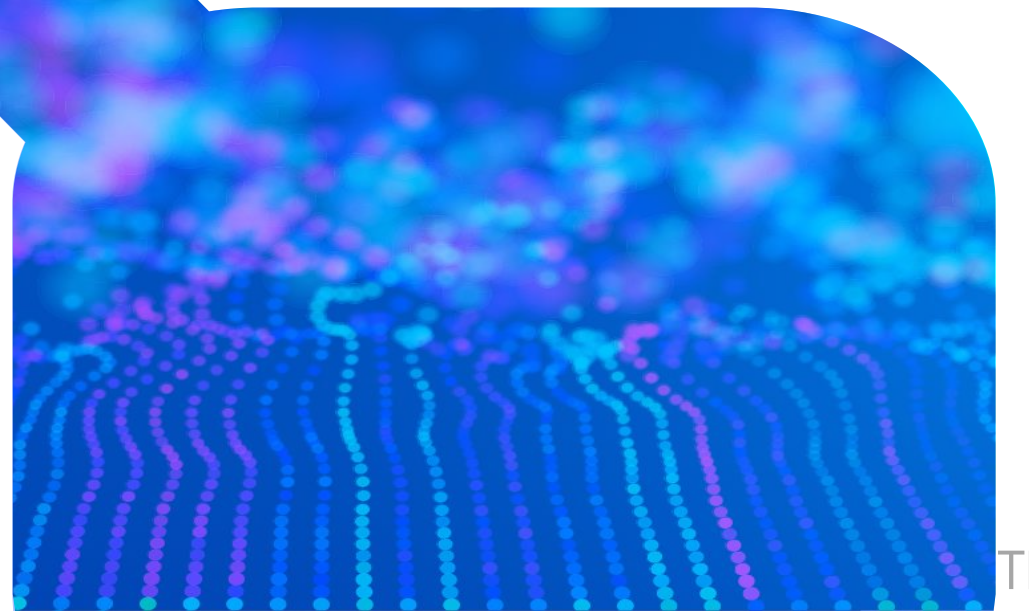
TDG

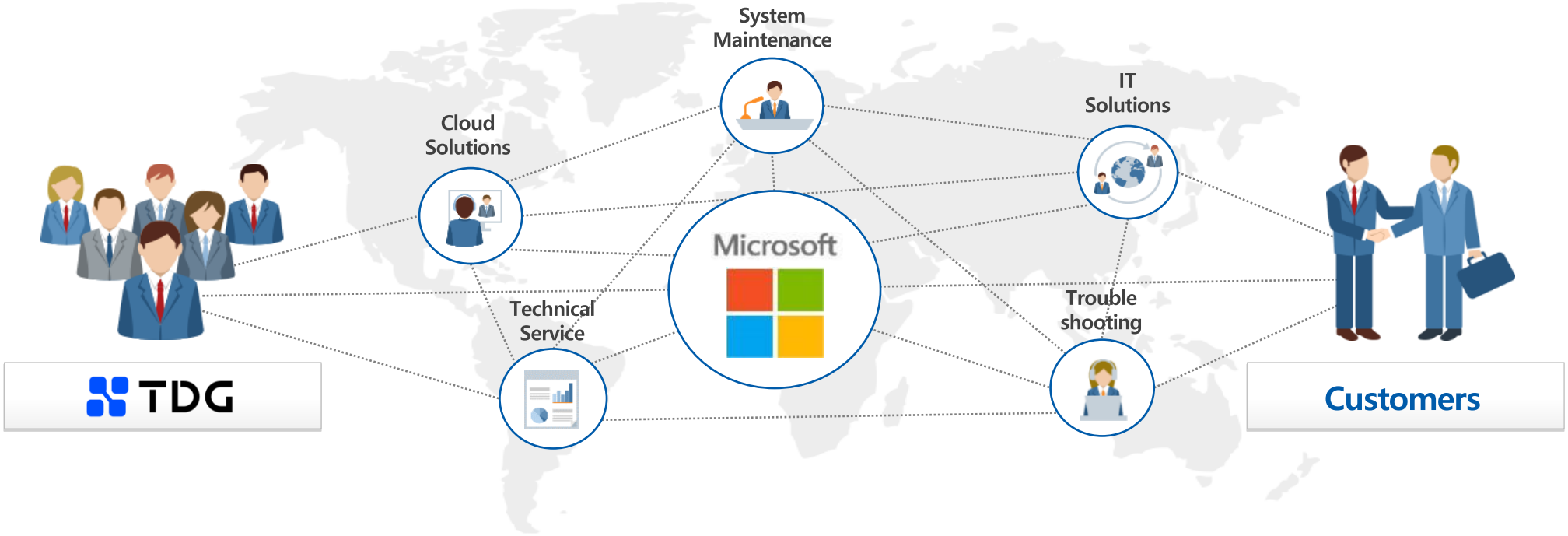
# Cloud Security Assessment Framework



# TDG 소개

**㈜TDG은 20여 년의 업력을 지켜온 IT 클라우드 전문 기업입니다**

Worldwide No.1 제품과 IT 유통 분야에의 전문성, 우수한 엔지니어 인력을 바탕으로
언제나 고객의 입장에서 더 나은 IT 환경 제공을 위해 고민할 것을 약속 드립니다.



# ㈜TDG의 사업 영역

## LSP - Licensing Solution Provider

- 한국 마이크로소프트 공인 라이선스 파트너
- 국내 커머셜 기업을 대상으로 EA(Enterprise Agreement), SCE(Server and Cloud Enrollment), MPSA 등 라이선스 프로그램 공급
- 기술 서비스, 컨설팅 제공

[ Key Clients ]

NH NongHyup, LOTTE, KB, 현대중공업, 신한금융그룹, kt

## Solution & Infra Build Service

- Active Directory 기반의 통합 인프라 관리 구축
- Microsoft Infra 구축 서비스
- Password 분실 관리 보안 솔루션
- 시스템 운영 현황 모니터링 대시보드

## CSP - Cloud Solution Provider

- Cloud 전문 파트너
- M365, Azure 등 Microsoft의 클라우드 서비스 공급
- 고객의 비즈니스 환경에 맞는 Cloud 시스템 제안
- Cloud 기반의 라이선스 유통, 설계, 구축, 모니터링, 유지보수 지원

[ Key Clients ]

kt, NAVER, HYUNDAI CONSTRUCTION EQUIPMENT

## MTS - Microsoft Technical Service

- Microsoft 관련 각종 장애 지원 및 기술 교육, 사전 지원, 고객관리
- 서비스 제공 (유상 기술 지원 서비스)
- Technical Account Management
- Proactive Support
