# FOCUS IN-DEPTH

# CLOUD SECURITY

보안도 이제 클라우드 시대

# 클라우드 시대의 보안 위협과 대응 전략

코로나19로 인해 언택트 기술이 각광받고 있다. 그 이면에는 클라우드 컴퓨팅이 존재한다. 초중고생들의 온라인 개학도 클라우드가 있기에 가능했다. 포스트 코로나를 대비해 많은 기업들이 핵심적인 업무를 클라우드로 이전하고 있다. KPMG의 클라우드 보안 위협보고서에 따르면, 90%에 달하는 기업들이 SaaS(Software as a Service)를, 76%의 기업들이 IaaS(Infrastructure as a Service)를 도입해 사용하고 있고, 절반 이상의 기업들은 향후 2년 안에 모든 데이터를 클라우드로 이전할 계획인 것으로 나타났다. 이런 가운데 클라우드 상에서 IT 부서와 클라우드 서비스 제공업체가 책임을 분담하는 과정에서 보안의 사각지대가 꾸준하게 발생하고 있다. 클라우드 시대에 어떤 보안 위협들이 공존하며 보안 대책으로 할 점은 무엇인지 알아본다.

2019년은 퍼블릭 클라우드 도입이 꽃 핀 한 해라고 해도 과언이 아니다. 시장조사기관 가트너는 전 세계 퍼블릭 클라우드 시장 규모가 2018년 1,824억 달러에서 2019년엔 17.5% 증가한 2,143억 달러로 증가했고 2022년까지 클라우드 서비스 시장 규모 및 성장세가 전체 IT 서비스 성장세의 3배에 달할 것으로 예측했다. 국내에서도 과학기술정보통신부가 2019년 말 제2차 클라우드 컴퓨팅 발전 기본계획을 공표하면서 클라우드 시장 규모가 해외는 23.1%, 국내는 16.8% 성장이 예상됨에 따라 국내 클라우드 산업을 적극 육성하겠다고 발표했다. 자료에 따르면

국내 클라우드 시장은 올해 2조 3천억 원에서 2022년엔 3조 7천억 원까지 성장할 것으로 전망된다.

## 클라우드 환경에서의 보안에 대한 우려

하지만 클라우드의 등장을 계기로 기존과는 다른 새로운 보안 위협과 과제가 등장하고 있다는 게 전문가들의 진단이다. 미국의 클라우드 컴퓨팅 관리 회사인 라이트스케일(RightScale)에 따르면 기업들은 클라우드 도입 시 보안 이슈를 가장 큰 어려움으로 생각한다고 보고서를 통해 전했다. 엔터프라이즈 컴퓨팅 기업 뉴타닉스가 발표한 2019 글로벌 엔터프라이즈 클라우드 인덱스 보고서에서도 조사 응답자 중 60%가 클라우드 전반의 보안 현황이 향후 클라우드 배포에 가장 큰 영향을 미칠 것이라는 조사 결과를 발표했다. 클라우드의 도입은 혁신, 비용절감, 유연성 등 여러 장점이 있지만, 클라우드 전문가 부족과 보안에 대한 문제가 가장 큰 우려 사항이라는 것이다.

최근 1~2년 동안 클라우드에서 발생한 보안 사고는 큰 파장을 일으켰다. 2018년 11월 AWS 서울 리전에서 내부 DNS 서버 설정 오류로 인해 84분 동안이나 DNS 기능을 할 수 없어 AWS를 사용하는 쿠팡, 배달의민족, 이스타항공, 업비트 등에서 접속 오류 현상이 나타났다. 2019년 7월 미국의 대형 은행인 캐피탈 원(Capital One)에서는 1억 600만 명이 넘는 고객 정보가 해킹 당했는데, 유출된 데이터는 AWS에 저장된 것으로 알려져 AWS의 보안 취약성이 드러나기도 했다. AWS는 클라우드 보안의 문제라기보다 클라우드를 사용하는 기업이 보안 설정을 잘못했기 때문이라고 밝혔다. 이 같은 클라우드 보안 사고에서 보듯이 가트너는 95% 이상의 클라우드 보안 사고가 클라우드 사용자의 관리 책임이 원인일 것이라고 발표했다.

