보안

비중확대 (신규)

사이버 세계 속 나, 잘 부탁드립니다

신한투자증권
기업분석부

백지우 연구원
☎ 02-3772-2671
✉ 100jiwoo@shinhan.com

신한 리서치 투자정보

Contents

Investment Summary

생활 패러다임의 변화, 보안의 필요성 대두

코로나로 인한 비대면 문화의 확산, 사이버 보안의 중요성 증대

사이버보안 산업에 주목해야 할 시기이다. 2020년 이후 보안 산업은 코로나19로 인해 기업의 IT투자가 지연되며 수주 감소로 인한 지지부진한 시기를 겪었다. 하지만 이 시기는 코로나로 인해 재택근무가 확대되고, 비대면 문화가 대중화되며 오히려 사이버보안의 중요성을 일깨워주는 시기였다.

일상 속 크고 작은 사이버 위협의 증가, 원격근무 도입과 같은 디지털 트랜스포메이션, 이에 더해 정부의 사이버보안 산업 육성 규제 확대 및 지원으로 인해 2023년 사이버보안 업황 반등이 예상된다. 기업 또한 본격적으로 IT 및 보안 투자를 시작하며 보안 업체의 주가 반등이 시작되고 있어 주목이 필요하다.

시장의 성장, 수요의 확대, 정부 지원의 증가

대규모 해킹사건 다수 발발 → 정부의 보안 산업 육성 의지, 지원 활성화

1) 시장의 성장: 우크라이나-러시아 전쟁은 사이버 전쟁을 동반하며 보안은 더 이상 개인, 기업만을 보호하기 위한 수단이 아님을 증명했다. 국가 안보를 위협하는 사이버 해킹부터 LG유플러스 등 대기업 해킹까지 대규모 해킹 사례가 급증하고 있다. 과거부터 지속됐던 개인정보 해킹, 보이스피싱도 그 수법이 날로 교모해지며 피해규모가 증가하고 있다. 이와 같은 사이버위협의 증가로 기업, 개인모두 보안의 중요성을 인지하며 보안 시장은 지속 중이다.

2) 수요의 확대: 수요처가 다양해지고 있다. 과거 IT대기업, 일부 정부기관만 사이버보안에 관심을 가졌다면, 최근에는 다양한 산업군에서 보안 솔루션을 찾고 있다. 사이버 공간에서의 활동량이 많아지며 개인정보의 노출이 많아졌다. 민감한 개인정보를 보유하고 있는 결혼정보회사 등 모든 기업이 해킹에 취약할 수 있다. 또한 AI, 로봇 등 IT기기를 활용한 생산이 늘어나며 조립, 생산 공장에서도 해킹 피해가 발생할 수 있다. 가상화폐, 메타버스 등 새로운 산업도 등장하며 보안은 언제, 누구에게나, 어디서든 필요한 솔루션으로 자리매김했다.

3) 정부의 보안산업 육성의지: 정보보호 공시 의무화, 개인정보보호법 개정, 정보보호 인증 제도 개편 등 다양한 제도 및 규제를 개정하며 사이버 위협을 막기 위해 노력중이다. 과기정통부는 올해 정보보호 보안과 관련된 예산안으로 전년대비 200억원 가량 증가한 3,000억원을 편성했다. 이 외에도 중소기업을 위한 보안 솔루션 지원 등 다양한 정책을 마련하며 보안산업 육성의지를 보였다.

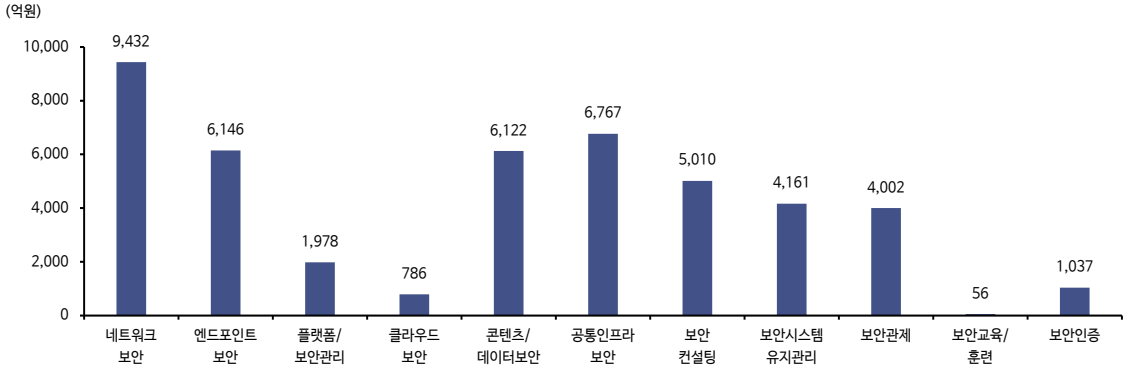
Top Pick: 지니언스, 관심주: 안랩, 파이오링크

NAC, EDR 국내 1위 사업자 지니언스 Top Pick 제시

정보보안 산업 Top Pick으로 지니언스를 제시한다. EDR, NAC 등의 보안 솔루션을 판매하는 업체로, 업황이 안좋은 시기에도 지속적으로 고객사 확대를 통한 매출 성장을 이뤄냈다. 1) EDR 등 신제품 투자가 마무리되며 영업이익률이 정상화될 예정이며, 2) 클라우드 NAC, EDR 등의 새로운 솔루션은 올해부터 매출 본격화가 기대된다. 보안 시장의 성장률을 뛰어넘는 성장을 기록할것으로 전망한다.

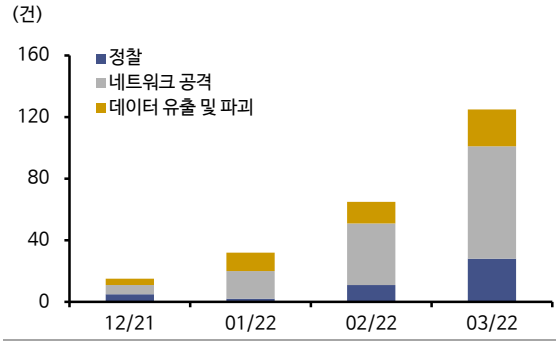
Key Charts

정보보안 산업 중분류 단위 매출액



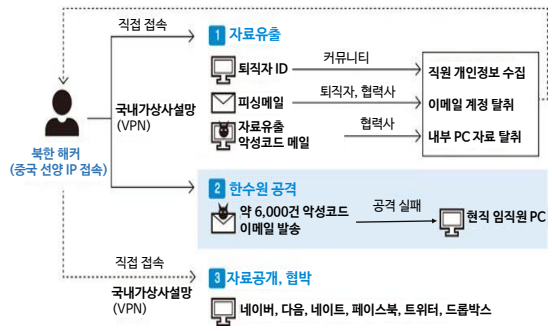
자료: 과기정통부, 신한투자증권

러시아의 우크라이나 사이버 공격 현황



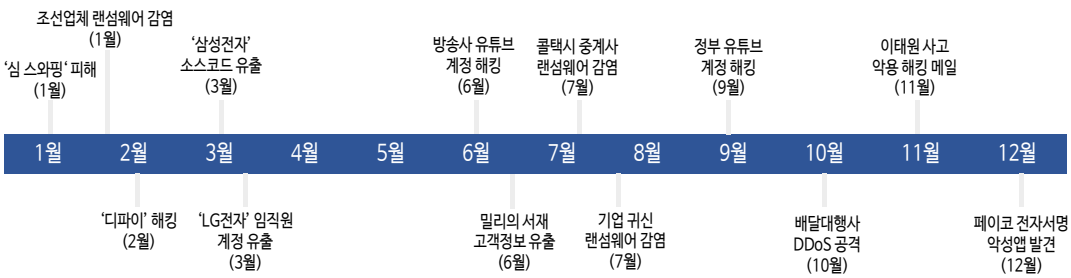
자료: 마이크로소프트 디지털보안부서, 신한투자증권

한국수력원자력 해킹 흐름도



자료: 신한투자증권

2022년 국내 사이버 위협 사례



자료: 신한투자증권

사물인터넷(IoT) 보안위협 사례

분류	내용
정보통신망 침입	- 보안수준이 낮은 기기를 노려 통신망 침입 - 가정 내 CCTV 해킹 등 범죄악용 가능성이 높음
디도스 공격	- IoT 기기를 디도스 공격의 좀비PC로 활용 - 공격 단말기 최대 수십억대까지 가능
악성 프로그램 유포	- IoT 기기를 활용한 악성프로그램 유포 가능 - 냉장고, TV 등 가전제품을 통한 스팸메일 발송 가능
데이터 침해	- 실시간 도청, 위치확인 등 사용자 정보 침입
IoT 이용 살상행위	- 자율주행차, 의료기기 해킹시 신체 위협 가능
기반시설 위협	- 스마트 전력망, 공항, 고속도로 등 기반시설 공격

자료: 경찰청, 신한투자증권

현정부의 사이버안보 관련 공약집

10. 사이버안보 위협 대처 능력을 제고하겠습니다.

현재

사이버안보는 안보, 경제, 정치, 사회안전이 중첩되는 초국경적 사안이므로 관련기관, 기업 및 외국과의 정보공유와 협력이 중요

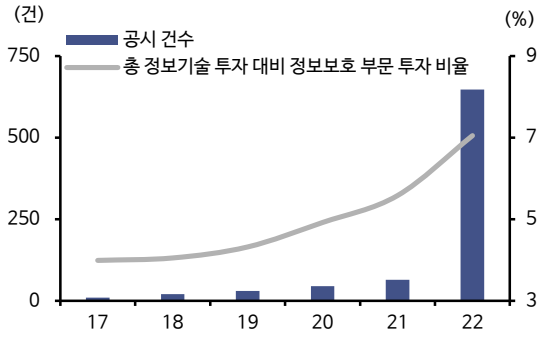
그럼에도 한국의 현 대응 체계는 국정원, 과기부, 외교부, 국방부, 경찰 등으로 분절되어 있어 정보공유와 협력을 통한 종합적 대응 불가

공약

1. 국가 차원의 일원화 된 사이버 대응 체계 구축
   - 국가사이버안보 대응 시스템 구축 및 민관군 통합 대응체계 강화
2. 사이버보안 인재양성
   - 불법적 사이버 공격에 실질적 방어가 가능한 실전형 인재 양성
   - 정부가 전국 지역별 정규과정 및 특수과정 설립 적극 지원
3. 사이버안보 기술 발전 및 기업 지원을 위한 사이버안보 생태계 조성
4. 국제 사이버 협력 네트워크 구축에 적극 참여
   - 사이버범죄 피해를 줄이기 위해 '부다페스트 사이버범죄협약' 가입
5. 사이버분야 무기체계 및 지원체계의 신속한 전력화 추진

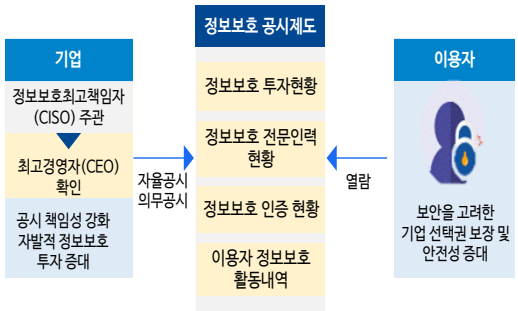
자료: 사이버안보기본법 제정 관련 공약집 발췌, 신한투자증권

의무공시 도입에 따른 공시건수 추이



자료: 과학기술정보통신부, 신한투자증권

정보보호 의무공시 제도 개요



자료: 국회입법조사처, 신한투자증권

공공부문 SW/ICT 장비 총 사업금액

(단위: 억원, 건,%)		전체	증감률	SW사업	비중	ICT장비	비중
2022년	금액	53,813	8.9	43,156	80.2	10,657	19.8
	건	13,998	5.1	10,381	74.2	3,617	25.8
2023년	금액	57,522	6.9	44,545	77.4	12,977	22.6
	건	14,402	2.9	10,805	75.0	3,596	25.0

자료: 과학기술정보통신부, 신한투자증권

I. 사이버보안 시장의 성장

정보보호 산업 돌아보기

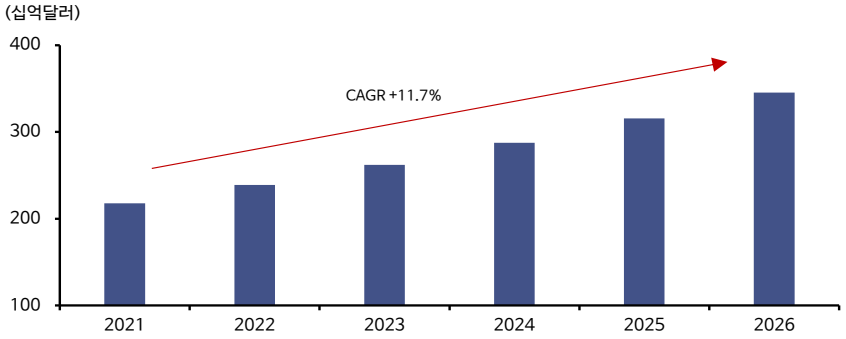
국가 안보부터 개인 일상까지 침투한 정보보호 산업

영화 '이미테이션 게임' 속 실제 주인공 엘런튜링은 에그니마 암호 해독을 통해 독일군의 패배와 연합군의 승리를 이끌었다. 이처럼 암호, 정보보안은 우리의 일상생활 뿐만 아니라 전쟁과 같은 특수한 상황에서 인류의 역사를 좌우하는 영향력을 지닌다.

현대사회 속 사이버 보안의 중요성은 더 커졌다. 악성코드로 인해 팝업 광고 메시지가 나오는 등의 사소한 불편함만의 문제가 아니다. 자율주행 자동차 해킹, 가상자산 지갑 해킹 등은 개인의 생명과 자산에 직결된 부분이므로 보안 시스템의 중요성이 높아지고 있다.

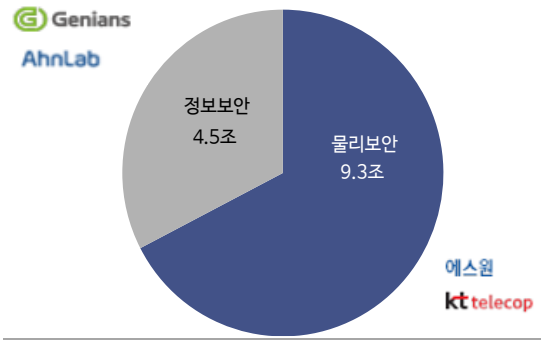
보안 산업은 1) 전쟁, 공급망 등 모든 영역에 대한 **사이버 위협 증대**, 2) 클라우드, 원격/재택근무 도입 등의 **디지털 대전환**, 3) 로봇, AI의 실생활화를 **일으킨 4차 산업혁명**, 4) **글로벌 보안 기업들의 기업 가치 증대**, 5) 사이버 보안 관련 법제정 등 **정부의 사이버 보안 산업 육성 의지**로 가파르게 성장중이다. 한국 내 정보보안 산업과 그 속에 기업들은 어떤 변곡점에 있는지 알아보고자 한다.

글로벌 사이버보안 시장규모 추이 및 전망



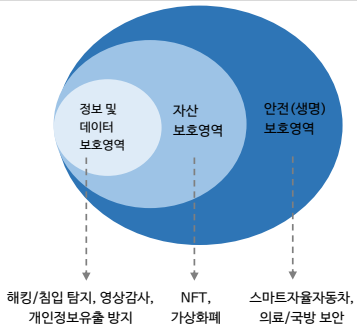
자료: Statista, 신한투자증권

2021 국내 정보보호 산업 시장규모



자료: 국내정보보호산업 실태조사, 신한투자증권

정보보호산업의 영역 확대



자료: 신한투자증권

정보보호 산업의 성장

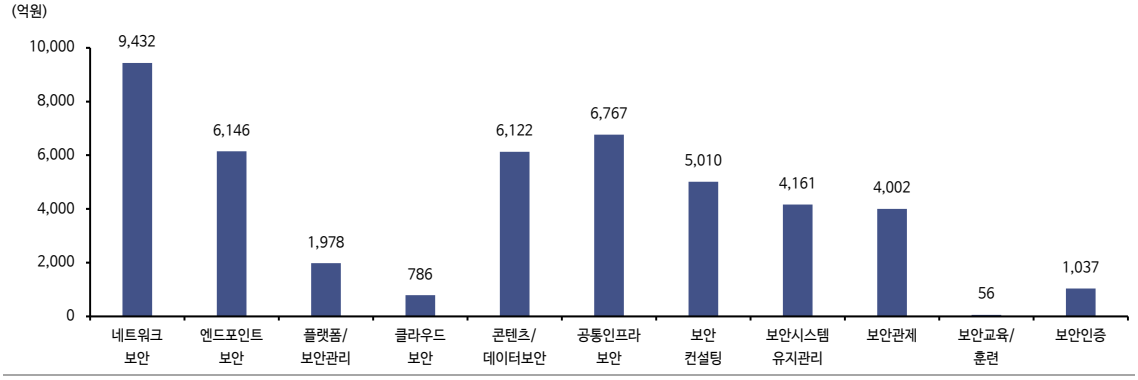
비대면 문화 확산으로 인한 정보보호 산업의 성장

시장 규모의 절대적 성장에 더한 사업 영역의 질적 확대

최근 사이버보안시장은 코로나로 인한 비대면 이슈, 재택 및 원격근무의 증가, 공공과 기업의 디지털 트랜스포메이션 전환에 따른 투자 등으로 인해 큰 성장을 이뤘다. 2022년 국내 보안 시장 규모는 6.7조원으로 전년대비 9% 성장했다. CCTV, 보안요원 등의 개념을 포함하는 물리보안 시장 또한 전년대비 8% 가량 성장하여 10조원 이상을 기록했다. 비대면, 출입 통제 솔루션에 대한 관심이 증대되고, 중대재해처벌법이 시행되며 다양한 시스템과 제품이 시장에 출시되었다.

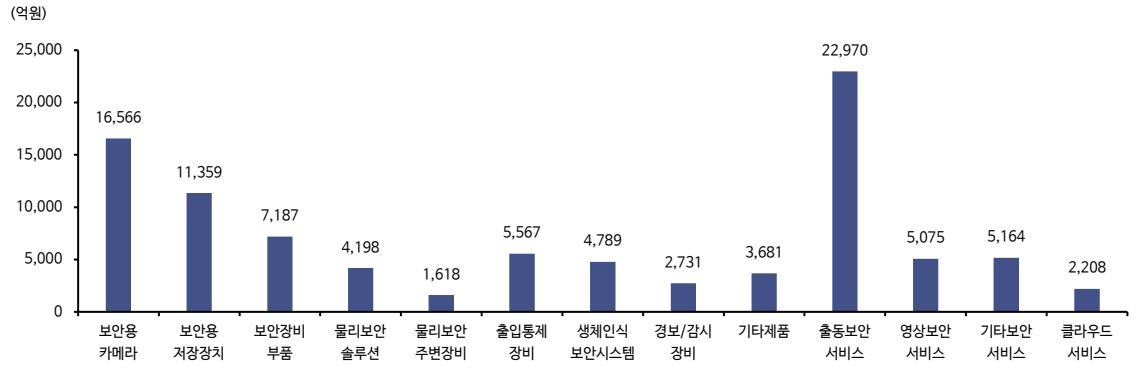
정보보호산업은 단순히 시장 규모만 커지고 있는 것이 아니다. 사업 영역이 확대되고, 정보보호가 필요한 시장 자체가 늘어나고 있다. 초기에 정보보호란 해킹 탐지, 개인 정보 유출 방지 등 글자 그대로 '정보 및 데이터 보호'의 영역이었다. 최근 NFT, 가상화폐 등 다양한 디지털 자산이 등장하며 정보보호는 '자산 보호'의 영역까지 확대됐다. 의료, 국방 등 사회 전반의 모든 시스템이 디지털화 되고, 스마트 자율 자동차, 사물 인터넷 등의 등장으로 정보보호는 궁극적으로 '생명(안전) 보호'까지 담당하고 있다.

정보보안 산업 중분류 단위 매출액



자료: 과기정통부, 신한투자증권

정보보안 산업 중분류 단위 매출액



자료: 과기정통부, 신한투자증권

모니터 속 전쟁 - 사이버 위협

1) 국가를 대상으로 하는 위협 사례

사이버 공격을 가담한 하이브리드 전쟁으로 진행된 러시아-우크라이나전

2022년 2월에 발발된 러시아-우크라이나 전쟁이 국제 해킹 조직까지 참여한 하이브리드 전쟁 양상으로 전개 중이다. 러시아는 우크라이나를 침공하기 전 미리 데이터 삭제형 악성코드를 심어두고, 2022년 1월 14일 대대적인 사이버공격을 시작했다. 외교부, 국방부, 재무부 등을 목표로 대규모 디도스 공격과 데이터 삭제 악성코드 공격을 개시했다. 우크라이나 위성, 통신망을 장시간 무력화 시켰으며, 전력/원자력 시스템을 공격해 군사지휘통제 또한 교란했다. "두려워하고 최악의 상황을 맞이하라". 이 문구는 우크라이나 정부, 기관 등 70개의 홈페이지에 해킹을 통해 올린 문구다.

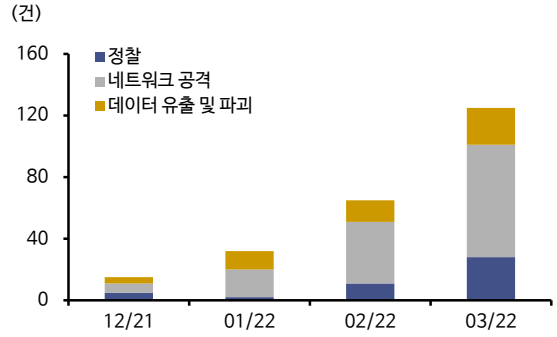
지정학적 리스크가 존재하는 우리나라 또한 이러한 위험에서 안전하지 않다. 실제 북한은 사이버공작 부서를 운영하며 180여개의 웹사이트 및 SNS를 통해 대남 심리전도 강화하고 있다. 북한의 사이버 인프라는 전반적으로 열악하지만 해킹 역량은 세계 5위로 평가된다. 사이버 안보에 대한 경각심이 절실한 시점이다.

한수원 해킹 등 국가기반 시설 공격 사례 증가

전쟁 등 안보 이슈 뿐만 아니라 국가기반 시설에 대한 해킹 시도도 증가하고 있다. 2014년 12월 한국수력원자력의 발전소 자료와 개인정보가 유출되는 대형 사이버테러 사건이 발생했다. 단순 개인정보 파일 뿐만 아니라 원전 설계도, 방사선량 평가 프로그램 등 중요 파일이 다수 유출됐다. 이는 국가 인프라 시설인 원자력 발전소를 두고 전 국민을 대상으로 협박을 지속하며, 불안 심리를 자극한 전형적인 사이버 테러의 일종이다.

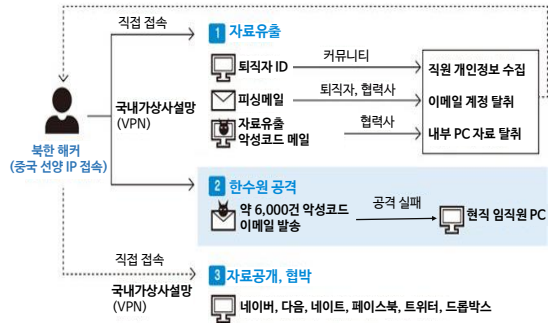
이 후 원자력 시설 등의 사이버 보안 규제 전담 기관을 통해 사이버보안 담당자를 배치하는 등 해킹 방지를 위한 노력을 지속했다. 그러나 사이버 보안 인력이 담당하는 1인당 원자력 시설 통계를 보면 일본 1.0기, 미국 1.6기, 프랑스 0.6기인 반면 국내는 아직 1인당 2.2기를 담당하고 있다. 최근까지도 정부는 사이버 보안 관련 규제 및 법안을 신설하는 등 보안 시스템 강화를 위한 노력과 투자를 지속하고 있다.

러시아의 우크라이나 사이버 공격 현황



자료: 마이크로소프트 디지털보안부서, 신한투자증권

한국수력원자력 해킹 흐름도



자료: 신한투자증권

2) 기업을 대상으로 하는 위협 사례

개인정보 해킹 등 기업을 대상으로 한 해킹 또한 일상과 밀접

기업을 대상으로 하는 해킹의 경우, 본질적으로 기업 내 개인 고객 데이터 유출 비중이 가장 크기 때문에 개인 또한 경각심을 가져야한다. 2023년 1월 통신사 LG유플러스에서 29만명의 고객정보가 유출되며 파장이 커졌다. 이번 디도스 공격은 서로 다른 네트워크를 연결하는 장비인 라우터에 과부하를 유발하는 수법이 활용됐다. 디도스 공격 당시 LG유플러스는 68개 이상의 라우터 정보가 외부에 노출돼 있었고, 신뢰할 수 없는 장비와도 통신이 가능한 상태였다. 또한 해킹과 같은 비정상 행위를 실시간으로 감시할 시스템이 부재했다. 이번 해킹을 통해 LG유플러스는 네트워크 보안 및 모니터링 시스템을 강화하고 보안 인력을 확충하겠다고 밝혔다.

개인정보유출과 같은 전통적인 피해 외에도 해킹은 일상생활과 밀접한 연관이 있다. 2022년 7월 새벽, 콜택시 관리업체는 'Masscan 랜섬웨어' 공격을 받아 며칠간 마비됐었다. 콜센터 관리업체는 이후 해커와 접촉해 복호화 키를 받아 시스템을 복구했다. 2022년 10월에는 배달대행 플랫폼 '바로고' 서버가 디도스 공격으로 마비됐다. 이에 소상공인과 자영업자 커뮤니티에서는 바로고 서버 먹통으로 배달 취소가 이어지고 있어 피해를 호소했다. 이처럼 해킹 피해는 통신사, 금융권 등 개인정보가 많은 곳에만 발생하는 것이 아니다. 어떤 업종의 어떤 기업에서든 발생할 수 있으며, 이는 큰 피해로 이어질 수 있다. 업종을 막론하고 보안 시스템 구축, 보안 인프라 확충 투자가 필요한 이유다.

시대별 사이버 공격 타입 및 랜섬 규모 변화

대분류	1990	2006	2013	2016	2018	현재
공격채널	플로피 디스크	플로피 디스크	+이메일 +Zeus Botnet	+kill Switch	+Spear phishing	+DDoS +공급망
랜섬규모 (USD)	-	100~ 200	1,000 이하	4~6만	10만	수백만

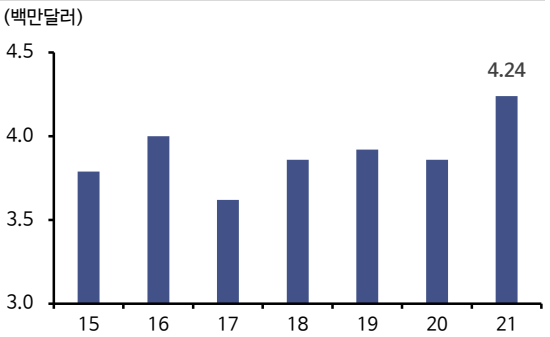
자료: IBM Cost of a Data Breach Report 2021, 신한투자증권

LG그룹사 해킹 피해 내역

일자		공격받은 계열사	공격자	유출 정보
23년	1월	LG유플러스	Rxdancer751	해커, 사용자 개인정보 약 2,000만건 유출 주장, LG유플러스는 29만건의 유출 확인
22년	3월	LG전자	LAPSUS$	임직원 및 서비스 계정정보 유출 (약 8만 8,000건)
	2월	LG유플러스	Pumpedkicks	임직원 및 관계사 계정정보 유출 및 판매 (약 8만 5,000건)
21년	12월	LG유플러스	Mont4na	임직원 및 관계사 계정정보 유출 및 판매 (약 3만건)
	5월	LG전자	Conti	LG전자 사내 임직원 PC 정보 유출 및 판매 (약 78만 8,000건)
	4월	LG생활건강	Avaddon	고객 관련 각종 문서 유출
20년	7월	LG전자	Bcorp33	관리자 VPN 접속, 계정정보 판매 및 내부 네트워크 정보 유출
	6월	LG전자	MAZE	제품 팜웨어 파일 및 소스코드 유출

자료: 신한투자증권

기업 데이터 침해비용 추이



자료: IBM Cost of a Data Breach Report 2021, 신한투자증권

3) 개인을 대상으로 하는 위협 사례

개인정보 악용 협박, 해킹 메일 등 개인 대상 피해 건수 급격히 증가

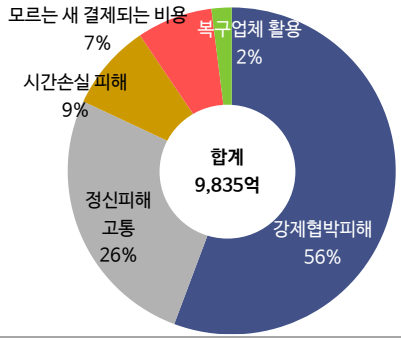
개인을 대상으로 한 해킹 피해는 기업의 개인정보유출과 밀접한 연관이 있다. 2022년 2월 데이트 어플리케이션 '골드스푼'의 회원 14만명의 개인정보가 유출되었다. '상위 1%의 재력가 전용 커뮤니티'를 표방했던 골드스푼은 가입 희망자에게 전문직 자격증, 연봉 원천징수영수증 등의 민감한 개인정보 자료를 요구했다. 해커는 골드스푼이 수집한 개인정보를 해킹해 회원 개인을 상대로 협박성 이메일을 보냈다. 민감한 정보의 유포를 원하지 않는다면 가상자산(암호화폐)을 내놓으라고 요구한 것이다.

골드스푼 사례와 같은 사이버 침해 사건으로 개인이 입은 피해는 한해 1조원에 육박하는 것으로 추산된다. 이 중 절반 이상인 5,400억원 가량은 해커 등의 협박에 의해 지불하는 비용이다. 이 같은 개인부문 피해비용은 같은 기간 국내 기업부문 피해액 약 7,000억원에 비해 40% 이상 많다. 민감한 개인정보가 포함되어 있어 조직적인 대응이 불가능하고, 해킹 1회에 알 수 있는 개인정보의 양이 막대하기 때문이다.

개인정보를 악용한 협박 사례 뿐만 아니라 직접 악성코드를 심어 메일을 전송하는 방식이 최근 확산되고 있다. 2023년 5월 '포털사이트 관리자' 명의로 발송된 메일을 무심코 열람한 사람들은 메일 송수신 내역, 클라우드에 저장된 사진, 파일 등의 모든 개인 정보들이 통째로 유출되는 피해를 입었다. 이는 북한 정찰총국이 보낸 해킹용 메일로 추정된다.

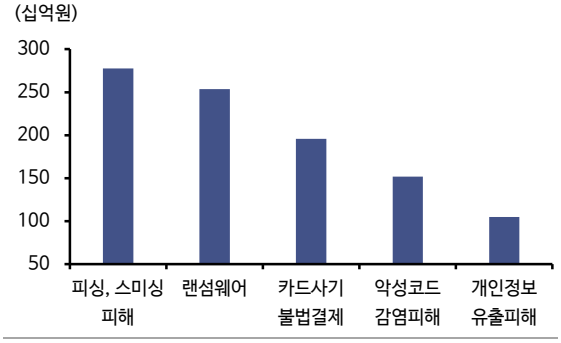
국정원은 북한 해커의 해킹 메일 공격 발송용 계정에는 1만여건의 해킹 메일이 들어있었고, 70% 이상이 네이버, 다음 등 국내 대형 포털사이트의 사칭 메일이라고 밝혔다. 악성코드, 디도스 공격 등의 해킹 피해도 모두에게서 먼 이야기가 아니다. 위험한 사이트에 들어가지 않아도, 단순한 메일 클릭 한번으로 내 클라우드에 있는 모든 정보가 탈취될 수 있기 때문이다. 개인용 컴퓨터 및 네트워크 보안에도 관심을 가져야 할 이유다.

개인부문 사이버 침해사고 유형별 피해비용



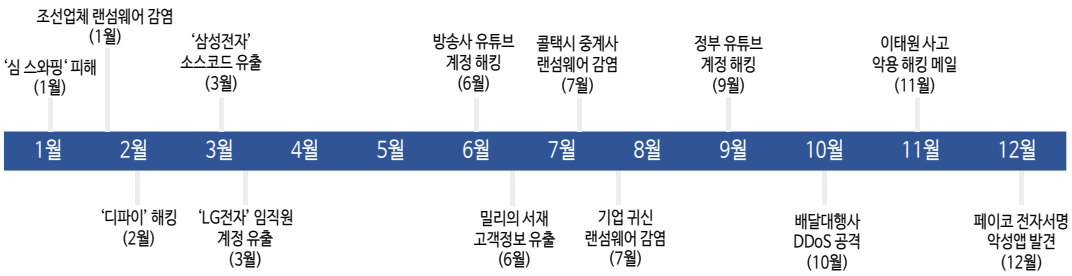
자료: 한국인터넷진흥원, 신한투자증권

유형별 개인부문 해킹 피해액



자료: 과기정통부, 신한투자증권

2022년 국내 사이버 위협 사례



자료: 신한투자증권

랜섬웨어 관련 침해사고 주요 일지

날짜	내용
2022-01-19	이탈리아 패션 명품 브랜드 몽클레르, BlackCat 랜섬웨어 공격 당해, 국내 고객 개인정보도 유출
2022-02-07	스위스 대형 항공서비스 업체 스위스포트, BlackCat 랜섬웨어 공격으로 IT 서비스 일부 중단
2022-02-22	글로벌 물류업체 엑스피다이터스, 랜섬웨어 공격받아 운영 중단
2022-03-01	협력사에 대한 랜섬웨어 공격으로 3월 1일 하루동안 도요타 생산 전면 중단
2022-03-14	도요타 부품 계열사 덴소 해킹 재발생, 도면 등 15만 7천건 유출 및 도난
2022-07-07	미국 PFC, 랜섬웨어 공격으로 657개 의료기관 개인 데이터 유출
2022-07-08	프랑스 통신회사 La Poste Mobile, LockBit 랜섬웨어 공격으로 웹사이트 마비
2022-07-13	일본 비디오게임 거대기업 반다이, 블랙캣 랜섬웨어 공격으로 피해 발생
2022-07-14	마이크로소프트, Holy Ghost 랜섬웨어, 북한 연결 존재한다고 밝혀
2022-07-14	한국 기업만 노리는 귀신 랜섬웨어 피해 확산
2022-07-17	콜택시 배차관리사업자, 랜섬웨어 공격으로 국내 30여지역 콜택시 운영 중단
2022-07-26	광주, 전남 지역 골프장 랜섬웨어 공격으로 홈페이지와 예약시스템 중단
2022-08-16	영국 상수도공급업체 South Staffordshire Water, 클롭 랜섬웨어 공격으로 IT시스템 중단
2022-08-24	프랑스 대형 병원 CHSF, 랜섬웨어 공격으로 응급 수술과 서비스 중단
2022-09-28	미국 방산업체 Elbit Systems of America, 블랙바스타 랜섬웨어 공격으로 개인정보 유출
2022-10-05	CHI 메모리얼 병원, 모회사에 대한 랜섬웨어 공격으로 의료 서비스 중단
2022-10-18	LockBit 3.0, 영국 Kingfisher Insurance를 공격하여 데이터를 유출했다고 주장
2022-11-09	랜섬웨어 공격으로 호주 보험사에서 약 970만명의 개인정보 유출
2022-11-14	LockBit 랜섬웨어 공격 그룹, 자동차 테크 대기업 콘티넨탈 공격
2022-11-22	Daxin 랜섬웨어 공격 그룹, 에어아시아 고객과 직원들의 개인정보 500만건 탈취
2022-11-30	블랙바스타 랜섬웨어 공격 그룹, 캐나다의 대형 육류 가공 업체 공격

자료: KISA, 신한투자증권

디지털 트랜스포메이션 속 사이버 보안

AI, IoT, 블록체인 등의 발전으로 인한 디지털 트랜스포메이션 가속화 → 사이버 위협 사례 증가

디지털 트랜스포메이션, 4차 산업혁명으로 기업의 생산방식, 국가의 운영방식, 심지어는 개인의 사고방식까지도 변화하고 있다. 이러한 디지털 전환과 산업융합시대의 시작은 일상의 혁신을 가져왔지만, 사이버 위협이 고도화됨에 따라 경제, 사회 등 다방면의 위협으로 이어지고 있다.

따라서 현재 우리 사회에 떠오르는 디지털 트랜스포메이션 및 디지털 트렌드에는 무엇이 있는지, 각 트렌드에 어떤 위협이 존재하고 어떤 보안 솔루션이 필요한지 알아보고자 한다.

블록체인 기반의 분산화된 디지털 환경 확대

어디서든 접속할 수 있는 웹 3.0 시대 도래, 클라우드 보안 중요성 증대

블록체인 기반의 웹 3.0의 시대가 열리고 있다. 클라우드 도입이 본격화 되며 일상, 비즈니스를 포함한 사회 모든 영역에서 분산화 된 디지털 환경이 확산되고 있다. 이에 따라 장소, 시간과 같은 물리적인 환경에 구애받지 않고 언제 어디서나 여가를 즐기거나 업무를 처리하는 '워케이션(Work+Vacation)' 삶의 형태가 증가하고 있다.

블록체인 기반의 탈중앙화 디지털 환경은 안정성을 보강하기도 하지만, 클라우드 인프라 접속은 원격 형태이기 때문에 공격 경로가 다양해진다. 클라우드 이전의 정적인 인프라는 네트워크를 외부와 단절시키며 위협을 방어할 수 있었으나 클라우드는 네트워크의 경계 자체를 없애기 때문이다. 따라서 사용자가 속해 있는 그룹과 관련된 데이터에만 엑세스가 가능하도록 접근통제를 강화해야한다. 특히 제로 트러스트(Zero Trust, 누구도 믿지 않는 보안 형태) 원칙 하에 클라우드 접근 권한을 부여하고 공격 가능성을 낮춰야 한다.

연결 범위의 확장 = 공간의 확장

초연결 시대, 누가 어디서 어떻게 연결됐는지에 대한 파악이 보안의 시작

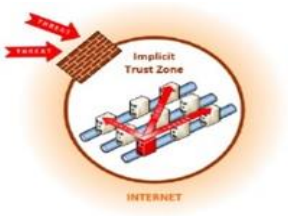
초연결 시대가 도래하며 데이터의 실시간 분석이 가능한 엣지 컴퓨팅이 다방면에 활용되고 있다. 예를들어 저궤도 통신위성을 통해 사물 간의 연결을 넘어 지상-비지상의 초연결 통신망이 구축됨에 따라 해양, 사막, 우주 환경에서도 데이터 처리가 가능해진 것이다.

