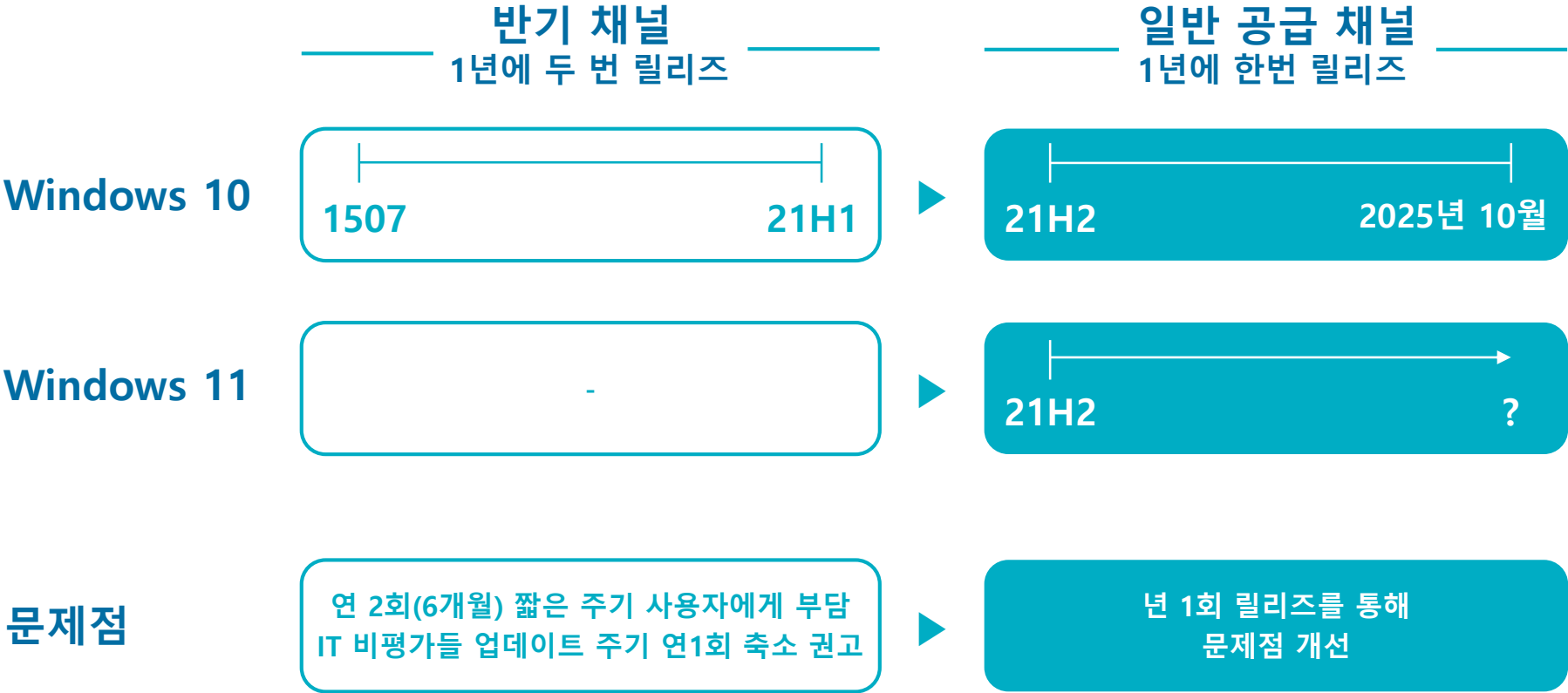
20H2

출시년도	출시시점 (상/하반기)
버전	

4

일반공급채널 서비스로 변화

새 버전 1년 단위 릴리즈 통해 사용자의 즉각적인 업그레이드 유도

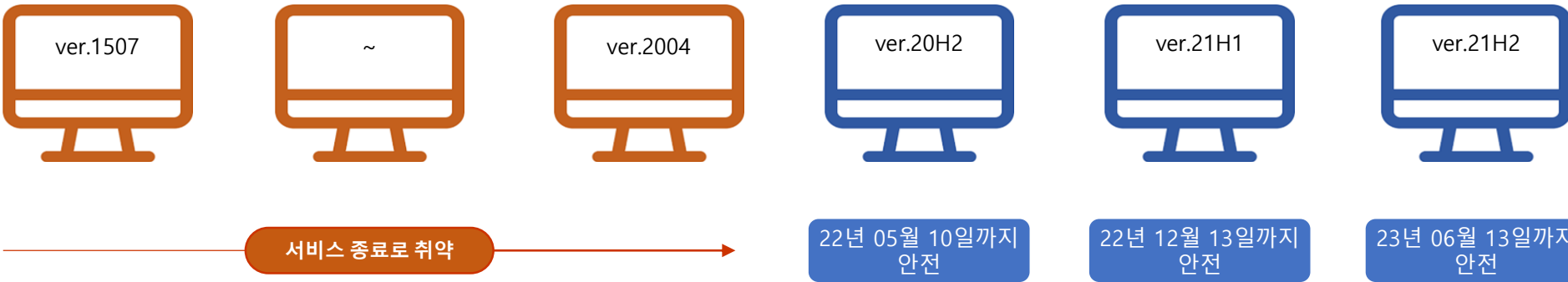


5 Windows 10/11 수명 주기 정책

MS의 지속적인 지원을 받으려면 현재 버전 서비스 종료 전 항상 최신 버전 설치 필요

