Digital Chaos 시대의 클라우드 운영 및 보안 대응방안

August 2024

pwc

Contents

최근 발생한
'MS클라우드 서비스 마비 사태'의
근본 원인을 짚어보고 민첩하되
안정적인 기업으로 진화하기 위한
방안을 모색합니다.

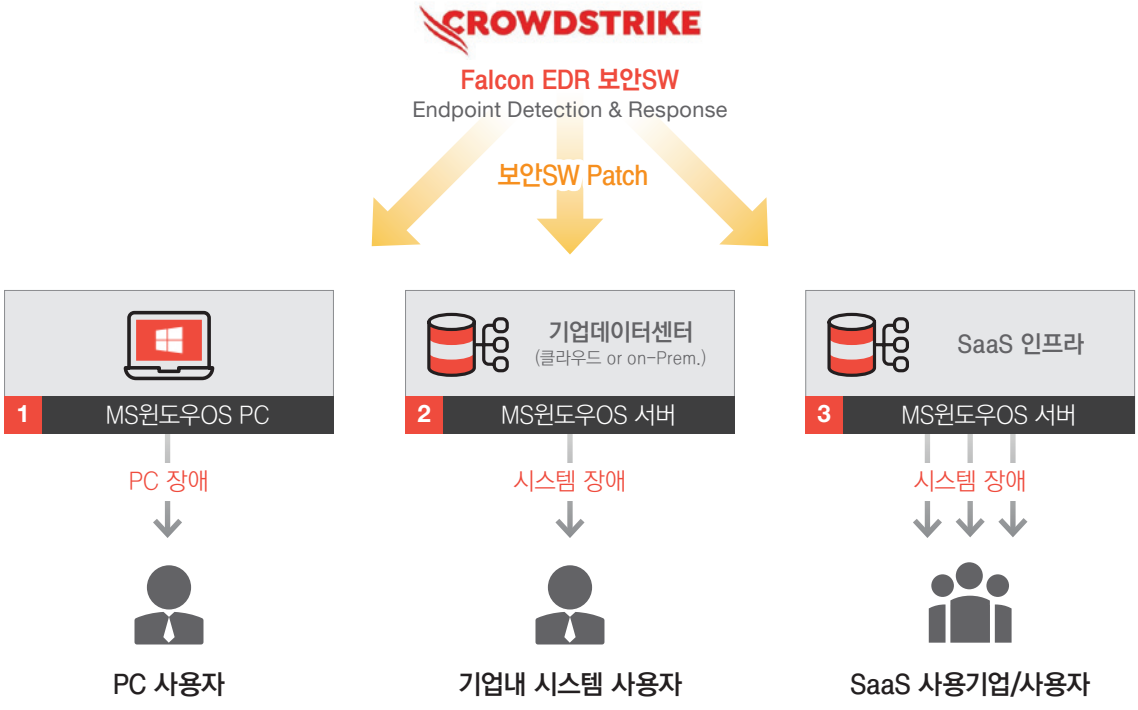
‘MS 클라우드 사태’의 실제

2024년 7월 19일 발생한 이른바 ‘MS클라우드 서비스 마비 사태’로 알려진 보안사고로 인해 전세계가 대혼란을 겪었다. 기업 업무환경 뿐만 아니라 항공, 의료, 방송 등 기간 인프라 까지 영향을 미치고 있고, 여러 매스컴에서는 10억달러 이상의 손실을 추정하고 있다. 초기 사고의 근원지가 MS 클라우드로 알려지고 클라우드 서비스 자체에 대한 독점, 높은 의존도 등의 이슈도 같이 제기되고 있다.

하지만, 사실 이번 사고가 클라우드 서비스 자체에 장애사고이기 보다는 MS윈도우OS에서 발생한 장애이며, 그 원인은 CrowdStrike의 보안SW인 팰콘(Falcon)의 보안패치가 MS윈도우OS에 자동배포 된 후 OS오류로 발생한 장애사고이다.

해당 보안프로그램은 주로 기업용 SW로 MS윈도우OS를 설치한 업무용PC와 회사 시스템을 운영중인 MS윈도우OS 서버에 영향을 미쳤다. 보안SW패치로 인한 원인은 동일하나 IT 인프라 관점에서는 다음의 세가지 형태로 장애가 발생하였다.

‘MS 클라우드 사태’가 영향을 미친 경로



Source: PwC

01

첫째, 보안SW 패치 후 오류로 MS윈도우OS가 블루스크린이 뜨거나 재부팅 되는 현상이다. CrowdStrike의 보안SW가 설치된 업무용 PC에 일괄적으로 적용되면서 피해가 가장 크게 발생되고 있다. PC 자체 사용이 불가능 해지면서 관련 업무도 불능 상태가 되었다. 전세계적으로 850만대 PC에서 오류가 발생했고, 기업별 IT부서 혹은 개개인이 오류조치 복구를 해야 함에 따라 그 영향도가 가장 크다 볼 수 있다.