IT 인프라 운영 및 보안 전문가들이 가장 우려하는 점은 데이터의 유출 또는 유실이다. 이러한 우려는 여러 원인이 있지만, 플랫폼으로서의 서비스(Platform as a Service) 활용이 보편화 되면서 클라우드에서 이루어지는 작업 대부분이 블랙박스 형태로 전문가들조차 내부에서 무슨 일이 일어나는지 확인이 어렵기 때문이다.

## 클라우드 환경에서의 보안 위협

클라우드 보안 협회(Cloud Security Alliance, CSA)는 241명의 클라우드 전문가들을 대상으로 설문조사를 진행해 2019 클라우드 위협 보고서를 발표했다. 이 보고서는 전통적으로 클라우드의 위협, 위험 및 취약성에 대한 인식을 제고하기 위한 것이다. 응답자들은 클라우드 환경에서의 주요 위협을 다음의 11가지로 꼽았다.

1. 데이터 침해
2. 잘못된 구성 및 부적절한 변경 제어

3. 클라우드 보안 아키텍처 및 전략 부족
4. 불충분한 아이덴티티, 자격 증명, 액세스 및 키 관리
5. 계정 도용
6. 내부자 위협
7. 안전하지 않은 인터페이스와 API
8. 취약한 제어 영역
9. 메타 구조와 응용 구조 실패
10. 제한된 클라우드 사용 가시성
11. 클라우드 서비스의 남용 및 악의적인 사용

서비스 거부, 공유 기술 취약성 및 CSP(Cloud Service Provider) 데이터 손실, 시스템 취약성과 같은 문제는 이 보고서에서 제외했다. CSP의 책임하에 있는 전통적인 보안 문제는 그다지 중요하지 않은 것으로 판단했기 때문이다. 대신, 고위 경영진들은 기존 기술보다 높은 보안 문제를 해결해야 할 필요성이 커지고 있다.

### 1. 데이터 침해

데이터 침해는 민감하면서도 반드시 보호해야 하는 사이버 보안 사고이다. 관리자는 기밀 정보의 공개, 열람, 도난, 데이터 유출을 막는 게 주요 목표이다. 여기에는 표적 공격 또는 단순한 사람의 실수, 취약성, 부적절한 보안 관행, 공개되지 않은 모든 종류의 데이터 유출이 포함된다. 개인의 건강 정보를 포함하여 재무 정보, 개인 식별 정보, 거래 비밀과 지적 재산 등이 여기에 포함된다.

### 2. 잘못된 구성 및 부적절한 변경 제어

컴퓨팅 자산을 설정할 때 구성 오류가 발생하기도 한다. 구성을 잘못함으로써 악의적인 활동에 취약해지는 경우가 많다. 몇 가지 일반적인 예는 다음과 같다.

- 보안되지 않은 데이터 저장 요소 또는 컨테이너
- 과도한 권한
- 기본 자격 증명 및 구성 설정을 그대로 유지
- 표준 보안 제어 비활성화

클라우드 리소스를 잘못 구성하면 데이터 유출과 서비스 중단의 주요 원인이 된다. 클라우드 환경에서 구성이

잘못되는 일반적인 이유는 효과적인 변경 제어 프로세스가 없을 경우이다. 클라우드 환경 및 컴퓨팅 방법론은 기존의 IT와 다르게 변경 제어하기가 더 어렵다.

기존의 변경 프로세스에는 여러 가지 역할 및 승인이 포함되어 있으며 생산 단계에 도달하는 데 며칠 또는 몇 주가 걸릴 수 있다. 회사의 데이터 센터에서 정적인 인프라 요소는 이제 클라우드의 소프트웨어로 추상화되며 전체 수명 주기는 몇 분 또는 몇 초 동안만 지속될 수도 있다. 클라우드 컴퓨팅 기술은 자동화, 역할 확장 및 액세스를 기반으로 빠른 변화를 지원한다.

클라우드 공급자는 거의 매일 향상되고 확장되는 고유한 기능을 가지고 있기 때문에 여러 클라우드 공급자를 사용하면 복잡성이 증가할 수밖에 없다. 이러한 역동적인 환경에는 많은 회사가 아직 익숙하지 않은 상태인 변화 제어 및 개선을 위한 민첩하고 능동적인 접근 방식이 필요하다.

