SK 쉴더스

Threat Intelligence Report

EQST INSIGHT

EQST(이큐스트)는 'Experts, Qualified Security Team' 이라는 뜻으로
사이버 위협 분석 및 연구 분야에서 검증된 최고 수준의 보안 전문가 그룹입니다.

2025
09

SK 쉴더스

Contents

Headline

생성형 AI 콘텐츠 진위 검증을 위한 워터마크 기술의 현황

컨설팅사업그룹 기업컨설팅 1 팀 권순철 책임

■ 생성형 AI 의 확산과 긍정적 영향

최근 생성형 인공지능(Generative AI)이 우리 일상과 산업에 빠른 속도로 스며들고 있다. 텍스트 작성, 이미지 생성, 음성 합성, 영상 편집 등 다양하게 활용돼, 인간의 창작 능력을 보완하거나 새로운 가능성을 높이는데 활용되고 있다. 기업은 마케팅 자료, 고객 응대 콘텐츠, 디자인 시안 등을 빠르게 제작해 시간을 절약하고, 개인은 전문 지식이 없이도 수준 높은 결과물을 손쉽게 얻을 수 있게 됐다.

이처럼 생성형 AI 는 생산성 향상과 창의성 증대, 맞춤형 서비스 확대 등 긍정적 효과를 가져오고 있으며, 디지털 전환을 가속화하는 핵심 동력으로 자리매김하고 있다.

■ 악용되는 생성형 AI 콘텐츠

생성형 AI 가 확산되는 만큼 악용 사례 증가도 발생하고 있다. 대표적인 것이 딥페이크(Deepfake) 기술이다. 특정 인물의 얼굴과 음성을 정교하게 합성해 허위 영상이나 음성을 만들어 명예훼손, 사생활 침해, 금융사기 등 사회 전반에 심각한 위협을 끼치고 있다. 실제로 SNS 와 유튜브에는 AI 합성 영상을 활용한 허위 정보 유포 사례가 꾸준히 보고되고 있다.

최근에는 이미지 편집에 특화된 생성형 AI 모델도 속속 등장하고 있다. 구글 딥마인드가 선보인 '나노바나나(Nano Banana)' 역시 큰 화제를 모으고 있다. 이 서비스는 단순한 지시만으로 배경을 변경하거나 인물을 합성하고, 심지어 가상의 의상을 입히는 작업까지 가능하다. 이러한 기능은 편리해 보이지만, 사실상 딥페이크와 유사한 결과물을 만들어낼 수 있어 초상권 침해, 허위 이미지 제작, 불법 합성물 확산으로 이어질 수 있다는 우려를 낳고 있다.

또한 가짜뉴스(Fake news) 전파로 선거 등 정치 영역에서도 문제가 발생하고 있다. 특정 후보자의 발언이나 사진을 불법적으로 조작·합성해 유권자를 혼란에 빠뜨리는 등 민주적 절차에 대한 신뢰를 무너뜨린다. 실제로 국내는 물론 해외에서, 선거 기간 중 딥페이크 영상이 대량 확산되어 사회적 파장을 일으킨 바 있다.

사이버 범죄와 결합하는 양상도 뚜렷하다. 가짜 음성을 활용한 보이스피싱, 위조 문서나 신분증 생성 등은 기존 보안 체계를 위협한다. 여기에 대화형 AI 를 통한 개인정보 및 민감정보 탈취 문제까지 더해지면서 피해 범위는 한층 확장된다. 공격자가 챗봇과의 일상정인 대화 과정에서 유출한 중요한 정보를 활용한다면 맞춤형 피싱 또는 정교한 스팸 공격 설계가 가능하다. 특히 기업 내부에서는 직원이 챗봇에 업무 관련 기밀을 입력할 경우, 영업비밀 유출로 이어질 수도 있다.

마지막으로 저작권 침해 문제 역시 간과할 수 없다. 작가의 화풍을 모방한 이미지 생성이나 음악 패턴을 학습한 결과물은 창작자의 권리를 직접적으로 위협한다. 더 나아가 AI 가 만들어낸 허위 리뷰와 광고 콘텐츠는 소비자 보호와 시장의 공정성을 무너뜨린다.

진짜와 가짜의 경계가 흐려지는 현상은 단순한 기술적 문제를 넘어 사회적 혼란, 법적 분쟁, 국가 안보 위협으로 이어질 수 있다.

■ 생성형 AI 콘텐츠 워터마크의 필요성

앞서 언급했듯이 생성형 AI 가 만들어내는 콘텐츠는 점차 사람들의 일상과 산업 전반으로 확산되는 동시에 위·변조 이미지, 허위 정보, 딥페이크와 같은 심각한 사회적 문제를 유발할 수 있다. 이에 따라 AI 생성물에 워터마크를 적용해 출처를 명확히 하고 위·변조 여부를 검증할 수 있는 기술적 장치의 필요성이 커지고 있다.

2026 년 1 월 국내에서 시행 예정인 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(이하 "AI 기본법")」에서도 합성 영상 및 이미지에 워터마크 삽입을 의무화하는 내용이 포함되어 있다. 또한, 고위험 AI 개념 도입을 통해 인권과 안전 관련 기술에는 강화된 관리와 책임을 부여하는 등 구체적인 컴플라이언스 요구사항이 제시되고 있다. 이는 기술적 대응이 단순한 선택지가 아니라, 기업이 고려해야 할 제도적 흐름과 맞물려 있다는 점을 시사한다. 결국 기업들은 워터마크 도입을 기술적 신뢰 확보 차원을 넘어, 미래 규제 환경을 대비하는 전략적 대응이 마련되어야 한다.

생성물 형태	기업명		상용 서비스 현황	워터마크 유형
이미지	국내	SAMSUNG	갤럭시 AI(갤럭시 스마트폰)	인지 가능
		SK telecom	에이닷(A.)	인지 가능
	국외		Porme AI(AI Tool)	인지 가능
		Meta	AI 챗봇(AI Chatbot)	인지 가능, 인지 불가능
		Adobe	파이어플라이(Firefly)	인지 가능, 인지 불가능
		OpenAI	DALL·E 3	인지 불가능
		Microsoft	코파일럿(Copilot)	인지 불가능
			이미지 크리에이터(Image Creator)	인지 불가능
		Google	제미나이(Gemini)	인지 불가능
동영상	국외		드림 머신(Dream Machine)	인지 가능
		Canva	매직 미디어(Magic Media)	인지 가능
		TikTok	심포니 아바타(Symphony Avatars)	인지 가능
		Meta	무비 젠(Movie Gen)	인지 가능
		DeepMind	비오(Veo)	인지 불가능
오디오	국내	NAVER	클로바 더빙(CLOVA Dubbing)	인지 가능
	국외	OpenAI	보이스 엔진(Voice Engine)	인지 가능
		Azure	AI 음성(AI Speech)	인지 불가능
텍스트	국외	OpenAI	챗GPT(ChatGPT)	인지 불가능
		Google	제미나이(Gemini)	인지 불가능

* 출처 : 한국정보통신기술협회

그림 1. 국내외 인공지능 생성물 워터마크 도입 현황('24.12)

■ 생성형 AI 콘텐츠 워터마크의 유형

기존의 디지털 워터마크는 문서, 이미지나 영상 중심으로 출처를 표시하고 무단 사용을 방지하는 역할을 했다. 이러한 워터마크는 단순한 표시를 넘어, AI 생성물의 출처와 무결성을 확인할 수 있도록 특정 정보를 삽입하는 기술적 장치로 발전하고 있다.

하지만 AI 기반 콘텐츠가 폭발적으로 증가하면서 기존 방식만으로는 생성 출처를 충분히 확인하기 어려워졌다. 이에 따라 텍스트, 이미지, 음성, 영상 등 다양한 AI 생성물의 눈에 보이거나 보이지 않는 정보를 삽입하여 사람이 만든 것인지 AI 가 만든 것인지를 추적하고 식별할 수 있는 생성형 AI 콘텐츠 워터마크가 등장하고 있다.

생성형 AI 워터마크는 눈에 보이는 인지 가능(Visible) 형태와 눈에 보이지 않는 인지 불가능(Invisible) 형태로 구분되며, 목적과 활용 환경에 따라 적절히 적용된다.

유형	설명	장점	단점
인지 가능 워터마크	콘텐츠 위에 눈으로 확인 가능한 표시	출처 확인 용이	시각적 품질 저하, 워터마크 제거에 취약
인지 불가능 워터마크	콘텐츠에 디지털 신호나 메타데이터(C2PA 표준 등) 등으로 삽입되어 눈에는 보이지 않지만 검증 가능한 데이터 삽입	시각적 품질 유지, 강화된 보안	즉각적인 출처 확인 제한
동시 적용 (인지 가능/인지 불가능 워터마크)	인지 가능 + 인지 불가능 워터마크를 함께 사용	출처 표기와 위조 방지 동시에 가능	구현 복잡도와 리소스 부담 증가

표 1. 식별 워터마크와 비식별 워터마크의 유형 비교

■ 생성형 AI 콘텐츠 워터마크의 활용 사례

생성형 AI 콘텐츠가 이미지, 음성, 영상 등 다양한 형태로 확장되면서 주요 국내·외 서비스들은 각 콘텐츠 특성에 맞춰 인지 가능(Visible) 또는 인지 불가능(Invisible) 워터마크를 적용하고 있으며, 그 활용 방식은 다음과 같다.

콘텐츠 유형	주요 서비스	워터마크 유형	활용 사례
이미지	에이닷(SKT)	인지 가능 워터마크	생성형 AI 사진 및 프로필 이미지에 좌측 하단 로고 삽입으로 식별 가능한 워터마크 제공
	제미나이(Google)	인지 불가능 워터마크	텍스트 기반 이미지 생성 시 SynthID 를 통해 픽셀 단위로 인지 불가능한 워터마크 삽입
음성	클로바 더빙(Naver)	인지 가능 워터마크	생성된 음성 콘텐츠에 출처 표기 자동/직접 삽입 기능 제공
	AI 음성(Microsoft Azure)	인지 불가능 워터마크	에코은닉기술, 양지화 지수 변조, 확산 스펙트럼 기술을 이용해 96 비트 키 기반 워터마크를 오디오에 삽입
영상	매직미디어(Canva)	인지 가능 워터마크	AI 생성 영상 우측 하단에 특정 이미지 삽입 방식으로 시각적 워터마크 적용
	비오(Google DeepMind)	인지 불가능 워터마크	SynthID 를 활용해 영상 프레임마다 인지 불가능한 디지털 워터마크 삽입

표 2. 국내외 주요서비스의 AI 생성형 콘텐츠 유형별 워터마크 활용 사례

* 출처 : 과학기술정보통신부 블로그 콘텐츠 '빠르게 발전하는 AI 워터마크 기술, 어디까지 왔을까?'

그림 2. SK 텔레콤 에이닷(A.)으로 생성한 이미지(AI 프로필) 및 좌측 하단 이미지(AI 프로필)인지 가능 워터마크

* 출처 : 과학기술정보통신부·한국정보통신기술협회《인공지능(AI) 워터마크 기술 동향 보고서》

그림 3. 구글 제미나이로 생성된 원본 이미지(왼쪽)와 인지 불가능 워터마크(신스 ID)를 적용한 이미지(오른쪽) 비교

■ 생성형 AI 콘텐츠 워터마크의 기술적 한계

생성형 AI 컨텐츠의 진위를 구별하고 투명성을 확보하기 위해 워터마크는 기술적 안전장치로서 중요한 역할을 한다. 그러나 현재의 워터마크 기술도 한계는 있다. 인터넷상에는 워터마크를 제거하거나 변조할 수 있는 상용 도구들이 광범위하게 유통되고 있어, 삽입된 식별 정보가 손쉽게 삭제될 수 있기 때문이다.

또한 워터마크 삽입 방식 자체의 취약점을 악용한 공격도 가능하다. 예를 들어, GAN(Generative Adversarial Networks)을 이용한 워터마크 제거 기술은 이미지별 워터마크 위치 차이를 학습하여 워터마크를 효과적으로 삭제할 수 있다. 더 나아가 VWGAN(Very Weak Generative Adversarial Network)을 적용하면 기존보다 약 20% 높은 성능으로 워터마크 제거가 가능하다는 연구 결과도 보고되고 있다.

인지 불가능 워터마크 역시 완벽하지 않다. 겉보기에는 사용자가 식별하기 어렵다는 장점이 있지만, 랜덤 노이즈 삽입 후 이미지 재구축, JPEG 압축, VAE 기반 공격 등으로 제거될 수 있다. 특히 RivaGAN 방식에 재생성 공격을 통해 93~99%의 제거율이 확인되기도 했다. 이러한 사례들은 현재의 워터마크의 기술적 발전이 더욱 필요하다는 것을 보여준다.

■ 생성형 AI 콘텐츠 워터마크의 보완 과제

현재의 생성형 AI 콘텐츠 워터마크는 변조, 무단 복제, 불법 배포 등 다양한 위협에 노출될 수 있으므로, 기술적 보완이 필요하다.

우선 워터마크 내구성을 강화하는 것이 중요하다. 인지 가능·불가능 워터마크 모두 JPEG 압축, 이미지 재구성, 랜덤 노이즈 삽입 등 공격에 취약하므로, 워터마크를 이미지나 영상의 다양한 주파수 영역과 구조적 특징에 분산 삽입하는 방식을 고려할 수 있다. 또한 다중 계층적 삽입과 오류 정정 코드 적용을 통해 변조나 압축에도 워터마크가 유지될 가능성을 높일 수 있다.

적응형 공격에 대응하기 위해서는 워터마크 삽입 방식을 정적 위치가 아닌 랜덤화한 동적 위치에 삽입하거나 변형 가능한 패턴으로 설계하고, 주기적 업데이트와 공격 탐지 기능을 결합하는 방법이 적용되어야 한다.

복합적 검증 체계 구축도 또한 필요하다. 단일 워터마크 방식만으로는 제거를 완전히 방지하기 어렵기 때문에, 식별 가능 워터마크와 인지 불가능 워터마크를 동시에 활용하거나, 블록체인 등 분산 원장 기술과 연계해 원본 생성 기록과 워터마크 정보를 함께 확인하는 방안이 고려될 수 있다.

마지막으로, 자동화된 탐지 및 모니터링 체계 구축이다. 워터마크 제거 시도를 실시간으로 탐지하고 경고할 수 있는 시스템을 마련하면 비정상적 이미지 변조나 손상 발생 시 신속한 대응이 가능하다. 특히 배포와 재배포가 활발히 이루어지는 SNS 플랫폼 사업자를 비롯해, 언론사, 포털 사업자, 클라우드 스토리지 서비스 제공자 등 대규모로 이미지와 영상을 다루는 기관에도 이러한 체계를 적용하는 것이 적절해 보인다.

이러한 방향들이 종합적으로 고려될 때, 생성형 AI 컨텐츠 워터마크는 단순한 표시 수단을 넘어 콘텐츠 안전성과 책임 있는 사회적 인식을 마련하는데 핵심 수단으로 발전할 수 있다.

■ 맺음말

AI 생성형 콘텐츠의 확산으로 오남용과 변조 가능성이 증가했다. 피해 위험성을 줄이기 위해서는 워터마크 기술의 필요성이 부각되고 있다. 단일 기술만으로는 충분하지 않다. 다층적이고 종합적인 기술적 대응이 필수다. 먼저, 식별 가능한 워터마크와 인지 불가능한 워터마크를 동시에 적용함으로써 생성물의 출처와 무결성을 다각도로 검증해야 한다. 여기에 블록체인 기반 기록 등을 활용하여 원본 생성 기록과 워터마크 정보를 함께 적용해야 변조 여부를 보다 정밀하게 검증할 수 있다. 또한, AI 생성물 탐지 알고리즘과 자동화 분석 도구를 활용하면 인간의 육안으로는 식별하기 어려운 변조나 조작 시도도 실시간으로 확인할 수 있으며, 지속적인 기술 개선과 업데이트를 통해 새로운 공격 유형에도 대응 가능성을 높일 수 있다.

기술적 대응과 함께, 국제적으로 통용될 수 있는 글로벌 표준을 마련하여 국가와 플랫폼 간 워터마크 반영 및 탐지 방식의 일관성을 확보하고, 기술 개발과 적용을 촉진할 수 있는 정책적 지원도 필요하다. 아울러 일반 사용자와 콘텐츠 제작자가 워터마크의 목적과 중요성을 인지하는 '인식 제고 활동'을 전개함으로써, 무분별한 제거 시도를 줄이고 안전하고 책임 있는 콘텐츠 이용 문화를 정착시키는 것도 중요하다.

무엇보다 생성형 AI 가 산업과 사회 전반으로 빠르게 확산되는 전환기적 상황에서, 기업들은 더욱 철저한 대비와 선제적 대응을 갖출 필요가 있다. 특히 사회적 파급력이 큰 고영향 AI 와 생성형 AI 를 사용하는 기업이라면, 단순한 기술 활용을 넘어 법적·윤리적 리스크를 최소화할 수 있는 컴플라이언스 체계를 정교하게 구축해야 한다. 향후 마련될 세부 법령과 지침을 면밀히 추적하고, 이를 실무 현장에 즉시 반영할 수 있는 관리 역량을 확보하는 것이 곧 기업의 지속 가능성과 직결될 수 있다.

이러한 변화 속에서 AI 기본법에 부합하는 정보 보호 체계와 신뢰할 수 있는 AI 보안은 선택이 아닌 기업의 핵심 과제가 되고 있다. 데이터 보호, 알고리즘의 투명성, 위험 대응 체계는 기업의 사회적 책임을 뒷받침할 뿐만 아니라, 글로벌 시장에서 신뢰받는 파트너로 자리매김하기 위한 필수 조건이기도 하다.