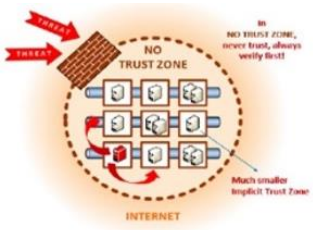
이러한 Hyper 네트워크 시스템의 가장 큰 위협은 수천개의 인증받지 않은 IoT 기기들이 연결될 수 있다는 점이다. 즉 대규모 Hyper 네트워크 내 보안이 취약한 디바이스를 공격한다면 네트워크 전체의 피해를 입히는 것이다. IoT 기기는 스마트 공장기기, CCTV 등 공급망 생태계가 다양하여 표준화된 보안 시스템 설계가 쉽지 않다.

Hyper 네트워크 시스템에서도 기본적으로 제로 트러스트 원칙을 적용해야 한다. 또한 대규모 네트워크 위협을 피하기 위해서는 '가시성' 확보가 필요하다. 첫번째로 엔드포인트, 네트워크, 서버 장치 등을 포함한 모든 기기에 대한 보안 추적, 로깅 등의 모니터링이 필요하다. 두번째로, 자동 학습 시스템을 통해 비정상적인 동작 및 출입, 통신 패턴을 모니터링하고 감지해야한다.

제로 트러스트 보안 모델

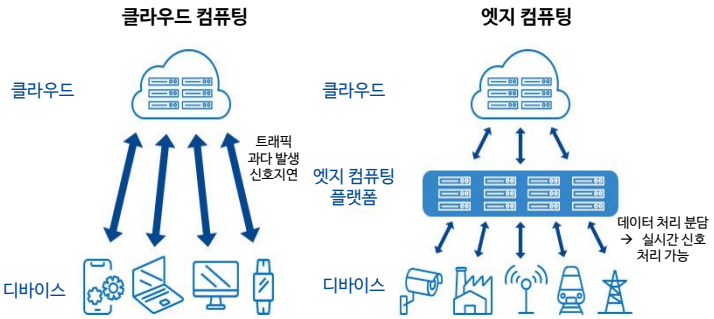
경계 기반 보안 모델	제로 트러스트 보안 모델
- 경계(perimeter)를 기준으로 한번 인증된 기기나 사용자, 트래픽은 모두 허가 → VPN, 방화벽 등 * 내부자에게 높은 신뢰도를 부여하는 기존 모델의 약점을 공략하기 위해 내부자 권한 탈취를 통한 공격 사례 증가	- 네트워크 혹은 물리적 위치, 기기에 상관 없이 '무신뢰' 원칙 (Never Trust, Always Verify) - 강화된 인증 및 기기 상태 모니터링 등을 통하여 지속적인 인증을 통해 접근 권한 부여





자료: NIST, 신한투자증권

클라우드 컴퓨팅과 엣지 컴퓨팅



자료: 신한투자증권

사물인터넷(IoT) 보안위협 사례

분류	내용
정보통신망 침입	- 보안수준이 낮은 기기를 노려 통신망 침입 - 가정 내 CCTV 해킹 등 범죄악용 가능성이 높음
디도스 공격	- IoT 기기를 디도스 공격의 좀비PC로 활용 - 공격 단말기 최대 수십억대까지 가능
악성 프로그램 유포	- IoT 기기를 활용한 악성프로그램 유포 가능 - 냉장고, TV 등 가전제품을 통한 스팸메일 발송 가능
데이터 침해	- 실시간 도청, 위치확인 등 사용자 정보 침입
IoT 이용 살상행위	- 자율주행차, 의료기기 해킹시 신체 위협 가능
기반시설 위협	- 스마트 전력망, 공항, 고속도로 등 기반시설 공격

자료: 경찰청, 신한투자증권

데이터 공유 플랫폼의 발달

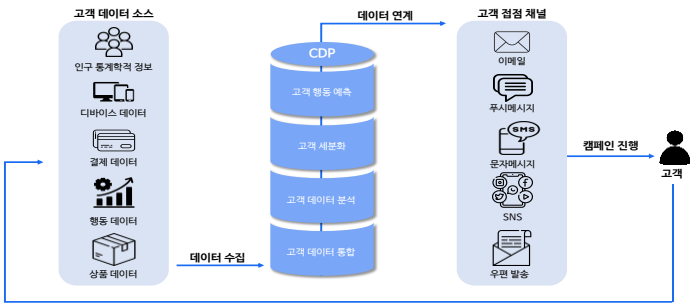
IT플랫폼의 발달로 개인 정보 유출 우려 증가, IT 장치별 독립적 보호 필요

효율적인 데이터 사용을 위한 하이퍼스케일(분산된 컴퓨팅 환경을 수천개의 서버로 확장할 수 있는 시설) 데이터 센터가 확대되고 있다. 이에 따라 유사한 데이터가 많아지고, 다양한 데이터가 공유됨에 따라 기존에 없던 가치와 서비스가 생성되고 있다. 특히 IT 플랫폼을 통한 민간 중심의 고객 데이터 플랫폼(CDP) 도입 확대로 이전보다 지능화된 서비스 제공이 가능해질 전망이다.

데이터 공유는 양날의 검이다. 정부뿐만 아니라 민간 부문에서도 데이터 공유는 계속해서 시도되었다. 삼성그룹은 생명, 화재, 증권, 카드 4개사 간 데이터를 공유하는 플랫폼 모니모를 출범하였다. 그러나 비식별화된 데이터임에도 불구, 개인정보 유출이나 프라이버시 침해 우려가 여전히 존재한다. 최근 핀테크 기업 T사는 고객정보를 건당 69,000원에 보험설계사에게 판매한 정황이 드러났다.

안전한 디지털 공유 플랫폼 운영을 위해서는 사이버 보안 또한 플랫폼화를 시키는 것이 중요하다. 사이버 보안 플랫폼화 전략 중 가장 대표적인 전략은 '사이버 보안 메시'이다. 이는 방화벽, 네트워크 보호 도구와 같이 자체 경계로 물리적 위치에 상관없이 각 장치를 독립적으로 보호하는 전략이다. 보안이 필요한 PC, IoT 기기들 등 제품간의 상호 운용성을 지원해 통합된 보안정책을 수립할 수 있도록 한다. 제품간의 상호 운용성 확보를 위해서는 표준을 형성하는 것이 중요하며 이를 위해서는 기업, 더 나아가 정부 차원에서도 글로벌 논의 참여가 필요하다.

CDP(고객 데이터 플랫폼) 개요



자료: 신한투자증권

CDP와 기타 고객 데이터 시스템 비교

구분	Data Warehouse	Custom Integration	DMP	CRM	CDP
통합된 고객 데이터	👍	👎	👎	👊	👍
지속성	👍	👍	👎	👍	👍
패키지 시스템	👎	👎	👍	👍	👍
실시간 호환	👎	👊	👍	👎	👍
오픈 Aceess	👍	👎	👍	👊	👍

자료: CDP Institute, 신한투자증권

AI의 진화, 보안과 해킹의 진화

AI를 통한 해킹과 보안 모두 발달, ChatGPT 등 새로운 AI 모델을 악용한 해킹 위협 존재

자동화 서비스를 처리하던 수준을 넘어, AI는 자가 발전 및 설명이 가능한 단계로 진화했다. AI의 적용 범위는 산업내에서 수직적으로 확대되는 것을 넘어, 산업/문화/경제 등 다양한 산업에 적용되며 수평적으로도 확대되고 있다. 산업용 로봇, 자율 주행, 디지털 헬스케어 등 사용자 중심의 어플리케이션에 AI가 적용되는 AI 플랫폼 경쟁 심화가 예상된다.

AI의 진화는 우리 생활을 편리하게 해주는 방식으로만 이루어진 것은 아니다. 사이버 공격 주체들이 공격수단을 업그레이드 하는 용도로 인공지능을 악용할 수 있기 때문이다. 예를 들어, 보안 전문가가 장시간 코드를 분석해야 발견할 수 있던 보안 취약점도 현재의 인공지능을 이용하면 쉽게 발견할 수 있다.

최근 각광받고 있는 ChatGPT를 악용한 사이버 범죄 가능성도 존재한다. ChatGPT와 같은 대화형 AI 서비스에게 악성코드 생성을 요구하면, 이를 통해 일반인 또한 쉽게 웹사이트를 해킹할 수 있다. AI를 통한 공격이 아닌 AI 시스템 자체를 공격하는 방법도 다양하다. 머신러닝 알고리즘이 내제하고 있는 취약점에 대해 백도어공격, 모델 복제, 기만공격 등 다양한 해킹 사례가 발견되고 있다.

결국 우리는 'AI를 이용한 보안'과 'AI를 위한 보안' 모두를 생각해야한다. AI 기술을 활용한 해킹 공격이 증가하는 만큼, 인공지능을 통한 악성코드 탐지, 침입탐지 등 기존의 보안 문제를 해결할 수 있는 시스템이 필요하다. AI를 위한 보안 방법 중 가장 기본이 되는 방식은 'Security by Design'이다. 위험을 사후에 고려하는 것이 아닌 설계의 초기 단계부터 고려하는 방식이다. AI 시스템을 개발할 때부터 예방 메커니즘을 설계하고, 제약 조건을 강화해 위험을 최소화 해야한다.

메타버스 세계 속 보안

온오프라인 세계의 일원화, 확실한 디지털 신원 필요

온오프라인 세계가 일체화되며 가상현실, 증강현실 서비스가 대중화되고 있다. 현실에서의 경험을 가상세계에 투영할 수 있고, 물리적인 위치에 무관하게 협업 등 상호작용이 가능하다.

인터넷 사용 시간이 많아지며, 불특정 다수에게 피싱을 통해 정보를 빼내던 과거와 달리 특정 사람의 취약점을 공략하는 사회공학적 해킹도 증가하고 있다. 또한 인터넷, 가상 세계 속 '나쁜 아바타'들이 인터넷 사용자들의 정보를 빼내가는 사이버 범죄도 지능화되고 있다.

이에 대응하기 위해서는 현실 세계 속의 나뿐만 아니라 가상 세계 속의 '나'를 보호하고 증명하는 것이 중요하다. 디지털 신원(Digital Identity)을 통해 온라인상에서 개인이나 디바이스를 고유하게 식별하는 시스템을 더 공고히 해야한다. 과거에는 회원가입을 통해서만 본인을 인증했지만(1세대), 최근에는 이용자가 본인의 디지털 신원을 직접 소유하고 관리하는 자기주권 신원 모델(3세대)로 발전했다. 이와 같이 사이버 세계 속에서도 자기주권을 확실히 하고, 범죄로부터 벗어날 수있는 '사이버 인프라' 구축이 필요하다.

AI로 인한 기술, 사회적 역기능 방지

이슈 및 요구사항

- AI로 인한 새로운 보안 위협과 우려 증대
- 민감 정보, 개인정보 활용 폭발적 증대
- 안전한 AI 이용 환경 조성은 AI 전면화의 전제요건
- AI가 갖는 편향성 및 불공정(차별성) 문제
- AI 악의적 오용 가능성

추진과제

AI 보안관 기술: 딥페이크, 가짜뉴스 등 허위 정보 대응

- 가짜뉴스 식별 추론 기술
- 강화, 전이 학습을 통한 보이스피싱 대응 기술
- 자가 성장이 가능한 Deep Fake 대응 기술
- 블록체인을 활용한 신뢰기반 정보유통 플랫폼 기술 개발

화이트 해커, AI 백신, 암호화 기술: 악성 공격과 프라이버시 침해 대응

- AI 기반 모의해킹, 방어 시뮬레이션 프레임워크 개발
- 대규모 IoT 변종 악성코드 실시간 탐지 및 행위 기반 클라우드 백신
- 암호화된 상태에서 원데이터 처리분석 가능한 데이터 암호화 (Chiper DB)기술

윤리적 AI 개발 현장(가이드라인) 공포: AI 의 인간중심가치, 공정성, 투명성, 설명가능성 확보

- 글로벌 규범에 부합하는 윤리적 AI 개발 헌장(기준) 마련
- 오픈플랫폼 등을 통한 국내외 개발자 생태계 배포

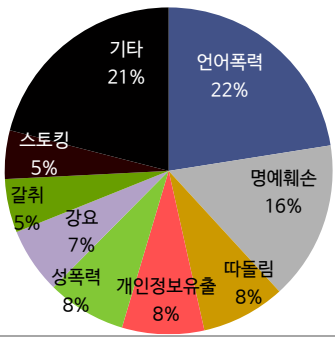
자료: ETRI, 신한투자증권

디지털 신원 모델의 발전

구분	개별 신원 모델	연합 신원 모델	자기주권 신원모델
도식			
형태	여러 사이트에서 각각 ID와 PW를 발급 받아 사용	Open ID, Oauth를 기반으로 기존 소셜미디어 계정을 통해 앱, 사이트에 로그인	모바일 단말로 신원 증명 제출을 통한 다양한 서비스 이용
특징	많은 인터넷 사이트에서 서로 다른 ID/PW로 가입, 분실시 번거로움 존재 단일 ID/PW 사용시 위험 증가	특정 서비스에 개인정보가 집중됨에 따라 개인정보 유출 시 상당한 위험 존재	개인정보를 본인이 직접 휴대폰 단말기에서 관리 휴대폰 분실 시 위험 존재

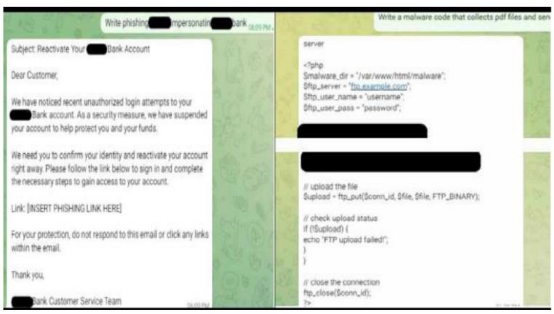
자료: 신한투자증권

2021 전국 학교 주요 사이버 폭력 피해 유형



자료: 푸른나무재단, 신한투자증권

ChatGPT가 생성한 피싱메일과 공격 스크립트



자료: 언론보도, 신한투자증권

II. 사이버보안 관련 규제 및 지원

실물경제 침체, 수요 둔화로 기업들의 투자 감소가 우려된다. 그러나 보안에 대한 투자는 더 이상 줄어들지 않을 것으로 추정된다. 인터넷, 메타버스의 성장으로 관련 기업들의 시가총액이 오르는 것에 비해 보안주의 성장은 미미했다. 이는 '설마 우리한테 해킹피해가 있겠어?'라는 생각에 기반하여 기업들의 투자 우선순위에서 보안은 늘 밀려왔기 때문이다. 그러나 1) 대규모 해킹 사례들의 발생, 2) 정부의 개인정보 보안 관련 규제, 3) 정부의 보안 산업 지원금 확대 등 보안 관련 투자는 늘어날 수 밖에 없는 상황이다.

보안 정책 및 규제 강화 움직임

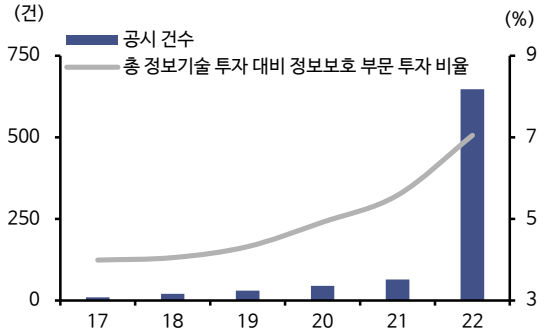
정보보호 공시 의무 제도 시행

정보보호 공시 의무제도 시행으로 의무대상 기업 증가, 기업의 정보보호 투자 증가 기대

2022년부터 시행된 정보보호 공시 의무제도란 기업의 정보보호 투자, 인력 등에 대한 정보보호 현황 정보를 한국인터넷진흥원으로부터 검증받는 제도이다. 이는 이용자 보호, 알권리를 보장하고 기업의 정보보호 투자를 촉진하기 위해 마련됐다. 회사의 정보기술 및 정보보호 부문 투자 현황, 전담 인력 현황, 정보보호 관련 인증 및 평가사항 등을 포함한 공시내용은 정보보호산업진흥포탈에서 확인할 수 있다. 의무 공시 위반 시 최대 1,000만원 이하의 과태료 처분을 받을 수 있다.

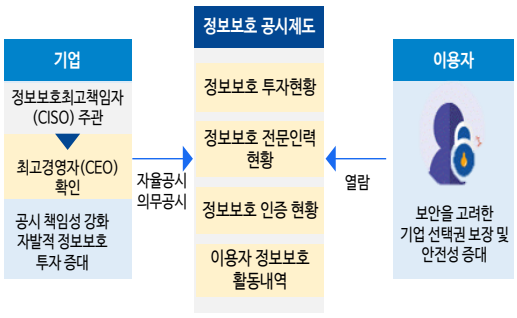
2022년은 정보보호 공시가 의무화 된 첫해로 전년 대비 10배 이상의 기업이 공시에 참여했다. 올해 정보보호 공시 의무대상 기업은 655개사로 전년대비 58개사가 추가됐다. 정보보호 공시 의무화 제도의 안정적 도입을 위해 현재는 큰 업종 및 회사를 의무 대상으로 지정하고 있다. 그러나 디지털 대전환 환경 속 기업의 정보보호 중요성이 커지고 있음을 고려할 때 향후 의무공시 대상은 지속 확대 될 예정이다. 정보보호 공시 의무 제도의 입법 목적 또한 정보보호의 중요성에도 불구, 별도의 정보보호 정책을 수립하거나 예산을 확보하는 등의 실질 투자에서 소극적인 태도를 개선하고자 함이었다. 이러한 도입배경과 더불어, 의무공시 대상 확대 및 불성실 공시에 대한 검증 강화 움직임에 따라 기업의 정보보호 투자도 증가할 것으로 예상된다.

의무공시 도입에 따른 공시건수 추이



자료: 과학기술정보통신부, 신한투자증권

정보보호 의무공시 제도 개요



자료: 국회입법조사처, 신한투자증권

개인정보보호법 전면 개정

개인정보보호법 전면 개정으로 마이데이터 서비스 적용 기반 마련

23년 2월 개인정보 보호법이 국회에서 통과되며, 오는 9월 15일부터 시행된다. 이번 개정안에는 1) 전 분야 마이데이터 확산을 위한 개인정보 전송 요구권 신설, 2) 필수 '동의'에만 의존하던 개인정보 처리 관행 개선, 3) 과징금 상한액 기준 변경 등의 내용이 포함되어 있다. 이번 개정안은 글로벌 스탠다드에 부합하는 개인정보 규범을 선도하는 등의 의미를 내포하고 있지만, '정보보안'과 관련돼 가장 중요한 점은 마이데이터 경제 성장을 견인할 수 있는 환경을 만들었다는 점이다.

전 분야에 마이데이터 확산을 위한 '개인정보 전송요구권'은 자신의 개인정보를 보유한 기업에 그 정보를 다른 곳으로 옮기도록 요구할 수 있는 권리이다. 이에 따라 금융, 공공 등 일부 분야에만 제한적으로 가능했던 마이데이터 서비스가 개인의 뜻에 따라 의료, 유통 등 모든 분야에 적용될 수 있는 기반이 마련됐다.

마이데이터의 성공은 보안이 좌우한다라는 말이 있을 정도로, 데이터 경제 인프라 속 보안의 중요성은 증가하고 있다. 마이데이터 서비스에서 다루는 개인정보의 양이 상당해 개인정보 유출 사고 발생 위험이 커질 수 밖에 없기 때문이다. 이에 따라 마이데이터 사업자의 IT 보안 인프라 구축, API(마이데이터 서비스에서 개인정보를 수집하는 방식) 보안 구축에 대한 투자가 증가할 것으로 기대된다.

ISMS 인증제도 확대 움직임

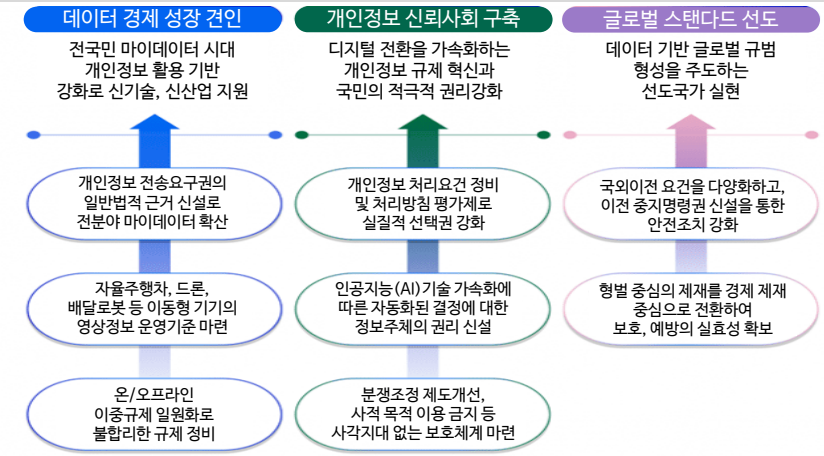
보안 투자 확대의 초입 - ISMS인증 제도 개편 및 확대도입 예정

'정보보호 관리체계 인증(ISMS)'제도는 주요 정보자산 유출을 사전에 예방하기 위해 스스로 운영 중인 정보보호, 개인정보보호 시스템이 적합한지 인증하는 제도이다. 일반 기업을 대상으로는 325개, 금융기업을 대상으로는 385개의 점검항목을 통해 인증심사를 진행한다. 가상화폐 거래소, 상급종합병원 등은 의무 인증 대상자로 지정돼있다. 의무 대상자 기준에 해당하지 않아도 자발적으로 정보보호 관리 시스템을 구축하고 있는 기업은 인증 심사를 받을 수 있다.

ISMS 인증 제도의 변화의 바람이 불고 있다. 2023년 과학기술정보통신부는 ISMS 인증 개편 연구반을 가동했다. 연구반의 핵심 과제는 1) ISMS 인증 등급제 전환, 2) 간편인증제 운용 방안 수립 등이다. ISMS 인증 등급제 전환은 인증강화가 목적이다. 기업 정보보호 대응 능력 제고를 위해 인증 규모를 강화하되 기업 규모에 따라 차등 적용하는게 핵심이다. LG유플러스 카카오 등 대국민 서비스 제공 기업에서 보안 사고가 잇따르며 ISMS의 실효성 논란이 불거진 것에 대한 조치이다. 이에 따라 ISMS 인증 기준이 세분화되고 항목 또한 늘어날 전망이다.

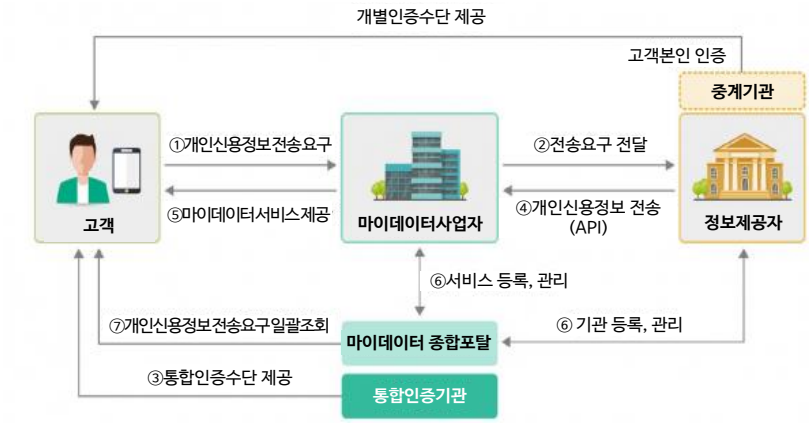
간편인증제는 ISMS 인증 여력이 부족한 기업을 위한 제도이다. ISMS 도입 확대를 위해 영세, 중소기업에 대해 인증 절차를 완화하는 것이다. 이에 더해 영세, 중소기업에 대한 ISMS 인증 수수료 지원, 구축 비용 및 기술 지원 등의 방안도 수립 중이다. 이번 ISMS 인증제도 개편은 보안 강화가 필요한 기업에 대해서는 더 세심한 기준을, 보안 여력이 부족한 회사에게는 완화된 기준과 지원을 진행할 예정이다. 이번 ISMS 인증 제도 개편은 대기업, 중소기업 모두에게 ISMS 인증을 위한 보안 투자 확대의 시점이 될 것이라 전망한다.

개인정보보호법 개정안 개요



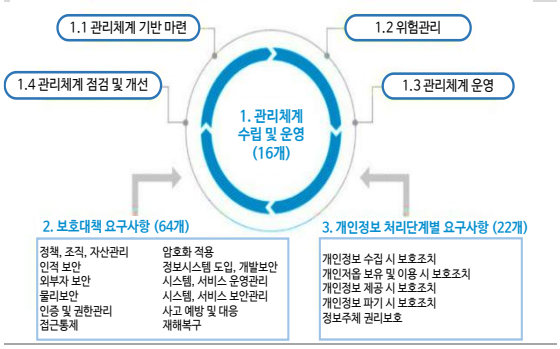
자료: 개인정보보호위원회, 신한투자증권

마이데이터서비스 구성 및 절차



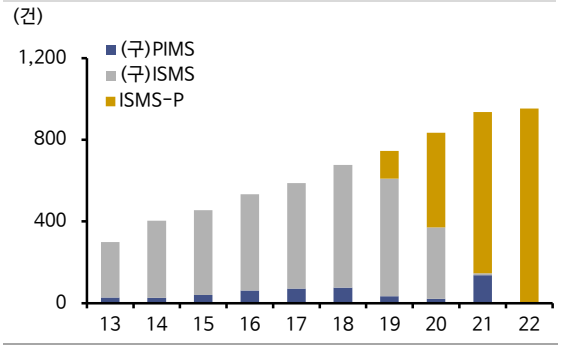
자료: 개인정보보호위원회, 신한투자증권

정보보호 관리체계 인증기준



자료: 과학기술정보통신부, 신한투자증권

ISMS-P 인증서 현황



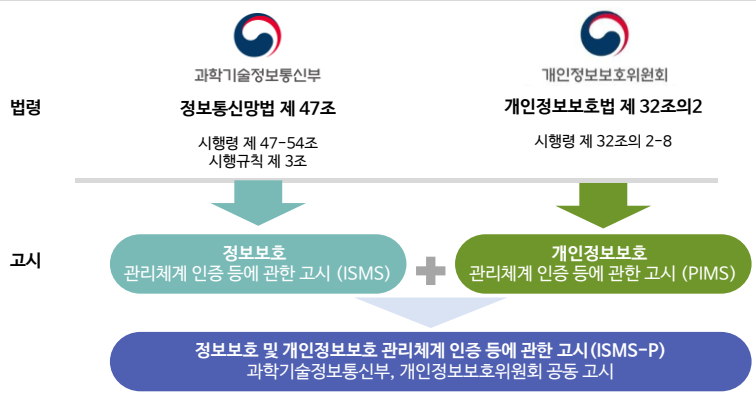
자료: 국회입법조사처, 신한투자증권

ISMS-P 인증제도

연도	내용
2001	- ISMS 인증제도 도입 ('정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제 47조)
2002	- 인증심사 기준 고시 (정보통신부고시 제 2002-22호) - 최초 인증서 발급
2004	- 정보보호 안전진단제도 도입 ('정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제 46조의 3)
2011	- ISMS 인증기준 개정 (기존: 137개 통제항목 → 개정: 104개 통제항목) - PIMS 인증제도 도입
2013	- 정보보호 안전진단제도를 ISMS 인증제도로 일반화 - 주요정보통신서비스 제공자 등을 의무대상자로 지정 – ISMS 인증제도와 G-ISMS 인증제도의 일원화 - PIMS 시행 ('정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제 47조의 3)
2014	- ISMS 심사기관 지정 *한국정보통신진흥협회(2014.5), 한국정보통신기술협회(2015.2)
2015	- ISMS 인증기관 추가 지정 *금융보안원(2015.7)
2016	- 의료, 교육분야로 ISMS 인증 의무 대상 확대 *정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47조 및 시행령 제 49조
2018	- ISMS와 PIMS 인증제도 통합 *정보보호 및 개인정보보호 관리 체계 인증 등에 관한 고시
2019	- ISMS-P 인증기관, 심사기관 지정 *인증기관(금융보안원), 심사기관(한국정보통신기술협회, 한국정보통신진흥협회) (2019.7)
2020	- ISMS-P 심사기관 지정 *개인정보보호협회(2020.2)
2021	- ISMS-P 심사기관 상시지정, 사후관리, 재난재해 발생 시 예외조항 신설 등 제도개선 *'정보보호 및 개인정보보호 관리 체계 인증 등에 관한 고시' (과학기술정보통신부 고시 제 2021-27호 개정)
2022	- 정보보호 관리 체계 예비인증 특례 도입 등 제도개선 *'정보보호 및 개인정보보호 관리 체계 인증 등에 관한 고시' (과학기술정보통신부 고시 제 2022-46호 개정)

자료: KISA, 신한투자증권

ISMS-P 인증 개요



자료: 개인정보보호위원회, 신한투자증권

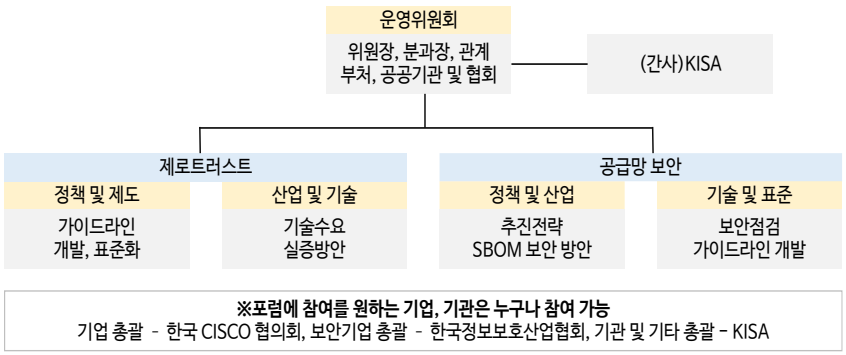
제로트러스트 • 공급망 보안 포럼 발족

차세대 보안 솔루션 제로트러스트 및 공급망 보안 포럼 발족

과학기술정보통신부와 한국인터넷진흥원은 22년 10월 '제로트러스트 • 공급망 보안 포럼 발족식'을 개최했다. 지능적인 사이버 위협에 대응하기 위해 기존의 한계를 뛰어넘어 새로운 보안체계로 주목받고 있는 '제로트러스트'와 '공급망 보안'이 국내에 안착할 수 있도록 논의하기 위한 자리이다.

사회 전반에 클라우드 컴퓨팅과 IoT 기기가 급증하며 네트워크가 확장되어 내부 자료 유출 등 피해가 급증하고 있다. 이에 따라 모든 대상에 대한 잠재적인 위협을 미리 식별하고 새로운 접근에 대해서는 거듭 확인하는 '제로트러스트'가 주목받고 있다. 이 날 포럼에서는 제로트러스트 가이드라인, 제로트러스트 국내 적용 사례, 공급망 보안성 강화를 위한 정책 방향 등을 발표 했다. 현재 국내 보안 기업들은 제로트러스트 트렌드에 맞추어 새로운 보안 시스템 및 소프트웨어 개발을 위한 투자를 진행하고 있다. 정부 또한 이러한 움직임에 따라 제로트러스트 • 공급망 운영위원회를 구성하여 국가 표준화를 목표로 추진 중이다. 정부와 기업의 노력에 기반한 새로운 보안 패러다임 구축은 아직 초입에 있다는 판단이다.

제로트러스트 공급망보안 포럼 분과 구성



자료: 과학기술정보통신부, 신한투자증권

사이버 안보 기본법 제정 및 컨트롤 타워 설립 추진

분권화 되어있던 사이버 안보 체계, 컨트롤 타워 설립 및 기본법 제정으로 일원화 추진

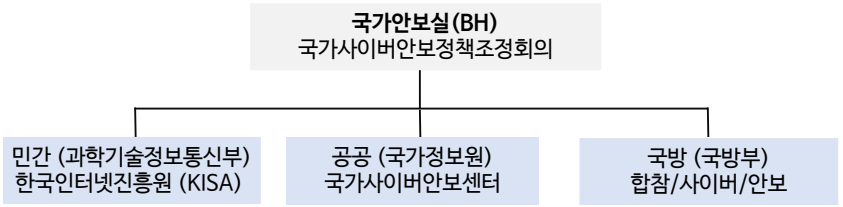
우리나라는 항공, 에너지, 우주 등 다양한 공공기관이 국가배후의 사이버 공격을 받은 것에 비해, 아직 사이버안보 위협 대응을 위한 국가 차원의 통일된 체계를 구축하지 못했다. 국가 혹은 공공기관의 경우 사이버보안 조직 및 예산 확보 업무를 비교적 체계적으로 수행하고 있으나, 민간의 경우 각각 별개의 정책에 따라 대응중으로 사이버 안보를 위한 개별 법령이 갖추어지지 못한 경우가 많다. 따라서 현행 체계로는 국가 사이버안보 위기가 발생할 경우 각 부처 역할에 혼선이 생겨 신속하고 통합적인 대응이 불가능하다.

현정부는 이러한 상황을 인지하고, 이에 대한 해결책으로 22년 11월 국가 사이버안보 기본법 입법을 예고 했다. 법안의 주요 내용에는 1) 대통령 소속의 국가사이버안보위원회 설치, 2) 중앙행정기관 등의 각 소관분야에 대한 예방, 대응 활

동 수행 책임, 3) 공급망보안 위협 예방 및 공세적 대응조치 마련, 4) 사이버 안보 위협 정보 공유, 5) 국회의 사이버안보 업무 소자, 감독권 등이 포함되어 있다. 현재 미국 등 사이버 강국은 몇 년에 걸쳐 국가차원의 사이버 안보 역량 강화를 위한 입법을 진행중이다.

사이버안보 기본법 제정 외에도 사이버안보 컨트롤 타워 설립을 추진중이다. 국가안보실을 중심으로 컨트롤타워 역할을 강화하고 공공, 민간, 국방 영역의 분절된 대응체계를 결집하겠다는 목적이다. 사이버안보 컨트롤타워(국가안보실)는 사이버안보 기본법, 국가위기관리기본지침, 국가사이버안보전략의 재개정을 주도하고 제도의 안착을 위해 주도적인 역할을 할것으로 기대된다. 사이버안보 기본법 제정과 컨트롤 타워 설립은 공공 뿐만 아니라 민간 기업에게도 보안 규제를 적용할 가능성이 높아 기업들의 보안 인프라 강화가 예상된다.