### 3. 클라우드 보안 아키텍처 및 전략 부족

전 세계적으로 기업들은 IT 인프라의 일부를 클라우드로 마이그레이션하고 있다. 이 전환 과정에서 가장 큰 문제 중 하나는 사이버 공격을 견딜 수 있는 적절한 보안 아키텍처를 구현하는 것이다. 불행하게도, 이 프로세스는 여전히 많은 기업에서 풀지 못하고 있다. 기업에서 클라우드 마이그레이션이 기존 IT 스택 및 보안 제어를 클라우드 환경으로 간단히 바꾸려고 하는 '리프트 앤 쉬프트(Lift-and-Shift)'를 할 때 데이터는 다른 위협에 노출된다. 공유 보안 책임 모델에 대한 이해 부족도 또 다른 요인이 되고 있다.

또한 마이그레이션 기능과 속도가 보안보다 우선시되는 것도 문제다. 이러한 요소로 인해 클라우드 보안 아키텍처 및 전략 부족으로 사이버 공격에 취약한 기업이 되고 있다. 적절한 보안 아키텍처를 구현하고 강력한 보안 전략을 개발하면 클라우드에서 비즈니스 활동을 운영하고 수행할 수 있는 강력한 기반을 기업에 제공할 수 있다. 또한 클라우드 네이티브 툴을 활용하여 클라우드 환경에서 가시성을 높이면 위험과 비용을 최소화할 수 있다. 이러한 예방 조치를 취하면 위험이 크게 줄어든다.

### 4. 불충분한 아이덴티티, 자격 증명, 액세스 및 키 관리

자격 증명, 액세스 관리 시스템에는 기업에서 중요한 리소스에 대한 액세스를 관리, 모니터링할 수 있는 도구 및 정책이 포함되어 있다. 클라우드 컴퓨팅은 ID 및 액세스 관리(IAM)와 관련된 기존의 내부 시스템 관리 방식에 여러 가지 변경 사항을 도입했다. 클라우드 컴퓨팅은 아이덴티티, 자격 증명 및 액세스 관리에 크게 영향을 미치기 때문에 클라우드를 처리할 때 더 중요하다. 퍼블릭 및 프라이빗 클라우드 설정에서 클라우드 서비스 제

공업자와 클라우드 소비자는 보안을 손상시키지 않으면서 IAM을 관리해야 한다. 다음과 같은 이유로 보안 사고 및 데이터 유출이 발생할 수 있다.

- 자격 증명의 부적절한 보호
- 암호화 키, 암호 및 인증서의 정기적, 자동적인 변경 미흡
- 확장 가능한 자격 증명, 자격 증명 및 액세스 관리 시스템 부족
- 다단계 인증 사용 실패
- 강력한 비밀번호 사용 실패

ID 관리 시스템은 CSP 뿐만 아니라 수백만 사용자의 수명 주기 관리를 처리하도록 확장되어야 한다. ID 관리 시스템은 작업 종료 또는 역할 전환과 같은 인력 변경이 있는 자원에 대한 액세스의 즉각적인 프로비저닝 해제를 지원해야 한다. 이러한 ID 관리 수명 주기 프로세스는 클라우드 환경 내에서 통합되고 자동화되어야 한다.

### 5. 계정 도용

계정 도용은 악의적인 공격자가 권한이 높거나 민감한 계정에 액세스하여 악용하는 위협이다. 피싱 공격, 클라우드 기반 시스템의 악용 또는 도난당한 자격 증명은 이러한 계정을 손상시킬 수 있다. 독특하고 잠재적인 강력한 위협으로 인해 데이터 자산 손실 및 운영 중단과 같은 클라우드 환경이 중단될 수 있다.

이러한 위험은 클라우드 서비스의 제공 모델과 조직 및 거버넌스의 모델에서 비롯된다. 데이터 및 애플리케이션은 클라우드 서비스 또는 클라우드 계정, 구독에 상주하고 있다. 특히 구독은 권한 및 자격 증명을 거친 모든 사람이 온라인으로 액세스할 수 있다. 기업들은 이러한 위협과 심층 방어 보호 전략을 인식해 적극적으로 위반 피해를 방지해야 한다.

### 6. 내부자 위협

카네기 멜론 CERT(Computer Emergency Response Team)는 내부자 위협을 다음과 같이 정의하고 있다. “조직의 자산에 대한 액세스 권한이 있거나 없는 개인이 악의적이거나 의도하지 않은 방식으로 액세스하여 악의적인 영향을 줄 수 있는 방식으로 행동하는 잠재적인 조직”이라고 설명한다.