구분	Windows 10 Pro	Windows 11 Pro
서비스 타임라인(연 1회 릴리즈)	출시일로부터 18개월	출시일로부터 24개월

현재 Windows 10의 안전한 버전은?



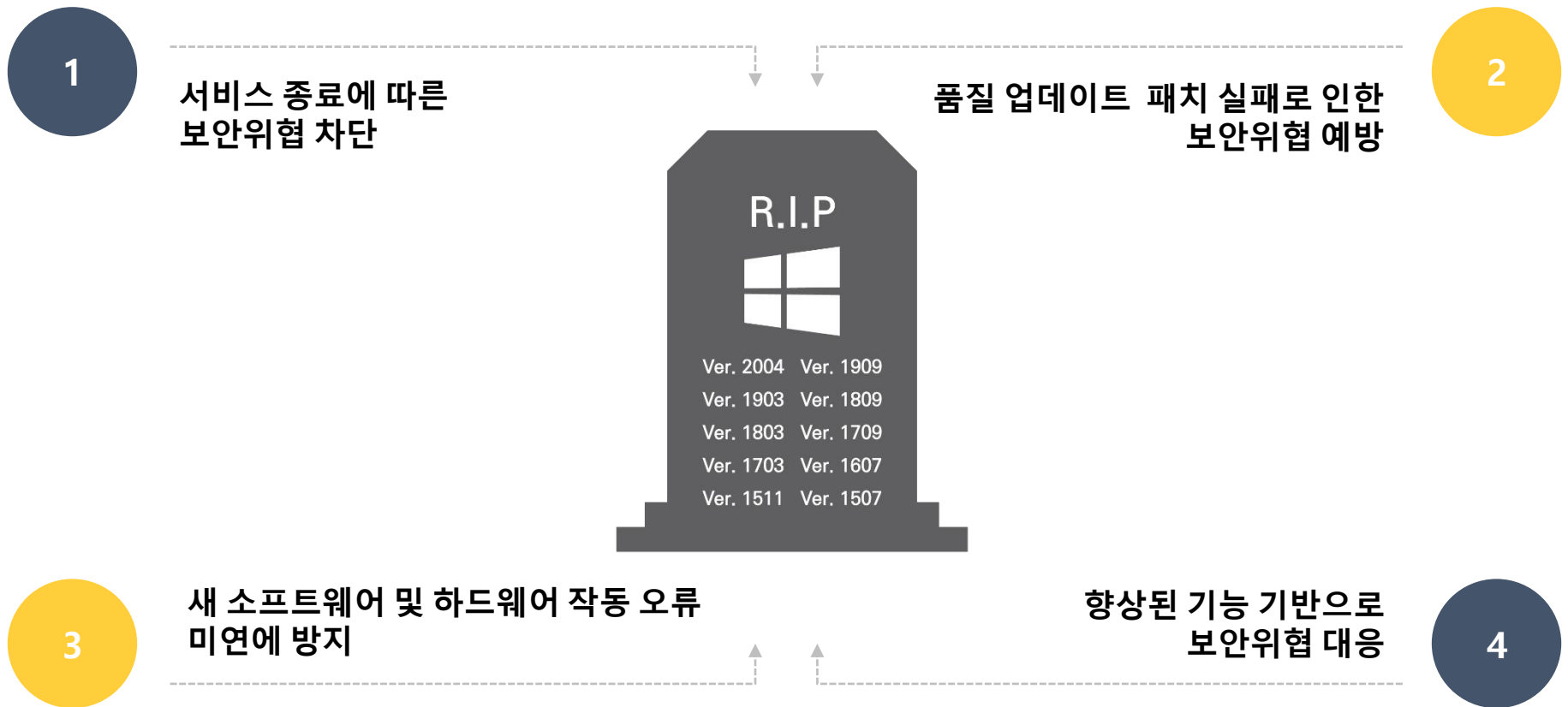
서비스 타임라인에 의해서 Windows 10 Pro 기준 안전한 버전은 20H2, 21H1, 21H2 입니다.
하지만, 20H2 버전은 다음달에 서비스가 종료되므로 빠른 업그레이드가 필요합니다.

