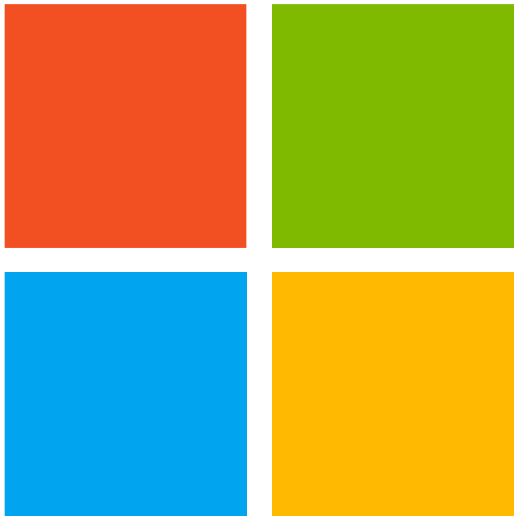






CLOUDMATE

Azure Expert Group



Microsoft

Azure는 쓰고 있는데.. 보안이 걱정되요!

<클라우드메이트 박상엽>

Agenda

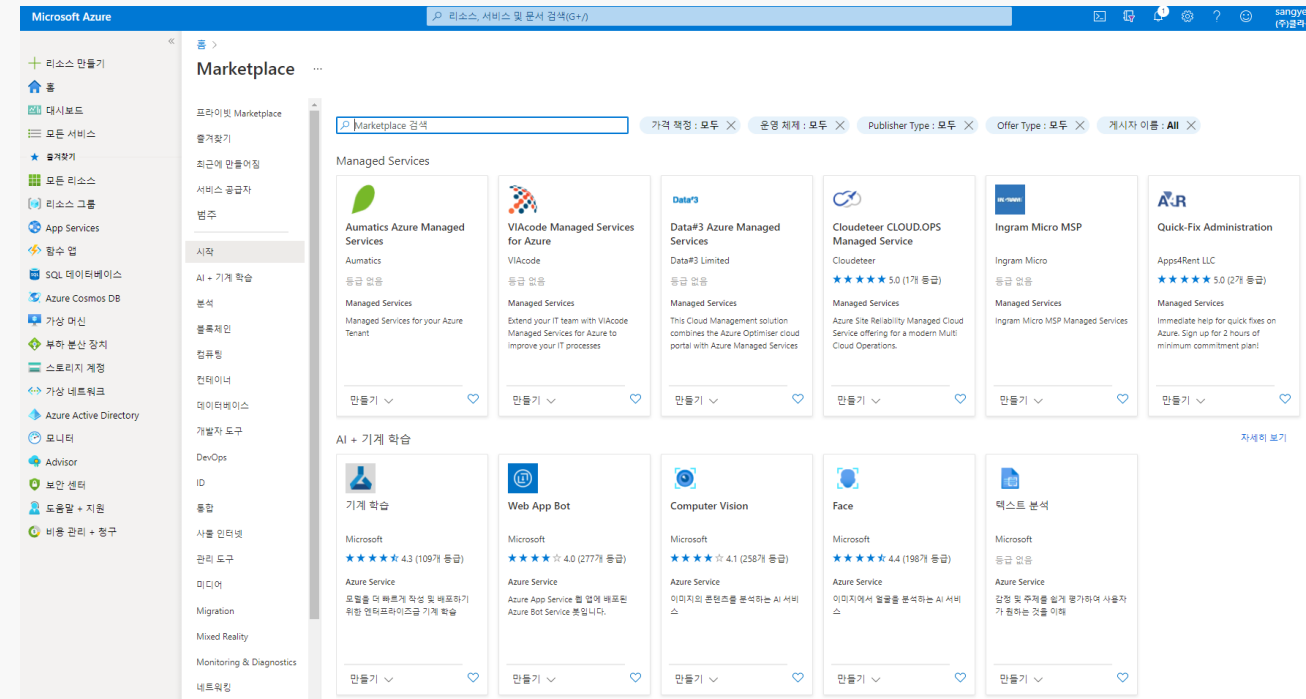
Azure를 사용합니다. 이제 뭘 해야 할까요?

내 계정은 안전할까?

다른 보안 설정은?

Azure를 사용합니다. 이제 뭘 해야 할까요?

Azure는 사용하고 있는데...



가상 컴퓨터 보안?