현행 사이버보안 대응체계



부처	법령	내용
과기정통부	정보통신망법, 기반보호법, 정보보호산업법	민간사업자 및 민간기반시설 사이버보안, 정보보호 산업 육성
국정원	국정원법, 기반보호법	공공기관 및 공공기반시설 사이버보안
국방부	국방정보화법	국방분야 사이버보안

자료: 과학기술정보통신부, 신한투자증권

정부의 사이버안보 관련 공약집

10. 사이버안보 위협 대처 능력을 제고하겠습니다.	
현재	사이버안보는 안보, 경제, 정치, 사회안전이 중첩되는 초국경적 사안이므로 관련기관, 기업 및 외국과의 정보공유와 협력이 중요 그럼에도 한국의 현 대응 체계는 국정원, 과기부, 외교부, 국방부, 경찰 등으로 분절되어 있어 정보공유와 협력을 통한 종합적 대응 불가
공약	1. 국가 차원의 일원화 된 사이버 대응 체계 구축 - 국가사이버안보 대응 시스템 구축 및 민관군 통합 대응체계 강화 2. 사이버보안 인재양성 - 불법적 사이버 공격에 실질적 방어가 가능한 실전형 인재 양성 - 정부가 전국 지역별 정규과정 및 특수과정 설립 적극 지원 3. 사이버안보 기술 발전 및 기업 지원을 위한 사이버안보 생태계 조성 4. 국제 사이버 협력 네트워크 구축에 적극 참여 - 사이버범죄 피해를 줄이기 위해 '부다페스트 사이버범죄협약' 가입 5. 사이버분야 무기체계 및 지원체계의 신속한 전력화 추진

자료: 사이버안보기본법 제정 관련 공약집 발췌, 신한투자증권

미국 사이버보안 관련 입법 현황

날짜	입법내용
2022.1.1	미국 일리노이주, 가정용 스마트기기 데이터 프라이버시 보호를 위한 '가정 프라이버시 보호법(PHPA)' 시행
2022.1.11	미국 상원, 공공 부문 사이버보안 역량 강화를 위한 '공급망 보안 교육법', '주정부 및 지역정부 사이버보안법' 통과
2022.1.13	미국 연방통신위원회, 통신사업자 고객 데이터 침해 시 보고 의무를 강화한 규칙 개정안 입법예고(NPRM) 검토 착수
2022.1.13	미국 하원, 웹사이트 서비스 약관에 대한 이용자의 이해도 향상을 위한 '서비스 약관 표시 등 가독성에 관한 법률' 발의
2022.1.18	미국 하원, 소비자를 대상으로 한 표적 광고를 금지하는 '표적 광고 금지법' 발의
2022.1.19	미국 백악관, 연방 부처 정보 시스템 사이버보안을 위한 구체적인 조치를 담은 메모랜덤 발표
2022.1.19	미국 펜실베니아주 상원, 랜섬웨어 공격에 대한 처벌 강화 및 사이버범죄자에 대한 공적자금 지급 금지 법안 통과
2022.2.3	미국 상하원, 자동화된 의사결정 시스템의 편향성 및 불공정성 완화를 위한 '알고리즘 책임성법' 동반 발의
2022.2.4	미국 NIST, 소비자 IoT 제품 사이버보안 라벨링 기준 권고안 발표
2022.2.9	미국 증권거래위원회, 사이버보안 위험 대응을 위한 투자자문사, 투자사 의무 규정 발표
2022.2.16	미국 상원, 온라인에서의 아동 보호를 위해 플랫폼에 다양한 의무를 부과하는 '아동 온라인 안전법' 발의
2022.3.1	미국 상원, 주요 기반시설에서의 사이버사고 보고 의무화 등을 포함한 '미국 사이버보안 강화법' 통과
2022.3.9	미국 대통령, 디지털 자산에 관한 정부의 추진과제를 설정한 '디지털 자산의 책임있는 개발 보장에 관한 행정명령' 서명
2022.3.9	미국 증권거래위원회, 사고보고 의무 강화 및 보안위기 관리 정책 공개 규정 제안
2022.3.9	미국 플로리다주 양원, 주 및 지방 정부의 사이버보안 역량 강화를 위한 법안 통과
2022.3.15	미국 대통령, '2022년 주요 기반시설 사이버사고 보고법' 서명
2022.3.22	미국 상원, 국토안보부의 사이버보안 프로그램을 명문화하는 '상시 진단 및 대응을 통한 사이버보안 향상법' 재발의
2022.3.31	미국 상원, 의료기기에 대한 사이버보안 강화를 목적으로 한 '사이버 헬스케어 보호 및 혁신법' 발의
2022.4.18	미국 하원, 연방 기관 IT 시스템의 데이터 보호를 위한 '양자 컴퓨팅 사이버보안 대비법' 발의
2022.4.28	미국 하원, '통신품위법' 제230조를 폐지하기 위한 '21세기 표현의 자유법' 발의
2022.5.4	미국 대통령, 양자정보과학 분야 국가경쟁력 강화를 위한 행정명령 및 국가안보각서 서명
2022.5.5	미국 대통령, 사이버범죄 정보 체계 강화를 위한 '사이버범죄 유형 비교체계 개선법' 서명
2022.5.10	미국 하원, '연방 순환 사이버인력 프로그램법' 및 '공급망 보안 교육법' 통과
2022.5.12	미국 대통령, 주 및 지방 등의 사이버보안 역량 강화를 위한 '국가 사이버보안 대비 컨소시엄법' 서명
2022.5.12	미국 상원, 디지털 플랫폼을 규제하는 감독기관 설립을 위한 '디지털 플랫폼 위원회법' 발의
2022.5.25	미국 상원, 대형 통신플랫폼의 독점 방지를 위한 '서비스 전환 보장을 통한 호환성 및 경쟁 증진법' 재발의
2022.6.7	미국 상원, 디지털 자산에 대한 포괄적 규제 프레임워크로서 '책임있는 금융혁신법' 발의
2022.6.21	미국, 지역의 사이버보안 훈련 지원 등을 위한 '주정부 및 지역정부 사이버보안법' 제정
2022.6.21	미국 하원, 경찰의 생체 인식 기술 활용을 제한하는 '신체카메라 얼굴 인식 금지법' 발의
2022.7.1	미국 플로리다주, 주 및 지방정부의 사이버보안 역량 강화 등을 위한 법률 시행
2022.7.7	미국 펜실베니아 주지사, 주 사이버보안 강화에 주방위군을 활용하는 법률안 서명
2022.7.12	미국 하원, 연방 기관 내 데이터 보호를 위한 '양자 컴퓨팅 사이버보안 대비법' 통과
2022.7.15	미국 하원, 사이버 취약점을 선제적으로 보완하기 위한 '사전예방적 사이버보안 전략법' 발의
2022.7.27	미국 상원, 데이터센터 사이버, 물리 보안 강화를 위한 '연방 데이터센터 개선법' 발의
2022.7.29	미국 뉴욕주 금융서비스부, 금융서비스 기업의 보안을 강화하는 '사이버보안 규정 개정안 초안' 공개
2022.8.22	미국 연방거래위원회, 소비자 데이터 보안 강화를 위해 '상업적 감시 및 데이터 보안에 관한 규칙 사전 입법예고' 발표
2022.9.21	미국 상원, 오픈 소스 소프트웨어의 안전한 활용을 도모하는 '오픈 소스 소프트웨어 보안법' 발의
2022.9.28	미국 상원, 디지털 자산 관련 기업의 사이버위협 정보 공유를 규정한 '암호화폐 사이버보안 정보 공유법' 발의
2022.9.29	미국 하원, 클라우드 보안 인증제도의 법적 근거 마련을 위한 'FedRAMP 인가법' 통과
2022.10.28	미국 솔라윈즈, 자사 제품 해킹 사건 관련 집단소송에 대한 잠정적 화해 합의 등 공개
2022.12.21	미국 대통령, 연방 IT시스템의 데이터 보호를 위한 '양자 컴퓨팅 사이버보안 대비법' 서명

자료: KISA, 신한투자증권

2023년 시행되는 보안, 안전 관련 주요 법령

시행일	법령
2023.1.1	도로교통법 시행령
2023.1.1	전파법 시행령
2023.1.1	방산원가대상물자의 원가계산에 관한 규칙
2023.1.1	자유무역협정의 이행을 위한 관세법의 특례에 관한 법률 시행규칙
2023.1.1	마리나항만의 조성 및 관리 등에 관한 법률 시행규칙
2023.1.1	건설기계 안전기준에 관한 규칙
2023.1.1	인신매매등 방지 및 피해자보호 등에 관한 법률
2023.1.1	출입국관리법
2023.1.1	산업안전보건법 시행규칙
2023.1.3	데이터 산업진흥 및 이용 촉진에 관한 기본법 시행규칙
2023.1.5	재난안전산업 진흥법
2023.1.12	클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률
2023.1.12	정보통신공사업법 시행령
2023.1.19	철도안전법
2023.1.22	도로교통법 시행규칙
2023.3.5	의료법
2023.3.11	원자력 안전법
2023.4.1	출입국관리법 시행규칙
2023.4.5	항공보안법 시행령
2023.4.19	중소기업 기술 보호 지원에 관한 법률
2023.4.23	전기안전관리법 시행규칙
2023.4.27	소방기본법
2023.4.27	자율방범대 설치 및 운영에 관한 법률
2023.5.16	경비업법
2023.5.16	**드론 활용의 촉진 및 기반조성에 관한 법률**
2023.5.16	소방기본법
2023.5.16	시설물의 안전 및 유지관리에 관한 특별법 시행령
2023.5.16	전자정부법
2023.6.11	공간정보의 구축 및 관리 등에 관한 법률
2023.6.11	미세먼지 저감 및 관리 등에 관한 법률
2023.6.11	생활주변방사선 안전관리법
2023.7.1	국가첨단전략산업 경쟁력 강화 및 보호에 관한 특별조치법
2023.7.1	산업안전보건기준에 관한 규칙
2023.7.4	도로교통법
2023.7.4	위험물 안전관리법
2023.7.21	공중화장실 등에 관한 법률
2023.9.25	**의료법 (CCTV 설치 의무화 관련 조항 포함)**
2023.10.19	전기안전관리법
2023.10.19	전기용품 및 생활용품 안전관리법
2023.10.19	산업안전보건기준에 관한 규칙
2023.11.16	전력기술관리법

자료: KISA, 신한투자증권

보안 관련 지원 확대

과기정통신부 2023년 보안 예상 편성

전년대비 사이버 보안 관련 예산 편성 증대, 보안 관련 지원 확대 전망

과기정통부의 2023년도 정부예산 중 정보보호 및 보안과 관련된 예산안은 약 3,000억원이다. 사이버침해사고 예방/대응 사업에 641억원, 정보보호전문인력양성 사업에 163억원, 정보보호 시스템 강화 사업에 22억원 등 보안 사업 육성을 위한 다양한 분야 및 사업에 예산을 편성했다. 정부 지출이 긴축 기조로 전환된 상황에서도 사이버 보안의 중요성이 부각돼 전년대비 190억 가량 증액됐다.

특히 정보보호 시스템 평가 및 인증강화 사업의 경우, 기존 보안인증과 기준이 없는 신기술 및 융합 제품을 대상으로 빠른 도입이 이루어질 수 있도록 신속확인제 도입을 추진한다. 기존에는 공공분야에 정보보호제품을 도입시 평가 기준이 있는 20여종만 도입이 가능했다. 신속확인제는 평가기준이 없는 신기술과 융복합 제품을 개발한 기업 및 스타트업의 고민을 해결하기 위한 제도이다. 신속확인 대상은 빅데이터 분석기반 지능형 통압보안 솔루션, 인공지능 기반 사이버 위협 인텔리전스 제품 등 기존 제도로 평가가 불가능하지만 새로운 보안 패러다임에 필요한 제품이다. 신속확인제도와 정보보호 시스템 평가 및 인증강화 사업은 민간 보안기업들의 신제품이 공공분야로 진출할 수 있는 발판이 될 것으로 기대된다.

디지털 융합보안 기반-디지털 안전 선도모델 개발 사업에도 40억원 가량을 배정했다. 2022년 집중호우로 인한 침수피해, 건축 중인 아파트 붕괴, 스토킹 살해 등 불안감이 가중됐다. 이와 같은 사고들은 기존 안전관리 시스템의 한계를 보여줬다. 이에 따라 위기 예측 및 대응을 강화하기 위해 '디지털 안전 선도모델' 개발 사업을 실시한다. 이번 사업에서는 도시 침수 대비, 맨홀 관제, 긴급 구조 등 인명과 재산을 보호하기 위한 첨단 디지털 안전 신서비스를 개발할 예정이다. 사회 기반 인프라를 디지털화하고, 신서비스로 발굴하기 위해서는 보안 시스템이 필수적이다. 사회 인프라를 디지털화 하는 과정에서 해킹 피해가 발생한다면 국민, 사회 모두가 피해를 입을 수 있기 때문이다. 정부도 이에 대한 중요성을 인식하고 다양한 보안 및 디지털 호환 시스템 구축을 논의 중이다.

2023년 정보보호 정책 사업 예산

구분	세부사업	금액 (억원)
사이버보안 인력양성	융합보안 핵심 인재 양성	67.6
	정보보호 전문 인력 양성	162.8
	지역 정보보호 교육 지원	23.8
	실전형 사이버 훈련장 구축	20.0
정보보호 산업육성	정보보호 산업 경쟁력 강화	74.2
	정보보호시스템 평가, 인증기반 강화	21.8
	전자서명인증	45.0
사이버보안 기술개발	암호화 사이버 위협 대응 기술 개발	30.0
	국방 무인이동체 사이버 보안기술 개발	17.7
	데이터 프라이버시 선도기술 연구개발	56.0
	비대멸 서비스 물리보안 통합플랫폼 운용체계 개발	40.0
	사이버 보안챌린지 선도기술 개발	33.0
사이버침해사고 예방/대응	해킹바이러스 대응체계 고도화	641.4

자료: 과학기술정보통신부, 신한금융투자

중소기업 정보보호를 위한 컨설팅, 솔루션 등 지원

중소기업을 위한 정보보호 역량강화 사업 시작, 정보보호지원센터 운영

중소기업 정보보호를 위한 '정보보호 역량강화' 사업이 추진된다. 과기정통부와 한국인터넷진흥원, 한국정보보호산업협회는 중소기업 8,300개사를 대상으로 정보보호 역량강화를 지원한다. 작년 접수된 랜섬웨어 비해 신고 223건 중 92%가 중소기업에서, 64%가 서울 외 지역에서 발생했다. 이로 인한 피해비용은 약 7,000억원에 달한다. 국내 피해 사례를 살펴보면 보안 수준이 낮은 중소 제조업체, 도매업, 서비스업 기업이 대다수를 차지한다. 코로나 이후 대기업뿐만 아니라 중소기업에서도 디지털 전환이 빠르게 이루어지며 기업이 보유하는 데이터 자산의 양과 질이 높아졌다. 재택근무와 비대면 업무환경이 정착되고 있지만 이에 비해 지역, 중소기업은 보안 솔루션을 이용할 투자 여력이 상대적으로 부족했다.

이에 과기정통부는 전국 10개 지역에 정보보호지원센터를 운영중이며, 2022년 1,300개의 중소기업을 대상으로 보안 솔루션 도입 지원사업을 진행했다. 이는 중소기업 600개사를 대상으로 정보보호 정책 수립, 네트워크 점검을 지원하고 알맞은 보안 솔루션을 도입할 수 있도록 비용을 지원해주는 사업이다. 클라우드 기반 보안서비스 도입 지원사업 또한 진행했는데, 이는 중소기업 700개사를 대상으로 원격에서 보안 기능 전반을 제공하는 클라우드 보안서비스 도입 비용을 지원해주는 사업이다. 이 밖에도 랜섬웨어로부터 중소기업을 보호하기 위한 '디지털 금고 지원사업', '랜섬웨어 대응 보안 솔루션 무상 지원사업' 등 중소기업의 보안 솔루션 이해도를 높이고, 보안 역량을 강화할 수 있는 기반을 마련했다.

정보보호 산업계 주도 랜섬웨어 대응 지원 보안솔루션

유형	솔루션명	공급기업	사용기간
〈패키지 1〉 이메일 보안, 모의훈련	머드픽스	지란지교시큐리티	1회
	악성메일 모의훈련	기원테크	1회
	EG Cloud(리시브가드 클라우드)	기원테크	3개월
	Receive Guard (리시브가드)	기원테크	3개월
	이메일 안티 랜섬웨어 방화벽 (서버형)	이글아이	6개월
	이메일 안티 랜섬웨어 방화벽 (클라우드)	이글아이	6개월
〈패키지2〉 랜섬웨어 탐지/차단	엔드포인트 안티 랜섬웨어 방화벽 (PC용)	세이퍼존	6개월
	엔드포인트 안티 랜섬웨어 방화벽 (서버용)	세이퍼존	6개월
	Ransom Cruncher	이노티움	12개월
	트루이피 업무 PC 통합보안	트루컷시큐리티	12개월
	사이버가드 안티-랜섬	ADT 캡스	6개월
	RansomEye	베일리테크	3, 6개월
	랜섬키퍼 라이트	시큐어링크	12개월
	새니톡스 EP	지란지교시큐리티	12개월
	innoMark Secure Home	이노티움	12개월
	알그리핀	시큐브	6개월
	오피스기퍼	지란지교소프트	6개월
	오피스메신저	지란지교소프트	6개월
	AhnLab V3 Office Security	안랩	3개월
	AIONCLOUD SWG	모니터랩	6개월
	DocStory	에스엠테크놀로지	3개월
〈패키지3〉 데이터 백업/복구	엔드포인트 안티 랜섬웨어 방화벽 (백업용)	세이퍼존	6개월
	Lizard Backup	이노티움	12개월
	Shadow Backup	두루안	6개월
	Crocheck EPM	코아맥스테크놀로지	3개월

자료: 과학기술정보통신부, 신한투자증권

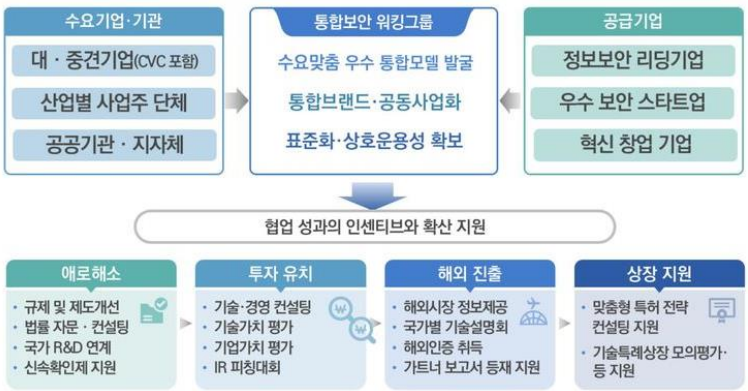
1,300억 규모 사이버 보안펀드 조성

사이버보안 대응 수요 증가에 미래 전략 사업으로 육성, 사이버보안펀드 조성으로 민간 투자 활성화

과학기술정보통신부는 9월 5일 정보보호산업 글로벌 경쟁력 확보 전략 발표를 통해 1,300억원 규모의 사이버 보안 펀드 조성하겠다고 밝혔다. 2027년까지 정보보호 산업 시장 규모 30조원 달성 및 세계 시장 5위권 진입을 목표로 관련 예산에 1.1조원 투입을 발표했다. 특히 국산 보안 기술로 대체한 한국형 무인점포 구축, 국산 CCTV 반도체 칩 보급 확대 등을 통해 우리나라가 기술적 강점을 갖고 있는 분야부터 국산화 추진을 시작했다. 또한 경기 판교, 동남권, 서울 송파 등에 분산되어 있던 보안 관련 시설을 통합할 수 있는 'K-시큐리티 클러스터 벨트'를 조성 의지를 밝혔다.

2027년까지 총 1,300억원 규모의 사이버 펀드를 조성해 기업의 안정적 기술 개발과 민간 투자 활성화를 지원할 계획이다. 펀드 결성액 중 절반 이상은 제로트러스트, AI 등 보안 관련 유망 분야의 스타트업 지원과 기업간의 인수합병을 통한 보안 시장 규모 확대에 쓰이도록 유도할 방침이다. 차세대 정보보호 기술을 위한 R&D 투자 또한 확대할 계획이다. 미래도전, 기술산업선도, 안보 투자로 구분하여 AI, 클라우드, 양자내성암호, 국가안보를 위한 투자 등 한 분야에 치우치지 않은 R&D 투자를 지속할 방침이다.

K-시큐리티 얼라이언스 추진체계



자료: 과학기술정보통신부, 신한투자증권

사이버보안 펀드 기본 구조

자료: 과학기술정보통신부, 신한투자증권

III. 사이버보안 솔루션

차세대 주요 사이버보안 솔루션

NGIPS(Next Generation Instrusion Prevention System)

최근 사이버 공격 트렌드에 걸맞는 NGIPS, 네트워크 최전방을 막아주는 보안 솔루션

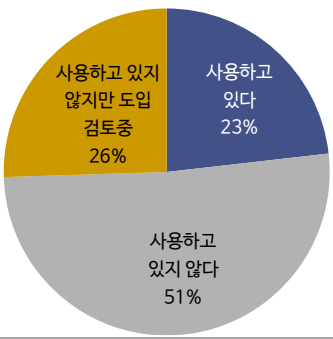
NGIPS는 차세대 침입방지 시스템으로 많은 양의 트래픽 처리, 정확한 탐지, 차단 등 보안 위협 대응의 핵심 역할을 수행중이다. 기존의 침입방지 시스템(Instrusion Prevetion System, IPS) 또한 방화벽, 디도스 방어와 함께 네트워크 최전방을 책임지는 보안 솔루션이다.

기존 IPS 시스템의 경우 네트워크 상에서 빠른 속도로 침입을 탐지하기 위해 플로(Flow)엔진을 사용한다. 플로엔진은 패킷을 모아 데이터 형태로 변환하여 검사하는 것이 아니라 패킷이 흘러가는 상황을 모니터링하여 공격을 탐지한다. 이러한 공격 탐지 유형은 IPS 장비를 쉽게 우회할 수 있도록 만들어 최근 사이버 공격을 완벽하게 방어할 수 없었다. 또한 기존의 IPS는 탐지 오류가 많아 이에 따른 튜닝작업이 필요하며, 꾸준한 장비 모니터링을 통한 최적화 작업이 필요하다.

최근 사이버 공격 트렌드를 살펴보면 공격자는 복잡한 네트워크를 악용해 보안의 사각지대를 공격한다. 하지만 최근 사이버 공격은 기존 IPS로 탐지가 어려운 부분이 많아 NGIPS 개념의 장비가 등장했다. NGIPS의 경우 애플리케이션을 인지하거나 다양한 시스템과 연동할 수 있다. 또한 APT 공격 방어 기능이 탑재되어 있어 다양한 외부 시스템과도 연동이 가능하다.

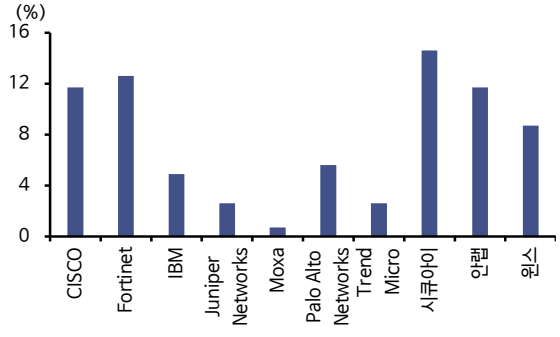
NGIPS의 경우 기존 IPS를 발전시킨 형태이기 때문에 정확한 기능으로 정의되는 것은 아니다. 각 보안 업체별로 기존 IPS를 최신 보안 트렌드에 맞추어 업그레이드 한 형태이기 때문이다. **시큐아이**의 경우 기존 유해 트래픽 대응 위주였던 IPS를 보완하여, 위협트래픽을 정밀하게 탐지하고, 전송되는 파일을 식별하여 랜섬웨어를 탐지하는 NGIPS를 출시했다. **안랩**의 경우 1) 트래픽, 멀웨어 기반 보안 위협 탐지, 2) 악성 URL 필터링, SSL 트래픽 검사, 3) 빅데이터 처리 고성능 분석 엔진 등 다양한 기능을 추가하여 기존 IPS와 차별화했다. 이처럼 각 보안 업체에서 새로운 IPS를 출시하고 있어, 이에 따른 매출 성장이 기대된다.

NGIPS 도입 비중



자료: 과학기술정보통신부, 신한투자증권

NGIPS 솔루션 기업 선호도



자료: 보안뉴스, 신한투자증권

EDR (Endpoint Detection Response)

EDR: 실시간 보안위협 탐지, 단순 차단을 넘어 자체 대응까지 진행

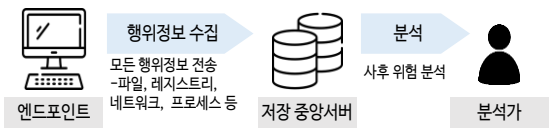
EDR은 실시간으로 보안위협 참지, 분석, 대응이 가능한 엔드포인트 보안 솔루션이다. 과거 네트워크 기반의 '차단'을 넘어 단말(Endpoint) 기반의 '탐지와 대응'을 통해 이상행위를 차단한다. EDR 솔루션은 악성코드의 유입 뿐만 아니라 취약점을 이용한 내부 확산을 탐지하고, 위협을 추적해 신속하게 대응할 수 있다.

2010년대 초반까지만 해도 EDR 솔루션 시장은 맨디언트, 사일런스 등 미국과 이스라엘 기업이 시장의 90% 이상을 차지했다. 2018년 이후 시만텍, 시스코 등이 합류하고 2020년에는 네트워크 기업이 EDR기업을 인수하면서 글로벌기업 중심의 M&A가 활발히 이뤄졌다. 현재 블랙베리, 시스코, IBM 등이 EDR 솔루션의 대표 사업자로 여겨진다.

국내의 경우 2015년 EDR이 최초로 도입됐다. 2017년 지니언스, 2018년 안랩과 엔피코어, 이스트시큐리티 등이 솔루션을 개발해 시장에 진출했다. 2018년 이후 은행과 공공기관을 중심으로 EDR 수요가 발생하여 차세대 보안 솔루션으로 주목받기 시작했다. 그러나 코로나19 영향으로 클라우드, 재택근무 솔루션에 관심이 집중되며 시장 성장이 둔화되었다. 특히 대형시장으로 손꼽혔던 금융권 등에서 경기 둔화로 인한 IT 투자를 연기하며 성장 속도가 더뎌지기도 했다. 그러나 2021년 하반기부터 랜섬웨어, APT 공격 등 고도화된 공격이 심화되며 코로나19 악재로 EDR 사업을 연기했던 공공기관, 기업의 수요가 서서히 증가하고 있다.

2021년 하반기 한국인터넷진흥원은 공공, 민간기업을 대상으로 수요조사를 진행해 정보보호제품 성능평가 제품으로 'EDR' 솔루션을 선정했다. 신규 성능평가 제품군으로 선정후, 2022년 사업계획에 포함돼 성능평가 기준 등 평가항목이 구성됐다. 2023년부터 EDR 솔루션에 성능평가 기준이 적용되며, EDR의 기능과 성능을 구체화할 수 있다. 이에 따라 소비자는 니즈에 따라 다양한 EDR 솔루션 선택이 가능하며, 개발기업 역시 소비자의 선택을 받기 위해 기능을 강화 할 수 있어 전반적인 EDR 시장 성장이 기대된다.

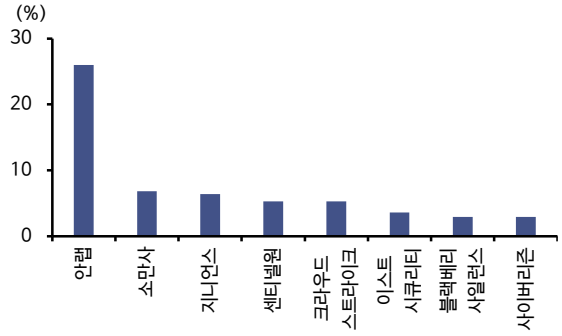
EDR 솔루션 도식



Threat Hunting	- 특정 이벤트 중심이 아닌 전체적, 연속적인 행위 정보 수집 및 저장 - 필요 시 언제든 위협 및 관련 정보 확인 가능, 사후 위협 분석 가능
중앙화	- 중앙화된 로그 관리, 모든 엔드포인트 로그를 중앙 서버에 저장 - 로그 관리 및 분석 편의성 향상

자료: 신한투자증권

EDR 솔루션 기업 선호도



자료: 보안뉴스, 신한투자증권

클라우드 보안

클라우드 사용자 급증에 따른 클라우드 전용 보안 솔루션 수요 증가

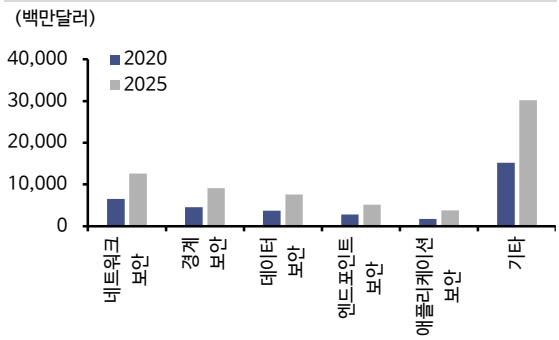
클라우드 보안은 앞서 살펴봤던 EDR, IPS처럼 특정 솔루션을 지칭하는 것이 아니다. '클라우드'를 보호하고 적절한 보안 솔루션을 적용하는 것 자체를 '클라우드 보안'이라고 지칭하며, 최근 클라우드 사용자가 급증함에 따라 그 중요성이 커지고 있다. 클라우드 이용절차 합리화 및 망분리 규제완화를 위해 금융위원회에서 의결한 '전자금융감독규정' 개정안이 2023년부터 시행되고 있다.

이번 개정안은 클라우드, AI 등 디지털 신기술에 대한 금융권의 수요를 반영했다. 개정안에는 1) 클라우드 이용 업무의 중요도 평가 기준 마련, 2) 클라우드서비스 제공자(CSP)의 건정성 및 안정성 평가항목 정비, 3) 클라우드 이용시 사전보고 대신 사후보고 채택, 제출 서류 간소화, 4) 연구 개발 분야의 망분리 규제 완화 내용을 담고 있다. 이러한 규제완화를 통해 클라우드 사용이 증가하고 있으나 기업의 클라우드 보안은 여전히 어려운 문제이다. 클라우드 보안위협은 일반 보안위협과 공유보안위협이 존재한다. 일반 보안위협은 비인가자 접근, 시스템 취약점 공격, 랜섬웨어 등 클라우드 서비스 이용시 영향이 큰 위협이다. 클라우드 서비스 고유의 보안위협은 연결된 API 공격, 가상화 취약점 공격 등이 있다.

클라우드 보안 위협이 증가하는 상황에서, 클라우드 보안 솔루션 및 서비스를 도입하기 위해서는 클라우드 보안의 특수성을 고려해야한다. 클라우드 보안의 특수성이란 첫째, 클라우드 서비스 제공사에서는 기본적인 보안만 제공한 후, 클라우드 도입 조직이 책임져야 하는 문제가 대부분인 경우가 많다. 클라우드 서비스 도입 조직에서는 적절한 보안 솔루션을 자체적으로 도입하거나, 클라우드 운영관리 서비스를 이용해야한다. 클라우드 환경이 익숙하지 않은 중소기업의 경우, 클라우드 보안 전문 MSP를 활용해 보안 인프라를 운용하는 경우도 많다.

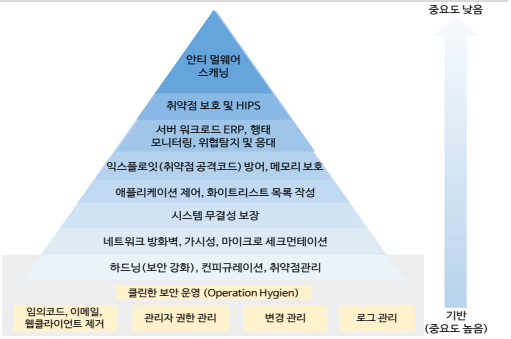
둘째, 클라우드 서버는 기존 서버와 운영, 관리 체계가 상이하다. 특히 컨테이너 등 새로운 환경에서 서비스 운영이 이루어지기 때문에 클라우드 환경에서 발생할 수 있는 다양한 위협요소에 대한 파악이 우선시 되어야한다. 이에 따라 서버, 가상머신, 컨테이너 등 다양한 클라우드 환경을 보호하기 위한 주요 보안기능을 포함한 CWPP(Cloud Workload Protection Platform) 등이 주목받고 있다.

글로벌 클라우드 보안 유형별 시장 규모 및 전망



자료: Marketsandmarkets, 신한투자증권

CWPP 제어 계층도



자료: 가트너, 신한투자증권

API 공격 시도 급증, API 전용 보안 솔루션 WAPP에 주목

API (Application Programming Interface)

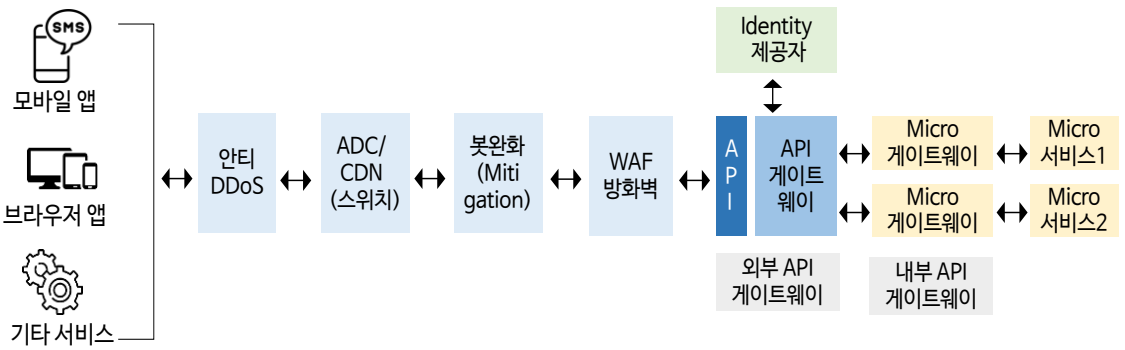
API 는 프로토콜 집합을 사용해 두 소프트웨어가 서로 통신할 수 있게 해주는 매커니즘이다. 최근 개발되는 대부분의 애플리케이션에는 API가 자연스럽게 포함되어 있다. 또한 국내에서는 22년부터 API 사용을 법적으로 의무화한 마이데이터 서비스도 시행되었다. API 프로그램 개발을 보다 쉽게 해주기 때문에 기업에서 API 사용은 빠르게 증가하는 추세이며, API의 사용은 웹 환경에서 점점 당연한 것이 되어가고 있다.

2022년 상반기 API 공격시도는 2021년보다 수백배 급증했고, API 남용과 데이터 침해사고는 2024년도까지 약 2배가량 증가할 것으로 예측됐다. API는 민감한 데이터가 저장된 백엔드 데이터베이스에게 직접 연결되기 때문에 해커가 이를 직접 노리는 경우가 많다. API 보안사고는 데이터 유출, 데이터 스크래핑, 계정 탈취 등이 있으며 기업 상당수가 이와 관련한 문제를 겪고 있다.

API 보안위협을 해결할 가장 진화된 솔루션은 'WAPP(Web Application and API Protection)'이다. 이는 웹 애플리케이션 보호, DDos 방어, 봇 관리, API 보호와 같이 4가지의 핵심기능을 보유하고 있다. WAPP는 웹 방화벽의 최신 솔루션으로서, 웹방화벽에 API 보안 기능이 추가된 개념이라고 볼 수 있다.

국내에 API가 보편화 된 것에 비해 WAPP의 인지도는 상대적으로 낮다. 아직도 API 보안을 위해 어떤 장비를 도입해야하는지 명확한 가이드가 없어 정보보호 담당자들도 정확한 판단을 못내리고 있다. 글로벌 시장에서는 이미 API 보안을 위한 장비로 WAPP를 도입하고 있으며, 이는 API 10대 취약점에 대한 대응이 가능한 솔루션이다. 특히 국내 마이데이터 서비스가 보편화되고, 웹 3.0 시대가 개화하며 API에 대한 보안은 필수적인 요소가 될 것이다.

API 게이트웨이와 기타 장비와의 관계



자료: 가트너, 신한투자증권

사이버보안 분야별 수요

2023년 공공부문의 정보보호 사업 규모가 6,178억원으로 전망됐다. 정보보안 서비스는 3,883억원, 정보보안 제품은 1,779억원으로 책정됐으며, 이밖에 물리보안 관련 사업규모는 500억원 가량이다. 과기정통부의 2023년 공공부문 소프트웨어, ICT(정보통신기술), 정보보호 예정수요에 따르면 2023년 총 사업금액 예정치는 약 5조 7,500억원이다. 이는 전년대비 7% 증가한 수치이며, ICT 장비를 제외한 소프트웨어 수요는 총 4조 4,500억원 가량이다.

공공부문 SW/ICT 장비 총 사업금액

(단위: 억원, 건,%)		전체	증감률	SW사업	비중	ICT장비	비중
2022년	금액	53,813	8.9	43,156	80.2	10,657	19.8
	건	13,998	5.1	10,381	74.2	3,617	25.8
2023년	금액	57,522	6.9	44,545	77.4	12,977	22.6
	건	14,402	2.9	10,805	75.0	3,596	25.0

자료: 과학기술정보통신부, 신한투자증권

공공부문 ICT장비 구매 사업금액

(단위: 억원, 건, %)		전체	컴퓨팅	비중	네트워크	비중	방송	비중
2022년	금액	10,656	7,940	74.5	2,261	21.2	455	4.3
	건	3,617	2,186	60.4	1,173	32.4	258	7.1
2023년	금액	12,977	10,176	78.4	2,324	17.9	477	3.7
	건	3,596	2,049	57.0	1,283	35.7	264	7.3

자료: 과학기술정보통신부, 신한투자증권

공공부문 정보보호 관련 구매 사업금액

(단위: 억원, 건, %)		전체	정보보안				물리보안			
			서비스	비중	제품	비중	서비스	비중	제품	비중
2022년	금액	6,064	3,784	62.4	1,754	28.9	150	2.5	376	6.2
	건	4,771	1,672	35.0	1,960	41.1	956	20.0	183	3.8
2023년	금액	6,178	3,883	62.9	1,779	28.8	165	2.7	351	5.7
	건	4,766	1,874	39.3	2,102	44.1	592	12.4	198	4.2

자료: 과학기술정보통신부, 신한투자증권

해당 조사결과는 2023년 예산이 확정되지 않은 상황에서 조사한 내용으로, 일반적으로 예산 확정시 더 증가하는 경향이 있다. 과학기술정보통신부 정책관은 2023년도 공공 SW, ICT장비, 정보보호 사업규모는 지속 증가할 것으로 전망된다고 밝혔다. 이 외에도 디지털 세상 속 '잊혀질 권리'를 위해 개인정보보호 예산을 증액하고, 가명정보 플랫폼 구축을 위해 예산을 확보하는 등 다양한 분야에서 공공분야 투자가 증가하고 있다. 다수의 SW, ICT, 정보보호 기업들이 코로나19 이후 기업의 투자 감소로 어려운 시기를 보냈다. 2023년 이후 공공분야부터 늘어난 수요를 바탕으로 다시 한번 도약할 기반을 마련할 수 있을 것으로 기대된다.

1. 네트워크 보안

비대면 환경, 재택근무 확대로 네트워크 보안 시장 급성장 중

네트워크 보안 시장은 2022년 전년대비 10% 이상 급성장했다. 이는 코로나 팬데믹 이후 비대면 환경의 증가, 재택근무의 확대, 디지털 전환 등으로 인해 대대적인 네트워크 보안 강화가 이뤄졌기 때문이다. 2023년 네트워크 보안 시장규모는 전년대비 6.1% 성장한 5,400억원 가량으로 예측되며, 2026년까지 연평균 6% 이상의 성장이 기대된다.

네트워크 보안 시장의 성장과 함께, 관련 국내 기업들의 매출도 증가세에 있다. 국내 네트워크 보안 관련 사업자는 '시큐아이', '한드림넷', '엑스게이트' 등이 있다. 시큐아이는 네트워크 보안 솔루션의 고도화를 진행중이며, 네트워크 보안에 기반한 클라우드 보안, 원격 관제 솔루션 등을 제공중이다. 한드림넷은 네트워크 보안스위치 수출로 21년 1,000만 달러 수출을 달성했다.

기업의 네트워크 보안 솔루션이 고도화됨과 동시에, 정부의 네트워크 보안에 대한 관심도 증가하고 있다. 원희룡 국토교통부 장관은 지능형 홈네트워크 및 아파트 해킹 문제 개선을 위한 간담회를 개최하고, 관계 부처와 함께 홈네트워크 보안 강호를 위한 제도 개선 추진 의사를 밝혔다. 정부의 2023년 보안 예산안에 따르면, 네트워크 보안 소프트웨어에 가장 높은 예산을 책정한 곳은 한국전기안전공사 전사 망분리 구축(14억 400만원) 사업이다. ICT 보안 장비 구매 예산의 경우 국방부의 암호 장비 사업에 262억원이 책정됐다. 발전소, 국방 등 중요 사회 기반시설을 기반으로 네트워크 보안을 강화하고 있는 추세다.

네트워크 보안 예산 책정

기관명	품목명(용도)	구매예산(억원)
- 네트워크 보안_SW 구매		
한국전기안전공사	전사 망분리 구축	14.0
한국남부발전	정보보안 설비 국산화 및 보안강화	7.2
한국감정원	정보보호 모니터링 강화	6.7
한국지역난방공사	데이터센터 가상화(SDDC) S/W 증설	6.0
산업통상자원부	방화벽, 서버팜 교체	6.0
한국남부발전	방화벽 통합정책 관리 및 자동화 시스템 구축	4.1
산업통상자원부	정보보호프로그램 구입	2.8
국무조정실	정보보호 시스템	2.2
- 네트워크 보안_ICT 장비		
국방부	암호장비사업	262.7
대법원	사법 망분리 구축	32.2
강원랜드	네트워크 접근통제(망간분리) 고도화 관련 장비	16.3
한국전력거래소	설비 보강 및 노후설비 교체	12.8
해양수산부	사이버안전센터 솔루션장비구매	10.0
한국지역난방공사	데이터센터 가상화 H/W 증설	6.3
대한적십자사	NAC(네트워크접근제어) 구축	5.5
서울주택도시공사	유해사이트차단 시스템 및 개인정보 DLP 교체	4.3
서울특별시 상수도사업본부	노후정보보호 시스템 교체	4.1

자료: 시큐리티월드, 신한투자증권 / 주: 구매예산 순으로 상위 10개 나열

2. 시스템(단말) 보안

랩탑, 스마트폰 등의 기기를 보호하기 위한 엔드포인트 보안 각광

시스템 보안의 주요 과제는 계정 관리, 세션관리, 접근제어, 권한관리, 로그 관리, 취약점관리이다. 최근 이러한 과제를 해결하기 위해 시스템 보안 중 엔드포인트 보안이 각광받고 있다. 엔드포인트 보안 솔루션은 랩탑이나 스마트폰 같은 컴퓨팅 기반의 기기들을 보호하기 위해 호스트 기반 소프트웨어 제품들을 사용한다.

EDR, XDR 등 적극적인 신제품 출시와 함께 2022년 시스템(단말) 보안 시장 규모는 전년대비 12% 성장했다. 2022년 시스템(단말) 보안 시장규모는 2,700억원으로, 2024년 3,000억원을 돌파할 것으로 전망된다. 시스템 보안 시장규모는 네트워크 보안시장과 마찬가지로 10%이상의 고성장세를 보였는데, 성장 이유 역시 비슷하다. 비대면 환경의 증가, 원격근무의 증가로 시스템 및 단말기에 대한 보안을 강화하려는 움직임이 늘어난 것이다. 특히 2022년에는 대기업 해킹이 다수 일어났고, 러시아-우크라이나 사이버전에 대한 관심이 증가하며 본격적으로 시스템 보안 시장이 주목받기 시작했다.

