EQST insight

클라우드 보안의 새로운 패러다임 CNAPP(Cloud Native Application Protection Platform)

유종훈 클라우드사업그룹장

■ 개요

작년 8 월 헤드라인에서는 On-Prem., Cloud 환경에서의 보안을 위한 가시성 확보와 인터넷에 연결된 자산의 취약점을 지속적으로 관리하는 ASM (Attack Surface Management)의 대두 배경과 필요성에 대해 설명했다.

이번 헤드라인에서는 지속적으로 증가하고 있는 보안의 위협과 더불어 기존 IT 환경이 급속도로 Cloud 로 전환해가는 과정에서 새롭게 부상하고 있는 CNAPP (Cloud Native Application Protection Platform)를 소개하고자 한다.

최근 SK 쉴더스가 금융권 고객을 대상으로 수주한 사업인 '멀티 클라우드 환경에서의 통합보안 관리 수립 및 구축'을 통해 빠르게 변화하는 고객의 IT 환경과 이를 반영한 보안 요구 사항을 다시 한번 확인할 수 있었다. 그 동안 고객들의 주된 요구사항은 비교적 가벼운 애플리케이션을 우선적으로 Cloud 에 배치하고, On-Prem. 환경에서 유효했던 보안조치들을 Cloud 에서도 구현할 수 있는가였다.

솔루션 관점에서는 웹 애플리케이션의 보호를 위한 WAF (Web Application Firewall), Database 와 주요 서버에 대한 접근제어 (계정의 권한관리 포함), Workload 를 위한 Agent 타입의 보안 솔루션의 구축이 많은 비중을 차지하고 있으며, 이렇게 구축된 솔루션에 대한 관리/운영을 위한 관제서비스를 제공할 수 있는지가 서비스 벤더를 평가하는 중요한 요소였다.

이와 같은 평가 방법은 Cloud 시대에 다소 전통적인(Legacy) 솔루션과 서비스로 바라볼 수 있다. 하지만, 고객이 사용하고 있는 다양한 Cloud 환경에서 상기 솔루션의 검증, 구축, 운영은 만만치 않은 과제다. 실제 몇몇 고객사들은 Cloud Governance 관점에서 기술체계 뿐만 아니라 조직, 정책 등의 관리적인 측면에서 완전한 재검토 또는 새로운 아키텍처 수립에도 예산을 투입하고 있다.

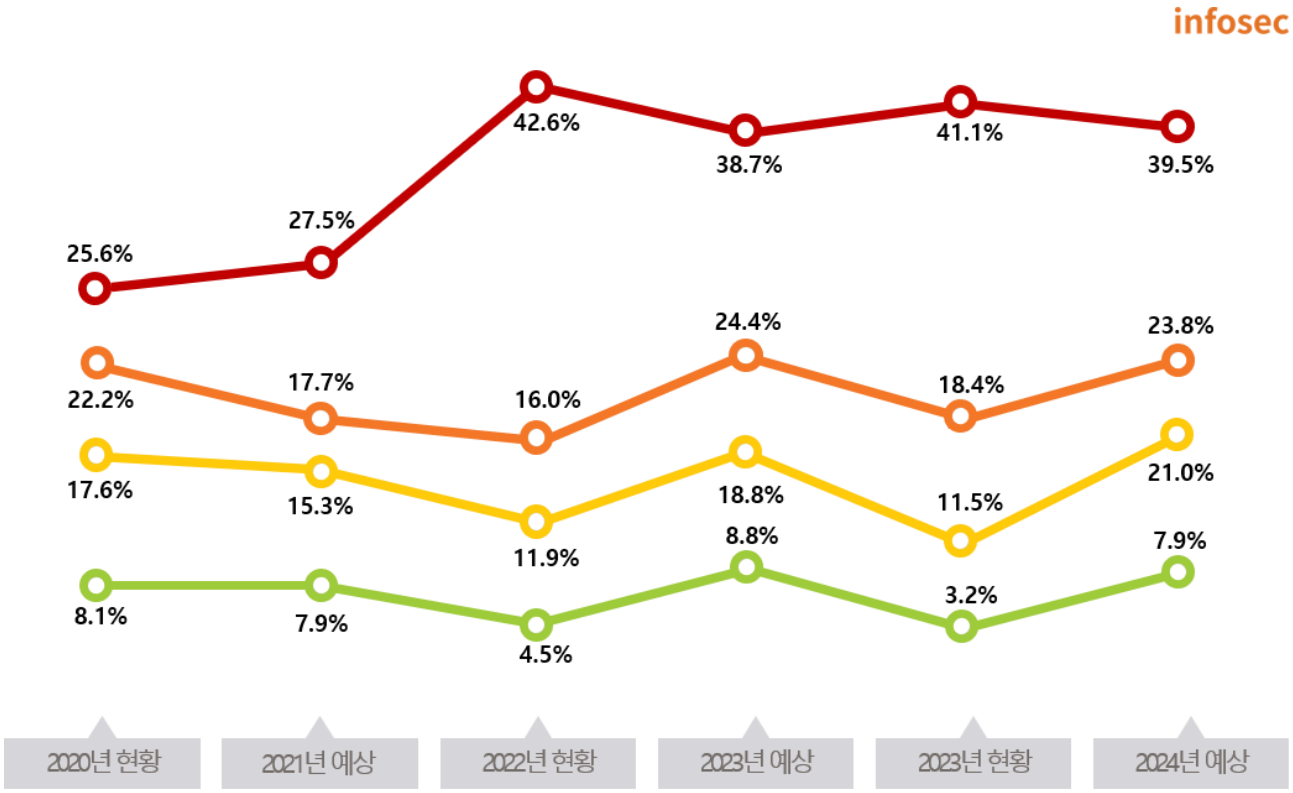
이번 금융권 고객 사례를 담당하며 느꼈던, 기존 관점에서 벗어나 주요 업무 시스템이 Cloud 에 배치될 때 필요한 보안 기능과 요구사항은 아래와 같다.

