KOSDAQ | 소프트웨어와서비스

신시웨이 (290560)

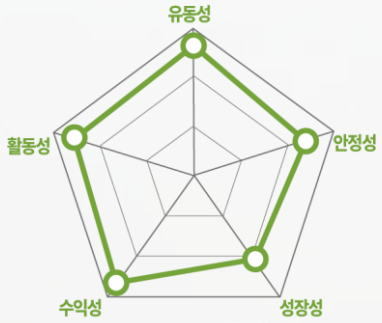
데이터베이스 보안 분야에서 꾸준히 매출 성장

체크포인트

- 신시웨이는 2005년 1월 21일에 설립되었으며 본사는 서울시 송파구에 위치. 주요 제품으로는 데이터베이스 및 시스템에 저장된 개인정보와 민감한 정보를 보호하기 위한 DB 접근제어와 DB 암호화, 파일 암호화 솔루션. 주요 고객사로는 공공기관, 금융기관, 제조 및 서비스 분야 기업
- 매출 비중이 가장 높은 제품은 'PETRA' 시리즈이며 데이터베이스(DB) 접근제어 솔루션으로, 사용자의 인증, 데이터베이스 접속 및 SQL 수행 권한 부여, 접속 및 SQL 로그 감사, 통계 리포트 등의 관리 기능을 제공. 최근 클라우드 환경에서 다양한 서비스들의 연동과 의존도가 높아지면서 데이터베이스 보안 수요 꾸준히 증가
- 데이터베이스 보안 소프트웨어 전문 공급사로서 안정적 실적 창출. 2023년 매출은 105억 원, 영업이익은 15억 원 달성. 퍼블릭 클라우드와 연동된 솔루션의 판매 호조에 힘입어 2024년 매출과 영업이익은 전년 대비 각각 15.0%, 7.4% 증가한 120억 원, 16억 원 달성 전망

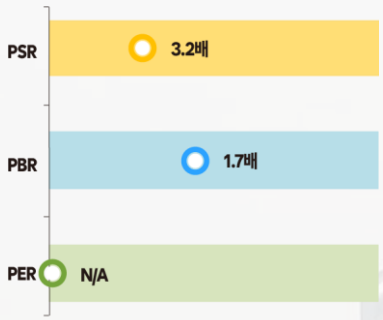
주가 및 주요이벤트

재무지표



주: 2023년 기준, Fnguide WICS 분류 상 IT산업 내 등급화

밸류에이션 지표



주: PSR, PER은 2023년 기준, PBR은 1Q24기준,
Fnguide WICS 분류상 IT산업 내 순위 비교, 우측으로 갈수록 저평가

신시웨이 (290560)

KOSDAQ
소프트웨어와서비스

연구위원 김경민, CFA clairekmkim@kirs.or.kr
연구원 이나연 lny1008@ kirs.or.kr

신시웨이의 설립 이후 꾸준히 연구개발 전개하며 업계 내에서 신뢰 확보

신시웨이는 데이터베이스 보안 제품을 주력으로 개발하며, 2005년 설립 이후 데이터베이스 접근 제어, 암호화, 비정형 파일 암호화, 권한 결재 및 데이터 변경 관리 제품을 제공. 2008년 기업부설 연구소의 KOITA 인증을 받았고, 2010년 제주 JDC R&D 센터를 설립하여 연구개발에 본격 투자 시작. 동사는 총 13종의 특허를 등록 및 출원했으며, 글로벌 시장 진출을 위해 일부 국내 특허를 국제 특허로 추가 등록하기 위한 PCT 국제출원서를 제출

페트라 브랜드를 중심으로 데이터베이스 분야에서 다양한 솔루션 제공 중

신시웨이의 대표 제품인 페트라(PETRA)는 데이터베이스 접근제어 솔루션으로, 사용자 인증, 데이터베이스 접속 및 SQL 수행 권한 부여, 접속 및 SQL 로그 감사, 통계 리포트 등의 관리 기능을 제공. 페트라 사이퍼(PETRA Cipher)는 데이터베이스 암호화 제품으로, 데이터의 기밀성을 유지하기 위해 검증된 암호화 모듈을 사용. 페트라 파일 사이퍼(PETRA File Cipher)는 서버에 저장된 비정형 파일을 암호화하는 제품

데이터베이스 보안 분야에서의 꾸준히 실적 성장 기록

신시웨이는 다양한 데이터베이스 환경에서 수많은 프로젝트를 수행한 경험을 바탕으로 높은 고객 만족도를 유지하고 있으며, 고객의 니즈를 파악하여 제품을 개선. 또한, 국내외 시장에서 경쟁력을 강화하기 위해 다양한 판매 전략을 수립하고 있으며, 조달청 디지털서비스몰 등을 통해 안정적인 매출을 창출. 2024년 매출과 영업이익은 전년 대비 각각 15.0%, 7.4% 증가한 120억 원, 16억 원 달성 전망

Forecast earnings & Valuation

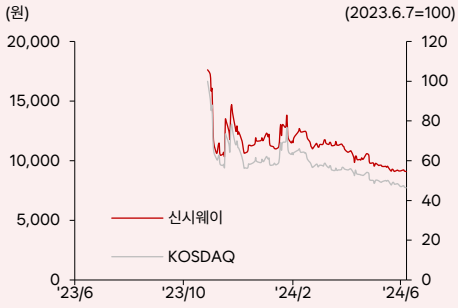
	2020	2021	2022	2023	2024F
매출액(억원)	73	79	97	105	120
YoY(%)	6.8	8.0	23.7	7.6	15.0
영업이익(억원)	8	11	21	15	16
OP 마진(%)	10.7	13.5	21.9	14.7	13.7
지배주주순이익(억원)	9	10	18	-0	29
EPS(원)	237	279	496	-5	769
YoY(%)	227.9	17.4	78.1	적전	흑전
PER(배)	0.0	0.0	0.0	N/A	11.8
PSR(배)	0.0	0.0	0.0	4.0	2.9
EV/EBITDA(배)	N/A	N/A	N/A	16.7	10.5
PBR(배)	0.0	0.0	0.0	2.2	1.6
ROE(%)	9.6	10.4	16.3	-0.1	14.3
배당수익률(%)	N/A	N/A	N/A	0.0	0.0

자료: 한국IR협의회 기업리서치센터

Company Data

현재주가 (6/13)		9,100원
52주 최고가		17,610원
52주 최저가		9,100원
KOSDAQ (6/13)		871.33p
자본금		19억원
시가총액		353억원
액면가		500원
발행주식수		4백만주
일평균 거래량 (60일)		1만주
일평균 거래액 (60일)		1억원
외국인지분율		0.06%
주요주주	엑셈 외 8인	62.87%

Price & Relative Performance



Stock Data

주가수익률(%)	1개월	6개월	12개월
절대주가	-5.3	-17.6	
상대주가	-7.1	-21.6	

참고

1) 표지 재무지표에서 안정성 지표는 '부채비율', 성장성 지표는 '매출액 증가율', 수익성 지표는 'ROE', 활동성지표는 '순운전자본회전율', 유동성지표는 '유동비율'임. 2) 표지 밸류에이션 지표 차트는 해당 산업군내 동사의 상대적 밸류에이션 수준을 표시. 우측으로 갈수록 밸류에이션 매력도 높음.

기업 개요

1 데이터 보안 전문 기업

신시웨이는 창업 초기부터 연구 개발에 적극 투자

신시웨이는 2005년에 설립된 데이터 보안 전문 기업으로, 창업 초기에 데이터베이스 보안 솔루션 개발에 집중하였으며, 국내외 다양한 인증을 획득하며 기술력을 입증받았다. 데이터베이스 보안 솔루션은 데이터 무단 접근, 유출, 변조 등의 위협으로부터 중요한 정보를 보호하기 위해 필수적이다. 특히, 금융기관, 의료기관, 공공기관 등에서 개인정보와 민감한 데이터를 안전하게 관리하기 위해서는 데이터베이스 보안이 핵심 요소로 작용한다. 신시웨이는 창업 초기부터 연구 개발에 적극 투자하여, 2008년 기업부설연구소의 KOITA 인증을 획득하고, 2010년에는 제주 JDC R&D센터를 설립하였다. 이러한 노력 덕분에 신시웨이는 설립 초기부터 안정적인 성장을 이룰 수 있었고, 점차 데이터베이스 접근 제어 및 암호화 솔루션 시장에서 중요한 위치를 차지하게 되었다. 현재 신시웨이는 데이터 보안 분야에서 다양한 특허를 보유하고 있으며, 국내외 시장에서 인정받는 기술력을 바탕으로 지속적인 성장을 이루고 있다.

신시웨이의 주요 연혁

연도	내용
2005	신시웨이 설립, 정재훈 대표 주도
2008	기업부설연구소 KOITA 인증 획득
2010	제주 JDC R&D센터 설립
2012	데이터베이스 접근 제어 및 암호화 솔루션 개발
2014	국내외 다양한 데이터 보안 인증 획득
2015	주요 금융기관 및 공공기관에 데이터 보안 솔루션 공급 시작
2017	데이터 보안 관련 특허 다수 획득
2019	글로벌 시장 진출, 아시아 지역에서 매출 증대
2021	클라우드 기반 데이터 보안 솔루션 출시
2023	코스닥 상장, 글로벌 시장 확대

자료: 신시웨이, 한국IR협의회 기업리서치센터

대표적인 제품은 페트라(PETRA) 시리즈

신시웨이는 데이터 보안을 위한 다양한 제품을 개발 및 제공하고 있다. 대표적인 제품으로는 페트라(PETRA), 페트라 사이퍼(PETRA Cipher), 페트라 파일 사이퍼(PETRA File Cipher), 페트라 사인(PETRA Sign)이 있다.

페트라: 데이터베이스 접근 제어 솔루션으로, 데이터베이스(DB) 시스템에 대한 접속 및 데이터를 조회, 삭제, 변경하는 권한을 세밀하게 통제한다. 동 솔루션은 데이터베이스에 접근하는 사용자의 권한을 효과적으로 관리하여, 비인가자가 중요한 데이터에 접근하거나 변조하는 것을 방지한다. 페트라는 데이터의 가용성과 무결성을 유지하는 데 중점을 두고 있으며, 특히 금융, 의료, 공공기관 등 민감한 데이터를 다루는 기관에서 필수적인 보안 도구로 활용되고 있다. 페트라는 다양한 접근 제어 정책을 통해 사용자별, 그룹별 권한을 설정할 수 있으며, 이를 통해 최소 권한 원칙을 준수함으로써 데이터 보안 수준을 강화한다.

페트라 사이퍼: 데이터베이스에 저장된 데이터를 보호하기 위한 암호화 솔루션이다. 동 제품은 데이터베이스 내의 모든 데이터를 검증된 암호화 모듈을 통해 암호화하여, 데이터를 안전하게 보호한다. 데이터 암호화는 정보의 기밀성을 유지하는 데 핵심적인 역할을 하며, 특히 데이터 유출이나 해킹으로 인한 정보 노출 위험을 줄이는 데 효과적이다. 페

트라 사이퍼는 데이터가 저장되는 모든 위치에서 자동으로 암호화를 수행하며, 데이터의 무결성을 보장하는 동시에, 데이터 접근 시 권한이 부여된 사용자만이 데이터를 복호화하여 사용할 수 있도록 설계되어 있다. 동 솔루션은 금융 거래 데이터, 개인 의료 기록 등 민감한 정보의 보호에 필수적이다.

페트라 파일 사이퍼: 서버에 저장된 비정형 파일을 암호화하는 솔루션이다. 비정형 파일에는 이미지, 로그 파일, 데이터 파일 등 다양한 유형의 파일이 포함되며, 이러한 파일들은 종종 민감한 정보를 포함하고 있어 보호가 필요하다. 페트라 파일 사이퍼는 이러한 파일들을 검증된 암호화 모듈을 통해 안전하게 암호화하여, 외부의 불법적인 접근으로부터 데이터를 보호한다. 동 솔루션은 특히 파일의 기밀성을 유지하고, 파일이 전송되거나 백업되는 과정에서도 암호화 상태를 유지하여 안전하게 관리할 수 있다. 페트라 파일 사이퍼는 클라우드 환경에서도 유연하게 작동하며, 기업의 데이터 보안 요구를 충족하는 중요한 도구로 자리 잡고 있다.

페트라 사인: 데이터베이스 접근 및 변경에 대한 권한 결재 솔루션이다. 동 제품은 데이터베이스에 접속하거나 SQL을 실행하며, 데이터를 변경하는 과정에서 결재 과정을 거치도록 설계되어 있다. 이를 통해 데이터베이스 접근 및 관리 권한을 세분화하고, 직무분리 원칙을 준수함으로써 내부 통제를 강화할 수 있다. 페트라 사인은 사용자의 행위에 대해 결재를 통해 검토 및 승인 절차를 도입하여, 데이터 보안 관리를 사용자 관점에서 수행할 수 있도록 지원한다. 동 솔루션은 조직 내에서 최소 권한 원칙을 엄격히 지키며, 데이터의 무결성과 보안을 유지하는 데 중요한 역할을 한다. 특히, 민감한 데이터를 다루는 산업에서 데이터 변경에 대한 추적 및 통제를 가능하게 하여, 보안 사고를 예방하고 효율적인 데이터 관리 체계를 구축할 수 있다.