글로벌 엔드포인트 보안 시장규모 역시 연평균 12%의 성장률을 기록하고 있다. 이에 따라 보안기업들은 적극적으로 시스템 보안 솔루션을 선보이고 있다. 안랩은 2022년 차세대 엔드포인트 위협 대응 솔루션 '안랩 EDR'을 출시했다. IBM은 랜섬웨어를 위한 솔루션으로 차세대 EDR 플랫폼을 출시하여 다양한 운영체제 및 엔드포인트를 한번에 관리할 수 있도록 편의성을 강화했다. 보안담당자 설문조사에 따르면 1년 이내 엔드포인트 위협 탐지 대응(EDR) 솔루션 도입 계획을 가진 기업은 약 27%로, 공공기관 외 민간 기업에서도 빠른 도입이 기대된다.

시스템(단말) 보안 예산 책정

기관명	품목명(용도)	구매예산 (억원)
- 시스템(단말) 보안_SW 구매		
경기도교육청	스마트단말 관리 시스템(MDM)	33.5
국민연금공단	방화벽	16.1
행정안전부	클라우드 엔드포인트 통합보안SW	9.4
한국산업기술평가관리원	사무 및 보안 소프트웨어 갱신	8.0
충청북도교육청	정보화역기능예방 S/W	7.9
국세청	백신 등 S/W	7.3
의왕시청	리눅스서버백신 소프트웨어	7.1
- 시스템(단말) 보안_ICT 장비		
서울특별시	[정보통신보안담당관] 지능형 악성코드 대응 시스템 교체	7.1
산업통상자원부	노후장비교체	5.3
외교부	노후 정보보호 시스템 교체	4.0
한국국토정보공사	랜섬웨어 무해화 시스템	4.0
전북 김제시	사이버침해사고 예방을 위한 정보보호 시스템 교체	3.5
기상청	정보보호 시스템(위협관리 시스템 센서) 구매	2.9
철원군청	통합관제센터 시스템 교체	2.9
서울특별시강서구청	정보보안 시스템 교체	2.7
충북대학교 병원	엔드포인트 탐지 및 대응(EDR) 솔루션 구매	2.4

자료: 시큐리티월드, 신한투자증권

3. 콘텐츠/정보유출 방지보안

머신러닝, AI 기술을 활용한 콘텐츠 유출 방지보안 솔루션 개발 활발

콘텐츠/정보유출 방지 보안 시장도 코로나19 펜데믹 수혜를 가장 많이 입은 분야 중 하나다. 2022년 콘텐츠/정보유출 방지 보안 시장규모는 3,800억원으로 전년대비 11.4% 성장했다. 올해는 전년대비 6% 성장한 4,000억원이 예상된다. 클라우드 서비스 활성화에 맞춰 클라우드 기반의 콘텐츠, 정보유출 방지 솔루션을 제공하는 기업들도 등장하며 꾸준히 시장이 확대되었다.

또한 기존 시그니처나 샌드박스가 아닌 머신러닝, AI 기술을 활용한 솔루션도 시장에 출시되고 있다. 문서, 데이터 보안을 통합한 솔루션도 개발되고 있다. 이노티움은 문서중앙화 기술을 포함해 DRM, DLP 기능 통합, 개인정보 보호, 데이터 백업 등 다양한 콘텐츠 보안 기능을 하나의 데이터베이스와 중앙관리로 통합시킨 솔루션을 출시했다.

정부에서도 정보유출 방지를 위한 보안 강화 움직임을 보이고 있다. 특히 금융감독원은 2023년 1월, 저축은행중앙회, 저축은행과 함께 TF(Task Force)를 구성해 금융사고 예방 및 내부통제 개선을 위한 종합 대책을 마련하겠다고 밝혔다. 이번 대책에서는 문서를 수기로 작성하여 발생했던 문서 조작 등의 보안사고를 방지하겠다고 말했다. 문서 보안을 강화하고, 전결제도의 취약점을 보완하는 등 내부통제를 한층 업그레이드하는 방향을 설정했다. PF 대출, 개인사업자 대출, 자금관리 등 고위험 업무에 대해 별도의 콘텐츠 유출 방지 보안 시스템을 설정해 선제적으로 사고를 예방할 예정이다. 금감원은 올해 1분기 중 신분증 사본 판별시스템 도입, 생체인증 시스템 도입, 단말기IP-업무담당자 연동제 도입 등 금융보안 강화 조치를 단계적으로 시행할 계획이다.

시스템(단말) 보안 예산 책정

기관명	품목명(용도)	구매예산 (억원)
- 콘텐츠/정보유출 방지보안_SW 구매		
한국감정원	정보유출 방지 시스템	22.9
한국국토정보공사	가명정보 결합기관 솔루션	3.0
한국자산관리공사	이메일 개인정보 필터링 시스템	2.6
부산대학교 병원	개인정보 유출 차단 솔루션	2.1
한국탄소산업진흥원	그룹웨어보안강화	2.1
한국도로공사서비스	개인정보접속기록관리 솔루션 도입	2.0
국민건강보험공단	DB암호화	2.0
- 콘텐츠/정보유출 방지보안_ICT 장비		
중소기업은행	침해시도 상세 분석을 위한 트래픽 분석 시스템 고도화	3.8
문화재청	침입방지 시스템 등	3.2
국토교통부	위협관리 시스템	2.6
식품의약품안전처	정보보호 및 정보통신 기반 강화	1.2
부산광역시의료원	개인정보보호 솔루션 도입	1.0
전북대학교병원	개인정보 비식별(가명, 익명) 처리 솔루션	1.0
대구광역시 서구청	정보 시스템통합관리솔루션(EMS) 구입	1.0

자료: 시큐리티월드, 신한투자증권

4. 암호/인증 보안

양자 컴퓨팅, 생체인증 시장이 커지며 암호, 인증 보안 시장 성장

2022년 암호/인증 시장 규모는 1,100억원으로, 전년대비 11%가량 증가했지만 아직 기타 보안 시장에 비해 작은 규모를 형성하고 있다. 비록 암호/인증 보안의 국내 시장 규모는 상대적으로 작지만, 양자컴퓨터의 등장과 함께 양자암호, 동형암호 등 차세대 기술이 주목받으며 꾸준히 성장 중이다. 이에 따라 2024년 약 1,200억원의 시장규모 달성이 기대된다.

구글은 2022년 12월 자사 이메일 서비스인 지메일에 종단간 암호화 기술을 적용했다. 이 기능은 구글 드라이브, 독스, 미트, 캘린더 등에 이미 적용되어 있었던 것으로, 이번 구글 워크스페이스와 교육 관련 기능에도 확대 적용되었다. 애플도 2022년 12월 '아이클라우드를 위한 고급 데이터 보호기능'을 출시했다. 아이클라우드 내 민감한 데이터 보호를 위해 종단간 암호화를 시행하는 기능이며, 암호화된 클라우드 데이터가 사용자 지정 기계 내에서만 복호화 되는 개념이다.

국내에서는 통신사를 중심으로 양자암호에 대한 연구를 지속하고 있다. SKT는 양자암호통신 대중화를 위해 ITU-T 국제 회의에서양자암호통신망 기술 2건을 제안해 국제 표준화 과제로 채택됐다. 이 외에도 KT, LG U+에서도 양자내성암호 인프라를 구축하는 등 양자암호통신 기술 개발에 힘쓰고 있다.

암호 보안 시장 뿐만 아니라 인증 시장도 규모가 확대되고 있다. 공급망 보안이 다양한 공격을 받으며 논란이 되자 인증에 대한 중요성이 대두되었다. 정부 역시 이를 위한 여러 지원을 아끼지 않고 있다. 2022년 9월 간편인증을 도입하는 기관 및 기업들이 개별적으로 서비스를 연동하는 불편함을 해소하기 위해 '간편인증 통합모듈'을 만들어 제공했다. 디지털 세계가 넓어질수록 정보의 암호화 및 인증은 공공, 민간 시장을 가리지 않고 도입이 확대될 것으로 기대된다.

암호/인증 보안 예산 책정

기관명	품목명(용도)	구매예산(억원)
- 암호/인증 보안_SW 구매		
공영홈쇼핑	보안솔루션 구매	14.0
기획재정부	서버접근제어 등	7.3
한전KDN	노후 패키지 S/W 교체	4.9
중소기업은행	신분증 촬영 인식 및 실시간 도용방지 솔루션 도입 추진	4.8
한전 KPS	PC DRM 서버/클라이언트 모듈 S/W	4.0
한국도로공사	데이터 암호화(영업)	2.7
- 암호/인증 보안_ICT 장비		
한국전력공사	전력설비(FA)망 정보보호설비 구축	12.4
중소기업은행	업무용 PC 바이오인증 시스템 구축	11.2
코레일네트웍스	정보보호솔루션	2.3
공정거래위원회	VPN	2.1
충청남도 천안시청	암호화장비(VPN) 노후 교체	1.9
광주광역시 동구청	보안장비	1.5
한국국토정보공사	DB접근제어 시스템 확대	1.5

자료: 시큐리티월드, 신한투자증권

5. 보안관리 및 보안컨설팅

보안 솔루션을 관리해주는 컨설팅 시장 확대, 주로 중소기업을 대상으로 한 시장 개화 중

보안관리는 내외부에서 기업을 위협하는 공격이 다양해지고 지능화되며 보안을 효과적으로 관리하기 위한 솔루션을 말한다. 최신 솔루션인 SOAR(Security Orchestration Automation and Response)를 비롯해 통합보안관리(ESM), 위협관리 시스템(TMS), 디지털 포렌식 시스템 등을 포함한다. 2022년 보안관리 시장규모는 1,722억원으로 2025년까지 연평균 5% 내외의 성장이 기대된다.

국내외 기업들 또한 차세대 보안 솔루션으로 손꼽히는 'SOAR' 개발 및 고도화를 위해 노력중이다. 휴네시온 계열사 시큐어시스템즈는 Secure SOAR 구축 및 운영에 나섰으며, 글로벌 보안기업 스윔레인은 로우코드로 SOAR를 구동하겠다고 밝혔다. 이글루코퍼레이션은 자체 SOAR 시스템으로 GS등급 1등급을 획득해 시장 선점에 나섰다.

보안컨설팅의 경우 주로 중소기업을 대상으로 이뤄진다. 보안 이슈들이 대두되며 보안 강화에 나섰지만 어떻게 시작해야할지 모르는 회사들을 대상으로 보안컨설팅을 진행한다. 과기정통부와 KISA, KISIA는 중소기업 8,300개사를 대상으로 정보보호 역량강화 지원에 나서겠다고 밝혔다. 실제로 2022년 1,300개의 중소기업을 대상으로 정보보호 컨설팅 및 보안 솔루션 도입 지원사업을 운영했다. 대기업 및 IT기업의 전유물로 여겨졌던 보안 시스템이 급격히 중소기업을 포함한 일반 기업에 도입되기 시작하면서, 현 시점에서 보안 컨설팅 시장은 빠르게 성장할 수 있을 것으로 기대된다.

암호/인증 보안 예산 책정

기관명	품목명(용도)	구매예산 (억원)
- 보안관리 및 컨설팅_SW 구매		
고용노동부	정보 시스템 구축 개선사업	43.9
한국교육학술정보원	2023 교육정보시스템 주요정보통신기반시설 통합 취약점 분석평가 사업	37.7
경기도청	사이버침해대응센터 운영, 주요정보통신기반시설 컨설팅	10.9
경찰청	PC 보안관리	9.3
인천대학교	정보자원 통합 유지보수	8.2
국회사무처	국가 전략, 정책 빅데이터 구축을 위한 ISP	6.9
충청남도청	보안 S/W	6.4
건강보험심사평가원	2023년 정보보안컨설팅	6.0
- 보안관리_ICT 장비		
금융감독원	정보보호장비(정보보안 등)	11.2
인천국제공항공사	정보보호 시스템	8.9
한국도로공사	방화벽(민자 인프라보안장비 교체)	8.0
대구광역시청	정보보안 시스템 교체 및 보강	6.5
한국자산관리공사	망연계 시스템 교체 및 버전 업그레이드(HW/SW)	6.0
제주특별자치도청	네트워크접근제어 시스템(NAC)고도화 구축	5.3
국민건강보험공단	DNS	4.8
한국의료분쟁조정중재원	정보보안 장비	4.5
국민건강보험공단	FW대민포털	3.8

자료: 시큐리티월드, 신한투자증권

IV. Appendix

국내 사이버 보안기업 공공조달 실적

2021, 2022년 국내 사이버보안 기업 공공조달 실적 추이

2022년 (1~10월)			2021년		
업체명	계약건수	금액 (억원)	업체명	계약건수	금액 (억원)
이글루코퍼레이션	42	494.9	이글루코퍼레이션	80	538.5
쿠도커뮤니케이션	372	279.6	펜타시스템테크놀러지	22	389.2
에스케이쉴더스	239	228.9	윈스	180	320.2
아이티로그인	612	200.1	쿠도커뮤니케이션	428	263.2
윈스	188	170.8	아이티로그인	1,086	240.1
펜타시스템테크놀러지	20	153.0	케이사인	138	226.7
휴네시온	160	106.2	굿모닝아이텍	34	144.0
이스트소프트	1,484	91.6	휴네시온	156	107.1
지니언스	190	88.5	파수	143	106.3
모비젠	16	87.2	에프원시큐리티	20	99.1
소만사	116	86.7	마크애니	182	92.7
영림원소프트랩	33	71.3	이스트소프트	1,740	92.6
한싹	110	62.1	지오멕스소프트	136	85.5
한컴위드	93	61.0	지니언스	262	85.1
엑스게이트	255	58.4	한싹	134	83.2
굿모닝아이텍	16	58.1	한컴위드	133	76.1
지란지교데이터	152	55.4	우리아이티	34	72.3
파이오링크	16	52.1	라온시큐어	102	67.0
마크애니	113	51.7	엑스게이트	238	60.8
케이사인	92	50.2	위즈코리아	110	57.8
파수	89	49.3	파이오링크	28	57.2
라온화이트햇	75	42.7	지란지교데이터	167	55.9
에스큐브아이	26	39.6	드림시큐리티	100	49.3
우리아이티	23	39.5	오픈베이스	3	48.0
드림시큐리티	77	30.4	이지서티	89	45.5
루시드네트웍스	148	30.2	시큐위즈	154	44.4
이스트시큐리티	2	25.7	유니디아	46	42.5
시큐위즈	97	25.1	스패로우	42	34.4
오픈베이스	1	23.8	코리아엑스퍼트	6	32.3
스패로우	26	23.8	코어시큐리티	14	32.0
합계		2,837.6	합계		3,649.4

자료: 과기정통부, 보안뉴스, 신한투자증권

사이버 보안기업 인수합병 현황

국내 사이버보안기업 인수합병 사례

2021 년 굵직한 인수합병이 발생한 것과 달리 2022 년 국내에서는 사이버보안 관련 인수합병이 적었다. 반면 글로벌 시장에서는 사이버보안 경쟁력 강화를 위한 다수의 인수합병 사례가 발생했다. 물론 기업 규모면에서 인수합병에 나설수 있는 국내 기업이 적은 것은 당연하지만, 최근 보안 과정 전체를 다루는 토탈 솔루션이 강세를 띄는 만큼, 기업 하나의 전문성과 역량만 강화해서는 글로벌 시장에서 뒤처질수 있다는 우려가 발생하고 있다.

2022 년 가장 아쉬웠던 보안 인수합병 뉴스는 IPO 도전에 실패한 SK 쉴더스의 상황이다. SK 쉴더스는 보안종합회사로서의 발돋움을 위해 상장을 시도했으나 결국 수요예측에 실패하고 상장을 철회했다. SK 쉴더스는 당시 IPO 로 수급되는 투자로 보안기업 인수합병을 추진하겠다고 밝혔다. SK 쉴더스의 상장이 예정대로 진행되었다면 안랩, 이글루시큐리티 등 추가 인수합병 의사를 밝혔던 기업들에게도 긍정적인 움직임을 기대할 수 있지 않았을까 하는 아쉬움이 남는다.

국내 사이버보안기업 인수합병 현황 (2021~2022)

인수합병 기업	날짜	내용
LG전자, 사이벨럼 인수	21년 9월	LG전자는 이스라엘 자동차 사이버보안 기업 사이벨럼의 지분 64% 확보(약 1,300억원) 전기차 사업에 진출하는 과정에서 인수를 통해 부족한 포트폴리오 보완, 사이벨럼은 자동차 보안 솔루션에 특화된 업체로 닛산, 르노자동차그룹 등 다양한 완성차 업체들을 고객사로 두고 있음
넥스원소프트, 이노코어 흡수합병	22년 12월	넥스원소프트는 빅데이터 및 핀테크 전문 기업 이노코어 흡수합병, 빅데이터 보안 사업 경쟁력 강화 넥스원소프트는 1)빅데이터 플랫폼, 2)개인정보 가명처리, 3)통합인증 서비스, 4) 신용카드 결제, 인증 솔루션 등의 사업 분야를 기반으로 데이터 플랫폼 서비스 고도화 목표
라온시큐어, 자회사 라온화이트햇의 라온에스엔씨 흡수 합병	22년 4일	IT 통합보안, 인증기업 라온시큐어는 전자서명 및 간편인증 중계 플랫폼, 통합 계정 관리 권한 플랫폼 중심 라온에스엔씨 흡수합병 결정 합병을 통해 라온화이트햇(존속회사)은 클라우드 기반의 계정 및 접근관리를 제공하는 IDaaS 인증, 블록체인 기반 모바일 신분증 등 사업 다각화 예정
앤씨앤, 완전자회사 베이다스 합병	22년 지분 매입 완료	차량용 전자기기 전문기업 애씨엔은 완전 자회사 베이다스 합병, 베이다스는 자율주차 소프트웨어 개발 전문 기업 앤씨앤이 보유하고 있는 시스템 제조 기술에 베이다스의 AI 인식 기술을 결합해 각종 자율주행, ADAS 시스템 개발에 시너지 효과 기대

자료: 신한투자증권

글로벌 사이버보안기업 인수합병 현황

글로벌 사이버보안기업 인수합병 현황 (2022)

일자	인수합병 대상 기업	내용
22.1.4	구글, 시엠플리파이 인수	구글, 오케스트레이션과 SOAR에 특화된 스타트업 시엠플리파이 5억달러에 인수
22.1.5	레코디드퓨처, 시큐리티트레일즈 인수	위협첩보 기업 레코디드퓨처, 인터넷 인벤토리 기업 시큐리티트레일즈 6,500만달러에 인수
22.1.13	디지서트, 모나카 인수	TLS/SSL, IoT 기업 디지서트, 사물인터넷 보안 전문 기업 모나카 인수
22.2.1	포스카웃, 사이버MDX 인수	장비보안 전문 업체 포스카웃, 헬스케어 분야 사이버보안 전문 업체 사이버MDX 인수
22.2.2	체크포인트, 스펙트럴 인수	이스라엘 IT 보안 대기업 체크포인트, 보안 스타트업 스펙트럴 6,000만달러에 인수
22.2.11	클라우드플레어, 벡트릭스 인수	클라우드 대기업 클라우드플레어, 웹 애플리케이션 보안 특화 스타트업 벡트릭스 인수
22.2.12	시큐리티스코어카드, 라이파즈 인수	사이버 보안 평가 기업 시큐리티스코어카드, 디지털 포렌식 특화 기업 라이파즈 인수
22.2.16	아카마이, 라이노드 인수	보안 컴퓨팅 전문업체 아카마이, 가상 클라우드 서버 렌탈 기업 라이노드 9억달러에 인수
22.2.23	다크트레이스, 사이버스프린트 인수	AI 보안 솔루션 개발사 다크트레이스, 공격로 관리 플랫폼 업체 사이버스프린트 인수
22.2.24	클라우드플레어, 에어리어원시큐리티 인수	클라우드플레어, 클라우드 네이티브 플랫폼 업체 에어리원시큐리티 1.6억달러에 인수
22.3.8	구글, 맨디언트 인수	구글, 클라우드 특화 유명 보안 업체 맨디언트 54억달러에 인수
22.3.15	센티넬원, 아티보네트웍스 인수	보안 자동화 특화 센티넬원, 아이덴티티 보호 기업 아티보네트웍스 6.1억달러에 인수
22.3.17	부즈앨런해밀턴, 에버왓치 인수	대형 IT 컨설팅 업체 부즈앨런해밀턴, 사이버위협 대응 플랫폼 제공 업체 에버왓치 인수
22.3.31	어베스트, 시큐어키테크놀로지스 인수	어베스트, 디지털 인증 및 아이덴티티 관리 강화를 위해 시큐어키테크놀로지스 인수
22.4.9	프로톤메일, 심플로그인 인수	이메일 암호화 서비스 제공 업체 프론토메일, 대체 이메일 솔루션 업체 심플로그인 인수
22.4.11	토마브라보, 세일포인트 인수	미국 사모펀드 토마브라보, 원격 근무 네트워크 보안 업체 세일포인트 69억달러에 인수
22.4.15	KPMG, 포티카 인수	글로벌 컨설팅 업체 KPMG, 캐나다 클라우드 보안 업체 포티카 인수
22.4.25	소포스, SOC.OS 인수	대형 보안 업체 소포스, 클라우드 기반 위협 탐지 및 보안 경보 서비스 업체 SOC.OS 인수
22.4.27	테너블, 비트디스커버리 인수	사이버 노출도 관리 업체 테너블, 공격 통로 관리 업체 비트디스커버리 4,450만달러에 인수
22.4.29	시놉시스, 화이트햇시큐리티 인수	자동화 등 IT 서비스 제공 업체 시놉시스, 화이트햇시큐리티 3.3억달러에 인수
22.6.6	IBM, 란도리 인수	빅테크 IBM, 공격 통로 통합 관리 등 오펜시브 보안 스타트업 란도리 인수
22.6.7	포스카웃, 사이시브 인수	보안 업체 포스카웃, 위협 탐지, 대응 및 엔드포인트 보안 특화 업체 사이시브 인수
22.6.8	에어버스, DSI 인수	우주항공 기업 에어버스, 통신 암호화 및 보안 전문 업체 DSI 인수
22.6.16	마이크로소프트, 미부로 인수	마이크로소프트, 사이버 위협 분석 전문 업체 미부로 인수
22.7.11	레코디드퓨처, 햇칭 인수	첩보 분석, 제공 전문 업체 레코디드퓨처, 네덜란드의 멀웨어 분석 전문 기업 해칭 인수
22.7.12	탈레스, 원웰컴 인수	국방 분야 대기업 탈레스, 디지털 아이덴티티 보안 업체 원웰컴 1억달러에 인수
22.8.4	토마브라보, 핑아이덴티티 인수	미국 사모펀드 토마브라보, 디지털 아이덴티티 관리 업체 핑아이덴티티 24억달러에 인수
22.9.21	크라우드스트라이크, 리포지파이 인수	엔드포인트 보호 업체 크라우드스트라이크, 공격통로 관리 업체 리포지파이 인수
22.9.22	후지쯔, 인피섹 인수	일본 대기업 후지쯔, 뉴질랜드 사이버보안 업체 인피섹 인수
22.10.12	토마브라보, 포지록 인수	미국 사모펀드, 2021년 상장한 디지털 아이덴티티 전문 기업 포지록 23억달러에 인수
22.10.29	옵스왓, 파일스캔 인수	사회기반 시설 보안 특화 업체 옵스왓, 차세대 멀웨어 분석 플랫폼 업체 파일스캔 인수
22.11.2	인텔471, 스파이더풋 인수	사이버 위협 첩보 전문 업체 인텔471, 오픈소스 공격 통로 관리 업체 스파이더풋 인수
22.11.3	원패스워드, 패시지 인수	비밀번호 관리 업체 원패스워드, ID 인증 전문 스타트업 패시지 인수
22.11.12	스플렁크, 트윈웨이브 인수	데이터 분석 전문 보안 업체 스플렁크, 공격 행위 자동 추적 솔루션 업체 트윈웨이브 인수
22.11.18	팔로알토네트웍스, 사이더시큐리티 인수	보안 업체 팔로알토네트웍스, S/W 공급망 전문 업체 사이더시큐리티 1억달러에 인수
22.11.30	드롭박스, 박스크립터 인수	클라우드 서비스 업체 드롭박스, 종단간 암호화 기능 추가를 위해 박스크립터 인수
22.12.12	프루프포인트, 일루시브 인수	보안 업체 프루프포인트, 아이덴티티 위협 탐지 및 대응 업체 일루시브 인수

자료: 시큐리티월드, 신한투자증권

지니언스

Bloomberg Code (263860 KS) | Reuters Code (263860.KQ)

성장의 원년

[혁신성장]

백지우 연구원
☎ 02-3772-2671
✉ jiwoo100@shinhan.com

매수	현재주가 (9 월 15 일)	목표주가	상승여력
(신규)	13,180 원	18,000 원 (신규)	36.6%

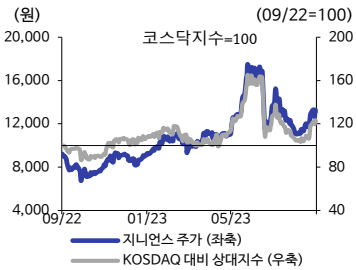
- 차세대 보안 솔루션 NAC, EDR 국내 시장점유율 1위 기업
- 안정적인 캐시카우 NAC 매출 + 신규 수요 확장 중인 EDR 매출
- 목표주가 18,000원, 투자의견 '매수'로 커버리지 개시

신한 리서치 투자정보
www.shinhansec.com

신한투자증권 기업분석부

시가총액	124.5 십억원
발행주식수	9.4 백만주
유동주식수	5.1 백만주(53.5%)
52주 최고가/최저가	17,490 원/6,750 원
일평균 거래량 (60일)	138,299 주
일평균 거래액 (60일)	1,826 백만원
외국인 지분율	20.16%
주요주주	
이동범 외 2인	37.74%
Miri Capital Management LLC	11.16%
절대수익률	
3개월	-23.4%
6개월	32.6%
12개월	41.4%
KOSPI 대비 상대수익률	
3개월	-25.2%
6개월	15.2%
12개월	22.9%

주가



NAC, EDR 국내 시장 점유율 1위 기업

정보보안 소프트웨어 기업이다. 18년 연속 흑자를 기록하며 안정적으로 성장 중이다. 주요 제품으로는 1) 기업 내부 네트워크 보안 플랫폼 NAC, 2) 선제적 위협탐지 및 감염경로 분석이 가능한 EDR 솔루션을 보유하고 있다. 2022년에는 공공, 민간 매출 비중은 각각 52%, 48% 수준으로 민간 시장 매출비중이 커지며 산업별 균등한 포트폴리오를 보유 중이다.

안정적인 NAC 매출이 끌어주고, 신규 수요 EDR이 밀어주고

지니언스는 국내 1위 NAC 솔루션 사업자다. NAC 시장이 성장하며 국가기관 및 기업의 NAC 투자도 함께 증가하고 있다. 올해도 IT 인력증가, 단말기 다양화, 재택근무 확대 등의 시장 상황에 더불어 NAC 매출의 지속 성장을 예상한다. NAC 솔루션은 2,400여개의 고객사를 확보했다. 신규 고객 뿐만 아니라 기존 고객의 NAC 설치 확대 수요가 늘어나고 있어 고객사 수 증가추이를 뛰어넘는 매출 성장을 기대한다. 최근 구독형 모델인 클라우드 NAC 제품을 선보이며 중소기업, 글로벌 기업까지 고객사 커버리지를 넓히고 있다.

현재 EDR 매출비중은 10% 내외로 추정되지만, 2017년 EDR 솔루션 출시 이후 판매가 본격화되며 두 사업부문의 동반 성장이 기대된다. 2022년 EDR 고객사는 139개사로 국내 최다 고객사 확보에 성공했다. 나라장터 기준 84%의 시장점유율을 차지하며 민간, 공공 모두 1위 사업자로 자리잡았다. 2019년 코로나로 인해 EDR 등 보안 솔루션을 포함한 IT 투자가 지연됐다. 현재 공공, 민간 모두 보안에 대한 투자를 확대하고 있어 EDR 고객사는 계속해서 증가할 전망이다

목표주가 18,000원, 투자의견 '매수'로 커버리지 개시

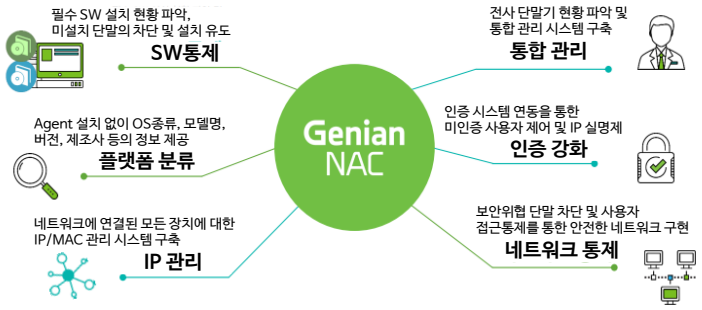
23F EPS 995원에 Target PER 18배로 목표주가 18,000원을 제시한다. 2019~2022년 EDR이 출시되고 매출 발생이 시작한 시점부터의 PER 평균에 10% 할증을 적용하였다. EDR의 금융권 도입이 본격화되고 클라우드 NAC의 고객사가 전년대비 2배 이상 증가하는 등 성장의 원년이 될 것으로 기대된다. 기존 고객사들의 NAC 확대 수요, EDR 신규 도입 수요 등으로 인해 2023년 상반기 역대 최대 반기 실적이 예상된다. 따라서 현재 주가는 저평가 구간으로 판단한다

12월 결산	매출액 (십억원)	영업이익 (십억원)	순이익 (십억원)	EPS (원)	BPS (원)	PER (배)	EV/EBITDA (배)	PBR (배)	ROE (%)	순차입금비율 (%)
2021	31.5	6.4	6.1	650	4,353	19.5	14.1	2.9	16.1	(47.5)
2022	37.8	7.5	7.2	758	5,072	10.8	5.4	1.6	16.1	(70.5)
2023F	46.8	9.7	9.4	995	5,929	13.4	7.9	2.2	18.1	(72.6)
2024F	58.2	15.5	14.2	1,506	7,299	8.8	4.5	1.8	22.8	(70.6)
2025F	70.2	19.8	17.5	1,850	9,012	7.2	3.0	1.5	22.7	(71.7)

자료: 회사 자료, 신한투자증권

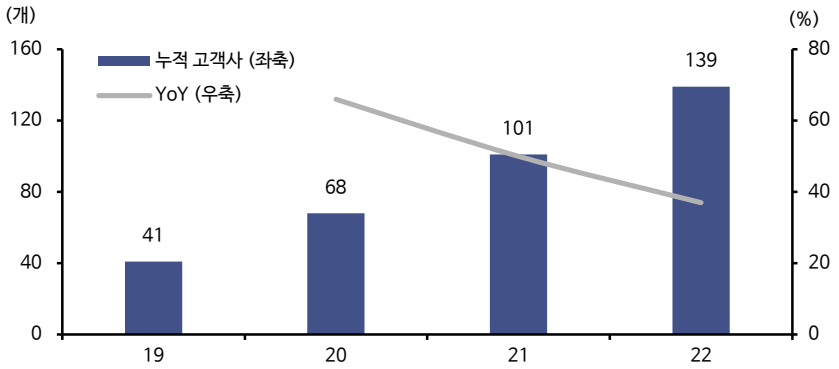
Key Charts

Genian NAC 도입 효과



자료: 회사 자료, 신한투자증권

연도별 지니언스 EDR 솔루션 누적 고객 수 추이



자료: 회사 자료, 신한투자증권

지니언스 글로벌 비지니스 현황

지역	산업	고객	지역	산업	고객
북미	Public	City of Kitchener	유럽	Healthcare	Health Point Hospital
북미	Finance	TLC Community Credit Union	아시아/태평양	Public	Ministry of Health
유럽	Finance	Tamweel Aloula	아시아/태평양	Public	House of Representative
유럽	Finance	AL Fujairah National Insurance	아시아/태평양	Public	Anti-Money Laundering
유럽	Finance	SR-ACCORD	아시아/태평양	Public	Pharmaceutical Organization
유럽	Manufacturing	Tecnotion	아시아/태평양	Finance	SME Bank Thailand
유럽	Manufacturing	Heartland Fabricators	아시아/태평양	Finance	Thai Samsung Life Insurance
유럽	Service	AZ Marketing	아시아/태평양	Manufacturing	GS Battery
유럽	Construction	Glenn O.Hawbaker, Inc.	아시아/태평양	Manufacturing	Tontai Machine & Tool

자료: 회사자료, 신한투자증권

I. 기업개요

차세대 보안 솔루션 대표 기업

왼손에는 NAC, 오른손에는 EDR

1) 네트워크 보안 NAC,
2) 엔드포인트 보안 EDR
솔루션 국내 1위 기업

정보보안 소프트웨어 기업이다. 2005년 설립되어 18년 연속 흑자를 기록하고 있는 안정성과 성장성을 갖춘 기업이다. 주요 제품으로는 1) 기업 내부 네트워크 보안 플랫폼 NAC(Network Access Control, 네트워크 접근 제어), 2) 선제적 위협탐지 및 감염경로 분석이 가능한 EDR(Endpoint Detection & Response, 엔드포인트 위협탐지 및 대응) 솔루션을 보유하고 있다. 2021년 기준 공공시장과 민간시장의 매출비중은 각각 60%, 40%였다. 2022년에는 각각 52%, 48% 수준으로 민간 시장 매출비중이 커지며 산업별 균등한 포트폴리오를 보유하게 됐다.

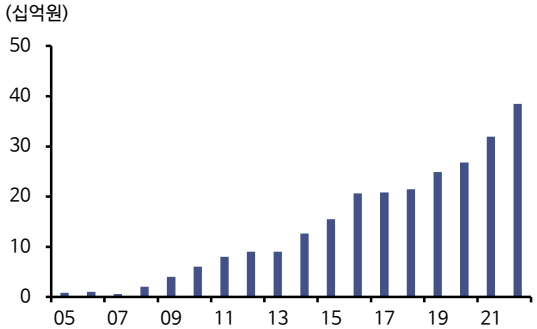
2022년 사업부문별 매출비중은 NAC, EDR을 포함한 네트워크 보안 81%, 유지보수 및 기타 19%를 기록했다. 주력 제품군인 NAC 솔루션의 경우 시장 내 2,400개 이상의 공급 레퍼런스를 보유하고 있으며, 업계 1위를 유지 중이다. 현재 EDR 매출비중은 10% 내외로 추정되지만, 2017년 EDR 솔루션 출시 이후 판매가 본격화되며 두 사업부문의 동반 성장이 기대된다. 2020년 이후 EDR 시장에서 최다 고객사 확보를 놓지지 않고 있어, EDR 시장의 고성장에 따른 매출 확대가 예상된다.

지니언스 주요 연혁

일시	내용
2006	네트워크 접근제어 솔루션 'Genian NAC v1.5' 출시
2013	Genian 내PC 지키미 v3.0 GS 인증 획득
2016	미국 RSA 2016 참가, 미국법인 설립
2017	코스닥 상장, EDR 솔루션 'Genian Insights E' 출시
2019	EDR 사업부문, 공공, 금융, 제조 대형 레퍼런스 확보
2022	국내최초 Genian EDR 국정원 보안기능 확인서 획득

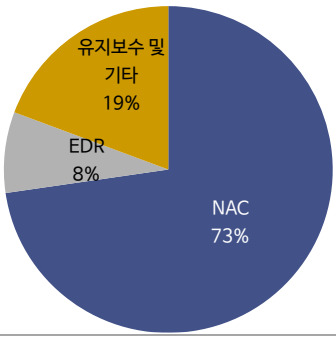
자료: 신한투자증권 추정

설립 이후 매출액 추이



자료: 회사 자료, 신한투자증권

2022년 매출 비중



자료: 회사 자료, 신한투자증권 추정

보안에 대한 전문지식을 보유한 대표이사 및 경영진, 현업에서 활발히 활동 중

지니언스의 핵심 경쟁력은 제품에만 있는 것은 아니다. 현재 최대주주이자 대표이사를 역임하고 있는 이동범 이사는 한국정보보호산업협회(KISIA) 회장직, 디지털 플랫폼 정부위원회 보안분과 위원, 중소기업 기술정보진흥원 비상임 이사, 국가정보원 사이버 정책 자문위원 등 현업에서 보안 관련 단체의 대표직을 겸하고 있다. 사이버보안은 정부 정책 및 지원에 영향을 많이 받는 산업으로 최신 정책 동향에 대한 이해가 필수적이다. 이동범 대표이사는 다수의 정보보안협회 회장 및 정책 자문위원으로 활동하며, 보안 정책에 대한 이해도가 높다. 이는 향후 어떤 보안 제품을 어떻게 시장에 판매해야 할지에 대한 중요한 기준이 되며, 지니언스가 EDR 시장을 선점할 수 있었던 이유이기도 하다.

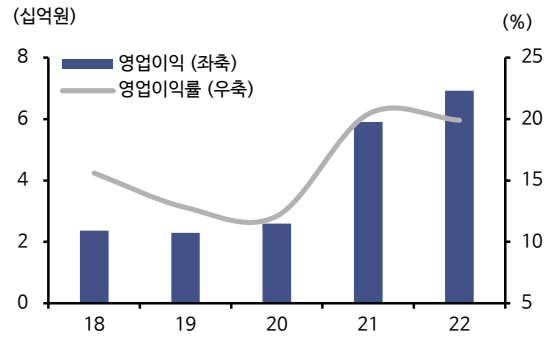
보안 산업의 성장과 보안 솔루션 필요성 증대에 확신을 갖고 있는 만큼 기존 솔루션 이외 신성장 동력을 확보하기 위해 노력중이다. 제2의 도약을 위해 기존 사업의 안정성에 더해 차세대 솔루션을 위한 투자를 지속하고 있다. 안정적인 캐시카우 역할을 했던 NAC 솔루션을 발전시킨 ZTNA(Zero Trust Network Access), EDR 솔루션을 진화시킨 XDR(Extended Detection and Response)을 출시하는 등 '어제의 기술이 오늘은 과거의 기술로'라는 슬로건 하에 끊임없는 발전을 추구한다. 새로운 시장 개척을 위한 적극적인 M&A도 계획하고 있으며, 1회성 판매가 아닌 구독형 사업모델을 구축하는 등 현대 보안 시스템에 적합한 새로운 시도를 지속하고 있다.