간단한 보안들

Network Security Group Bastion

...



adm01365

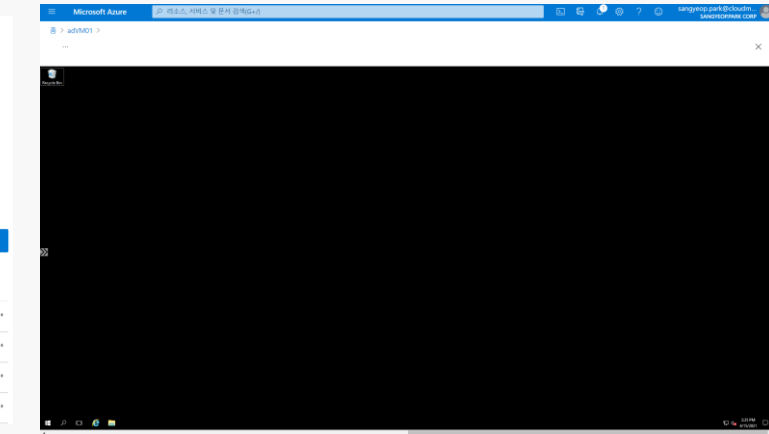
IP 구성
 ipconfig1 (기본)

네트워크 인터페이스: adm01365 [유요한 보안 규칙](#) [VM 연결 문제 해결](#) [트러블러지](#)
가상 네트워크(서브넷: assignNet/VMSubnet) NIC 공용 IP: 52.230.2.16 NIC 프라이빗 IP: 10.0.0.4 [가속화된 네트워크 사용 안 함](#)

인바운드 포트 규칙 [아웃바운드 포트 규칙](#) [해결리제이션 보안 그룹](#) [부하 분산](#)

네트워크 보안 그룹 adm-mng (네트워크 인터페이스에 연결됨: adm01365) [인바운드 포트 규칙 추가](#)
영향 0개 서브넷 2개 네트워크 인터페이스

우선 순위	이름	포트	프로토콜	소스	대상 주소	작업
100	RDP-connect	3389	모두	모두	모두	허용 ***
65000	AllowVnetInbound	모두	모두	VirtualNetwork	VirtualNetwork	허용 ***
65001	AllowAzureLoadBalancerInbound	모두	모두	AzureLoadBalancer	모두	허용 ***
65500	DenyAllInbound	모두	모두	모두	모두	거부 ***






가상 컴퓨터 보안?

좀 더 자세히..

VPN
Backup
Disk Encryption
Just In Time Access

...

가상 머신의 관리 포트는 Just-In-Time 네트워크 액세스 제어로 보호해야 합니다. ...

 제외  정책 정의 보기  쿼리 열기

심각도

높음

새로 고침 간격

 24시간

^ 설명

Azure Security Center에서 네트워크 보안 그룹의 관리 포트에 대해 허용 범위가 과도하게 큰 인바운드 규칙을 확인했습니다. 인터넷 기반의 무작위 암호 대입 공격으로부터 VM을 보호하려면 Just-In-Time 액세스 제어를 사용하도록 설정하세요. [자세히 알아보세요.](#)

^ 수정 단계

빠른 수정:

비정상 리소스를 선택하고 "수정"을 클릭하여 "빠른 수정" 수정을 실행합니다. [자세한 정보 >](#)

참고: 프로세스가 완료된 후, 리소스가 '정상 리소스' 탭으로 이동하는 데 몇 분 정도 걸릴 수 있습니다.

수동 수정:

Just-In-Time VM 액세스를 사용하도록 설정하려면 다음과 같이 하세요.

- 목록에서 VM을 하나 이상 선택하고 "수정"을 클릭하거나 특정 VM에 대한 권장 사항에 도달한 경우 "작업 수행"을 클릭합니다.
- "JIT VM 액세스 구성" 페이지에서 Just-In-Time VM 액세스를 적용할 수 있는 포트를 정의합니다.
 - 포트를 추가하려면 왼쪽 위에 있는 "추가" 단추를 클릭하거나 기존 포트를 클릭하여 편집합니다.
 - "포트 구성 추가" 블레이드에서 필요한 매개 변수를 입력합니다.
- "저장"을 클릭합니다.

데이터베이스 서비스 또한

아주 간단하게

Endpoint
IP Firewall

...

cloudmatesqlserver | 방화벽 및 가상 네트워크

SQL Server

검색(Ctrl+/)

저장 취소 클라이언트 IP 추가

설정

Active Directory 관리자

SQL 데이터베이스

SQL Elastic Pool

DTU 할당량

속성

잠금

데이터 관리

백업

삭제된 데이터베이스

장애 조치(failover) 그룹

가져오기/내보내기 기록

보안

감사

방화벽 및 가상 네트워크

프라이빗 엔드포인트 연결

보안 센터

퍼블릭 네트워크 액세스 거부

예 아니요

새 프라이빗 엔드포인트를 만들려면 여기를 클릭하세요.
프라이빗 엔드포인트 만들기

최소 TLS 버전

1.0 1.1 1.2

연결 정책

기본값 프록시 리디렉션

Azure 서비스 및 리소스가 이 서버에 액세스할 수 있도록 허용

예 아니요

클라이언트 IP 주소 1.209.17.35

규칙 이름	시작 IP	종료 IP	
Cloudmate	1.209.17.35	1.209.17.35	...