첫번째, CSP (Cloud Service Provider)가 제공하는 다양한 Cloud 인프라를 업무 특성에 맞게 활용하고 있는 사례가 증가함에 따라 보안의 복잡성이 크게 증가하고 있으며, 우선적으로 인프라에 대한 '가시성' 확보가 더욱 중요해지고 있다. 이와 더불어 S/W 공급망 보안, Compliance 준수도 기업의 입장에서는 중요한 과제로 떠오르고 있다.

두번째, Workload 와 환경 모두 VM, Container (Kubernetes), Serverless 등으로 다양하게 전개되고 있는 가운데, 시장에서 언급되는 CWPP (Cloud Workload Protection Platform) 솔루션이 위의 모든 환경을 지원하지 않는다.

세번째, '멀티 클라우드 환경'에서 새로운 보안 대책 및 솔루션을 운영하기 위한 고객의 준비와 인적 역량은 부족한 상태이며, 이를 지원하기 위한 '보안운영'의 수요도 새롭게 부상하고 있다.

이러한 이유로 인해 향후 몇 년간 소위 미션 크리티컬한 업무가 Cloud 로 전환될 때에는 진정한 Cloud 환경에 맞는 새로운 보안 대책이 필요한 시대가 되었다.



[그림 1] 클라우드 컴퓨팅 활용 현황과 전망

* 출처: 2023 년 국내 클라우드 컴퓨팅 현황과 전망 ('23. 4., IT World/CIO) 보고서 이미지 재가공

■ CNAPP 개념

최근 계속해서 Cloud 서버 Workload, Container 보안을 담당하는 CWPP (Cloud Workload Protection Platform), 전반적인 인프라와 개별 리소스에 대한 Compliance, Configuration 을 모니터링 할 수 있는 CSPM (Cloud Security Posture Management), Cloud 에서 사용되는 다양한 성격의 Identity 와 권한을 관리하는 CIEM (Cloud Infrastructure Entitlement Management), CSNS (Cloud Security Network Security), DSPM (Data Security Posture Management) 등의 솔루션이 속속 소개되고 있으며, 나아가 이를 통합한 CNAPP (Cloud Native Application Protection Platform)이 떠오르고 있다.

먼저 CNAPP 의 개념을 살펴보자. 가트너에 따르면 CNAPP 는 '기업이 Cloud Native 생태계의 이점을 전체적으로 활용할 수 있는 간소화된 보안 아키텍처'이다. 조금 더 확장해서 설명하면 Cloud Native 애플리케이션에 대해 '개발에서 운영 전반에 걸쳐 보안과 Compliance 를 지속적으로 관리할 수 있는 도구의 통합'이다.

■ CNAPP 도입의 중요성

CNAPP 의 주요 컴포넌트와 기능 설명에 앞서 반복적으로 이야기하고 있는 통합에 대해 강조의 이유 등을 먼저 생각해 볼 필요가 있다.