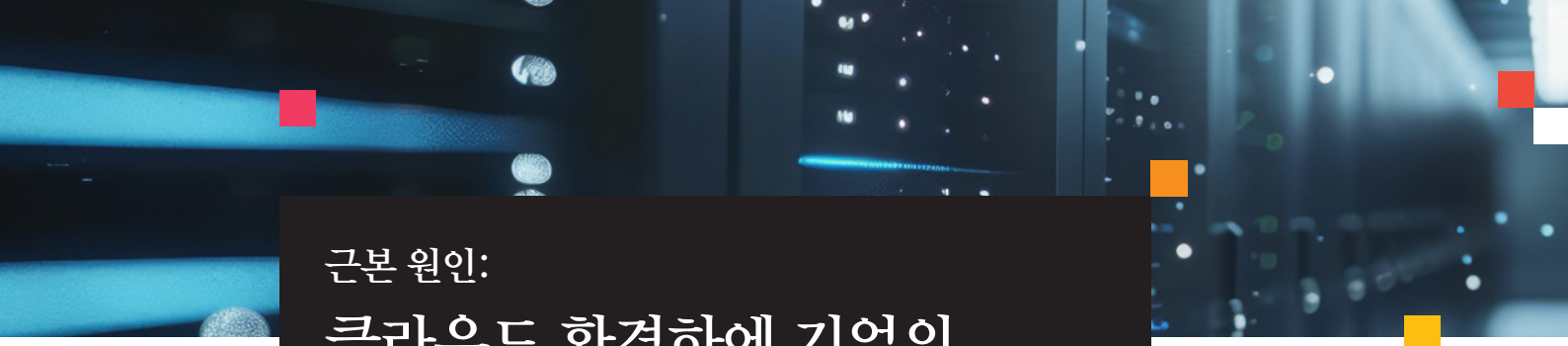
02

둘째, AWS, MS Azure, GCP(Google Cloud Platform) 등 퍼블릭 클라우드 환경뿐만 아니라 온프레미스 대상의 MS윈도우OS가 적용된 서버 시스템의 장애 발생이다. 서버OS에도 해당 패치가 적용된 경우 동일한 장애가 발생되고 있으며, 기업 ERP등 내부 시스템, 병원 의료시스템, 게임 서비스 등의 장애가 이에 해당한다. 특히, 병원 의료시스템의 경우 국내외적으로 리눅스 서버 대비 MS윈도우OS비중이 높아 영향이 큰 걸로 추정되고 있다. 또한 윈도우OS 기반 서버는 AWS 및 GCP에도 설치구성 가능은 하나, 상대적으로 MS Azure 클라우드를 많이 사용하다 보니, 초기에 해당 사건이 MS클라우드 장애로 알려진 이유도 있는 듯하다.

03

마지막으로 MS윈도우OS서버를 사용하는 SaaS 서비스 장애이다. 현상 자체는 MS윈도우 서버 장애이나 SaaS서비스를 제공하는 서비스 자체에 장애가 발생되다 보니 이 다수의 기업 및 사용자에게 영향도가 크다고 볼 수 있다. 예컨대 항공사 SaaS형 발권서비스인 나비테어(Navitaire)를 주로 사용하는 저비용 항공사(LCC) 등에서 장애가 발생하는 경우이다.

특히 공항에서 이러한 상황들이 복합적으로 발생하고 많은 여행객들에게 불편함을 가중하여 보다 이슈화 된 것으로 보고 있다. 예를 들면 항공사 데스크 직원 PC 및 키오스크 장애로 인한 업무이 불가한 경우는 첫번째 경우인 윈도우PC OS장애에 해당하며, 저비용 항공사의 발권서비스 불능은 두번째 경우인 MS윈도우OS기반 서버 장애문제로 볼 수 있다.



근본 원인:

클라우드 환경하에 기업의 IT 운영 통제 및 보안의 허점

이 문제를 야기시킨 CrowdStrike의 팰콘 솔루션은 악성코드를 자동으로 탐지하고 제거하는 EDR(Endpoint Detection & Response) 소프트웨어로, 윈도우 OS 커널 영역까지 영향을 미칠 수 있는 강력한 보안 솔루션이다. 아직 정확한 오류 원인은 공식적으로 밝혀지지 않았지만 이 SW패치로 인해 윈도우OS 오류가 발생하였다고 알려져 있다.

MS윈도우OS 오류에 대해 기술적인 관점에서 원인을 규명하는 것이 뿐만 아니라, 공급망 보안, 그리고 클라우드 전반적인 운영 통제 및 보안 관점에서 보다 근본적인 원인을 살펴볼 필요가 있다.

우선 업무용 PC에 대해서는 업그레이드의 경우 SW오류에 대한 파급력이 커서, 지연설치 후 테스트 PC환경에서 어느 정도 검증 후에 전직원 대상 PC환경으로 업그레이드되는 것이 통상적이다. 하지만 이번 마이너 패치는 '하루에도 수차례 설치되는 패치'여서 자동설치가 되었다고 알려져 있는데, 이에 대한 그 피해가 너무 크게 귀결되었다. 기업의 업무용 PC는 마이너한 패치여도 그 파급력이 커서 신중한 검증 과정을 거쳐야 하는데 그 부분이 간과되었다고 볼 수 있다.

사실 이보다 더 심각한 부분은 기업 서버OS 대상 발생한 장애이다. 실제 서버의 보안 패치 이후 품질 테스트(QA) 환경에서 충분한 검증 없이 운영 환경(PRD)에 반영된 점이다. 통상적으로 서버 대상의 구성 변경(보안 패치나 SW버전 업그레이드 등)은 일정 기간(최소 수일에서 수개 월까지)의 테스트 검증 기간을 거친 후 운영 환경에 동일한 패치를 반영해야 한다. 그러나 이번 사고는 이러한 통제 절차가 지켜지지 않아 발생한 것으로 판단된다.