신시웨이의 이러한 주요 제품들은 데이터 보안의 다양한 측면을 포괄적으로 다루고 있으며, 데이터의 기밀성, 무결성, 가용성을 보장하여 다양한 산업 분야에서 신뢰할 수 있는 보안 솔루션으로 자리매김하고 있다.

신시웨이의 주요 제품 (소프트웨어 솔루션)

제품명	내용
페트라 (PETRA)	데이터베이스(DB) 접속 및 데이터 조회, 삭제, 변경 등의 권한을 통제하여 비인가자로부터 데이터를 보호하여 가용성 및 무결성 유지
페트라 사이퍼 (PETRA Cipher)	데이터베이스(DB)에 저장된 데이터를 검증받은 암호화 모듈로 암호화하여 데이터의 기밀성 유지
페트라 파일 사이퍼 (PETRA File Cipher)	서버에 저장된 이미지, 로그 파일, 데이터 파일 등을 검증받은 암호화 모듈로 암호화하여 데이터의 기밀성 유지
페트라 사인 (PETRA Sign)	데이터베이스(DB)의 접속, SQL의 실행, 데이터 변경 관리 등을 결재를 통해 수행할 수 있도록 하여 사용자 관점의 보안 관리로 최소 권한과 직무 분리 원칙 준수

자료: 신시웨이, 한국IR협의회 기업리서치센터

2023년 11월 3일에 코스닥 시장에 상장

신시웨이는 2023년 11월 3일에 코스닥 시장에 상장했다. 상장은 아이비케이에스제17호기업인수목적 주식회사(SPAC)와의 합병을 통해 이루어졌으며, 신시웨이가 SPAC를 흡수하는 형태로 합병이 진행되었다. 합병의 비율은 1:0.2278683으로 설정되었다. 신시웨이는 상장을 준비하는 과정에서 2023년 7월 13일 한국거래소로부터 코스닥 상장을 위한 예비심사를 통과하였다. 예비심사 통과 당시, 신시웨이는 2022년 기준 전년 대비 20.7% 증가한 97억 원의 매출을 기록하였으며, 영업이익률과 당기순이익률은 각각 22%와 19%로 높은 수익성을 나타낸 바 있다. 아울러 신시웨이가 데이터베이스 접근 제어와 암호화 솔루션 등 주력 제품이 DB 보안 업계에서 경쟁력을 인정받고 있다는 점이

예비심사에서 긍정적 영향을 끼쳤다. 신시웨이는 업계 최초로 DB 암호화 CC 인증을 획득하였고, 현재 주요 제품인 DB 접근제어와 DB 암호화 솔루션 모두에 대해 GS 인증과 CC 인증을 보유하고 있다. GS 인증은 'Good Software'의 약자로, 제품의 품질과 성능을 공인기관이 평가하여 인증하는 제도이다. CC 인증은 'Common Criteria'의 약자로, 정보기술 보안 평가 기준으로, 제품이 국제적으로 인정받을 수 있는 보안성을 갖추고 있음을 증명하는 인증이다. 코스닥 시장에 상장한 이후 신시웨이는 연구 개발 및 글로벌 시장 진출을 위한 기반을 강화할 계획을 발표했다.

신시웨이의 코스닥 시장 상장 관련 주요 내용 요약

항목	내용
상장일	2023년 11월 3일
상장 방식	아이비케이에스제17호기업인수목적 주식회사(SPAC)와의 합병
합병 대상	신시웨이가 SPAC를 흡수
합병 비율	1:0.2278683
예비심사 통과일	2023년 7월 13일
2022년 매출	97억 원 (전년 대비 20.7% 증가)
2022년 영업이익률	22%
2022년 당기순이익률	19%
주요 제품	DB 접근제어, DB 암호화 솔루션
주요 인증	GS 인증, CC 인증

자료: 신시웨이, 한국IR협의회 기업리서치센터

2 기술 혁신과 제품 개선을 통해 차별화된 서비스를 제공하며 시장에서의 입지를 강화

주요 경쟁사로는 DB 보안 분야의 강자인 안랩, 윈스, 지란지교시큐리티, 이글루 등

신시웨이는 데이터베이스 보안 솔루션을 주요 제품으로 제공하는 기업으로, 이와 유사한 제품을 제공하는 다양한 경쟁사들이 존재한다. 주요 경쟁사로는 DB 보안 분야의 강자인 안랩, 윈스, 지란지교시큐리티, 이글루 등이 있다. 이들 기업은 신시웨이와 마찬가지로 데이터베이스 접근 제어 및 암호화 솔루션을 제공하며, 각각의 제품은 다양한 산업에서 데이터 보안을 위한 주요 수단으로 사용되고 있다. 데이터베이스 접근 제어 및 암호화 솔루션은 중요 데이터에 대한 무단 접근을 방지하고, 데이터 유출을 예방하는 데 필수적이다. 금융기관, 의료기관, 공공기관 등에서는 이러한 솔루션을 통해 개인정보와 민감 정보를 안전하게 관리하고 보호할 수 있다. 데이터베이스 접근 제어는 데이터베이스에 접근하는 사용자의 권한을 엄격히 통제하여 불법적인 접근을 차단하고, 암호화는 데이터가 외부에 유출되더라도 그 내용이 보호되도록 기밀성을 유지한다.

또한, 신시웨이는 클라우드 기반 보안 솔루션을 통해 시장에서의 입지를 확장하고자 노력하고 있으며, 이와 관련해서는 펜타시큐리티, SK인포섹 등의 기업과도 경쟁하고 있다. 클라우드 기반 보안 솔루션은 데이터가 물리적 서버가 아닌 클라우드 환경에 저장될 때 발생할 수 있는 보안 위협을 효과적으로 관리하는 역할을 한다. 클라우드 서비스는 유연성과 접근성이 뛰어나지만, 동시에 분산된 환경에서의 데이터 보호가 중요하다. 따라서 클라우드 기반 보안 솔루션은 데이터 접근을 실시간으로 모니터링하고, 이상 징후를 감지하여 즉각적인 대응을 가능하게 한다. 이러한 솔루션은 데이터 보안의 복잡성을 줄이고, 다양한 디바이스와 위치에서 안전하게 데이터를 접근하고 관리할 수 있도록 돕는다.

이러한 경쟁사들은 각각의 특화된 기술력과 시장 점유율을 바탕으로 강력한 경쟁 관계를 형성하고 있다. 동 외에도 글로벌 시장에서는 오라클(Oracle), IBM, 사이베이스(Sybase) 등의 거대 IT 기업들이 데이터베이스 보안 솔루션을 제공

하며 신시웨이와의 경쟁을 이어가고 있다. 특히, 오라클과 IBM은 데이터베이스 시장에서 높은 점유율을 차지하고 있으며, 데이터 보안 솔루션에서도 높은 신뢰성을 갖춘 제품을 제공하여 글로벌 경쟁력을 유지하고 있다. 이러한 경쟁사들과의 경쟁에서 신시웨이는 기술 혁신과 제품 개선을 통해 차별화된 서비스를 제공하며 시장에서의 입지를 강화하고 있다.

신시웨이와 데이터베이스 보안 솔루션 또는 클라우드 보안 솔루션에서 경쟁하는 기업

기업	솔루션
안랩	DB 보안 및 암호화 솔루션 (AhnLab TrusGuard DP)
윈스	DB 접근 제어 솔루션 (WINS Database Protection)
지란지교시큐리티	DB 보안 솔루션 (Jiran Security DB Shield)
이글루	DB 모니터링 및 접근 제어 솔루션 (Igloo Security SIEM)
펜타시큐리티	클라우드 기반 데이터 암호화 솔루션 (Penta Cloud Security)
SK인포섹	클라우드 보안 관리 솔루션 (SK Infosec Cloud Security)
오라클	Oracle Database Security, Oracle Advanced Security
IBM	IBM Guardium Data Protection, IBM Cloud Security
사이베이스	SAP Sybase ASE Security, SAP Sybase SQL Anywhere

자료: 신시웨이, 업계 자료, 한국IR협의회 기업리서치센터

공공부문은 신시웨이의 주요 고객군

신시웨이의 매출은 주로 공공부문, 금융부문, 일반 기업 부문, 그리고 해외 시장에서 발생한다. 공공부문은 신시웨이의 주요 고객군 중 하나로, 전체 매출의 상당한 부분을 차지하고 있다. 공공기관은 데이터 보안의 중요성을 높이 평가하여 신시웨이의 데이터베이스 접근 제어와 암호화 솔루션을 적극적으로 도입하고 있다. 금융부문도 주요 고객사에 포함되며, 금융기관들은 민감한 금융 데이터를 안전하게 보호하기 위해 신시웨이의 솔루션을 채택하고 있어 매출의 큰 비중을 차지한다. 일반 기업들은 데이터 보안의 필요성을 인식하고, 신시웨이의 제품과 서비스를 통해 데이터 보안 솔루션을 도입함으로써 매출에 기여하고 있다. 또한, 신시웨이는 해외 시장에서도 활동하고 있으며, 아시아 지역을 중심으로 글로벌 시장 확대를 통해 매출의 다각화를 꾀하고 있다. 주로 일본, 중국, 동남아시아 지역에서 시장을 확대하고 있으며, 현지의 주요 IT 기업과의 협력 및 파트너십을 통해 매출을 증대시키고 있다. 특히, 신시웨이의 주요 제품인 '페트라' 시리즈는 아시아 지역에서의 데이터 보안 요구 사항을 충족시키기 위한 맞춤형 솔루션으로서 인기를 얻고 있다. 2024년 1분기 기준, 신시웨이의 총 매출 중 수출 매출액은 약 2억 1천만 원이다. 또한, 신시웨이는 클라우드 기반 보안 솔루션을 통해 글로벌 고객들에게도 데이터 보호 서비스를 제공하고 있으며, 이를 통해 해외 매출 비중을 점진적으로 확대하고 있다.

신시웨이와 데이터베이스 보안 솔루션 또는 클라우드 보안 솔루션에서 경쟁하는 기업

부문	설명
공공부문	공공기관은 데이터 보안의 중요성을 높이 평가하여 신시웨이의 데이터베이스 접근 제어와 암호화 솔루션을 적극적으로 도입하고 있음
금융부문	금융기관들은 민감한 금융 데이터를 안전하게 보호하기 위해 신시웨이의 솔루션을 채택
일반 기업 부문	일반 기업들은 데이터 보안의 필요성을 인식하고, 신시웨이의 제품과 서비스를 통해 데이터 보안 솔루션을 도입
해외 시장	아시아 지역을 중심으로 글로벌 시장 확대를 통해 매출의 다각화를 꾀하고 있으며, 주요 IT 기업과의 협력 및 파트너십을 통해 매출을 증대시키고 있음. 2024년 1분기 기준 수출 매출액은 약 2억 1천만 원.

자료: 신시웨이, 업계 자료, 한국IR협의회 기업리서치센터

데이터베이스 접근 제어 솔루션은 다양한 산업 분야에서 데이터의 무단 접근을 방지하고 데이터 무결성을 유지하는 데 사용되어 신시웨이의 주요 매출원에 해당

신시웨이의 매출 비중은 응용처별로 데이터베이스 접근 제어, 데이터 암호화, 클라우드 기반 보안 솔루션으로 나뉜다. 데이터베이스 접근 제어 솔루션은 다양한 산업 분야에서 데이터의 무단 접근을 방지하고 데이터 무결성을 유지하는 데 사용되어 신시웨이의 주요 매출원에 해당한다. 특히 금융과 공공기관에서는 반응이 우호적이다. 한편, 데이터 암호화 솔루션은 금융, 의료, 공공기관 등에서 개인정보와 민감한 데이터를 안전하게 보호하기 위한 핵심 기술로 활용되며, 매출의 중요한 부분을 차지한다. 또한, 신시웨이는 클라우드 기반 보안 솔루션을 통해 클라우드 환경에서의 데이터 보호를 지원하고 있으며, 클라우드 보안에 대한 수요 증가로 인해 이 부문에서도 상당한 매출 비중을 기록하고 있다. 이러한 응용처별 매출 비중은 신시웨이가 다양한 산업과 기술 분야에서 매출을 창출하고 있다는 것을 보여준다.