내부자는 현재 또는 이전 직원, 계약자 또는 기타 신뢰할 수 있는 비즈니스 파트너일 수도 있다.

외부 위협 행위자와 달리 내부자는 방화벽, VPN(가상사설망) 및 다른 경계 보안 방어에 침투할 필요가 없다. 내부자는 네트워크, 컴퓨터 시스템 및 민감한 회사 데이터에 직접 액세스할 수 있는 회사의 보안 신뢰 범위 내에서 운영된다.

### 7. 안전하지 않은 인터페이스와 API

클라우드 컴퓨팅 제공업체는 일련의 소프트웨어 사용자 인터페이스를 제공하고 있다. 사용자 인터페이스와 API를 통해 고객은 클라우드 서비스를 관리하고 상호 작용할 수 있다. 일반적인 클라우드 서비스의 보안 및 가용성은 이러한 API의 보안에 따르고 있다.

인증 및 액세스 제어에서 암호화 및 활동 모니터링에 이르기까지 이러한 인터페이스는 보안 정책을 우회하려는 우발적이거나 악의적인 시도로부터 보호하도록 설계되어야 한다. 잘못 설계된 API는 데이터 유출을 유발하거나 더 악화시킬 수 있다. 따라서 기업들은 이러한 인터페이스를 디자인하고 제시하는 데 필요한 보안 요구 사항을 이해할 수 있어야 한다.

API와 사용자 인터페이스는 일반적으로 시스템에서 가장 노출된 부분으로, 외부에서 사용 가능한 공개 IP 주소를 가진 유일한 자산이다. 때문에 지속적으로 공격받을 가능성이 높다. 따라서 의도적인 보안 공격으로부터 보호할 수 있는 적절한 제어가 필요하다.

### 8. 취약한 제어 영역

데이터 센터에서 클라우드로 이동하면 데이터 스토리지 및 보호 프로그램을 구축하는 데 있어 몇 가지 어려움이 발생한다. 사용자는 데이터 복제, 마이그레이션 및 스토리지를 위한 새로운 프로세스를 개발해야 하며, 멀티 클라우드를 사용하는 경우 훨씬 더 복잡해진다.

제어 영역은 데이터의 안정성과 런타임을 제공하는 데이터 영역을 보완하는 역할을 가능하게 하므로 이러한 문제에 대한 솔루션을 제시할 수 있어야 한다. 제어 영역이 약하면 시스템 설계자 또는 데브옵스(DevOps) 엔지니어가 데이터 인프라의 논리, 보안 및 검증을 완전히 제어하지 못한다. 이러한 제한으로 인해 데이터 손상, 사용 불가 또는 유출이 발생할 수 있다.

### 9. 메타 구조와 응용 구조 실패

클라우드 서비스 제공 업체는 시스템을 성공적으로 구현하고 보호하는데 필요한 운영 및 보안 보호 기능을 정기

적으로 제공한다. 일반적으로 API 호출은 이 정보를 공개하고 보호 기능은 CSP의 메타 구조 계층에 통합된다.

이 모델에는 여러 수준에서 장애 가능성이 존재한다. 예를 들어 CSP에 의한 API 구현이 좋지 않으면 공격자는 서비스의 기밀성, 무결성 또는 가용성을 방해해 클라우드 고객을 혼란에 빠뜨릴 수도 있다. 고객에 대한 클라우드 가시성을 높이기 위해 CSP는 보안 프로세스와 API 상호 작용을 공개하거나 허용하고 있다. 하지만 서투른 CSP는 종종 고객에게 API를 어떻게 제공해야 하는지 방법과 범위에 대해 잘 알지 못한다.

클라우드 소비자는 클라우드 플랫폼을 완전히 활용하기 위해 클라우드 애플리케이션을 올바르게 구현하는 방법을 이해해야 한다. 예를 들어, 클라우드 인프라용으로 설계되지 않은 응용 프로그램은 사용 가능한 클라우드 리소스 및 기능을 완전히 활용할 수 없다. 비즈니스 운영 및 애플리케이션을 클라우드로 마이그레이션 할 때 '리프트 앤 쉬프트(Lift-and-Shift)' 접근 방식만으로는 충분치 않을 수 있다.

### 10. 제한된 클라우드 사용 가시성

조직 내 클라우드 서비스 사용이 안전한지 아니면 악의적인지 분석할 수 있는 능력이 없는 기업에서는 클라우드 사용의 가시성이 제한된다. 이 개념은 두 가지 주요 과제로 나뉜다.

