다보링크

Investor Relations

Disclaimer

본 자료는 투자자들을 위한 정보 제공을 목적으로 주식회사 다보링크(이하 “회사”)에 의해 작성되었습니다.

본 자료에 포함된 주식회사 다보링크의 경영실적 및 재무성과와 관련된 모든 정보는 한국채택회계기준에 따라 작성되었습니다.

본 자료에 포함된 “예측정보”는 개별 확인 절차를 거치지 않은 정보들입니다. 이는 과거가 아닌 미래의 사건과 관계된 사항으로 회사의 향후 예상되는 경영현황 및 재무실적을 의미하고, 표현상으로는 ‘예상’, ‘전망’, ‘계획’, ‘기대’, ‘(E)’ 등과 같은 단어를 포함합니다.

위 “예측정보”는 향후 경영환경의 변화 등에 따라 영향을 받으며, 본질적으로 불확실성을 내포하고 있는바, 이러한 불확실성으로 인하여 실제 미래 실적은 “예측정보”에 기재되거나 암시된 내용과 중대한 차이가 발생할 수 있습니다.

또한, 향후 전망은 현재 시장상황과 회사의 경영방향 등을 고려한 것으로, 향후 시장환경의 변화와 전략수정 등에 따라 별도의 고지 없이 변경될 수 있음을 양지하시기 바랍니다.

본 자료의 활용과 관련하여 발생하는 손실에 대하여 회사 및 회사의 임직원들은 과실 및 기타의 경우 포함하여 그 어떠한 책임도 부담하지 않음을 알려드립니다.

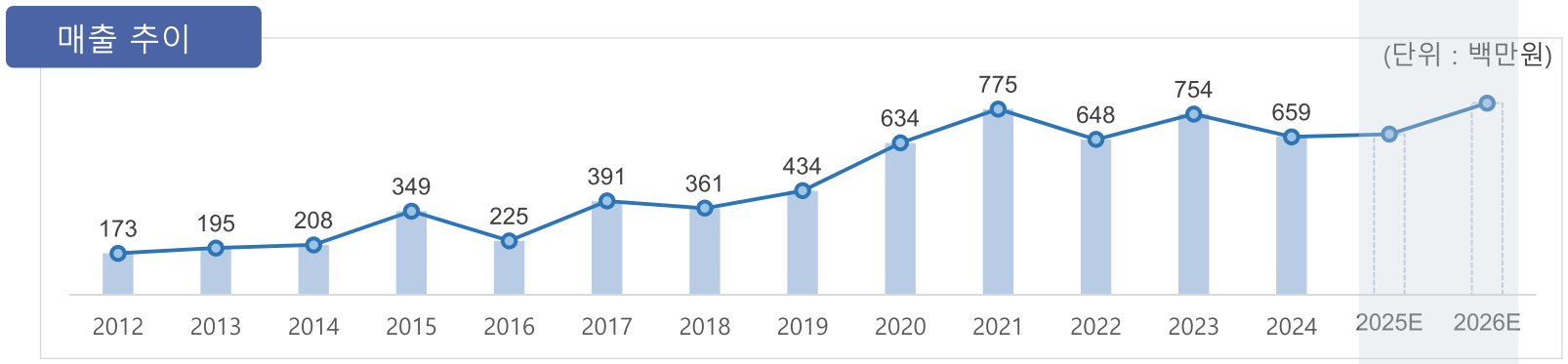
본 문서는 주식의 매매를 위한 권유를 구성하지 아니하며 문서의 그 어느 부분도 관련 계약 및 약정 또는 투자 결정을 위한 기초 또는 근거가 될 수 없음을 알려드립니다.

본 자료는 비영리 목적으로 내용 변경 없이 사용이 가능하고(단, 출처표시 필수), 회사의 사전 승인 없이 내용이 변경된 자료의 무단 배포 및 복제는 법적인 제재를 받을 수 있음을 유념해 주시기 바랍니다.

DAVOLINK

Corporate Identity_성장스토리

주식회사 다보링크는 **뛰어난 RnD 역량을 바탕으로** "Wi-Fi 토탈 솔루션 전문기업 " 으로 성장해 왔습니다.
→ **기존사업의 안정성을 기반**으로 미래 성장성을 담보할 수 있는 **신규사업**도 활발하게 검토 중에 있습니다.