SK 쉴더스는 다년간 축적된 AI 보안 및 데이터 보호 전문성을 기반으로, 각 기업 환경에 맞춤화된 위험 관리 및 대응 체계를 설계해왔다. 기업들이 규제 변화와 새로운 위협 환경에 능동적으로 대응할 수 있도록 지원하며, 안전하고 책임 있는 AI 활용을 위한 최적의 컨설팅 서비스를 제공하고 있다. SK 쉴더스의 전문적 지원은 기업들이 단순히 규제를 준수하는 데 그치지 않고, 안전성·투명성·경쟁력을 고루 갖춘 신뢰성 있는 기업으로 도약할 수 있을 것이다.

■ 참고문헌

[1] 과학기술정보통신부/한국정보통신기술협회, “인공지능(AI) 워터마크 기술 동향 보고서”, 2025.01

[2] Cao, Z., Niu, S., Zhang, J., & Wang, X., "Generative adversarial networks model for visible watermark removal", 2019.07

[3] Zhao, X., Zhang, K., Su, Z., Vasan, S., Grishchenko, I., Kruegel, C., ... & Li, L., “Invisible Image Watermarks Are Provably Removable Using Generative AI”, 2023.06

■ 참고 자료

[1] 방송통신위원회/정보통신정책연구원, “생성형 인공지능 서비스 이용자 보호 가이드라인”, 2025.06

[2] 과학기술정보통신부, 빠르게 발전하는 AI 워터마크 기술, 어디까지 왔을까?, 2025.02

[3] EY, “Identifying AI generated content in the digital age: The role of watermaking”, 2024.09

[2] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system

[3] 행정안전부, 공공기관 AI 보안 가이드라인, 23.10

[4] NIPA, 산업별 생성형 AI 활용과 보안 위협 보고서, 2024

[5] SK쉴더스, EQST Insight 블로그 시리즈 (2023~2024)

Keep up with Ransomware

Rust 버전의 INC 랜섬웨어 분석 및 위협 대응 방안

■ 개요

2025년 8월 랜섬웨어 피해 사례 수는 지난 7월(485건) 대비 약 13% 증가한 549건을 기록했다. 8월에는 각국의 법집행 활동이 한층 강화되는 동시에, 공격자들의 기술 역시 더욱 정교해지는 양상이 두드러졌다.

미국 법무부는 8 월 11 일, BlackSuit 랜섬웨어 그룹을 겨냥한 국제 합동 작전의 성과를 발표했다. 이번 작전을 통해 수사팀은 해당 조직이 운용하던 서버 4 대와 도메인 9 개를 압수하고, 약 109 만 달러(한화 약 15 억 원) 상당의 암호화폐 자산을 몰수하는 데 성공했다. 미국뿐 아니라 영국, 독일, 프랑스, 캐나다 등 여러 국가의 법집행기관 협력으로 진행됐다. 하지만 암호화 파라미터, 랜섬노트 등에서 확인된 BlackSuit 와 Chaos 랜섬웨어의 연관성으로 인해 BlackSuit 그룹이 완전히 해체되지 않고, 활동을 이어갈 가능성이 제기된다.

8 월초 Akira 랜섬웨어 그룹은 정상 CPU 성능 조정 툴(ThrottleStop)의 드라이버 취약점을 악용해 Microsoft Defender 를 비활성화하는 BYOVD[1] 공격을 수행했다. 공격자는 취약한 드라이버(rwdrv.sys)를 서비스로 등록해 커널 수준의 권한을 확보한 후, 악성 드라이버(hlpdrv.sys)를 로드해 Defender 의 보안 설정을 변경했다. Akira 그룹이 취약한 드라이버를 악용한 공격 기법을 지속적으로 활용하고 있으므로, ThrottleStop 드라이버의 취약점에 대한 보안 조치가 요구된다.

8 월에 등장한 신규 랜섬웨어 그룹인 Cephalus 는 SentinelOne 의 정상 실행 파일(SentinelBrowserNativeHost.exe)을 악용하여 DLL 사이드로딩[2] 방식으로 악성 DLL 을 로드함으로써 랜섬웨어를 실행했다. 이러한 기법은 보안 제품 자체를 역이용해 탐지와 대응을 한층 어렵게 만들며, 랜섬웨어 공격의 복잡성과 정교함을 보여준다.

[1] BYOVD(Bring Your Own Vulnerable Driver): 공격자가 취약점이 존재하는 합법적인 드라이버를 직접 시스템에 설치하여, 운영체제 커널 권한을 탈취한 뒤 보안 솔루션 무력화 등 악성 행위를 수행하는 공격 기법

[2] DLL 사이드로딩: 정상 프로그램이 실행 시 참조하는 DLL 파일을 공격자가 조작하거나 악성 DLL 로 교체해, 정상 프로세스를 통해 악성코드가 실행되도록 하는 공격 기법

8 월 말, PromptLock 이라는 이름의 AI 기반 랜섬웨어가 공개되었다. PromptLock 은 뉴욕대 보안 연구팀이 LLM 으로 공격 과정을 자동으로 실행할 수 있는지를 확인하기 위해 제작·공개한 POC[3] 로 알려졌다. 로컬 LLM[4] 을 Ollama[5] 프레임워크로 호출해 실시간으로 Lua[6] 스크립트를 생성한다. PromptLock 은 Windows, macOS, Linux 등 여러 운영체제에서 동작하며, AI 가 파일을 스캔한 뒤 파일 유형, 경로, 내용 등 스캔 정보를 사용자가 사전 작성한 프롬프트에 따라 유출 또는 암호화 수행 여부를 결정한다. 현재 공개된 PromptLock 은 POC 이지만, 실제 공격자가 이 접근법을 악용할 경우 매 실행마다 새로운 코드가 생성돼 해시 등이 바뀌어 정적 탐지의 효용이 낮아질 수 있다. 위험도가 유의미하게 상승하는 것을 고려해 행위 기반 탐지 강화의 필요성이 요구된다.

[3] POC(Proof of Concept): 연구·검증을 위한 시연용 구현으로, 제한된 조건에서 개념의 가능성만 확인하는 코드/설계

[4] 로컬 LLM(Local Large Language Model): 사용자의 시스템에 직접 설치·실행되는 대규모 언어 모델을 의미

[5] Ollama: 오픈소스 기반의 LLM 실행 프레임워크로, 로컬 환경에서 대형 언어 모델을 손쉽게 불러오고 실행할 수 있도록 지원

[6] Lua: 1993 년 개발된 경량 스크립트 언어로, 임베디드 시스템과 게임 엔진 등에서 널리 활용

■ 랜섬웨어 뉴스

BlackSuit 그룹에 대한 국제 합동 작전 결과

- 8월 11일, 미국 법무부가 합동 작전 결과 발표
- 운영 서버 4대·도메인 9개 압수, 암호화폐 $1.09M(약 15억 원) 몰수
- 작전 이후 Chaos 그룹 활동 부각 BlackSuit와의 구조적 유사성에 근거한 연계 정황 제기

일본 경찰청(NPA) Phobos·8Base 무료 복호화기 공개

- 지원 확장자 .phobos·.8base·.elbie·.faust·.LIZARD 등, 복호화 성공 사례 확인
- NPA 홈페이지 및 No More Ransom 등에 공개

Akira 랜섬웨어 BYOVD 기법으로 Windows Defender 비활성화

- ThrottleStop의 취약 드라이버 rwdrv.sys를 서비스로 등록해 커널 권한 획득
- 악성 드라이버(hlpdrv.sys)를 로드해 Microsoft Defender의 보안 설정을 수정하고 기능을 비활성화

신규 그룹 Cephalus, SentinelOne 파일을 이용한 공격

- SentinelOne 정상 실행 파일(SentinelBrowserNativeHost.exe) 악용
- DLL 사이드로딩 기법으로 악성 DLL 실행

AI 기반 PromptLock 랜섬웨어 공개

- 로컬 LLM(Ollama)을 활용해 실시간으로 Lua 스크립트를 생성·실행
- 파일을 스캔한 뒤, 사전 프롬프트에 따라 유출 또는 암호화 여부를 결정
- Windows, MacOS, Linux 등 멀티플랫폼 환경을 지원하며, 공격 자동화와 변종 생성이 더욱 가속화

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

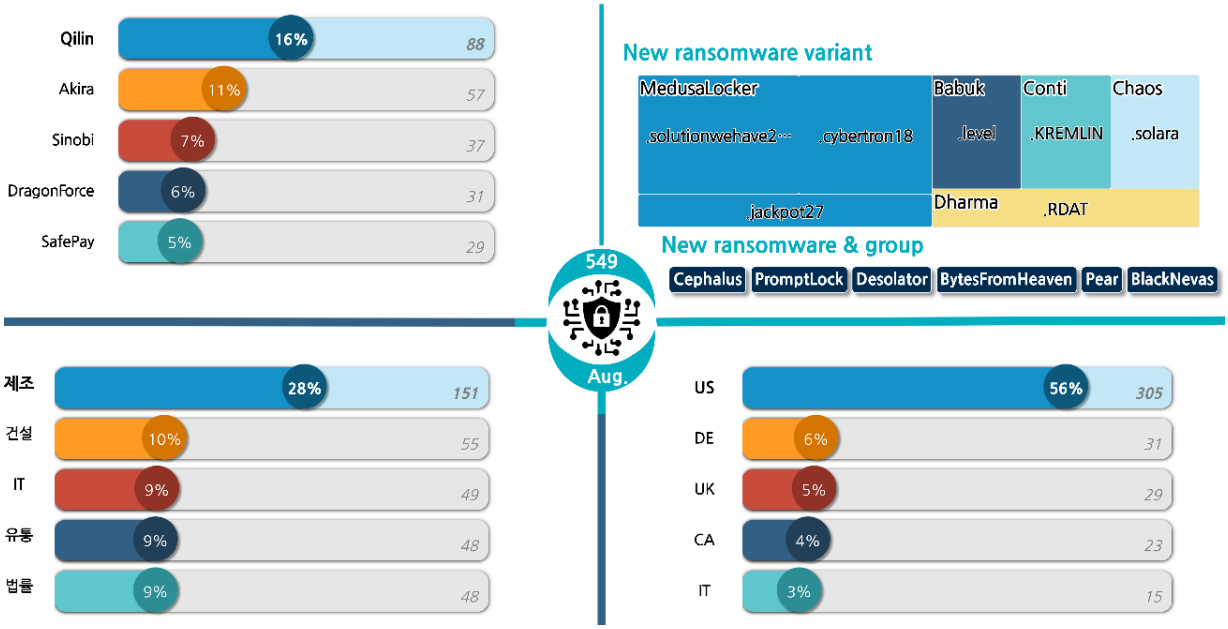


그림 2. 2025 년 8 월 랜섬웨어 위협 현황

새로운 위협

8 월 한 달 동안 총 549 건의 랜섬웨어 피해 사례가 확인됐으며, 이 기간 신규 랜섬웨어 6 개가 새롭게 등장했다. 이 중 Cephalus, Desolator, PEAR, BlackNevas 등 4 개 그룹은 자체적으로 운영하는 데이터 유출 사이트에 피해 사실을 게시했다.

그림 3. Cephalus 의 데이터 유출 사이트

2025 년 8 월에 처음 발견된 Cephalus 랜섬웨어 그룹은 여러 피해 사례를 발생시킨 것으로 확인되었다. 그러나 8 월 말 기준, Cephalus 가 운영하던 다크웹 유출 사이트는 접근이 불가능한 상태로 이후 추가적인 활동은 확인되지 않고 있다.

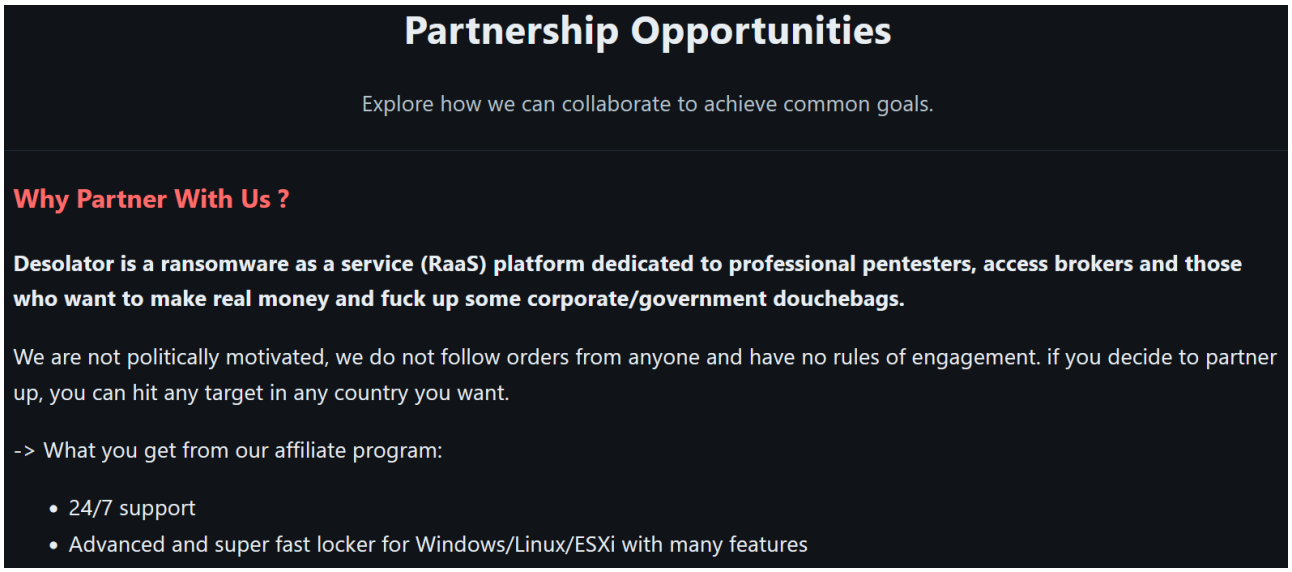


그림 4. Desolator 의 RaaS[7] 모집글

2025 년 8 월 말에 처음 발견된 Desolator 랜섬웨어는 현재까지 총 3 건의 피해 사례가 확인되었으며, 해당 그룹은 RaaS 계열사 모집 글에서 상시 지원을 내세우며, Windows·Linux·ESXi 용 랜섬웨어를 제공하고, 수익의 10%만 지불하면 된다고 명시했다. 또한 피해자가 요구액을 지급하지 않을 경우 탈취 데이터를 공개할 것임을 밝혔다.

[7] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 쉽게 랜섬웨어를 만들고 공격할 수 있도록 하는 비즈니스 모델

Top5 랜섬웨어

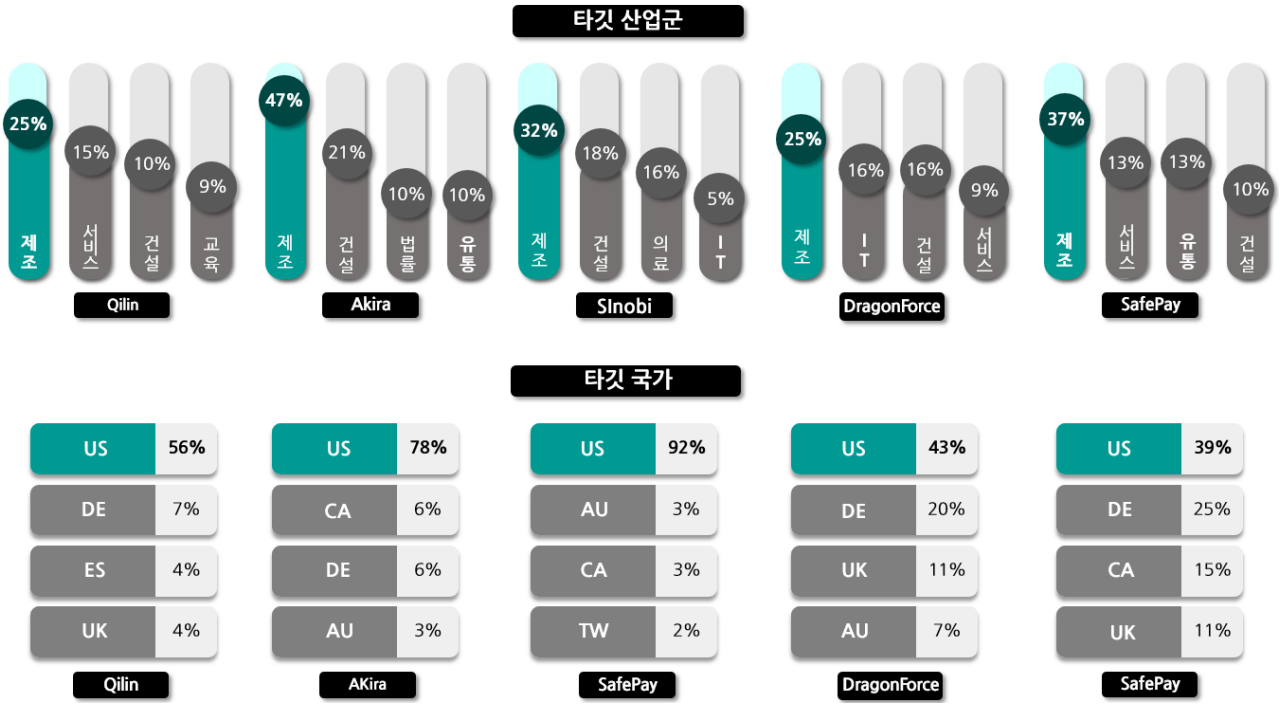


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

Qilin 그룹은 8 월 20 일 일본의 닛산 디자인 자회사 Nissan Creative Box 를 공격해 약 4TB 분량의 내부 정보를 탈취했다고 주장했다. 이들은 자사 다크웹 유출 사이트에 생산 설계 자료와 각종 내부 문건의 목록을 게시하며, 추가 유출을 예고하는 등 강도 높은 협박을 이어갔다.