첫째는 승인되지 않은 앱 사용이다. 직원이 회사 IT 및 보안에 대한 특정 권한 및 지원없이 클라우드 애플리케이션 및 리소스를 사용하는 경우에 발생한다. 이 시나리오에서는 섀도(Shadow) IT라는 자체 지원 모델이 생성된다. 안전하지 않은 클라우드 서비스 활동이 회사 지침을 충족하지 않는 경우, 특히 민감한 회사 데이터와 같이 발생할 경우 이 동작이 매우 위험할 수 있다. 가트너는 2020년까지 기업에 대한 모든 보안 공격의 3분의 1이 섀도 IT 시스템 및 리소스를 통해 발생할 것으로 예측하고 있다.

둘째는 승인된 앱의 오용이다. 기업에서는 승인된 앱을 사용하는 내부자가 승인된 애플리케이션을 어떻게 활용하는지 분석할 수 없는 경우가 많다. 이 경우엔 회사의 허락없이 외부 위협 행위자가 자격 증명을 도용하고 SQL 인젝션, DNS 공격 등의 방법을 사용할 수 있다. 대부분의 경우 이 같은 행동이 표준을 벗어난 건지, 회사 정책을 준수하는 건지 여부를 결정해서 사용자를 구분할 수 있어야 한다.

### 11. 클라우드 서비스의 남용 및 악의적인 사용

공격자는 클라우드 컴퓨팅 리소스를 활용하여 사용자, 조직 또는 기타 클라우드 공급자를 대상으로 악의적인 행위를 할 수 있다. 공격자는 클라우드 서비스에서 멀웨어를 호스팅할 수도 있다. 멀웨어가 CSP 도메인을 사용

하기 때문에 멀웨어를 호스팅하는 클라우드 서비스가 합법적으로 보일 수 있다. 또한 클라우드 호스팅 멀웨어는 클라우드 공유 도구를 공격 경로로 사용하여 자체 전파할 수도 있다. 클라우드 리소스 오용의 다른 예는 다음과 같다.

- DDoS 공격 감행
- 스팸 및 피싱 메일 발송
- 디지털 화폐 채굴
- 대규모 자동화된 클릭 공격 감행
- 크리덴셜 스터핑(Credential Stuffing)
- 악성 또는 불법 복제된 콘텐츠 호스팅

클라우드 서비스 오용에는 지불 수단 사기의 CSP 탐지 및 클라우드 오퍼링 오용이 포함된다. CSP는 리소스 오용을 해결하기 위해 사고 대응 프레임워크와 고객이 공급 업체에서 발생한 남용을 보고할 수 있는 수단을 갖추어야 한다. CSP에는 고객이 파일 공유 또는 스토리지 애플리케이션뿐만 아니라 클라우드 워크로드의 상태를 모니터링할 수 있는 관련 제어 기능도 포함해야 한다.

## 클라우드 환경에서의 보안 대책

모든 기업과 기관들은 프라이빗, 하이브리드 및 퍼블릭 클라우드를 포함하는 디지털 서비스의 안전한 사용을 위해 그에 적합한 솔루션을 요구하고 있다. 따라서 IaaS(Infrastructure as a Service), aPaaS(Application Platform as a Service), fPaaS(function Platform as a Service) 및 SaaS(Software as a Service) 등 점점 더 복잡해지고 있는 클라우드 인프라에 대한 장기적인 관점에서의 보안 전략을 세워야 한다.

그러기 위해서는 전략 및 아키텍처, 리더십, 운영, 그리고 기술 분야 전반에 걸친 새로운 보안 기술이 필요하다. 클라우드 서비스 벤더가 제공하는 툴과 클라우드 보안 제공업체의 서비스를 제대로만 활용한다면 클라우드 위협에 대한 효과적인 방어를 수행할 수 있다. 그러나 보안 관리자가 이러한 최신 클라우드 기술을 얼마나 잘 이해하고 효과적으로 활용하느냐가 관건이다. 따라서 보안 관리자는 최신 기술을 학습하기 위해 힘쓰는 것은 물론 이를 활용하여 비즈니스 환경 및 클라우드 보안 요구 사항을 모두 충족하는 방법에 대해 끊임없이 고민해야 한다.

