

# 사이버 보안, AI와의 동행



Global Equity Analyst

심지현

☎ (02) 3772-3174

✉ simjin@shinhan.com

## 보안 S/W는 발전 초기

24년 낙관의 이유:

- 1) AI, 새로운 공격 방식
- 2) 보안 예산의 증대
- 3) 클라우드 환경 전환

주요 업체:

클라우드스트라이크

## AI는 사이버 보안의 수요도 증대

사이버 보안은 방어자와 공격자가 서로를 이기기 위해 노력하기 때문에 빠른 속도로 혁신의 피드백 루프가 이어진다. 즉 공격 방식이 기술 발전에 빠르게 발맞춰 변화하기 때문에 산업 지형의 변화도 크게 이루어지는 편이다. 특히 2023년 AI가 시장에 소개됨에 따라 사이버 공격 및 보안에도 새로운 지평이 열린 상황이다. 따라서 보안 소프트웨어는 여전히 발전의 초기 단계에 있다. 반면 사이버 보안 관련주의 주가는 2022년 가파르게 하락한 후 2023년에 기대만큼의 상승폭을 보여주지 못했다. 금리 우려와 시장의 빠른 변화 그리고 경쟁 강도 때문이다. 그러나 2024년에는 다음의 이유로 산업의 수요, 테마 반등에 대해 낙관한다.

## 새로운 공격에는 새로운 보안이 필요

1) AI의 등장은 새로운 공격 방식을 가능하게 하여 사이버 보안의 수요를 비약적으로 증가시킨다. 2) 보안은 IT 예산 내에서 가장 방어적으로 운영되는 지출 항목으로, 다른 주요 IT 아젠다를 제치고 가장 중요하게 다뤄진다. 보안 총괄자의 37%는 향후 5년 내 보안 예산을 25% 이상 증액할 계획이다. 3) AI 등장 이전 클라우드 작업 환경으로의 전환이 이미 사이버 보안 산업을 크게 변화시키고 있었다. 특히 사이버 환경 내 데이터 규모가 기하급수적으로 증가함에 따라 데이터 보안, 나아가 이를 관리해야 하는 클라우드 기반의 보안 중요도가 커지고 있다.

## 여섯 가지 분류: 클라우드/엔드포인트 보안 주목

보안 시장은 1세대 레거시 형태인 온프레미스부터 시작해 2세대 리프트 앤 시프트 단계를 거쳐 3단계 클라우드 네이티브 형태로 나아가고 있다. 이 흐름 하에 주력 영역에 따라 다시 크게 여섯 가지로 분류할 수 있다. 1) 애플리케이션, 2) 데이터, 4) 아이덴티티, 5) 네트워크, 5) 인프라/엔드포인트, 6) 보안 운영이 그것이다. 기술 영역에 어떤 테마가 부상하는지, 그리고 어떤 사이버 공격이 주목받는지에 따라 시기별로 다른 영역의 보안이 주목받는 경향이 있으며, 최근 떠오르는 부문은 클라우드 보안과 엔드포인트 보안(EDR) 보안이다.

## 클라우드스트라이크(CRWD): EDR 강자

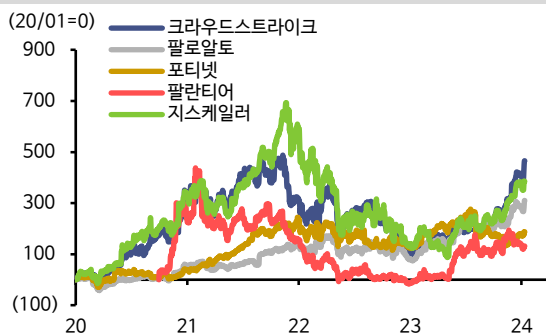
클라우드스트라이크는 EDR 보안의 대표 사업자로, EDR 업계 최초로 클라우드 보안을 접목해 단말기 내 모든 행위를 분석해 새로운 공격 유형에 대응한다. 대표적 서비스는 보안 플랫폼 ‘팔콘’으로, 플랫폼에 더 많은 데이터가 유입될수록 알고리즘 훈련에 사용되는 데이터 규모가 늘어나 네트워크 효과를 누린다. 동사는 1) 매출총이익률 및 ARR이 꾸준히 늘어나고, 2) 경쟁사 대비 공격적 R&D를 집행하고 있으며, 3) 기록적 파이프라인을 획득해 경쟁사와 격차를 넓히고 있다.

## 2024년의 대표 기대 테마, 사이버 보안

### 3가지 투자포인트

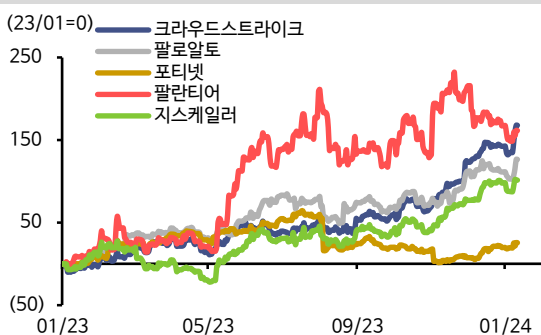
사이버보안 테마가 강세다. 2022년 긴 하락세를 거친 후 2023년 전반에 걸쳐 AI 테마와 함께 전반적으로 반등한 바 있지만 금리 우려 때문에 다수 업체들의 상단이 다소 제한되어 아쉬운 바 있었다. 또한 공격 방식이 기술 발전에 발맞춰 변화함에 따라 신생 업체가 계속해서 등장하고 있어, 최근 몇 년간 여러 차례의 인수 거래에도 불구하고 보안 시장은 여전히 잘게 쪼개져있고 경쟁 강도가 높다. 그럼에도 불구하고 산업의 장기 수요 전망을 여전히 낙관하는 가운데 2024년에 테마의 본격 상승을 기대하는 이유는 다음과 같다.