Corporate Identity_기업역량

다보링크의 기술력 및 제품은 국내의 통신사업자에게 인정받고 있으며, 최대 4천대 AP를 관리하는 Enterprise AP Controller를 국내최초로 상용화하여 그 영역을 확장해 가고 있습니다.

- 국내통신3사의 1차협력사로 제품공급
- **국내 최초 기업용 와이파이 솔루션개발**
- **국내 최초 와이파이6E인증 제품 출시**
- 생산EMS업체와 장기간신뢰 구축

- **AP컨트롤러 S/W 100%자체 개발**
- 외부연구기관 기술협력 신기술 R&D진행
- **20년 이상** 와이파이 제어 S/W기술축적
- 해외 R&D센터 구축을 통한 백업기능충족 및 사내능력 보강

- **제품 H/W 자체개발 능력보유**
- R&D를 위한 무선 성능측정 계측장비 보유
- 임직원의 50%이상 개발관련 엔지니어 유지(시험인력 포함)

- 풍부한 A/S 지원 경험을 바탕으로 고객관리
- 지역 및 프로젝트별 협력사 구축 및 운영

Business Model_주요고객사

다보링크 & Partners

통신사

LG U+ | kt | SK broadband | LG HelloVision

솔루션 고객

서울 중랑구 Jungnang-gu | 강원도 | 영덕군 Yeongdeok-Gun | 청/송/군 CHEONGSONG COUNTY | 서울특별시 상수도사업본부

국립현대미술관 National Museum of Modern and Contemporary Art, Korea | 대구성서산업단지관리공단 | KERIS 한국교육학술정보원 | 경 찰 병 원 NATIONAL POLICE HOSPITAL | 고려대학교구로병원 KOREA UNIVERSITY GURO HOSPITAL

RAMADA SONGDO | Value Hotel Worldwide Seogwipo JS | 서울특별시교육청 | 경기도교육청 GYEONGGIDO OFFICE OF EDUCATION | 충청남도교육청

전라북도교육청 JEOLLABUKDO OFFICE OF EDUCATION | 고려대학교 KOREA UNIVERSITY | 상명대학교 SANGMYUNG UNIVERSITY | 한양여자대학교 | 한국외국어대학교

서울이태원초등학교 SEOUL ITAEWON ELEMENTARY SCHOOL | 상계고등학교 SANGGYE HIGH SCHOOL | 상패초등학교 | 보령중학교

구매 고객

Qualcomm | REALTEK | audiocodes | BROADCOM

ODM Partner

T&W | zioncom

Appendix_다양한 디자인 및 기술역량

다보링크 제품이 가진 경쟁력은 아래와 같습니다.

다양한 제품 구성

가정용 AP		기업용 AP	AP Controller	Home Gateway
 GAPD-7500	 DV02-012H	 DVW-624i	 SC-240	 HGWD-1GR
 DVW-G500	 DVW-2700L	 DVW-624o	 SC-2000A	

기술적 역량

01 가격경쟁력
경쟁업체 동일장비 대비

02 국내최초 국산화
국내최초 국산화 AP Controller (핵심원천기술보유)

03 제품설계 역량
자체 H/W,S/W개발 및 검증부서 운영

04 Wi-Fi 6/7
매년 장비투자 및 선행개발진행

→ **핵심 경쟁력**

Appendix_산업현황 (국가간 기술/보안 이슈 강화)

티피링크: 미국 내 65%의 시장 점유율을 차지 (제공제품: 와이파이7, 주요고객: 버라이즌, 월마트)

美공화 의원들, 中 와이파이 공유기 'TP링크' 판매 금지 촉구

기사입력 : 2025년05월15일 11:19 | 최종수정 : 2025년05월15일 11:19

가 + 가 - 프린트

[서울=뉴스핌] 최원진 기자= 미국 공화당 의원들이 14일(현지시간) 전 세계 판매량 1위인 중국 와이파이(Wi-Fi) 공유기 제조업체 TP링크(TP-Link)에 대해 미국 내 장비 판매를 금지해야 한다고 촉구했다.