3 신시웨이의 최대주주는 엑셈

신시웨이의 최대주주와 2대 주주는 각각 엑셈과 정재훈 대표이사

2024년 3월 31일 기준으로, 신시웨이의 최대주주는 소프트웨어 기업 엑셈으로, 1,437,597주의 주식을 보유하여 지분율 39.58%를 차지하고 있다. 이는 신시웨이의 최대 지분 보유자로서 중요한 의사결정에 큰 영향을 미치는 위치에 있다. 2대 주주는 신시웨이의 창업자인 정재훈 대표이사로서 443,201주의 주식을 보유하고 있으며, 지분율은 12.20%이다. 그밖에 유경석 대표이사도 269,843주의 주식을 보유하고 있어 지분율은 7.43%이다. 한편 김재현, 김광연 등 등기임원의 지분율은 각각 5% 미만이다. 주요 지배 주주의 지분율은 64.72%이다.

주요 지배 주주의 지분율은 64.72%(1Q24말 기준) (단위: 주, %)

성명	관계	소유주식수 및지분율	지분율
엑셈	최대주주	1,437,597	39.58%
정재훈	대표이사	443,201	12.20%
유경석	대표이사	269,843	7.43%
김재현	등기임원	110,000	3.03%
김광열	등기임원	90,045	2.48%
합산		**2,350,686**	**64.72%**

자료: 신시웨이, 한국IR협의회 기업리서치센터

엑셈은 2000년 1월 2일에 설립된 IT 성능 관리 솔루션 전문 기업

신시웨이의 최대주주인 엑셈은 2000년 1월 2일에 설립된 IT 성능 관리 솔루션 전문 기업으로, 2015년 6월 26일 코스닥 시장에 상장되었다. 엑셈의 주요 사업은 데이터베이스(DB) 성능 관리, IT 전구간(end-to-end) 성능 관리를 위한 애플리케이션 성능 관리(APM), 빅데이터 통합 관리, 클라우드 통합 모니터링, 인공지능(AI) 기반 IT 운영 지능화 솔루션, 통합 IT 성능 모니터링 SaaS 플랫폼 개발 및 공급 등이다. 엑셈은 이러한 솔루션들을 통해 다양한 산업 분야에서 IT 성능을 최적화하고, 기업의 데이터 관리 효율성을 높이는 데 기여하고 있다.

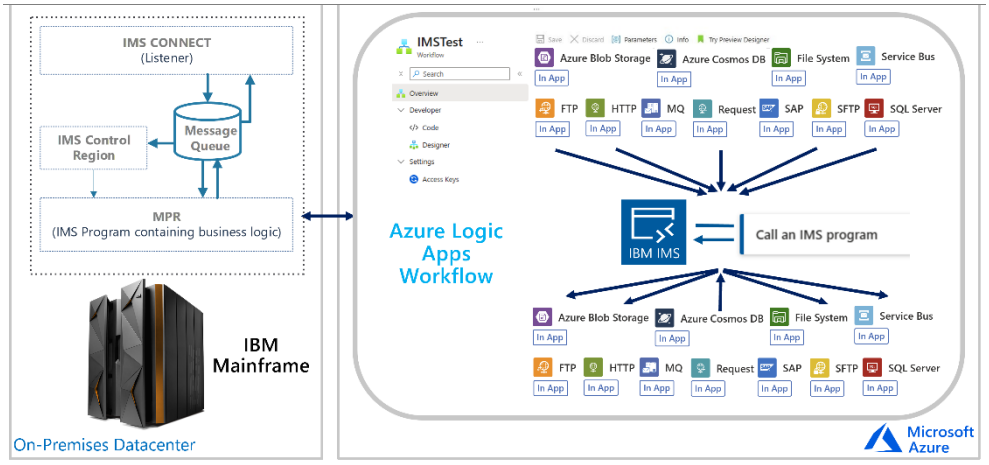
산업 현황

1 데이터베이스 관련 산업은 1960년대부터 성장

대형 컴퓨터 시스템이 대량의 데이터를 효율적으로 저장하고 관리

데이터베이스 관련 산업은 1960년대 후반에서 1970년대 초반에 본격적으로 등장하기 시작했다. 동 시기는 대형 컴퓨터 시스템이 대량의 데이터를 효율적으로 저장하고 관리하는 데 초점을 맞춘 시대였다. 초기의 데이터 저장 방식은 파일 기반 시스템으로, 데이터를 파일 단위로 관리했으며, 각 파일이 독립적으로 운영되어 데이터 관리가 매우 비효율적이었다. 이러한 문제를 해결하기 위해 IBM은 1960년대에 계층형 데이터베이스 관리 시스템인 IMS(Information Management System)를 개발하였다. 계층형 데이터베이스는 데이터를 계층 구조로 저장하고 관리하는 방식으로, 데이터의 구조화와 빠른 접근을 가능하게 하여 데이터베이스 산업의 기틀을 마련하였다. IMS는 대량의 데이터를 효율적으로 관리하고, 데이터의 일관성을 유지할 수 있는 혁신적인 시스템으로 평가받았으며 오늘날에도 클라우드 서비스와 통합되어 활용되고 있다. (하기 그림 참조)

IBM이 개발한 계층형 데이터베이스 관리 시스템인 IMS(Information Management System)의 워크플로우



주 1) 상기 그림은 Azure Logic Apps를 사용하여 IBM IMS 프로그램을 호출하는 워크플로우, 2) IBM 메인프레임의 IMS 시스템은 계층형 데이터베이스 관리 시스템의 일종이며 IMS CONNECT, IMS Control Region, MPR, Message Queue와 같은 구성 요소들이 포함, 3) Azure Logic Apps는 다양한 Azure 서비스와 통합되어 IMS 프로그램과 상호 작용 가능, 4) IBM 메인프레임의 IMS 시스템은 온프레미스 시스템인데 상기 워크플로우에서는 클라우드 서비스와 온프레미스 IMS 시스템 간의 통합을 강조

자료: IBM, 한국IR협의회 기업리서치센터

데이터베이스 관리 시스템(Database Management System, DBMS)이 발전하면서 데이터베이스 산업은 급격히 성장

1970년대 이후, 데이터베이스 관리 시스템(Database Management System, DBMS)이 발전하면서 데이터베이스 산업은 급격히 성장하였다. DBMS는 데이터를 체계적으로 저장하고, 쉽게 접근하고 조작할 수 있도록 해주는 소프트웨어 시스템이다. 1970년대 후반, IBM의 연구원 Edgar F. Codd는 관계형 데이터베이스 관리 시스템(Relational Database Management System, RDBMS)의 개념을 제안하였으며, 이는 데이터베이스 관리의 혁신을 가져왔다. RDBMS는 데이터를 표(Table) 형태로 관리하여, 서로 다른 데이터 테이블 간의 관계를 정의하고 유지하는 방식이다. 이를 통해 데이터의 무결성과 일관성을 유지하며, 데이터 조회와 업데이트가 매우 용이해졌다.

예를 들어 도서관을 생각해보자. DBMS에서는 각 책의 정보를 개별 파일에 저장한다고 가정할 수 있다. 각 파일에는 책의 제목, 저자, 출판년도 등의 정보가 포함되지만, 파일 간에 아무런 관계가 정의되어 있지 않다. 특정 저자가 쓴 모든 책을 찾으려면, 각각의 파일을 일일이 열어 확인해야 한다. 반면에, RDBMS에서는 책 정보를 저장하는 테이블과 저자 정보를 저장하는 테이블이 존재한다. 책 테이블에는 책의 제목, 출판년도, 그리고 저자 테이블의 참조 키가 포함되어 있다. 저자 테이블에는 저자의 이름과 기타 저자 관련 정보가 있다. 이렇게 테이블 간의 관계가 정의되어 있기 때문에, 특정 저자가 쓴 모든 책을 쉽게 쿼리하여 찾을 수 있다. 이러한 구조는 데이터의 무결성을 유지하고, 검색 및 관리 효율성을 높인다.

또한, RDBMS는 SQL(Structured Query Language)이라는 표준화된 언어를 통해 데이터를 질의하고 조작할 수 있게 하였으며, 이는 데이터베이스를 다루는 데 있어 매우 강력한 도구가 되었다. SQL은 데이터베이스에서 데이터를 검색하거나 수정하기 위해 사용하는 언어로, 데이터베이스와의 상호작용을 쉽게 해준다. 예를 들어, SQL을 사용하면 특정 고객의 주문 내역을 조회하거나, 매장별 재고를 업데이트하는 작업을 쉽게 수행할 수 있다. SQL은 "SELECT * FROM orders WHERE customer_id = '12345'"와 같은 간단한 명령어를 통해 특정 조건을 만족하는 데이터를 조회할 수 있다. 이러한 명령어는 데이터베이스에 대한 전문 지식이 없어도 쉽게 데이터를 관리하고 조작할 수 있도록 해주며, 다양한 비즈니스 애플리케이션에 폭넓게 적용되었다.

SQL 등 관계형 데이터베이스 관리 시스템(Relational Database Management System, RDBMS) 분야의 글로벌 기업

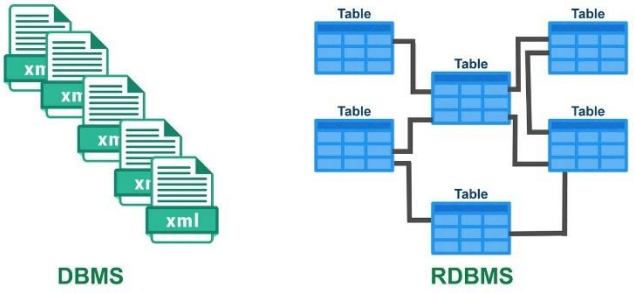
기업(또는 시스템명)	Ranking Score
Oracle Database Management System	1,240.88
MySQL	1,111.49
Microsoft SQL Server	902.22
PostgreSQL	620.75
IBM Db2	136.72
SQLite	129.20
Microsoft Access	128.56
Snowflake	120.89

주: 상기의 Ranking Score는 website mentions, search frequency, technical discussion frequency, current job offers, professional network profiles, social network relevance 등을 반영한 종합 평가 지표
자료: DB-Engines, 업계 자료, 한국IR협의회 기업리서치센터

RDBMS (Relational Database Management System)의 채택은 대기업뿐만 아니라 중소기업에도 빠르게 확산

1980년대에 접어들면서 관계형 데이터베이스 관리 시스템(RDBMS, Relational Database Management System)은 기업과 기관에서 대규모 데이터 처리를 위한 필수 도구로 자리 잡았다. 전술했던 바와 같이, RDBMS는 데이터를 표 형태로 저장하고 관리하여, 데이터 간의 관계를 쉽게 정의하고 유지할 수 있도록 한다. 예를 들어, 맥도날드는 전 세계 수많은 매장에서 주문과 재고 데이터를 효율적으로 관리해야 한다. RDBMS를 통해 맥도날드는 고객 주문 정보와 재고 데이터를 서로 연관 지어, 각 매장에서 어떤 상품이 얼마나 팔렸는지, 재고가 얼마나 남았는지를 실시간으로 파악할 수 있다. 이러한 구조는 데이터의 일관성과 무결성을 유지하며, 데이터를 효율적으로 조회하고 업데이트할 수 있도록 지원한다. RDBMS의 채택은 대기업뿐만 아니라 중소기업에도 빠르게 확산되었고, 데이터베이스를 사용하는 비즈니스 애플리케이션이 급격히 증가하였다. 이러한 변화는 데이터베이스 산업의 성장과 확장을 촉진하였으며, 데이터 관리의 중요성이 부각되기 시작했다. 또한, 1980년대와 1990년대에 인터넷과 네트워크 기술의 발전으로, 데이터베이스는 웹 기반 애플리케이션과 클라우드 컴퓨팅의 핵심 구성 요소로 자리 잡았다.