첫번째, 기술적(기능) 관점의 통합이다. 기존 On-Prem. 보다 훨씬 복잡한 Cloud 인프라를 관리하기 위해 기업은 통합된 보안도구를 통해 다양한 보안 이슈에 효율적으로 대응하고, 유기적인 보안체계를 유지할 필요가 있다. 예를 들어 CWPP를 통해 식별된 보안문제를 CSPM과 연계한다면 보다 빠르게 문제를 해결할 수 있다.

두번째, 업무 프로세스의 통합이다. DevOps 를 넘어 DevSecOps 가 적용되고 있는 현실을 보면 애플리케이션의 개발, 테스트, 배포, 운영 프로세스에서 일관된 보안성을 유지하기 위한 다양한 보안정책과 도구가 개발되어 활용되고 있다. 이는 비용적 측면뿐만 아니라 속도감 있게 비즈니스를 전개하는데 있어 매우 유용한 방법이다. 이를 통해 업무 전반의 보안수준 관리 및 가시성을 확보할 수 있다.

마지막으로 기업의 입장에서 보면 통합의 필요성이 더욱 명확해진다. 많은 기업들은 보안을 위해 대략 40~70 개 정도의 솔루션을 구매, 구축, 운영 및 유지보수하고 있다. 물론 일부 통합 솔루션을 사용하는 고객도 있으나, 대부분 영역별로 벤더가 나뉘어지는 것이 현실이다. 이러한 구조는 보안 업무의 복잡성을 야기해 효율 저하로 이어지며, 증가하는 보안위협의 대응 속도를 떨어뜨린다.

RSA Conference 2022 에서 확인한 결과 북미에서는 이러한 통합의 움직임이 '구매'업무에서 나타나고 있었으며, 적극적인 M&A 를 통한 Vendor Consolidation 이 이루어지고 있다. (e.g., Microsoft, Palo Alto Networks, Orca Security, Aqua Security, Wiz, etc. …)

다른 '통합'의 좋은 예로는 최근에 많은 벤더가 강조하고 있는 'EDR (Endpoint Detection & Response), MDR (Managed Detection & Response), XDR (eXtended Detection & Response)'이 있다. 이러한 솔루션들은 최신 보안 위협을 탐지하는 센서(기술)들의 유기적인 통합은 물론 '위협탐지 → 대응 → 재발방지 및 사전 대응'의 과정(프로세스)을 Platform 관점에서의 통합으로 풀어 내고 있다.

■ CNAPP 주요 기능

CNAPP 의 주요 기능에 대해 자세히 알아보면, XDR 와 같이 CNAPP 는 'Cloud Native' 환경에서 완전한 End-to-End 보안을 제공하는 것을 목표로 개별 포인트 솔루션이 아닌 Platform 기반의 통합으로 접근하는 자세를 취하고 있다.

CNAPP 를 통해 제공되는 기능은 아래와 같다.

CWPP (Cloud Workload Protection Platform, 클라우드 워크로드 보호)

- Cloud 인프라 상의 다양한 Workload, VM, Container (Kubernetes), Serverless에 악성코드 검사, 위협탐지, 침입방어, 애플리케이션 제어, 취약점 진단 및 관리 등의 보안기능을 제공해 안심하고 신속하게 애플리케이션을 실행할 수 있도록 도와준다.

CSPM (Cloud Security Posture Management, 클라우드 보안형상 관리)

- Cloud 서비스 구성, 보안설정, 규정 준수, 거버넌스 등의 문제를 기록, 탐지, 관리, 보고하여 Cloud 인프라 전체에 대한 모니터링, 자산 식별 및 분류, 리소스 구성관리 기능을 제공한다.

CSNS (Cloud Service Network Security, 클라우드 서비스 네트워크 보안)

- 개별 사용자 네트워크 보안 정책 및 업계 표준을 기반으로 Cloud 인프라를 보호하는 IP, Data, 애플리케이션 및 서비스에 이르는 광범위한 도구의 집합이다.

CIEM (Cloud Infrastructure Entitlement Management, 클라우드 인프라 권한 관리)

- 과도한 Cloud 인프라 권한을 줄이고 최소 권한의 액세스를 시행하도록 설계된 Identity 및 액세스 거버너스 제어기능을 제공한다.