- Technical Support
- On-Site Support

[ Key Clients ]

NH NongHyup, 신한금융그룹, KB

Microsoft

# 최상의 클라우드 파트너 역량 보유

TDG

Microsoft Solutions Partner
Infrastructure
Azure

**Specialist**
Azure Virtual Desktop

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Security

Microsoft Solutions Partner
Modern Work

**Specialist**
Teamwork Deployment

Microsoft Solutions Partner
Modern Work

**Specialist**
Adoption and Change Management

Microsoft Solutions Partner
Modern Work

**Specialist**
Meetings and Meeting Rooms for Microsoft Teams

# ㈜TDG 클라우드 사업 영역

## AZURE INFRA BUILD SERVICE

- Azure 클라우드 구축 지원
- On Premise와 M365 연동을 통한 보안 및 관리 일원화

## Microsoft 365 SETUP SERVICE

- 현재 고객사에서 운영 중인 Infra와 M365에 대한 통합, Migration 구축 서비스
- M365 기반 보안, 정보 보호, 문서 관리 서비스 구축 지원
- Power Platform 컨설팅 및 구축서비스

## SOLUTION AND SETUP SERVICE

- Active Directory 기반의 통합 인프라 관리 구축
- Microsoft Infra 구축 서비스
- Password 분실 관리 보안 솔루션
- 시스템 운영 현황 모니터링 대시보드

## CLOUD MANAGED TECH SUPPORT

- TDG 자체 Hot-Line 기술지원 콜센터 운영

# 클라우드 보안의 중요성

클라우드 환경은 On-Premise 환경과 또다른 성격의 보안 통제가 필요합니다.