사이버보안 관련주 상대주가 추이(20년~)



자료: 신한투자증권

사이버보안 관련주 상대주가 추이(23년~)



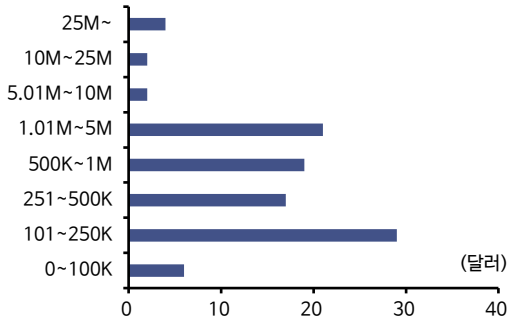
자료: 신한투자증권

- 1) AI로 신규 공격 수단
- 2) 보안 예산, 가장 중요
- 3) 클라우드 전환 수요

1) AI의 등장은 사이버 보안의 수요를 비약적으로 증가시킨다. 작년부터 사이버 공격의 증가, 특히 대중의 이목을 크게 끌거나 여러 기업에 이전과는 다른 규모의 피해를 입히는 종류의 공격이 크게 늘어나고 있다(ex. Log4j, solarwinds 침해 사고). 특히 AI의 등장과 함께 기존에는 방법에 있어서 자원이나 시간의 한계가 있어 시행하지 못했던 공격도 가능하게 되었기 때문에 다양하고 새로운 솔루션에 대한 수요도 크게 늘고있으며 이에 따라 신생 업체도 계속해서 생겨나고 있다. 즉, 사이버보안은 S/W에서 가장 중점적으로 다뤄지는 문제 중 하나다.

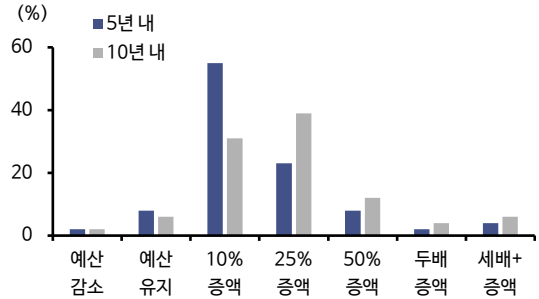
2) 보안은 IT 예산 내에서 가장 보수적으로 운용되는(방어 가능한) 지출 영역이다. 500인 이상 조직 내 60개 이상의 CSO(보안 총괄)를 대상으로 설문결과를 실시한 결과 약 30%가 타사 보안에 백만달러 이상을 지불하고 있으며, 약 25%는 향후 10년간 보안 예산을 50% 이상 늘릴 예정이다. 게다가 많은 기업들의 경영진은 AI가 중요하고 큰 기회가 될 것이라는 사실을 2023년을 거치며 이미 인지했지만 실제로 어떤 식으로 적용해야 하고 리스크에 대비해야 하는지는 아직 잘 알지 못하는 것 같다. 사이버보안도 마찬가지로, AI가 재편하는 소프트웨어 3.0 및 그 이후의 세계에서는 보안의 필수성이 더욱더 강조가 될 것이다.