Akira 그룹은 8 월 말 미국의 과학 계측기기 제조사 The Fredericks Company 를 공격해 내부 재무자료와 직원·고객 데이터를 탈취했다고 밝혔다. 이들은 다크웹 유출 사이트에 수십 GB 의 정보 유출을 예고하며 피해사를 압박하는 전형적인 전술을 사용했다. 같은 시기, 미국의 교정치료 장비 제조사 RMO Orthodontics 또한 피해 대상으로 등재되었으며, Akira 는 추후 데이터 샘플을 공개하겠다고 경고했다.

Sinobi 그룹은 8 월 중순 호주의 에너지 기업 Energy Developments 를 공격해 운영자료 및 내부 보고서를 탈취했다. 공격자는 다크웹 유출 사이트를 통해 해당 기업의 공급망 및 전력 운영 관련 정보 일부를 공개하며 협박 수위를 높였다. 이외에도 미국의 중견 보험사 Eagan Insurance 와 투자사 Norwest Venture Partners 를 연이어 공격 대상으로 삼아, 고객·계약·내부 재무자료 등 다양한 유형의 정보 탈취를 주장했다.

DragonForce 그룹은 8 월 21 일 독일의 오디오 기기 제조업체 InEar GmbH 를 공격했다고 밝히며, Hear the Difference 브랜드 관련 제품 설계도 및 유통정보 등을 다크웹에 게시했다. 또한 미국의 전자기기 유통기업 ABM Wireless 와 뉴욕 소재 고급 골프클럽 Park Country Club 에 대한 공격도 연이어 게시했다.

SafePay 그룹은 8 월 29 일, 미국 코네티컷 주의 재가 요양 서비스 기관인 Companions & Homemakers 를 공격해 환자 관리 및 내부 인사 기록 등을 암호화하고 탈취했다고 주장했다. 이들은 자사 다크웹 유출 사이트에 피해사를 게시하고 곧 데이터를 전면 공개하겠다며 협상에 응할 것을 강하게 압박했다. 같은 날, 독일의 화장품 제조사 Lipcare.de 에 대해서도, 민감한 제조 문서와 고객 관련 데이터를 암호화했다고 밝혔다.

■ 랜섬웨어 집중 포커스

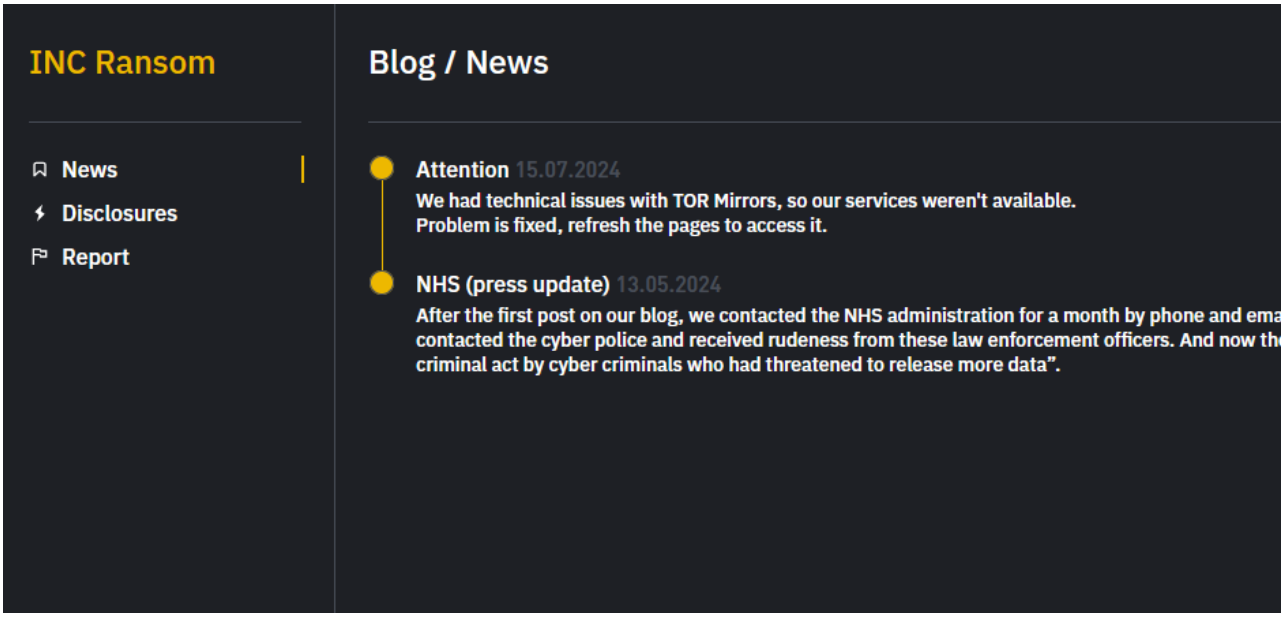


그림 6. INC 랜섬웨어 그룹의 다크웹 유출 사이트

INC 랜섬웨어 그룹은 2023 년 7 월 활동을 시작한 이후 2024 년 4 월 소스코드 판매 정황이 확인된 뒤에도 활동을 중단하지 않았으며, 최근에는 Rust 언어로 제작된 랜섬웨어를 사용해 활동하고 있다. 다크웹 유출 사이트에는 피해 게시가 누적되고, C/C++ 버전 이후 Rust 로 제작된 새로운 버전이 발견되었으며, 다크웹 유출 사이트에는 피해자를 꾸준히 공개했다.

피해 규모는 지속적으로 확대되고 있으며, 의료·제조·교육·공공 등 사회 기반을 구성하는 주요 분야까지 넓히고 있다. 이러한 양상은 INC 랜섬웨어 그룹이 특정 산업이나 지역에 국한되지 않고 폭넓은 대상을 노리며, 전 세계적으로 위협 활동을 확대해 나가고 있음을 보여준다.

본 보고서에는 새롭게 제작된 Rust 버전의 INC 랜섬웨어를 중점으로 분석해 랜섬웨어 위협에 효과적으로 대비할 수 있도록 하고자 한다.

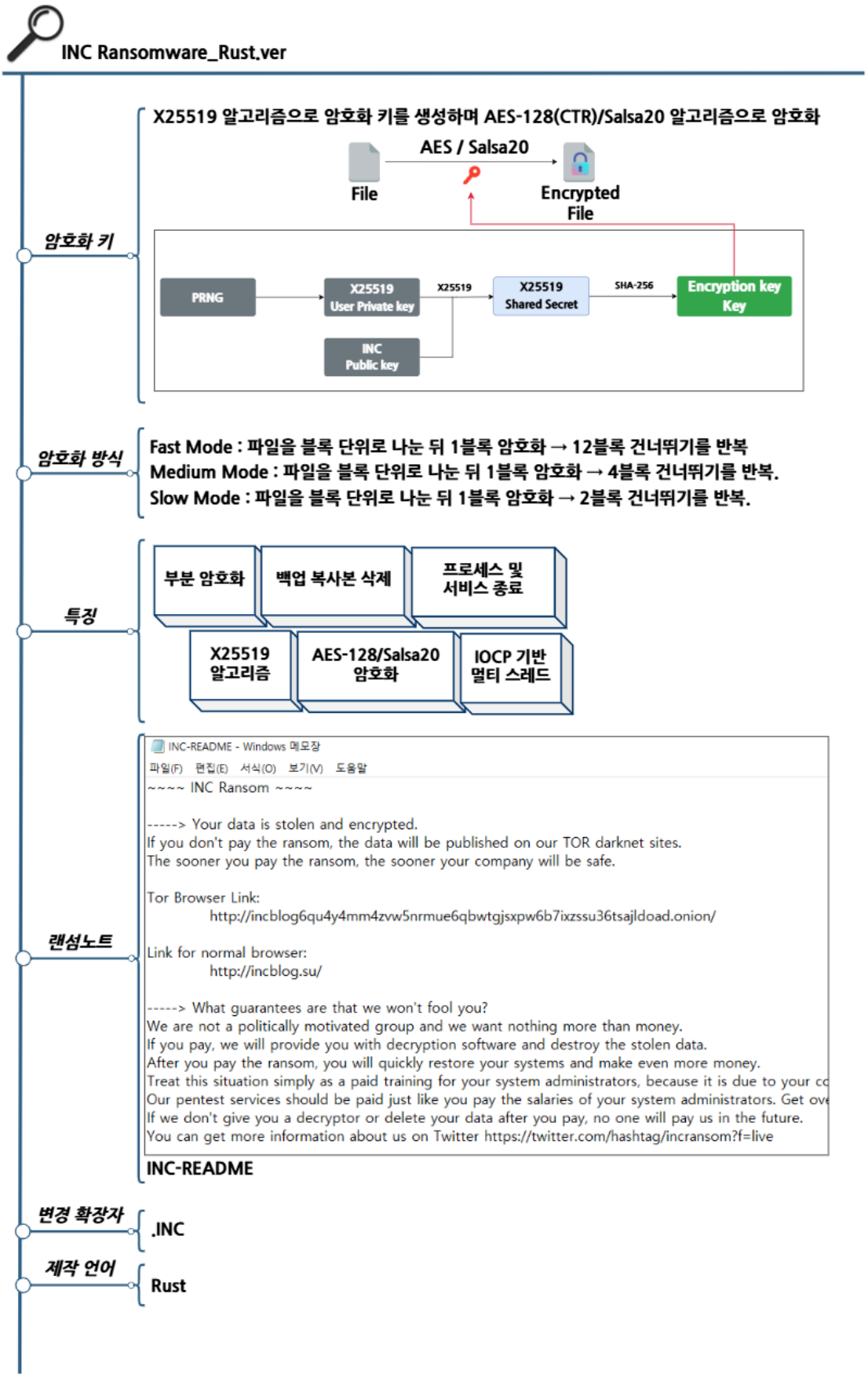


그림 7. INC 랜섬웨어 개요

INC 랜섬웨어 전략

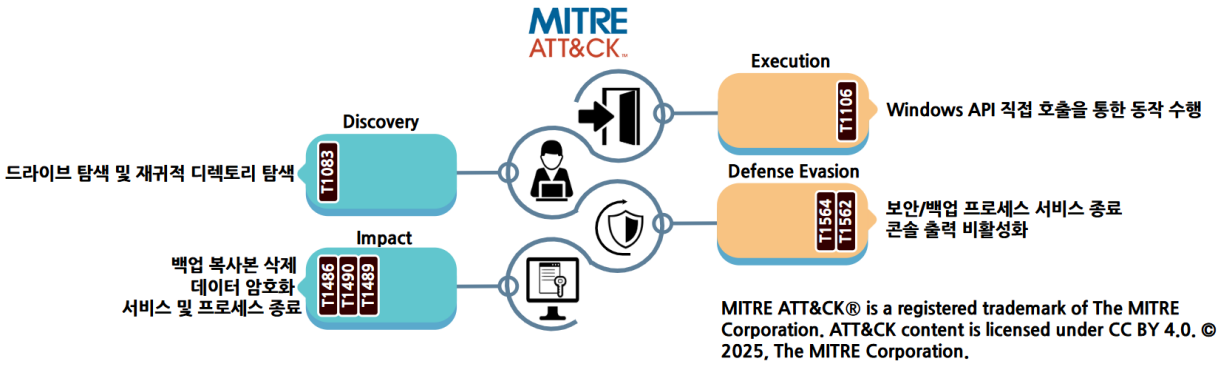


그림 8. INC 랜섬웨어 공격 전략

INC 랜섬웨어 Rust 버전은 실행 시 입력된 인자를 확인하여 기능을 제어한다. 실행에 반드시 필요한 인자는 없으며, 별도의 인자를 지정하지 않아도 랜섬웨어는 정상적으로 동작한다. 확인된 인자와 기능은 아래 표와 같다.

구분	설명
--def	파일 암호화 없이 랜섬노트만 저장
-h / --help	실행 도움 메시지 출력
--hide	콘솔창 숨기기
--sup	암호화 대상이 실행중이라면 해당 프로세스 종료
-v / --version	랜섬웨어 파일명 출력
--dir <directories>	암호화 대상 폴더 지정
--file <files>	암호화 대상 파일 지정
--mode <fast|medium|slow>	암호화 모드 설정 (기본: medium)
--proc <processes>	프로세스 종료 대상 설정
--serv <services>	서비스 종료 대상 설정

표 1. INC 랜섬웨어 실행 인자

INC 랜섬웨어는 실행 시 --proc, --serv 옵션을 통해 지정된 프로세스와 서비스를 종료할 수 있다. 사전에 내장된 고정 목록 대신, 공격자가 상황에 맞게 종료 대상을 유연하게 지정하는 구조다. 또한 --file, --dir 옵션으로 암호화 대상을 명시하지 않으면, 시스템의 모든 드라이브를 열거해 존재 여부와 유형을 확인한 뒤 암호화 대상으로 설정한다.

이때 --dir 인자로 암호화 대상 폴더를 지정한 경우나 전체 드라이브 암호화에서 특정 드라이브를 암호화하는 경우, 지정한 폴더와 그 하위 폴더를 재귀적으로 탐색하며 랜섬노트를 생성한 후 현재 디렉터리의 항목을 열거한다. 이 중 디렉터리는 예외 디렉터리 리스트와 비교해 제외 여부를 결정하고, 제외되지 않으면 탐색 함수를 재귀 호출해 하위 폴더를 계속 탐색한다. 파일은 예외 확장자 리스트와 비교하여 해당하지 않는 경우에만 암호화 대상에 포함한다. 확인되는 리스트는 아래 표와 같다.

예외 확장자 및 파일	예외 폴더
*.exe, *.log, *.dll, *.INC, INC-README.txt	windows, program files, appdata, $recycle.bin, programdata, all users, sophos

표 2. INC 랜섬웨어 암호화 예외 대상

INC 랜섬웨어에서 백업 복사본 삭제는 일반적으로 사용되는 Windows 유틸리티(vssadmin, wmic shadowcopy, wbadmin, bcdedit) 호출 없이, DeviceIoControl 을 직접 사용해 볼륨 섀도 복사본의 저장 공간을 작은 값으로 재설정하는 방식으로 수행된다. 이때 OS 는 저장 공간 부족 상태로 인식해 공간 확보를 위해 기존 백업 복사본을 자동으로 삭제하게 된다.

각 파일에 대해 32 바이트 난수로 X25519 키쌍을 생성하고, 하드코딩된 INC 의 공개키를 사용해 ECDH 공유 비밀을 만들어 암호화에 활용한다. 생성된 공유 비밀은 SHA-256 해싱 과정을 거쳐 파일 암호화 키로 사용한다. 블록 크기는 시스템 클러스터[8] 크기와 동일하게 설정한다. 파일을 해당 블록 단위로 분할한 뒤, 한 번에 1 블록만 암호화하고 이어지는 블록들은 설정된 간격만큼 건너뛰는 절차를 끝까지 반복한다. 설정되는 간격은 옵션에서 설정된 Fast/Medium/Slow 모드에 따라 각각 12/4/2 블록의 간격을 사용한다. 예를 들어 블록 크기가 0x10000 바이트(64KB), 클러스터의 크기가 0x1000 바이트(4KB), 암호화 모드가 Medium(default)인 경우 4KB 크기의 1 블록을 암호화한 뒤 16KB 크기만큼 건너뛰고 다음 4KB 크기의 1 블록을 암호화하는 형태로 반복 동작한다. 암호화 알고리즘은 하드웨어에 따라 선택되며, CPU 가 AES-NI 를 지원하면 AES-128, 미지원 시 Salsa20 을 사용한다.

[8] 시스템 클러스터: 파일시스템이 파일 데이터를 배치·관리할 때 사용하는 최소 할당 단위

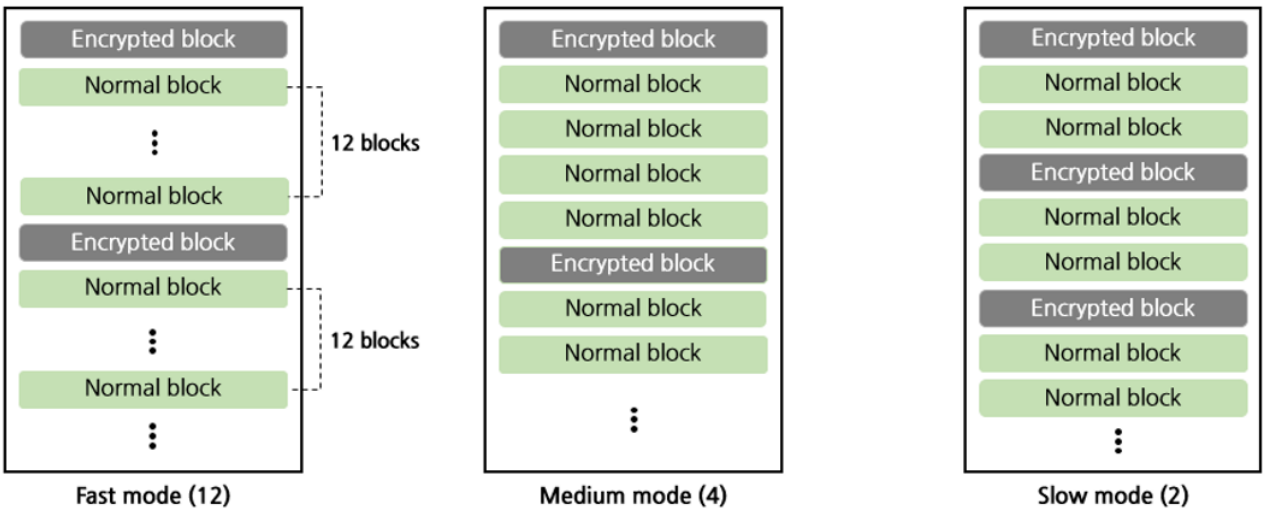


그림 9. INC 랜섬웨어 암호화 방식

파일 암호화가 완료되면 파일 끝에 83 바이트 Footer 를 추가한다. Footer 에는 순서대로 X25519 공개키, 공개키의 SHA-256, 암호화 알고리즘 구분자(0: AES-128, 1: Salsa20), 암호화 블록 크기, 암호화 간격, 암호화된 총 블록 수, "INC" 마커가 저장된다.