블룸버그 통신에 따르면 아칸소주 공화당 상원의원 톰 코튼을 포함한 상·하원 의원 17명은 하워드 러트닉 미 상무장관 앞으로 보낸 서한에서 TP링크를 "명백하고 현존하는 위협(clear and present danger)"으로 규정하며, 판매 금지를 요구했다.

이들은 TP링크가 중국 공산당과 긴밀한 관계를 맺고 있다면서, 이 회사의 와이파이 라우터를 포함한 네트워크 장비가 중국 정보기관의 사이버 공격에 활용된 정황이 있다는 언론 보도 등을 그 근거로 제시했다.

서한에는 "우리가 조치를 미루는 하루하루가 중국 공산당의 승리이며, 미국 경쟁 기업은 고통받고 국가 안보는 계속 위협받는다"고 적혔다.

TP링크는 중국 선전에 본사를 둔 글로벌 네트워크 장비 제조업체로, 전 세계 가정용 와이파이 공유기 시장에서 1위를 차지하고 있다. 미국과 유럽 등 주요 시장에도 진출해 있다.

지난달 24일 블룸버그는 미 법무부가 TP링크의 가격 정책을 둘러싼 반독점법 위반 여부에 대해 수사 중이라고 보도한 바 있다.

美, '해킹 우려' 中 TP링크 조사…"라우터 판매 금지 검토"

이혜인 기자

입력 2024.12.19 09:34 수정 2024.12.19 09:42 가가

"사이버 보안에 취약하다" 지적 잇달아
中 "국가안보 구실로 중국 기업 억누르려는 조치"

미국 정부가 중국 기업 TP링크의 미국 내 판매 금지를 검토하고 있다. 중국의 사이버 공격에 이용될 수있다는 우려에서다.

19일 월스트리트저널(WSJ) 보도에 따르면 미 상무부, 국방부, 법무부가 중국 라우터 제조업체 TP링크를 합동 조사하고 있다. 다음 달 출범하는 트럼프 2기 행정부에서 TP링크에 대한 판매 금지 조치를 내릴 가능성이 높다는 설명이다.

Appendix_산업현황 (미 국방부 보안 강화 지침)

미 국방부 (DoD: Department of Defense)는 2025년 7월 18일 보안 프로토콜 강화 지침을 발표하였음.

미 국방부 최고정보책임자(CIO)의 명령을 통해서 미국 국방부 산하 정보기술(IT) 및 클라우드 서비스, 하드웨어, 소프트웨어 등 모든 정보기술 역량에 대해 중국과 러시아 등 적대국의 공격을 대비해서 보안 검증 절차를 강화하는 것을 목표로 함.

이 명령으로 인해서 미국 국방부 관련 제품 및 서비스 공급망에서 향후 외국 정부 또는 적대세력의 영향력이 있는 하드웨어/소프트웨어는 조달하지 못하고, 악성 코드나 취약점이 포함될 위험이 있는 제품의 도입이 금지됨.

SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUL 18 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJ: Enhancing Security Protocols for the Department of Defense

I direct the Department of Defense (DoD) Chief Information Officer (CIO), in coordination with the Under Secretaries of Defense for Acquisition and Sustainment, Intelligence and Security, and Research and Engineering, to take immediate actions to ensure to the maximum extent possible that all information technology capabilities, including cloud services, developed and procured for DoD are reviewed and validated as secure against supply chain attacks by adversaries such as China and Russia.

The DoD will not procure any hardware or software susceptible to adversarial foreign influence that presents risk to mission accomplishment and must prevent such adversaries from introducing malicious capabilities into the products and services that are utilized by the Department. To that end, the Department will fortify existing programs and processes utilized within the Defense Industrial Base (DIB) to ensure that adversarial foreign influence is appropriately eliminated or mitigated and determine what, if any, additional actions may be required to address these risks. Specifically, the DoD CIO will leverage efforts such as the Cybersecurity Maturity Model Certification, the Software Fast Track Program, the Authority to Operate process, the Federal Risk and Authorization Management Program, and initiatives such as the Secure Software Development Framework. Moreover, the Under Secretary of Defense for Intelligence and Security will review and validate personnel security practices and insider threat programs of the DIB and cloud service providers to the maximum extent possible.