### 제 3자 보안 밴드에 지출하는 예산 규모



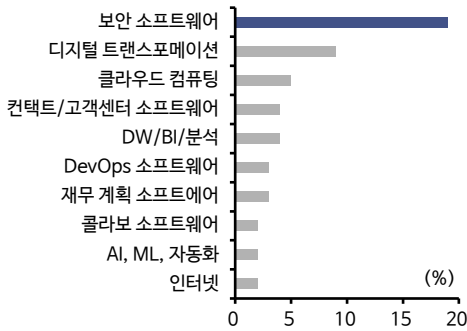
자료: Cloudinrastructure, 신한투자증권

### 보안 예산의 증가폭 예상



자료: Cloudinrastructure, 신한투자증권

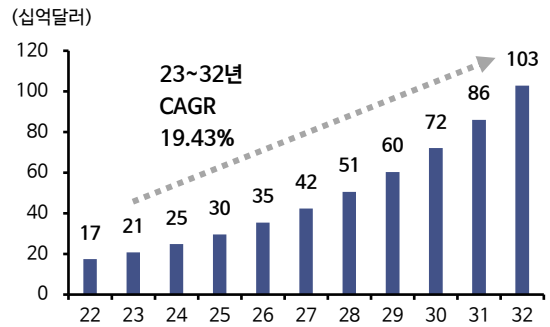
### IT 프로젝트 중 예산 삭감의 가능성이 적은 부문



자료: Morgan Stanley, 신한투자증권

주: 4Q22 CSO 서베이, Most likely와 Lease likely의 Net 수치

### 사이버보안 분야의 AI 시장 규모 예측

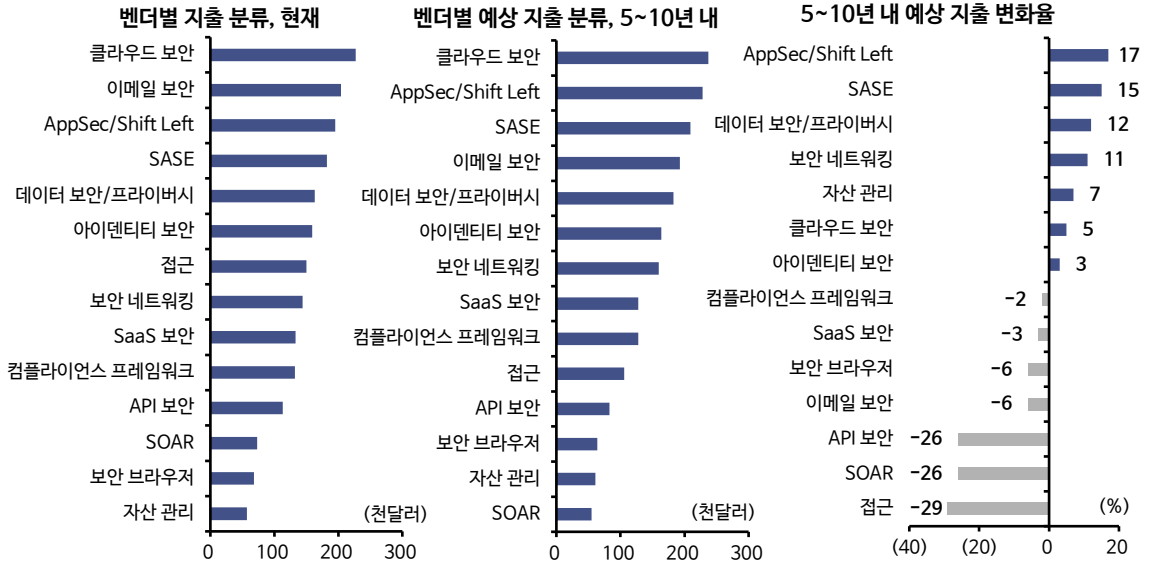


자료: Precedence Research, 신한투자증권

3) AI 등장 이전 클라우드 작업 환경으로의 전환이 이미 사이버보안 산업을 크게 변화시키기 시작했다. 클라우드 도입의 증가는 보안 방식부터 적용 범위까지 일정 수준의 공백을 만든다. 기존 기업의 네트워크에서 일반적으로 적용되는 보안 정책을 클라우드 환경에서는 적용할 수 없거나 쉽게 우회할 수 있기 때문이다. 연구에 따르면 5년 후에는 전체 기업의 4분의 1이 거의 모든 보안 워크로드를 클라우드에서 처리할 것으로 나타나기도 했다.

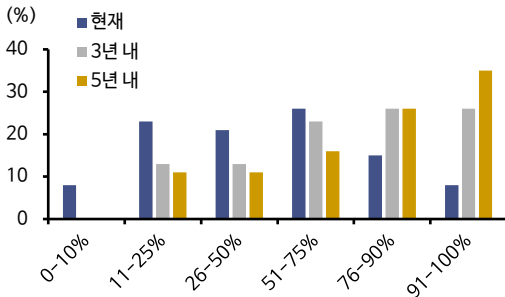
같은 맥락에서 데이터 보안 역시 점점 중요해지고 있다. 각 기업이 다루는 데이터가 빅데이터, 머신러닝(ML), AI 등에 따라 폭발적으로 증가함에 따라 기업들은 새로운 데이터 인프라에 더 의존하게 되거나 새로운 클라우드 데이터 스택을 채택하고 있다. 글로벌 빅데이터 지출은 2021년 1,630억달러에서 2029년 3,670억달러로 CAGR 12.3%에 달할 것으로 예상된다. 이러한 지출을 뒷받침하는 것은 클라우드 기반 스토리지로의 급격한 전환(ex. 스노우플레이크, 데이터브릭스, S3 등)이었으며, AI의 등장으로 데이터의 규모가 더 기하급수적으로 늘어나며 이를 관리해야 하는 클라우드 기반의 보안 역시 중요도가 커지고 있다.