Windows 수명 주기 관리의 중요성

1. Windows 수명 주긴 관리가 필요한 이유
2. 서비스 종료에 따른 보안위협 차단
3. 품질 업데이트 패치 실패로 인한 보안위협 예방
4. 새 프로그램 및 하드웨어 작동 오류 미연에 방지
5. 향상된 기능 기반의 보안위협 대응

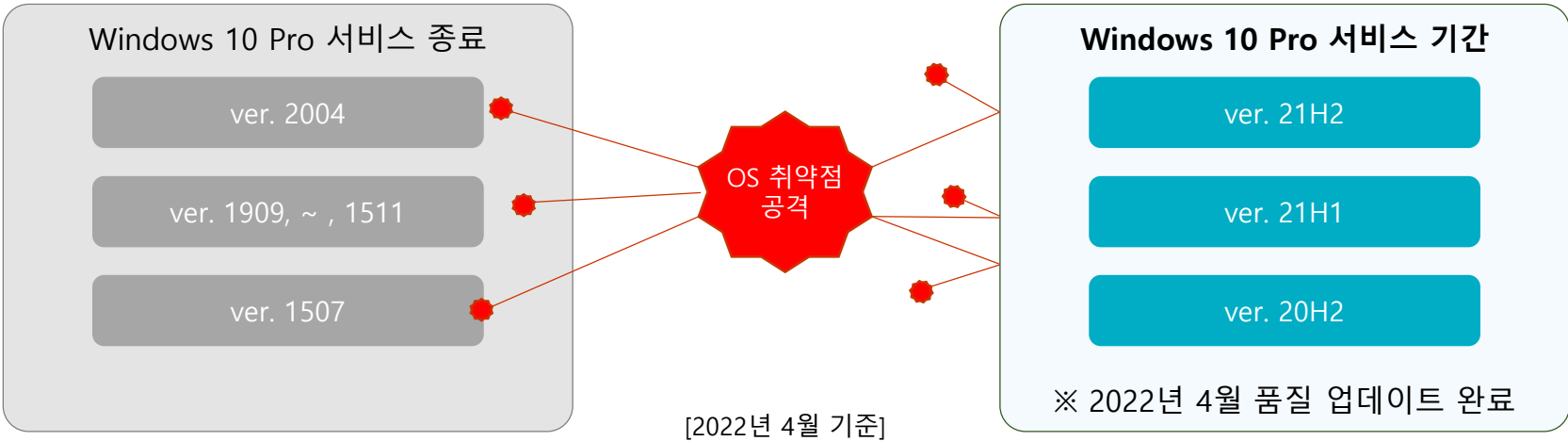
1 Windows 수명 주기 관리가 필요한 이유

서비스가 종료된 Windows 운영체제 환경의 경우 심각한 보안 위협에 노출 될 수 있습니다.
지원 종료 전에 최신 버전의 운영체제로 업그레이드하는 것을 권장합니다.



2 서비스 종료에 따른 보안위협 차단

수명 주기가 종료된 OS는 여전히 사용할 수 있습니다.
단, OS 지원(서비스)이 종료되면 더 이상 보안 업데이트를 받을 수 없기에 보안위협으로 부터 안전할 수 없습니다.
관리의 효율성 및 안정성을 위해서는 서비스 종료 전 윈도우 최신 버전으로 업그레이드가 필요합니다.