인터넷을 기반으로 데이터, 서버, 저장공간, 애플리케이션, DB 등을 언제 어디서나 접근 가능하여 편리하지만 이 때문에 큰 보안 문제가 대두됩니다.

전세계적으로 이러한 클라우드 보안의 중요성을 강조하며 예상 피해액, 관련 주요 위협 요소를 선별한 보고서를 발표한 바 있습니다.

EDITORS' PICK | 7,160 views | Feb 13, 2020, 06:22am EST

## The FBI Issues A Powerful $3.5 Billion Cybercrime Warning

**Davey Winder** Senior Contributor

Cybersecurity

*I report and analyse breaking cybersecurity and privacy stories*


Newly published FBI report reveals that the cybercrime economy shows no sign of slowing down LIGHTROCKET VIA GETTY IMAGES

The Federal Bureau of Investigation (FBI) has released the Internet Crime Complaint Center (IC3) "2019 Internet Crime Report." For everyone but those engaged in cybercrime, it makes for very difficult reading. Across that one year, the number of cybercrime complaints from both individuals and business organizations reached a

> 뉴스

How To / 보안 / 클라우드 2019.10.16

## 최악의 클라우드 보안 위협 11가지

Bob Violino | CSO

**클라우드 컴퓨팅은 기업이 데이터와 애플리케이션, 워크로드를 사용하고, 보관하고, 공유하는 방식을 혁신하고 있다. 하지만 동시에 여러 새로운 보안 위협과 도전과제도 생겨난다. 많은 데이터가 퍼블릭 클라우드 서비스를 중심으로 클라우드로 이동하면서 자연스레 해커의 표적이 되었다.**

가트너의 클라우드 보안 리서치 책임자 제이 하이저는 "퍼블릭 클라우드 이용이 급증하면서 많은 민감한 정보가 잠재적인 위험에 노출된 상태이다"라고 지적했다. 많은 사람의 생각과 달리 클라우드에 보관된 기업 데이터를 보호하는 책임은 클라우드 서비스 업체가 아니라 클라우드 서비스 고객인 기업에 있다.

하이저는 "우리는 클라우드 보안에 있어 변환기에 있다. 초점이 공급자에서 고객으로 이동하는 단계이다. 기업은 특정 클라우드 서비스 업체가 안전한지, 해당 서비스에서 ROI를 회수할 수 있을지 여부를 파악하는데 많은 시간을 투자하고 있으며, 이를 학습하고 있다"라고 말했다.

클라우드 보안 협회(Cloud Security Alliance, CSA)는 기업이 클라우드 보안에 관한 최신 정보를 기반으로 올바른 클라우드 도입 의사결정을 내릴 수 있도록 지원하기 위해 매년 클라우드 컴퓨팅 보안 위협 관련 보고서를 발표한다. 이 보고서는 현재 클라우드의 가장 중대한 보안 문제에 있어, CSA 공동체의 보안 전문가들이 동의하는 내용이 반영되어 있다.

올해 보고서는 '클라우드 컴퓨팅 최고의 위협 : 심각한 11가지(Top Threat to Cloud Computing: Egregious Eleven)'란 제목으로, 특히 클라우드 컴퓨팅의 특징 중 공유, 온디맨드에 관련된 11가지 보안 문제로 초점을 맞췄다. 지난 해 보고서는 12가지 위협 요소를 제기했는데, 이 중 서비스 거부 공격, 공유 기술의 취약점, 클라우드 서비스 업체의 데이터 손실 및 시스템 취약점 등은 새 보고서에서 빠졌다. 대신 기술 스택에서 더 높은 곳에 위치한 보안 문제들을 해결할 필요성이 커졌다.

# 클라우드 보안의 위협 요소

클라우드 환경에서 고려해야 할 보안의 위협 요소이며 도입하기 전, 후 검토와 관리가 필요한 부분들입니다.

| | | |
|---|---|---|
| 데이터 유출 | 접근 방식의 불충분성 | 계정 권한 관리 |
| 안전하지 않은 인터페이스와 API | 시스템 취약성 | 계정 도용 |
| 악의적인 내부자 | APT (Advanced Persistent Threats) | 데이터 손실 |
| 불충분한 실사 | DoS | 공유 기술 취약점 |

# 클라우드 보안 진단 프로세스

TDG의 클라우드 보안 진단 프로세스는 아키텍처 구성부터 시작됩니다. (요청에 따라 구축 후 진단 및 조치가 수행될 수도 있습니다.)