## 보안 스택 전반에 따른 예산 지출



자료: Redpoint, 신한투자증권

## 향후 클라우드에 있을 것으로 추정되는 데이터 비중



자료: Redpoint, 신한투자증권

## 사이버 보안의 주요 구분

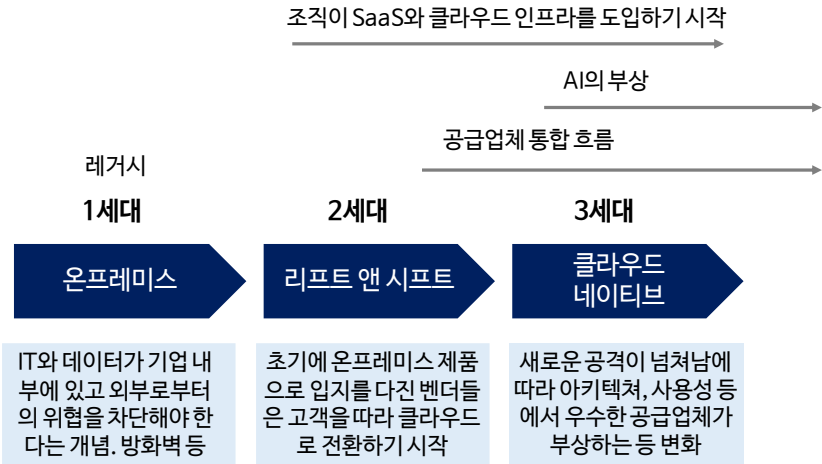
구분	규모 및 CAGR	주요 종목
네트워크 보안	~20bn, ~10% CAGR	팔로알토, 포티넷, 지스케일러, 클라우드플레어
엔드포인트 보안	~16bn, ~20% CAGR	마이크로소프트, 시큐리티윈, 크라우드스트라이크
보안 관리	~14bn, ~15% CAGR	마이크로소프트, 옥타, 사이버아크
클라우드	<1bn, ~50% CAGR	지스케일러, 팔로알토, 클라우드플레어

자료: Gartner, IDC, SPEAR Invest, 신한투자증권

## 사이버 보안의 주요 트렌드

사이버 보안은 방어자와 공격자가 서로를 이기기 위해 필사적으로 시간과 자원을 쏟기 때문에 빠른 속도로 혁신의 피드백 루프가 이어지는 독특한 구조의 산업이다. 특히 상기 기술했듯 기술의 발전에 따라 계속해서 새로운 대응을 필요로 하는데, 공격 범주의 확장(클라우드, 원격 근무, SaaS 도입, 분산 시스템 등)과 공격의 폭과 깊이(자동화를 활용한 공격 규모 확대 또는 표적 공격 전략) 모두 점점 더 커지고 있음이 특징이다. 이는 오늘날 전 세계적으로 보안에 약 2천억달러가 지출되고 있음에도 불구하고 계속 사고가 발생하는 이유를 설명한다. 따라서 보안 소프트웨어는 여전히 발전의 초기 단계에 있다.

## 사이버 보안 시장의 발전



자료: 신한투자증권

보안 시장의 분류는 여러 형태가 가능하지만 크게 여섯 가지로 나눌 수 있다. 각각의 구분과 시장별 주요 업체는 다음과 같다. 1) 애플리케이션(시놉시스, 클라우드플레어, SNYK 등), 2) 데이터(Cyera 등), 3) 아이덴티티(사이버아크, auth0, 옥타 등), 4) 네트워크(시스코, 포티넷, 체크포인트, 주피터, 클라우드플레어, 팔로알토, 지스케일러 등), 5) 인프라/엔드포인트(클라우드스트라이크, 팔로알토, 센티넬원, 위즈 등), 6) 보안운영(데이터독, Splunk, 주피터원 등).

### 사일로 문제: 통합은 업계의 핵심 과제

팬데믹 이후 생겨난 많은 신생 보안업체들의 통합과 기존 업체들의 서비스 통합이 지속되고 있지만 분산된 보안 서비스는 여전히 업계가 해결해야 할 주요 과제 중 하나로 남아있다. 이러한 분산된 형태를 'Silo'라고 부른다. 기술의 발전 속도가 특정 회사가 자리잡는 속도보다 빠르기 때문에 생겨나는 현상이다.

연구에 따르면 78%의 기업이 보안 문제를 해결하기 위해 50개 이상의 개별 사이버 보안 제품을 사용하고 있으며, 37%는 100개 이상의 사이버 보안 제품을 사용하고 있다. 특히 기업들이 비즈니스 워크로드를 클라우드로 이전하면서 IT팀과 클라우드 서비스 제공업체가 데이터 보안에 대한 책임소재를 파악하는 과정에서 사각지대가 생겨나고 있다. 현재 거의 90%의 기업이 서비스형 소프트웨어(SaaS)를, 76%의 기업이 서비스형 인프라(IaaS)를 사용하고 있으며, 50%는 향후 2년 내에 모든 데이터를 클라우드로 이전할 것으로 예상하고 있다.













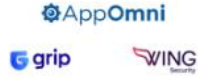

이에 따라 많은 주요 사이버보안 업체는 자신들의 플랫폼 하에서 고객이 보안 기능을 통합할 수 있도록 하는데 집중한다. 가령 클라우드스트라이크의 경우 최근 분기에서 8개 이상의 모듈이 포함된 거래가 78% YoY 증가하며, 계속해서 통합을 동사의 핵심 아젠다로 가져가고 있다.