그렇다면 요즘 주목받고 있는 클라우드 보안 기술은 무엇인가? 기술 전문가들은 클라우드에서 주목받고 있는 핵심 보안 기술로 클라우드 액세스 보안 브로커(Cloud Access Security Broker, CASB), 클라우드 워크로드 보

안 플랫폼(Cloud Workload Protection Platform, CWPP), 클라우드 보안 형상 관리(Cloud Security Posture Management, CSPM) 등을 꼽고 있다.

CASB는 기업이 SaaS(Software as a Service)에서 사용하는 애플리케이션에 대한 가시성(Visibility), 데이터 보호(Data Security), 규정준수(Compliance), 위협 보호(Threat Protection) 등을 담당한다.

CWPP는 워크로드 중심의 보안 제품이며, 하이브리드 및 멀티클라우드 데이터 센터 아키텍처에서 서버 워크로드를 보호한다. 따라서, CWPP는 위치와 관계없이 물리적 시스템, 가상 시스템, 컨테이너 및 서버리스 워크로드에 대해 일관된 가시성과 제어 기능을 제공해야 한다. CWPP 오퍼링은 런타임에서 시스템 무결성 보호, 애플리케이션 제어, 메모리 보호, 행위 모니터링(behavioral monitoring), 호스트 기반 침입 방지 및 안티-멀웨어 옵션을 결합하여 워크로드를 공격으로부터 보호해야 한다.

CSPM은 클라우드 서비스의 구성 위험 평가 및 관리를 하는 것으로, IAM 서비스, 네트워크 연결/구성, 스토리지 구성 및 PaaS 서비스를 관리한다. CSPM 핵심 엔터프라이즈 통합은 IaaS에서 SIEM 및 분석 플랫폼에 대한 클라우드 구성 및 서드 파티(3rd party) 툴의 커스터마이즈를 통해 PaaS(Platform as a Service)의 구성 문제를 감지한다. 여러 IaaS 클라우드에서 일관된 보안 위협 흐름도를 기업에 제공할 수 있다. 이러한 도구는 데브섹옵스(DevSecOps) 기능과 통합되어 구성 및 배포를 돕고 일부 치료(remediation) 기능을 자동화할 수 있다.

CASB, CSPM, CWPP는 클라우드 보안 위협을 해결할 수 있는 중복된 기능을 제공하지만, 하나의 기술이 다른 기술의 모든 기능을 수행하지 못한다. 따라서 여러 제공업체가 이 3가지 기술의 모든 기능을 제공하려는 추세이다. CASB는 주로 SaaS 보안에 중점을 두고 있으며 일부 기능은 IaaS까지 확대된다. CWPP는 IaaS 보안 및 컨테이너 워크로드에 대한 보호 기능, CSPM은 주로 IaaS 클라우드 스택 전반의 보안 평가 및 컴플라이언스 모니터링에 중점을 둔다.

그 외에도 클라우드 보안을 위해 관리자는 개발 및 운영팀의 애자일 방식 협력을 통해 지속적 통합/지속적 전달(CI/CD) 파이프라인으로 구축하고 데브섹옵스(DevSecOps) 프로세스 및 기능을 최대한 활용하는 데 힘써야 한다.

무엇보다 중요한 것은 클라우드 전환에 있어서 새로운 방식에 대한 오픈 마인드(open-mind)를 갖는 것이다. 클라우드 기술 및 트렌드는 빠르게 변화할 것이다. 클라우드 보안 관리자는 CASB/CSPM/CWPP 툴, 클라우드 보안 프레임워크, 아키텍처 요구 사항과 모범 사례, 클라우드 ID 및 액세스 관리(IAM), IaaS/PaaS/SaaS 환경의

네이티브 보안 기능 등에 대한 핵심 역량을 습득하거나 발전시키기 위해 노력해야 한다.

그러나, 클라우드 보안이 아무리 혁신적인 기술과 접근 방식을 가지고 있어도 여전히 '보안'이다. 이는 곧 보안의 가장 기본이 되는 것부터 집중하면 된다는 것이다. 기존의 기술을 클라우드 보안 아키텍처로 이전하여 새롭게 적용시키고 재고하는 능력이 요구될 것이다.

더불어 전략 계획을 수립하기 위해 비즈니스 아키텍처가 클라우드 보안에 미치는 영향을 분석하고, 클라우드를 사용하고 있거나 클라우드에 관심 있는 비즈니스와의 원만한 관계를 형성하는 방법도 잘 알아둬야 한다.