관계형 데이터베이스 관리 시스템 (RDBMS)와 전통적인 데이터베이스 관리 시스템(DBMS)의 차이



주 1) DBMS와 RDBMS의 주요 차이점은 데이터의 구조와 관계 정의의 유무, 2) DBMS는 XML 파일과 같은 비구조화된 데이터를 관리하는 시스템이며, 데이터 간의 관계를 정의하지 않음. 예를 들어, 도서관에서 각 책의 정보를 별도의 파일로 저장하므로 특정 저자가 쓴 모든 책을 찾으려면, 각각의 파일을 일일이 열어서 확인해야 하는 상황 발생, 3) RDBMS는 테이블 형태의 구조화된 데이터를 관리하며, 테이블 간의 관계를 정의하고 이를 통해 데이터의 무결성과 일관성을 유지. 도서관에서 특정 저자가 쓴 모든 책을 찾을 수 있음, 4) RDBMS는 관계형 데이터베이스 모델을 기반으로 하여 보다 효율적인 데이터 저장과 검색을 가능하게 함

자료: Medium, 한국IR협의회 기업리서치센터

관계형 데이터베이스 관리 시스템(Relational Database Management System, RDBMS) 적용 사례

업종	사례
패스트푸드	매장에서 주문과 재고 데이터를 관리
은행	계좌, 거래 내역, 대출 정보를 관리
의료	환자 기록, 진료 일정, 처방전 정보를 관리
소매	제품 재고, 판매 내역, 고객 데이터를 관리
교육	학생 등록, 성적, 수업 일정을 관리

자료: 업계 자료, 한국IR협의회 기업리서치센터

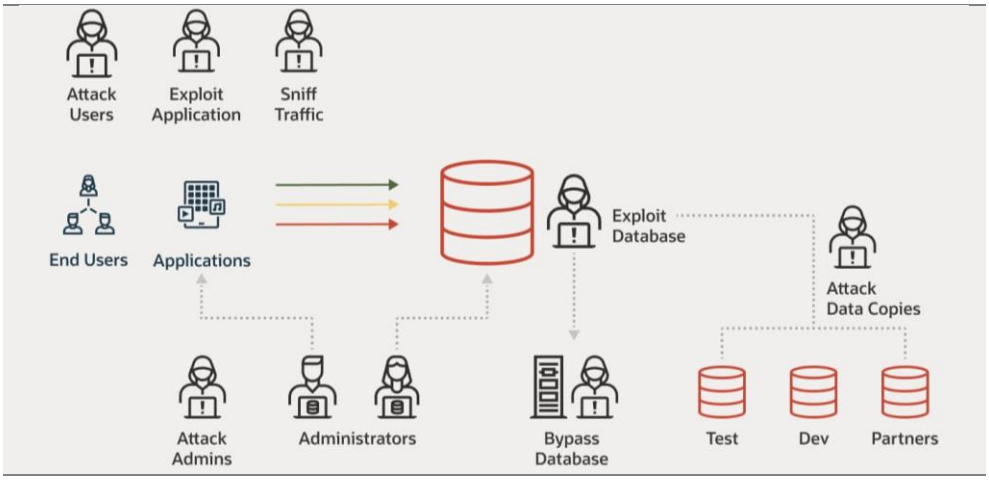
2 1980년대 이후 데이터베이스의 광범위한 사용과 함께 데이터 보안에 대한 필요성이 부각

데이터베이스의 광범위한 사용과 함께 데이터 보안에 대한 필요성 부각

1980년대와 1990년대에 걸쳐 관계형 데이터베이스 관리 시스템(RDBMS)이 대중화됨에 따라 데이터베이스의 사용이 폭발적으로 증가하였다. 데이터베이스는 다양한 비즈니스 애플리케이션의 핵심 구성 요소로 자리 잡았고, 기업들은 대량의 데이터를 효과적으로 저장하고 관리하기 위해 RDBMS를 채택하였다. 그러나 데이터베이스의 광범위한 사용과 함께 데이터 보안에 대한 필요성이 부각되었다.

데이터베이스에는 기업의 핵심 자산인 중요한 정보들이 저장되어 있으며, 이 정보들은 외부 공격이나 내부 부정행위로부터 보호받아야 했다. 이에 따라 데이터베이스 보안 산업은 급속히 성장하기 시작하였다. 데이터베이스 보안 산업은 초기에는 데이터 접근 제어와 데이터 무결성 유지를 중심으로 발전하였다. 접근 제어는 데이터베이스에 접근할 수 있는 사용자의 권한을 관리하여 비인가된 접근을 차단하는 기능으로, 데이터의 기밀성을 유지하는 데 필수적이었다. 이와 함께 데이터 무결성을 유지하기 위해 데이터베이스 내 데이터의 일관성과 정확성을 보장하는 기술이 도입되었다. 1980년대 후반부터는 암호화 기술이 데이터베이스 보안에 중요한 요소로 자리 잡기 시작하였다. 데이터 암호화는 데이터가 저장되거나 전송될 때 기밀성을 보장하여, 데이터가 유출되더라도 내용을 해독할 수 없도록 하는 보안 기술이다.

데이터베이스 보안 관련 소프트웨어 기업 중 Oracle의 보안 방식 플로우



자료: Oracle, 한국IR협의회 기업리서치센터

공격자는 사용자(End Users), 애플리케이션(Applications), 관리자(Administrators) 등 다양한 경로를 통해 데이터베이스에 접근하여 데이터를 유출하거나 조작 가능

위 그림은 데이터베이스 보안 위협과 이를 방어하기 위한 다양한 접근 방법을 시각적으로 설명하고 있다. 특정 데이터베이스 관리 시스템의 공격자는 사용자(End Users), 애플리케이션(Applications), 관리자(Administrators) 등 다양한 경로를 통해 데이터베이스에 접근하여 데이터를 유출하거나 조작할 수 있는 방법을 보여준다.

사용자 공격 (Attack Users): 공격자는 최종 사용자를 목표로 하여 다양한 방식으로 계정 정보를 탈취하거나 악성 소프트웨어를 설치할 수 있다. 예를 들어, 피싱 공격을 통해 사용자가 신뢰할 수 있는 출처에서 온 것처럼 보이는 이메일을 열게 하여 사용자 이름과 비밀번호를 입력하게 만들 수 있다. 또한, 사용자가 악성 웹사이트를 방문하도록 유도하거나, 소셜 엔지니어링을 통해 민감한 정보를 누설하도록 유도할 수 있다. 이러한 방식으로 탈취된 계정 정보는 공격자가 시스템에 무단 접근하는 데 사용될 수 있다.

애플리케이션 악용 (Exploit Application): 애플리케이션의 취약점을 이용하여 데이터베이스에 접근하거나 데이터를 탈취하는 방법이다. 예를 들어, SQL 인젝션 공격을 통해 애플리케이션의 입력 필드를 악용하여 데이터베이스 쿼리를 조작할 수 있다. SQL 인젝션 공격은 웹사이트의 입력 필드를 통해 악성 SQL 코드를 삽입하여 데이터베이스를 조작하는 방법이다. 공격자가 사용자 이름 입력란에 admin' --와 같은 문자열을 입력한다면, 비밀번호와 관계없이 admin 계정으로 로그인할 수 있게 된다. 이를 통해 공격자는 데이터베이스 내의 민감한 정보에 접근하거나 데이터를 조작할 수 있다.

트래픽 스니핑 (Sniff Traffic): 네트워크 트래픽을 가로채어 민감한 데이터를 탈취하는 방법이다. 공격자는 네트워크 상에서 전송되는 데이터를 스니핑 도구를 사용하여 가로챌 수 있다. 이를 통해 로그인 정보, 신용카드 번호, 개인 식별 정보(PII) 등 중요한 데이터를 탈취할 수 있다. 트래픽 스니핑은 특히 암호화되지 않은 네트워크에서 더 큰 위협이 된다. 따라서 데이터 전송 시 암호화 프로토콜을 사용하는 것이 중요하다.

관리자 공격 (Attack Admins): 데이터베이스 관리자의 계정을 탈취하여 관리자 권한으로 데이터베이스를 조작하거나 데이터를 유출하는 방법이다. 공격자는 피싱, 또는 직접적인 해킹을 통해 관리자 계정 정보를 탈취할 수 있다. 관리자 권한을 획득하면 공격자는 데이터베이스의 설정을 변경하거나, 데이터를 삭제, 수정, 또는 유출할 수 있다.

데이터베이스 우회 (Bypass Database): 공격자는 데이터베이스의 네트워크 경로를 탐색하여 보안 취약점을 찾고 이를 악용할 수 있다. 또한, 물리적 접근을 통해 데이터베이스 서버를 직접 조작하거나, 미흡한 보안 설정을 악용하여 데이터베이스에 접근할 수 있다.

데이터베이스 악용 (Exploit Database): 데이터베이스 자체의 취약점을 이용하여 데이터를 탈취하거나 시스템을 손상시키는 방법이다. 예를 들어, 데이터베이스 소프트웨어의 버그나 취약점을 발견하고 이를 악용하여 비정상적인 쿼리를 실행하거나, 악성 코드를 주입할 수 있다. 이러한 공격은 데이터베이스의 무결성을 훼손하고, 시스템의 가용성을 저하시킬 수 있다.

데이터 복사본 공격 (Attack Data Copies): 테스트, 개발, 파트너 시스템에 저장된 데이터 복사본을 공격하여 민감한 정보를 탈취하는 방법이다. 많은 조직이 테스트와 개발 목적으로 운영 데이터의 복사본을 사용하며, 이 복사본이 적절히 보호되지 않을 경우 공격에 취약해질 수 있다. 또한, 파트너 시스템과 공유된 데이터가 보안 조치가 미흡할 경우에도 데이터 유출의 위험이 있다.

이러한 위협을 방지하기 위해, 데이터베이스 보안 솔루션은 접근 제어, 암호화, 모니터링 및 감사 등의 기능을 통해 데이터를 보호하고, 비정상적인 접근 시도를 탐지하며, 데이터 유출을 방지하는 데 중점을 두고 있다. 그렇다면 1970년대 이후, 데이터베이스 관리 시스템(Database Management System, DBMS)이 등장한 이후 데이터베이스 보안 솔루션의 필요성은 어떤 계기로 대두되었을까? 데이터베이스가 온프레미스 환경을 벗어나 인터넷 환경 또는 외부 네트워크 환경에서 사용되기 시작하며 데이터베이스 보안 솔루션 시장이 커지기 시작했다.

데이터 전송 중 발생할 수 있는 보안 위협을 막기 위한 데이터 전송 암호화 기술이 도입

1990년대에 접어들면서 인터넷과 네트워크 기술이 발전함에 따라, 데이터베이스는 더욱 다양한 환경에서 사용되기 시작하였다. 이로 인해 데이터베이스 보안의 필요성은 더욱 커졌고, 보안 기술은 빠르게 발전하였다. 네트워크를 통해 데이터가 전송되면서 데이터 전송 중 발생할 수 있는 보안 위협을 막기 위한 데이터 전송 암호화 기술이 도입되었다. 또한, 데이터베이스에 저장된 데이터를 보호하기 위한 저장 데이터 암호화 기술도 발전하였다. 동 시기에 데이터베이스 보안 솔루션은 데이터 접근 제어, 데이터 암호화, 데이터 무결성 유지, 데이터 유출 방지 등 다양한 기능을 제공하는 통합 보안 솔루션으로 진화하였다.

1990년대 이후 점차적으로 등장하기 시작한 데이터베이스 보안 솔루션 종류

종류	목적	기능
데이터 접근 제어	허가되지 않은 접근으로부터 데이터 보호	사용자 인증 및 권한 부여
데이터 전송 암호화	데이터 전송 중 발생할 수 있는 보안 위협 방지	데이터 전송 시 암호화
저장 데이터 암호화	저장된 데이터에 대한 무단 접근 방지	데이터 저장 시 암호화
데이터 무결성 유지	데이터의 정확성과 일관성 유지	데이터 변경 추적 및 모니터링
데이터 유출 방지	데이터 유출과 정보 손실 방지	데이터 유출 방지 및 침해 탐지

자료: 업계 자료, 한국IR협의회 기업리서치센터

데이터 유출 사건이 빈번하게 발생하면서 데이터베이스 보안 솔루션의 필요성이 크게 부각

2000년대 이후, 데이터 유출 사건이 빈번하게 발생하면서 데이터베이스 보안 솔루션의 필요성이 크게 부각되었다. 특히 2013년 타깃(Target)사의 데이터 유출 사건은 4천만 건 이상의 고객 신용카드 정보가 유출되면서, 데이터 보안의 중요성을 전 세계적으로 인식시키는 계기가 되었다. 동 사건은 보안이 취약한 시스템이 어떻게 고객 데이터를 보호하지 못하고 공격에 노출될 수 있는지를 보여주었으며, 기업들이 데이터 보호를 위한 투자를 대폭 늘리게 되는 계기가 되었다. 이와 함께, 2014년 홈디포(Home Depot)사의 데이터 유출 사건에서도 5천만 건 이상의 고객 데이터가 유출되면서, 기업들은 데이터베이스 보안 솔루션을 도입하지 않으면 엄청난 경제적 손실과 브랜드 신뢰성에 타격을 입을 수 있다는 것을 깨닫게 되었다. 이러한 사건들은 데이터베이스 접근 제어와 암호화 솔루션 도입을 촉진하며, 보안 솔루션 시장의 수요를 크게 증가시켰다.

개인정보 보호 법률과 데이터베이스 보안 솔루션의 도입

2000년대 이후 전 세계적으로 개인정보 보호와 데이터 보안에 대한 법률과 규제가 강화되면서, 데이터베이스 보안 솔루션의 도입이 더욱 필수적으로 되었다. 미국에서는 2002년 Sarbanes-Oxley Act(SOX)가 제정되어 기업들이 재무 데이터를 보호하고 투명하게 관리하도록 요구하였다. 이는 기업들이 데이터베이스 내 재무 데이터를 안전하게 보호하기 위한 보안 솔루션을 도입하는 계기가 되었다. 또한, 1996년 제정된 Health Insurance Portability and Accountability Act(HIPAA)는 의료 데이터의 보호를 강화하는 법률로, 의료기관들이 엄격한 데이터 보호 기준을 준수하도록 하였다. 유럽에서는 2016년 General Data Protection Regulation(GDPR)이 도입되면서, 기업들이 개인정보를 보호하고 데이터 유출 방지를 위한 조치를 취하도록 강력히 요구하였다. GDPR은 개인정보 보호에 대한 강력한 규제를 통해, 기업들이 데이터베이스 보안 솔루션을 도입하여 법적 요구사항을 준수하게 하는 중요한 동기가 되었다. 이러한 법률들은 데이터 보호의 중요성을 강조하고, 기업들이 법적 요구사항을 충족하기 위해 데이터베이스 보안 기술을 적극적으로 도입하도록 촉진했다.