## 사이버 보안 시장의 지형

	GEN I: "ON-PREM"	GEN II: "LIFT & SHIFT"	GEN III: "EMERGING CLOUD-NATIVE"
APPLICATION	BLACKDUCK <sup>®</sup> imperva <sup>®</sup> SYNOPSYS <sup>®</sup>	Checkmarx CLOUDFLARE MEND sonar <sup>®</sup> VERACODE <sup>®</sup>	Cheunguard <sup>®</sup> DAZZ <sup>®</sup> ENDOR LABS <sup>®</sup> GitGuardian <sup>®</sup> OLEGIT <sup>®</sup> Semgrep <sup>®</sup> STACKHAWK <sup>®</sup> snyk <sup>®</sup>
DATA	Forcepoint <sup>®</sup> mimecast <sup>®</sup> proofpoint <sup>®</sup> VARONIS <sup>®</sup>	BigID <sup>®</sup> COHESITY <sup>®</sup> rubrik <sup>®</sup> OneTrust <sup>®</sup>	Abnormal <sup>®</sup> cyera <sup>®</sup> Dig <sup>®</sup> HYCU <sup>®</sup> Normalizer <sup>®</sup> Owni{backup} <sup>®</sup> privacera <sup>®</sup> veza <sup>®</sup>
IDENTITY	BeyondTrust <sup>®</sup> CYBERARK <sup>®</sup> imprivata <sup>®</sup> SailPoint <sup>®</sup>	auth0 <sup>®</sup> feedzai <sup>®</sup> ForgeRock <sup>®</sup> okta <sup>®</sup> PingIdentity <sup>®</sup>	clerk <sup>®</sup> descopie <sup>®</sup> jumpcloud <sup>®</sup> Opal <sup>®</sup> ORY <sup>®</sup> oso <sup>®</sup> SILVERFORT <sup>®</sup> STYTCH <sup>®</sup>
NETWORK	CHECK POINT <sup>®</sup> CISCO <sup>®</sup> FORTINET <sup>®</sup> JUNIPER <sup>®</sup>	CLOUDFLARE <sup>®</sup> netskope <sup>®</sup> paloalto <sup>®</sup> zscaler <sup>®</sup> wandera <sup>®</sup>	DOPE SECURITY <sup>®</sup> ngrok <sup>®</sup> tailscale <sup>®</sup> Teleport <sup>®</sup> Twingate <sup>®</sup>
INFRASTRUCTURE / ENDPOINT	McAfee <sup>®</sup> Symantec <sup>®</sup>	CROWDSTRIKE <sup>®</sup> paloalto <sup>®</sup> SentinelOne <sup>®</sup>	HUNTRESS <sup>®</sup> uptycs <sup>®</sup> orca security <sup>®</sup> LACEWORK <sup>®</sup> Stairwell <sup>®</sup> WIZ <sup>®</sup>
SECURITY OPERATIONS	ArcSight <sup>®</sup> Secureworks <sup>®</sup>	DATADOG <sup>®</sup> exabeam <sup>®</sup> splunk <sup>®</sup> sumo logic <sup>®</sup>	ARCTIC WOLF <sup>®</sup> Coralogix <sup>®</sup> eXeI <sup>®</sup> HUNTERS <sup>®</sup> JupiterOne <sup>®</sup> panther <sup>®</sup> redcanary <sup>®</sup> torq <sup>®</sup>

자료: Sapphire, 신한투자증권

## 보안 환경의 초기 성장 구도 (스타트업 분류)

AppSec / Shift Left		Cloud Security
		
Secure Networking	SASE	Asset Management
		
Secure Browsers	Identity Orchestration	Access
		
Email Security	API Security	SOARs / Automation
		
Compliance Frameworks	SaaS Security	Data Security + Privacy
		

자료: Redpoint, 신한투자증권

## 클라우드스트라이크

## 시장 주도권 굳히기 구간

Ticker

CRWD.US

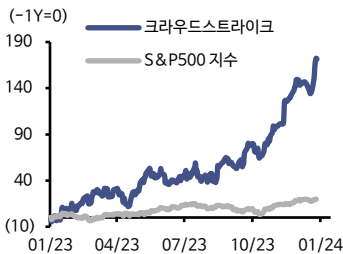
현재가 (1월 16일, 달러)	286.3
최고 목표가 (달러)	330.0
최저 목표가 (달러)	172.0
평균 목표가 (달러)	272.1

심지현

✉ simjin@shinhan.com

S&P500 지수 (pt)	4,766.0
시가총액 (조원)	92.0
유동주식비율 (%)	97.4
52 주 최고가 (달러)	290.2
52 주 최저가 (달러)	97.3
주요주주 (%)	
Vanguard Group, Inc.	5.78
BlackRock International	4.06
절대수익률 (%)	
3개월	52.5
6개월	91.6
12개월	187.6
S&P500 대비 상대수익률 (%)	
3개월	43.6
6개월	85.8
12개월	168.5

### 주가차트



### 엔드포인트 보안 부문의 대표 사업자

클라우드 스트라이크는 EDR(Endpoint Detection and Response, 엔드포인트 탐지 및 대응) 보안 부문의 대표 사업자다. 엔드포인트란 네트워크 끝에 연결된 PC나 모바일 등의 디바이스를 의미한다. 대표적 서비스는 보안 플랫폼 ‘팔콘’으로, 플랫폼에 더 많은 데이터가 유입될수록 그에 맞는 대응을 모든 고객에게 적용 가능해 네트워크 효과를 창출한다. 특히 팔콘은 모듈과 엔드포인트를 쉽게 확장할 수 있다.