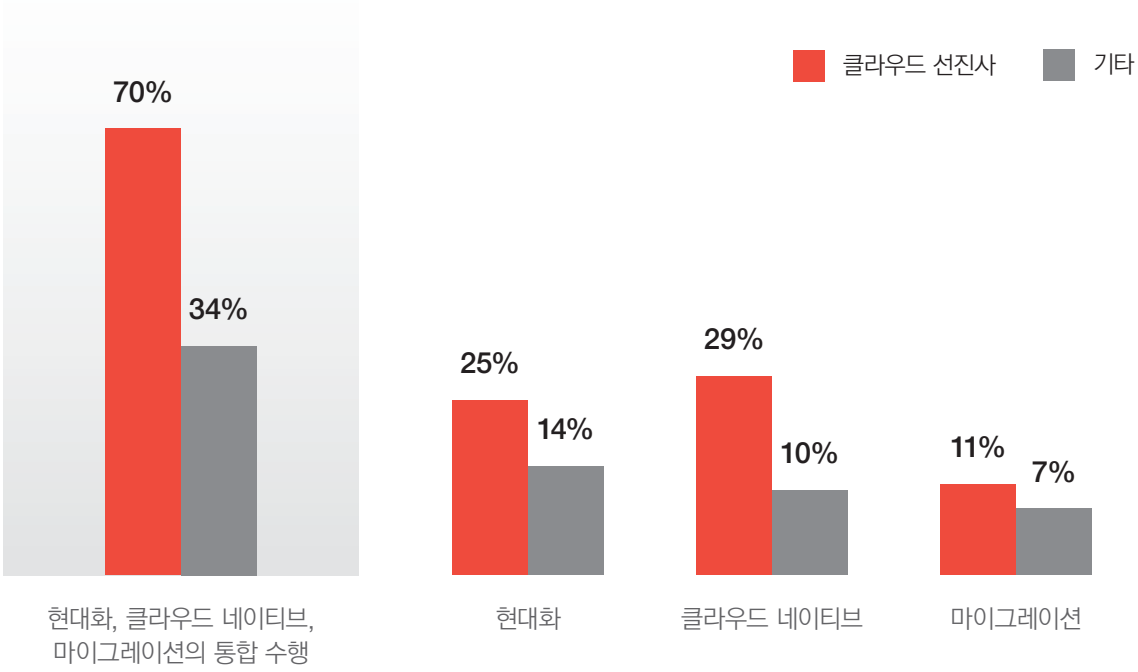
이 부분은 AWS, Azure, GCP와 같은 클라우드 사업자(CSP)의 책임이 아닌 해당 인프라 위에 시스템을 설치 활용하는 기업의 책임 영역에 속한다. 사실 이 부분에 대해서 클라우드 사업자는 전체 네트워크에 대한 보안과 관련 기술 요소를 제공하고, 세부적인 시스템 단위에 테스트 환경 구성과 이에 대한 운영 정책은 기업에 있다고 할 수 있다. 이러한 배포 패치 업그레이드 정책은 CrowdStrike에서 적용하여 실행했다 하더라도, 이에 대한 정책을 동의하고 기업의 IT자산(PC, 서버)에 적용하는 부분에 대해서는 상당 부분 기업에도 책임이 있다고 보인다.

사실은 PC나 서버가 단절된 네트워크에 위치한 온프레미스 환경에서는 이러한 장애가 발생될 가능성이 희박하다. 예컨대 법제도적으로 망분리가 의무화된 국내 금융권 IT 인프라 환경에서는 발생될 수 없으며, 실제로 해당 사태에 국내 금융권 사례는 전무했다. 물론 클라우드 환경도 외부 공공망과의 분리는 가능하나, 회사 환경에 따라 다르겠지만 보다 유연하고 개방되어 있는 것도 사실이다.

시스템 대비 클라우드의 경우 상대적으로 구성의 변경 및 가용성 확보가 용이하고 백업/복구가 간편해지면서 IT부서들도 업그레이드/패치 등의 구성 변경에 대해 다소 무감각 해지고 있는 듯하다. 그에 따른 통제 미비로 인해 이번과 같은 대란이 발생했음을 추정해 볼 수 있다. 역설적으로 90년대 이미 EOS(End Of Service) 버전인 MS윈도우3.1을 사용하는 사우스웨스트항공은 이번 재난으로부터 상대적으로 영향을 덜 받는 것으로 보인다.

선진사의 클라우드 도입 유형

Q. 다음 중 귀사가 클라우드 기술을 활용하는 방법을 가장 잘 설명하는 것은 무엇입니까?



Source: PwC 2023 Cloud Business Survey

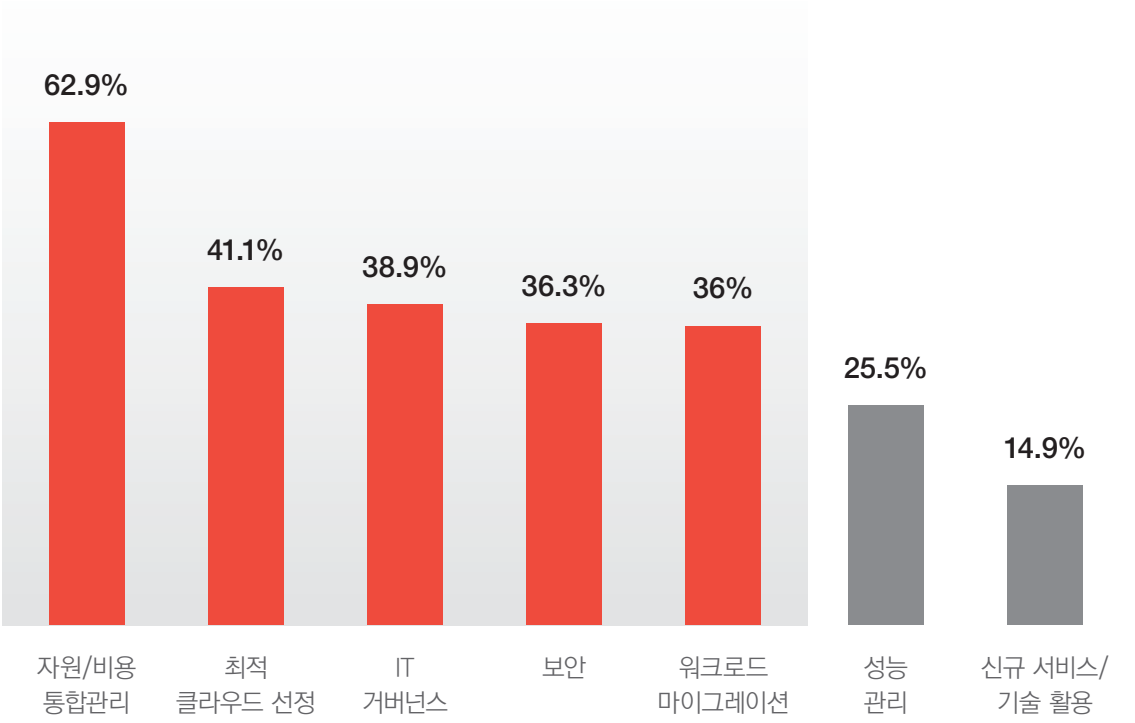
클라우드 도입 선도사들은 다양한 비즈니스 요구사항에 적합한 클라우드 도입 모델과 서비스를 활용하고 있다. 즉, 클라우드 도입 초기에는 단일 CSP 환경을 활용했던 것과 달리, SaaS 서비스 등 다양한 모델을 같이 활용하는 멀티 클라우드 환경의 활용도가 다변화되고 있는 추세이다.