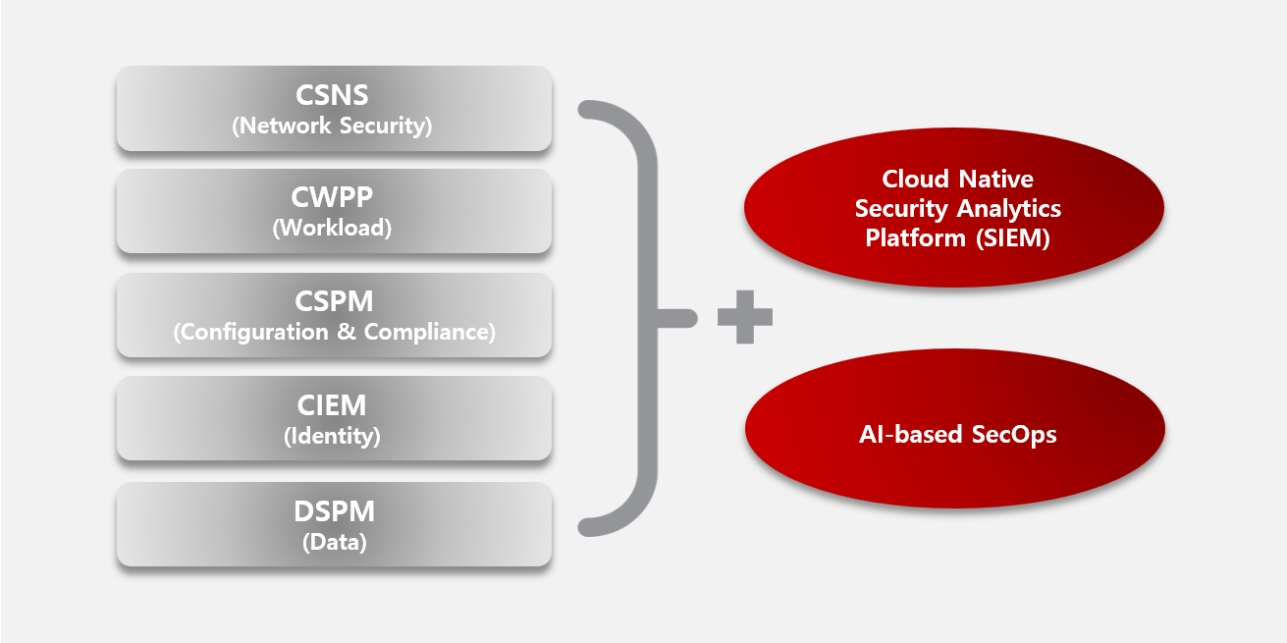
DSPM (Data Security Posture Management, 클라우드 데이터 보안 관리)

- Cloud 인프라 내 주요 데이터 탐지 및 보호작업을 자동화함으로써 민감한 데이터를 더 효과적으로 발견/모니터링할 수 있는 기능을 제공한다. 추가적으로 데이터 접근에 대한 부적절한 권한, 잘못된 자격을 포함한 위험을 적시에 교정하고 데이터 손실을 방지한다.

위의 3 가지 기능이 조합되어 단일한 플랫폼으로 통합될 경우 기업은 보다 빠르게 위협을 탐지하고 일관된 정책에 의한 Compliance 준수 및 효율성 높은 보안운영 (Security Operations)을 기대할 수 있다. 이러한 접근방법은 글로벌 보안업체들이 Cloud 보안을 제공하는 일반적인 Trend 다.

앞서 언급한 최신의 보안운영 기법을 통합하여 도식화하면 아래와 같다.

infosec



■ 맺음말

글로벌 보안업체들과 CNAPP 벤더에서는 이와 같은 Framework 가 일반화되고 있으나, 국내 고객과 Cloud 환경에 적용하기에는 현실적으로 아직 이른 부분이 있다. SK 쉴더스는 On-Premise, Cloud 환경에서의 보안 서비스 1 위 역량을 보유하고 있으며, 다양한 산업에서의 프로젝트 수행 경험을 보유하는 등 강력한 사업 경쟁력을 유지하고 있다. 앞으로도 변화하는 Cloud 보안 Trend 를 계속 Tracking 하고 시장과 고객의 요구에 대한 면밀히 분석 및 Vendor 와의 긴밀한 협력을 통해 보다 고도화된 보안 서비스 전문업체로 거듭나기 위해 더욱 노력할 것이다.