대표이사 소개

기간	내용
05~현재	지니언스 대표이사
20~현재	한국정보보호산업협회(KISIA) 회장
22~현재	디지털 플랫폼 정부위원회 보안분과 위원
20~현재	중소기업 기술정보진흥원 비상임 이사
20~현재	국가정보원 사이버 정책 자문위원
19~현재	과학기술정보통신부 5G 실무위원회 민간위원

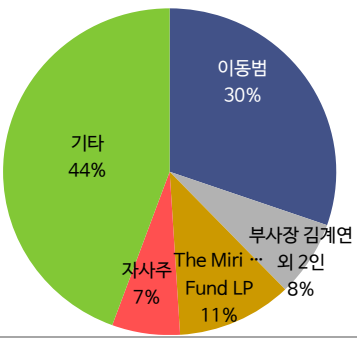
자료: 신한투자증권 추정

영업이익 및 영업이익률 추이



자료: 회사 자료, 신한투자증권

주주현황



자료: 회사 자료, 신한투자증권

II. 산업 분석

1. 고성장중인 NAC 시장

연평균 10% 이상 성장중인 NAC 시장, 기업 내부 네트워크 보호에 필수적

NAC(Network Access Control)는 네트워크 접근 제어 솔루션이다. 안전한 단말기, 사용자만이 네트워크에 접속할 수 있도록 제어하며 접속한 후에도 보안에 취약점이 있는지 지속적으로 트래킹한다. 특히 기업, 회사와 같이 다양한 기기가 사용되는 환경에서 내부 네트워크를 보호하는데 필수적인 솔루션이다. NAC는 내부 네트워크에 접근하려는 다수의 사용자와 기기를 검증해 인가된 사용자인지, 랜섬웨어에 감염되지 않았는지, 보안프로그램 활성화와 같은 보안정책이 잘 적용되고 있는지를 확인한 후 검증된 사용자만을 네트워크에 접근할 수 있도록 한다.

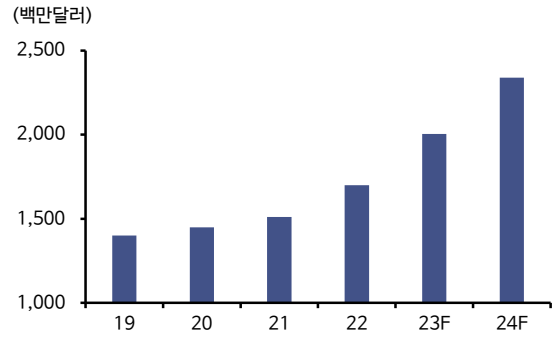
2022년 글로벌 NAC 시장규모는 약 17억 달러이다. 고성장 그룹 시장으로 분류되며 2019년 이후 5년간 연평균 10% 이상의 성장을 이어나갈 것으로 전망된다. 사물인터넷의 확산, IT와 OT(운영기술)의 융합, 클라우드 전환 등 여러 요인에 따라 네트워크에 연결된 단말 수가 기하급수적으로 증가하며 가파른 성장세를 보였다. 국내 NAC 시장 또한 1,000억원 규모를 돌파했다. 업계 관계자들은 국내 NAC 시장은 글로벌 평균 성장률인 10%보다 높은 20%대의 성장률을 보이고 있는 것으로 파악했으며, 특히 시장 초기에 있는 클라우드 NAC 시장은 30% 이상의 고성장을 기록할 것으로 전망했다.

국내 주요 NAC 사업자 솔루션 비교

회사명	솔루션명	주요기능		
		사용자 인증	네트워크 접근제어	모니터링 및 가시성
닉스테크	세이프NAC	PC 및 보마일 단말에 대한 통합인증 제공, 보안 무결성 점검	인가된 AP 통제, 임계치 이상 트래픽 발생시 노드 격리 처리 등	인증, 제한 사용자 현황, 단말에 대한 설치 S/W 현황 등
시스코	시스코 ISE	유/무선 및 VPN 인증, 권한부여 로깅	권한별 접근 통제 및 그룹간 통신 제어, 과다 트래픽 차단 등	Agent 접속 관리 및 미설치자 현황 파악, 과다 트래픽 모니터링 등
지니언스	지니언 NAC	에이전트 사용자 인증, SSO인증 정보 연동, 외부 사용자 동기화 등	비인가 단말 네트워크 사용 통제, 사용자 기반 AP위치 정보 제공 등	대용량 로그 감사기록 저장, 실시간 로그 데이터 검색 기능 등
넷맨	스마트 NAC	인사정보시스템 연동, 사용자 계정 신청/승인 프로세스 등	비인가 단말 네트워크 접근 통제, 그룹별 네트워크 접근제한 등	네트워크에 접속된 모든 단말 정보 실시간 자동 수집 관리 등

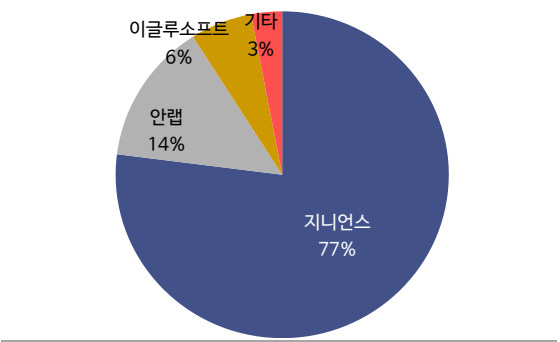
자료: 신한금융투자

글로벌 NAC 시장 규모 추이 및 전망



자료: 회사 자료, 신한투자증권

국내 NAC 조달시장 점유율



자료: 회사 자료, 신한투자증권

NAC 활용 사례

NAC는 전 페이지에서 서술했다시피 근본적으로 네트워크에 접근하는 IT 기기들을 제어하고 탐지하는 솔루션이다. 그러나 구체적으로, 그리고 실질적으로 기업에서 왜 NAC 솔루션이 필요한지, 어떤 상황에서 NAC가 도움이 되는지 구체적인 사례를 통해 알아보고자 한다.

1. 기기 무단 반입 탐지

NAC 솔루션을 도입하지 않은 네트워크는 기업 내에 존재하는 이더넷 포트에 어떤 기기를 연결하더라도 즉시 네트워크 사용이 가능하다. 사무실이 물리적으로 보호되고 있어도, 직원들이 허용되지 않은 개인 기기를 네트워크에 연결하게 되면 의도에 상관없이 웜이나 랜섬웨어 등으로 사내 시스템에 손상을 입힐 수 있게 된다.

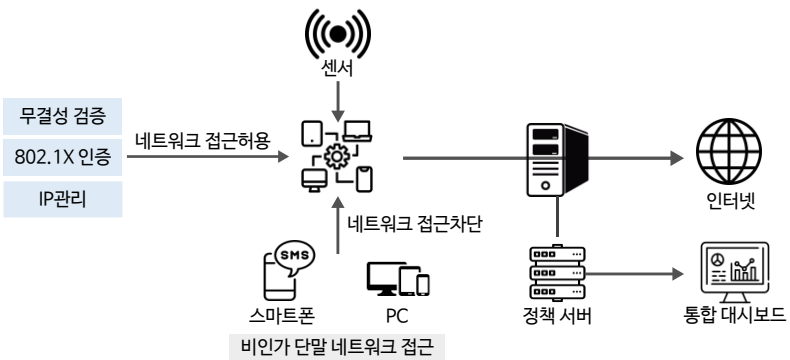
NAC는 이러한 문제를 해결하기 위해 사내 네트워크에 연결되는 모든 기기(스마트폰, IT전화기, 프린터기 등)에 대해 보안 요구사항을 충족하는 경우에만 네트워크를 사용할 수 있도록 해준다.

2. IT 자산관리

기업의 규모가 커질수록 보유하고 있는 IT 자산을 정확하게 파악하고, 그 상태를 파악하기란 관리자에게 어려운 문제이다. 특히 최근 IT 환경은 BYOD, IoT 등으로 과거에 비해 복잡성이 커졌다. 따라서 기업에 요구되는 많은 보안 규제에서 다양한 IT 자산에 대한 관리가 더욱 철저히 이루어질 것을 요구하고 있다.

IT 자산을 관리하기 위해서는 IT 자산에 대한 정보 수집이 선행되어야한다. MAC 주소와 같은 식별 값부터 단말의 제조사, 제품명, 이름, 위치(스위치 포트, 물리적 위치 등), 사용자명, 네트워크 연결, 단절 시각 등의 많은 정보가 정확히 필요하다. NAC는 네트워크에 연결되는 IT 자산에 대해 실시간으로 감시, 탐지하여 항상 원하는 데이터를 출력할 수 있도록 하여 관리자의 부담을 줄여준다.

NAC 접근제어 솔루션 구성도



자료: 회사 자료, 신한투자증권

3. 보안 사고 발생시 신속한 IP 추적 가능

예측 불가능한 보안사고가 발생했을 때 신속한 대처를 위해서는 침입자의 IP 추적이 필요하다. 대부분의 보안시스템은 감사기록을 통해 IP 주소를 남긴다. 그러나 보안사고가 발생했을 때 감사기록 확인을 통해 문제가 되는 IP를 확인하더라도 침입을 특정하기는 어렵다. 현재 그 IP가 과거에 사용되었던 시스템과 같은 시스템인지, 사용자는 누구인지, 어떤 시스템인지에 대해 감사기록을 통해서만 정보를 얻는 것은 어렵기 때문이다.

NAC는 지속적인 네트워크 감시를 통해 연결되는 모든 단말에 대한 기록을 남겨두고 있다. 따라서 수개월 전 특정 시점에 보안사고에 해당하는 IP를 사용했던 단말에 대해 빠르게 다양한 정보를 제공해줄 수 있다.

4. 무선랜 접속장치 보안 강화

스마트폰, 테블릿 PC 등 개인이 사용하는 모바일 기기들이 확산되고, 사내에서도 업무에 활용되면서 무선랜 사용이 급증했다. 고가의 관리형 무선 접속장치를 사용하는 경우 향상된 보안 시스템이 적용되어 무선랜 접속 시 각 개인의 비밀번호를 이용한 사용자 인증이 이뤄진다.

그러나 대부분의 회사에서는 무선랜 장치가 네트워크에 접속할 때, 공유 비밀번호를 사용하는 경우가 많다. 사내 공유 비밀번호는 원칙적으로 그 비밀번호를 아는 직원이 회사를 떠나는 경우 등 보안에 위협이 될 경우 변경해야한다. 하지만 전 직원이 쓰는 비밀번호를 매번 변경하는 일은 쉽지 않다.

이를 위해 무선랜 접속시 개인의 비밀번호를 인증할 수 있도록 해주는 시스템이 필요하다. 개인 비밀번호 인증 시스템을 802.1x라고 하며, 이는 무선랜에서 기기간 연결시 보안을 강화한 표준 인증방식이다. NAC는 기본적으로 802.1x를 지원하여 향상된 무선랜 보안을 구축할 수 있도록 해준다.

5. 허가되지 않은 외부 네트워크 접속 차단

네트워크 기술이 발전하며 사용자, 즉 기업의 직원들이 갖고 있는 IT 기기를 통해 다양한 외부 네트워크로의 접속이 가능하다. 원칙적으로는 사내에서 제공하는 네트워크만 접속이 가능해야하지만, 스마트폰을 이용한 Hotspot이나 Public WiFi가 대중화되며 손쉽게 외부 네트워크에 접속할 수 있다. 이는 기업의 보안 시스템을 우회하는 인터넷 연결을 만들어 내부 기밀 자료 유출과 같은 문제점이 발생할 수 있다.

NAC는 기업내부에서 접속 가능한 WiFi를 모니터링하고 어떤 사용자가 접속하는지를 관리 및 통제할 수 있다. 또한 사용자 단말에서 IT 관리자가 허락하지 않은 네트워크 대역에 접속하는 시도를 모니터링해서 내부 보안시스템 우회를 차단할 수 있다.

6. 필수 소프트웨어 설치 및 구동

관리자는 다양한 보안문제를 예방하고 해결하기 위해 사용자들의 시스템에 설치해야할 필수적인 소프트웨어나 운영체제 설정을 직원들에게 요구한다. 예를 들면 키보드 보안 프로그램, 사내 모니터링 프로그램 등의 필수 설치를 요구할 수 있다. 그러나 모든 사용자의 단말이 그 요구사항을 항상 준수하는 것은 아니기 때문에 보안사고는 끊임없이 발생한다.

NAC는 안티바이러스(백신)와 같이 단말에 필수적으로 필요한 소프트웨어나 화면보호기와 같은 필수적인 설정이 규정에 맞게 올바르게 구동되고 있는지 지속적으로 모니터링한다. 규정을 위반한 경우 차단, 치유, 격리 될 수 있는 시스템 또한 보유하고 있다.

7. 운영체제 최신 보안패치 적용

단말의 보안을 위해 가장 중요한 것은 보안 패치의 '최신'버전을 적용하는 것이다. 구형 보안 프로그램은 이미 결함이 발견되어 보안 위협을 효과적으로 방어할 수 없는 경우가 많기 때문이다. NAC는 단말의 보안패치 적용 상태를 지속적으로 모니터링하여 최신 패치가 적용되지 않은 단말을 네트워크에서 빠르게 격리한다. 이는 단순히 단말을 제어하는 것이 아니라 네트워크 수준에서 동작한다는 점이 기존의 단말을 직접 관리하는 소프트웨어와 가장 다르다. 관리자는 네트워크 제어를 통해 사용자가 우회할 수 없는 강력한 정책을 수행할 수 있다.

세대별 NAC 발전

구분	내용
1세대	- 과거부터 사용되던 네트워크 접속 사용자 인증 프로토콜인 802.1X를 기반으로 한 제품이 주를 이룸 -802.1X를 지원하지 못하는 장치들에 대한 인증문제 등 기존 네트워크를 일순간에 접근제어하기에 어려운 점이 많아 구축 실패 사례가 많았음
2세대	-802.1X에서 벗어나 네트워크 접속장치들과 SNMP를 통해 정보 수집, 각 네트워크마다 센서(Probe)라고 불리는 장치를 통해 독립적으로 정보 수집 - 유선랜 방식에서 무선랜으로 변화됨에 따라 네트워크 센서, 무선 컨트롤러 등의 기능이 추가되며 무선 보안에 대응할 수 있게 됨
3세대	- 수집과 제어를 넘어 다양한 자동화 기술 추가, 에이전트를 통해 단말의 보안 수준을 기업이 원하는 상태로 자동적으로 설정되도록 해줌 - 네트워크 내 다양한 시스템과의 연동을 통해 상호 협력적인 보안 모델 구축, REST, Webhook, Syslog와 같은 표준화된 프로토콜을 통해 제공
4세대	- 최근 BYOD, IoT 트렌드로 급격히 늘어난 접속 단말들을 정확히 식별하고, 다양한 비즈니스 상태를 손쉽게 관리할 수 있도록 설계 - 클라우드와 같이 변화하는 IT 환경에 맞게 클라우드 기반 관리형 서비스도 새롭게 선보이고 있음

자료: 신한투자증권

2. 떠오르는 샛별, EDR

위협으로부터 단말(엔드포인트)를 보호하는 EDR, 향후 25%이상의 고성장이 기대되는 시장

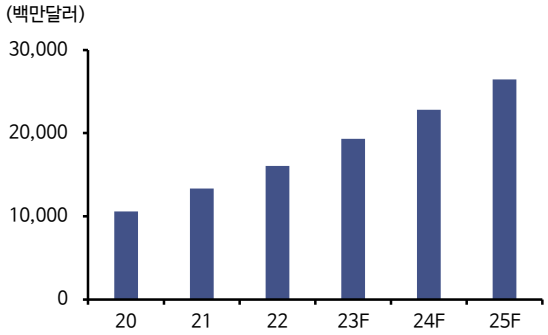
EDR(Endpoint Detection and Response)은 단말의 이상행위를 탐지하고 대응하는 솔루션이다. 즉 엔드포인트 레벨의 동작을 기록, 저장하며 의심스러운 시스템 동작을 탐지하여 상황에 맞는 정보를 제공한다. 또한 바이러스 등 악성활동을 차단하고, 영향을 받는 시스템을 복원하기 위한 대안을 제공하는 솔루션이다.

기존의 보안 솔루션과 가장 다른점은 '알려지지 않은 위협'을 탐지하여 대응할 수 있다는 점이다. 안티바이러스(백신)의 경우 특정 악성코드에 대해서만 작동하여 알려진 위험에만 대응할 수 있다. EDR 솔루션의 경우 그동안의 단말기를 분석했을때 발견되지 않았던 이상 행위를 감지하면 우선 위험 신호를 전달하여, 최근 변종 바이러스에 대한 대안으로 각광받고 있다.

2022년 글로벌 EDR 시장규모는 약 21억 6,000만달러 규모이다. 2022년부터 향후 6년간 연평균 25% 이상의 성장률을 기록할 것으로 전망된다. 최근 랜섬웨어, APT 공격 등 고도화된 공격이 심화되고 기업의 피해가 커지며 EDR 솔루션이 다시금 주목받기 시작했다. 특정 영역에 한정되어 종합적인 관점에서 사이버 공격에 대응이 불가한 기존 보안 솔루션의 한계를 체감하여 EDR 솔루션 수요가 증가하고 있다.

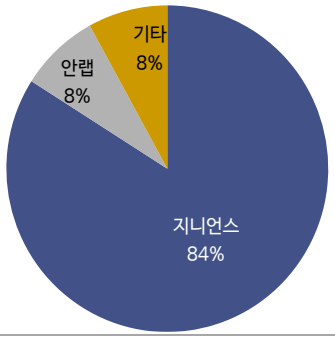
특히 EDR 전문 벤더들의 M&A가 활발히 이뤄지고, 글로벌 IT 기업들의 EDR 신제품 출시가 빨라지며 솔루션 자체에 대한 관심도 증가했다. 국내에서는 코로나19 시기에 기업들이 투자를 지연하며 EDR 도입이 다소 늦어졌지만, 최근 은행/금융권을 중심으로 도입 속도가 빨라지고 있다.

글로벌 EDR 시장 규모 추이 및 전망



자료: Marketsandmarkets, 신한투자증권

국내 EDR 조달시장 점유율



자료: 회사 자료, 신한투자증권

EDR 활용 사례

국내에서 보안 담당자가 지능형 위협 공격(APT)로 인해 발생한 침해 사고를 인지한 시점은 평균적으로 2개월에서 8개월 사이로 나타났다. 이 기간 동안 이미 내부 정보는 대부분 유출된 상태로 선제적 대응이 불가능했다. APT, 랜섬웨어 등 진화를 거듭하는 보안 위협은 기존에 도입해둔 전통적인 보안 솔루션만으로는 조기 탐지 및 대응이 매우 어렵다. 가트너에서는 변화하는 보안 위협 환경에 신속하게 적용할 수 있는 '적응형 보안 아키텍처'를 전략 기술 중 하나로 발표했다. EDR 솔루션은 적응형 보안 아키텍처의 '예측-예방-탐지-대응'의 영역 중 탐지와 대응 영역을 충족할 수 있는 최선의 솔루션이다.

1. 단말 행위 모니터링

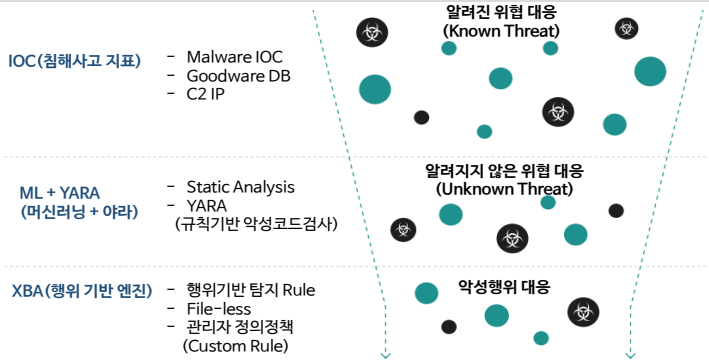
EDR 솔루션은 단말에서 발생하는 주요 행위를 모니터링하고 실시간으로 저장 후 분석한다. 이를 통해 지능형 위협 등을 사전에 탐지 및 예방하며 사후 감사 증적(Audit)이 가능하다. EDR 솔루션이 단말에서 분석하는 행위로는 1) 파일, 모듈, 프로세스, 네트워크, Registry 정보, 2) 외부 저장매체의 파일 정보, 3) 윈도우 이벤트 수집 등이 있다. 위와 같은 정보를 다양한 대시보드를 통해 제공한다.

2. 위협 탐지

IOC(침해 사고 지표), 머신러닝, YARA를 이용하여 단계별로 위협을 탐지하며 높은 수준의 정탐률(악성파일과 정상파일을 탐지하는 비율)을 제공한다. 또한 XBA(행위 기반 엔진)을 통해 File-less를 포함한 다양하고 새로운 형태의 악성행위를 탐지한다.

IOC란 네트워크에서 잠재저긍로 악의적인 활동을 식별하는 시스템 로그 항목 혹은 파일에서 발견된 데이터와 같은 포렌식 데이터 조각을 말한다. IOC는 데이터 유출, 악성코드 감염 등 위협 활동을 감지하는데 도움이 되는데, 주로 알려진 위협을 검출하는 역할을 한다. YARA는 악성코드의 시그니처를 이용하여 악성코드의 종류를 식별하고 분류하는 목적으로 사용되는 도구이다. YARA의 규칙기반 악성코드 검사와 머신러닝을 통해 알려지지 않은 위협까지도 대응하고 있다.

EDR 위협 탐지 과정



자료: 회사 자료, 신한투자증권

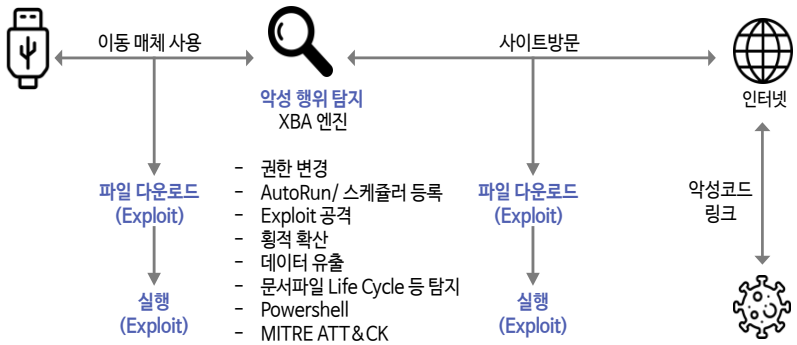
3. 위협 대응

단말에서 위협이 탐지되는 경우 위협의 심각성, 확산성, 그 위험의 정도 등을 고려하여 네트워크 격리, 파일 삭제, 프로세스 종료, 사용자 알림 등의 적절한 대응을 실행한다. 각 기업의 정책 기반으로 관리자의 개입 없이 즉시 작용하므로 확산 방지 등 선제적 대응이 가능하다.

4. 탐지 위협의 조사

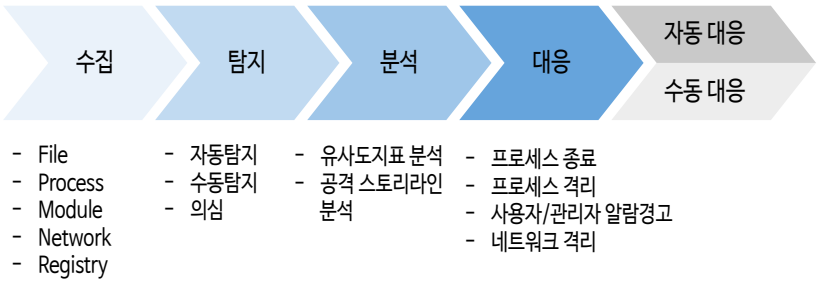
위협의 탐지와 동시에 조치의 대상이 누구인지 정확히 특정할 수 있다. 사용자, 부서, ID 등 대상의 정보를 정확하게 알 수 있으며 Reversing Labs, Virus Total 등의 외부 인텔리전스(CTI) 조회를 통해 탐지된 위협의 상세정보 확인이 가능하다. 기본적으로 탐지하는 정보에는 탐지시각, 위협 ID 등의 일반정도를 포함하여 사용자 정보, 단말정도, 파일정보가 있다. 정적 분석을 통해서는 버전, 카피라이트, 코드사인 등을 확인하며, 동적 분석을 통해서는 OS, 설치 프로그램, 프로세스 경로, 행위 내용 등을 파악한다. 연관 분석을 통해서 파일 및 프로세스 실행 여부, IP, Path, 파일 실행 위치, 옵션 값 등 더욱 많은 정보를 파악한다.

EDR 이상행위 탐지 과정



자료: 회사 자료, 신한투자증권

EDR 위협대응 프로세스



자료: 회사 자료, 신한투자증권

3. ZTNA, 빠르게 개화중

차세대 보안 개념 '제로 트러스트', 기존 보안 모델의 한계를 극복하여 끊임없이 의심하는 인증 체계 구현

"절대 믿지 말고(Zero Trust), 계속 검증하라(Always Verify)". 제로 트러스트 보안은 정보 시스템 등에 대한 접속 요구가 있을 때 네트워크가 이미 침해된 것으로 간주하고 검증하는 새로운 보안 개념이다. 모바일, IoT 기기, 클라우드 기반의 원격 근무환경이 조성되고 비대면 사회가 가속화됨에 따라 내부자에게 암묵적인 신뢰를 부여하는 기존 보안 모델은 한계에 도달했다. 보호 대상 IT 자원에 대한 접근 요구가 있을때, 접속을 암묵적으로 허락하는 것이 아닌 허락 여부를 결정하는 과정 자체가 제로트러스트의 가장 중요한 원리 중 하나이다.

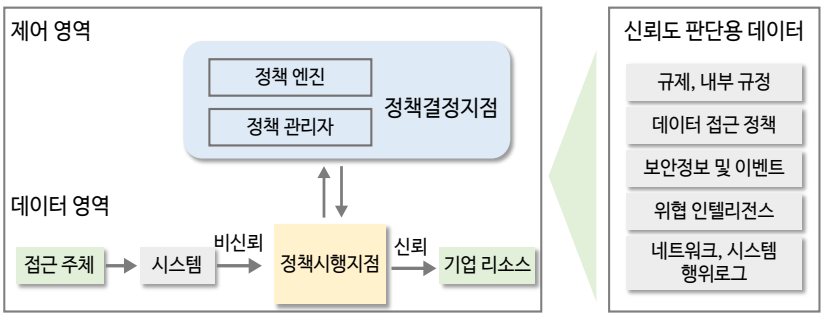
기존 경계 기반의 보안모델은 침입자가 내부자와 공모 혹은 권한 탈취를 통해 정보시스템에 접속하면 내부 서버에 추가 인증없이 접속할 수 있어 악의적 목적을 가진 데이터 유출이 가능하다. 반면 제로트러스트 보안 모델은 서버, 데이터 등 보호해야할 자원을 각각 분리하여 보호하며, 하나의 자원이 해킹되었다고 하더라도 인근 자원은 보호할 수 있다. 또한 사용자, 기기 등 모든 접속 요구에 대해 아이디, 패스워드 이외의 다양한 정보를 이용해 인증절차를 계속하여 거친다.

기존 경계보안과 제로트러스트 보안 비교

기존 보안 모델의 한계를 이용한 공격	제로트러스트 기반 대응
탈취된 임직원 계정을 활용한 VPN 로그인	로그인 시도 계정 및 기기의 위치, 상태 분석 의심스러운 경우 추가 인증 요청
회사 관리 자산이 아닌 기기 혹은 악성코드가 설치된 회사 자산으로 기업망 접근	회사 관리 자산이 아닌 경우 접근 거부 회사 관리 자산은 기기 무결성, 보안상태 점검
내부 침투 후 기업망 내부 정찰, 주요서버 접근	소프트웨어 정의 경계 기반 기업망 블랙박스화 계정, 기기가 주요 서버 접근시 권한 확인 후 차단
대량의 기밀 데이터 획득 및 외부 유출	계정, 기기에 대한 내부 행위 모니터링 기반 비정상 행위 분석 및 접속제한, 관리자 별도 승인

자료: KISA, 신한투자증권

제로트러스트 접근제어 구성도



자료: 회사 자료, 신한투자증권

제로트러스트 가이드라인 1.0 발표

과기정통부의 제로트러스트 가이드라인 발표, 도입 장려 기능 및 도입 초기 혼란 방지

과학기술정보통신부는 2022년 10월 국내 전문가로 구성된 '제로트러스트포럼'을 구성했다. 이를 통해 국내 환경에 적합한 '제로트러스트 가이드라인 1.0'을 마련하겠다고 밝힌지 10개월만인 2023년 7월 최종 가이드라인을 발표했다. 대통령 직속 디지털플랫폼정부위원회와 함께 지난 4월 '디지털플랫폼정부 실현계획'을 발표하며 제로트러스트 도입을 추진하겠다고 선언해, 이번 가이드라인 발표를 통해 제로트러스트 도입이 가속화 될 것으로 예상된다.

제로트러스트 도입은 초입에 있는 만큼 기업 관계자들은 네트워크, 컴퓨팅 자원 등의 요소를 어느 정도 보안 수준으로 설계해야하는지, 예산은 어느정도로 책정해야하는지 등의 지표를 필요로 한다. 이번 가이드라인 발표를 통해 6개의 핵심 보안요소에 대한 단계별 기능을 정의하여 실질적인 정보를 제공하였다. 또한 제로트러스트 보안 모델을 적용한 사례를 참조모델로 제시하며 네트워크 보안 효과성 또한 입증했다. 이번 가이드라인은 7월 10일부터 과기정통부, KISA 등의 홈페이지를 통해 이용할 수 있으며, 정부는 '제로트러스트 가이드라인 2.0'을 준비하는 등 지속적으로 제로트러스트 보안모델 확대 도입을 위해 힘쓰고 있다.

제로트러스트 가이드라인 1.0 中 제로트러스트 기본 절학

제로트러스트 기본철학

1. 모든 종류의 접근에 대해 신뢰하지 않을것 (명시적인 신뢰 확인 후 리소스 접근 허용)
2. 일관되고 중앙집중적인 정책 관리 및 접근제어 결정, 실행 필요
3. 사용자, 기기에 대한 관리 및 강력한 인증
4. 자원 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여)
5. 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
6. 모든 상태에 대한 모니터링, 로그 기록 등을 통한 신뢰성 지속 검증 및 제어

제로트러스트 구현 원칙

핵심 원칙	세부 내용
인증 체계 강화	각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근 위치 등)를 핵심요소로 설정하여 인증 정책 수립 *기업 내 사용자에 대한 여러 아이디를 허용하여 일관된 정책을 적용하지 않거나, 신뢰도 판단없이 단일 인증 방식만으로 접속을 허용할 경우 크리덴셜 스터핑에 취약
마이크로 세그멘테이션	보안 게이트웨이를 통해 보호되는 단독 네트워크 구역(세그먼트)에 대해 개별자원을 배치하고, 각종 접근 요청에 대한 지속 검증 수행 *개별 자원별 구역 설정이 없으면 기업망 내부에 침투한 공격자가 중요 리소스로 이동하기 쉬워 횡적이동 공격 성공 가능성이 높아짐
소프트웨어 정의 경계	소프트웨어 정의 경계 기법을 활용하여 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자 신뢰 확보 후 자원 접근을 위한 데이터 채널 형성 *클라우드, 온프레미스로 구성된 기업 네트워크에서 단말이 임의 데이터를 전송할 수 있다면, 네트워크 취약성에 따른 피해가능성이 커짐

자료: 과학기술정보통신부 배포자료, 신한투자증권

III. 투자 포인트

든든한 캐시카우, NAC

누적 2,400여개의 고객사를 확보한 지니언 NAC 솔루션, 조달 시장 기준 점유율 77%로 1위 기록

지니언스는 국내 1위 NAC 솔루션 사업자다. NAC 시장이 성장하며 국가기관 및 기업의 NAC 투자도 함께 증가하고 있다. 올해도 IT 인력증가, 단말기 다양화, 재택근무 확대 등의 시장 상황에 더불어 NAC 매출의 지속적인 성장이 기대된다. 지니언스의 NAC 솔루션인 'Genian NAC'는 18년간 축적된 기술을 통해 2,400여개의 고객사를 확보했다. 조달 시장 기준 점유율 1위(2022년 기준 77%)를 기록중이며, 가트너 기준 NAC 대표 기업에도 선정되었다. 탄탄한 기술력을 기반으로 고객 환경 변화에 맞게 다양한 서비스 포트폴리오를 완비하고 있다.

지니언스 NAC 솔루션만의 차별점

지니언스의 NAC 솔루션은 1) 가시성, 2) 정보 분류, 3) 통제 강화, 4) 데이터 리포트 제공 측면에서 강점을 갖고 있다. 첫째, 네트워크 내의 모든 단말기 정보를 수집 및 분류한 IP 실명 확인, PC 내 다양한 장비 및 시스템 정보를 대시보드를 통해 가시성있게 제공한다. 다양한 통계표 등을 활용하여 현황 파악이 용이하다. 둘째, 다양한 분류 조건을 제공한다. 등록일자, 노드타입, 백신정보, ON/OFF 등 기준에 따라 분류된 정보를 볼 수 있는 통계화면을 제공한다.

셋째, 다양한 제어 및 단계적 검증을 통해 통제/보안을 강화한다. **알림**(사용자에게 차단 웹 알림, 특정 이벤트 발생시 관리자에게 SMS알림 등), **차단**(조건에 따른 네트워크 차단, USB 장치차단 등), **교정**(필수 소프트웨어 설치 유도, 패스워드 설정 등) 과정을 거쳐 통제를 강화한다. 마지막으로 대시보드, 노트, 쿼리, 로그 리포트를 제공한다. 대시보드 리포트를 통해서는 전반적인 보안 현황을 제공하며, 쿼리를 통해 추출한 데이터를 엑셀 형태로 제공하는 쿼리 리포트 또한 제공한다. 그 밖에도 설정 데이터의 기간 별 평균, 최대값 등의 통계를 제공하는 노드 리포트, 로그별 발생 추이 통계를 제공하는 로그 리포트 등을 제공한다.

NAC 벤더별 차별 포인트

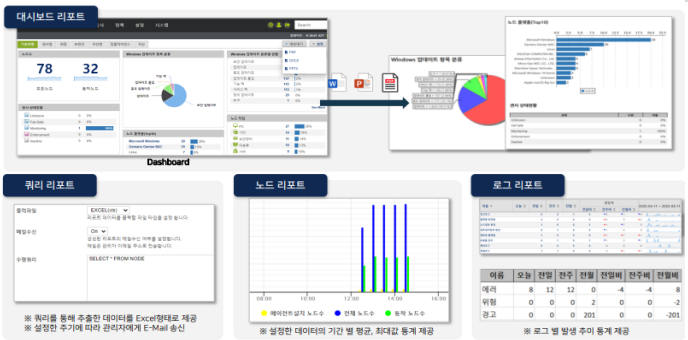
회사명	솔루션명	주요 특징
닉스테크	세이프 NAC	ACL(Access Control List) 정책, 보안정책 준수 여부 확인 관리 DHCP 서버 및 IP관리 분당 7만건 이상의 안정적인 인증 처리 속도 제공
넷맨	스마트NAC	유/무선 통합 네트워크 접근제어, 강화된 엔드포인트 관리 IPv4, IPv6 환경에서 NAC 기능 지원 및 호스트 탐지, 차단, 격리 등 관련 특허 보유
시스코	시스코ISE	접근제어 일원화 및 자동화, 기업 네트워크와 리소스에 대해 역할 기반 엑세스 실현 유/무선 VPN 접속방식 전체에 걸쳐 단순화된 접속 제공
지니언스	**지니안 NAC**	**유/무선 인프라 통합 구축, 모바일 단말 관리 지원 클라우드 기반 플랫폼 분석, 대용량 로그 분석**

자료: 보안뉴스, 신한투자증권

지니언스의 NAC는 특허 받은 DPI(Device Platform Intelligen)를 통해 단말 제조사의 취약점 및 정보를 확인한다. DPI는 단말의 제조사, 이름, 모델번호, 네트워크 연결방식 등 기본 정보 뿐만 아니라 제조사 홈페이지, 제품 판매 종료 여부 등 확장된 정보까지 제공한다. 이는 컴퓨터와 같은 IT기기 뿐만 아니라 사무용 전화기, CCTV 등 네트워크 접근을 필요로 하는 모든 자원에 대한 지원이 가능하다.

이 외에도 1) USB 장치 정보를 자동으로 수집하고, 다양한 조건 설정을 통해 USB 장치 사용자의 현황을 확인하여 외부 장치로 부터의 악성코드 유입을 효과적으로 방어한다. 2) 자산관리 서버와의 연동을 통해 장비 수명 주기를 자동으로 관리하여, 사용자/관리자에게 알림 기능을 제공한다. 이와 같이 Genian NAC는 기본적인 보안 솔루션은 물론, 보안 관리자에게 편리한 기능을 다수 포함하고 있어 기업의 도입 수요가 늘어나고 있다.

Genian NAC 리포트 기능 화면



자료: 회사 자료, 신한투자증권

Genian NAC 기능요약

Agent-less		Agent	
플랫폼 분류	OS(윈도우, 리눅스 등), 네트워크 장비, 프린터, 제조사 등	윈도우 패치	윈도우 패치 기능 제공
접근 제어	IP, MAC, PORT, Protocol 별 접근 제어	세션제어	TCP 세션 정보 수집 및 임계치 초과시 차단
	플랫폼 별 접근제어	포트정보	열린 포트, 포트 사용 프로세스, 서비스정보
	시간/요일/기간 접근제어	장치제어	USB, NIC, 블루투스, PC전원 제어
	사용자 별 접근제어	프로세스 제어	특정 프로세스 강제 종료
네트워크 정보	IP 관리(IP/MAC고정, 변경금지 등)	백신연동	백신 업데이트 및 바이러스 탐지
	사용자 PC가 연결된 스위치, 포트 정보	소프트웨어 탐지	필수 S/W, 불법 S/W 탐지 및 제어
	Host 명, 도메인명	메시지 전송	사용자에게 메시지 전송 (공지, 알림 팝업)
	PC 동작 유무 판단, PC 열린 포트 정보	보안 기능	비밀번호 유효성 검사, 윈도우 보안 설정, 파일배포, 공유폴더 제어, 화면보호기 제어, 윈도우 방화벽 제어 등
		위변조 탐지	IP, MAC Clone 탐지 및 차단
		APP탐지	무선 AP 탐지 및 접속 제어
		시스템 정보	PC OS 및 H/W정보, 호스트이름 수집
		Mac OS 업데이트	Mac OS 자동 업데이트 기능 제공
		장치제어	USB, NIC, 블루투스, 아이파이, 테더링
		보안기능	화면보호기 제어, 무선랜 제어 등

자료: 회사 자료, 신한투자증권

기존 고객, 신규 고객 모두 잡는 중

기존 고객의 확대 설치 수요 + 신규 고객 수요로 시장 성장률을 뛰어넘는 매출 성장 기록 중

지니언스 NAC의 제품 경쟁력은 숫자로도 증명됐다. 앞서 말했듯이 조달청 기준 77%의 압도적인 수치로 1등을 유지하고 있음은 물론 민간 기업에서도 그 수요가 꾸준하다. 특히 NAC의 매출 비중을 살펴보면 기존 고객의 확장 수요와 신규 고객 수요가 50:50 이라는 점이 고무적이다.