3 품질 업데이트 패치 실패로 인한 보안위협 예방

디바이스 또는 운영상의 문제로 인하여 버전에 따라 매월 발표되는 품질 업데이트가 정상적으로 패치되지 않은 경우 보안위협으로 부터 안전할 수 없습니다.

하지만, 정기적 릴리즈(상반기/하반기)에 맞춰 업그레이드 진행 시 이전 품질 업데이트를 포함하고 있기에 보안위협으로 부터 좀 더 안전할 수 있습니다.

4 새 프로그램 및 하드웨어 작동 오류 미연에 방지

이전 OS에 최근 출시된 프로그램 설치 또는 하드웨어 장착 시 작동하지 않을 가능성이 높습니다. 이는 새로운 하드웨어 및 소프트웨어 제조업체가 최신 운영 체제의 향상된 기능에 적합하도록 설계하기 때문입니다. 또는 제조업체가 이전 운영 체제에서 제품 지원을 중단하는 것이 적절하다고 결정할 수도 있습니다.

5

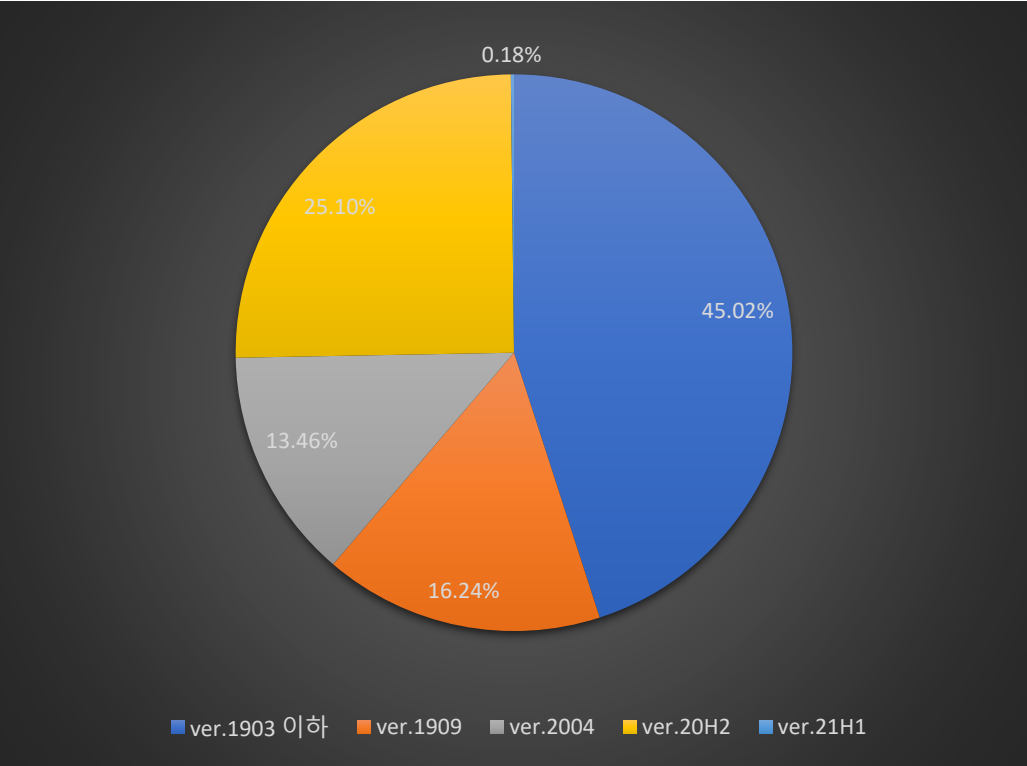
향상된 기능 기반의 보안위협 대응

버전	보안기능	비 보안기능
21H2	<ul style="list-style-type: none">Wi-Fi WPA3-Personal H2E 지원	<ul style="list-style-type: none">GPU 컴퓨팅에 대한 Linux용 Windows 하위 시스템최신 CSP 다운로드Azure Virtual Desktop을 사용하여 앱이 로컬로 표시
21H1	<ul style="list-style-type: none">WDAG(Windows Defender Application Guard : 정의한 신뢰할 수 없는 사이트를 격리하여 인터넷을 검색하는 동안에 보호할 기업을 보호함) 성능 향상WMI(Windows Management Instrumentation) 서비스는 보안 설정이 WMI 네임스페이스 권한에 적용될 때마다 힙 누출 현상 해결	<ul style="list-style-type: none">Chromium 기반의 새로운 Microsoft Edge 브라우저 제공시작할 때 중지 오류 해결