# 클라우드 보안 진단 기준(체크리스트 예시)

TDG의 클라우드 보안 진단은 Microsoft 의 Azure Security Benchmark를 기준으로 한 세부 항목들로 진행됩니다.

클라우드 보안 진단은 고객사의 Azure Portal 과 CLI(Powershell 등)을 통해 수행합니다.

## ❑ 보안 진단 영역

| 구분 |
|---|
| 보안성 검토 및 관리 |
| 클라우드 콘솔 계정 및 권한관리 |
| 네트워크 보안 |
| 리소스 보안 |
| Bastion Host 보안 |
| DB 보안 |
| 스토리지 보안 |
| 개인정보보호 |
| 보안운영 |
| 침해대응/로깅 |

## ❑ 보안 진단 체크리스트 (SAMPLE)

| TDG_Azure 클라우드 보안 진단 체크리스트 | | | | 점검일자 : 00/00/2020 | | O | X | N/A | Overall |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 점검자 : 이재성M | | 7 | 1 | 1 | 9 |
| | | | | 점검대상 : OO은행 OO프로젝트 | | | | 조치율 | 88.89% |
| Cloud Platform Team | | 93 ea | | | | O / X / N/A | | | |
| 구분 | 항목 | 번호 | 세부항목 | 체크리스트 | Microsoft Docs 가이드 Link | 체크 | 예외 여부 | 예외 근거 | 비고 |
| 보안성 검토 및 관리 | 보안성 검토 실시 | 1 | 클라우드 서비스 오픈 전 보안부서에 보안성 검토를 수행하고 검토 | 보안성 검토 | - | O | | | * 운영Microsoft 보안성 심의 문서 |
| | 보안 사후 관리 | 2 | 서비스 오픈 후, 보안관제 및 보안 모니터링을 실시하고, 최신 보안 | 보안 관리 | - | X | | | * 운영 |
| | | 3 | 연 1회 정기 보안점검을 실시해야 한다. | 정기 보안점검 | - | N/A | | | * 운영 |
| | | 4 | 아래의 경우 비정기 보안점검을 실시해야 한다.- 신규 서비스 오픈, 7 | 비정기 보안점검 | - | - | | | * 운영 |
| 클라우드 Portal 계정 및 권한관리 | Portal 관리자 계정관리 | 5 | 사용목적에 | | | | | | * 구축 |
| | | 6 | 용도별(개 | | | | | | |
| | | 7 | Portal 관리 | | | | | | |
| | | 8 | Portal 관리 | | | | | | |
| | | 9 | App 등록 시 | | | | | | |
| | | 10 | Portal 관리 | | | | | | |
| | Portal 사용자 계정 관리 | 11 | 모든 Portal | | | | | | |
| | | 12 | 모든 Portal | | | | | | |
| | | 13 | 모든 Portal | | | | | | |
| | | 14 | Portal 및 Ap | | | | | | |
| | | 15 | 모든 Portal | | | | | | |
| | | 16 | MFA 미설정 | | | | | | |
| | App 방식 액세스 보안 | 17 | 관리Portal( | | | | | | |
| | | 18 | Portal에 Ap | | | | | | |
| | | 19 | Portal에 Ap | | | | | | |
| | 계정 관리 | 20 | 업무담당자 | | | | | | |
| | | 21 | 업무담당자 | | | | | | |
| | | 22 | 모든 업무담 | | | | | | |
| | | 23 | 공용계정 사 | | | | | | |
| | | 24 | 미사용 계정이 발생한 경우, 해당 계정을 삭제하여 미사용 계정이 없 | 미사용 계정 삭제/관리 | https://docs.microsoft.com/ko-kr/azure/ | - | | | * 운영 |
| | | 25 | 모든 Portal 계정의 사용과 관련된 모든 이벤트(접근이력, 사용이력) | Portal 사용이력 보관(1년 이상) | https://docs.microsoft.com/ko-kr/azure/ | - | | | * 구축 |
| | SSO(Single Sign On) 적용 | 26 | Azure Portal/Azure AD 이용 시 SSO 설정을 적용한다. | Azure AD Single Sign-On 적용 여부 | https://docs.microsoft.com/ko-kr/azure/ | - | | | * 구축 |

SAMPLE

# 클라우드 보안 진단 결과보고서 예시

클라우드 보안 진단 결과보고서는 보안 수준 진단 결과(점수) 및 조치 권장 사항을 포함합니다.