클라우드 환경에서의 데이터베이스 보안 필요성 대두

2000년대 중반부터 클라우드 컴퓨팅이 본격적으로 도입되면서, 데이터베이스가 클라우드 환경에서도 사용되기 시작했다. 이는 데이터베이스가 물리적 서버뿐만 아니라, 클라우드 환경에서도 보안을 유지해야 한다는 새로운 도전 과제를 안겨주었다. 클라우드 환경에서는 데이터가 여러 위치에 분산 저장되고, 다양한 기기에서 접근할 수 있어 보안 위협이 크게 증가하였다. 이에 따라 클라우드 기반 데이터베이스 보안 솔루션이 등장하였으며, 이는 데이터의 접근 통제, 데이터 암호화, 데이터 유출 방지 등 다양한 보안 기능을 클라우드 환경에서도 제공하게 되었다. 예를 들어, Amazon Web Services(AWS)는 클라우드 환경에서의 데이터 보안을 강화하기 위해 AWS Key Management Service(KMS)를 제공하여, 데이터베이스에 저장된 데이터를 암호화하고 접근을 통제할 수 있도록 하였다. 또한, Google Cloud는 Cloud SQL을 통해 데이터베이스에 대한 실시간 모니터링과 보안 업데이트를 제공하여 데이터의 안전성을 높이고 있다. 이러한 클라우드 기반 데이터베이스 보안 솔루션은 데이터 보호의 새로운 표준을 제공하며, 기업들이 클라우드 환

경에서도 데이터를 안전하게 관리할 수 있도록 지원하고 있다.

클라우드 컴퓨팅 환경에 특화된 데이터베이스 보안 솔루션 종류

종류	목적	기능
클라우드 접근 보안 중개 (Cloud Access Security Broker)	클라우드 애플리케이션에 대한 안전한 접근 관리	사용자 행동 분석 및 위협 탐지
클라우드 데이터 암호화	클라우드 내 데이터 암호화를 통한 데이터 보호	클라우드 데이터 저장 및 전송 시 암호화
클라우드 환경 모니터링	클라우드 환경의 보안 상태 지속적 모니터링	클라우드 리소스 사용 및 보안 로그 분석
클라우드 데이터 무결성 유지	클라우드 데이터의 정확성과 일관성 유지	데이터 변경 추적 및 클라우드 데이터 복구
클라우드 데이터 유출 방지	클라우드 환경에서의 데이터 유출 방지	데이터 유출 탐지 및 차단, 위협 대응

자료: 업계 자료, 한국IR협의회 기업리서치센터

빅데이터와 데이터베이스 보안 솔루션의 진화

2000년대 후반부터 빅데이터 기술이 발전하면서, 데이터베이스에 저장되는 데이터의 양이 기하급수적으로 증가하였다. 빅데이터 환경에서는 대량의 데이터를 빠르게 처리하고 분석하는 것이 중요하지만, 동시에 데이터 보안의 중요성도 크게 증가하였다. 데이터 유출이나 무단 접근으로 인해 빅데이터가 악용될 경우, 기업은 막대한 경제적 손실과 법적 문제에 직면할 수 있다. 이에 따라 빅데이터 환경에서도 데이터를 안전하게 보호하기 위한 보안 솔루션이 필요하게 되었다. 예를 들어, Hadoop과 같은 빅데이터 플랫폼은 다양한 보안 기능을 제공하여 데이터를 보호하고 있다. Hadoop은 Kerberos 인증을 통해 데이터 접근을 제어하고, HDFS(Hadoop Distributed File System)를 통한 데이터 암호화를 제공하여 데이터의 기밀성을 유지한다. 또한, Apache Ranger와 같은 데이터 보안 프레임워크는 Hadoop 클러스터 내 데이터 접근을 실시간으로 모니터링하고, 보안 정책을 적용하여 데이터의 안전성을 강화하고 있다. 이러한 보안 솔루션은 빅데이터 환경에서 데이터베이스 보안의 중요성을 강조하며, 데이터 보호의 새로운 기준을 제시하고 있다.

클라우드 컴퓨팅 환경에 특화된 데이터베이스 보안 솔루션 종류

종류	목적	기능
데이터 마스킹	민감한 데이터를 보호하기 위해 데이터의 일부를 가림	데이터베이스 내 특정 데이터 요소를 마스킹
데이터 익명화	개인 식별 정보를 비식별화하여 프라이버시 보호	데이터에서 개인 식별 요소 제거 또는 변환
빅데이터 암호화	대량의 데이터를 암호화하여 보안 강화	빅데이터 저장 및 처리 시 암호화 적용
빅데이터 접근 제어	빅데이터 시스템에 대한 접근 권한 관리	사용자 및 역할 기반 접근 제어
빅데이터 감사 및 모니터링	빅데이터 활동을 추적하고 이상 징후 감지	로그 기록 및 실시간 모니터링

자료: 업계 자료, 한국IR협의회 기업리서치센터

다수의 기업의 데이터베이스 보안 솔루션 시장에서 자리매김하기 위해 노력 중

개별 기업, 공공기관, 금융기관들은 중요한 데이터를 보호하기 위해 강력한 보안 솔루션을 필요로 하고 있음

시장 조사 기관 Market Reports World에 따르면, 글로벌 데이터베이스 보안 시장 규모는 2022년 73억 달러에서 연평균 10.9% 성장해 2028년 134억 달러까지 커질 것으로 예상된다. 이러한 성장은 한국뿐만 아니라 해외에서도 다수의 기업들이 이 시장에서 자리매김하기 위해 적극적으로 노력하는 중요한 이유가 되고 있다. 데이터가 핵심 자산으로 인식됨에 따라, 개별 기업, 공공기관, 금융기관들은 중요한 데이터를 보호하기 위해 강력한 보안 솔루션을 필요로 하고 있다. 데이터 유출 사건과 엄격한 데이터 보호 법률이 등장하면서 데이터베이스 보안의 중요성은 더욱 강조되고 있다. 글로벌 시장의 주요 플레이어로는 오라클(Oracle), IBM, 사이베이스(Sybase), 펜타시큐리티(Penta Security), 트렌드마이크로(Trend Micro) 등이 있다. 이들은 모두 데이터베이스 보안 솔루션 분야에서 강력한 입지를 다지고 있으며, 지속적인 연구 개발과 혁신을 통해 시장 점유율을 확대하고 있다. 예를 들어, 오라클은 Oracle Advanced Security를

통해 다양한 산업에서 데이터 암호화와 접근 제어를 강화하고 있으며, IBM은 Guardium 솔루션을 통해 실시간 데이터 모니터링과 보안 관리 기능을 제공하여 시장에서의 리더십을 유지하고 있다. 이처럼 다양한 기업들이 데이터베이스 보안 솔루션 시장에서 경쟁하는 이유는 이 시장의 성장 가능성이 매우 크기 때문이다. 데이터베이스 보안 솔루션은 금융, 의료, 제조, 공공 기관 등 다양한 산업에서 필수적인 요소로 자리 잡고 있으며, 데이터 보호와 관련된 규제와 법률이 강화되면서 그 수요는 꾸준히 증가하고 있다. 글로벌 데이터베이스 보안 솔루션 시장은 데이터 보호의 중요성이 갈수록 강조되면서 지속적인 성장이 예상된다. 기업들은 이러한 시장 성장의 기회를 포착하여 혁신적인 보안 솔루션을 개발하고, 시장에서의 입지를 강화하기 위해 노력하고 있다.

오라클은 글로벌 데이터베이스 및 소프트웨어 솔루션 제공 업체

오라클: 글로벌 데이터베이스 및 소프트웨어 솔루션 제공 업체로, 특히 데이터베이스 관리 시스템(RDBMS) 분야에서 선도적인 위치를 차지하고 있다. 오라클은 데이터 보안 솔루션에서도 높은 신뢰성을 바탕으로 다양한 제품을 제공하고 있으며, 그 중 Oracle Advanced Security는 데이터베이스의 암호화와 접근 제어 기능을 강화하여 데이터 보호를 철저히 관리한다. 동 솔루션은 금융, 의료, 정부 기관 등 민감한 데이터가 다루어지는 여러 산업에서 필수적인 보안 수단으로 활용되고 있다. 오라클은 또한 클라우드 환경에서의 데이터 보안 솔루션을 강화하여, 다양한 클라우드 플랫폼에서 데이터의 안전한 저장과 전송을 보장하고 있다. 이러한 종합적인 데이터 보안 솔루션은 오라클이 글로벌 데이터베이스 보안 시장에서 강력한 경쟁력을 유지하게 하는 주요 요소이다.

IBM은 데이터베이스 보안 솔루션 분야에서 신뢰성과 안정성을 갖춘 다양한 제품을 제공

IBM: 데이터베이스 보안 솔루션 분야에서 신뢰성과 안정성을 갖춘 다양한 제품을 제공하며, 전 세계적으로 인정받는 IT 서비스 제공 업체이다. IBM의 Guardium 솔루션은 데이터베이스 보안, 실시간 데이터 모니터링, 및 규제 준수를 위한 기능을 포함하여, 데이터 보안의 전반적인 관리를 가능하게 한다. 동 제품은 데이터베이스에 대한 비정상적인 접근을 실시간으로 탐지하고, 민감한 데이터에 대한 보호를 강화하며, 규제 요구 사항을 준수하는 데 중요한 역할을 한다. IBM은 또한 인공지능(AI)과 머신러닝을 활용한 보안 분석 기술을 통해, 위협에 대한 빠르고 효율적인 대응을 가능하게 함으로써 데이터베이스 보안 분야에서의 혁신을 이어가고 있다.

사이베이스는 데이터베이스 관리 및 데이터 보안 솔루션에서 오랜 역사를 가진 기업

사이베이스: 데이터베이스 관리 및 데이터 보안 솔루션에서 오랜 역사를 가진 기업으로, SAP에 인수된 후에도 여전히 강력한 데이터베이스 보안 솔루션을 제공하고 있다. SAP Sybase ASE와 SAP Sybase IQ는 데이터 암호화와 접근 제어를 포함한 종합적인 데이터 보안 기능을 제공하며, 특히 대규모 데이터 처리 환경에서의 보안 요구를 충족시키는 데 초점을 맞추고 있다. 사이베이스의 솔루션은 다양한 산업에서 사용되며, 특히 금융 서비스와 공공 부문에서 민감한 데이터를 안전하게 관리하는 데 중점을 두고 있다. 이러한 전문성과 신뢰성은 사이베이스가 글로벌 데이터베이스 보안 시장에서 지속적인 성장을 이루는 데 기여하고 있다.

펜타시큐리티는 데이터베이스와 웹 보안 솔루션을 제공하는 글로벌 보안 업체

펜타시큐리티: 데이터베이스와 웹 보안 솔루션을 제공하는 글로벌 보안 업체로, 특히 아시아 시장에서 강력한 입지를 다지고 있다. 동사의 D'Amo 제품군은 데이터베이스 암호화와 접근 제어를 위한 솔루션으로, 다양한 산업에서 민감한 데이터를 보호하는 데 필수적인 역할을 한다. 펜타시큐리티는 또한 클라우드 환경에서도 효율적인 보안 솔루션을 제공하여, 데이터가 클라우드로 전송되고 저장되는 동안 발생할 수 있는 다양한 보안 위협에 대응하고 있다. 펜타시큐리티의 제품은 금융, 의료, 제조 등 다양한 산업에서 신뢰할 수 있는 보안 솔루션으로 평가받고 있으며, 이로 인해 글로벌 시장에서도 그 영향력을 확대하고 있다.

트렌드마이크로는 사이버 보안 솔루션을 제공하는 글로벌 선도 기업

트렌드마이크로: 사이버 보안 솔루션을 제공하는 글로벌 선도 기업으로, 데이터베이스 보안 솔루션에서도 강력한 제품군을 보유하고 있다. 동사의 Trend Micro Database Security는 데이터베이스 환경의 취약점을 탐지하고, 실시간으로 위협을 차단하는 기능을 갖추고 있다. 특히 트렌드마이크로는 클라우드와 하이브리드 환경에서의 데이터 보호를 중점으로 하여, 다양한 클라우드 플랫폼에서의 데이터 보안을 강화하고 있다. 트렌드마이크로의 솔루션은 빠른 배포와 실시간 모니터링을 가능하게 하여, 기업들이 데이터 보안에 대한 규제 요구 사항을 효율적으로 준수할 수 있도록 돕는다. 이러한 기능적 강점은 트렌드마이크로가 글로벌 데이터베이스 보안 시장에서 중요한 위치를 차지하게 하는 요인이다.