20H2	<ul style="list-style-type: none">Microsoft Defender ATP(Advanced Threat Protection) 자동 IR(인시던트 응답)에 대한 향상된 비 ASCII 파일 경로 지원Office용 Microsoft Defender Application Guard를 사용하여 격리된 컨테이너에서 신뢰할 수 없는 Office 문서를 실행하여 잠재적 악성 콘텐츠가 장치를 손상시키지 못하도록 방지	<ul style="list-style-type: none">Windows 10 사용자 인터페이스 기능 향상
2004	<ul style="list-style-type: none">Windows Defender System Guard를 사용하여 펌웨어 보호기능 제공Wi-Fi 6 및 WPA3를 사용하여 최신 Wi-Fi 표준을 지원. Wi-Fi 6을 사용하여 무선 커버리지 및 성능을 높이고 보안을 강화. WPA3는 향상된 Wi-Fi 보안을 제공하고 열린 네트워크를 안전하게 보호	<ul style="list-style-type: none">Windows 설치 관련 기능 개선EAP(확장할 수 있는 터널 인증 프로토콜)을 인증 방법으로 추가하여 여러 자격 증명을 단일 EAP 트랜잭션으로 연결. TEAP 네트워크는 엔터프라이즈 정책으로 구성샌드박스 버그 수정(샌드박스는 디바이스에 미치는 지속적인 영향을 걱정할 필요 없이 소프트웨어를 설치할 수 있는 격리된 데스크톱 환경으로 버전 1903에서 릴리스 되었음)
1909	<ul style="list-style-type: none">ARM64 디바이스에 Windows Defender Credential Guard통해 배포하는 기업의 자격 증명 도난에 대해 추가적인 보호TLS(전송 계층 보안) 1.3버전 실험적 제공	<ul style="list-style-type: none">Windows 프로세서 요구사항 업데이트 Windows 프로세서 요구 사항 Microsoft Docs운영 체제 및 응용 프로그램의 성능과 안정성을 높이기 위해 CPU에서 명령을 처리하는 방법 최적화특정 프로세서를 사용하는 PC에 대한 일반 배터리 사용 시간 및 전원 효율성 개