SAMPLE

## Azure 클라우드 보안 진단
## 결과 보고서

점검 대상 : OO 은행 OO 프로젝트

*이 문서는 Microsoft Azure 의 Cloud 보안 요건을 체크리스트 기반으로 점검한 후의 결과 보고서입니다.*

Contents



Page | 1

SAMPLE

## Azure Security Assessment 결과

- 점검 일자 : 00/00/2020
- 점검 인원 : 이재성 M

✔ 점검 요약

| O | X | 확인 필요 | N/A | Overall |
|---|---|---|---|---|
| 35 | 25 | 11 | 22 | 93 |
| | | | 조치율 | 61.29% |

| 구분 | 조치율 | O | X | 확인 필요 | N/A | Sub Total |
|---|---|---|---|---|---|---|
| 보안성 검토 및 관리 | 100.0% | 4 | 0 | 0 | 0 | 4 |
| 클라우드 콘솔 계정 및 권한관리 | 50.0% | 11 | 11 | 0 | 0 | 22 |
| 네트워크 보안 | 66.7% | 10 | 1 | 4 | 0 | 15 |
| 리소스 보안 | 62.5% | 2 | 1 | 2 | 3 | 8 |
| Bastion Host 보안 | 100.0% | 0 | 0 | 0 | 11 | 11 |
| DB 보안 | 100.0% | 1 | 0 | 0 | 2 | 3 |
| 스토리지 보안 | 71.4% | 5 | 2 | 0 | 0 | 7 |
| 개인정보보호 | 16.7% | 1 | 0 | 5 | 0 | 6 |
| 보안운영 | 66.7% | 1 | 3 | 0 | 5 | 9 |
| 침해대응/로깅 | 12.5% | 0 | 7 | 0 | 1 | 8 |
| Grand Total | 61.29% | 35 | 25 | 11 | 22 | 93 |

- "확인 필요" : 개인정보 취급 여부 및 고객사 내 계정 권한, 네트워크 접속 승인 절차 등 현업과 인터뷰 후 확인해야하는 항목

Page | 3

SAMPLE

42. VM 이미지 보안

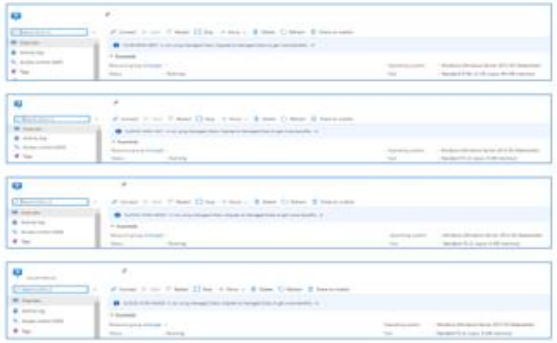
- 평가 : 양호
- 현황 : Azure 의 기본 제공 OS 중 하나인 Windows Server 2012 R2 DC 로 생성되어 있습니다.
- 가이드 링크 :

  * Windows

  https://docs.microsoft.com/ko-kr/azure/virtual-machines/windows/quick-create-portal

  * Linux

  https://docs.microsoft.com/ko-kr/azure/virtual-machines/linux/quick-create-portal