### ARR, GPM, 파이프라인 모두 기록적 수준

1) 당사는 대부분의 매출을 구독에서 얻고있기 때문에 보다 예측 가능하고 반복적인 비즈니스 구조를 가지고 있으며, 선제 수익지표의 향후 1년간 추정치가 높게 잡혀있다. 특히 지난 분기 기준 순 신규 ARR은 13%로 가속되며 네트워크 효과를 계속 확장해나가고 있다는 점이 특징이다. 2) 향후 실적에서 가장 주목할 점은 구독 부문에 대한 매출총이익률로, 최근 몇분기간은 약 78%대를 유지하고 있다(GAAP 기준, Non-GAAP 기준으로 80%). 목표 수준은 82~85%다.

3) 특히 매출총이익률이 꾸준히 늘어나는 가운데 타 경쟁사 대비 공격적인 R&D 투자를 단행하고 있어 플랫폼의 강력한 수요를 증명한다. 또한 최근 분기에 다수의 대체 및 확장계약을 체결하여 기록적 파이프라인을 확보하고 있다. 특히 기존 경쟁사 외에도 마이크로소프트 같은 대형사를 상대로도 강점을 드러내는 점이 장기적 매력을 더한다.

### 산업 전반의 수요 확장 + 수익성 확대 수혜

2024년 외형 성장이 주목되는 사이버보안 시장 내에서도 클라우드/엔드포인트 보안을 특히 주목한다. 당사의 12M FWD는 70배 근처로 최근 주가 상승을 통해 밸류에이션이 다소 높아진 상태나, 주가는 2022년 말 고점 수준을 갓 회복한 상태다. 경쟁사 대비 높은 FCF 마진을 보유해 향후 실적 구체화에 따른 이익 추가 상향을 충분히 기대한다.

1월 결산	매출액 (백만달러)	증가율 (%)	영업이익 (백만달러)	영업이익률 (%)	순이익 (백만달러)	EPS (달러)	증가율 (%)	PER (배)	EV/EBITDA (배)	PBR (배)	ROE (%)
2022	1,452	66.0	(143)	(9.8)	(235)	(1.03)	적지	-	-	58.1	16.9
2023	2,241	54.4	(190)	(8.5)	(183)	(0.79)	적지	-	-	45.8	29.6
2024F	3,049	36.1	635	20.8	717	2.95	흑전	97.0	87.4	30.6	32.3
2025F	3,932	29.0	879	22.4	922	3.73		76.8	64.3	21.9	28.4
2026F	4,920	25.1	1,159	23.6	1,169	4.66		61.4	48.7	16.2	26.5

자료: Bloomberg, 신한투자증권 / 주: Non-GAAP 기준



대표적인 EDR 사업자  
최초로 클라우드 접목  
데이터 네트워크 효과

## 클라우드스트라이크(CRWD)

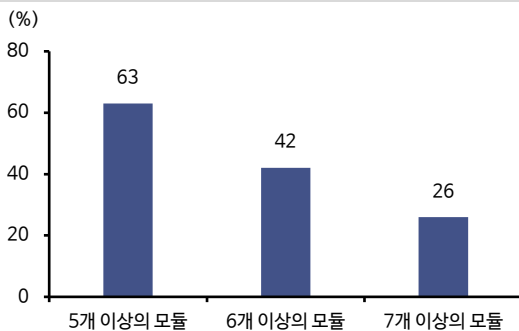
### EDR 대표 사업자 & 클라우드 보안의 초기 진입자

클라우드 스트라이크는 EDR(Endpoint Detection and Response, 엔드포인트 탐지 및 대응) 보안 분야의 대표 사업자다. 엔드포인트란 네트워크 끝에 연결된 PC나 모바일 등의 디바이스를 의미한다. EDR 업계 최초로 클라우드 보안을 접목해 단 말기 내 모든 행위를 분석해 새로운 공격 유형에 대해서 유연하게 대처 가능하다. 대표적 서비스는 보안 플랫폼 ‘팔콘’으로, 플랫폼에 더 많은 데이터가 유입될 수록 그에 맞는 대응을 모든 고객에게 적용 가능해 네트워크 효과를 창출한다. 즉 회사의 Security Cloud에 신규 고객이 추가될 때마다 플랫폼에 더 많은 데이터가 제공되고 이는 다시 알고리즘을 훈련시키는데 사용된다.

특히 클라우드스트라이크의 팔콘은 차세대 안티바이러스, EDR, 디바이스 제어 등 다양한 부문을 처리하는 클라우드 모듈을 통합해, 여러 제품으로 분열된 보안 서비스를 사용하는 고객을 통합된 클라우드 모듈로 모을 수 있다. 고객은 팔콘 플랫폼을 사용할 때 원하는 수의 클라우드 모듈로 시작해 모듈을 쉽게 추가할 수 있고, 엔드포인트가 늘어날 경우 이 역시 추가하는 식으로 확장할 수 있다.

수익 대부분이 구독 형태며, 구독은 다시 구독 고객 수, 고객당 엔드포인트 수, 구독에 포함된 클라우드 모듈 수에 의해 결정된다. 팔콘은 23개의 클라우드 모듈로 구성되어 있으며 고객은 이를 5개의 번들로 구매하도록 선택할 수 있다. 수익 구조상 고객이 플랫폼에서 더 많은 모듈을 구매할수록 플랫폼의 알고리즘에 더 많은 기여를 하게되며, 다른 서비스로 전환하는데 더 많은 비용이 들게된다. 이는 동사의 역사적으로 높은 총 유지율(GRR)을 설명한다.