클라우드 환경이 보다 다양한 서비스와 짧은 기술 생애주기, 복합적 기술 구조로 디지털화 됨에 따라 기업의 IT부서들은 민첩하고 신속한 대응에 집중하고 있다. 하지만, 클라우드의 활용도가 다양해지고 복잡도가 커져 장애 포인트도 보다 다양하게 발생하고 있다. 민첩성을 중심으로 안정성과 신뢰성 확보를 다소 후순위로 둔 결과, 이러한 디지털 혼돈기(Digital Chaos)를 겪는 것이라 본다. 즉, 이번 사태에서 클라우드 자체의 과실은 없다고 해도, 클라우드 서비스와 네트워크로 연결되는 초연결 시대가 또 하나의 근본적 원인을 제공했다고 판단할 수 있다.

멀티 클라우드 환경이 가속화되면서, 기업의 인프라 자원 활용의 편의성과 효율성이 향상되는 것은 사실이나 자원 또는 비용의 통합관리와 함께 보안관리에 어려움을 겪고 있다. 특히, 보안과 통제관리 부분에서는 클라우드의 장점을 활용하되, 적정 수준에서는 양보할 수 없음을 인식해야 한다. 이번 사태를 계기로 '보안에 있어서는 어떤 것도 신뢰하지 말고 검증해야 한다'는 마인드를 가지고 클라우드 환경에 적합한 IT 보안 체계 및 통제관리 체계를 정비할 필요가 있다.

멀티 클라우드 도입 및 활용의 페인 포인트

Q. 다음 중 귀사가 멀티 클라우드를 도입하고 활용할 때 이슈는 무엇입니까?



Source: IDC, 2024

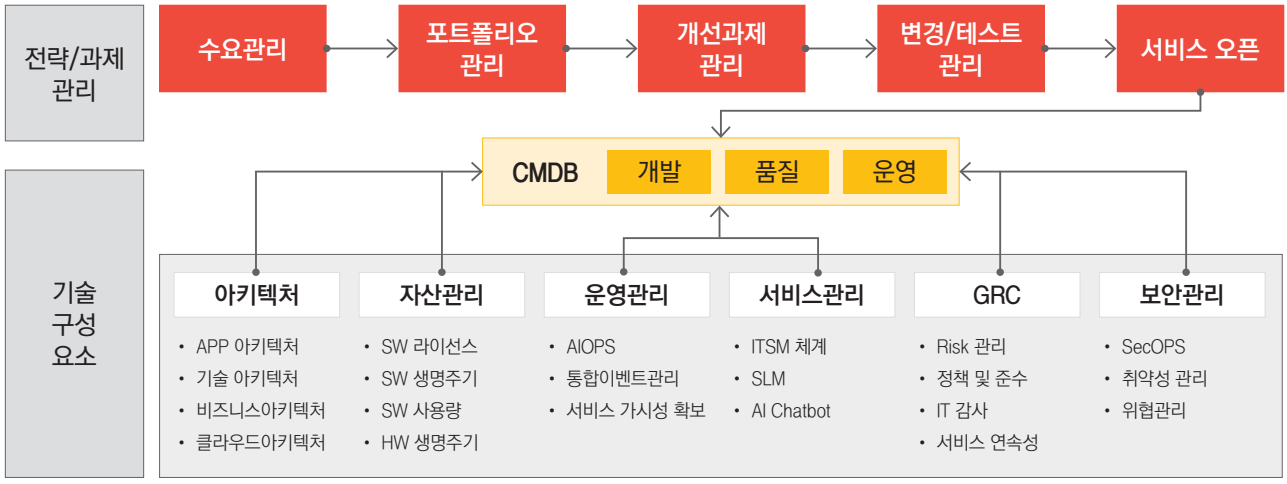
대응 전략:
민첩하되 안정적인 기업으로

기업의 IT 부서는 PC OS뿐만 아니라 더욱이 서버OS의 경우 더욱이 SW패치 등의 변경을 자동화하기보다는 변경의 중요도를 판단하고, 영향도를 검토하며, 검증 및 적용 시점을 신중히 결정하는 프로세스를 마련해야 한다. 전체 구성 변경에 대한 변경 관리 프로세스와 검증 체계, 기준 및 정책을 강화하는 것이 중요하다.

사실 지금까지 시스템 개발 및 인프라 구성변경 등에 대한 통제관리 활용은 많은 기업들이 노력하고 관리해왔던 영역이다. 하지만 지금처럼 멀티 클라우드와 같이 다변화하는 기술 아키텍처와 인프라 환경에서는 단일 인프라 구성 요소에만 국한하여 그 변경을 통제하거나 관리하면, 상호간의 복잡한 구성요소 간의 영향도와 파급력을 통제하고 관리하기가 어렵다. 부분에서는 문제가 없으나 전체에 영향을 미치는 것을 효율적으로 대응하기 어려운 환경이다.