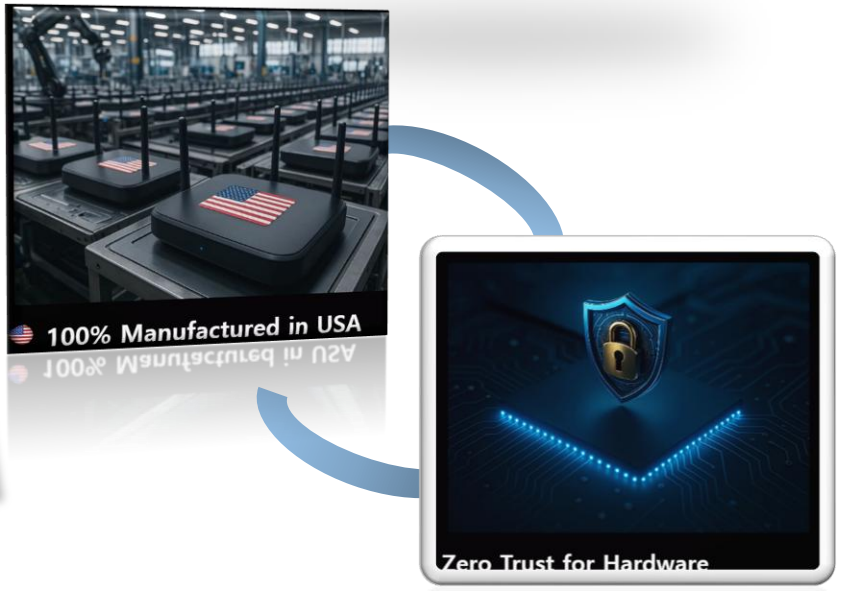
I direct the DoD CIO to issue additional implementing guidance within 15 days of the date of this memorandum to achieve and maintain a secure environment for our warfighters. My point of contact in this matter is David McKeown, david.w.mckeown.civ@mail.mil, 703-695-8705.

Business Model_Zero Trust AP Router Project (추진배경)

DAVOLINK

국가	내용	내용
미국	제로트러스트 표준화	2020년 8월 국립표준기술연구소(NIST)는 '제로트러스트 아키텍처(ZTA) 표
	행정명령을 통한 제로트러스트 전략 채택	2021년 5월 바이든 대통령은 '국가 사이버보안 개선을 위한 행정명령'을 통해 제로트러스트 전략 채택을 발표
	제로트러스트 성숙도 모델 발표	• 2021년 6월 사이버보안 및 인프라 보안청(CISA)은 '제로트러스트 성숙도 모델 1.0'을 발간 • 2023년 4월 '제로트러스트 성숙도 모델 2.0' 발간
싱가폴	제로트러스트 도입 원칙 발표	2021년 10월 싱가포르 사이버보안 전략 2021에서 사이버 보안 현대화 전략으로 제로트러스트 도입 원칙을 발표
영국	제로트러스트 아키텍처 설계 원칙 발표	2021년 7월 제로트러스트 아키텍처 설계 원칙(Zero trust architecture design principles v1.0)을 발표
일본	제로트러스트 적용 정책 발표	2022년 6월 제로트러스트 아키텍처 적용 정책(ゼロトラストアーキテクチャ適用方針)을 발표
한국	한국 제로트러스트포럼 발족	2022년 10월 과학기술정보통신부에서 제로트러스트 도입에 대해 논의하기 위한 산/학/연 전문가 구성
	디지털플랫폼정부 실현 계획	2023년 4월 대통령 직속 디지털플랫폼정부위원회와 함께 국가적 차원의 제로트러스트 도입 추진계획 발표
	제로트러스트 가이드라인 1.0 발표	2023년 7월 과학기술정보통신부 등에서는 6가지 기본원리, 3가지 핵심원칙의 제로트러스트 가이드라인 1.0 발표
	실증지원 사업 추진	2023년 6월 과학기술정보통신부는 제로트러스트 모델 발굴/확산을 위해 2개 과제 10억원 규모의 실증 지원사업 추진하고 24년도에는 6억원 예산 배정
	사이버안보 민관합동협의체	국가정보원에서는 국가공공 영역에서의 사이버보안 강화를 위한 정책 논의 24년까지 K-제로트러스트 구축 가이드 및 시범 적용 추진