Windows 수명 주기 관리 현황

1. ComVoy 고객사 Windows 버전 현황
2. Windows 버전에 따른 보안 상태
3. 취약의 의미

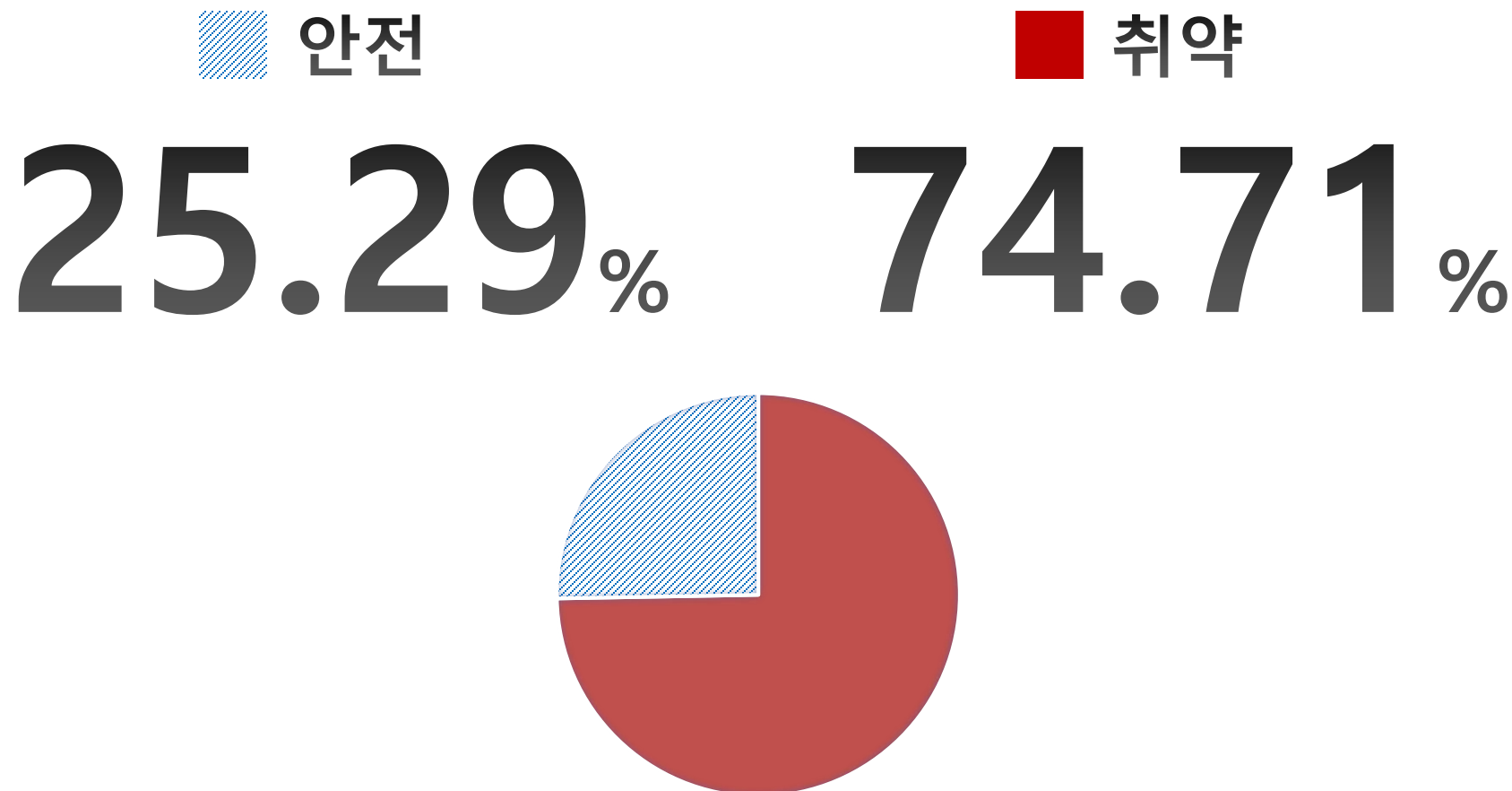
1 ComVoy 고객사 Windows 버전 현황



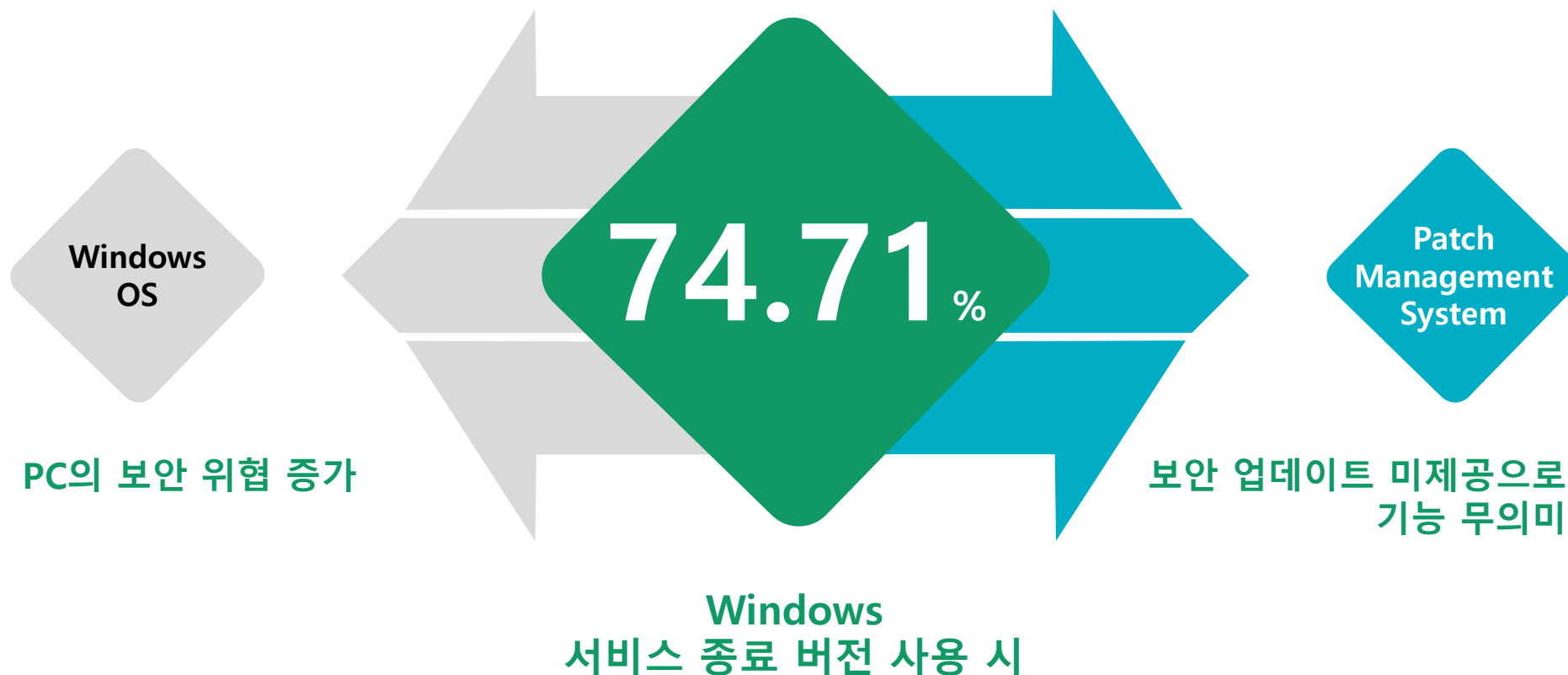
※ 2022년 3월 ComVoy 고객사 대상 기준

ver.1903이하	ver.1909	ver.2004	ver.20H2	ver.21H1
45.02%	16.24%	13.46%	25.10%	0.18%

2 Windows 버전에 따른 보안 상태



3 취약의 의미

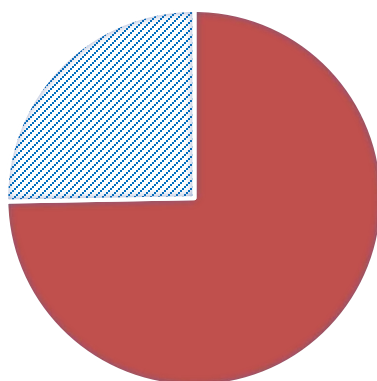


귀 기관의 취약한 PC는 몇% ?

74.71%

?%

■ 취약 ■ 안전



수명 주기에 기반한 PC보안 강화방안

1. Windows 최신 버전으로 업그레이드하기 위한 절차
2. Discover : 정보 수집
3. Assess : 상태 진단
4. Target : 대상 선정
5. Upgrade : 업그레이드

1 Windows 최신 버전으로 업그레이드하기 위한 절차



2 Discover : 정보 수집

어떤 H/W 및 S/W를 기반으로 운영 중인가?

Windows 정보 수집

- 유형 : Windows 에디션(Pro, Enterprise)
- 정보 : 버전