따라서, 기업내에서 수행하고 있는 비즈니스 수요와 개선과제를 관리함과 동시에 이에 영향을 미칠 수 있는 아키텍처, IT자산, 운영, 권한/통제(GRC), 보안 등의 통합 구성관리(CMDB, Configuration Management Database) 정보를 구성하여 관리해야 한다. 전체적인 IT에 변화에 대한 과제와 이에 영향 되는 클라우드 자원 간의 가시성을 확보하고 사전 검증과정과 함께 혹여 문제 발생시에 신속하고 즉각적인 대응체계 마련이 필요하다.

클라우드 서비스 통합관리체계



Source: PwC

한편으로는 기업의 보안 부서는 클라우드 보안 전략과 거버넌스를 수립하고, 클라우드 보안체계가 Prepare → Prevent → Detect → Respond → Recover 단계에 따라 잘 운영될 수 있어야 하며, 이를 위해 클라우드 보안의 필수적이고 핵심적인 구성요소를 갖추고 있어야 한다. 이를 보다 살펴보면 다음과 같다.

01

첫째, 클라우드 보안 전략 및 거버넌스 수립을 위해서는 클라우드 보안 조직 구성과 R&R 정의를 토대로 정책, 표준, 가이드라인 및 업무 절차가 마련되어야 하고, 현재의 클라우드 보안 수준에 대한 인지를 토대로 발생 가능한 리스크를 통제하기 위한 계획 및 프로그램을 보유해야 한다.

02

둘째, 클라우드 보안체계의 지속적이고 안정적인 운영을 위해서는 위협 시뮬레이션 및 시나리오 플래닝을 통한 사전 준비(Prepare) 단계, 클라우드 서비스 및 리소스에 대한 가시화를 통한 취약점 진단 및 조치를 통한 예방(Prevent) 단계, 외부 및 내부 위협 모니터링을 통한 탐지(Detect) 단계, 사고 대응 및 조사를 통한 대응(Respond) 단계, 비즈니스 연속성 확보를 통한 회복(Recover) 단계가 유기적으로 연계되고 보안체계 운영의 실행력을 갖추고 있어야 한다.

03

셋째, 이러한 클라우드 보안체계 운영과 더불어 필수적이고 핵심적인 구성요소로서 IAM(ID 및 접근 관리, Identity and Access Management), 인프라 보호(Infrastructure Protection), 보안 엔지니어링 및 하드닝(Hardening) 등을 갖춤과 동시에 클라우드 데이터 암호화 및 키관리 등의 프라이버시 및 보호 체계를 갖추어야 한다.

클라우드 보안관리 체계

Source: PwC

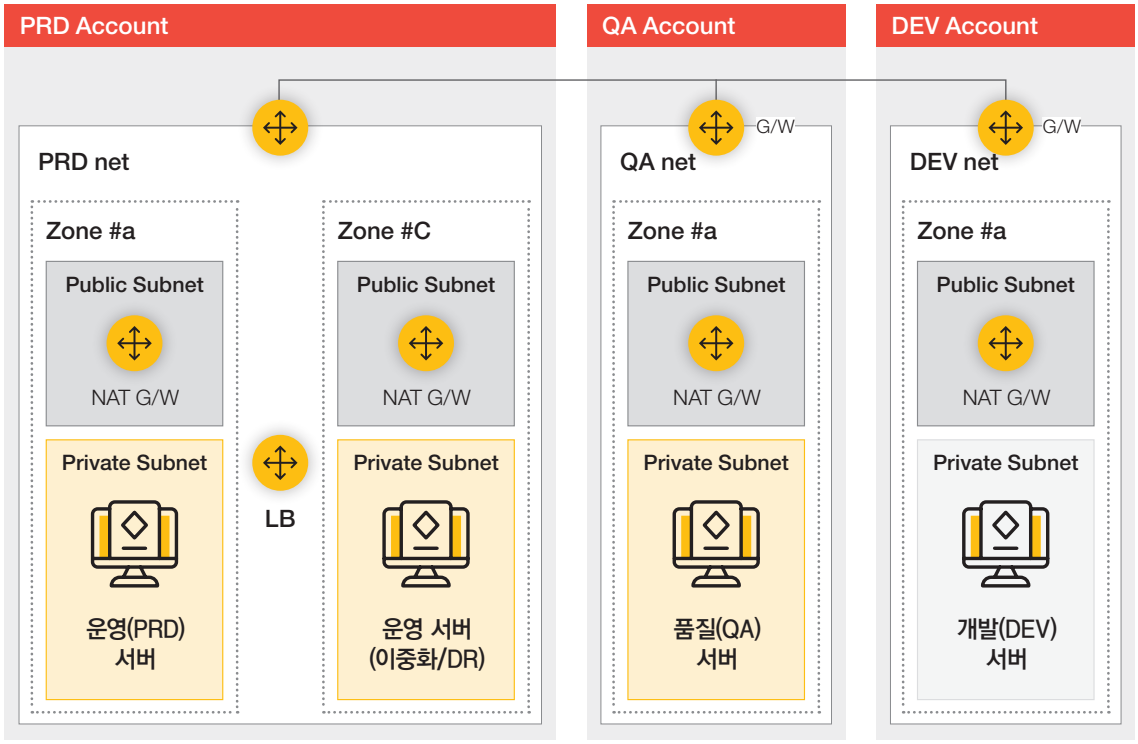
이러한 클라우드 보안관리체계를 갖추고 클라우드 서비스 및 리소스에 대한 가시화를 통해 최적화된 보안 기능 및 서비스를 구성하고 보안 설정을 상시 모니터링하여 누락되거나 잘못된 보안 설정을 개선 조치한다면 다양한 보안사고를 예방할 수 있다.