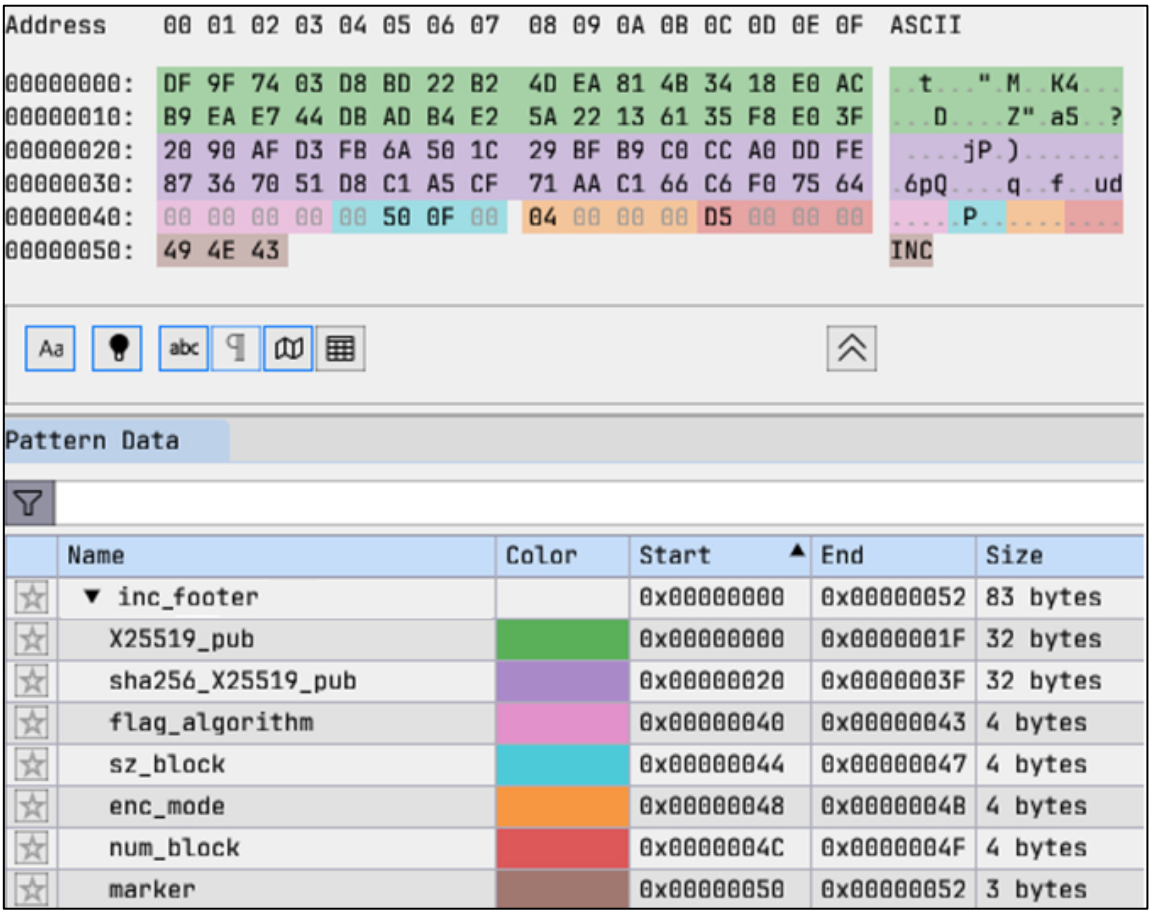


그림 10. 암호화 파일 Footer

INC 랜섬웨어 대응방안

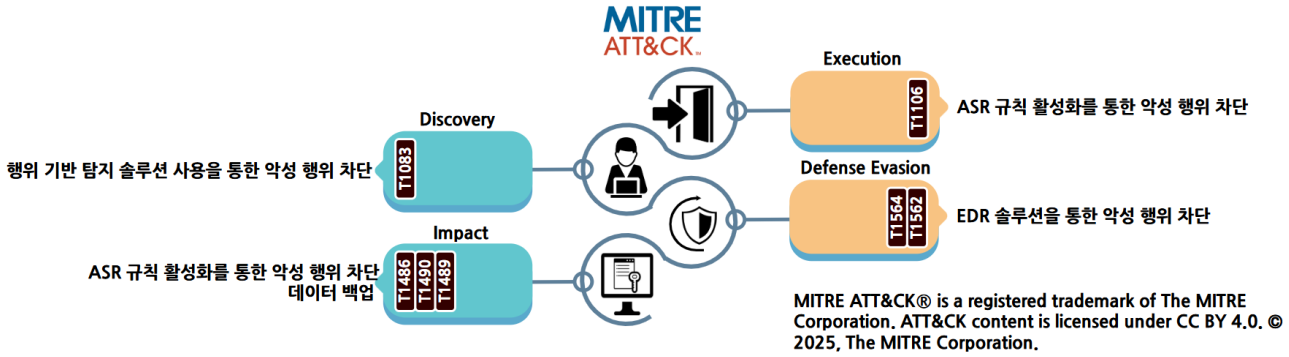


그림 11. INC 랜섬웨어 대응방안

INC 랜섬웨어는 실행 직후 보안 관련 서비스와 특정 프로세스를 강제 종료하고, 볼륨 섀도 복사본을 삭제한 뒤 부분 암호화를 진행한다. 이에 따라 ASR 규칙을 활성화하면, 백업 파괴·서비스 종료·암호화와 연관된 비정상 프로세스를 사전에 차단하여 악성 행위를 효과적으로 억제할 수 있다.

또한 EDR 솔루션을 도입하고 최신 보안 패치를 적용하여, 알려진 취약점을 통한 침투나 비정상적인 동작을 신속히 식별·차단할 수 있도록 해야 한다. 이를 통해 파일 암호화 과정에서 발생하는 행위 기반 패턴을 실시간으로 탐지하고, 악성 프로세스의 실행을 중단할 수 있다.

백업 복사본을 별도 네트워크 구간, 외부 저장소, 오프라인 매체에 주기적으로 분산해 두면 시스템이 암호화되더라도 복구할 수 있다. 이때 백업 장치에는 업무상 필요한 최소 권한만 부여하고, 정기 복구 테스트를 통해 백업 데이터의 무결성과 실제 복원 가능성을 확인하는 것이 중요하다.

IoCs

Hash(SHA-256)
17317ee3c9bd706ef2942a38f55c05176e4abdf377a5b72250d89ebf2a795ca0
fd0dbc6d941ff76e5204df4c644ba0d3241d05995f30e6b837618cd9dcc8b99c
b1815ef993b2649be791f0cf4249e502e7c3763fe69451b8b32508089e15d103
61f70b9a0bde499d764807fe24517e64ea0130a3f6e493ead360058e59854776
be9e1fd4dcf8a644aba70c8e92fa07a54d0ce96fb74217b48991700d281083bd

■ 참고 사이트

• Techradar (https://www.techradar.com/pro/security/the-first-ai-powered-ransomware-has-been-spotted-and-heres-why-we-should-all-be-worried)

• Cyberscoop (https://cyberscoop.com/ai-ransomware-promptlock-nyu-behind-code-discovered-by-security-researchers)

• NYU (https://engineering.nyu.edu/news/large-language-models-can-execute-complete-ransomware-attacks-autonomously-nyu-tandon-research)

• Bankinfosecurity (https://www.bankinfosecurity.com/rise-chaos-ransomware-tied-to-blacksuit-groups-exit-a-29067)

• SC Media (https://www.scworld.com/news/cephalus-ransomware-abuses-sentinelone-executable-for-dll-sideloading)

• Bleepingcomputer (https://www.bleepingcomputer.com/news/security/akira-ransomware-abuses-cpu-tuning-tool-to-disable-microsoft-defender/)

• Justice.gov (https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal)

• Brinztech (https://www.brinztech.com/breach-alerts/brinztech-alert-partnership-program-of-desolator-ransomware-service-is-detected)

Special Report

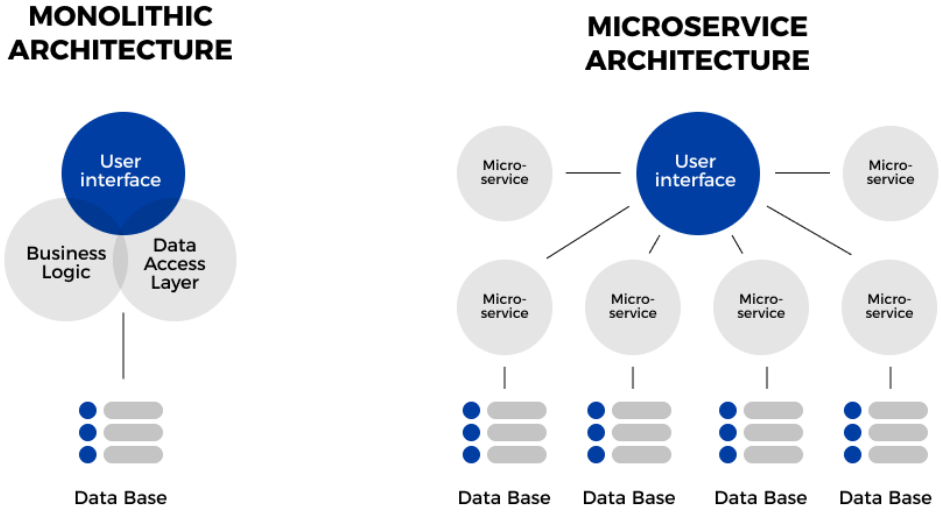
제로트러스트 보안전략 : 애플리케이션 및 워크로드 (Application&Wokrdload)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

■ 애플리케이션 및 워크로드 (Application&Wokrdload) 필러 개요

제로트러스트 아키텍처에서 어플리케이션 및 워크로드 필러는 기업 망의 관리 시스템, 프로그램 등 온프레미스 및 클라우드 환경에서 실행되는 모든 서비스를 포괄한다. 이는 조직의 비즈니스 로직과 데이터가 실제로 실행·처리되는 동적인 영역으로, 컨테이너나 가상머신(VM)과 같은 개별 실행 단위 보호 및 데이터의 안전한 전달 보장을 목표로 한다. NIST 가이드라인에서는 제로트러스트의 핵심을 개별 '리소스(Resource)' 보호에 두고 있으며, 애플리케이션과 워크로드는 가장 중요한 리소스에 해당한다.

디지털 전환이 가속화되면서 애플리케이션 아키텍처는 근본적으로 변화했다. 과거의 거대한 단일 애플리케이션(Monolithic)은 독립적으로 실행되었으나, 현재는 통신하는 수많은 작은 서비스의 집합(Microservices Architecture, MSA)으로 진화했다. 이로 인해 애플리케이션의 경계는 기존의 데이터센터에서 퍼블릭·프라이빗 클라우드, 하이브리드 환경으로 확장되었으며, 수많은 API 가 새로운 통신 통로이자 공격 표면이 되었다. 또한, 개발과 운영이 통합된 DevOps 문화와 CI/CD 파이프라인의 도입은 애플리케이션의 배포 속도를 획기적으로 높였지만, 동시에 보안이 고려되지 않은 코드가 운영 환경에 빠르게 배포될 수 있는 새로운 위험을 만들었다.



출처 : Cloudflight, "Monolithic Architecture vs Microservices Architecture"

그림 1. 어플리케이션 관리의 변화

이러한 환경에서 웹 방화벽(WAF)와 DDoS 장비 같은 전통적인 경계 기반 보안 모델은 어플리케이션 관리의 명백한 한계를 드러낸다. 경계 기반 보안 모델은 어플리케이션 공격 시 주로 외부에서 내부로 들어오는 공격을 통제하는 데 중점을 둔다. 클라우드 환경 내부, 쿠버네티스 클러스터 내부 등 서비스 간에 발생하는 어플리케이션 통신에 대한 가시성과 통제력을 경계하기는 어렵다. 경계를 통과한 위협이 내부망 안에서 자유롭게 확산(Lateral Movement)하는 것을 막기 어려운 구조이다. 결국, 암묵적인 신뢰에 기반한 기존의 방식으로는 동적으로 변화하고 분산된 현대의 애플리케이션과 워크로드를 더 이상 효과적으로 보호할 수 없게 된 것이다.

미국의 CISA 가 발표한 제로 트러스트 성숙도 모델 역시 이러한 변화를 반영하여 '어플리케이션 및 워크로드'를 핵심 필러로 지정하고, 성숙도 진화 경로를 제시한다. 이 모델에 따르면, 성숙한 제로트러스트 환경은 단순히 경계를 방어하는 수준을 넘어, 애플리케이션 수준의 마이크로세그멘테이션을 통해 워크로드 간의 모든 통신을 제어하고, 보안 SDLC 를 구현하여 개발 생명주기 전반에 보안을 내재화해야 한다고 강조한다. 국내 KISA 의 제로 트러스트 가이드라인 또한 어플리케이션 및 워크로드를 주요 필러로 정의하며, 국내 IT 환경과 규제에 맞는 보안 체계 구축의 중요성을 반복해서 강조하고 있다.

따라서 제로트러스트 환경에서 어플리케이션 및 워크로드 필러는 개별 애플리케이션의 보안을 강화하는 수준을 넘어, 서로 다른 환경에서 운영되는 서비스들을 일관된 정책과 중앙화된 가시성을 통해 통합 관리하는 데 핵심적인 의미가 있다. 이는 소프트웨어 개발 생명주기(SDLC) 초기 단계부터 보안을 내재화하는 'Shift Left' 접근을 통해 애플리케이션 자체의 신뢰도를 확보하고, 접근하는 주체의 컨텍스트와 API 호출의 적정성 등 모든 상호작용을 지속적으로 검증하여, 조직의 핵심 자산과 서비스를 안전하게 보호하는 실질적인 통제 체계를 구현하는 것을 목표로 해야 한다.

■ 애플리케이션 및 워크로드 (Application&Wokrdload) 필러의 주요 요소

애플리케이션 및 워크로드 필러는 제로트러스트 아키텍처 내에서 조직의 비즈니스 로직이 실행되고 데이터가 실질적으로 처리되는 동적인 영역을 보호하는 데 중점을 둔다. 온프레미스 데이터센터를 넘어 클라우드, 컨테이너, 서버리스 등 다양한 환경에 분산된 애플리케이션과 API 는 과거 경계 기반 보안 모델로는 더 이상 효과적으로 통제하기 어렵다.

특히 제로트러스트 환경에서는 애플리케이션의 위치가 아닌, 애플리케이션 자체의 신뢰도와 접근하는 주체, API 호출의 적정성 등 모든 상호작용을 지속적으로 검증해야 한다. 이를 위해 애플리케이션 인벤토리, 위험 관리, 접근 관리, 보안 테스트, 소프트웨어 개발 및 통합, 정책 및 통합 등 애플리케이션 필러 기준의 여러 관리적·기술적 요소들이 상호 유기적으로 결합되어야만, 조직의 핵심 비즈니스 로직과 데이터를 안전하게 보호하고 서비스의 무결성을 확보할 수 있다.

아래는 애플리케이션 필러의 주요 요소들과, 이를 구현하기 위한 구체적인 관리·기술 방안을 제로트러스트 성숙도 관점에서 정리한 내용이다.

1. 애플리케이션 인벤토리

제로트러스트 환경에서 애플리케이션 인벤토리 관리는 조직 내에서 운영되는 모든 응용 프로그램, 조직에서 공급하는 응용 프로그램, API 등을 식별하고 그 현황을 항상 최신으로 유지하는 애플리케이션 보안 관리의 출발점이다. 관리 범위는 자체적으로 개발한 업무 시스템이 운영되는 온프레미스 환경뿐만 아니라, 클라우드 서비스, SaaS 등을 포괄하며, 이들 모두를 통합된 자산관리 체계 내에서 목록화해야 한다. 이는 목록을 단순히 유지하는 수준을 넘어, CI/CD 파이프라인과 연계하여 애플리케이션의 생성, 배포, 변경, 폐기에 이르는 전체 생명주기에 걸쳐 주요 속성과 상태 정보가 실시간으로 갱신되는 동적 인벤토리 관리 체계를 의미한다.

정확한 인벤토리 관리를 위해서는 모든 애플리케이션에 대해 책임과 역할을 명확히 하는 소유자 관리가 이루어져야 하며, 비즈니스 영향도와 처리하는 정보의 민감도를 기준으로 중요도 관리 체계가 수립되어야 한다. 이렇게 정의된 소유자 및 중요도 정보는 향후 위험 평가, 접근 권한 부여, 취약점 조치 우선순위 결정 등 보안 활동의 객관적인 기준으로 활용된다. 성숙도가 높은 조직에서는 이러한 중요도에 따라 패치 확인이나 소스코드 점검과 같은 보안 활동이 자동으로 수행될 수 있다.