멀티 클라우드 모듈 구독자의 모듈 수 비중



자료: 회사 자료, 신한투자증권

장기 재무 목표(Non-GAAP 기준, 매출 대비)

기준	목표
구독 매출총이익률	82~85%
S&M(영업 및 마케팅비)	28~33%
R&D(연구개발비)	15~20%
G&A(일반관리비)	5~7%
영업이익률	28~32%
FCF	34~38%

자료: 회사 자료, 신한투자증권

### ARR과 매출총이익률의 상승

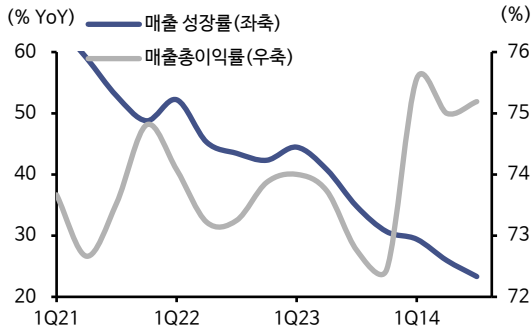
매출 성장률은 초기만큼 가파르지는 않으나 1) 매출총이익률이 꾸준히 늘어나고, 2) 보다 예측 가능하고 반복적인 매출 구조를 가지고 있으며, 3) 선제 수익 지표로 볼 수 있는 Billings, Backlog의 향후 1년간 추정치가 높다는 점에서 동사의 견조한 펀더멘털을 가늠할 수 있다.



지난 분기 기준 순 신규 ARR은 13%로 가속되며 네트워크 효과를 계속 확장해 나가고 있다. ARR은 주로 구독형 매출 구조를 가지고 있는 회사의 주요 지표로 사용되는데, 연간 단위로 계산되는 회사 구독의 예측 가능하고 반복적인 구성 요소, 즉 기존 고객으로부터 기대되는 안정적인 수익 흐름을 나타낸다. 한편 매출 백로그는 SaaS 또는 구독 계약 기간 동안의 매출 일정 부분에서 미인식된 매출의 합계다. 여기에는 비반복 서비스에 대한 수익이 모두 포함될 수도 있다.

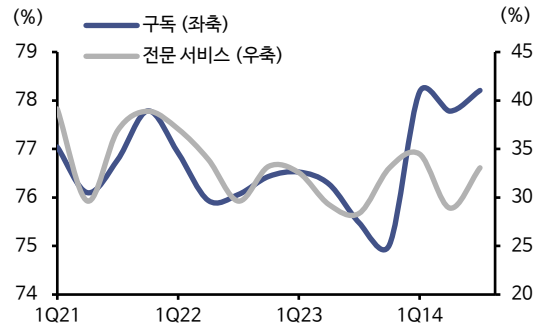
향후 실적에서 가장 주목할 점은 구독 부문에 대한 매출총이익률로, 최근 몇분기 간은 약 78%대를 유지하고 있다(GAAP 기준, Non-GAAP 기준으로 80%). 목표 수준은 82~85%로, 동사의 가장 큰 운영 비용인 영업 및 마케팅(S&M)에서 꾸준히 비용을 낮추고 있다. 종합하자면 산업 전반의 수요 확장과 함께 외형 성장 잠재력을 풍부히 보유하면서도 수익성이 성장하고 있는 점이 매력적이다.