[출처: 국회입법조사처]



Business Model_Zero Trust AP Router Project (타임라인)

DAVOLINK

- 제품생산 & EMS회사 협력 (Fulfillment)
- 제품 개발/생산지원 → 다보링크
- 인증시험 → A사 (미국)
- 제품판매 → F사 (미국)

- Zero Trust / 보안 SW 및 솔루션 제공
- Pods(논리적공간) & 포탈 제작 / 클라우드 제공
- 사업총괄
- 제품판매

- 기존제품 제공 및 보안 S/W 탑재지원
- PoDs & portal product 개발
- 고사양 무선 AP 개발
- JV 생산 협업

- ORION (미 공군 지원 보안인증 프로그램) 승인 프로그램
- 보안기능 점검/테스트
- 군사, 정부 및 민간사업자 고객군 네트워크 형성

상업생산 이후
영업이익 기준

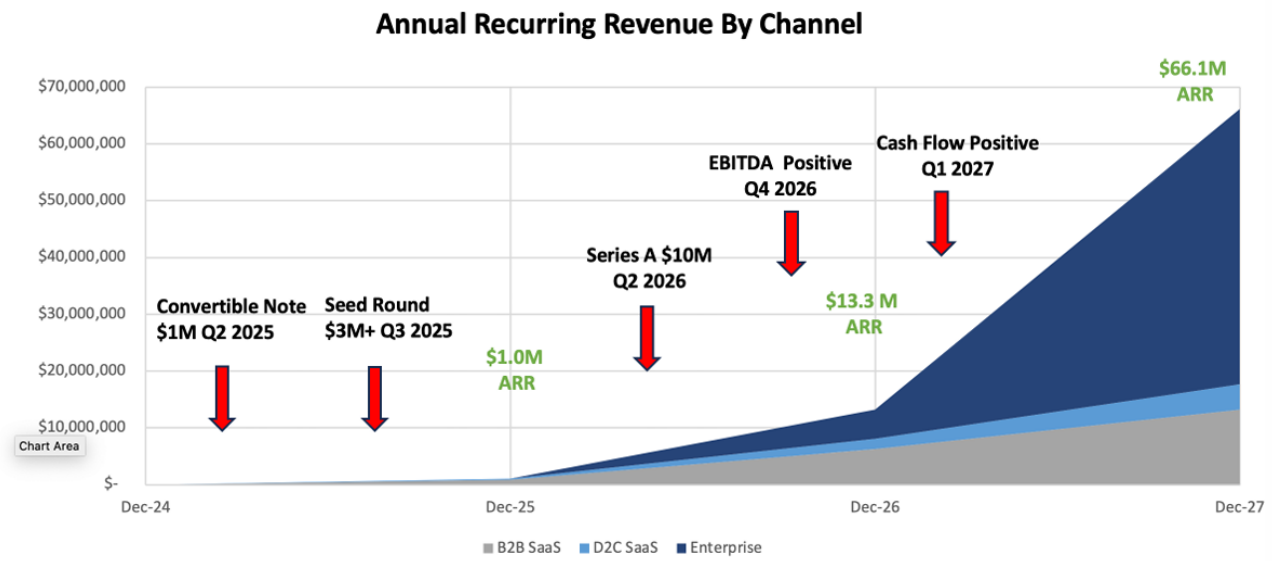
성과배분 Forecast
2026년: 50억
2027년: 100억 + Alpha

Business Model_Zero Trust AP Router Project (예상 매출)

DAVOLINK

	2026	2027	2028	2029	2030
OA Tech 매출목표 :	$ 4M	$ 187M	$ 937M	$ 2.3B	$ 4.6B
예상 제품출하량 :	150K	4.5M	4.75M	9.37M	18.7M
Davolink 매출목표 :	**$ 2.9M**	**$ 13.5M**	**$ 14.3M**	**$ 28M**	**$ 56M**

Our Goal : 20% of market share in the Americas + Europe within 5 years



Faction Networks

DAVOLINK

Faction 구성원

Faction Networks (Faction Communications Operation)는 30년 이상 보안 분야에서 성공적인 업적을 쌓은 이들이 Real Zero Trust 솔루션 개발을 목표로 설립 하였음.