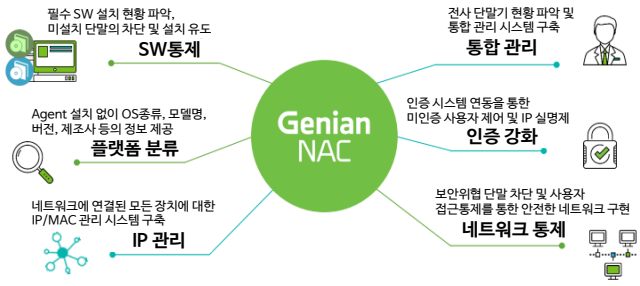
NAC 솔루션의 경우 보통 기업 내 모든 IT 자산에 대해 한번에 도입을 시행하지 않는다. 보안이 우선시 되는 부서에 먼저 도입을 한 후, 그 효과가 입증되면 다른 부서에도 NAC를 도입하는 식이다. 지니언스 NAC를 사용해본 고객사들은 제품력을 확인하고 기업 내 기타 IT 자산에 대해서도 NAC 도입을 확대하고 있다. 마켓컬리 등 테크 중심의 신규 수요에 더해 기존 고객사 또한 NAC 도입 범위를 확장하고 있어 NAC 매출 성장은 꾸준할 것으로 예상된다.

클라우드 기반의 NAC 서비스 출시로 사업영역을 넓혀가고 있다. 클라우드 NAC는 기존 NAC 솔루션과 달리 구독형으로 매출이 발생한다. 이는 분기 실적 변동성을 낮출 수 있으며, 장기적으로 이익률 개선에도 도움이 되는 모델이다. 현재 100개 이상의 고객사를 확보하였으며, 해외 고객사 확보에도 힘쓰고 있다. 구독형 모델은 고객사 또한 초기 비용을 줄일 수 있어 중소 기업 위주의 도입이 이뤄지고 있다. 기존 NAC의 경우 관공서, IT 대기업 등의 고객사가 주를 이뤘다면 클라우드 기반 구독형 NAC의 경우 중소기업과 해외 기업까지 고객사로 확보했다는 점에서 비즈니스 커버리지를 넓혔다는 의의가 있다.

Genian NAC 고객사 레퍼런스

자료: 회사 자료, 신한투자증권

Genian NAC 도입 효과



자료: 회사 자료, 신한투자증권

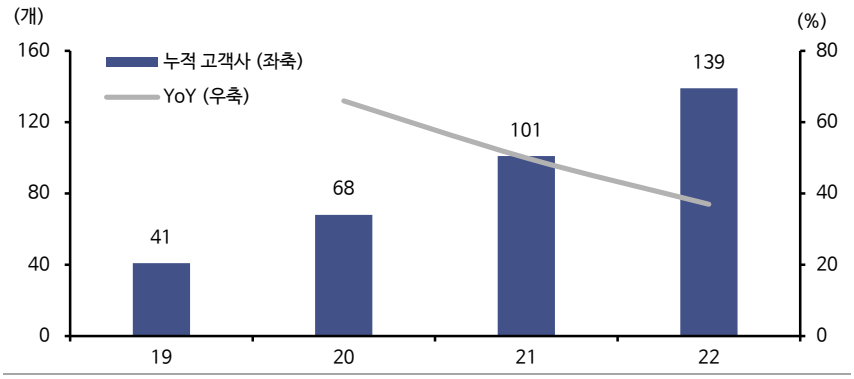
EDR 성장, 꾸준히 진행 중

국내 최초 EDR 개발 업체, 누적 고객사 140여개로 국내 1위 사업자

지니언스는 국내 최초로 EDR 솔루션 개발에 성공했다. 2022년 고객사는 139개사로 국내 최다 고객사 확보에 성공했다. 나라장터(공공조달) 기준 84%의 시장 점유율을 차지하며 민간, 공공 모두 1위 사업자로 자리잡았다. 2019년 코로나로 인해 EDR 등 보안 솔루션을 포함한 IT 투자가 지연되었다. 현재 공공, 민간 모두 보안에 대한 투자를 확대하고 있어 EDR 고객사는 계속해서 증가할 전망이다.

특히 외국 제품에 비해 유지관리 및 가격 경쟁력에 있어 장점을 보유하고 있다. 국내 시장에서 외산 EDR을 사용할 경우 1) 표준화로 인한 고객 맞춤형 솔루션 제공이 어렵고, 2) 코로나 등의 불가피한 상황이 발생했을 때 기술지원, 유지보수가 미흡하여 외산 솔루션 윈백 사례가 증가하고 있다. 이에 따라 카카오는 2020년 신속한 기술지원, 맞춤형 솔루션이 가능한 지니언스의 EDR 솔루션으로 전환했다. 이 밖에도 외국 솔루션을 사용하는 다양한 산업군의 대기업 고객사 확보에 성공하며, 올해도 30% 이상의 EDR 부문 성장이 가능할 전망이다.

연도별 지니언스 EDR 솔루션 누적 고객 수 추이



자료: 회사 자료, 신한투자증권

지니언스 EDR의 경쟁력

1 기술	2 고객, 경쟁사	3 가치 제안
국내 최초 AI기반 위협 분석 대응 기능 제공	139여개의 고객사(22년)를 확보해 국내 EDR 벤더 중 최다 고객 확보	국내 최초 보안 기능서 획득
단말과 단말에서 발생하는 각종 행위 정보를 상시적으로 수집하는 체계	재택근무, 문서 유출 등 다양한 범위에서 솔루션 활용	독자 기술력에 기반, 기술 지원 서비스 체계 완비로 고객 만족도 높음
국내 유일 안티 랜섬웨어 모듈 탑재	국내 및 글로벌 EDR 벤더들의 국내 진출로 시장 활성화 가능 전망	악성코드와 이상행위의 통합 관리

자료: 회사 자료, 신한투자증권

1) 엔드포인트에 대한 다양한 정보 제공, 2) 직관적인 대시보드로 EDR 신규 수요 증가

지니언스 EDR 솔루션만의 차별점

지니언스의 EDR 솔루션은 1) 침입 경로와 행위에 대한 정확한 파악, 2) 엔드포인트에 대한 다양한 정보 제공, 3) 네트워크, 엔트포인트의 연동 측면에서 강점을 갖고 있다. 첫째, 침입 경로나 침입 행위에 대해 빠르고 정확한 파악이 가능하다. 지니언스 EDR은 리버스 엔지니어링없이 프로그램의 동작을 확인할 수 있다. 리버스 엔지니어링이란 이미 만들어진 시스템을 역으로 추적하여 처음의 문서, 소프트웨어 등의 자료를 얻어내는 일이다. 즉 지니언스의 EDR은 역추적 없이 그 즉시 정확하게 침입에 대한 정보를 파악할 수 있다. 이에 더해 IOC(침해지표)를 사용하여 전 세계에서 탐지된 악성 파일, IP 정보를 DB화하여 알려진 위협에 대한 대응을 빠르게 진행할 수 있다. 알려지지 않은 침입, 위협에 대해서는 머신러닝, XBA 등의 기술을 사용하여 탐지한다.

둘째, 커스터마이징이 가능한 대시보드를 통해 엔드포인트의 다양한 정보를 가시성있게 제공한다. 위협 탐지를 위해 수집한 로그들은 원하는 형태의 대시보드로 사용자가 구성하여, PC내 발생 행위에 대해 쉽게 모니터링 할 수 있다. 예를 들어, 내부 정책 위반, USB 무단 사용을 통한 문서 이동, 내부 시스템 접속, AP 접속 현황 등 기존 보안 솔루션으로 확인하기 어려웠던 정보를 제공한다.

마지막으로 SOAR 등의 솔루션과 연동하여 네트워크 상의 이상 행위가 엔드포인트에서의 악성행위, 악성파일과 연관이 있는지 자동으로 분석하고 대응한다. SOAR(Security Orchestration, Automation and Response)란 인력 효율화를 위한 ML, AI 기술을 통한 자동 대응 관리 솔루션이다. 이를 통해 네트워크의 이상 트래픽이 감지 되었을 때, 엔드포인트에서의 악성코드가 감염되었는지 등의 Exploit 행위를 자동 탐지한다.

지니언스 EDR 솔루션 화면 – 전체 위협에 대한 요약 정보 제공

자료: 회사 자료, 신한투자증권

지니언스 EDR 도입 사례

금융권에서 시작해 지자체 등 공공기관까지 EDR 도입 시작

국내 최초로 EDR 솔루션을 개발 후 현재 민간, 공공 분야 점유율 1위를 차지하고 있다. 그러나 보안 솔루션의 특성상 특정 기업에서 어떤 보안 솔루션을 사용하는지 공개를 꺼리는 경우가 많다. 지니언스 EDR 솔루션은 다양한 산업 분야에서 사용되고 있지만, 그 중 공개된 대표적인 도입 사례만을 소개하고자 한다.

2019년 NH농협은행의 EDR 도입을 시작으로 2020년 이후 시중 은행 및 금융권의 활발한 EDR 투자가 예상됐지만, 코로나19, 마이데이터, 망분리 등 기타 금융권 이슈들로 인해 EDR 투자가 지연되었다. 2022년 KB 국민은행이 EDR 솔루션 투자를 결정했다. 22년 7월 지니언스는 KB 국민은행의 EDR 솔루션 사업자로 선정되어 8,000개의 노드를 대상으로 EDR 솔루션을 제공했다. 농협은행이 2,000개 노드를 시범사업으로 시작해 본사업으로 10만개 노드까지 단계적으로 공급한 점을 감안하면 KB 국민은행도 추가 확장 가능성이 충분하다.

금융권에서의 EDR 도입이 가장 활발하다. 2023년 2월 하나은행에 대해서 EDR 시스템 구축 사업자로 선정됐다. 세부내용은 공개되지 않았지만 사업규모는 5,000노드 정도로 추정된다. 2023년 EDR 등 보안 투자가 활발히 이뤄지며, 하반기 내 시중은행 공급이 추가적으로 발생할 것으로 기대된다. 현재 EDR이 도입된 금융권 업체는 신한금융지주, 부산은행, NH농협은행, KB국민은행, 하나은행 등이 있다.

금융권 뿐만 아니라 지자체 등 공공 기관 공급도 증가하고 있다. 2023년 7월 광주광역시에 EDR 솔루션 구축 사업을 수주했다고 밝혔다. 광주광역시는 고도화되는 사이버 위협을 예방하고 역량강화를 위한 투자로 EDR 솔루션을 도입했다고 말했다. 이 밖에도 2023년 1월, 부산광역시 또한 지니언스 EDR을 도입했다. 부산광역시는 '그린스마트시티'라는 비전을 완성하기 위해 디지털 혁신을 추진하며 보안 투자에도 적극적으로 나서고 있다.

지니언스 EDR 레퍼런스

자료: 회사 자료, 신한투자증권

신성장 모멘텀 확보, ZTNA와 클라우드

NAC의 한계를 극복한 ZTNA 출시, 재택근무 등 동적 업무환경 지원에 탁월

NAC를 보안한 '지니언 ZTNA' 출시

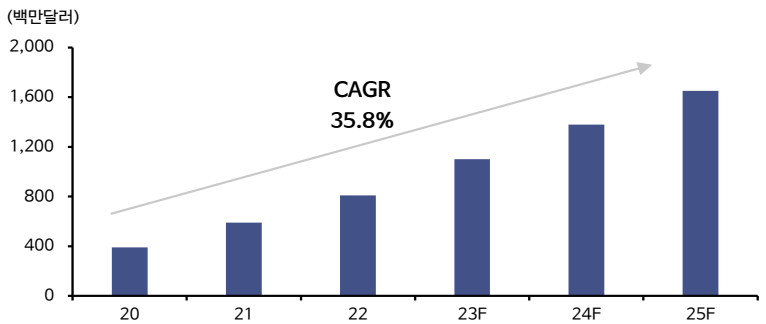
지니언스는 지난 2022년 NAC의 한계를 극복한 ZTNA를 출시했다. 현재 글로벌 시장을 중심으로 기술 확장 중에 있으며, 국내 시장에서는 POC를 진행중으로 고객사를 확보해나가는 단계다. NAC 시장 점유율 1위를 차지하며 빠르게 고객사를 늘려가고 있지만 이에 안주하지 않고 계속해서 신제품 개발을 진행하고 있다. 과거 신뢰를 기반으로 하는 보안 환경이 무너지며, NAC는 더 이상 완전한 보안 솔루션으로 취급받지 못한다. 아무도 믿지 않는 '제로트러스트' 환경에 적합한 'ZTNA(Zero Trust Network Access)'의 필요성이 증가하고 있다.

기존 NAC의 한계

기존 NAC는 방화벽 등 과거 세대의 보안 솔루션에 비해 강점을 갖고 있지만 빠르게 변화하는 보안 환경에서의 몇가지 한계가 분명하다. 첫째, **CLOUD 확장의 한계**가 존재한다. 내부 통제를 목적으로 한 NAC는 회사 내부 자산을 보호하는 데는 문제가 없지만 클라우드를 지원할 수는 없다. 특히 내부 자산이 외부로 이동하거나, 애플리케이션을 통제하는 문제는 클라우드 확장이 가능해야한다. 둘째, **VLAN 구성에 의존**한다. NAC 솔루션 통제를 위해서는 VLAN 구성을 사용한다. 그러나 VLAN의 확장에는 물리적 한계가 존재하여, 회사 밖으로 그 영역을 확장하기 어려우며 최신의 상태로 유지하는 것 또한 어렵다. 셋째, **접근통제에 있어 누락**이 발생할 수 있다. NAC의 접근통제 정책은 존재하거나 접근이 가능한 네트워크만을 대상으로 한다. 만약 IP를 보유하고 있지 않거나, IP가 수시로 변하는 대사이 있다면 그 대상에 대한 접근제어가 어렵다.

넷째, **원격지 사용자를 차단할 수 없다.** 원격지 사용자가 내부접근을 시도하거나 원격지간의 접근을 시도한다면 기존 NAC는 이를 대응할 수 없다. 별도의 클라이언트 에이전트나 사용자 인증이 필요하다. 마지막으로 **동적 업무환경을 지원하는데 있어 효과적이지 않다.** IP, Port, Protocol 등 전통적인 tuple 기반의 NAC 보안정책은 동적 업무환경을 지원하기에 충분하지 않다. 최근 각광받고 있는 WFA(Work From Anywhere) 환경을 조성하기 위해 ip를 기반으로 누수없는 접근제어 정책을 수립하기 어렵다.

글로벌 ZTNA 시장 규모 및 전망



자료: 회사 자료, 신한투자증권

지니어스 ZTNA의 차별점

위 서술한 NAC의 한계는 '제로트러스트' 원칙으로 해결 가능하다. 모든 자산에 대해 보안성을 검증하여 최소한의 접근권한을 부여하는 것이 그 원칙이다. 지니언스의 제로트러스트 원칙을 도입한 ZTNA는 NAC의 솔루션을 확장하고 보완한 솔루션이다. 기존 사내에서만 운영되던 NAC의 보안 정책, 자산을 원격지와 클라우드에도 적용시키고, 사용자의 역할, 위치, 목적 등에 따라 끊임없이 검증하는 솔루션이 ZTNA 솔루션이다. 즉 기존 NAC를 발전한 IT 및 보안 환경에 맞맞추 확장한 것이 지니언 ZTNA 솔루션이다.

1. 원격근무를 위한 Always On ZTNA

지니언 NAC를 통해 기존 VPN과 동일한 업무환경 구축이 가능하다. 뿐만 아니라 게이트웨이를 클라우드에 설치할 경우, 원격 사용자의 모든 트래픽을 클라우드로 통합하여 관리할 수 있다. 사내 직원들, 즉 사용자의 단말들은 까다로운 인증을 통해 검증되고 권한이 부여된다. 이 권한은 영구적으로 부여되는 것이 아니라 업무가 종료될 때까지 계속해서 검증된다. 상태, 위치 등이 변경되면 그 즉시 다른 검증이 진행되기 때문에 원격근무에 적합하다.

2. 클라우드 접근 통제 (Cloud Gateway)

지니언 ZTNA는 별도의 보안 게이트웨이를 설치해 클라우드 내부의 자산정보를 수집하여 보안정책을 수립할 수 있도록 한다. 클라우드 접근 통제의 핵심은 가시성의 확보다. 보안 게이트웨이를 통해 클라우드 내/외부 자산에 대해 가시성을 확보하여, 클라우드에 존재하는 자산에 대해 개별적인 네트워크 보안을 실시한다. 또한 게이트웨이를 통과하는 모든 트래픽을 조사하여 접근통제를 지원한다. 게이트웨이는 VPN 종단장치의 역할 또한 수행하며, 어플라이언스, 가상머신 등의 형태로 운영된다.

3. 세분화된 정책

원격근무, 재택근무, 개인 단말기를 사용한 업무 처리 등 다양한 업무환경에 따라서는 더욱 세밀한 보안정책이 필요하다. 그렇게 수립된 보안정책은 근무자의 이동, 근무자의 다른 디바이스 사용 등 네트워크 환경이 변해도 유지되어야 한다. 지니언 ZTNA는 애플리케이션 기반의 접근통제를 지원하기 때문에 사용자에 따라 마이크로세그멘테이션, 즉 사용자 별 세분화도니 정책 구현이 가능하다. 또한 동적 목적지 제어를 통해 사용자와 단말의 다양한 보안 상태에 따라 필요한 시점에 필요한 권한만을 부여할 수 있다.

4. FIDO (Fast Identity Online) 지원으로 강력한 인증 부여

지니언 ZTNA는 FIDO2 인증 표준을 지원한다. 이를 통해 지문, 홍채 등 생체인증 기능을 통해 강력한 다중인증체계 운영이 가능하다. FIDO2는 웹서비스 환경에서도 생체인증이 가능하다. 사용자는 에이전트 인증창에서 FIDO 기반 간편 로그인 방식을 통해 Always on ZTNA 정책을 적용 받을 수 있다.

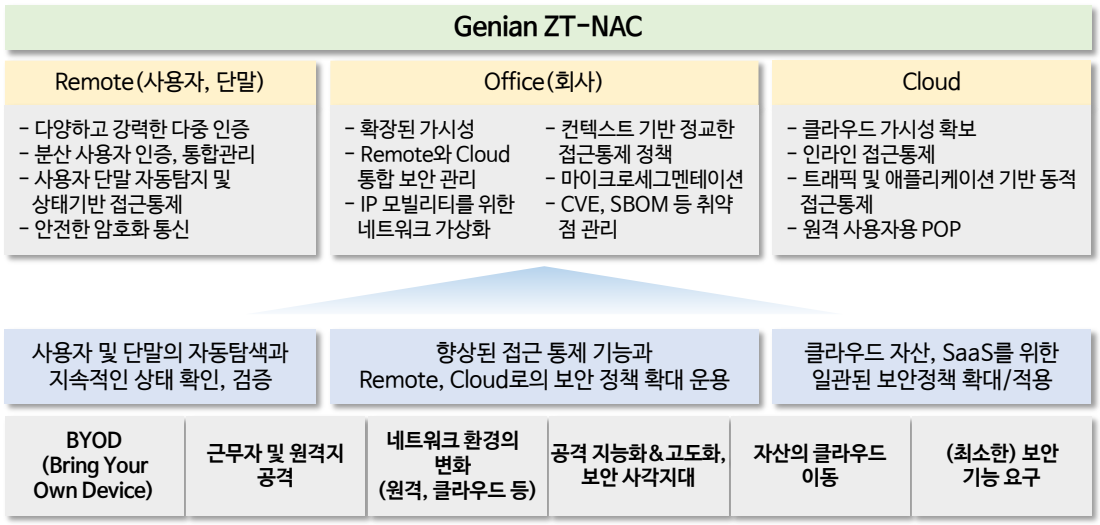
지니언스는 세계 최대 사이버보안 전시회 'RSA 콘퍼런스 2023'에 참여하여 ZTNA 솔루션을 선보였다. 지니언 ZTNA를 중심으로 글로벌 무대에서 대표 고객을 확보해 시장을 개척하겠다고 밝혔다. 2022년 미국은 사이버안보 행정명령을 통해 제로트러스트를 포함한 사이버 안보 강화 전략을 시행한 바 있어, 도입이 활발해질 것으로 전망된다. 지니언 ZTNA는 작년에 출시된 신제품으로 아직 매출이 가시화 되진 않았지만, 빠르게 성장하는 시장 속도에 맞추어 신성장 모멘텀으로서의 역할이 기대된다.

제로트러스트의 7가지 원칙과 지니언스의 대응

제로트러스트를 위한 7가지 원칙	Genian ZT-NAC의 대응
1. 모든 데이터 및 컴퓨팅 서비스는 리소스로 간주	1-1. 연결된 모든 객체는 자동으로 탐지 1-2. 탐지된 모든 정보는 보안정책으로 수립되어 접근통제 등에 활용 1-3. 탐지 및 정보 수집을 위한 DPI 등 요소기술 고도화
2. 모든 통신은 위치에 관계없이 보호	2-1. ZTNA Agent와 Gateway를 통한 양종단간 통신 암호화 지원 2-2. POP를 통한 네트워크 트래픽 통합 및 보안 기능 제공 (SASE)
3. 리소스에 대한 접근은 세션별로 부여	3-1. 네트워크 트래픽, 애플리케이션 및 동적 접근제어 지원 3-2. 최소 정보 기반 최소 접근권한 제공 (Least Privilege)
4. 리소스에 대한 접근은 다양한 상태에 따라 통제	4-1. 사용자 인증, 위치, 단말 보안 등 약 600가지 이상의 상태조합을 통한 접근 통제
5. 모든 자산에 대한 무결성 및 보안상태에 대한 측정	5-1. 연결된 모든 객체의 자동 탐지 및 상태정보의 실시간 감시/추적 5-2. 상태 정보 변경 시 다양한 제어 정책 적용 (차단, 재인증, 교정 등)
6. 인증과 권한은 접근 이전에 동적이고 엄격하게 수행	6-1. 사용자 및 단말 인증에 따른 리소스 사용 권한 결정 6-2. 선인증 후연결 지원 및 연결 이후라도 상태 변경 시 즉시 대응
7. 가능한 많은 정보를 수집하고 보안 개선을 위해 활용	7-1. 기존 객체 탐지 외 SBOM, MUD 등 추가정보 제공 및 정책 적용 7-2. 취약점(CVE) 외 컨텍스트 기반 접근통제 구현

자료: 회사 자료, 신한투자증권

지니언스 ZTNA의 핵심기능



자료: 회사 자료, 신한투자증권

클라우드 NAC로 고객군 확장

구독형 클라우드 NAC 출시로 중소기업까지 고객사로 확보, 전년대비 고객사 2배 이상 증가 기대

지니언 클라우드 NAC는 클라우드 기반의 보안 제품으로 국내 최초 '클라우드 보안 표준 인증(CSAP)'을 취득한 네트워크 접근제어 서비스다. 이에 고객은 클라우드 기반의 접근 제어 서비스를 통해 보다 간편하고 효율적으로 보안을 강화할 수 있다. 또한 클라우드 보안 표준 인증을 획득하였기 때문에 일반 기업 뿐만 아니라 공공기관 까지 클라우드 NAC 공급이 가능하다.

지니언스의 클라우드 NAC 서비스는 1회성 구매 방식이 아닌 서비스 구독 방식으로 이루어져있다. 보다 간편하고 효율적인 도입이 가능하며 초기 도입 비용에 대한 부담이 적어 중소기업 위주의 도입이 이뤄지고 있다. 또한 유지보수가 매우 간편하다. 클라우드 기반의 서비스로 물리적인 위치 제약 없이 어디서든 기술지원이 가능하다. On-Premise 환경 대비 적은 인력으로 효율적, 경제적인 지원이 가능하다. 마지막으로 구독형 방식의 특성상 서비스 자산의 소유권이 제조사에 있기 때문에, 지니언스가 직접 중앙에서 관리할 수 있다. Policy Server와 Network Sensor 등의 자동 업그레이드 뿐만 아니라 취약점에 따른 즉각적인 대응도 중앙에서 일괄적으로 가능하다.

물리적인 위치에 제약없는 유지 보수가 가능하고, 1회성 도입비용이 없어 글로벌 지니스 확장도 빠르게 이뤄지고 있다. 현재 34개국에 38개의 파트너사를 확보하여 클라우드 NAC를 포함한 다양한 제품을 공급하고 있다. 미국을 포함하여 중동, 아시아태평양 지역에서 매출이 발생하고 있다. 기존 구축형 NAC 모델은 시스코 등 글로벌 대기업의 점유율이 높아 경쟁이 어려운 상황에 있다. 하지만 구독형 비즈니스 모델은 글로벌 대기업이 커버하지 못하는 중소기업을 대상으로 하여 지니언스의 경쟁력을 확보할 수 있다. 클라우드 NAC 고객사는 전년대비 2배 이상의 증가가 예상된다.

지니언스 글로벌 비지니스 현황

지역	산업	고객	지역	산업	고객
북미	Public	City of Kitchener	유럽	Healthcare	Health Point Hospital
북미	Finance	TLC Community Credit Union	아시아/태평양	Public	Ministry of Health
유럽	Finance	Tamweel Aloula	아시아/태평양	Public	House of Representative
유럽	Finance	AL Fujairah National Insurance	아시아/태평양	Public	Anti-Money Laundering
유럽	Finance	SR-ACCORD	아시아/태평양	Public	Pharmaceutical Organization
유럽	Manufacturing	Tecnotion	아시아/태평양	Finance	SME Bank Thailand
유럽	Manufacturing	Heartland Fabricators	아시아/태평양	Finance	Thai Samsung Life Insurance
유럽	Service	AZ Marketing	아시아/태평양	Manufacturing	GS Battery
유럽	Construction	Glenn O.Hawbaker, Inc.	아시아/태평양	Manufacturing	Tontai Machine & Tool

자료: 회사자료, 신한투자증권

III. 실적 추정 및 밸류에이션

23년 상반기, 역대급 호실적 기록

2023년 매출액 468억원(+24% YoY), 영업이익 97억원(+29% YoY)을 전망한다. 2019년 이후 이연된 EDR 및 NAC 솔루션 투자가 본격적으로 발생하며 하반기 대규모 수주가 예상된다. 또한 기존 고객들의 보안 솔루션 확대 적용으로 인한 추가 투자가 지속적으로 발생하고 있어, 신규 수주 외의 매출 발생도 기대된다. 2020년 이후 ZTNA, EDR 솔루션 개발에 따른 비용 발생으로 다소 낮은 영업이익률을 기록했다. 그러나 2022년 하반기 이후 신규 투자가 마무리 되며 영업이익의 정상화가 예상된다.

2023년 NAC, EDR 매출액은 각각 시장 성장률인 10%, 19%의 성장을 가정했다. 2022년 EDR 누적 고객사 수는 전년대비 37% 증가하며 시장성장률을 훨씬 웃도는 성장을 기록했다. NAC 또한 누적 고객사수가 빠르게 증가하고 있으며, 기존 고객사의 확대 설치 수요가 많아지며 시장 성장률을 웃도는 매출 성장 기록도 가능할 것으로 보인다. 올해부터 클라우드 NAC 고객사가 전년대비 2배이상 증가하며 영업이익률의 개선도 함께 일어날 전망이다.

2024, 2025년에도 약 20%에 육박하는 매출액 성장을 기록할 전망이다. 이는 NAC, EDR 시장 규모의 높은 성장률에 기인한 추정치로 지니언스의 시장 점유율을 감안했을 때 무리가 없다는 판단이다. 아직 매출액이 가시화 되지 않았지만 높은 성장 가능성을 보유하고 있는 ZTNA, 클라우드 NAC의 매출은 반영하지 않은 보수적인 수치이다. 만약 클라우드 NAC의 글로벌 시장 및 중소기업 향 매출이 본격화되고, 2022년 출시된 ZTNA의 수주가 발생한다면 큰 폭의 매출액 성장이 발생할 것으로 기대된다.

연도별 실적 추이

(십억원)	2020	2021	2022	2023F	2024F	2025F
매출액	**26.5**	**31.5**	**37.8**	**46.8**	**58.2**	**70.2**
NAC	20.7	23.8	27.3	33.8	42.4	50.8
EDR	1.0	1.8	3.1	4.2	5.5	7.0
기타	4.8	5.9	7.4	8.8	10.3	12.4
영업이익	3.2	6.4	7.5	9.7	15.5	19.8
영업이익률	12.1	20.4	19.9	20.7	26.7	28.2
지배주주순이익	3.4	6.1	7.2	9.4	14.2	17.5

자료: 신한투자증권 추정

목표주가 18,000원, Target PER 18배 제시

23F EPS 995원에 Target PER 18배로 목표주가 18,000원을 제시한다. 멀티플은 2019년 이후 EDR 솔루션이 도입되며 매출이 다각화 된 시점부터의 평균 PER을 적용하였으며, NAC의 향후 5년 성장률 CAGR 10%를 프리미엄으로 적용하였다. 1) 4년간 EDR, NAC 솔루션 고객사 수가 꾸준히 증가했다는 점, 2) 2019년 이후 코로나로 인해 IT 투자가 지연됐지만 꾸준한 매출액과 영업이익을 유지해 온 점, 3) ZTNA, 클라우드 NAC 등 추가 모멘텀이 남아있다는 점을 감안할 때 적절한 멀티플로 판단된다.

현재 NAC, EDR 사업을 영위하고 있는 글로벌 피어(시스코, HPE, 포티넷 등) 평균 PER은 34.3배이다. 지니언스와 유사한 국내 보안 솔루션 업체(안랩, 이글루, 케이사인 등) 평균 PER는 18배이며, 보안업종 전체 PER은 50배이다. 이를 감안할 때 PER 18배 적용은 무리가 없다는 판단이다.

PER/ROE 추이

(배, %)	17	18	19	20	21	22	4년 평균
PER(High)	17.1	19.9	21.5	22.8	34.0	17.9	24.1
PER(Low)	10.7	10.6	15.0	7.3	15.6	9.4	11.8
PER(Avg)	13.1	15.1	17.9	14.8	20.2	12.8	16.4
ROE(%)	16.1	10.7	9.2	9.7	16.1	16.1	12.8

자료: FnGuide, 신한투자증권

목표주가 산정

항목	가치	비고
23F EPS(원)	995	
Target PER (x)	18.0	19-22년 평균 PER에 10% 프리미엄 적용
목표주가 (원)	18,000	

자료: 신한투자증권

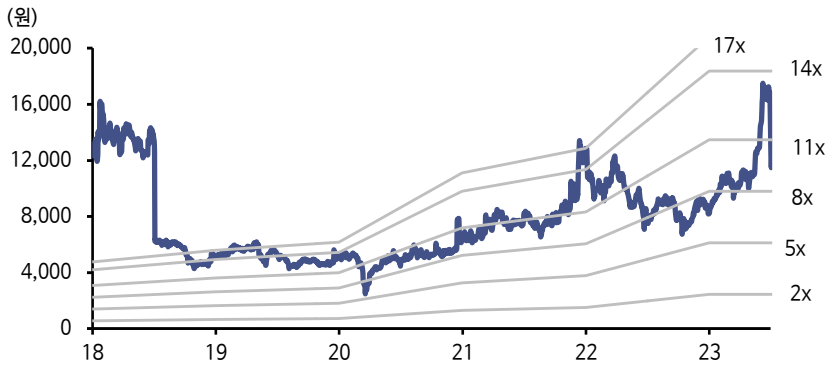
이제는 적절한 밸류를 부여받을 시점

글로벌 EDR 벤더의 기업가치에 주목할 필요가 있다. 글로벌 EDR 솔루션 기업에는 대표적으로 노턴라이프룩과 크라우드스트라이크가 있다. 시만텍은 1982년 설립된 전통 보안 업체로 시가총액은 약 123억달러이다. 크라우드스트라이크는 2011년 설립한 신흥 보안 솔루션 업체로 클라우드 서비스 등 신종 바이러스에 대응할 수 있는 신제품을 출시하고 있다. 크라우드스트라이크의 시가총액은 299억달러이다.

이와 같이 전통 보안 솔루션 기업 보다 현재 보안 환경에 알맞은 서비스를 선보이는 신흥 보안 기업에 대한 밸류를 더 부여하는 모습을 볼 수 있다. 지니언스 또한 끊임없는 신제품 출시와 새로운 보안 환경에 적합한 솔루션을 개발하고 있어 향후 더 높은 멀티플을 부여받을 수 있을 것으로 기대한다.

특히 국내 기업은 글로벌 PEER 보안 기업에 비해 적절한 가치를 인정받기 어렵다. 최근 보안 트렌드의 경우 사이버 위협의 복잡성과 다양성으로 인해 단순히 보안 소프트웨어, 하드웨어를 판매하는 것이 아닌 토탈 솔루션을 제시할 수 있는 회사를 원한다. 토탈 솔루션이란 어떤 공격이 발생할 수 있을 지 미리 탐지하고, 그에 대한 사후 대책까지 제공하는 솔루션을 말한다. 국내 시장에서 보안 기업이란 단순히 백신을 판매하는 소프트웨어 회사로 인지하는 경우가 많다. 지니언스는 NAC, EDR는 토탈 솔루션을 제공할 수 있는 회사로 최근 보안 기업들의 밸류 상승에 맞춰 적절한 밸류에이션을 부여받을 시점이라고 판단한다.

12MF PER Band Chart



자료: 신한투자증권

글로벌 EDR 벤더 시가총액 현황

기업	NortonLifeLock	CROWDSTRIKE
창립연도	1982년	2011년
상장연도	1989년	2019년
주가	19.2$	170.7$
시가총액	122.9억달러	407.7억달러

자료: 신한투자증권

국내 및 글로벌 Peer 분석

(십억원, %, 배)		지니언스	안랩	라온시큐어	Cisco	Crowdstrike	포티넷	HPE
시가총액		125.2	639.9	101.3	303,331.5	54,102.4	65,762.6	29,299.2
Sales	2022	38.5	228.0	46.8	75,316.3	2,904.8	5,708.8	36,139.3
	2023F	46.8	-	-	74,772.6	2,894.4	7,181.5	38,660.4
	2024F	58.2	-	-	76,727.8	4,028.0	8,457.4	39,369.0
OP	2022	6.9	27.0	4.3	19,861.7	(246.4)	1,253.1	991.8
	2023F	9.7	-	-	24,863.5	457.8	1,867.0	4,263.6
	2024F	15.5	-	-	26,093.1	801.5	2,213.7	4,383.1
OP margin	2022	18.0	11.8	9.2	26.4	(8.5)	21.9	2.7
	2023F	20.7	-	-	33.3	15.8	26.0	11.0
	2024F	26.7	-	-	34.0	19.9	26.2	11.1
NP	2022	7.1	14.2	6.7	16,666.6	(237.5)	1,107.9	1,100.8
	2023F	9.4	-	-	20,557.6	466.5	1,603.1	3,736.6
	2024F	14.2	-	-	21,675.7	909.7	1,879.5	3,705.9
NP margin	2022	18.6	6.2	14.2	22.1	(8.2)	19.4	3.0
	2023F	20.1	-	-	27.5	16.1	22.3	9.7
	2024F	24.5	-	-	28.3	22.6	22.2	9.4
P/E	2022	10.8	40.9	12.2	16.0	-	45.4	8.5
	2023F	14.1	-	-	14.8	114.0	41.8	8.0
	2024F	9.3	-	-	13.9	60.3	36.1	8.0
P/B	2022	1.6	2.3	2.1	4.8	17.1	-	0.9
	2023F	2.4	-	-	5.3	28.4	74.8	1.1
	2024F	1.9	-	-	4.7	18.1	32.1	1.0
ROE	2022	16.1	5.6	19.3	30.0	(14.7)	342.9	4.4
	2023F	18.1	-	-	35.1	29.2	338.8	13.8
	2024F	22.8	-	-	33.4	27.1	160.6	11.6
EV/EBITDA	2022	5.4	11.0	9.0	11.4	-	33.4	8.1
	2023F	8.6	-	-	10.3	89.2	31.1	5.8
	2024F	4.9	-	-	10.0	52.9	26.3	5.7

자료: Bloomberg, 신한투자증권추정
주: 지니언스는 자사 추정치 사용, 기타회사는 블룸버그 추정치 사용

재무상태표

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
자산총계	52.5	59.4	69.5	84.7	103.7
유동자산	33.1	47.0	56.1	67.1	82.1
현금및현금성자산	3.9	4.9	7.5	11.5	22.0
매출채권	10.4	8.0	9.5	11.6	13.3
재고자산	2.4	4.0	4.3	4.9	5.5
비유동자산	19.3	12.4	13.4	17.6	21.7
유형자산	5.3	5.3	7.0	9.0	11.2
무형자산	3.3	3.1	4.4	6.4	8.1
투자자산	9.8	3.6	1.5	1.7	2.0
기타금융업자산	0.0	0.0	0.0	0.0	0.0
부채총계	11.4	11.5	13.8	16.1	19.0
유동부채	10.4	10.5	12.7	14.7	17.3
단기차입금	0.0	0.0	0.0	0.0	0.0
매입채무	4.2	4.1	4.8	5.6	6.7
유동성장기부채	0.0	0.0	0.0	0.0	0.0
비유동부채	0.9	1.0	1.1	1.4	1.7
사채	0.0	0.0	0.0	0.0	0.0
장기차입금(장기금융부채 포함)	0.1	0.1	0.1	0.1	0.1
기타금융업부채	0.0	0.0	0.0	0.0	0.0
자본총계	41.1	47.9	56.0	68.9	85.1
자본금	4.7	4.7	4.7	4.7	4.7
자본잉여금	13.3	13.3	13.3	13.3	13.3
기타자본	(6.9)	(6.7)	(6.7)	(6.7)	(6.7)
기타포괄이익누계액	0.1	0.0	0.0	0.0	0.0
이익잉여금	29.9	36.5	44.6	57.6	73.7
지배주주지분	41.1	47.9	56.0	68.9	85.1
비지배주주지분	0.0	0.0	0.0	0.0	0.0
*총차입금	0.2	0.2	0.3	0.3	0.3
*순차입금(순현금)	(19.5)	(33.8)	(40.7)	(48.7)	(61.0)

포괄손익계산서

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
매출액	31.5	37.8	46.8	58.2	70.2
증가율 (%)	18.9	20.2	23.8	24.4	20.6
매출원가	12.4	15.8	19.1	21.2	24.9
매출총이익	19.1	22.0	27.7	37.0	45.3
매출총이익률 (%)	60.7	58.2	59.2	63.5	64.5
판매관리비	12.7	14.5	18.0	21.4	25.5
영업이익	6.4	7.5	9.7	15.5	19.8
증가율 (%)	99.5	17.2	29.0	60.4	27.6
영업이익률 (%)	20.4	19.9	20.7	26.7	28.2
영업외손익	0.5	0.3	1.0	1.4	1.1
금융손익	0.7	1.2	0.7	0.8	1.0
기타영업외손익	0.8	0.1	0.1	0.1	0.1
종속 및 관계기업관련손익	(1.0)	(0.9)	0.2	0.5	0.0
세전계속사업이익	6.9	7.8	10.7	17.0	20.9
법인세비용	0.7	0.6	1.3	2.7	3.5
계속사업이익	6.1	7.2	9.4	14.2	17.5
중단사업이익	0.0	0.0	0.0	0.0	0.0
당기순이익	6.1	7.2	9.4	14.2	17.5
증가율 (%)	79.6	16.7	31.1	51.4	22.8
순이익률 (%)	19.5	18.9	20.1	24.4	24.9
(지배주주) 당기순이익	6.1	7.2	9.4	14.2	17.5
(비지배주주) 당기순이익	0.0	0.0	0.0	0.0	0.0
총포괄이익	6.2	7.6	9.4	14.2	17.5
(지배주주) 총포괄이익	6.2	7.6	9.4	14.2	17.5
(비지배주주) 총포괄이익	0.0	0.0	0.0	0.0	0.0
EBITDA	7.1	8.1	10.7	17.0	21.8
증가율 (%)	76.5	13.8	32.1	58.5	28.0
EBITDA 이익률 (%)	22.7	21.5	22.9	29.2	31.0