안랩은 대한민국의 대표적인 보안 소프트웨어 기업으로, 다양한 정보 보안 솔루션을 제공

안랩: 대한민국의 대표적인 보안 소프트웨어 기업으로, 다양한 정보 보안 솔루션을 제공하고 있다. 데이터베이스 보안 분야에서 안랩은 DB 접근 제어 및 암호화 솔루션을 통해 데이터의 안전성을 강화하고 있다. 특히, 안랩의 AhnLab DB Security는 기업의 중요한 데이터를 보호하기 위한 강력한 보안 기능을 제공하며, 데이터베이스에 대한 불법 접근을 실시간으로 감지하고 차단하는 기술력을 갖추고 있다. 또한, 클라우드 환경에서도 유연하게 적용 가능한 솔루션을 통해 다양한 산업군에서 활용되고 있다. 안랩은 이와 같은 기술력을 바탕으로 국내뿐만 아니라 아시아, 북미 등 글로벌 시장에서도 영향력을 확대하고 있으며, 지속적인 연구개발 투자로 경쟁력을 유지하고 있다.

윈스는 네트워크 및 데이터베이스 보안 솔루션을 전문으로 제공하는 기업

윈스: 네트워크 및 데이터베이스 보안 솔루션을 전문으로 제공하는 기업으로, 네트워크 보안 및 데이터베이스 보안 분야에서 강력한 입지를 보유하고 있다. 윈스의 대표 제품인 Sniper DB는 데이터베이스에 대한 접근 제어와 데이터 암호화 기능을 제공하여 데이터 유출 방지와 무결성 보장을 목표로 하고 있다. 또한, 윈스는 네트워크 침입 탐지 시스템(IDS)과 침입 방지 시스템(IPS)을 통해 데이터베이스 접근을 보다 정밀하게 모니터링하고 차단할 수 있는 기능을 강화하고 있다. 윈스는 이러한 종합적인 보안 솔루션을 통해 공공기관 및 대기업을 중심으로 신뢰를 구축해왔다. 글로벌 시장에서는 특히 아시아와 중동 지역에서 성장세를 보이고 있으며, 데이터 보안 분야의 선두주자로 자리매김하고 있다.

지란지교시큐리티는 다양한 IT 보안 솔루션을 제공하는 기업

지란지교시큐리티: 다양한 IT 보안 솔루션을 제공하는 기업으로, 데이터베이스 보안 및 클라우드 보안 솔루션에서 두각을 나타내고 있다. 동사의 Jiransoft DB Security는 데이터베이스 접근 제어와 데이터 암호화 기능을 통합적으로 제공하여 기업의 데이터를 안전하게 보호한다. 특히, 지란지교시큐리티는 클라우드 환경에서도 적용 가능한 클라우드 데이터 보호 솔루션을 개발하여 데이터의 기밀성을 유지하고, 데이터 유출을 방지하는 데 중점을 두고 있다. 동사는 또한, 클라우드 기반의 보안 솔루션을 통해 중소기업 및 대기업을 대상으로 시장을 확대하고 있으며, 기술력을 바탕으로 국내외에서 경쟁력을 강화하고 있다.

이글루는 사이버 보안 및 데이터베이스 보안 솔루션을 전문으로 제공하는 기업

이글루: 사이버 보안 및 데이터베이스 보안 솔루션을 전문으로 제공하는 기업으로, 통합 보안 관리 시스템(SIEM)과 데이터베이스 보안 솔루션을 제공하고 있다. 동사의 Igloo DB Secure는 데이터베이스에 대한 접근 제어와 데이터 암호화 기능을 통합하여 기업의 데이터를 안전하게 보호한다. 이글루는 데이터베이스 보안 외에도 보안 정보 및 이벤트 관리(SIEM) 솔루션을 통해 기업의 전체적인 보안 상태를 실시간으로 모니터링하고 분석할 수 있도록 지원하고 있다.

하나의 지배적인 기업이 시장을 완전히 장악하는 경우는 거의 없음

데이터베이스 보안 솔루션 분야는 매우 다양한 요구와 환경에 따라 여러 기업이 각각의 특화된 솔루션을 제공해야 하기 때문에, 하나의 지배적인 기업이 시장을 완전히 장악하는 경우는 거의 없다. 데이터베이스 보안은 금융, 의료, 정부기관, 대기업 등 여러 산업에서 각기 다른 요구를 충족해야 하며, 이에 따라 맞춤형 솔루션이 필요하다. 또한, 기술 발

전 속도가 빠르고, 보안 위협도 지속적으로 변화하기 때문에 다양한 접근 방식과 혁신이 요구된다. 이러한 특성으로 인해 데이터베이스 보안 시장은 여러 기업이 각기 다른 강점을 바탕으로 경쟁하는 다각적인 구조를 형성하게 되었다.

다양한 기업들이 경쟁하는 이유는 각 산업마다 요구되는 보안 솔루션이 다르기 때문

예를 들어, 오라클(Oracle)과 IBM은 대규모 엔터프라이즈 환경에서의 보안을 강화하는 솔루션을 제공하며, 고도화된 기능과 안정성을 자랑한다. 이와는 달리, 펜타시큐리티(Penta Security)와 트렌드마이크로(Trend Micro)는 클라우드와 하이브리드 환경에 특화된 보안 솔루션을 제공하여, 데이터가 다양한 플랫폼에서 안전하게 보호될 수 있도록 한다. 사이베이스(Sybase)는 대규모 데이터 분석과 처리에 중점을 둔 솔루션을 제공하여, 빅데이터 환경에서의 데이터 보안을 강화하고 있다.

이러한 다양한 기업들이 경쟁하는 이유는 각 산업마다 요구되는 보안 솔루션이 다르기 때문이다. 예를 들어, 금융 산업에서는 엄격한 데이터 무결성과 실시간 모니터링이 중요하며, 의료 산업에서는 환자 데이터의 기밀성 유지와 규제 준수가 필수적이다. 이처럼 산업별로 특화된 요구가 존재하기 때문에, 하나의 기업이 모든 요구를 충족하는 것은 거의 불가능하다.

이런 환경은 신시웨이와 같은 중소기업에게는 큰 기회가 된다. 신시웨이는 특정 산업이나 니치 마켓을 타겟으로 하여 맞춤형 솔루션을 개발하고 제공함으로써, 대형 기업들이 다루기 어려운 세부 시장에서의 입지를 강화할 수 있다. 예를 들어, 신시웨이는 공공기관과 중소기업을 대상으로 데이터베이스 접근 제어 및 암호화 솔루션을 제공하여, 이들 기업의 데이터 보안 요구를 충족하고 있다. 신시웨이는 이러한 시장에서 빠르게 적응하고 고객의 구체적인 요구를 반영한 솔루션을 제공함으로써, 매출을 성장시키고 고객 기반을 확장할 수 있다.

투자포인트

1 비정형 데이터 암호화 솔루션에서 높은 기술력 확보

GS인증 최고 등급인 1등급을 획득했고 국내 주요 금융권과 공공기관에 비정형 파일 암호화 솔루션을 공급

신시웨이는 비정형 파일 암호화 분야에서 높은 기술력을 확보한 기업이다. 비정형 데이터 암호화 솔루션 '페트라 파일 사이퍼 V3.2'를 통해 한국정보통신기술협회(TTA)로부터 GS인증 최고 등급인 1등급을 획득했다. GS(Good Software)인증은 소프트웨어 제품의 품질을 보증하고 소프트웨어 개발 기업의 판로를 지원하기 위해 시행되는 제도로, 과학기술정보통신부 고시에 따라 소프트웨어의 품질을 인증하는 제도이다. 문서심사만으로 인증을 부여하는 타 인증제도와는 달리 실제 운영환경과 유사한 시험환경에서 기능성, 신뢰성, 효율성, 사용성, 유지보수성, 이식성, 상호운용성 등에 관한 체계적인 시험 평가를 통해 SW 제품의 품질을 인증하는 제도이다. GS 인증마크 획득 제품의 경우, 정부 및 공공기관이 우선적으로 구매하게 된다.

페트라 파일 사이퍼는 에이전트(Agent)와 API 방식을 통해 비정형 파일 암호화를 지원하는 솔루션이다. 에이전트는 서버에 설치되어 특정 작업을 수행하는 소프트웨어 컴포넌트로, 이미지, 로그 파일, 녹취 파일 등 다양한 형식의 비정형 데이터를 실시간으로 암호화할 수 있다. API(Application Programming Interface) 방식은 애플리케이션이 특정 기능을 수행할 수 있도록 제공되는 인터페이스로, 애플리케이션 서버에 암·복호화 라이브러리를 설치하여 프로그램의 수정 없이 효율적인 암호화 관리를 가능하게 한다.

또한 페트라 파일 사이퍼에서는 SAM(Sequential Access Method: 데이터를 순차적으로 접근하는 방식으로 저장) 파일, CSV(Comma-Separated Values: 데이터 값을 쉼표로 구분하여 저장하는 형식 파일) 등 일정한 형식을 갖춘 파일들의 특정 영역 및 패턴 정보를 통한 암호화도 가능하다. 한편, 스케줄링을 기반으로 한 에이전트 방식, 즉, 서버에 설치된 에이전트 소프트웨어가 정해진 시간이나 주기에 따라 자동으로 작업을 수행하는 방식을 통해 파일을 실시간으로 암호화할 뿐 아니라, 프로그램의 API 수정을 최소화 (기존 애플리케이션의 코드를 크게 변경하지 않고도 API를 활용하여 필요한 기능을 추가하거나 수정)하여 효율적인 암호화 관리를 가능하게 한다. 또한, API 방식을 통해 애플리케이션 서버에 암·복호화 라이브러리를 설치함으로써 성능 부하를 최소화하고 애플리케이션 및 배치(Batch) 프로그램의 보안성과 안정성을 보장한다.

신시웨이는 NH농협은행, 농협중앙회, 우리은행, 우리카드, IBK기업은행, 고용정보원 등 국내 주요 금융권과 공공기관에 비정형 파일 암호화 솔루션을 공급하며, 기술력과 신뢰성을 인정받아 왔다. 신시웨이는 비정형 데이터 암호화 분야에서의 높은 기술력과 신뢰성을 바탕으로, 지속적인 기술 개발과 시장 확대를 통해 데이터 보안 산업에서의 입지를 더욱 강화해 나가고 있다. 최근에는 클라우드 SaaS 모델 개발에 주력하고 있으며, 이를 통해 통합 데이터 보안 시장을 선도하기 위해 노력 중이다. 페트라 파일 사이퍼를 포함한 페트라 사이퍼 솔루션 제품군은 2023년에 22억 원의 매출 달성에 기여했다. 전사 매출 (105억 원)의 21%의 비중에 해당한다.

2 2017년부터 클라우드 사업에 진출해 점진적으로 성과 드러내고 있어

클라우드 마켓플레이스에서 데이터베이스(DB) 접근제어와 정형 및 비정형 암호화 서비스를 제공

신시웨이는 지난 2017년 KT 클라우드 마켓플레이스를 시작으로 현재 10여 개의 마켓플레이스에서 데이터베이스(DB) 접근제어와 정형 및 비정형 암호화 서비스를 제공하고 있다. 코로나 19 팬데믹 이후 다수의 클라우드 파트너들과 유기적인 협력 관계를 맺으며 클라우드 DB 보안 밸류체인 구축에 나섰고, 개인정보와 민감정보를 보유한 기업들이 클라우드 환경으로 전환함에 따라 클라우드 환경에 적합한 보안 솔루션의 중요성도 함께 부각되고 있다.

클라우드 환경 변화에 선제적으로 대응하기 위해 신시웨이는 '클라우드개발팀', '클라우드QA팀', '클라우드전략기획팀' 등을 조직하여 적극 나서고 있다. 또한, 지속적인 매출 확대와 클라우드 시장 선점을 위해 연구개발(R&D)과 클라우드 인재 양성을 위한 투자를 지속적으로 확대하고 있으며, 국내 주요 클라우드 서비스 제공자(CSP)와의 공동 마케팅도 활발하게 진행하면서 적극적인 시장 공략에 나서고 있다.

신시웨이의 클라우드 솔루션은 업계 유일의 DB 접근제어와 DB 암호화를 클라우드 환경에서 서비스하며 솔루션 간의 연동을 통해 강력한 보안 서비스를 제공한다. DB 서버 사양과 시스템 규모에 따른 효율적인 가격정책(Standard, Enterprise)을 운영하며, 아마존 AWS, 마이크로소프트 AZURE, NCP (Naver Cloud Platform), KT, 가비아 등 다양한 퍼블릭 클라우드 환경을 지원한다. 이러한 노력의 결과로, 2023년 기준 클라우드 솔루션에서 19.6억 원의 매출을 기록했고, 2024년 1분기에는 4.1억 원의 매출을 달성하며 단일 솔루션 매출로는 유의미한 성과를 보였다.