특히 CEO와 CTO를 겸하고 있는 Dave Land는 세계적인 보안 전문회사인 Trend Micro에서 10년 이상 CTO로 근무하면서 전세계 보안 기술과 시장을 주도하였음.

최근 미국내에서 정치 사회적으로 문제가 되고 있는 Cyber Security 이슈를 근본적으로 해결하기 위한 보안 솔루션 사업화를 추진하고 있음.

Experienced Innovators and Operators with Multiple Successful Exits

Dave Rand

Co-Founder, CEO and Chief Technologist

- Cybersecurity and Internet Entrepreneur
- Co-founder & CTO, AboveNet (IPO, $1.7B Sale)
- Founder & CEO, Kelkea, sold to Trend Micro
- CTO, Trend Micro 2007 - 2018

Geoff Halstead

Co-Founder and Chief Product Officer

- Visionary and innovative product leader
- CPO, Circle Security
- CPO, Connexient (Sold to Everbridge)

Dan O'Sullivan

Co-Founder and VP, Business Development

Building early-stage tech startups in Business Development, Sales & Marketing for 30+ years including successful exits at MapInfo, Netegrity, LogMeIn.

Les Wilson

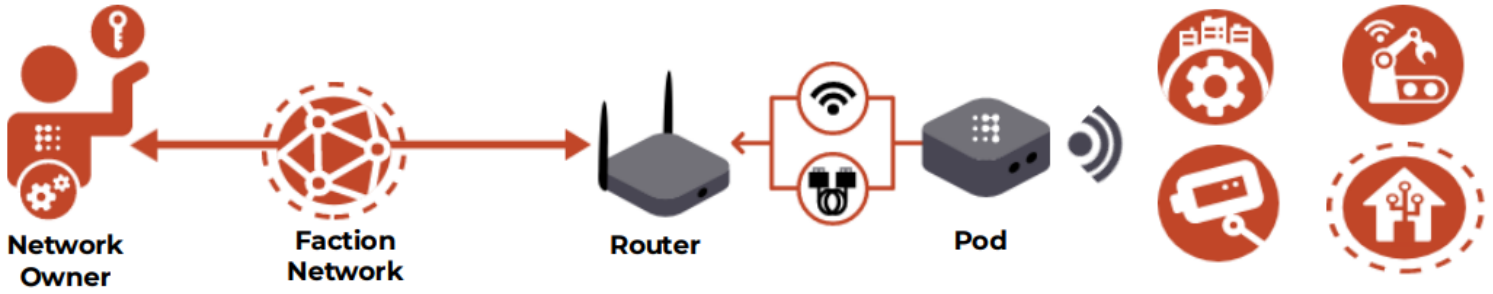
VP, OEM Partnerships

Vast experience, knowledge and success in maximizing growth for both large and early stage companies across Silicon IP, EDA tools, 3D wafer scale semiconductors, communications, industrial, CyberSecurity, IoT and medical markets.

Introduction of Faction Networks (서비스 모델)

DAVOLINK

미국에서 사용되는 다양한 IoT 장치들은 보안에 취약해서 인터넷상 다양한 경로로 해킹 위험에 노출되어 있음.
Faction Networks의 Pod와 Portal 라우터는 CCTV, 프린터, 산업용 장비 등 다양한 IoT 장치들을 Cloud 상 Faction Network로 연결하고 관리함으로써 해킹을 근본적으로 차단함.



Plug & Play

Just plug into your existing router and use the same local password. Nothing changes.

Flexible

Just connect the devices you want to protect. View & manage them in your App.

No Firewall, No Configuration

No firewall needed because your Faction Network is not visible or accessible to the Internet.

Still Cloud Friendly

You can create & manage private Faction tunnels to any device, server or resource on the Internet.