최적화된 애플리케이션 인벤토리 관리체계는 수동 관리를 벗어나 관리 시스템을 통해 자동화되며, 최종적으로는 모든 애플리케이션의 변화가 정책에 따라 시스템에 자동 등록되고 모니터링 시스템과 연동되어 실시간 가시성을 제공해야 한다. 이렇게 확보된 정보는 정교한 접근 제어, 신속한 취약점 관리, 효율적인 보안 정책 배포를 가능하게 함으로써 제로트러스트 실현의 핵심 기반으로 작동한다.

2. 애플리케이션 위험 관리

제로트러스트 환경에서 애플리케이션 위험 관리는 소프트웨어에 내재된 위험 요소를 지속적으로 식별하고 조치하여 공격 표면을 최소화하는 핵심적인 활동이다. 공격자가 악용할 경우, 애플리케이션에 존재하는 취약점을 이용해 정보 유출, 권한 상승과 같은 심각한 침해사고로 이어질 수 있으며, 널리 사용되는 오픈소스 라이브러리에 포함된 보안 약점 또한 조직 전체를 위험에 빠뜨릴 수 있다. 따라서 개발 단계부터 운영에 이르기까지 전 과정에 걸쳐 잠재적 위험을 체계적으로 관리하는 것이 필수적이다.

취약점 조치는 운영 전환 이전에 개발 애플리케이션을 점검하는 수준으로는 한계가 있다. 성숙한 제로트러스트 환경에서는 소스코드 점검을 포함하여 개발 애플리케이션의 취약점을 지속적으로 관리하며, 운영 중에도 정기적인 점검을 통해 발견된 취약점을 자동화된 프로세스로 처리한다. 또한, 직접 수정이 어려운 상용 애플리케이션의 경우, 취약점 발견 시 IAM, Micro-Segmentation 등과 같은 시스템과 연계해 해당 애플리케이션의 계정과 권한을 회수하거나, 애플리케이션을 격리하는 등 보완 통제를 적용하여 위험을 완화해야 한다.

오픈소스 관리 또한 현대 애플리케이션 개발 환경에서 매우 중요하다. 오픈소스는 빠른 개발과 협업을 가능하게 하지만, 라이선스 이슈나 잠재적인 보안 위협을 내포할 수 있다. 초기에는 수동으로 라이선스와 취약점을 관리할 수 있으나, 점차 오픈소스 통합 관리 시스템을 통해 라이선스, SBoM(Software Bill of Materials), 외부 취약점 DB 등과 연계해 체계적으로 운영해야 한다. 최적화된 단계에서는 머신러닝을 통해 취약점을 점검하고 소스코드 수정을 자동화하여 관리함으로써, 오픈소스로부터 발생하는 위협을 선제적으로 통제할 수 있다.

3. 애플리케이션 접근 관리

제로트러스트 환경에서 애플리케이션 접근 관리는 단순히 로그인 성공 여부를 판단하는 것을 넘어, 인증된 사용자가 허용된 범위 내에서만 작업을 수행하도록 지속적으로 통제하고 모든 활동을 기록하여 위협을 차단하는 포괄적인 과정을 의미한다. 이는 애플리케이션에 대한 인증을 강화하고, 역할에 기반한 세밀한 권한을 부여하며, 모든 접근 이력을 관리하고, 애플리케이션 간 불필요한 통로를 차단하여 잠재적인 횡적 이동을 방지하는 것을 포함한다.

애플리케이션 인증 및 접근 관리는 기존의 1 차 인증만 수행하는 단계에 그치지 않고, 사용자의 역할과 부서 등 컨텍스트를 연동하여 메뉴 접근부터 조회, 수정, 삭제와 같은 세부 기능까지 권한을 분류하여 관리하는 방향으로 나아가야 한다. 일반적으로 SSO 나 정보보안포탈을 통해 구현되며 최적화된 제로트러스트 환경에서는 SDP 와 같은 기술로 사용자가 애플리케이션 서버에 직접 접근하기 전에 컨트롤러에서 보안 패킷과 단말 정보를 먼저 검증하는 선 인증 접속 방식을 도입하면 보안성을 근본적으로 강화할 수 있다.

이러한 모든 통제는 투명한 애플리케이션 접근 이력 관리를 통해 완성된다. 초기에는 애플리케이션 자체적으로 로그인 정보만 관리하는 수준에 머무를 수 있으나, 점차 SSO 로그인을 포함한 메뉴 조회, 데이터 생성·수정·삭제(CRUD) 이력까지 개별적으로 관리해야 한다. 궁극적으로는 통합 접근 관리 시스템을 활용하여 모든 애플리케이션의 접근 통제 이력을 중앙에서 통합 관리함으로써, 전사적인 가시성을 확보하고 신속한 위협 추적 및 분석을 지원해야 한다.

더 나아가, 제로트러스트는 애플리케이션 간 횡적 확산 및 우회 접속 차단을 매우 중요하게 다룬다. 초기 대응으로는 연동 API 나 소스코드 개발 시 취약점을 제거하고 DB Link 사용을 금지하는 정책을 적용할 수 있다. 하지만 보다 근본적인 통제를 위해서는 시스템 내에서 애플리케이션 단위로 개별 방화벽을 설정하는 것과 같은 Micro-Segmentation 을 적용하여 불필요한 횡적 확산과 우회 접속 경로를 원천적으로 차단해야 한다. 최적화된 환경에서는 이를 통합 모니터링 시스템과 연동하여 횡적 이동 시도와 같은 이상 행위를 지속적으로 탐지하고 대응하는 체계를 갖추게 된다.

4. 애플리케이션 보안 테스트

제로트러스트 환경에서 애플리케이션 보안 테스트는 개발 생명주기 초기에 보안을 내재화하는 'Shift Left' 개념을 실현하는 핵심적인 활동이다. 단순히 운영 단계의 보안에만 의존하는 것이 아니라, 개발 과정에서부터 코드 레벨의 취약점을 찾아 수정하고, 런타임 환경에서 발생할 수 있는 잠재적 위협을 사전에 식별하여 제거함으로써 애플리케이션 자체의 신뢰도를 확보하는 것을 목표로 한다.

정적 애플리케이션 보안 테스트(SAST)는 개발자의 관점에서 애플리케이션의 소스 코드, 바이너리, 바이트 코드를 직접 분석하여 SQL 인젝션이나 크로스 사이트 스크립팅(XSS)과 같은 코드 기반의 보안 취약점을 식별하는 '화이트박스' 방식이다. 초기에는 중요 애플리케이션을 대상으로 운영 전환 시점에만 수동으로 점검을 수행할 수 있었다. 이후, 성숙한 조직은 개발 생명주기 전반에 걸쳐 주기적인 점검을 자동화하고, 코딩과 설계 단계부터 보안 결함을 검증하여 개발 초기부터 보안을 보장하는 체계를 갖추어야 한다.

이와 상호 보완적으로 동적 애플리케이션 보안 테스트(DAST)는 실제 운영 중인 애플리케이션을 외부 공격자의 관점에서 분석하는 '블랙박스' 방식이다. 소스 코드 접근 없이 실제 요청과 응답을 분석하여 세션 관리 문제나 서버 설정 오류와 같은 런타임 환경의 취약점을 파악하는 데 효과적이다. 성숙도가 높아질수록 주기적인 분석을 넘어, 외부 공격을 지속적으로 시뮬레이션하고 테스트하며 애플리케이션의 보안 상태를 상시적으로 검증하는 단계로 발전해야 한다.

최근에는 SAST 와 DAST 뿐만 아니라, 오픈소스 라이브러리의 취약점을 분석하는 SCA(Software Composition Analysis, 소프트웨어 구성 분석)까지 애플리케이션 보안 테스트의 필수 요소로 여겨지고 있다. 이 세 가지 핵심 테스트 방식(SAST, DAST, SCA)을 개별적으로 운영하기보다는, 이들을 모두 지원하는 통합 애플리케이션 보안 테스트 플랫폼을 통해 SDLC(소프트웨어 생명주기) 정책에 반영하고 CI/CD 파이프라인에 보안을 완벽하게 내재화해 개발부터 배포, 운영까지 전 과정에 걸쳐 일관된 보안 관리를 수행하는 것이 최신 동향이다.

5. 리소스 승인 및 통합

제로트러스트 환경에서 리소스 승인 및 통합은 사용자가 인증 후에 애플리케이션 내부의 특정 기능이나 데이터에 접근할 때, 사전에 정의되고 승인된 권한만을 부여하는 핵심적인 통제 활동이다. 이는 단순히 로그인 성공 여부로 모든 기능을 허용하는 것이 아니라, 최소 권한 원칙에 따라 사용자의 역할과 책임에 맞는 최소한의 리소스 접근만을 허용함으로써 내부 위협과 권한 오남용의 위험을 크게 줄이는 것을 목표로 한다.

애플리케이션 승인 절차는 조직의 제로트러스트 성숙도에 따라 발전한다. 초기 단계에서는 별도의 리소스 승인 없이 로그인만으로 애플리케이션의 모든 기능에 접근하거나, 일부 애플리케이션에 한해 제한적인 접근 권한을 부여하는 수준에 머무를 수 있다. 성숙한 단계로 나아가기 위해서는 개별 애플리케이션별로 화면, 기능, 배치 작업 등 각각의 리소스에 대해 정식 승인 절차를 거쳐 접근 권한을 부여하는 체계를 갖추어야 한다.

최적화된 제로트러스트 환경에서는 이러한 승인 절차를 부서, 역할, 사용자별로 더욱 세분화하고, 모든 애플리케이션에 걸쳐 일관된 정책으로 통합 관리한다. 이를 통해 특정 사용자는 어떤 애플리케이션을 사용하더라도 자신의 역할에 맞는 특정 기능과 데이터에만 접근할 수 있게 되며, 이는 중앙화된 접근 관리 시스템(IAM, ICAM)을 통해 체계적으로 통제된다.

6. 소프트웨어 개발 및 통합

제로트러스트 환경에서 소프트웨어 개발 및 통합은 보안을 개발 생명주기의 가장 첫 단계부터 내재화하는 'Shift Left' 원칙을 적용하는 핵심적인 과정이다. 이는 단순히 완성된 애플리케이션의 취약점을 점검하는 것을 넘어, 코드를 작성하는 순간부터 안전한 코딩 규칙을 준수하고, 개발 과정에서 활용되는 외부 플랫폼과 오픈소스의 위협까지 체계적으로 관리하여 잠재적 위험 요소를 원천적으로 제거하는 것을 목표로 한다.

시큐어 코딩은 개발 과정에서 발생할 수 있는 보안 취약점을 최소화하기 위한 일련의 보안 활동을 의미하며, 안전한 소프트웨어를 개발하기 위해 지켜야 할 코딩 규칙과 소스코드 취약점 목록을 포함한다. 초기에는 개발자 대상의 교육과 자료 전달에 의존할 수 있으나, 보다 성숙한 단계에서는 시큐어 코딩 점검 시스템을 통해 개발 단계별로 코딩 취약점을 점검하고 조치해야 한다. 최적화된 환경은 개발자의 보안 인식을 높이기 위한 지속적인 교육과 함께, 기술적으로 시스템을 활용한 개발 단계별 점검 및 조치를 병행하여 문화와 기술 양측면에서 안전한 개발 환경을 보장할 수 있어야 한다.

또한, 현대 개발 환경은 깃허브(GitHub)와 같은 외부 소스코드 호스팅 서비스 및 오픈소스 활용이 필수적이므로, 이에 대한 위협 여부 탐지 체계를 갖추는 것이 매우 중요하다. 이러한 외부 플랫폼은 해커의 공격 발판으로 악용되거나 플랫폼 자체의 취약점에 노출될 수 있다. 단순히 외부 개발 환경 사용을 금지하는 정책은 비공식적인 사용(Shadow IT)을 낳을 수 있으므로 효과적이지 않다. 따라서 주기적으로 오픈소스 통제와 라이선스를 관리하는 단계를 거쳐, 최종적으로는 주기적인 취약점 통제 및 조치와 함께 실시간 모니터링을 수행하여 외부 개발 환경으로부터 유입될 수 있는 위협에 선제적으로 대응해야 한다.

7. 소프트웨어 개발 생명주기(SDLC) 및 지속적인 통합과 배포(CI/CD)

제로트러스트 환경에서 CI/CD(지속적 통합/지속적 배포) 파이프라인은 단순히 개발 생산성을 높이는 자동화 도구를 넘어, 조직의 보안 소프트웨어 개발 생명주기(SDLC) 정책을 체계적으로 이행하고 강제하는 핵심 프레임워크 역할을 수행한다. 이는 개발자가 코드를 공유 저장소에 병합하는 순간부터 빌드, 테스트, 배포, 그리고 운영에 이르기까지 전 과정에 걸쳐 보안을 내재화하고, 수동 개입으로 인한 오류와 보안 공백을 최소화하여 신뢰할 수 있는 소프트웨어를 지속적으로 제공하는 것을 목표로 한다.

이러한 보안 SDLC 의 첫 단계는 안전한 코드 통합에서 시작된다. 초기에는 관리자가 여러 개발자의 코드를 수동으로 점검하고 빌드할 수 있으나, 성숙한 조직은 CI 서버를 통해 코드 통합 프로세스를 자동화하고, 코드 검사 도구와 테스트 프레임워크를 연동하여 코드 병합 과정에서부터 보안 검증을 자동으로 수행한다. 이어서 보안 빌드 프로세스는 통합된 코드를 검사하고 오픈소스 라이브러리 취약점 및 SQL 인젝션과 같은 공격을 사전에 탐지하는 단계를 거친다. 최적화된 환경에서는 빌드의 결과물인 아티팩트에 GPG 서명과 같은 암호화 기술을 적용하여 위변조를 방지하고, 배포 전 서명 검증을 통해 무결성을 보장한다.

이렇게 생성된 결과물은 보안 아티팩트 관리 체계에 따라 안전하게 관리되어야 한다. 단순히 특정 매체에 저장하는 단계를 넘어, 전용 시스템을 통해 버전 관리, 서명 검증, 접근 제어를 수행하고, 최종적으로는 암호화된 보안 저장소에서 체계적으로 관리되어야 한다. 보안 배포 프로세스 역시 수동 배포의 위험성을 제거하고 자동화를 지향한다. 성숙한 파이프라인은 배포 전 변경 영향 분석과 보안 취약점 평가를 포함한 공식적인 검토 및 승인 프로세스를 거치며, 승인된 빌드는 아티팩트의 서명을 검증한 뒤 배포 자동화 도구로 자동 배포된다.

소프트웨어 배포 이후에도 제로트러스트 원칙은 지속적인 모니터링 및 감사를 통해 유지된다. 문제 발생 시 수동으로 로그를 분석하는 단계를 벗어나, SIEM 과 같은 시스템과 연동하여 로그를 중앙에서 수집하고 위협을 식별하며, 최적화된 단계에서는 머신러닝과 AI 를 활용하여 잠재적 위협을 예측하고 선제적으로 조치한다. 마지막으로, 이 모든 기술적 통제는 사람, 즉 개발자를 위한 보안 교육으로 완성된다. 조직 내 보안 인식 문화를 촉진하기 위해 주기적인 교육을 실시하고, 이를 자동화된 시스템으로 관리하며, 보안 교육을 수료한 개발자만이 개발에 참여하도록 통제하는 것이 가장 성숙한 보안 SDLC 의 모습이다.

8. 클라우드 워크로드 보호

제로트러스트 환경에서 클라우드 워크로드 보호는 동적으로 생성·변경·소멸하는 클라우드 자원(가상머신, 컨테이너 등)의 특성을 이해하고, 애플리케이션과 데이터가 실행되는 전 과정을 보호하는 것을 목표로 한다. 온프레미스와 달리 물리적 통제가 어려운 클라우드 환경에서는 구성 오류, 취약점, 시스템 무결성 훼손, 악성코드 감염 등이 더 심각한 위협으로 작용할 수 있으므로, 다층적이고 자동화된 보안 체계가 필수적이다.

워크로드 보호의 기반은 강화, 구성, 취약점 관리에서 시작된다. 초기에는 온프레미스에서 사용하던 점검 도구를 활용할 수 있으나, 성숙한 단계에서는 여러 클라우드 환경을 단일 콘솔에서 통합 관리하며 워크로드의 시스템 구성과 애플리케이션/운영체제 취약점을 지속적으로 점검하고 확인해야 한다. 또한, 클라우드 네트워크 방화벽, 가시성, 세분화를 통해 기존의 물리적 네트워크 관리에서 벗어나 SDN(소프트웨어 정의 네트워크)을 기반으로 워크로드 단위의 방화벽 기능을 제공하고, 이를 통해 각 워크로드를 외부 위협으로부터 보호하고 모니터링해야 한다.

더 나아가 시스템 무결성 보증을 위해 워크로드의 환경 설정 및 구성, 권한 등을 실시간으로 모니터링하고, 이상 발생 시 자동으로 조치하는 체계를 갖추어야 한다. 애플리케이션 제어 및 허용 목록 관리 역시 중요하다. 단순히 블랙리스트 기반으로 차단하는 것을 넘어, 중앙 관리 시스템을 통해 화이트리스트 기반으로 허용된 애플리케이션만 실행되도록 제어하고, 승인 절차와 연동하여 허가된 애플리케이션을 자동으로 적용하는 것이 바람직하다.