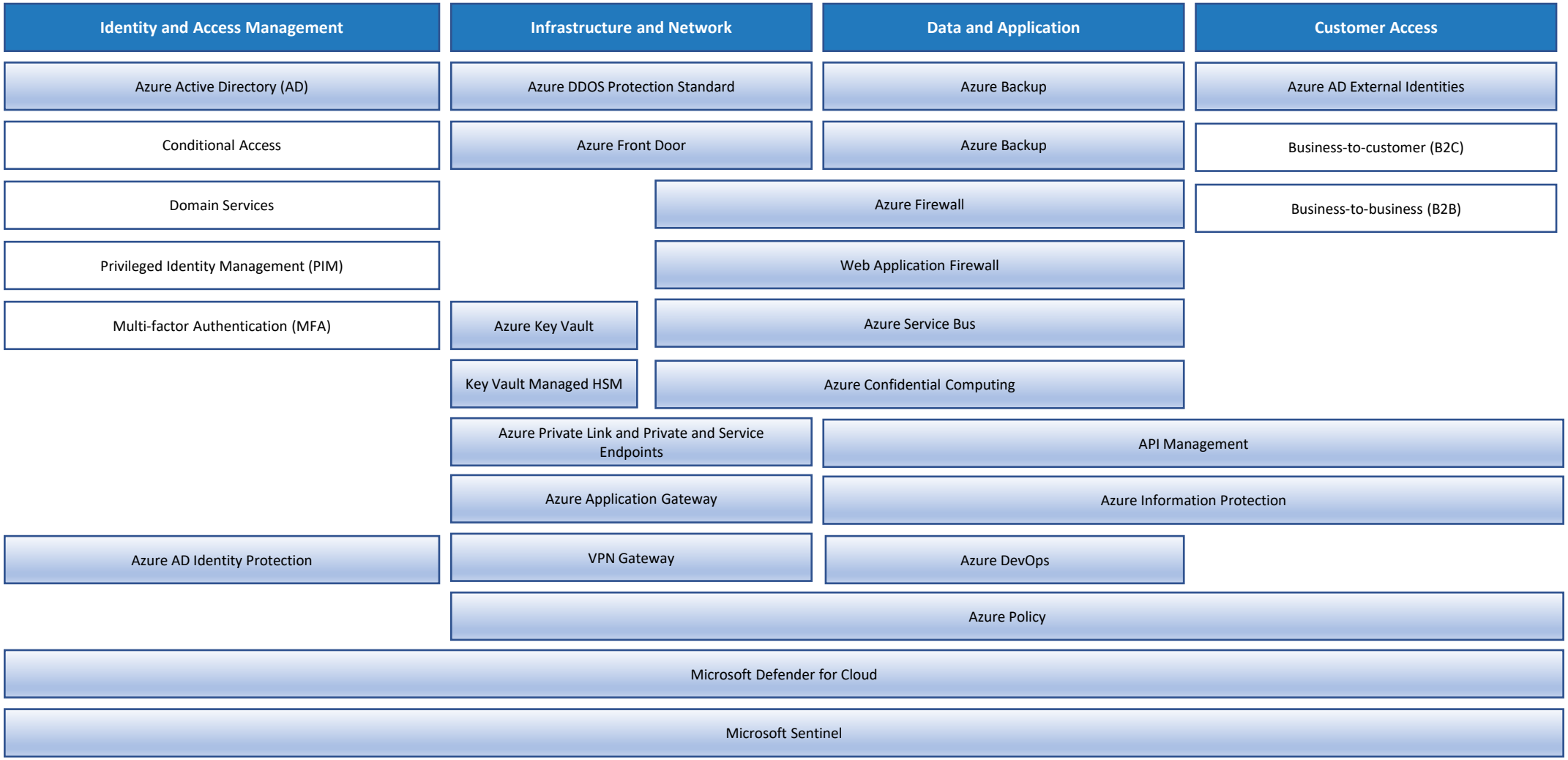


Page | 40

# 클라우드 보안 진단 일정

클라우드 보안 진단은 고객 담당자 인터뷰 및 점검 리소스의 수량 및 복잡도에 따라 유동적입니다.
보안 진단 수행부터 진단 결과 보고서 전달 까지 약 2주 정도 소요됩니다.
취약 항목 조치는 고객사마다 상이합니다.

# (참고)Microsoft 보안 서비스 맵



www.tdgl.co.kr

TDG

변화와 혁신을 통해 고객에게 최고의 가치를 제공하고 함께 성장하는 TDG가 되겠습니다.


☎ Contact. Tel. 02-2135-3311 I Fax. 02-2135-3316

✉ E-Mail. MKT@tdgl.co.kr

🏠 Address. 서울특별시 강남구 언주로 709 송암빌딩 15층