특히 모든 보안 리스크를 사전에 차단할 수 없기 때문에 회복탄력성(Resilience)도 같이 고려해야 한다. 클라우드 백업, 이중화, 오토 스케일링, 멀티 클라우드 DR센터 도입을 통한 내결함성과 고가용성을 확보해야 한다. 클라우드 백업을 통해 데이터 손실을 방지하고, 시스템 이중화를 통해 장애 발생 시에도 서비스가 지속될 수 있도록 해야 한다. 특히, 오토 스케일링 기능을 골든 이미지와 결합하여 활용하면 더욱 효과적이다.

골든 이미지를 사용하면 검증된 상태의 시스템 이미지를 자동으로 배포할 수 있어 신속하게 안정적인 시스템 상태를 유지할 수 있다. 이를 통해 트래픽 증가나 시스템 부하에도 유연하게 대응할 수 있다. 이러한 대책에도 불구하고 특정 CSP의 문제로 인해 클라우드 중단에 대비하기 위해서는 멀티 클라우드 DR 센터를 통해 지속 가능한 서비스를 제공할 수 있도록 대비할 필요가 있다.

클라우드 인프라 구성의 특성상 기존 온프레미스 구성대비 복수의 데이터센터를 활용하여 이중화 및 DR 구성(Multi-Zone HA/DR) 구성이 상대적으로 용이하고 장애 발생시 Web/Was 서버 및 DB서버간의 가용성 확보가 용이하다. 다만, 이러한 구성에서도 보안요소는 충분히 고려되어야 하는데, 예를 들면 운영(PRD)와 품질(QA), 개발(DEV)는 별도의 네트워크 구간으로 구분 구성이 필요하며, 가급적 각 네트워크 구간은 망분리가 필요하다.

클라우드 인프라 구조



Source: PwC

이렇듯 기업은 보안, 성능 및 가용성의 확보는 클라우드 공급사에 의존해서는 안되며, 자체적으로 지속적인 보안 환경을 구성해야 한다.

PwC의 클라우드 보안 컨설팅 방법론 및 운영 통합 어프로치 Fin-Sec Ops

PwC는 클라우드 보안 수준을 진단하고 대책을 제시할 수 있는 자체 방법론을 보유하고 있다.

클라우드 보안 컨설팅 방법론은 SaaS, IaaS, PaaS에 따라 IAM, 위협 및 취약점 관리, 보안아키텍처 및 서비스, 사고 및 위기 대응, 프라이버시 및 정보보호, 리스크 및 컴플라이언스 관리, 신기술 및 트랜드의 7개 영역과 13개 세부 영역으로 구분되어 클라우드 보안을 위해 갖추어야 하는 통제 기준 및 관리 수준을 제시한다.

클라우드 서비스 통합관리체계

SaaS IaaS PaaS	리스크 및 컴플라이언스 관리	**변경통제 & 구성 관리**	• 신규 개발/인수 • 비인가 소프트웨어 설치 • 품질 테스트 • 비인가 소프트웨어 • 운영 변경
		감사 & 보증 컴플라이언스	• 정보 시스템 규제 맵핑
		연속성 관리 & 회복력	• 공급자 비즈니스 연속성 계획 장비 유지 보수 • 보존 정책
		거버넌스 & 리스크 관리	• 기준 요구사항 • 위험 평가 • 정책

SaaS IaaS PaaS	프라이버시 및 정보 보호	데이터 보안 & 정보 흐름 관리	• 분류 • 데이터 인벤토리 • 민감 데이터 거래	• 취급, 라벨링, 보안정책 • 관리 비생산 데이터 • 안전한 폐기
		암호화 & 키 관리	• 권한 부여 • 키 생성	• 민감 데이터 보호/암호화 • 저장 및 접근
	보안 아키텍처 및 서비스	어플리케이션 & Interface 보안	• 데이터 무결성	
		인프라 & 가상화 보안	• 감사 로그/침입 탐지 • 변경 탐지 • 시계 동기화 • 용량/자원 계획 • 취약점 관리 • 네트워크 보안 • 운영체제 강화 및 기본제어 • 생산/비생산 환경 • 분리 • VM 보안 – vMotion 데이터 보호 • VMM 보안 – 하이퍼바이저/강화 • 안전한 네트워크 아키텍처	
	신기술 및 트렌드	상호운용성 & 이식성	• APIs(표준, 개방형) • API 사용을 위한 정책 및 절차	• 표준(보안) 네트워크 프로토콜 • 가상화 표준 형식
		모바일 보안	• 클라우드 서비스	
	사고 및 위기대응	보안사고관리 E-Discovery	• 사건 관리 • 사건 보고	• 사건 대응 법적 준비 • 사건 대응 매트릭스
	TVM	위협 & 취약점 관리	• 안티바이러스/악성 소프트웨어 • 취약점/패치 관리	
	IAM	인증 & 접근관리	• 감사 도구 접근 • 사용자 접근 정책 • 진단/구성 포트 접근 • 사용자 식별 및 관리(정책 및 절차) • 제 3자 접근 • 사용자 접근 권한 부여 • 사용자 접근 검토 • 사용자 접근 철회 • 사용자 ID 자격 증명 • 유틸리티 프로그램 접근	

Source: PwC

PwC는 이러한 클라우드 보안 컨설팅 방법론을 통해
클라우드 보안 전략 수립, 클라우드 보안 취약점 진단, 거버넌스 및 아키텍처 수립,
클라우드 보안 인증 및 규제 대응 자문 서비스를 제공한다.