이러한 기반 위에 악용 방지 및 메모리 보호, 호스트 기반 침입 방지, 멀웨어 방지 스캐닝과 같은 능동적인 위협 대응 기술이 적용되어야 한다. 성숙한 제로트러스트 환경에서는 알려진 위협은 물론, 알려지지 않은 위협과 파일리스 공격까지 방어하기 위해 머신러닝과 샌드박스 기술을 활용하며, 위협 탐지 시 대상을 자동으로 격리하는 등 자동화된 대응을 수행한다. 이 모든 활동의 중심에는 엔드포인트 감지 및 대응(EDR)과 행동 모니터링이 있다. 개별 백신 프로그램을 넘어, 중앙 관리 시스템을 통해 클라우드 환경 내 모든 워크로드의 행위를 모니터링하고, 위협 발생 시 삭제, 격리, 차단 등의 조치를 자동으로 수행하여 클라우드 환경 전반의 보안을 완성한다.

9. SaaS 관리 플랫폼(SMP)

제로트러스트 환경에서 SaaS 관리 플랫폼(SMP, SaaS Management Platform)은 조직 내에서 사용하는 모든 서비스형 소프트웨어(SaaS) 애플리케이션을 중앙에서 통합적으로 관리하고 운영하는 역할을 수행한다. 클라우드 기반 SaaS 애플리케이션의 도입이 증가하면서 관리되지 않는 Saas 가 늘어나고, 개별 서비스마다 운영 및 보안 정책이 분산되어 일관성을 유지하기 어려워지는 문제가 발생한다. SMP 는 이러한 문제를 해결하기 위해 모든 SaaS 애플리케이션의 사용 현황, 관리, 보안 정보를 단일 대시보드에 집계하여 제공한다.

성숙한 제로트러스트 환경에서의 체계적인 SaaS 관리는 단순히 사용 현황을 추적하는 것에서 그치지 않는다. SMP 는 IAM 시스템 등과 연동하여 현재 사용 중인 모든 SaaS 애플리케이션을 추적하고, 누가 어떤 애플리케이션을 얼마나 자주 사용하는지에 대한 정보를 집계한다. 최적화된 단계에서는 라이선스 관리, 사용자 온보딩 및 오프보딩, 애플리케이션 내 사용자 그룹 관리와 같은 운영 작업을 중앙에서 직접 수행하여 관리 효율성을 극대화한다.

또한, SMP 는 보안 및 규정 준수를 위한 중앙 제어 센터로 기능한다. 개별 SaaS 애플리케이션에 일일이 접속하여 보안 설정을 관리하는 대신, SMP 를 통해 데이터 보호, 접근 제어 및 기타 보안 설정을 중앙에서 일괄적으로 적용하고 관리할 수 있다. 이를 통해 조직의 보안 규정과 지침을 실시간으로 모든 SaaS 애플리케이션에 최신화하고 일관되게 운영함으로써, 분산된 클라우드 환경 전반에 제로트러스트 원칙을 효과적으로 확장할 수 있다.

최근에는 이러한 SaaS 관리에 SMP 보안 기능을 포함하여, 더 넓은 클라우드 보안 프레임워크를 구현하는 추세가 나타나고 있다. 예를 들어, SASE(보안 액세스 서비스 엣지) 와 같은 통합 보안 시스템은 내재된 CASB(클라우드 접근 보안 브로커) 기능을 통해 SaaS 가시성을 확보하고 데이터 보안 정책을 적용하는 역할을 수행한다. 더 나아가 성숙한 클라우드 보안 전략은 IaaS, PaaS 인프라의 형상을 관리하는 CSPM(클라우드 보안 형상 관리), 가상머신이나 컨테이너 등 실제 워크로드를 보호하는 CWPP(클라우드 워크로드 보호 플랫폼) 기능까지 통합하여, 인프라부터 워크로드, SaaS 애플리케이션 접근에 이르기까지 일관된 제로트러스트 보안을 적용한다.

10. 보안 액세스 서비스 엣지(SASE)

제로트러스트 아키텍처에서 SASE(Secure Access Service Edge)는 특정 시스템이나 솔루션을 지칭하기도 하지만, 개념적으로 이해하면 분산된 사용자와 클라우드 중심의 업무 환경에 맞춰 네트워크와 보안을 클라우드 기반의 단일 서비스로 통합하여 제공하는 보안 프레임워크로 이해해야 한다. 즉, 제로트러스트를 효과적으로 구현하기 위해 클라우드 엣지에서 반드시 수행되어야 할 핵심 기능들의 집합이다. SASE 는 사용자의 위치에 상관없이 모든 리소스에 대해 일관되고 강력한 보안을 적용하는 것을 목표로 한다.

SASE 프레임워크의 네트워킹 기반은 고급 SD-WAN 기능으로, 하드웨어에서 추상화된 가상 네트워크 오버레이를 생성하여 분산된 조직 환경에서도 데이터센터 및 클라우드 애플리케이션에 안정적이고 빠른 연결을 보장한다. 제로트러스트 관점에서 잘 구성된 SD-WAN 은 트래픽을 지능적으로 라우팅하여 모든 연결이 보안 검사를 위해 SASE 의 클라우드 인프라를 거치도록 하는 토대를 마련한다.

SASE 프레임워크의 네트워킹 기반은 고급 SD-WAN 기능으로, 하드웨어에서 추상화된 가상 네트워크 오버레이를 생성하여 분산된 조직 환경에서도 데이터센터 및 클라우드 애플리케이션에 안정적이고 빠른 연결을 보장한다. 제로트러스트 관점에서 잘 구성된 SD-WAN 은 트래픽을 지능적으로 라우팅하여 모든 연결이 보안 검사를 위해 SASE 의 클라우드 인프라를 거치도록 하는 토대를 마련한다.

SASE 의 핵심 접근 제어 모델은 제로 트러스트 네트워크 액세스(ZTNA) 이다. 이는 기존 VPN 을 대체하는 기술로, 어떤 사용자나 기기도 기본적으로 신뢰하지 않는다는 원칙하에 최소 권한 액세스를 지원한다. 성숙한 ZTNA 는 단순히 초기 접근 인증에서 그치지 않고, 접속 후에도 사용자의 행위에서 이상 징후가 탐지되면 자동으로 추가 인증을 요구하거나 세션을 차단하는 등 지속적인 검증을 수행한다.

또한 SASE 는 클라우드 및 웹 트래픽을 보호하기 위한 다양한 보안 기능을 통합한다. 대표적인 기능은 CASB(클라우드 접근 보안 브로커) 보안 정책을 통해 클라우드 애플리케이션의 가시성을 확보하고 민감 데이터를 보호하는 기능이다. 해당 기능은 아래 별도의 항목에서 조금 더 자세히 다룰 예정이다.

보안 웹 게이트웨이(SWG)는 웹으로 향하는 모든 사용자 트래픽을 검사하여 멀웨어나 악성코드를 필터링하고 조직의 보안 정책을 강제하는 역할을 한다. 성숙한 SWG 는 단순 URL 필터링을 넘어, 실시간 위협 인텔리전스 DB 와 연동하여 알려지지 않은 위협까지 차단하고, 맬웨어 방지 스캔, 애플리케이션 제어 기능까지 통합하여 포괄적인 웹 위협 방어 체계를 구축한다.

서비스형 방화벽(FWaaS)은 클라우드에서 제공되는 차세대 방화벽(NGFW) 기능이다. 이는 URL 필터링, IPS, DNS 보안과 같은 고급 L7 제어 기능을 포함하며, 물리적인 방화벽 장비 없이도 모든 네트워크 경계를 사이버 위협으로부터 보호한다. 성숙한 SASE 프레임워크 기반의 FWaaS 는 일부 중요 서버만이 아닌, 조직의 전체 네트워크 경계를 포괄적으로 보호하는 역할을 수행한다. 이처럼 SASE 는 여러 핵심 보안 기능들을 유기적으로 결합하여 제로트러스트 원칙을 네트워크 엣지 단에서 실현하는 통합 프레임워크로 기능한다.

11. 클라우드 엑세스 보안 브로커(CASB)

CASB(클라우드 액세스 보안 브로커)는 클라우드 서비스 사용자와 클라우드 서비스 제공자 사이에 위치하여, 온프레미스 기반의 조직의 보안 정책을 클라우드 기반 리소스까지 확장하고 일관되게 적용하는 핵심적인 보안 정책 시행 지점이다. 제로트러스트 환경에서 CASB 는 조직이 통제하기 어려운 외부 클라우드 서비스에 대한 가시성을 확보하고, 데이터 보안과 위협 방지, 컴플라이언스 준수를 가능하게 하는 중추적인 역할을 수행한다.

CASB 의 가장 기본적인 기능은 클라우드 가시성 확보다. 성숙한 CASB 는 인증, 암호화, 악성코드 탐지 등 모든 클라우드 보안 영역의 현황을 실시간 대시보드로 제공하여, 조직 내에서 어떤 클라우드 서비스가 어떻게 사용되고 있는지에 대한 완전한 가시성을 제공한다. 이를 통해 관리되지 않는 'Shadow IT'를 탐지하고 통제할 수 있다.

확보된 가시성을 기반해 클라우드 데이터 보안 기능이 작동한다. CASB 의 핵심 구성 요소인 DLP(데이터 손실 방지)는 클라우드 내에서 저장되거나 이동하는 모든 데이터에 대해 기업의 보안 정책을 확장 적용한다. 최적화된 환경에서는 DLP 뿐만 아니라 암호화, 데이터 유출 관련 이상 행위 탐지 기능까지 통합 운영하고 지속적으로 모니터링하여 데이터 유출 위험을 최소화한다.

또한 CASB 는 강력한 위협 방지 기능을 제공한다. 일반적인 사용자 사용 패턴을 분석하여 비정상적인 활동을 식별하고, 적응형 접근 제어 및 악성코드 탐지 기능을 활용하여 내부 및 외부 위협으로부터 조직을 보호한다. 성숙한 CASB 시스템은 접근 제어, 악성코드 탐지, 암호화 등 다양한 보안 위협에 대해 실시간 탐지 및 모니터링 체계를 운영한다. 마지막으로, 컴플라이언스 준수는 CASB 의 중요한 역할 중 하나다. 조직은 CASB 를 통해 데이터 3 법, PCI DSS, HIPAA 와 같은 다양한 규제 표준 준수 여부를 모니터링할 수 있으며, 최적화된 단계에서는 자동화된 시스템으로 각종 규정 요구사항을 상시 만족시키며 운영한다.

12. 정책 및 프로세스

제로트러스트 환경에서 정책 및 프로세스는 다양하게 분산된 애플리케이션과 워크로드를 일관된 보안 수준으로 관리하기 위한 최상위 거버넌스 체계이다. 효과적인 통제를 위해서는 먼저 용어를 통일하고 정책을 통합하는 과정이 필수적이다. 각기 다른 팀이나 환경에서 서로 다른 기준과 절차를 따른다면 제로트러스트의 핵심인 일관성 있는 보안 정책 적용이 불가능하기 때문이다.

성숙한 정책 및 프로세스 정의는 조직의 비즈니스 구조와 서비스 방향성을 반영하여 수립되어야 하며, 컴플라이언스 준수와 업무 효율성을 모두 고려해야 한다. 초기에는 표준화된 정책 없이 필요시마다 절차를 정의하거나, 기본적인 정책이 있더라도 현행화가 이루어지지 않는 단계에 머무를 수 있다. 하지만 제로트러스트를 지향하기 위해서는 명확한 정책과 프로세스를 정의하고, 이를 준수하도록 지속적인 통제가 이루어져야 한다.

최적화된 단계에서는 이러한 정책과 프로세스가 일부 수기 작업에 의존하는 것을 넘어, 시스템으로 자동화되어 모든 애플리케이션과 워크로드에 명확하게 적용된다. 또한, 실시간 모니터링 체계를 통해 정책 준수 여부를 상시 확인하고, 변화관리가 이루어지는 선순환 구조를 갖추어야 한다. 이렇게 잘 정의되고 통합된 정책과 프로세스는 다른 모든 기술적 통제를 하나로 묶어주는 거버넌스 역할을 수행하며, 조직 전체의 보안 수준을 실질적으로 향상시키는 기반이 된다.

이처럼 어플리케이션 및 워크로드 필러는 제로트러스트 아키텍처에서 가장 방대한 영역을 다루고 있으며, 위에서 다룬 주요 요소 SMP, SASE, CASB 등은 솔루션으로 맵핑될 수 있으며 적용 범위가 조직마다 다르게 정의되거나 기능이 중복될 수 있어 명확한 접근이 필요하다. 따라서 조직은 먼저 관리해야 할 영역을 정확히 식별하고, 위에서 다룬 주요 요소들을 기반으로 일관된 정책과 프로세스를 수립하는 것이 무엇보다 중요하다.

애플리케이션 및 워크로드 필러의 고도화는 조직의 전체 소프트웨어 생명 주기에 제로트러스트 원칙을 일관되게 적용할 수 있는 관리 체계와 기술적 토대를 마련하여, 각 애플리케이션 단위에서 발생할 수 있는 위협을 사전에 방지하고 신속하게 대응할 수 있는 환경을 실현하게 한다. 또한, 이 필러의 효과적인 구현은 조직 내 핵심 비즈니스 로직과 데이터가 처리되는 지점을 직접적으로 보호하고, 변화하는 IT 환경과 갈수록 정교해지는 사이버 위협으로부터 조직의 핵심 서비스를 효과적으로 방어하는 데 필수적인 역할을 수행한다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행할 수 있는 시스템이 필수적이다. 제로트러스트 아키텍처는 "신뢰하지 않고 항상 검증한다"는 원칙을 기반으로 하며, 이를 실현하기 위해 각 시스템 별 상태를 확인하고, 지속적으로 검증하며, 최소 권한 접근 보장 등을 수행하는 시스템을 갖춰야 한다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 중요한 역할을 담당하며, 이들 시스템은 상호 연계되어 조직의 보안 태세를 강화할 수 있다. 각 시스템 별로 제로트러스트 환경 구현을 위해 수행해야 할 기능과 이를 통해 조직이 얻을 수 있는 보안 강화 효과를 구체적으로 살펴보고자 한다.

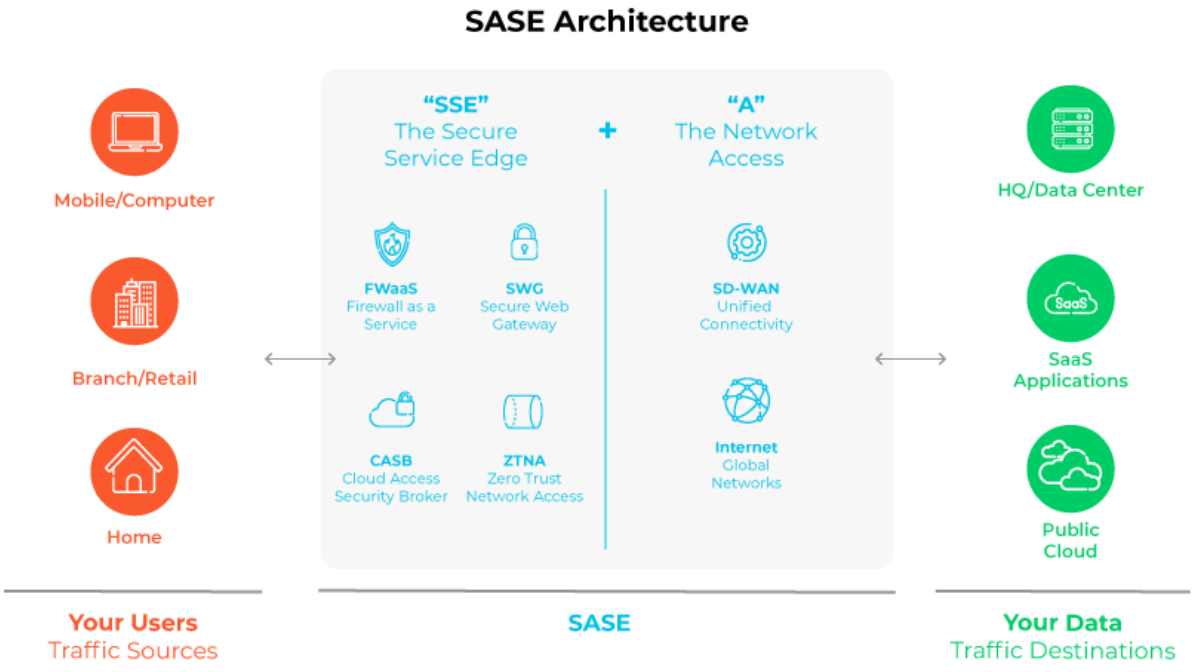
출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

그림 2. 어플리케이션 필러 주요 시스템

1. SASE (Secure Access Service Edge, 보안 액세스 서비스 엣지)

SASE 는 기존의 온프레미스 중심 네트워크 및 보안 아키텍처의 한계를 극복하기 위해 등장한 클라우드 네이티브 프레임워크이다. 이는 사용자와 기기가 어디에 있든, 애플리케이션과 데이터가 어디에 있든 관계없이 일관된 보안 정책과 최적화된 네트워크 성능을 제공하는 것을 목표로 한다. SASE 는 단순히 여러 보안 시스템을 합친 것이 아니라, 네트워크 기능과 보안 기능이 클라우드 상에서 본질적으로 융합된 구조를 가진다.

SASE 의 구조를 정확히 이해하기 위해서는 SSE(Secure Service Edge)와의 관계를 파악하는 것이 중요하다. SSE 는 클라우드를 통해 제공되는 보안 기능의 집합으로, 주로 ZTNA(제로 트러스트 네트워크 액세스), CASB(클라우드 접근 보안 브로커), SWG(보안 웹 게이트웨이), FWaaS(서비스형 방화벽)등을 핵심 구성 요소로 한다. 즉, SSE 는 '보안'에 중점을 둔다. SASE 는 이러한 SSE 의 모든 보안 기능에 A(Access)의 기능인 지능형 네트워크 기능 SD-WAN 을 결합하여 완성되는 더 넓은 개념의 프레임워크이다.