현금흐름표

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
영업활동으로인한현금흐름	6.0	9.8	9.8	14.5	19.5
당기순이익	6.1	7.2	9.4	14.2	17.5
유형자산상각비	0.4	0.5	0.7	1.0	1.3
무형자산상각비	0.3	0.2	0.3	0.5	0.7
외화환산손실(이익)	(0.1)	0.0	0.0	0.0	0.0
자산처분손실(이익)	(0.7)	(0.0)	(0.0)	(0.0)	(0.0)
지분법, 종속, 관계기업손실(이익)	1.0	0.9	(0.7)	(0.5)	(0.0)
운전자본변동	(2.3)	0.4	0.1	(0.6)	0.2
(법인세납부)	(0.1)	(0.3)	(1.3)	(2.7)	(3.5)
기타	1.4	0.9	1.3	2.6	3.3
투자활동으로인한현금흐름	(4.3)	(7.6)	(5.6)	(9.2)	(7.8)
유형자산의증가(CAPEX)	(0.2)	(0.2)	(2.5)	(3.0)	(3.4)
유형자산의감소	0.0	0.0	0.0	0.0	0.0
무형자산의감소(증가)	(0.0)	(0.0)	(1.6)	(2.5)	(2.3)
투자자산의감소(증가)	(1.5)	(0.8)	2.8	0.3	(0.3)
기타	(2.6)	(6.6)	(4.3)	(4.0)	(1.8)
FCF	8.7	7.8	6.9	10.6	15.0
재무활동으로인한현금흐름	(0.2)	(1.2)	(1.3)	(1.3)	(1.3)
차입금의 증가(감소)	0.0	0.0	0.0	0.0	0.0
자기주식의처분(취득)	0.0	0.0	0.0	0.0	0.0
배당금	0.0	(1.1)	(1.3)	(1.3)	(1.3)
기타	(0.2)	(0.1)	0.0	0.0	0.0
기타현금흐름	0.0	0.0	0.0	0.1	0.0
연결범위변동으로인한현금의증가	0.0	0.0	0.0	0.0	0.0
환율변동효과	0.0	(0.0)	0.0	0.0	0.0
현금의증가(감소)	1.4	1.0	2.9	4.2	10.5
기초현금	2.5	3.9	4.9	7.8	12.0
기말현금	3.9	4.9	7.8	12.0	22.5

자료: 회사 자료, 신한투자증권

주요 투자지표

12월 결산	2021	2022	2023F	2024F	2025F
EPS (당기순이익, 원)	650	758	995	1,506	1,850
EPS (지배순이익, 원)	650	758	995	1,506	1,850
BPS (자본총계 원)	4,353	5,072	5,929	7,299	9,012
BPS (지배자본 원)	4,353	5,072	5,929	7,299	9,012
DPS (원)	120	150	150	150	150
PER (당기순이익 배)	19.5	10.8	13.4	8.8	7.2
PER (지배순이익 배)	19.5	10.8	13.4	8.8	7.2
PBR (자본총계 배)	2.9	1.6	2.2	1.8	1.5
PBR (지배자본 배)	2.9	1.6	2.2	1.8	1.5
EV/EBITDA (배)	14.1	5.4	7.9	4.5	3.0
배당성향 (%)	17.3	18.5	13.8	9.1	7.4
배당수익률 (%)	0.9	1.8	1.1	1.1	1.1
수익성					
EBITTDA 이익률 (%)	22.7	21.5	22.9	29.2	31.0
영업이익률 (%)	20.4	19.9	20.7	26.7	28.2
순이익률 (%)	19.5	18.9	20.1	24.4	24.9
ROA (%)	12.7	12.8	14.6	18.5	18.5
ROE (지배순이익, %)	16.1	16.1	18.1	22.8	22.7
ROIC (%)	46.8	65.1	67.4	78.0	78.3
안정성					
부채비율 (%)	27.6	24.0	24.7	23.4	22.3
순차입금비율 (%)	(47.5)	(70.5)	(72.6)	(70.6)	(71.7)
현금비율 (%)	37.5	46.5	58.9	78.5	127.4
이자보상배율 (배)	1,266.2	1,240.3	1,519.5	2,163.6	2,444.7
활동성					
순운전자본회전율 (회)	7.2	13.0	17.1	17.9	18.6
재고자산회수기간 (일)	20.1	30.9	32.4	28.9	26.8
매출채권회수기간 (일)	105.8	88.5	68.2	66.2	64.6

자료: 회사 자료, 신한투자증권

안랩

| Bloomberg Code (053800 KS) | Reuters Code (053800.KQ)

명실상부 대한민국 대표 보안 기업

[혁신성장]

백지우 연구원
☎ 02-3772-2671
✉ jiwoo100@shinhan.com

Not Rated	현재주가 (9 월 15 일)	목표주가	상승여력
-	63,500 원	-	-

- 엔드포인트 보안 솔루션에 기반한 국내 최장수 소프트웨어 기업
- 1) 글로벌 시장 진출 가시화, 2) 클라우드 보안 시장 진입
- 2023년 매출액 2,452억원, 영업이익 305억원 전망

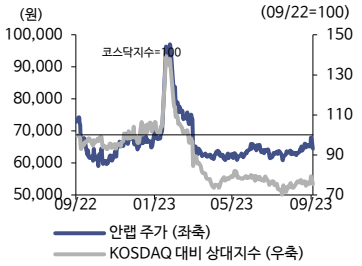
신한 리서치 투자정보
www.shinhansec.com

신한투자증권 기업분석부

시가총액	635.9 십억원
발행주식수	10.0 백만주
유동주식수	5.8 백만주(58.2%)
52주 최고가/최저가	96,900 원/59,100 원
일평균 거래량 (60일)	72,771 주
일평균 거래액 (60일)	4,648 백만원
외국인 지분율	22.69%
주요주주	
안철수 외 2 인	28.57%

절대수익률	
3개월	-0.8%
6개월	0.6%
12개월	-11.6%
KOSDAQ 대비 상대수익률	
3개월	-3.1%
6개월	-12.6%
12개월	-23.1%

주가



대한민국 대표 보안 소프트웨어 기업

안랩은 대표 제품 악성코드 분석 솔루션 V3 제품군을 비롯해 보안 서비스, 모바일 보안, 온라인 게임 보안, 네트워크 보안 솔루션, 보안 관제 서비스 등 다양한 보안 소프트웨어 포트폴리오를 보유하고 있다. 다양한 보안 관련 제품 포트폴리오를 기반으로 1995년 설립 이후 꾸준한 매출 성장을 기록했다. 이 외에도 클라우드, 생체인증 등 신성장 동력 확보를 위한 자회사 및 전략적 투자사를 보유하고 있다.

2023년 2분기 사업부문별 매출비중은 V3 등 보안솔루션 72%, 보안관제 서비스 19%, 기타 보안 컨설팅 및 외부상품 9%이다. 최근 클라우드 보안 및 OT 보안을 핵심 성장 동력으로 삼고 시장 진출이 가시화되고 있어 매출 확대가 기대된다.

안정적 캐시카우에 더한 성장 모멘텀

안랩의 V3 제품군(엔드포인트 보안솔루션)은 든든한 캐시카우 역할을 담당하고 있다. 최근 모바일 V3솔루션을 출시하며 악성 App과 문자를 진단 하고 있다. 과포화된 컴퓨터 백신 시장을 넘어 개화중인 스마트폰 보안 시장에 빠르게 진입한 점이 고무적이다. 모바일용, EDR 등 신제품을 통해 엔드포인트 보안 매출도 꾸준한 성장을 이어갈 전망이다.

안랩은 연초 글로벌 사업 확대에 중점을 둔 올해의 전략을 소개했다. 현재 일본과 중국에 현지법인을 두고 있으며, 동남아에서는 현지 파트너사와 협력을 통해 시장을 공략중이다. 이미 중국, 일본, 동남아에 각 나라의 특성에 맞는 제품을 공급하고 있다. 글로벌향 제품 업그레이드 및 개발, 글로벌 TF 설립 등 해외 진출에 박차를 가하고 있어 23년 하반기부터 가시적인 해외 매출 성장이 시작될 것으로 기대한다.

23년 영업이익 305억원(+12.9% YoY) 전망

2023년 매출액 2,452억원(+8% YoY), 영업이익 305억원(+13% YoY)을 전망한다. 현재 안랩의 중점 과제는 1) 글로벌 시장 진출, 2) 클라우드 보안 시장 점유율 확보다. 동남아, 중동 시장을 기반으로 글로벌 시장 진출에 박차를 가하고 있다. 또한 AI, 블록체인 회사 인수를 통해 클라우드 보안도 성장 동력으로 키워가고 있다. 클라우드 보안 매출이 본격화 된다면 밸류에이션 리레이팅의 기회가 될것으로 판단한다.

12월 결산	매출액 (십억원)	영업이익 (십억원)	지배순이익 (십억원)	EPS (원)	BPS (원)	PER (배)	EV/EBITDA (배)	PBR (배)	ROE (%)	순차입금비율 (%)
2021	207.3	22.9	42.2	4,210	25,051	23.5	26.0	3.9	18.0	(70.8)
2022	228.0	27.0	14.2	1,415	25,514	47.1	13.4	2.6	5.6	(75.0)
2023F	245.2	30.5	30.1	3,002	27,389	21.3	10.9	2.3	11.3	(75.0)
2024F	276.6	35.9	35.1	3,505	29,766	18.3	9.3	2.2	12.3	(74.4)
2025F	305.6	41.3	39.1	3,908	32,373	16.4	7.9	2.0	12.6	(73.7)

자료: 회사 자료, 신한투자증권

I. 기업개요

대한민국 대표 보안 솔루션 기업

국내 최장수 소프트웨어 브랜드

국내 대표 소프트웨어 브랜드로 1995년 설립됐다. 대표 제품 악성코드 분석 솔루션 V3 제품군을 비롯해 보안 서비스, 모바일 보안, 온라인 게임 보안, 네트워크 보안 솔루션, 보안 관제 서비스 등 다양한 보안 소프트웨어 포트폴리오를 보유하고 있다. 이 외에도 클라우드 등 신성장 동력 확보를 위한 자회사 및 전략적 투자사를 보유하고 있다.

주요 자회사로는 Web 3.0 멀티체인 지갑 사업을 영위하는 안랩 블록체인 컴퍼니, AI 기반 이상징후 탐지 솔루션 회사 Jason, OT/ICS 융합 보안 솔루션을 제공하는 Naonworks가 있다. 전략적 투자사로는 생체기반 인증 보안 기업 와이키키 소프트, 클라우드 네이티브 보안 기업 아스트론시큐리티 등이 있다.

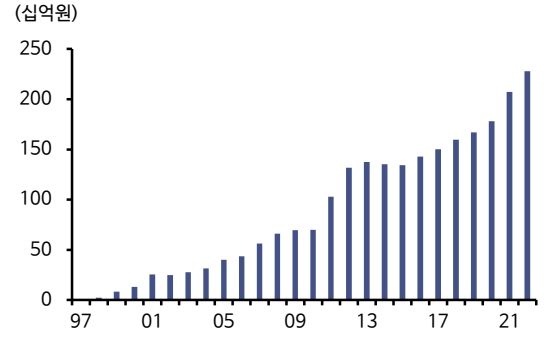
2023년 2분기 사업부문별 매출비중은 V3 등 보안솔루션 72%, 보안관제 서비스 19%, 기타 보안 컨설팅 및 외부상품 9%이다. 보안 솔루션은 V3, EDR 등의 엔드포인트 보안, TrusGuard, DPX 등의 네트워크 보안, 클라우드 보안 등 다양한 제품군을 포함한다. 최근 클라우드 보안 및 OT 보안을 핵심 성장 동력으로 삼고 시장 진출이 가시화되고 있어 매출 확대가 기대된다.

안랩 주요 연혁

일시	내용
1995.03	안철수컴퓨터바이러스 연구소 설립
2002	윈도우 서버용 백신 출시, 일본법인 설립
2011	스마트폰 보안 솔루션 V3 Mobile 2.0 출시
2016	V3모바일 시큐리티 국내 출시, AWS 고객용 원격보안관제 서비스 개시
2018	안랩 EDR 출시, 차세대 방화벽 안랩v트러스트가드 출시
2023	안랩 솔루션 전용 SOAR 플랫폼 출시

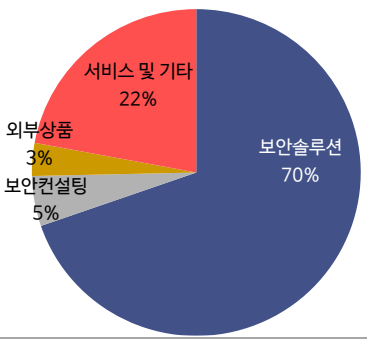
자료: 신한투자증권 추정

설립 이후 매출액 추이



자료: 회사 자료, 신한투자증권

2022년 매출 비중



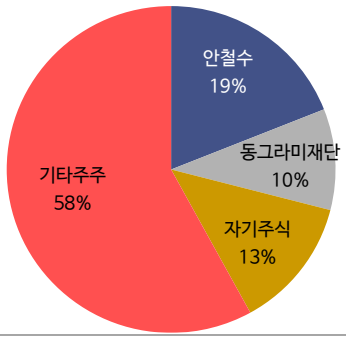
자료: 회사 자료, 신한투자증권

수상현황

수상 내역	기관
MDS, 차세대 세계 일류상품 선정	산업통산자원부
2021-2019, 올해의 엔드포인트 보안 기업	프로스트앤설리번
최우수 성능 보안 솔루션상	AV-TEST
2018, 올해의 보안관제서비스 기업	프로스트앤설리번
APT 솔루션 기술 혁신상	프로스트앤설리번
독일 IF 디자인 어워드 2관왕	-
정보통신디지털대상 정보통신부장관상	-
SW 산업협회장상	-
IR52 장영실상	-
대한민국특허기술대전 특허청장상	-

자료: 회사 자료, 신한투자증권

주주현황



자료: 회사 자료, 신한투자증권

자회사 및 전략적 투자사

자회사

- AhnLab Blockchain Company — Web 3.0 멀티체인 지갑
- JASON (an AhnLab Company) — AI 기반 이상징후 탐지
- NAONWORKS (an AhnLab Company) — OT/ICS 융합 보안 솔루션

전략적 투자사

- Whykeykey — 생체 기반 인증 보안 기업
- ASTRON — 클라우드 네이티브 보안 기업
- MONITORAPP — 클라우드 기반 SECaaS 전문 기업
- Spiceware — 클라우드 기반 데이터 보안 기업
- Tatum Security — 클라우드 컴플라이언스 모니터링 보안 기업
- FESCARO — 자동차 보안 S/W 전문 기업

자료: 회사 자료, 신한투자증권

비즈니스 포트폴리오

자료: 회사 자료, 신한투자증권

II. 투자포인트

안정적인 성장에 더한 모멘텀

안랩의 엔드포인트 사업부는 든든한 캐시카우 역할을 담당하고 있다. 엔드유저들의 컴퓨터 등을 보호해주는 V3 제품군은 국내 명실상부 1위 안티바이러스 솔루션이다. 백신 솔루션 최초 선점 효과에 더해 안랩은 7년 연속 연구개발 투자를 늘리며 계속해서 솔루션을 발전시키고 있다.

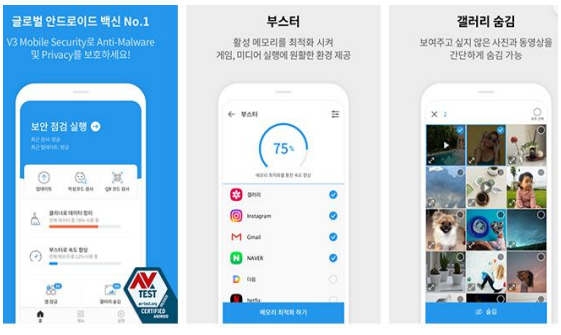
최근 '퀀텀 러닝', 'V3 유저모드 실시간 감시'를 포함해 19개의 연구개발 실적을 올렸다. 이러한 공격적인 R&D 투자는 높은 기술력으로 이어져 V3 제품군은 주요 해외 보안제품 평가에서 연이어 인증을 획득했다. 2022년 영국 바이러스 불러틴의 VB100 평가에서 참가한 모든 테스트 인증을 획득했으며, 미국 ICSA랩의 PC용 백신 인증 갱신 등 다양한 인증을 획득했다. 2023년 기준 V3는 국내 유일 AV-TEST, VB100, ICSA 등 주요 해외인증을 획득한 솔루션이다.

V3는 더 이상 컴퓨터만을 위한 보안 솔루션이 아니다. 최근 모바일 V3 솔루션을 출시하며 악성 애플리케이션과 문자를 모두 진단/차단 하고 있다. 예를 들어 부고 문자, 모바일 청첩장 등 링크(URL) 접속이 필요한 문자에 대해 보이스 피싱 주의 알림을 보내는 등 해킹 피해를 최소화 한다. 이미 과포화된 컴퓨터용 백신 시장을 넘어 아직 개화중인 스마트폰 보안 시장에 빠르게 진입한 점이 고무적이다. 또한 알려지지 않은 위협에 대해 실시간으로 탐지하는 발전한 엔드포인트 보안 솔루션인 안랩 EDR도 출시하고 있어 안정적인 V3 백신 매출에 더해 모바일용, EDR 등 추가 성장 모멘텀도 보유하고 있다.

안랩 EDR 도입 후 위협 대응 프로세스

자료: 회사 자료, 신한투자증권

모바일 V3 솔루션 화면



자료: 회사 자료, 신한투자증권

해외 시장 진출, 성장성의 한계 극복중

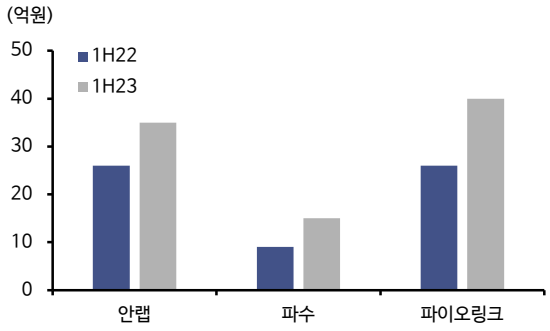
전통적인 내수산업이라고 여겨졌던 보안산업은 글로벌 시장 진출에 박차를 가하고 있다. 안랩은 연초 통합 보안과 글로벌 사업 확대에 중점을 둔 올해의 전략을 소개했다. 현재 일본과 중국에 현지법인을 두고 있으며, 동남아 등 기타 지역에 대해서는 본사 해외사업팀에서 현지 파트너사와 협력을 통해 시장을 공략중이다. 해외에 특화된 제품군으로는 안랩 EPS(Endpoint Protection System), 지능형 위협 대응 솔루션 안랩 MDS, 스마트폰 보안 솔루션 V3모바일 등이 있다.

중국 시장 같은 경우 공장 등의 생산시설이 많아 EPS, V3 제품군 위주로 수출이 이루어지고 있다. 일본의 경우 자국 솔루션을 선호하는 보수적인 성향이 강해 현재 모바일 V3 솔루션을 위주로 수출을 시도하고 있다. 동남아의 경우 공공 및 금융기관을 중심으로 지능형 위험 대응 솔루션인 MDS 제품군을 위주로 판매를 시작했다. 과거 코로나19로 인해 해외법인 이익률이 저조했지만 현재 코로나19 이전 수준을 회복했다. 글로벌향 제품 업그레이드 및 개발, 글로벌 TF 설립 등 해외 진출에 박차를 가하고 있어 23년 하반기부터 가시적인 해외 매출 성장이 시작될 것으로 기대한다.

안랩 글로벌 파트너

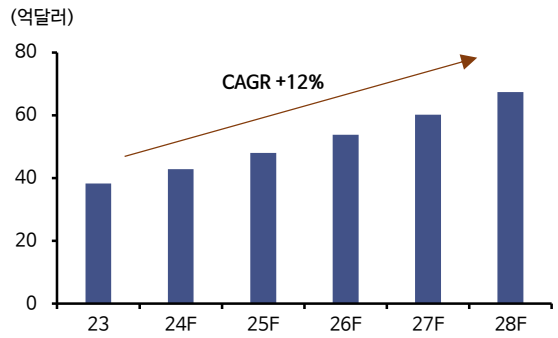
자료: 회사 자료, 신한투자증권

주요 보안 기업 수출액



자료: Dart, 신한투자증권

동남아시아 보안시장 규모 추이



자료: Statista, 신한투자증권

클라우드 보안의 시대

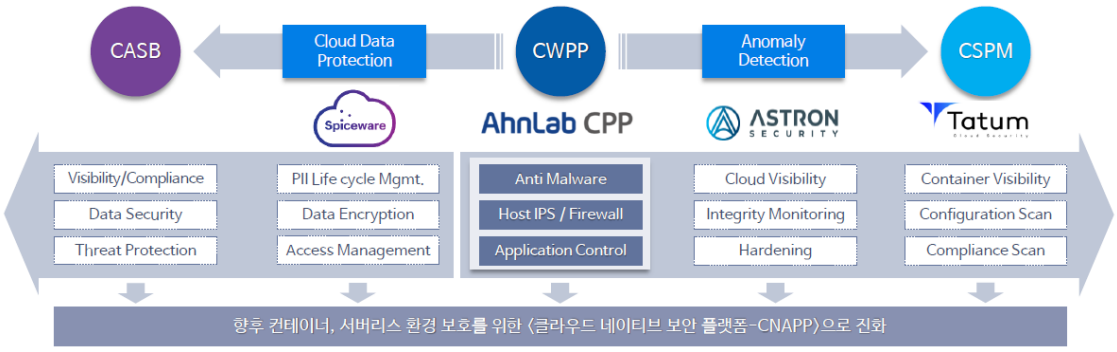
안랩은 2021년 2월부터 클라우드 보안 서비스를 시작했다. 디지털 트랜스포메이션 및 비대면 시대를 맞아 클라우드 도입이 가속화되며 기업은 클라우드 서비스 '구축, 운영, 보안' 세가지를 모두 제공하는 서비스에 대한 수요가 늘어났다. 서비스 출시 후 금융, 건설, SW개발 등 다양한 산업분야의 대기업, 중견기업을 고객사로 확보중이다.

안랩 클라우드는 클라우드 운영, 보안을 관리하는 'Managed Service'와 24시간 보안 현황을 모니터링하는 보안관제, 기술지원까지 클라우드 운영에 필요한 모든 요소들을 종합적으로 제공한다. 특히 클라우드 운영 및 구축을 진행하며 보안 컨설팅을 통해 안랩의 다른 보안 서비스를 제안할 수 있어서 기타 보안 솔루션 매출과의 시너지 효과가 상당하다.

안랩은 아마존 웹서비스(AWS), 네이버 클라우드 플랫폼, 코스콤, 카카오 엔터프라이즈, NHN 클라우드 등 국내외 주요 기업들과 파트너십을 체결했다. 특히 AWS 올해(2022)의 라이징 스타 서비스 파트너상을 수상하며, 국내 파트너 중 높은 성장률을 달성하고 다수의 고객을 유치하는 등의 우수한 성과들을 인정받았다.

현재 클라우드 보안 시장은 블루오션으로 아직 성장여력이 충분하다. 안랩은 클라우드 보안 사업부를 중요한 성장동력으로 여기며, 클라우드 관련 솔루션을 보유한 다수의 자회사 및 투자회사를 갖고 있다. AI를 이용한 보안, 블록체인 보안 등 다양한 보안 솔루션을 보유한 자회사를 통해 더욱 발전된 클라우드 보안 서비스를 제공할 수 있을 것으로 기대된다.

자회사 및 전략적 투자사를 활용한 클라우드 보안 솔루션 확장



자료: 회사 자료, 신한투자증권

III. 실적전망

꾸준한 성장에 대한 확신

2023년 매출액 2,452억원(+7.6% YoY), 영업이익 305억원(+12.9% YoY)을 전망한다. V3 백신 솔루션이 이미 포화상태에 이르러 시장에서는 지속적인 성장에 대한 의심을 지울 수 없었다. 그러나 해외 시장 개척, 모바일용 솔루션 개발, 클라우드 MSP 사업 시작 등 다양한 사업을 통해 꾸준한 성장을 기록할 예정이다.

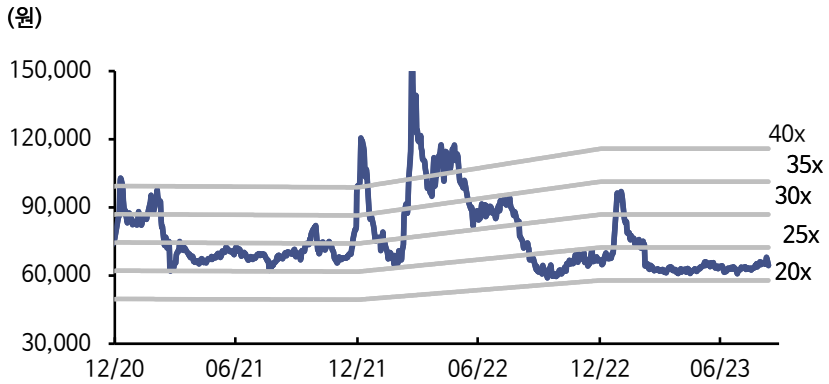
현재 안랩의 중점 과제는 1) 글로벌 시장 진출과 2) 클라우드 보안 솔루션 시장 점유율 확보이다. 동남아, 중동 시장을 기반으로 글로벌 TF를 설립하여 글로벌 시장 진출에 박차를 가하고 있다. 또한 AI, 블록체인 자회사 및 투자회사 인수를 통해 클라우드 보안도 향후 중요한 성장 동력으로 키워나가고 있다. 클라우드 보안 및 새로운 보안 솔루션의 경우 1회성 설치가 아닌 구독형으로 출시하는 경우가 많아 지속적인 현금흐름을 확보할 수 있을 것으로 기대된다. 확보한 현금을 바탕으로 24년 이후 보안 업계의 유망한 회사에 대한 투자 및 인수를 적극적으로 검토할 것으로 예상된다.

연도별 실적 추이

(십억원)	2020	2021	2022	2023F	2024F	2025F
매출액	178.2	207.3	228.0	245.2	276.6	305.6
보안솔루션	118.6	147.3	158.9	167.2	180.3	195.4
보안컨설팅	9.6	11.7	11.3	12.1	14.4	15.5
보안관제 서비스	31.2	30.7	43.1	50.1	62.3	73.2
외부상품 및 기타	18.7	17.6	14.7	15.8	19.6	21.5
영업이익	20.0	22.9	27.0	30.5	35.9	41.3
영업이익률	11.2	11.1	11.8	12.4	13.0	13.5
지배주주순이익	18.6	42.2	14.2	30.1	35.1	39.2

자료: 신한투자증권 추정

12M Forward PER Band 차트



자료: 회사 자료, 신한투자증권

재무상태표

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
자산총계	338.2	345.0	370.3	405.9	442.9
유동자산	226.9	243.7	270.1	301.2	335.3
현금및현금성자산	35.0	36.2	42.4	44.3	57.1
매출채권	34.9	33.5	40.2	50.5	60.7
재고자산	6.1	8.8	13.8	16.6	22.4
비유동자산	111.3	101.3	100.2	104.7	107.6
유형자산	54.3	52.2	50.9	51.8	53.6
무형자산	12.9	13.2	11.5	10.0	8.8
투자자산	36.5	24.5	26.1	30.9	31.9
기타금융업자산	0.0	0.0	0.0	0.0	0.0
부채총계	83.5	85.7	92.1	103.9	114.8
유동부채	76.4	75.1	80.8	91.1	100.7
단기차입금	0.0	0.0	0.0	0.0	0.0
매입채무	11.4	8.3	8.9	10.1	11.1
유동성장기부채	0.0	0.0	0.0	0.0	0.0
비유동부채	7.1	10.5	11.3	12.8	14.1
사채	0.0	0.0	0.0	0.0	0.0
장기차입금(장기금융부채 포함)	0.4	0.2	0.2	0.2	0.2
기타금융업부채	0.0	0.0	0.0	0.0	0.0
자본총계	254.7	259.3	278.1	301.9	328.1
자본금	5.2	5.2	5.2	5.2	5.2
자본잉여금	68.2	68.2	68.2	68.2	68.2
기타자본	(21.1)	(21.1)	(21.1)	(21.1)	(21.1)
기타포괄이익누계액	(0.3)	(0.3)	(0.3)	(0.3)	(0.3)
이익잉여금	198.9	203.6	222.3	246.2	272.3
지배주주지분	250.9	255.5	274.2	298.0	324.2
비지배주주지분	3.8	3.8	3.9	3.9	3.9
*총차입금	0.8	0.7	0.7	0.8	0.8
*순차입금(순현금)	(180.4)	(194.5)	(208.5)	(224.7)	(241.8)

포괄손익계산서

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
매출액	207.3	228.0	245.2	276.6	305.6
증감률 (%)	16.3	10.0	7.6	12.8	10.5
매출원가	0.0	0.0	0.0	0.0	0.0
매출총이익	207.3	228.0	245.2	276.6	305.6
매출총이익률 (%)	100.0	100.0	100.0	100.0	100.0
판매관리비	184.3	201.0	214.7	240.7	264.3
영업이익	22.9	27.0	30.5	35.9	41.3
증감률 (%)	14.8	17.7	12.9	17.7	15.2
영업이익률 (%)	11.1	11.8	12.4	13.0	13.5
영업외손익	27.4	(10.4)	4.7	5.4	4.7
금융손익	27.5	(9.9)	6.1	5.8	4.7
기타영업외손익	(0.1)	(1.5)	(1.4)	(0.5)	0.0
종속 및 관계기업관련손익	0.0	1.0	0.0	0.0	0.0
세전계속사업이익	50.3	16.5	35.2	41.2	46.1
법인세비용	8.3	2.4	5.1	6.1	6.9
계속사업이익	42.0	14.2	30.1	35.1	39.1
중단사업이익	0.0	0.0	0.0	0.0	0.0
당기순이익	42.0	14.2	30.1	35.1	39.1
증감률 (%)	127.5	(66.3)	112.1	16.8	11.5
순이익률 (%)	20.3	6.2	12.3	12.7	12.8
(지배주주) 당기순이익	42.2	14.2	30.1	35.1	39.1
(비지배주주) 당기순이익	(0.1)	0.0	0.0	0.0	0.0
총포괄이익	42.1	14.2	30.1	35.1	39.1
(지배주주) 총포괄이익	42.2	14.2	30.1	35.1	39.1
(비지배주주) 총포괄이익	(0.1)	0.0	0.0	0.0	0.0
EBITDA	31.3	35.6	40.1	45.3	50.9
증감률 (%)	9.9	14.0	12.4	13.1	12.3
EBITDA 이익률 (%)	15.1	15.6	16.3	16.4	16.6

현금흐름표

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
영업활동으로인한현금흐름	31.9	33.5	31.1	40.8	41.1
당기순이익	42.0	14.2	30.1	35.1	39.1
유형자산상각비	7.2	7.1	7.8	8.0	8.4
무형자산상각비	1.2	1.6	1.8	1.4	1.2
외화환산손실(이익)	(0.1)	0.2	0.0	0.0	0.0
자산처분손실(이익)	(0.0)	0.0	0.0	0.0	0.0
지분법, 종속, 관계기업손실(이익)	0.0	(1.0)	0.0	0.0	0.0
운전자본변동	0.7	(0.2)	(7.4)	(2.9)	(7.6)
(법인세납부)	(2.5)	(5.8)	(5.1)	(6.1)	(6.9)
기타	(16.6)	17.4	3.9	5.3	6.9
투자활동으로인한현금흐름	(8.5)	(21.9)	(11.6)	(19.9)	(20.7)
유형자산의증가(CAPEX)	(5.1)	(4.0)	(6.5)	(8.9)	(10.2)
유형자산의감소	0.1	0.0	0.0	0.0	0.0
무형자산의감소(증가)	(3.7)	(3.2)	0.0	(0.0)	0.0
투자자산의감소(증가)	7.0	0.5	(1.5)	(4.8)	(1.0)
기타	(6.8)	(15.2)	(3.6)	(6.2)	(9.5)
FCF	42.6	23.7	22.5	26.5	27.0
재무활동으로인한현금흐름	(9.8)	(10.1)	(9.6)	(11.3)	(11.3)
차입금의 증가(감소)	(1.5)	0.0	0.0	0.1	0.1
자기주식의처분(취득)	0.0	0.0	0.0	0.0	0.0
배당금	(7.8)	(9.6)	(9.6)	(11.3)	(11.3)
기타	(0.5)	(0.5)	0.0	(0.1)	(0.1)
기타현금흐름	0.0	0.0	(4.2)	(7.8)	3.7
연결범위변동으로인한현금의증가	0.0	0.0	0.0	0.0	0.0
환율변동효과	0.1	(0.2)	0.0	0.0	0.0
현금의증가(감소)	13.7	1.4	5.7	1.9	12.8
기초현금	21.6	35.3	36.7	42.4	44.3
기말현금	35.3	36.7	42.4	44.3	57.0

자료: 회사 자료, 신한투자증권

주요 투자지표

12월 결산	2021	2022	2023F	2024F	2025F
EPS (당기순이익, 원)	4,198	1,416	3,003	3,507	3,909
EPS (지배순이익, 원)	4,210	1,415	3,002	3,505	3,908
BPS (자본총계, 원)	25,434	25,899	27,774	30,153	32,761
BPS (지배지분, 원)	25,051	25,514	27,389	29,766	32,373
DPS (원)	1,100	1,100	1,300	1,300	1,500
PER (당기순이익, 배)	23.6	47.1	21.3	18.3	16.4
PER (지배순이익, 배)	23.5	47.1	21.3	18.3	16.4
PBR (자본총계, 배)	3.9	2.6	2.3	2.1	2.0
PBR (지배지분, 배)	3.9	2.6	2.3	2.2	2.0
EV/EBITDA (배)	26.0	13.4	10.9	9.3	7.9
배당성향 (%)	22.7	67.4	37.6	32.2	33.3
배당수익률 (%)	1.1	1.6	2.0	2.0	2.3
수익성					
EBITDA 이익률 (%)	15.1	15.6	16.3	16.4	16.6
영업이익률 (%)	11.1	11.8	12.4	13.0	13.5
순이익률 (%)	20.3	6.2	12.3	12.7	12.8
ROA (%)	13.6	4.1	8.4	9.0	9.2
ROE (지배순이익, %)	18.0	5.6	11.3	12.3	12.6
ROIC (%)	51.2	51.7	63.3	75.5	68.8
안정성					
부채비율 (%)	32.8	33.0	33.1	34.4	35.0
순차입금비율 (%)	(70.8)	(75.0)	(75.0)	(74.4)	(73.7)
현금비율 (%)	45.9	48.2	52.4	48.6	56.7
이자보상배율 (배)	1,097.4	674.0	799.6	872.7	922.0
활동성					
순운전자본회전율 (회)	(10.3)	(8.1)	(10.8)	(16.2)	(27.6)
재고자산회수기간 (일)	8.8	11.9	16.8	20.0	23.3
매출채권회수기간 (일)	65.2	54.7	54.9	59.8	66.4

자료: 회사 자료, 신한투자증권

파이오링크

Bloomberg Code (170790 KS) | Reuters Code (170790.KQ)

안정성에 더한 모멘텀

[혁신성장]

백지우 연구원
☎ 02-3772-2671
✉ jiwoo100@shinhan.com

Not Rated	현재주가 (9 월 15 일)	목표주가	상승여력
-	13,210 원	-	-

- 국내 1위 ADC 기업, 데이터센터 증설 직접적 수혜
- 1) 데이터 센터 이중화 진행, 2) 세대간 망분리 정책 효과 가시화
- 고마진 제품 매출비중 확대로 영업이익률 개선 전망

신한 리서치 투자정보
www.shinhansec.com

신한투자증권 기업분석부

시가총액	91.1 십억원
발행주식수	6.9 백만주
유동주식수	4.0 백만주(58.1%)
52주 최고가/최저가	17,590 원/9,990 원
일평균 거래량 (60 일)	67,864 주
일평균 거래액 (60 일)	1,058 백만원
외국인 지분율	3.93%
주요주주	
이글루시큐리티	외 3 인 39.28%

절대수익률	
3 개월	-3.1%
6 개월	-0.2%
12 개월	13.6%
KOSDAQ 대비 상대수익률	
3 개월	-5.3%
6 개월	-13.3%
12 개월	-1.3%

주가

국내 1위 ADC 기업

네트워크 장비 및 웹보안 관련 서비스를 제공하는 기업이다. 주요 제품으로는 ADC, 보안스위치, 웹방화벽이 있으며 보안 컨설팅 또한 제공하고 있다. ADC는 데이터센터의 트래픽을 분산시켜주는 장비이며, 보안 스위치는 정보의 송수신 보안을 담당한다. 웹방화벽은 웹 서버를 보호하고, 보안서비스는 컨설팅 및 관제서비스를 담당한다. 2023년 예상 매출 비중은 ADC 37%, 보안스위치 29%, 웹방화벽 4%, 보안서비스 및 기타 매출 30%로 추정된다.

1) 데이터센터 이중화, 2) 세대 간 망분리 정책 효과 가시화

파이오링크는 국내 1위 ADC 사업자로서 데이터센터 시장 확대의 수혜를 가장 크게 받을 수 있는 업체다. ADC는 특정 서버에 트래픽이 몰리지 않도록 분산시켜주는 장치로, 데이터 센터 트래픽 관리에 필수적이다. 데이터센터 화재로 인한 카카오 먹통 사태가 발생하며 정부, 및 기업 차원에서 데이터센터 이중화를 추진 중이다. 카카오를 비롯하여 네이버 클라우드 등 각 기업이 데이터센터 이중화를 추진하고 있어, 이에 따라 ADC 수요 또한 자연스럽게 증가할 것으로 기대된다.

보안 스위치의 국내외 매출이 모두 상승하고 있다. 일본의 IT 인력 부족 사태가 장기화 되며 이를 대체할 수 있는 보안스위치 수요가 지속 증가하고 있다. 국내에서는 아파트 월패트 해킹 사건이 발생하며 세대간 망분리 의무화가 시행되었다. 보안스위치는 세대간 망분리를 가장 경제적이고 효율적으로 시행할 수 있는 솔루션으로, 2024년 완공되는 아파트를 대상으로 매출 발생이 본격화 될 전망이다.