PwC의 클라우드 보안 자문 서비스

클라우드 거버넌스 진단/체계

- Cloud 보안 역량 진단 / Cloud 전환 조직 설계
- Cloud 정책 지침 제·개정

클라우드 마이그레이션 보안

- Cloud 보안 아키텍처 수
- Cloud 랜딩존 환경 설계 컨설팅
- Cloud Native 서비스 구축 컨설팅
- 3rd party 솔루션 구축 컨설팅

클라우드 취약점 진단

- Cloud 보안 설정 취약점 진단
- 보안 설정 개선 컨설팅
- 보안 상시 진단 서비스

클라우드 보안 인증/규제 대응

- Cloud 자산 관리 체계 수립
- 정보보안 통합 인증 관리 체계 수립
- 정보 클라우드 규제 대응

Source: PwC

특히 AWS, MS Azure 등 다양한 CSP의 클라우드 보안 취약점 진단 도구(Cloud Shield)를 보유하고 있어 짧은 시간 내 사용 중인 모든 클라우드 상의 서비스 및 리소스를 가시화하고 랜딩존, 네트워크, EC2 등을 대상으로 계정, 패스워드/인증, 암호화, 권한, 로깅, 접근통제 등의 각종 보안 기능 및 설정들이 활성화 또는 적용되어 있는지 보안 관점에서 진단할 수 있으며 패치 설정, 가용성, 백업, 변경 방지, 작업 알람 설정 등 시스템 안정성 관점에서도 진단할 수 있다.

Cloud Shield는 고객의 클라우드 계정과 연동하는 즉시, 웹 콘솔을 통해 보안 설정 진단 기능을 사용할 수 있다. 이를 통해 AWS, MS Azure의 다양한 서비스에 대한 보안 설정을 자동으로 점검하여 이에 따른 조치 방안까지 제공한다. 특히 Cloud Shield는 PwC의 풍부한 온프레미스 및 클라우드 보안 전문가들의 경험과 노하우를 반영하여 개발된 진단 항목을 제공하기 때문에 정보보안 담당자들이 더욱 쉽게 점검 항목과 결과를 이해할 수 있도록 도움을 준다. Cloud Shield 진단 결과를 토대로 클라우드 네이티브 아키텍처 분석과 제3자 솔루션 분석과 대체 통제 현황 분석을 통해 맞춤형 개선 방안을 수립하는 서비스를 제공한다.

PwC Cloud shield 기반 진단 및 개선 서비스

Cloud 보안 설정 자동화 진단

리소스별 보안 설정 값 검토	실시간 리소스 변화 탐지	자동화 Alert& Alarm
Cloud 리소스 특성에 맞는 보안 설정 및 구성 항목 상세 점검	컴플라이언스 충족 비율 점검	Cloud 인프라 환경에 심각한 보안 설정 오류 발견 시 담당자 알람 (Ticketing, E-mail 등) 생성

대체 통제 현황분석

담당자 인터뷰	대체 통제 시나리오 분석	3rd party 보안 솔루션 분석
담당자 인터뷰가 필요한 점검 항목을 정의하여 고객 Cloud 인프라 환경 상세 분석	Cloud 내 유사 서비스 및 리소스를 분석, 대체 보안 통제 적용 여부 검토	Native Cloud 보안 서비스 외 3rd party 솔루션/장비 분석, 대체 통제 적용 여부 검토

개선안 제시

Cloud Native 조치 가이드 제공	3rd Party 보안 솔루션 조치 가이드 제공
3rd Party 보안 솔루션 적용 미흡 사항 및 적용 방안 제공 *온프레미스 및 Cloud 적용 사항 교차 분석 및 가이드	Cloud Native 보안 설정 오류 및 미흡 사항 조치 방안 제공 *개별 설정이 아닌 전체 인프라 보안아키텍처 분석 및 가이드

Source: PwC

또한, 클라우드 보안 및 성능/가용성의 확보 수준과 클라우드 TCO는 상호 밀접하게 연관되어 있고, 상충관계가 있다. 즉, 비용을 들이면 들일수록 보안 및 성능은 높아질 수 있으나, 그에 따른 과다할 수 있는 비용도 수반된다. 기업의 비즈니스 특성에 따라 적정 보안과 성능/가용성 수준을 설정하고 이에 따른 클라우드 인프라 구성을 설계 정의해야 한다.

클라우드 비용을 아키텍처 및 구성을 변경하여 일회성으로 최적화하는 것뿐만 아니라, 기술적인 관점이 아닌 업무, 서비스 중심으로 비용의 가시성을 확보하고 이를 지속적으로 최적화할 수 있는 프로세스와 조직 체계를 갖추는 것을 핵심으로 한다. 또한 각 클라우드 비용을 현업 부서에 명확히 귀속함으로써 그 책임성을 명확히 함도 아울러 목적으로 하고 있다. 글로벌에는 FinOps, Finance기반 클라우드 오퍼레이션 접근이 주목받고 있다.

PwC는 클라우드 보안과 함께 IT역량 및 아키텍처 그리고 비용까지 종합적 관점에서 최적화하여 과다 혹은 과소하지 않은 최적의 인프라 환경구성을 제언할 수 있다. 기업의 전반적 클라우드 보안/IT환경 이슈에 선제적 대응과 안정적 운영을 위해 객관적으로 현 수준을 진단해보고, 대책을 마련할 수 있다.

PwC Cloud Fin Ops 진단모델

일반적으로 클라우드 비용을
10~20% 절감하는
기회 발굴 가능

*Global PwC 고객사를 대상으로 산정된 추정치임

Cost optimization

- 기업의 클라우드 리소스에 대한 보다 효율적인 지출과 전반적인 비용 절감 전략을 제시
- 클라우드 자원활용의 낭비를 제고하고, 리소스 할당관리 등 비용 효율적인 관점에서 최적화 방안 도출

Improved financial visibility and accountability

- 클라우드 비용추적, 자원할당, 리포팅을 위한 프로세스 · 도구를 설정하여 전체적인 클라우드 비용 가시성 확보
- 이해관계자의 요구사항 및 의사결정이 클라우드 비용에 재정적 영향도를 시뮬레이션 하여 비용 오너십 강화

Better decision making

- 클라우드 비용 및 사용패턴에 대한 분석을 통에 인프라 투자에 대해 데이터 기반 의사결정을 지원
- 클라우드 활용에 의한 비즈니스 목표를 보다 효율적으로 달성 하도록 기여