출처 : Paloalto, "SASE vs. SSE: What Is the Difference?"

그림 3. SASE Architecture

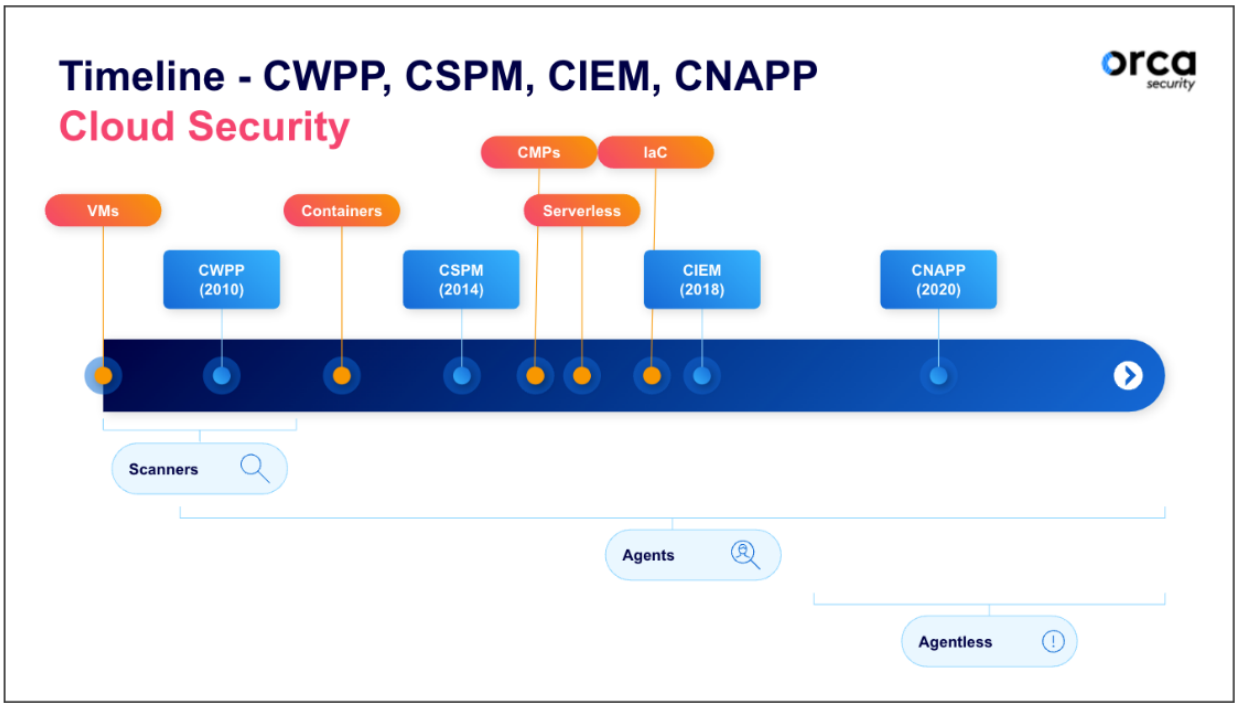
제로트러스트 관점에서 SASE 는 분산된 환경의 모든 '접근'을 통제하는 핵심적인 역할을 수행한다. 하지만 최근 기술력이 뛰어난 글로벌 기업들은 SASE 의 범위를 더욱 확장하고 있다. 글로벌 벤더의 경우 통합 플랫폼은 전통적인 SASE 의 기능을 넘어 클라우드 환경 내부를 보호하는 CNAPP(클라우드 네이티브 애플리케이션 보호 플랫폼)의 영역까지 포함하기도 한다. 즉, 하나의 플랫폼 안에서 CWPP(클라우드 워크로드 보호) 나 CSPM(클라우드 보안 형상 관리) 기능 등을 함께 제공하는 것이다. 다만, 이는 벤더의 기술력과 플랫폼 설계 역량에 따라 상이하며, 대부분 별도의 라이선스로 분리되어 제공되므로 조직의 필요에 따라 기능 범위를 신중하게 검토해야 한다.

예를 들어 팔로알토 네트웍스의 Prisma SASE 같은 플랫폼은 기본적으로 SASE 로 분류되지만, 라이선스 정책에 따라 CWPP, CSPM 등 CNAPP 의 주요 기능들을 추가하여 활용할 수 있다. 더 나아가 최근 팔로알토 네트웍스가 아이덴티티 기업인 사이버아크(CyberArk)를 인수하기로 한 것은 SASE 플랫폼이 나아가야 할 방향을 명확히 보여준다. 과거 대부분의 보안 침해가 도용된 자격 증명에서 시작되었다. 때문에 제로트러스트 아키텍처 측면에서 SASE 플랫폼에 강력한 IAM 및 특권 접근 관리(PAM) 기능을 통합하여 '접근'뿐만 아니라 '신원'까지 완벽하게 통제하는 통합 보안 플랫폼으로 진화하려는 것이다. 벤더에 따라 SASE 로 구현할 수 있는 범위는 확장될 수 있지만, 이러한 단일 플랫폼 접근 방식은 특정 벤더에 대한 종속성 심화, 각 기능별 최고 수준의 성능대비 일부 기능의 제약, 복잡한 라이선스 체계 등의 문제점을 야기할 수 있으므로 도입 시 장단점을 함께 고려해야 한다.

결론적으로 SASE 는 벤더의 기술력, 글로벌 PoP(Point of Presence) 커버리지, 실제 통합 수준에 따라 제공 기능과 품질의 차이가 크다. 따라서 도입 시에는 국내 비즈니스 환경의 특수성, 특히 망분리 정책과의 호환성을 반드시 고려해야 한다. 클라우드 기반으로 동작하는 SASE 의 특성상 망분리 환경에서는 기능이 제약될 수 있으므로, 온프레미스와의 연동 방안 등을 포함한 면밀한 아키텍처 설계가 선행되어야 한다.

2. CNAPP (Cloud-Native Application Protection Platform, 클라우드 네이티브 애플리케이션 보호 플랫폼)

CNAPP 은 복잡한 최신 클라우드 환경의 보안을 위해 등장한 통합 보안 플랫폼이다. 클라우드 네이티브 애플리케이션은 컨테이너, 인스턴스 등 동적인 기술로 구축되어 멀티·하이브리드 클라우드에 배포된다. 이러한 환경에서는 기존의 파편화된 개별 보안 시스템으로는 전체적인 가시성을 확보하기 어렵고, 보안팀은 수많은 경고 속에서 실제 위협을 식별하는 데 어려움을 겪는다. CNAPP 는 이러한 문제를 해결하기 위해 개발부터 운영까지 클라우드 애플리케이션의 전체 생명주기에 걸친 보안 기능을 단일 플랫폼에서 통합하여 제공한다.



출처 : orca security, "Know Your Cloud Security Acronyms"

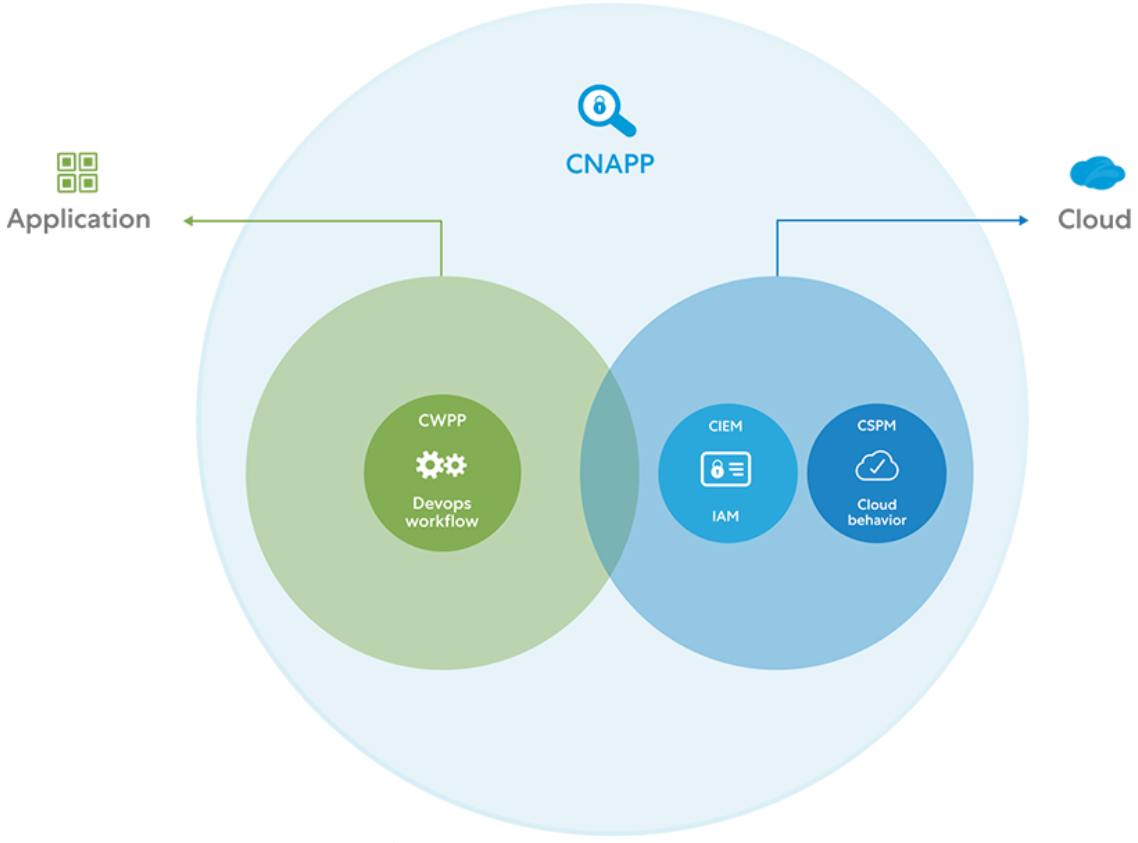
그림 4. A History of Cloud Security Technologies(by Gatner)

CNAPP 는 클라우드 보안의 진화 과정을 보여주는 개념으로, 여러 개별 보안 시스템들이 하나의 플랫폼으로 통합된 형태이다. 이 통합의 핵심 구성 요소는 다음과 같다.

(1) CSPM (Cloud Security Posture Management, 클라우드 보안 형상 관리)
클라우드 인프라의 보안 설정을 자동으로 지속 모니터링하는 기능으로 설정 오류, 정책 위반, 오픈 스토리지 버킷과 같은 규정 준수 이슈를 식별하여 클라우드 환경 자체의 안전한 보안 '태세'를 확립하고 유지하는 역할을 수행한다.

(2) CWPP (Cloud Workload Protection Platform, 클라우드 워크로드 보호 플랫폼)
가상머신, 컨테이너 등 클라우드에서 실행되는 워크로드 자체를 보호하는 데 중점을 둔다.
실시간 위협 탐지, 취약점 스캐닝, 시스템 무결성 보증 등의 기능을 통해워크로드가 동작하는 동안 발생하는 다양한 위협을 능동적으로 방어하는 역할을 수행한다.

(3) CIEM (Cloud Infrastructure Entitlement Management, 클라우드 인프라 권한 관리)
복잡한 클라우드 환경 내 사용자 및 서비스 계정의 권한을 관리하고 적용한다. 과도하게 부여되었거나 사용하지 않는 권한을 식별하고 회수함으로써 최소 권한 원칙을 실현하고 계정 탈취로 인한 위험을 근본적으로 줄이는 역할을 수행한다.



출처 : Gartner, “How to protect your clouds with CSPM, CWPP, CNAPP, and CASB”

그림 5. Cloud Technologies Simply

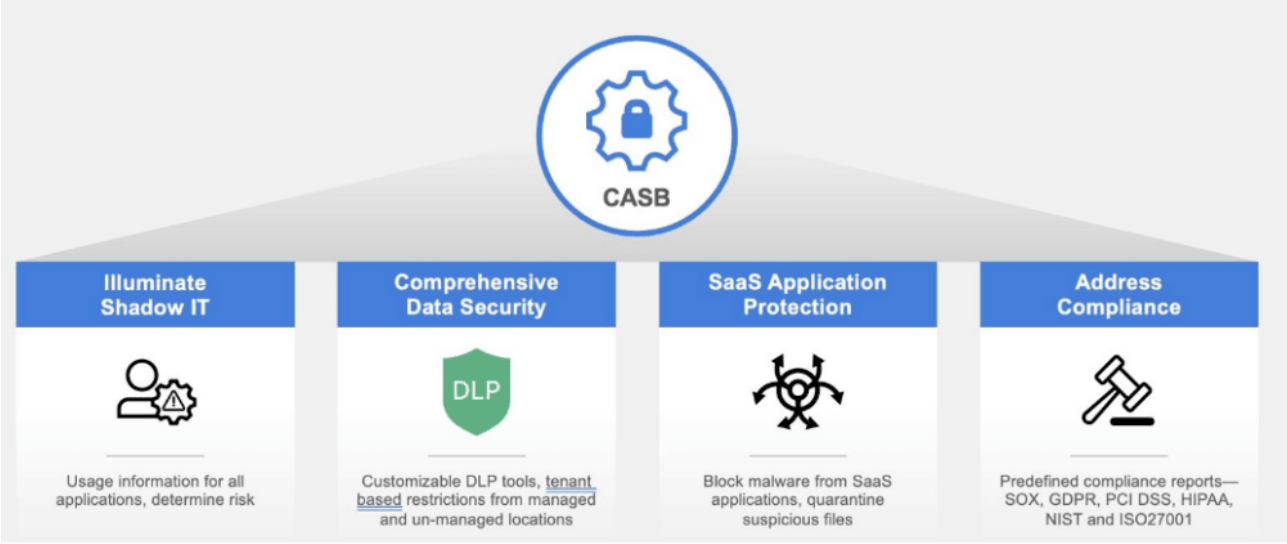
이처럼 성숙한 CNAPP 는 CSPM, CWPP, CIEM 과 같은 핵심 기능을 통합하고, 나아가 코드형 인프라(IaC) 스캐닝, 쿠버네티스 보안 형상 관리(KSPM)까지 확장하여 클라우드 기반 어플리케이션 개발 초기부터 운영까지 전반적인 보안을 책임진다.

CNAPP 의 동작 방식은 취약점, 설정 오류, 사용자 행동 등 클라우드 환경의 모든 데이터를 수집하고(침입), 비정상적이거나 알려진 위협 패턴을 분석하여(이해), 최종적으로 보안팀에 위험 우선순위가 높은 경고와 컨텍스트를 시각화하여 제공함으로써 신속한 해결을 돕는다. 이를 통해 조직은 파편화된 시스템 운영으로 인한 비효율성과 비용을 줄이고, 통합된 가시성을 바탕으로 클라우드 보안을 크게 강화할 수 있다. 제로트러스트 아키텍처에서 SASE 가 '클라우드로의 안전한 접근'을 책임진다면, CNAPP 는 '클라우드 내부의 애플리케이션과 인프라'를 안전하게 보호하는 핵심적인 역할을 수행한다.

3. CASB (Cloud Access Security Broker, 클라우드 액세스 보안 브로커)

CASB 는 클라우드 서비스 사용자와 클라우드 서비스 제공자(CSP) 사이에 위치하여, 조직의 보안 정책을 클라우드 환경까지 확장하고 일관되게 적용하는 보안 정책 시행 지점이다. 제로트러스트 아키텍처에서 SASE 가 '클라우드로의 안전한 접근 경로'를 보호하고, CNAPP 가 '클라우드 인프라와 워크로드 자체'를 보호한다면, CASB 는 '사용자와 SaaS 애플리케이션 간의 상호작용'을 안전하게 만드는 데 특화된 역할을 한다. CASB 는 SASE 프레임워크 내에 통합된 기능으로 제공되거나, 조직의 보안 요구에 따라 독립된 시스템으로 구축 및 운영될 수 있다.

CASB 의 주요 기능은 크게 네 가지로 분류된다. 첫째, 가시성 확보를 통해 조직 내에서 사용되는 모든 승인 및 비승인 클라우드 어플리케이션을 탐지하고 위험도를 평가한다. 둘째, 데이터 보안을 위해 클라우드에 저장되거나 이동하는 민감 정보에 대해 실시간 DLP(데이터 손실 방지) 정책을 집행하여 무단 공유를 차단한다. 셋째, 위협 방지를 위해 사용자 행동을 분석하여 비정상 행위를 탐지하고 랜섬웨어나 내부자 위협 등으로부터 클라우드 환경을 보호한다. 마지막으로, 규정 준수를 위해 HIPAA, PCI DSS, GDPR 등 국내외 주요 규제에 대한 데이터 정책 및 보안 준수 현황을 지속적으로 모니터링한다.