3 고성능 보안 리파지토리 (Repository) 기술로 메모리 기반 빠른 처리 속도 구현

메모리 기반 DBMS(SOAH)는 데이터를 저장 장치인 디스크가 아닌 메모리에 저장하여 빠른 데이터 처리 속도를 제공하는 시스템

신시웨이 부설연구소는 고성능 보안 리파지토리 (Repository) 기술을 통해 메모리 기반 DBMS(SOAH: Security Optimized in-memory Architecture for High-speed SQL processing의 약자로 고속 SQL 처리를 위한 보안 최적화 메모리 아키텍처 의미)를 개발하여, SQL 고속 처리 및 비인가 사용자의 데이터 접근과 위/변조를 방지하는 기능을 구현하였다. 고성능 보안 리파지토리 (Repository) 기술은 데이터의 보안성, 처리 속도, 관리 효율성, 개발의 유연성 등 여러 측면에서 중요한 역할을 하는데, 메모리 기반 DBMS(SOAH)는 데이터를 저장 장치인 디스크가 아닌 메모리에 저장하여 빠른 데이터 처리 속도를 제공하는 시스템으로, 대규모 데이터의 신속한 접근과 처리가 가능하다.

이로 인해 정책 (데이터베이스 접근, 보안, 로그 관리 등과 관련된 규칙이나 규정)의 빠른 적용과 대용량 로그의 신속한 처리가 가능하며, 로그 파티셔닝 기능을 통해 검색 속도를 향상시킨다. 로그 파티셔닝 기능은 로그 데이터를 여러 파티션으로 나누어 저장하여 검색 및 관리 효율성을 극대화하는 기술이다.

또한, 메모리 주소 접근 방식 외에도 SQL 및 프로시저 프레임워크 기반의 외부 인터페이스를 제공하여 효율적인 사용자 서비스 개발 환경을 지원한다. 즉, 사용자들이 표준화된 SQL 언어와 절차를 통해 데이터베이스와 상호 작용할 수 있어 개발의 편리성과 유연성을 제공한다는 의미이다. 이러한 혁신적인 기술력은 데이터베이스 로그 정보 관리 장치 및 방법, 개인정보 데이터베이스의 접근 관리 등 다양한 특허로 인정받아, 신시웨이가 데이터 보안 분야에서 선도적인 위치를 차지하는 데 기여하고 있다. 신시웨이의 고성능 보안 리파지토리 (Repository) 기술은 타사의 기술 대비 뛰어난 성능과 안정성을 자랑하며, 특히 대용량 데이터를 빠르게 처리하고 높은 보안성을 유지하는 점에서 탁월하다.

메모리 기반 데이터베이스 관리와 디스크 기반 데이터베이스 관리 비교

종류	디스크 기반 DBMS	메모리 기반 DBMS
데이터 저장	데이터는 주로 디스크에 저장	데이터는 주로 메모리에 저장
데이터 접근 속도	디스크 I/O 작업 필요, 속도 느림	메모리 접근, 속도 빠름
캐싱	자주 사용되는 데이터를 메모리에 캐싱	일부 시스템에서 추가적인 디스크 백업
데이터 처리 속도	디스크 접근으로 인해 상대적으로 느림	메모리 접근으로 인해 매우 빠름
휘발성	전원이 끊겨도 데이터가 보존됨	전원이 끊기면 데이터가 손실될 수 있음
주요 용도	대량의 데이터 영구 저장 및 관리	실시간 데이터 처리, 고속 연산 필요 시
데이터 보존	디스크에 데이터 영구 보존	주기적으로 디스크에 백업 필요

자료: 업계 자료, 한국IR협의회 기업리서치센터

실적 추이 및 전망

1 2023년 실적 리뷰

매출은 증가했지만 영업이익은 감소했고 합병비용으로 인해 소폭의 당기순손실 발생

신시웨이의 2023년(제19기) 매출은 전년 대비 7.58% 증가한 105억 원을 기록했다. 매출은 창사 이래 역대 최고 실적이며 처음으로 100억 원대 수준에 해당한다. 매출이 증가한 이유는 주요 제품 매출 중에서 페트라 클라우드 매출이 20억 원에 근접한 매출 (19.6억 원)을 시현했기 때문이다. 아울러 용역/유지보수 매출이 늘어난 것도 전사 매출 성장에 기여했다. 매출이 증가했지만 영업이익은 전년 대비 27.91% 감소한 15억 원을 기록했다. 영업이익이 감소한 이유는 다수의 소프트웨어 프로젝트를 수행하는 과정에서 지급수수료와 기술지원료가 늘어났기 때문이다. 한편, 영업외손익에서는 기타비용이 크게 발생했다. 2023년 10월 12일 주식회사 신시웨이와 아이비케이에스제17호기업인수목적 주식회사의 합병으로 인하여 18.5억 원이 기타비용에 계상되었다. 이와 같은 비용은 코스닥 시장 상장 전후에 발생한 비용이므로 2024년 실적에는 크게 영향을 끼치지 않을 것으로 전망된다. 합병비용이 영업이익보다 크다 보니 2023년에 소폭의 당기순손실이 발생한 점은 아쉽다. 재무적인 측면에서는 부채비율 20.3%, 자기자본비율 83.1%로 안정적인 재무구조를 유지했다.

신시웨이 실적 추이 및 전망 (단위: 억 원, %, 원)

구분	2021	2022	2023	2024F
매출액	79	97	105	120
YoY(%)	8.0	23.7	7.6	15.0
솔루션 성격별 매출				
PETRA	31.0	32.3	30.8	35.4
PETRA CIPHER	11.2	22.3	22.2	25.5
PETRA Cloud	9.6	14.2	19.6	22.5
용역(유지보수)	26.0	28.0	31.6	36.3
서비스	0.2	0.2	0.4	0.5
기타	0.3	0.2	0.1	0.1
영업이익	11	21	15	16
YoY(%)	36.9	100.1	-27.9	7.4
OP 마진(%)	13.5	21.9	14.7	13.7
순이익 (억원)	10	18	-0	29
EPS (원)	279	496	-5	769
YoY(%)	17.4	78.1	적전	흑전
ROE (%)	10.4	16.3	-0.1	14.3
자본총계	101	120	191	220
BPS	2,788	3,314	5,246	5,669
YoY(%)	N/A	N/A	N/A	8.1
부채비율	64.4	43.8	20.3	19.6

자료: 신시웨이, 한국IR협의회 기업리서치센터

2024년 실적 전망

매출은 10% 이상 증가하지만 영업이익은 한 자릿수 성장

신시웨이의 2024년 1분기 매출액 18억 원으로 전년 동기 대비 18.2% 증가했다. 동 기간 영업이익은 -3.2억 원으로 전년동기 대비 적자가 지속되었다. 관련 매출은 주요 고객의 차세대 관리시스템 개선 사업 및 국내 의료기관의 차세대 인프라 사업으로 전년 동기 대비 93.3% 증가한 3.2억 원을 달성했다. 암호화 매출은 국내 주요 공공기관의 보안 시스템 구축 사업 등을 수주하며 35.1% 증가한 3.9억 원을 달성했다. 소프트웨어 매출의 36.8%의 비중을 차지하는 클라우드 매출 또한 지속적으로 순항 중이다. 신시웨이는 네이버 클라우드 플랫폼 (NCP), 케이티 클라우드 (KT Cloud), 엔에이치엔 클라우드 (NHN Cloud) 등 국내 주요 클라우드 서비스 공급업체 (CSP)가 운영하는 마켓플레이스에서 DB 접근제어와 DB 암호화 서비스를 제공하고 있다.

신시웨이의 클라우드 고객사향 매출 증가에 힘입어 2024년 매출은 전년 대비 15.0% 증가한 120억 원으로 기대된다. 다만, 영업이익은 전년 (15억 원) 대비 소폭 증가한 16억 원으로 추정된다. 연구개발인력 채용으로 인한 급여 증가 때문이다. 이는 공시된 분기보고서 중에서 "비용의 성격별 분류" 항목을 통해 어느 정도 가늠할 수 있다. 2024년 1분기 매출원가와 판매관리비 합계는 21.3억 원인데 그중에서 종업원 급여는 11.7억 원으로 50% 내외를 기록했다. 2023년 1분기 8.5억 원 대비 37% 증가했다. 연구개발 인력의 경상적인 연구개발은 주로 DB 보안 위협에 대응하기 위한 서비스 고도화를 목적으로 전개되고 있지만, 신규사업인 PETRA Cloud SaaS 제품과 PETRA Secure CPS 사업을 위해 연구개발인력 관련 지출이 늘어났다. PETRA Cloud SaaS 제품은 퍼블릭 클라우드와 연동 가능한 페트라와 페트라 사이퍼 제품군을 포함하고 있으며, PETRA Secure CPS는 블록체인 기반의 DID(분산 신원 증명) 발급 및 데이터 접근 권한 증명 솔루션이다. 이처럼 클라우드 솔루션 및 블록체인 기반 솔루션 관련 연구개발로 인해 2024년 영업이익은 전년 대비 제한적으로 증가하는 것으로 추정된다.

Valuation

투자자들의 전반적인 무관심이 아쉽지만, 신시웨이는 저평가 국면을 쉽게 벗어날 수 있을 것

퍼블릭 클라우드 관련 솔루션 매출 성장 및 안정적 재무구조가 긍정적

신시웨이의 2024년 추정 실적 기준 P/E는 11.8배이다. 동종 업종 또는 유사 업종의 안랩, 윈스, 지란지교시큐리티, 이글루의 P/E는 2024년 추정 실적 기준으로 존재하지 않아 신시웨이의 밸류에이션과 비교하기 어렵다. 소프트웨어 업종 중에서 인공지능 관련된 분야 위주로 투자자들이 관심을 갖고 있으며 데이터베이스 보안 솔루션 관련 기업에 관해서는 상대적으로 투자자들의 관심이 적다 보니 커버리지 애널리스트도 거의 없어서 안랩, 윈스, 지란지교시큐리티, 이글루의 2024년 실적 추정치가 존재하지 않는다.

아쉽지만 이들 기업의 2023년 확정 실적 기준 P/E 밸류에이션을 살펴보면 각각 19.2배, 8.0배, 3.2배, 7.9배이다. 그중에서 지란지교시큐리티가 2023년에 일회성 요인으로 당기순이익이 118억 원을 기록했기 때문에 P/E 밸류에이션이 유난히 낮다는 점을 감안하더라도 안랩, 윈스, 지란지교시큐리티, 이글루의 P/E 밸류에이션이 코스닥 지수(43.4배) 또는 동종 업종 (Oracle 25.0배, International Business Machines 17.8배) 대비 낮다는 것을 확인할 수 있다. 전술했던 바와 같이 소프트웨어 업종 중에서 인공지능 관련된 분야는 상대적으로 큰 관심을 받지만 안랩, 윈스, 지란지교시큐리티, 이글루가 인공지능 관련 기업이라고 보기는 어렵기 때문이다.

신시웨이도 역시나 저평가된 상태이다. 2023년 11월에 SPAC 합병을 통해 상장한지 1년이 채 지나지 않았기 때문에 코스닥 시장에 직상장한 기업 대비 상대적으로 소외되었다. 그럼에도 불구하고 신시웨이는 동종 업종에서도 저평가 국면을 쉽게 벗어날 수 있을 것으로 사료된다. 그 이유는 첫째, 2023년에 이어 2024년에도 매출과 영업이익이 증가하고 있으며, 둘째, 전사 매출 중에 퍼블릭 클라우드와 연동 가능한 PETRA Cloud 매출 비중이 유의미하게 상승하고 있기 때문이다. 셋째, 부채비율이 낮아 재무적으로 탄탄하다는 점도 중요한 요인이다.