### 분기 실적 추이



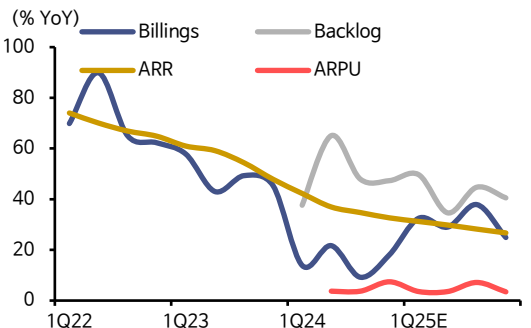
자료: 회사 자료, 신한투자증권

### 부문별 매출총이익률



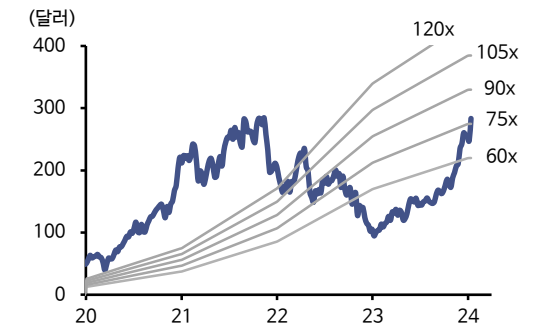
자료: 회사 자료, 신한투자증권

### 주요 지표 컨센서스 추이



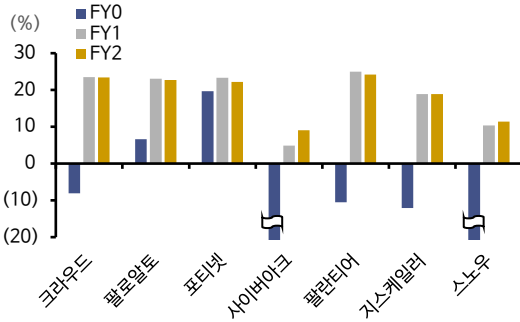
자료: 회사 자료, 신한투자증권

### 12개월 선행 PER 밴드 차트



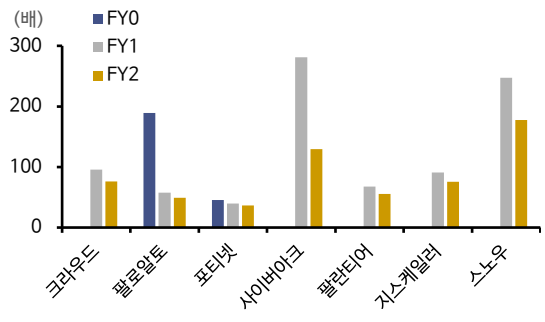
자료: Refinitive, 신한투자증권

### 사이버보안 주요 업체 순이익률 비교



자료: Bloomberg, 신한투자증권

### 사이버보안 주요 업체 PER 비교



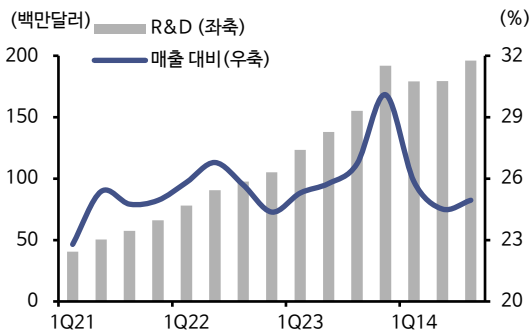
자료: Bloomberg, 신한투자증권

### 경쟁사간의 격차 확대: R&D 투자와 대체 계약

클라우드스트라이크의 또 한가지 강점은 타 경쟁사들이 대체로 R&D 투자 비용을 소극적으로 운용하고 있는 대신 동사는 수익성을 확대하면서도 공격적인 투자를 단행하고 있다는 점이다. 다수의 사이버보안 업체가 기업들이 보안 예산을 면밀하게 검토하고 있는 등 매크로 환경의 리스크가 여전히 잔존한 상태지만, 동사는 플랫폼의 강력한 수요와 이에 따른 기록적 파이프라인을 확보하고 있다.

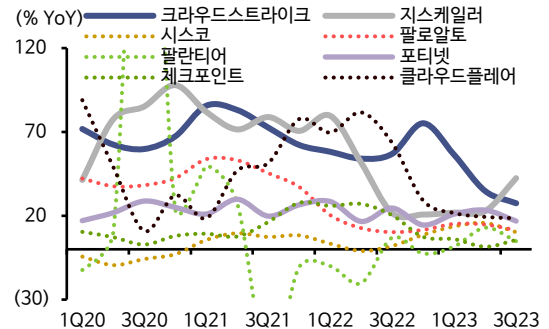
가령 3분기에 팔콘은 숙박업 분야에서 기존 마이크로소프트를 대체한 몇천만달러 규모의 계약을 체결했다. 또한 대형 엔터프라이즈 SaaS 제공업체 중 한 곳과 몇백만달러대 규모의 보안 확장 계약을 통해 기존의 여러 포인트 제품을 대체했으며, 주요 의류 브랜드와 몇백만달러대 규모의 보안 확장 계약을 맺으며 방화벽 하드웨어 공급업체의 클라우드 보안을 대체했다. 이는 앞서 언급한 사이버 보안의 주요 과제인 통합 문제에서 클라우드스트라이크가 진일보하고 있다는 것을 보여준다. 특히 기존 경쟁사들 뿐만 아니라 마이크로소프트 같은 확고한 대형사를 상대로도 강점을 드러내고 있다는 점이 장기적 매력을 더한다.

### 클라우드스트라이크 R&D 지출 추이



자료: 신한투자증권

### 주요 사이버보안 업체 R&D 비용 증감 추이



자료: 신한투자증권

## Compliance Notice

- ◆ 이 자료에 게재된 내용들은 본인의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭없이 작성되었음을 확인합니다(작성자: 심지현).
- ◆ 본 자료는 과거의 자료를 기초로 한 투자참고 자료로서, 향후 추가 움직임은 과거의 패턴과 다를 수 있습니다.
- ◆ 자료 제공일 현재 당사는 상기 회사가 발행한 주식을 1% 이상 보유하고 있지 않습니다.
- ◆ 자료 제공일 현재 당사는 지난 1년간 상기 회사의 최초 증권시장 상장시 대표 주관사로 참여한 적이 없습니다.
- ◆ 자료제공일 현재 조사분석 담당자는 상기회사가 발행한 주식 및 주식관련사채에 대하여 규정상 고지하여야 할 재산적 이해관계가 없으며, 추천의견을 제시함에 있어 어떠한 금전적 보상과도 연계되어 있지 않습니다.
- ◆ 당자료는 상기 회사 및 상기회사의 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 허락없이 복사, 대여, 재배포될 수 없습니다.