Windows 업데이트 정보 수집

- 유형 : 최신 보안 업데이트
- 정보 : 설치 유무

소프트웨어 정보 수집

- 유형 : 보안소프트웨어, 일반소프트웨어
- 정보 : 소프트웨어명, 상세버전, 공급자명, 소프트웨어ID

시스템 사양 수집

- 유형 : 하드웨어 정보
- 정보 : HDD(사용가능공간), RAM, CPU, Direct X

3 Assess : 상태 진단

어떤 용도로 운영 중인가?

유형

크리티컬 시스템
비즈니스 시스템
개발 시스템
폐기

복잡도 & 위험도

상, 중, 하
(보안 S/W설치,
별도 개발된 S/W 등)

4 Target : 대상 선정

수집된 정보를 기반으로 업그레이드 대상 분류



5 Upgrade : 업그레이드

호환성 검증을 위한 파일럿 진행

1단계

파일럿 대상 추출

시스템 사양
및
운영 소프트웨어
상이한 조건으로 추출

2단계

자원요구사항 검토

H/W, S/W
최소 요구사항
적합도 분석
및
필요 업데이트 패치여부

3단계

업그레이드 진행

현재 운영중인 상태로
업그레이드 진행

4단계

문제점 파악 및 전사 적용

기존 OS설정 값 유지
및 SW 동작 여부
확인

자동화를 통한 Windows 수명 주기 관리 사례

1. 자동화 업그레이드 사례1
2. 자동화 업그레이드 사례2
3. 자동화 업그레이드 사례3
4. 국방 POC 사례
5. Windows 업그레이드 주기관리 솔루션의 요건