동종 업종의 실적 컨센서스 및 밸류에이션

(단위: 십억 원, 배, 십억 원, 현지통화, %)

기업명	매출액		영업이익		P/E	
	2023	2024F	2023	2024F	2023	2024F
코스피	3,532,364.4	2,863,620.6	173,770.8	268,439.4	17.3	11.2
코스닥	331,711.2	119,078.3	11,072.5	11,219.4	43.4	24.8
신시웨이	**10.5**	**12.0**	**1.5**	**1.6**	**N/A**	**11.8**
안랩	239.2	N/A	26.4	N/A	19.2	N/A
윈스	106.9	N/A	23.1	N/A	8.0	N/A
지란지교시큐리티	35.3	N/A	1.8	N/A	3.2	N/A
이글루	107.0	N/A	5.7	N/A	7.9	N/A
Oracle	70,257.4	79,368.9	20,367.1	34,984.4	25.0	22.4
International Business Machines	80,795.2	86,417.3	11,350.0	15,251.1	17.8	17.0

주 1) 안랩, 윈스, 지란지교시큐리티, 이글루의 실적 컨센서스가 존재하지 않음, 2) 지란지교시큐리티의 2023년 P/E는 3.2배로 유난히 낮은데 이는 일회성 요인으로 당기순이익이 118억 원을 기록했기 때문이며 매출과 영업이익은 각각 353억 원, 18억 원이었음

자료: QuantiWise, 한국IR협의회 기업리서치센터

동종 업종의 주가 수익률 비교

(단위: 십억 원, 배, 십억 원, 현지통화, %)

기업명	시가총액	종가	1주전대비 수익률	1개월전대비 수익률	3개월전대비 수익률	6개월전대비 수익률
코스피	2,174,071	2,755	+2.4%	+1.0%	+2.3%	+9.7%
코스닥	422,122	871	+2.4%	+2.0%	-2.1%	+5.1%
신시웨이	**35**	**9,100**	**-0.5%**	**-5.3%**	**-22.5%**	**-17.6%**
안랩	617	61,600	-0.5%	-5.2%	-9.0%	-15.6%
윈스	189	13,870	+3.4%	+7.7%	+8.2%	+12.4%
지란지교시큐리티	33	3,680	-2.5%	-15.4%	-3.3%	-12.2%
이글루	63	5,720	+2.9%	-7.4%	-12.0%	-8.8%
Oracle	526,985	140	+13.2%	+20.2%	+11.4%	+35.8%
International Business Machines	212,990	169	+0.5%	+0.9%	-14.0%	+3.4%

자료: QuantiWise, 한국IR협의회 기업리서치센터

리스크 요인

1 매출의 계절성 관련 위험

구독형 서비스의 비중을 증가시키며 매출의 계절성을 줄이기 위한 노력을 전개

신시웨이는 공공기관, 금융기관, 대기업부터 중소기업에 이르기까지 다양한 고객군을 확보하고 있다. 이러한 고객군의 특성상 매출은 계절성의 영향을 크게 받는다. 특히 공공기관의 경우, 연도별 예산 집행의 특성으로 인해 4분기에 집중적으로 보안 시스템에 대한 투자가 이루어지는 경향이 있다. 이는 연말까지 예산을 소진해야 하는 공공기관의 특성 때문이다. 따라서 신시웨이의 매출액은 분기별로 큰 차이를 보인다. 신시웨이가 2023년 코스닥 시장의 상장을 앞두고 제출했던 공시자료 기준, 최근 5개년 동안의 분기별 매출액 분포를 살펴보면, 1분기에는 매출의 16.41%, 2분기에는 19.80%, 3분기에는 21.20%, 그리고 4분기에는 42.60%가 발생했다. 이러한 분포는 매출이 하반기에 집중되어 있음을 나타내며, 이는 공공기관과 금융기관, 대기업의 시스템 개선 및 보안 투자 집행이 주로 하반기에 이루어지는 경향을 반영하고 있다. 한편, 신시웨이는 연간 단위 유지보수 계약과 PETRA Cloud와 같은 구독형 서비스의 비중을 증가시키며 매출의 계절성을 줄이기 위한 노력을 전개하고 있다. 이러한 서비스는 매월 일정한 매출을 발생시키기 때문에 계절성에 덜 민감하므로 신시웨이의 매출 안정성 측면이나 기업 가치 측면에서 긍정적 영향을 끼칠 것으로 기대된다.

2 신규 사업 관련 위험

블록체인 기술을 접목한 PETRA Secure CPS의 안정화 추진

신시웨이는 창업 이후 현재까지 데이터베이스 접근 제어 및 암호화 시장에서 안정적인 위치를 차지하고 있으며, 이를 바탕으로 클라우드 데이터베이스 보안 시장과 스마트 팩토리 내 데이터 보안 시장으로 진출을 시도 중이다. 이를 위해 신시웨이는 지속적으로 연구개발에 많은 시간과 자금을 투자해왔다. 특히, SaaS 형태의 PETRA Cloud 제품과 블록체인 기술을 접목한 PETRA Secure CPS의 안정화를 추가적인 인력과 자금 투자를 계획하고 있다. 동 기술 중에 PETRA Cloud 제품의 매출은 성장 궤도에 진입했다고 볼 수 있지만, 블록체인 기술을 접속한 제품의 경우 추가적인 안정화를 위한 연구개발이 이어져야 한다. 이러한 기술들이 성공적으로 정착되면 신시웨이의 사업 규모와 영역 확장에 크게 기여할 것으로 예상된다. 그러나 기술 상용화에 실패할 경우, 비용 손실이 발생하여 회사의 운영에 부정적인 영향을 미칠 가능성이 있다.

포괄손익계산서

(억원)	2020	2021	2022	2023	2024F
매출액	73	79	97	105	120
증가율(%)	6.8	8.0	23.7	7.6	15.0
매출원가	29	26	31	39	45
매출원가율(%)	39.7	32.9	32.0	37.1	37.5
매출총이익	44	53	66	65	75
매출이익률(%)	60.7	66.8	67.7	62.4	62.7
판매관리비	36	42	45	50	59
판관비율(%)	49.3	53.2	46.4	47.6	49.2
EBITDA	11	14	24	18	19
EBITDA 이익률(%)	15.5	18.0	24.6	17.3	15.9
증가율(%)	230.2	25.7	68.9	-24.2	5.6
영업이익	8	11	21	15	16
영업이익률(%)	10.7	13.5	21.9	14.7	13.7
증가율(%)	5,295.3	36.9	100.1	-27.9	7.4
영업외손익	-0	-0	-1	-16	3
금융수익	1	1	1	3	3
금융비용	1	2	2	1	1
기타영업외손익	0	0	0	-18	1
종속/관계기업관련손익	0	0	0	0	0
세전계속사업이익	8	10	20	-1	19
증가율(%)	1,644.1	35.4	96.7	적전	흑전
법인세비용	-1	0	2	-1	-10
계속사업이익	9	10	18	-0	29
중단사업이익	0	0	0	0	0
당기순이익	9	10	18	-0	29
당기순이익률(%)	11.8	12.9	18.5	-0.2	24.4
증가율(%)	227.9	17.4	78.1	적전	흑전
지배주주지분 순이익	9	10	18	-0	29

재무상태표

(억원)	2020	2021	2022	2023	2024F
유동자산	73	90	100	155	190
현금성자산	25	37	56	58	79
단기투자자산	26	32	13	74	85
매출채권	21	21	28	20	23
재고자산	0	0	0	0	0
기타유동자산	1	1	2	3	3
비유동자산	79	76	73	74	73
유형자산	51	45	48	45	44
무형자산	2	1	0	0	0
투자자산	17	17	13	14	15
기타비유동자산	9	13	12	15	14
자산총계	152	166	173	229	263
유동부채	19	60	50	28	32
단기차입금	0	0	10	0	0
매입채무	2	4	4	5	6
기타유동부채	17	56	36	23	26
비유동부채	39	5	3	11	11
사채	0	0	0	7	7
장기차입금	39	4	2	2	2
기타비유동부채	0	1	1	2	2
부채총계	58	65	53	39	43
지배주주지분	94	101	120	191	220
자본금	16	16	16	19	19
자본잉여금	9	10	10	78	78
자본조정 등	0	-4	-4	-4	-4
기타포괄이익누계액	0	1	0	0	0
이익잉여금	69	79	98	98	127
자본총계	94	101	120	191	220

현금흐름표

(억원)	2020	2021	2022	2023	2024F
영업활동으로인한현금흐름	8	27	20	27	32
당기순이익	9	10	18	-0	29
유형자산 상각비	3	3	2	3	3
무형자산 상각비	0	0	0	0	0
외환손익	0	0	0	0	0
운전자본의감소(증가)	-4	12	-3	4	1
기타	0	2	3	20	-1
투자활동으로인한현금흐름	-13	-6	18	-5	-12
투자자산의 감소(증가)	0	1	3	-0	-1
유형자산의 감소	0	0	0	0	0
유형자산의 증가(CAPEX)	-3	-1	-4	-1	-1
기타	-10	-6	19	-4	-10
재무활동으로인한현금흐름	-2	-10	-18	-20	0
차입금의 증가(감소)	-2	-5	-18	-19	0
사채의증가(감소)	0	0	0	0	0
자본의 증가	0	0	0	0	0
배당금	0	0	0	0	0
기타	0	-5	0	-1	0
기타현금흐름	-0	0	-0	0	0
현금의증가(감소)	-7	12	20	2	20
기초현금	32	25	37	56	58
기말현금	25	37	56	58	79

주요투자지표

	2020	2021	2022	2023	2024F
P/E(배)	0.0	0.0	0.0	N/A	11.8
P/B(배)	0.0	0.0	0.0	2.2	1.6
P/S(배)	0.0	0.0	0.0	4.0	2.9
EV/EBITDA(배)	N/A	N/A	N/A	16.7	10.5
배당수익률(%)	N/A	N/A	N/A	0.0	0.0
EPS(원)	237	279	496	-5	769
BPS(원)	2,592	2,788	3,314	5,246	5,669
SPS(원)	2,004	2,165	2,677	2,880	3,157
DPS(원)	0	0	0	0	0
수익성(%)					
ROE	9.6	10.4	16.3	-0.1	14.3
ROA	5.8	6.4	10.6	-0.1	11.9
ROIC	12.6	20.6	46.1	4.0	61.4
안정성(%)					
유동비율	391.0	149.2	200.4	551.4	588.7
부채비율	61.4	64.4	43.8	20.3	19.6
순차입금비율	-7.0	-28.8	-39.3	-63.8	-69.5
이자보상배율	7.6	10.5	21.8	16.4	27.5
활동성(%)					
총자산회전율	0.5	0.5	0.6	0.5	0.5
매출채권회전율	4.0	3.8	4.0	4.3	5.5
재고자산회전율	N/A	N/A	N/A	N/A	N/A

최근 3개월간 한국거래소 시장경보제도 지정 여부

시장경보제도란?

한국거래소 시장감시위원회는 투기적이거나 불공정거래 개연성이 있는 종목 또는 주가가 비정상적으로 급등한 종목에 대해 투자자주의 환기 등을 통해 불공 정거래를 사전에 예방하기 위한 제도를 시행하고 있습니다. 시장경보제도는 「투자주의종목 투자경고종목 투자위험종목」의 단계를 거쳐 이루어지게 됩니다.

※관련근거: 시장감시규정 제5조의2, 제5조의3 및 시장감시규정 시행세칙 제3조~제3조의 7

종목명	투자주의종목	투자경고종목	투자위험종목
신시웨이	X	X	X

Compliance notice

본 보고서는 한국거래소, 한국예탁결제원과, 한국증권금융이 공동으로 출연한 한국IR협의회 산하 독립 (리서치) 조직인 기업리서치센터가 작성한 기업분석 보고서입니다. 본 자료는 시가총액 5천억원 미만 중소형 기업에 대한 무상 보고서로, 투자자들에게 국내 중소형 상장사에 대한 양질의 투자 정보 제공 및 건전한 투자문화 정착을 위해 작성되었습니다.

- 당사 리서치센터는 본 자료를 제3자에게 사전 제공한 사실이 없습니다.
- 본 자료를 작성한 애널리스트는 자료작성일 현재 해당 종목과 재산적 이해관계가 없습니다.
- 본 자료를 작성한 애널리스트와 그 배우자 등 관계자는 자료 작성일 현재 조사분석 대상법인의 금융투자상품 및 권리를 보유하고 있지 않습니다.
- 본 자료는 중소형 기업 소개를 위해 작성되었으며, 매수 및 매도 추천 의견은 포함하고 있지 않습니다.
- 본 자료에 게재된 내용은 애널리스트의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 신의 성실하게 작성되었음을 확인합니다.
- 본 자료는 투자자들의 투자판단에 참고가 되는 정보제공을 목적으로 배포되는 자료입니다. 본 자료에 수록된 내용은 자료제공일 현재 시점의 당사 리서치센터의 추정치로서 오차가 발생할 수 있으며 정확성이나 완벽성은 보장하지 않습니다.
- 본 조사자료는 투자 참고 자료로만 활용하시기 바라며, 어떠한 경우에도 투자자의 투자 결과에 대한 법적 책임 소재의 증빙자료로 사용될 수 없습니다.
- 본 조사자료의 지적재산권은 당사에 있으므로, 당사의 허락 없이 무단 복제 및 배포할 수 없습니다.
- 본 자료는 텔레그램에서 "한국IR협의회(https://t.me/kirsofficial)" 채널을 추가하시어 보고서 발간 소식을 안내받으실 수 있습니다.
- 한국IR협의회가 운영하는 유튜브 채널 'IRTV'에서 1) 애널리스트가 직접 취재한 기업탐방으로 CEO인터뷰 등이 있는 '小中한탐방'과 2) 기업보고서 심층해설방송인 '小中한 리포트 가치보기'를 보실 수 있습니다.