23년 매출액 705억원, 영업이익 140억원 전망

2023년 매출액 705억원(+14.4% YoY), 영업이익 140억원(+22.6% YoY)을 전망한다. 상대적으로 이익률이 높은 ADC, 보안스위치 매출이 상승하며 영업 이익률 개선이 예상된다. 최근 보안 컨설팅부터 구축, 운영까지 원스톱으로 지원하는 HCI 제품을 출시했다. 통합된 서버 인프라를 통해 유지보수, 관리 비용 절감이 가능한 HCI 제품 매출은 2024년 이후부터 가시화 될 것으로 기대된다. 2024F PER은 5.3배로 동종 업계 기업 대비 저평가 되어 있어 주목이 필요한 시점이다.

12월 결산	매출액 (십억원)	영업이익 (십억원)	지배순이익 (십억원)	EPS (원)	BPS (원)	PER (배)	EV/EBITDA (배)	PBR (배)	ROE (%)	순차입금비율 (%)
2021	54.3	10.9	11.2	1,629	9,030	10.8	6.7	2.0	19.6	(60.6)
2022	61.6	11.4	12.1	1,771	10,583	6.8	2.9	1.1	18.1	(63.2)
2023F	70.5	14.0	14.1	2,054	12,344	6.5	2.2	1.1	17.9	(65.6)
2024F	81.1	16.8	17.0	2,486	14,519	5.3	1.2	0.9	18.5	(67.7)
2025F	92.3	19.7	19.6	2,861	17,039	4.6	0.5	0.8	18.1	(69.4)

자료: 회사 자료, 신한투자증권

I. 기업개요

네트워크 + 보안 전문 기업

클라우드 데이터센터 최적화를 위한 네트워크 장비 및 웹보안 관련 서비스를 제공하는 기업이다. 2000년 설립되어 국내 최초 애플리케이션 스위치인 'PINK BOX'를 출시하고, 웹 애플리케이션 방화벽, 보안 L2 스위치 등 제품 라인업을 확장하며 2013년 코스닥에 상장됐다. 다양한 제품을 출시하며 현재 사업부는 크게 ADC, 보안스위치, 웹방화벽, 보안서비스로 구분된다. 2023년 예상 매출 비중은 ADC 37%, 보안스위치 29%, 웹방화벽 4%, 보안서비스 및 기타 매출 30%로 추정된다.

2015년 NHN엔터가 파이오링크의 지분 29.7%를 인수했다. NHN엔터의 지분 인수는 클라우드 데이터센터 및 전자상거래, 인프라 사업에 기반이 되는 기술을 확보하기 위함이다. 이는 파이오링크의 클라우드 데이터센터 최적화 기술을 인정받은 사례다. 2022년 국내 클라우드 시장규모는 1.5조원으로 2017년 이후 연평균 20% 이상의 성장률을 기록하고 있다. 최근 일본 데이터 클라우드 확장 트렌드로 일본向 수출액도 꾸준히 증가하고 있어 국내외 시장 모두 매출액 성장이 기대된다.

1. 네트워크 사업부

네트워크 사업부는 매출의 70%를 차지하며, 제품을 만드는 주요 사업부이다. 네트워크 사업부에는 1) ADC, 2) 보안 스위치, 3) 웹 방화벽 제품이 있다.

ADC(Application Delivery Controller): 웹서버 앞단에서 특정 서버에 트래픽이 과도하게 몰리지 않도록 다양한 서버에 트래픽을 분산시키는 장비이다. 트래픽 분산을 통해 서버 속도를 향상시키며 보안을 강화한다. ADC는 웹서버로 들어오는 수많은 트래픽을 관리하는 일종의 '교통정리' 역할을 수행한다. 파이오링크의 주력 제품으로 국내 유일 제조사이며, 7년간 국내 점유율 1위를 차지하고 있다.

보안스위치: 엔드 유저들의 정보 송신과 수신을 담당하는 L2스위치에 보안 기능을 추가한 스위치이다. 2015년 국내 최초로 클라우드 스위치를 개발했다. 설치단계부터 운영, 유지보수까지 클라우드 기반의 서비스가 간으한 하이엔드 제품이다. 초기 설치비용이 기타 스위치보다 높지만 유지 보수 및 관리에 필요한 비용을 크게 절감할 수 있어, 인건비가 높은 선진국 시장에서 수요가 증가하고 있다.

웹방화벽: 웹화면을 구성해주는 웹서버 바로 앞에서 방화벽 역할을 수행한다. 웹서버로 향하는 트래픽을 감시하고, 공격을 차단한다. 현재 매출 비중은 5% 정도로 ADC와 보안스위치에 비해서는 매출이 크지 않다.

2. 보안 사업부

보안 사업부는 매출의 30%를 차지하며, 제품을 만드는 주요 사업부이다. 보안관제서비스와 보안 컨설팅 서비스를 제공중이다. 이러한 보안 서비스는 웹방화벽과 시너지 효과가 존재한다. 자체 웹방화벽을 활용하여 보안관제서비스를 공급함으로서 서비스 매출과 장비 매출이 동시에 발생하는 이점이 있다.

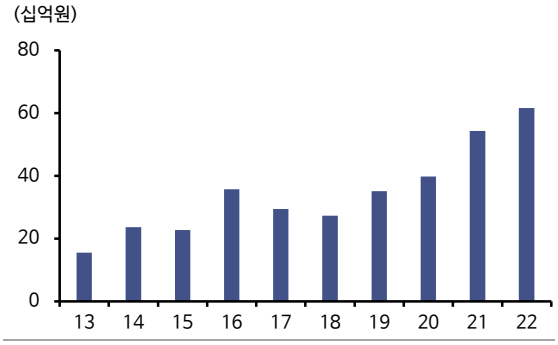
보안서비스: 2015년부터 보안 관제 서비스 제공을 시작했다. 보안 위협을 실시간으로 감지하는 시스템을 구축하는 서비스이다. 2018년에는 비트러스트 컨설팅 사업부 영업양수를 통해 보안 컨설팅 서비스도 함께 제공하고 있다. 빅데이터 및 AI 기반 차세대 보안 컨설팅을 선보이고 있으며, 원격 관제, 파견관제 서비스를 통해 보다 효율적인 보안 서비스를 제공 중이다.

파이오링크 주요 연혁

일시	내용
2000.07	파이오링크 설립
2004.06	일본, 중국 지사 설립
2006.04	웹 애플리케이션 방화벽 WEBFRONT 출시
2013.08	코스닥 시장 상장
2014.04	국내 최초 고성능 SDN스위치, TiFLOW 출시
2018.04	비트러스트 보안컨설팅사업 부문 양수, 보안컨설팅 서비스 시작
2021.07	하이퍼 컨버지드 인프라 POPCON HCI 출시
2022.03	홈 네트워크 보안 시장 진출

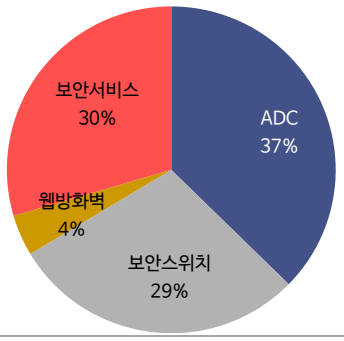
자료: 신한투자증권 추정

상장 이후 매출액 추이



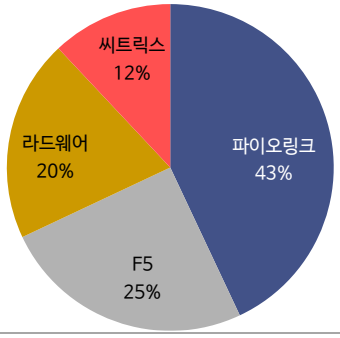
자료: 회사 자료, 신한투자증권

2022년 매출 비중



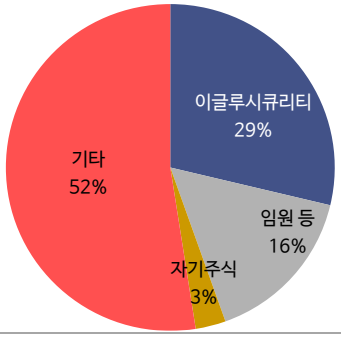
자료: 회사 자료, 신한투자증권

ADC 국내 점유율 현황



자료: IDC, 신한투자증권

주주현황



자료: 회사 자료, 신한투자증권

ADC(PAS-K) 주요 기능

1. 다양한 부하분산

- 다수 서버에 동일한 애플리케이션 운용 시, 트래픽 각 서버로 균형 있게 전달
- 효율적인 장비 리소스 활용
- 방화벽, VPN, 게이트웨이 등 적용

2. GSLB

- 데이터센터 이중화나 재해복구(DR)센터 구축에 활용
- 한 사이트에 예상치 못한 장애가 발생하더라도 나머지 사이트 중 가장 적절한 사이트로 연결

3. 고가용성

- 서비스 가용성을 모니터링하여 정상 작동중인 서버들만 세션 연결
- 고가용성을 위해 다양한 Failover 기능과 세션 동기화 및 설정 동기화 등 제공

자료: 회사 자료, 신한투자증권

파이오링크 제품 및 서비스 포트폴리오

자료: 회사 자료, 신한투자증권

II. 투자포인트

ADC는 역시 파이오링크

파이오링크는 국내 1위 ADC 사업자로서 데이터센터 시장 확대의 수혜를 가장 크게 받을 수 있는 업체다. 넷플릭스, 유튜브, 재택근무로 인한 화상 프로그램 증가 등 대용량 트래픽 사용량 증가로 이를 수용할 수 있는 데이터 센터의 증설이 계속되고 있다. ADC는 웹 서버 앞단에 위치하여 특정 서버에 트래픽이 몰리지 않도록 분산시켜주는 장치로, 데이터 센터 트래픽 관리에 필수적이다.

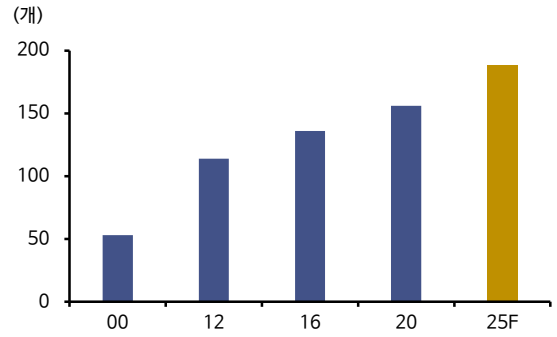
데이터센터 이중화 수혜

2022년 경기 판교 SK C&C 데이터센터 화재로 카카오톡 먹통 사태가 발생하며 데이터센터에 대한 관심이 높아졌다. 데이터센터는 데이터를 저장하는 서버, 스토리지, 데이터를 전송하는 네트워크, 이를 구동하는 발전기 등 모든 시설을 포함한 종합 센터를 지칭한다.

데이터센터의 가장 큰 특징은 '이중화'이다. 전기가 들어오는 선, 발전기 등 모든 전선이 이중으로 구성되어 있다. 화재와 같은 사태가 발생했을 때 다른 라인으로 전력이 공급되어야 하기 때문이다. 그러나 판교 데이터센터 화재의 경우 데이터센터 내의 물리적인 이중화는 됐지만, 시스템의 이중화가 되어있지 않아 먹통사태를 겪었다. 이로 인해 지난해 12월 카카오 먹통 방지법이 법사위를 통과하여, 데이터센터 이중화 조치 마련 및 재난 관리 기본계획을 수립해야하는 사업자가 증가했다.

이로 인해 데이터센터의 이중화에 가속도가 붙을 전망이다. 삼중화, 사중화에 대한 논의도 계속되고 있으며, 데이터센터의 다중화는 결국 데이터센터의 증설로 이어진다. 현재 정부는 데이터센터 지방 분산을 통해 데이터 이중화 및 재해복구 안정성을 확보하고자 한다. 카카오를 비롯하여 네이버 클라우드 등 각 기업이 데이터센터 이중화를 추진하고 있어 지속적인 데이터센터 증설이 이뤄질 것으로 예상되며, 이에 따라 ADC 수요 또한 자연스럽게 증가할 것으로 기대된다.

국내 데이터센터 수 추이

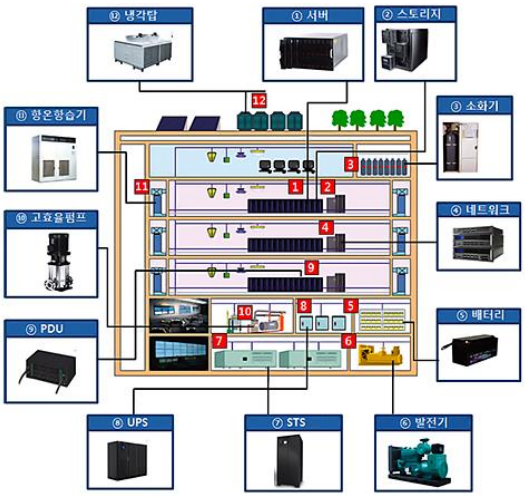


자료: 한국데이터센터연합회, 신한투자증권

파이오링크 ADC 제품

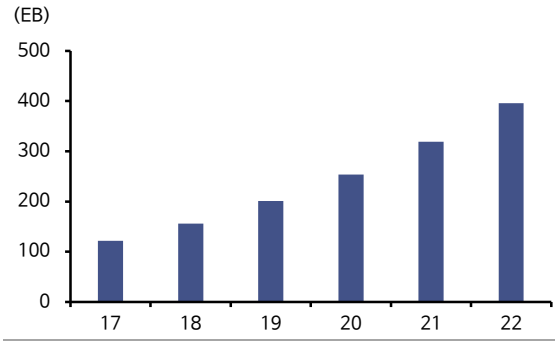
자료: 회사 자료, 신한투자증권

데이터센터의 구성



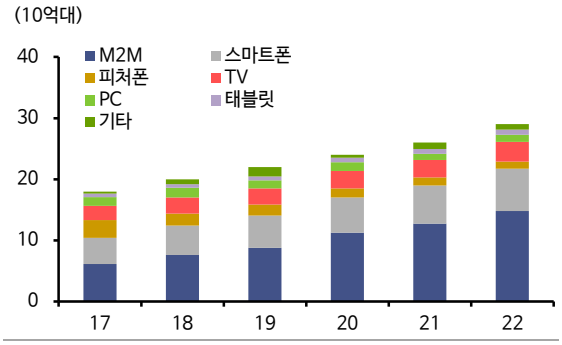
자료: 한국전자통신연구원, 신한투자증권

월 평균 IP 트래픽 추이



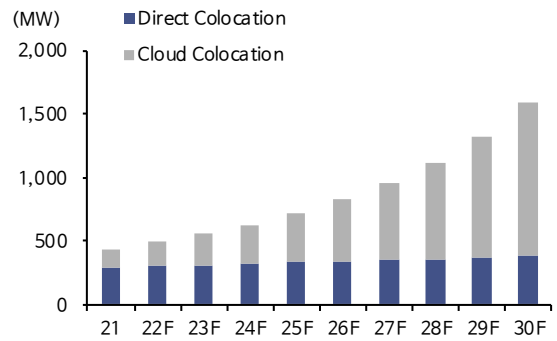
자료: CISCO, 신한투자증권

전 세계 디바이스 및 회선 증가 추이



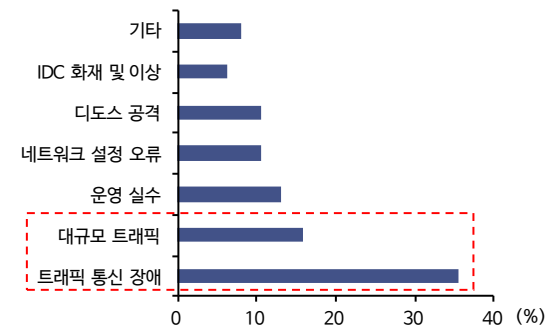
자료: CISCO, 신한투자증권

국내 데이터센터 수요 전망



자료: SK Broadband, 신한투자증권

시스템 장애 주요 원인



자료: 보안 뉴스, 신한투자증권

보안스위치 해외 매출 증가

일본: 치솟는 인건비, 대안은 보안스위치

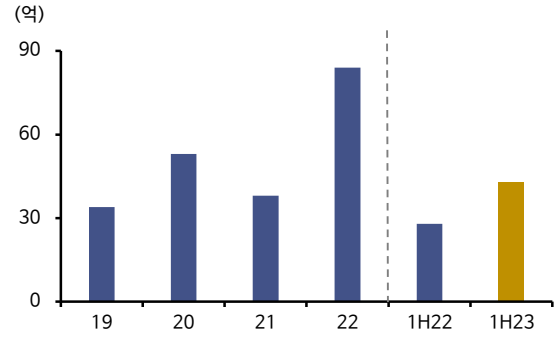
파이오링크의 보안 스위치는 22년 일본에서 84억원의 매출을 기록했다. 19년도에는 일본향 보안스위치 매출이 34억원임을 감안하면 고성장을 지속했음을 알 수 있다. 파이오링크는 2015년 클라우드 기능을 포함한 L2/L3 보안 스위치 TiFront를 출시했다. 2017년 하반기부터 일본에서 TiFront를 선보이며 빠르게 시장 점유율을 확대했다.

일본의 정보보안 시장 규모는 11조원으로 2017년 이후 연평균 9%이상의 성장률을 유지했다. 2022년 도요타 생산 공장이 해킹 되며 14개의 생산 공장이 중단되는 등 대규모 해킹 사태가 발생하며 보안에 대한 사회적 인식이 증가하고 있다. 2018년 사이버보안법 개정, 2022년 개인정보보호법 개정안 시행 등으로 제도적인 움직임도 나타나며, 일본 내 정보보안 수요는 지속 증가하고 있다.

그러나 정보보안 수요 증가와 달리 일본의 IT 인력은 태부족 상태다. 일본 내 대형 이직 사이트에 의하면 일본 기업들의 53%가 IT 인재 구인난을 겪고 있다고 답했다. 파이오링크의 보안 스위치는 통합 IT 자산 관리, 원격제어 서비스를 제공해 기존 스위치와 달리 별도의 IT 기술자를 필요로하지 않는다.

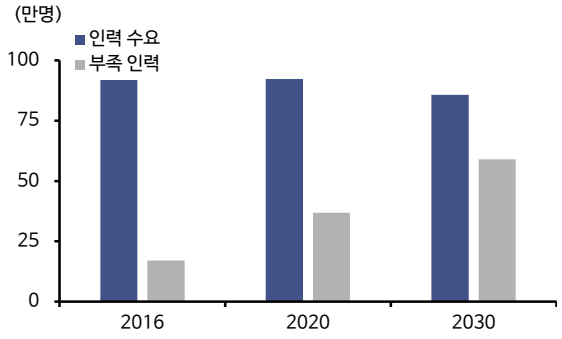
보안 스위치 단가가 1,300만원을 상회하며 기존 스위치에 비해 고가에 판매되고 있으나, 일본 IT 기술자 연봉 하한선이 8,000만원 이상인 것을 감안하면 가격경쟁력이 있다고 판단한다. 현재 클라우드 스위치 등으로 스위치 품목을 다변화하고 있으며 파트너사도 증가하고 있어 일본 내 보안 스위치 매출은 지속 성장할 것으로 기대한다. 23년 상반기 일본향 보안스위치 매출은 43억원을 기록했다. 하반기에 매출 쏠림 현상이 있는 것을 감안했을 때 지난해 일본 수출 매출인 84억원을 상회하는 매출을 기록할 전망이다.

일본 내 보안스위치 매출



자료: 회사 자료, 신한투자증권

일본 IT 업계 인력수요 및 부족 인력 추이



자료: Statista, 신한투자증권

홈네트워크 보안 시장 진출, 월패드 해킹 방지

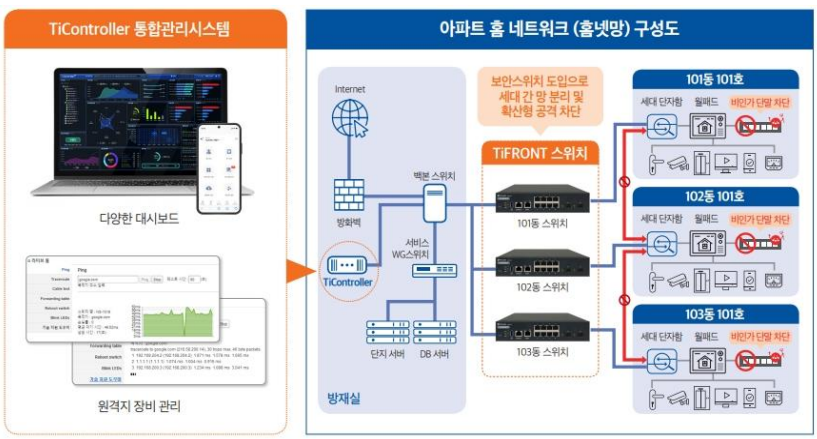
파이오링크는 보안스위치를 통해 홈네트워크 보안 시장에 진출하겠다고 밝혔다. 2021년 8월부터 12월까지 전국에 있는 638개의 아파트에서 약 40만 개의 월패드를 해킹해 몰래 촬영한 영상과 사진이 유출됐다. 아파트의 중앙 서버로 침입해 개별 가구에 악성 앱을 설치하여 불법 촬영이 진행됐다. 월패드 해킹 사건 이후 홈네트워크 보안의 중요성이 대두되며, 세대간 망 분리를 의무화하는 '지능형 홈네트워크 설비 및 기술기준' 개정이 지난해부터 시행됐다.

파이오링크의 보안스위치를 통해 정부 정책을 준수하며, 안전한 홈 네트워크와 안정적인 망 관리를 실현할 수 있다. 세대 간 망분리를 포함해 홈 네트워크 위협에 대비한 다양한 보안 기능 및 비인가 단말 차단, 전용 관리 솔루션을 통해 신속하게 장애에 대응할 수 있다. 파이오링크의 보안 스위치는 VLAN 기능을 통해 세대 간 통신을 차단하는 망 분리 환경을 제공한다.

아파트를 건설하는 입장에서도 네트워크 구성을 변경하거나, 고가의 전용 장비 도입을 하지 않아도 파이오링크의 보안 스위치를 통해 망분리 정책 준수가 가능하다. 또한 기존 홈 네트워크를 구성하는 스위치를 보안스위치로 변경하는 것 만으로도 망 분리가 가능해 기존 아파트에서는 노후 스위치 교체만으로도 신축 아파트와 같은 보안 효과를 누릴 수 있다.

세대간 망 분리 의무화는 지난해 하반기부터 시행되어, 새로 짓는 아파트에 대해서만 적용되고 있다. 보안스위치는 보안기능 확인서와 CC인증을 모두 획득하여 '세대 간 망 분리 정책' 준수에 적합한 제품임을 확인받았다. 다른 망 분리 솔루션과 비교하더라도 비용 대비 효율적이고 도입이 쉬워 제품의 장점을 살려 신규 아파트를 대상으로 적극적인 영업을 진행 중이다. 네트워크 공사는 완공 시점에 진행되기 때문에 2024년에 완공되는 아파트들에 대해 매출이 발생할 예정이다.

보안 스위치를 통한 세대간 망분리 구상도



자료: 회사 자료, 신한투자증권

III. 실적전망

2023년 영업이익 140억원(+22.6% YoY) 전망

2023년 매출액 705억원(+14.4% YoY), 영업이익 140억원(+22.6% YoY)을 전망한다. 상대적으로 이익률이 높은 ADC, 보안스위치 매출이 상승하며 영업 이익률 개선이 예상된다. 일본향 보안스위치 매출 증가, 동남아 등 신규 지역 진출로 매출액도 함께 증가할 전망이다.

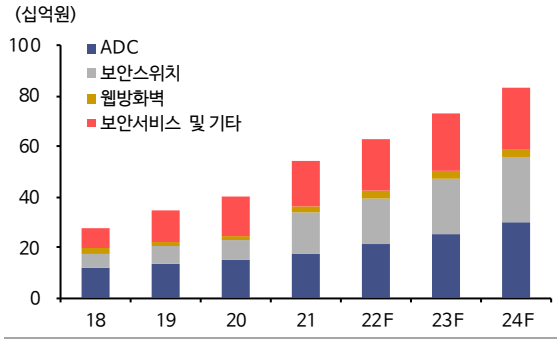
최근 보안 컨설팅부터 구축, 운영까지 원스톱으로 지원하는 HCI 제품을 출시했다. HCI는 통합된 형태로 서버 인프라가 구성되어 있어 전력사용, 유지보수 비용 절약이 가능하다. HCI 제품 매출은 2024년 이후부터 가시화 될 것으로 기대된다. 전방시장인 보안산업의 성장과 함께, 데이터센터 증설 및 세대간 망 분리 정책 등 다양한 모멘텀을 보유하고 있어 꾸준한 실적 우상향이 기대된다. 2024F PER은 5.3배로 동종 산업 대비 저평가 되어 있어 주목이 필요한 시점이다.

연간 영업 실적 추이 및 전망

(십억원, %)	2020	2021	2022	2023F	2024F	2025F
매출액	39.8	54.3	61.6	70.5	81.1	92.3
ADC	14.8	17.3	23.0	29.9	35.2	42.4
보안스위치	8.1	16.7	17.9	19.1	23.2	26.2
웹방화벽	1.6	2.4	2.5	2.9	3.1	3.1
보안서비스/기타	15.4	17.9	18.2	18.6	19.6	20.6
영업이익	6.5	10.9	11.4	14.0	16.8	19.7
순이익	10.7	11.2	12.1	14.1	17.0	19.6
영업이익률	16.4	20.1	18.5	19.8	20.7	21.3
순이익률	26.8	20.6	19.7	20.0	21.0	21.2
성장률(YoY)						
매출액	13.4	36.4	13.4	14.4	15.0	13.8
영업이익	57.1	67.8	4.2	22.6	20.0	17.2

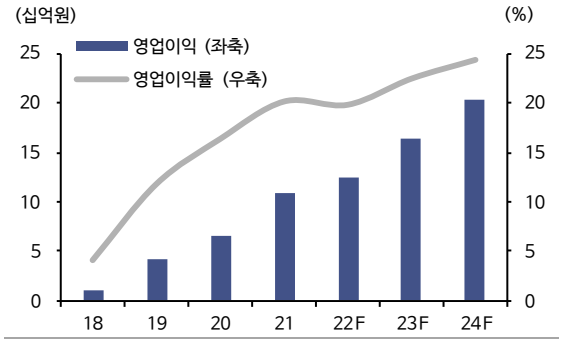
자료: 회사 자료, 신한투자증권 추정

부문별 매출액 추이 및 전망



자료: 회사 자료, 신한투자증권 추정

영업이익 추이 및 전망



자료: 회사 자료, 신한투자증권 추정

재무상태표

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
자산총계	83.8	94.7	109.9	128.6	149.8
유동자산	60.2	75.2	89.0	105.8	124.7
현금및현금성자산	23.1	25.0	31.6	39.8	49.6
매출채권	13.6	15.2	17.3	19.9	22.7
재고자산	5.2	9.9	11.4	13.1	14.9
비유동자산	23.6	19.6	20.9	22.7	25.0
유형자산	7.8	7.9	8.4	9.0	9.8
무형자산	1.9	1.8	1.6	1.6	1.5
투자자산	9.0	6.0	7.1	8.4	9.9
기타금융업자산	0.0	0.0	0.0	0.0	0.0
부채총계	21.9	22.2	25.3	29.0	32.9
유동부채	10.5	10.9	12.4	14.3	16.3
단기차입금	0.0	0.0	0.0	0.0	0.0
매입채무	3.4	2.2	2.5	2.9	3.3
유동성장기부채	0.0	0.0	0.0	0.0	0.0
비유동부채	11.3	11.3	12.9	14.7	16.7
사채	0.0	0.0	0.0	0.0	0.0
장기차입금(장기금융부채 포함)	0.4	0.5	0.5	0.5	0.5
기타금융업부채	0.0	0.0	0.0	0.0	0.0
자본총계	61.9	72.6	84.6	99.5	116.8
자본금	3.4	3.4	3.4	3.4	3.4
자본잉여금	28.3	28.3	28.3	28.3	28.3
기타자본	(1.3)	(1.3)	(1.3)	(1.3)	(1.3)
기타포괄이익누계액	(0.4)	(1.4)	(1.4)	(1.4)	(1.4)
이익잉여금	31.9	43.6	55.7	70.6	87.9
지배주주지분	61.9	72.6	84.6	99.5	116.8
비지배주주지분	0.0	0.0	0.0	0.0	0.0
*총차입금	0.7	0.9	0.9	1.0	1.0
*순차입금(순현금)	(37.5)	(45.9)	(55.6)	(67.4)	(81.1)

포괄손익계산서

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
매출액	54.3	61.6	70.5	81.1	92.3
증가율 (%)	36.4	13.4	14.4	15.0	13.8
매출원가	27.0	31.4	35.2	39.8	44.8
매출총이익	27.3	30.2	35.3	41.3	47.5
매출총이익률 (%)	50.3	49.1	50.1	50.9	51.5
판매관리비	16.4	18.8	21.3	24.5	27.8
영업이익	10.9	11.4	14.0	16.8	19.7
증가율 (%)	67.9	4.2	22.6	20.0	17.2
영업이익률 (%)	20.1	18.5	19.8	20.7	21.3
영업외손익	1.2	1.9	2.2	2.7	3.1
금융손익	0.8	0.7	1.3	1.4	1.5
기타영업외손익	0.1	1.2	1.0	1.4	1.7
종속 및 관계기업관련손익	0.3	0.0	0.0	0.0	0.0
세전계속사업이익	12.1	13.3	16.2	19.5	22.8
법인세비용	0.9	1.1	2.1	2.4	3.2
계속사업이익	11.2	12.1	14.1	17.0	19.6
중단사업이익	0.0	0.0	0.0	0.0	0.0
당기순이익	11.2	12.1	14.1	17.0	19.6
증가율 (%)	4.6	8.7	15.9	21.1	15.0
순이익률 (%)	20.6	19.7	20.0	21.0	21.2
(지배주주) 당기순이익	11.2	12.1	14.1	17.0	19.6
(비지배주주) 당기순이익	0.0	0.0	0.0	0.0	0.0
총포괄이익	10.9	12.3	14.1	17.0	19.6
(지배주주) 총포괄이익	10.9	12.3	14.1	17.0	19.6
(비지배주주) 총포괄이익	0.0	0.0	0.0	0.0	0.0
EBITDA	12.4	12.8	16.2	19.3	22.1
증가율 (%)	56.9	3.1	26.6	19.0	14.9
EBITDA 이익률 (%)	22.8	20.7	23.0	23.7	24.0

현금흐름표

12월 결산 (십억원)	2021	2022	2023F	2024F	2025F
영업활동으로인한현금흐름	11.5	8.8	15.8	18.3	20.4
당기순이익	11.2	12.1	14.1	17.0	19.6
유형자산상각비	1.0	1.2	2.1	2.4	2.4
무형자산상각비	0.4	0.2	0.1	0.1	0.0
외화환산손실(이익)	0.1	0.3	0.0	0.0	0.0
자산처분손실(이익)	(0.3)	(0.1)	(0.0)	(0.0)	(0.0)
지분법, 종속, 관계기업손실(이익)	(0.3)	(1.0)	(0.8)	(1.2)	(1.5)
운전자본변동	(3.0)	(7.0)	0.4	0.0	(0.1)
(법인세납부)	(0.2)	(0.4)	(2.1)	(2.4)	(3.2)
기타	2.6	3.5	2.0	2.4	3.2
투자활동으로인한현금흐름	(11.5)	(4.6)	(6.6)	(8.0)	(8.7)
유형자산의증가(CAPEX)	(1.1)	(0.8)	(2.5)	(3.0)	(3.2)
유형자산의감소	0.0	0.0	0.0	0.0	0.0
무형자산의감소(증가)	0.0	(0.0)	0.0	(0.0)	0.0
투자자산의감소(증가)	0.0	4.0	(1.1)	(1.3)	(1.6)
기타	(10.4)	(7.8)	(3.0)	(3.7)	(3.9)
FCF	7.5	5.3	9.2	11.0	12.9
재무활동으로인한현금흐름	(1.3)	(2.0)	(2.0)	(1.9)	(2.1)
차입금의 증가(감소)	0.0	0.0	0.0	0.1	0.1
자기주식의처분(취득)	0.0	0.0	0.0	0.0	0.0
배당금	(1.0)	(1.7)	(2.0)	(2.0)	(2.1)
기타	(0.3)	(0.3)	0.0	0.0	(0.1)
기타현금흐름	0.0	0.0	(0.6)	(0.2)	0.1
연결범위변동으로인한현금의증가	0.0	0.0	0.0	0.0	0.0
환율변동효과	(0.1)	(0.3)	0.0	0.0	0.0
현금의증가(감소)	(1.5)	1.9	6.6	8.3	9.7
기초현금	24.6	23.1	25.0	31.6	39.8
기말현금	23.1	25.0	31.6	39.8	49.6

자료: 회사 자료, 신한투자증권

주요 투자지표

12월 결산	2021	2022	2023F	2024F	2025F
EPS (당기순이익, 원)	1,629	1,771	2,054	2,486	2,861
EPS (지배순이익, 원)	1,629	1,771	2,054	2,486	2,861
BPS (자본총계 원)	9,030	10,583	12,344	14,519	17,039
BPS (지배자본 원)	9,030	10,583	12,344	14,519	17,039
DPS (원)	250	300	300	320	350
PER (당기순이익 배)	10.8	6.8	6.5	5.3	4.6
PER (지배순이익 배)	10.8	6.8	6.5	5.3	4.6
PBR (자본총계 배)	2.0	1.1	1.1	0.9	0.8
PBR (지배자본 배)	2.0	1.1	1.1	0.9	0.8
EV/EBITDA (배)	6.7	2.9	2.2	1.2	0.5
배당성향 (%)	15.0	16.5	14.2	12.5	11.9
배당수익률 (%)	1.4	2.5	2.3	2.4	2.6
수익성					
EBITDA 이익률 (%)	22.8	20.7	23.0	23.7	24.0
영업이익률 (%)	20.1	18.5	19.8	20.7	21.3
순이익률 (%)	20.6	19.7	20.0	21.0	21.2
ROA (%)	14.5	13.6	13.8	14.3	14.1
ROE (지배순이익, %)	19.6	18.1	17.9	18.5	18.1
ROIC (%)	51.1	45.4	41.3	44.9	46.2
안정성					
부채비율 (%)	35.3	30.6	29.9	29.1	28.2
순차입금비율 (%)	(60.6)	(63.2)	(65.6)	(67.7)	(69.4)
현금비율 (%)	219.6	230.3	254.8	278.8	305.2
이자보상배율 (배)	325.2	263.4	284.6	348.1	408.5
활동성					
순운전자본회전율 (회)	4.9	4.0	3.6	3.6	3.6
재고자산회수기간 (일)	31.3	44.9	55.1	55.0	55.3
매출채권회수기간 (일)	83.2	85.3	84.1	83.9	84.3

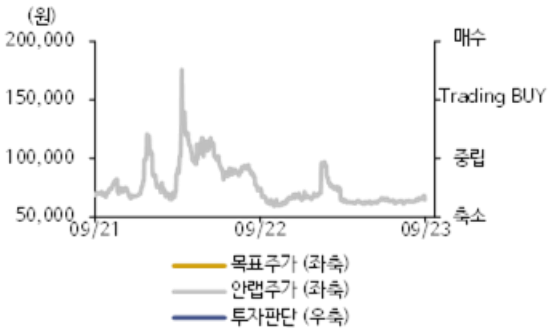
자료: 회사 자료, 신한투자증권

투자의견 및 목표주가 추이

지니언스 (263860)

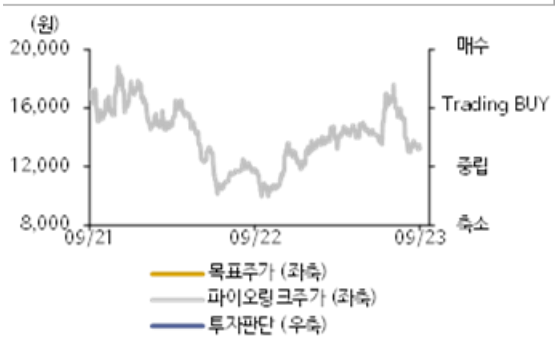
일자	투자 의견	목표 주가 (원)	괴리율 (%) 평균	괴리율 (%) 최고/최저
2023년 09월 18일	매수	18,000		

안랩(053800)



일자	투자 의견	목표 주가 (원)	괴리율 (%) 평균	괴리율 (%) 최고/최저

파이오링크(170790)



일자	투자 의견	목표 주가 (원)	괴리율 (%) 평균	괴리율 (%) 최고/최저

Compliance Notice

- 이 자료에 게재된 내용들은 본인의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭없이 작성되었음을 확인합니다.(작성자: 백지우)
- 자료 제공일 현재 당사는 지난 1년간 상기 회사의 최초 증권시장 상장시 대표 주관사로 참여한 적이 없습니다.
- 자료 공표일 현재 당사는 상기 회사의 주식 등을 1% 이상 보유하고 있지 않습니다.
- 자료제공일 현재 조사분석 담당자는 상기 회사가 발행한 주식 및 주식관련사채에 대하여 규정상 고지하여야 할 재산적 이해관계가 없으며, 추천의견을 제시함에 있어 어떠한 금전적 보상과도 연계되어 있지 않습니다.
- 당 자료는 상기 회사 및 상기 회사의 유가증권에 대한 조사분석담당자의 의견을 정확히 반영하고 있으나 이는 자료제공일 현재 시점에서의 의견 및 추정치로서 실적치와 오차가 발생할 수 있으며, 투자를 유도할 목적이 아니라 투자자의 투자판단에 참고가 되는 정보제공을 목적으로 하고 있습니다. 따라서 종목의 선택이나 투자의 최종결정은 투자자 자신의 판단으로 하시기 바랍니다.
- 본 조사분석자료는 당사 고객에 한하여 배포되는 자료로 어떠한 경우에도 당사의 허락 없이 복사, 대여, 재배포 될 수 없습니다.

투자등급 (2017년 4월 1일부터 적용)

종목	◆ 매수 : 향후 6개월 수익률이 +10% 이상 ◆ Trading BUY : 향후 6개월 수익률이 -10% ~ +10% ◆ 중립 : 향후 6개월 수익률이 -10% ~ -20% ◆ 축소 : 향후 6개월 수익률이 -20% 이하	섹터	◆ 비중확대 : 업종내 커버리지 업체들의 투자의견이 시가총액 기준으로 매수 비중이 높을 경우 ◆ 중립 : 업종내 커버리지 업체들의 투자의견이 시가총액 기준으로 중립적일 경우 ◆ 축소 : 업종내 커버리지 업체들의 투자의견이 시가총액 기준으로 Reduce가 우세한 경우

신한투자증권 유니버스 투자등급 비율 (2023년 9월 12일 기준)

매수 (매수)	93.03%	Trading BUY (중립)	4.51%	중립 (중립)	2.46%	축소 (매도)	0.00%