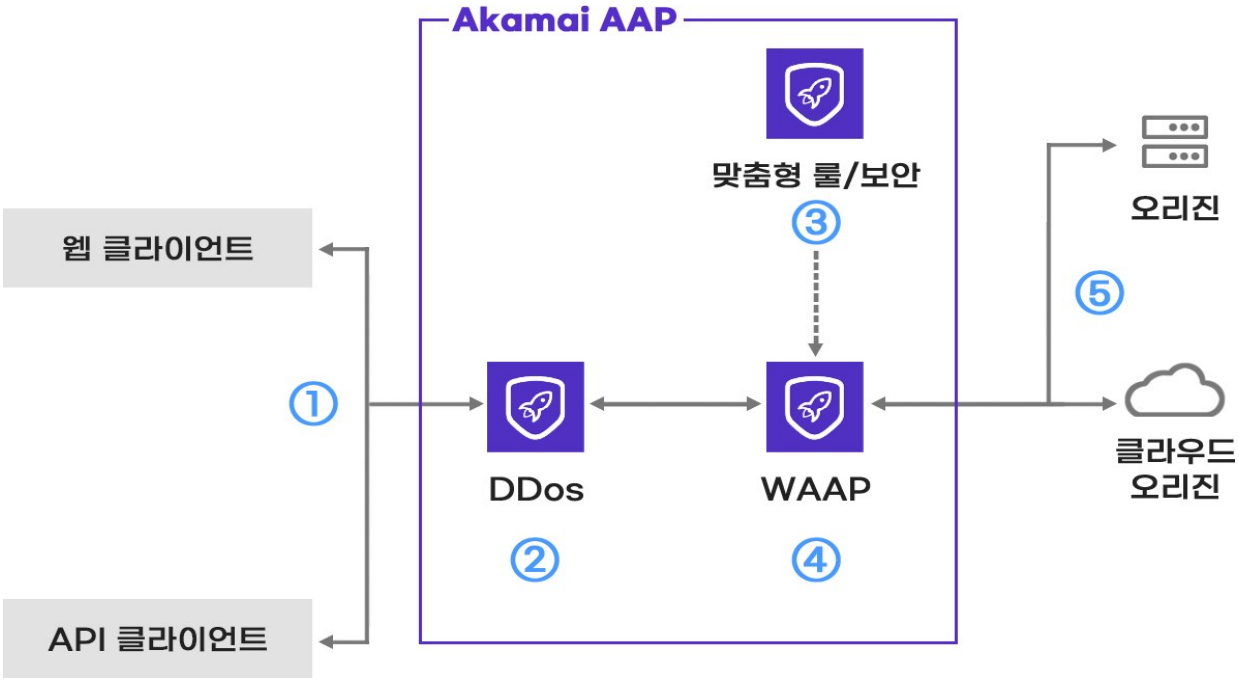
출처 : Fortinet, "What Is CASB (Cloud Access Security Broker)?"

그림 6. CASB Key Features

이러한 기능들은 주로 세 단계의 프로세스를 거쳐 체계적으로 작동한다. 먼저 탐지 및 식별(Discovery) 단계에서 조직 내에서 사용 중인 모든 클라우드 서비스를 식별하여 가시성을 확보한 다음 분류(Classification) 단계에서 각 서비스와 데이터의 위험 요소와 민감도를 평가한다. 마지막 수정(Remediation) 단계에서 평가 결과를 바탕으로 DLP, 접근 차단, 암호화 등 조직의 정책에 맞는 보안 통제를 자동으로 적용하여 지속적으로 클라우드 환경을 보호한다. 이처럼 CASB 는 다른 클라우드 보안 시스템들과 상호 보완적으로 연동하며, 제로트러스트 원칙을 SaaS 애플리케이션 영역까지 확장하는 필수적인 역할을 담당한다.

4. WAAP (Web Application and API Protection, 웹 애플리케이션 및 API 보호)

최근 IT 인프라가 클라우드·API 중심으로 변화함에 따라, 기존의 경계형 WAF(웹 방화벽)나 DDOS 방어 시스템만으로는 고도화된 최신 위협에 효과적으로 대응하기 어려운 한계가 명확해졌다. WAAP 는 이러한 한계를 극복하기 위해 등장한 클라우드 네이티브 보안 모델로, 분산된 환경 전반에 걸쳐 웹 애플리케이션과 API 를 포괄적으로 보호하는 데 중점을 둔다. 제로트러스트 환경에서 WAAP 는 온프레미스에 종속되지 않고 네트워크(L3/L4) 및 애플리케이션(L7) 계층의 공격을 실시간으로 탐지하고 차단하는 통합된 구조를 제공한다.



출처 : 굿모닝아이텍(주), "Akamai AAP 소개자료"

그림 7. Akmai WAAP 구성도

WAAP 의 핵심적인 역할 중 하나는 정교한 API 보안이다. WAAP 는 단순히 API 요청을 허용하거나 차단하는 것을 넘어, 트래픽의 구조, 메타데이터, 행위 특성까지 정밀하게 분석하여 비정상적인 호출이나 데이터 유출 시도 등 고도화된 위협을 체계적으로 방어한다. 또한, API 게이트웨이의 역할을 일부 수행하며 모든 API 요청에 대한 인증과 권한을 관리하고, 미 승인된 숨겨진 API 를 탐지하는 등 API 의 전체 생명주기에 걸쳐 일관된 보안 정책을 적용한다.

더 나아가 WAAP 는 정교한 봇(Bot) 트래픽 탐지 및 차단, IP 평판이나 지리적 위치 등 최신 위협 인텔리전스를 활용한 실시간 위협 차단, 그리고 개별 서비스에 맞는 맞춤형 규칙 및 가상 패치적용 등 다층적인 웹 공격 방어 기능을 포함한다. 결론적으로 WAAP 는 클라우드 기반 인프라 위에서 웹 및 API 보안 정책의 중앙 집중적 집행, 지속적인 검증, 자동화된 대응을 통해 경계가 없는 제로트러스트 아키텍처 기반으로 다양한 API 를 사용하는 환경에서 실질적인 어플리케이션 보호 체계를 실현하는 시스템으로 동작한다.

5. SCA (Software Composition Analysis, 소프트웨어 구성 분석)

SCA 는 조직 내에서 사용되는 다양한 오픈소스 소프트웨어에 대해 취약점, 라이선스, 지원 종료(EOL/EOS), 버전 등을 통합적으로 식별, 분석, 모니터링하여 소프트웨어 공급망의 보안을 강화하는 시스템이다. 기존의 취약점 관리 시스템이 운영체제나 서버 등 인프라 전반의 취약점을 다룬다면, SCA 는 애플리케이션을 구성하는 오픈소스 구성 요소의 보안성과 신뢰성에 집중한다는 점에서 차별화된다.

SCA 의 핵심 기능은 개발 프로젝트에서 사용 중인 모든 오픈소스의 목록, 즉 SBOM(Software Bill of Materials)을 자동으로 수집하고 생성하는 것에서 시작한다. 이를 바탕으로 알려진 취약점(CVE), 라이선스 준수 여부, 지원 중단 상태 등을 실시간으로 분석하고, 신규 위협이 탐지되면 즉시 경고를 보낸다. 제로트러스트 환경에서는 이러한 분석 결과를 바탕으로, 정책에 위배되는 오픈소스의 사용을 CI/CD 파이프라인 단계에서 자동으로 차단하거나 안전한 버전으로 업데이트하는 등 지속적이고 자동화된 통제를 수행하여 신뢰할 수 없는 외부 요소가 운영 환경에 유입되는 것을 원천적으로 방지한다.

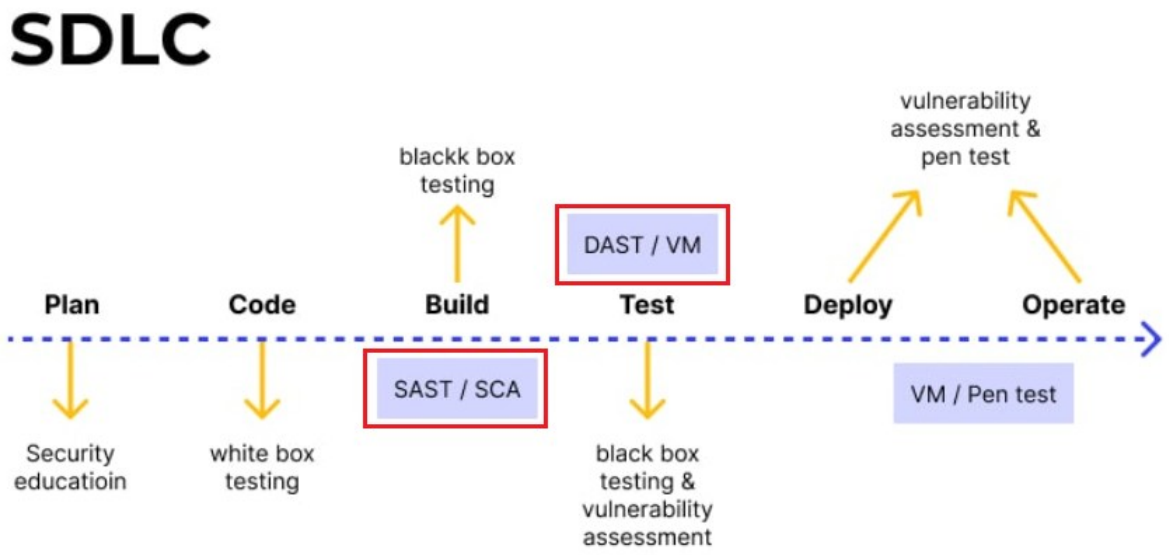
최근 보안 시장에서 SCA 는 독립된 시스템으로 존재하기보다 다른 보안 체계와 통합되는 추세가 뚜렷하다. 첫째, SAST, DAST 와 결합하여 개발자가 작성한 코드와 가져온 오픈소스 코드를 모두 분석하는 통합 애플리케이션 보안 테스트(AST) 플랫폼 형태로 제공된다. 둘째, 클라우드 네이티브 환경에서는 SASE 나 CNAPP 과 같은 통합 보안 플랫폼의 핵심 모듈로 포함되는 경우가 많다. 이는 컨테이너와 마이크로서비스 환경에서 오픈소스 활용이 폭발적으로 증가함에 따라, 클라우드 애플리케이션의 안전성을 확보하기 위해 SCA 가 필수 요소로 자리 잡았기 때문이다.

궁극적으로 제로트러스트 관점에서 SCA 는 단순히 취약점을 찾는 도구를 넘어, 신뢰할 수 없는 외부 요소로 취급되어야 하는 소프트웨어 공급망 전체의 무결성을 지속적으로 검증하는 핵심 시스템으로 기능한다.

6. SAST/DAST (Static/Dynamic Application Security Testing, 정적/동적 에플리케이션 보안 테스트)
제로트러스트 환경의 애플리케이션 보안은 소프트웨어 개발 생명주기(SDLC) 전반에 걸쳐 보안을 내재화하는 'Shift Left' 개념에서 출발한다. 이는 보안 위협을 개발 초기 단계에서부터 식별하고 제거함으로써, 운영 환경에 배포되는 애플리케이션 자체의 신뢰도를 근본적으로 확보하는 것을 목표로 한다. SAST 와 DAST 는 이러한 보안 SDLC 를 구현하는 핵심적인 자동화 테스트 방식이다.

SAST 는 소프트웨어 공급망 공격과 취약한 개발 코드로 인한 위협이 증가함에 따라, 애플리케이션을 운영 환경에 배포하기 전에 코드 레벨에서 보안 취약점을 사전에 탐지하고 조치하는 역할을 수행한다. SAST 는 애플리케이션이 구동되기 이전인 개발 및 코딩 단계에서 소스 코드, 바이너리 등을 직접 분석하여 취약한 함수 사용, 미흡한 입력값 검증, 인증·권한 처리 오류 등 잠재적인 보안 결함을 식별하는 '화이트박스' 방식이다. 제로트러스트 아키텍처에서 SAST 는 코드 작성부터 배포 전까지 지속적인 보안 검증을 자동화함으로써, 신뢰할 수 없는 코드가 운영 환경에 유입되는 것을 원천적으로 차단하는 핵심적인 역할을 한다.

DAST 는 SAST 와 상호 보완적으로 작동하는 '블랙박스' 방식의 테스트다. 코드 내부를 분석하는 것이 SAST 라면, DAST 는 실제 구동 중인 애플리케이션을 외부 공격자의 관점에서 테스트한다. DAST 는 소스 코드를 보지 않고 웹 애플리케이션이나 API 에 실제 공격과 유사한 요청을 보내고 그 응답을 분석하여, SQL 인젝션, 세션 하이재킹, 서버 설정 오류 등 운영 환경에서만 드러나는 취약점을 탐지한다. 이를 통해 SAST 만으로는 발견하기 어려운, 실제 서비스 환경과 외부 연동 요소까지 고려한 실전적인 보안 결함을 검증할 수 있다.



출처 : Wallarm, “Dynamic Application Security Testing: Advantages and Disadvantages”

그림 8. SDLC 내 SCA,SAST,DAST

어플리케이션 및 워크로드 필러는 제로트러스트 아키텍처에서 조직의 비즈니스 로직과 데이터가 실제로 실행되고 처리되는 동적인 영역을 다룬다. SASE, CNAPP, CASB 와 같은 클라우드 네이티브 보안 프레임워크를 중심으로 사용자의 안전한 접근을 보장하고, 클라우드 내부의 인프라와 워크로드, SaaS 애플리케이션 사용 전반을 보호한다. 나아가 WAAP 를 통해 웹과 API 의 경계를 방어하고, SCA, SAST/DAST 를 SDLC 에 통합하여 소프트웨어 공급망부터 코드 레벨까지 신뢰성을 확보하는 심층 방어 체계를 구축한다.

어플리케이션 및 워크로드 필러의 주요 시스템들은 식별자 필러의 IAM, 네트워크 필러의 ZTNA 등 다른 필러의 핵심 시스템들과 유기적으로 연동된다. 이러한 상호 연동을 통해 온프레미스와 클라우드를 아우르는 복잡한 환경에서도 애플리케이션 접근, 데이터 흐름, 개발 및 배포 전 과정에 걸쳐 '지속적인 검증'과 '최소 권한' 원칙을 일관되게 적용하고 강화할 수 있다.

■ 맺음말

제로트러스트 아키텍처에서 애플리케이션 및 워크로드 필러는 앞서 다룬 주요 요소와 시스템들을 기준으로 다양한 환경에 일괄적이고 체계적인 보안 아키텍처를 수립하고 관리할 수 있다. 앞선 내용과 같이, 소프트웨어 개발 생명주기(SDLC) 내의 개발 코드에 대한 보안체계(SCA, SAST, DAST 등)부터, 사용자의 안전한 접근을 보장하는 클라우드 네이티브 보안 프레임워크(SASE, WAAP, CASB 등), 그리고 클라우드 내부의 인프라와 워크로드를 직접 보호하는 CNAPP 에 이르기까지, 애플리케이션 및 워크로드 필러는 다층적이고 심층적인 방어 체계를 요구한다.

제로트러스트 아키텍처 내에서 애플리케이션 및 워크로드 필러는 특성상 보안 뿐만 아니라 인프라와 개발 영역까지 깊숙이 관여한다는 점에서 거버넌스의 중요성이 더욱 두드러진다. 여기서 거버넌스란, 단순히 규칙을 만드는 것을 넘어 개발, 인프라, 보안팀이 공동의 목표 아래 협업할 수 있도록 명확한 정책과 프로세스, 그리고 역할과 책임(R&R)을 정의하는 통합적인 관리 체계를 의미한다.

성공적인 제로트러스트 전환은 기술의 도입만으로는 불가능하다. 반드시 조직 문화와 협업 체계의 변화가 동반되어야 하기 때문이다. 이런 부분이 반영되지 않는다면 실무 환경에서는 각 부서 간의 이해관계가 복잡하게 얽힐 수 있다. 예를 들어, 개발 부서는 신속한 배포를, 인프라 부서는 안정성을, 그리고 보안 부서는 통제를 최우선으로 여기면서 충돌이 발생할 수 있다.

결론적으로, 온프레미스, 하이브리드, 멀티 클라우드 등 다양한 환경으로 워크로드가 계속해서 확장되는 상황에서, 제로트러스트 아키텍처는 조직의 나침반 역할을 할 핵심 기반이 될 수 있다. 이를 통해 보호해야 할 애플리케이션 및 워크로드의 적용 범위를 명확히 정의하고, 이에 필요한 기술들을 체계적으로 식별하여 조직의 실제 환경에 최적화된 형태로 구현하는 것이 무엇보다 중요하다. DevSecOps 와 같은 긴밀한 협업 체계를 바탕으로 제로트러스트 원칙을 적용해 나갈 때, 비로소 조직은 끊임없이 변화하는 디지털 환경 속에서 핵심 자산인 애플리케이션과 데이터를 안전하게 관리하고 지켜낼 수 있을 것이다.

■ 참고 문헌

[1] KISA, “제로트러스트가이드라인 V2.0”, 2024.12

[2] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[3] NIST SP 1800-35 Final,“Implementing a Zero Trust Architecture:High-Level Document”, 2025.06

[4] NIST SP 800-218, “Secure Software Development Framework (SSDF)”, 2022.02

[5] NIST SP 800-204, “Security Strategies for Microservices-based Application Systems”, 2019.08

[6] NIST SP 800-190, “Application Container Security Guide”, 2017.09

[7] CISA, “CISA Zero Trust Maturity Model V2”, 2023.11

[8] DoD, “Zero Trust Overlays”, 2024.06

[9] 국가사이버안보센터, “국가 망 보안체계 보안 가이드라인(Draft)”, 2025.01

■ 참고 자료

[1] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” – 브로슈어

[2] SK쉴더스, “SW 공급망 보안 위협과 대응 방안”

[2] Gartner, “Best Security Service Edge Reviews 2025”

[3] Gartner, “What is Cloud-Native Application Protection Platforms?”

[4] Akamai, “What Is Web Application and API Protection (WAAP)?”

[5] ATLASSIAN, “Microservices vs. monolithic architecture”

[6] ATLASSIAN, “What is SDLC? Software Development Life Cycle Explained”

[7] Paloalto, “Secure Access Service Edge (SASE) Technical Guides”

EQST INSIGHT

2025.09

SK쉴더스

SK쉴더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 SK쉴더스 EQST사업그룹
제 작 SK쉴더스 마케팅그룹