Increased agility and innovation

- 기업의 인프라의 성능 및 안정성에 중점을 두면서, 새로운 클라우드 서비스를 실험
- 클라우드 비용 절감의 기회를 식별하면서도, 지속적인 개선과 혁신 문화를 장려함

Enhanced collaboration

- IT 및 재무, 비즈니스 현업 부서간 협업을 촉진
- 전사 조직의 재무 목표에 맞춰 조정되고, 이를 달성하기 위한 협력체계를 구성함

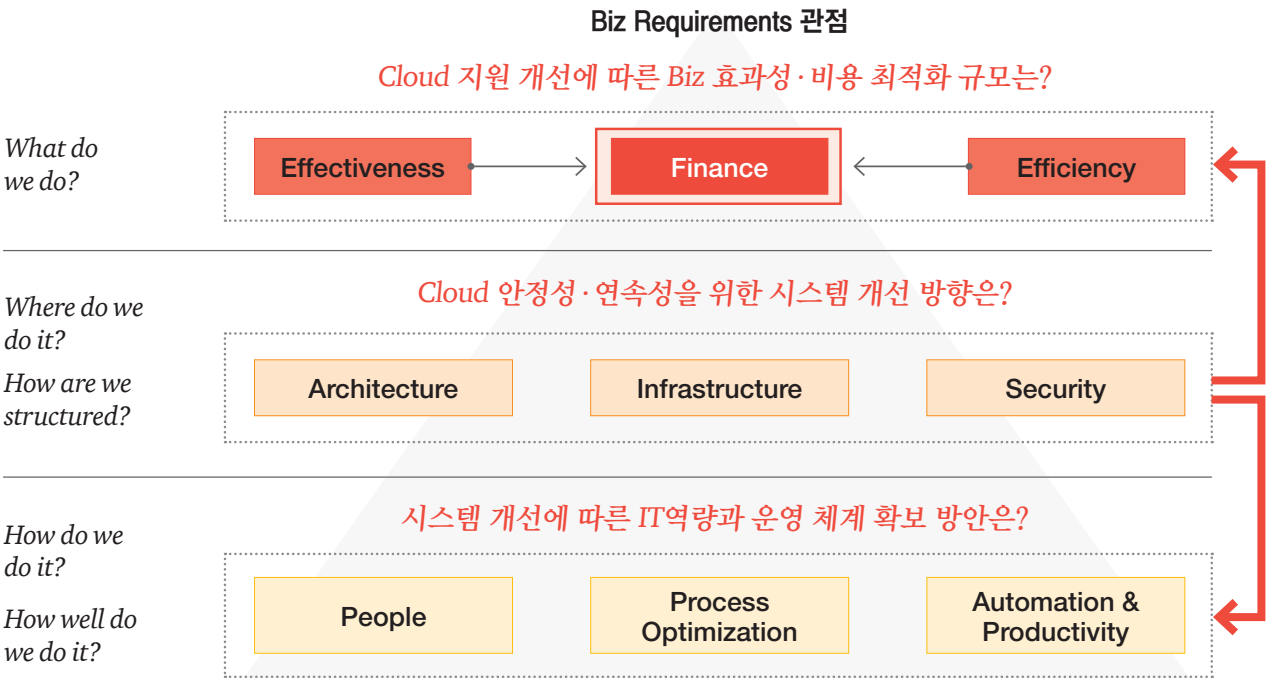
Scalability

- 비즈니스가 성장함에 따라 클라우드 인프라가 확장되더라도 TCO를 효과적으로 관리할 수 있는 프레임워크 제공
- 지속적 사용량 증가에 따라 클라우드 지출의 통제 가능

Source: PwC

PwC Fin-Ops 진단 접근은 아키텍처와 보안, TCO가 별개의 문제가 아니라
하나의 통합된 관점에서 살펴보고 상호간의 균형 잡힌 대안을 모색이 가능하며,
기업의 비즈니스 특성, 환경을 고려하여 아키텍처의 구성 및 안정성,
보안을 TCO 관점에 최적화하여 전체적인 종합적인 대안 제시가 가능하다.

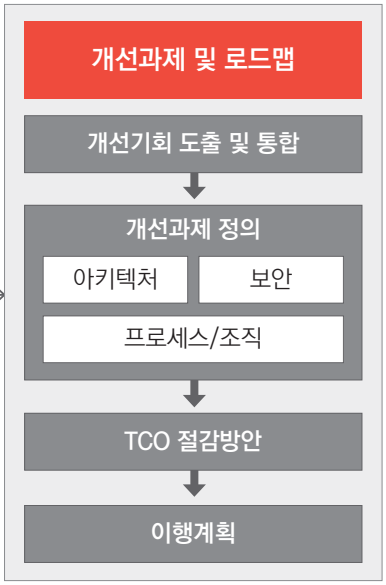
PwC Fin-Sec Ops 진단 접근방안



1. 운영 비용
- 클라우드/on-Prem기반 고려할 수 있는 비용 분석 항목 정의
- 항목별 운영 비용 추이 분석, 비용 효율화 지표 정의

2. 기술 아키텍처/보안
- IT아키텍처 · 구성 Inventory 분석
- 시스템 구성 및 구조, 장애,성능, 가용성 이슈 도출 분석
- 개인정보 보호, SW 취약점, 인프라/NW 취약점 진단 분석

3. 조직 · 프로세스
- IT/보안 거버넌스 및 운영 프로세스 · 정책분석
- IT/보안 조직 구조 및 역할/책임인적자원, 역량 분석



출처: PwC

Contacts

문 홍 기 Partner
hong-ki.moon@pwc.com
02-709-0394

구 본 재 Partner
bon-jae.koo@pwc.com
02-3781-1435

박 현 주 Partner
hyun-joo.park@pwc.com
02-3781-9675

이 성 호 Partner
sungho1.lee@pwc.com
02-3781-1773

www.pwcconsulting.co.kr

S/N: 2408C-RP-046