1 자동화 업그레이드 사례1

2020년 외부망 도입 경험으로 2021년 내부망 도입

개요

- 업그레이드 기간
2021년 4월 ~ 5월
- 업그레이드 대상
4,500 PC
- 업그레이드 버전
ver 1709, ver 1809, ver 1903 → 20H2

결론

- 수동 업그레이드 시 OS 설정 값 초기화로 업무 시스템 접속에 문제 발생으로 자동화 시스템 도입
- 3주만에 대상 PC 중 85% 업그레이드 완료

장애발생 (69건, 1.53%)

처리완료	56건
• 알 수 없는 계정 보유	8건
• 설치용량 부족	28건
• 라이선스 인증 오류	10건
• 특정 제조사 PC 오류	10건
• 필수 업데이트 미설치	0건
처리불가	13건
• OS깨짐	3건
• Driver 노후로 업그레이드 미지원	7건
• 장시간CMOS 미입력 롤백	2건
• 타사 보안프로그램 정보삭제	0건
• 기타 오류	1건
• 원인 분석 불가	0건

2 자동화 업그레이드 사례2

수차례 데모 진행으로 안정성 확인 후 도입

개요

- 업그레이드 기간
2021년 8월
- 업그레이드 대상
3,200 PC
- 업그레이드 버전
Ver 1709, Ver 1903 → 21H1

결론

- 업그레이드 중 문제 발생 시 로그분석을 통한 원인 및 해결 방안 제공하나,
- OS 재설치로 로그 수집 불가
- 한 달에 걸쳐 95% 업그레이드 완료(재택 등으로 5% 미진행)

장애발생 (7건, 0.21%)

처리완료	0건
• 알 수 없는 계정 보유	0건
• 설치용량 부족	0건
• 라이선스 인증 오류	0건
• 특정 제조사 PC 오류	0건
• 필수 업데이트 미설치	0건
처리불가	7건
• OS깨짐	0건
• Driver 노후로 업그레이드 미지원	0건
• 장시간CMOS 미입력 롤백	0건
• 타사 보안프로그램 정보삭제	0건
• 기타 오류	0건
• 로그 반출 불가로 원인 분석 못함	7건

3 자동화 업그레이드 사례3

Windows 7을 Windows 10으로 업그레이드 진행

개요

- **업그레이드 기간**
2019년 10월
2021년 12월
- **업그레이드 대상**
1,200 PC (Windows 7 약 953대)
- **업그레이드 버전**
Windows 7 --> Windows 10 ver. 1903
Ver 1709, Ver 1903, Ver 2004 → 21H2

결론

- Windows 7에서 Windows 10으로 업그레이드 시 장비 노후로 인한 Driver 미지원 및 라이선스 인증 오류로 인한 실패
- 주기적으로 EOS 대상에 대해서 버전 업그레이드 진행

최초 장애발생 (93건, 9.75%)

처리완료	44건
• 알 수 없는 계정 보유	0건
• 설치용량 부족	0건
• 라이선스 인증 오류	44건
• 특정 제조사 PC 오류	0건
• 필수 업데이트 미설치	0건
처리불가	76건
• OS깨짐	0건
• Driver 노후로 업그레이드 미지원	76건
• 장시간CMOS 미입력 롤백	0건
• 타사 보안프로그램 정보삭제	0건
• 기타 오류	0건
• 원인 분석 불가	0건

4. 국방 POC 사례



5. Windows 업그레이드 주기관리 솔루션의 요건

01

업그레이드 실패 요소 최소화

CPU 1GHz 이상, 메모리 2GB 이상, HDD 32GB 이상 등 기본 요구 사항이 충족되어야 하기에 업그레이드 전 요구사항에 적합하지 않은 장치 추출 방법 필요

02

기존 PC 환경 유지를 통한 업무의 연속성 보장

Windows 10 최신 버전으로 업그레이드 후 업무 공백 시간 단축을 위해 업무 시스템 관련 애플리케이션 환경 및 브라우저 옵션 등을 유지(복원) 필요

03

운영의 효율성 제공

안정적인 업그레이드를 위해서 대용량 업그레이드 파일 배포가 용이한 시스템 구성 방안 제공

PC 용도에 따른 강제, 자동, 수동 등 다양한 업그레이드 설치 방법 제공 필요

사용자 행위기반 보안지수 플랫폼