가상 네트워크
+ 기존 가상 네트워크 추가 + 새 가상 네트워크 만들기

규칙 이름	가상 네트워크	서브넷	주
-------	---------	-----	---

이 서버에 대한 vnet 규칙이 없습니다.

웹 앱은 어떻게 할까

아주 간단하게

HTTPS, 인증서
액세스 제한

...

홈 > Microsoft.Web-WebApp-Portal-d54f6fa2-965a > cloudmatewebappspark >

🚫 액세스 제한 ...

🗑️ 제거 🔄 새로 고침

🚫 액세스 제한

액세스 제한을 사용하면 앱 트래픽을 제어하기 위해 허용/거부 목록을 정의할 수 있습니다. 정의된 규칙이 없는 경우에는 앱에서 모든 주소의 트래픽을 수락합니다. [자세히](#)

cloudmatewebappspark.azurewebsites.net

cloudmatewebappspark.scm.azurewebsites.net

+ 규칙 추가

<input type="checkbox"/> 우선 순위	이름	소스	엔드포인트 상태
<input type="checkbox"/> 1	Allow all	Any	

엑세스 제한 추가

일반 설정

이름 ⓘ
IpAddress 규칙의 이름 입력 ✓

작업
☒ 허용 ☐ 거부

우선 순위 *
예: 300

설명
✓

원본 설정

형식
IPv4

IP 주소 차단 *
IPv4 CIDR을 입력하세요(예: 208.130....

HTTP 헤더 필터 설정

X-Forwarded-Host ⓘ
예: exampleOne.com, exampleTwo.com

X-Forwarded-For ⓘ
IPv4 또는 IPv6 CIDR 주소를 입력하세요...

X-Azure-FDID ⓘ
Front Door 또는 역방향 프록시 ID를 ...

규칙 추가

내 계정은 안전할까?

계정 기반의 접근

접근해서 할 수 있는 일들

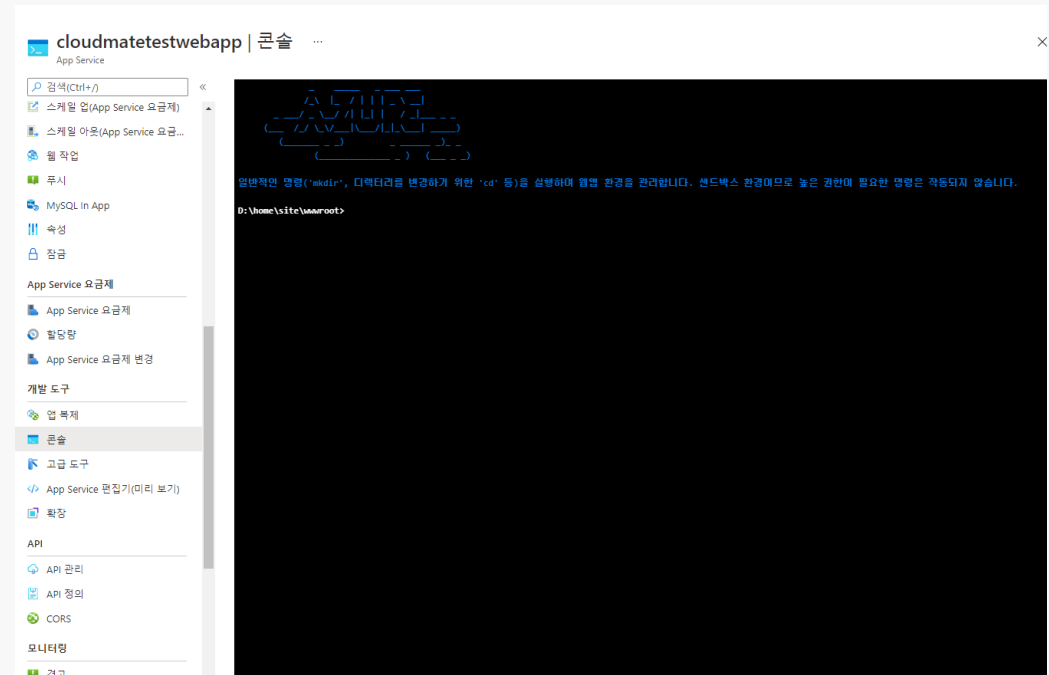
서비스 생성 및 삭제

외부 사용자 초대

권한 부여

앱 서비스 연결

...



계정을 지켜야 할 때

가장 중요한 것

MFA

조건부 액세스

...

홈 > Sangyeop.Park Corp >

🛡️

보안 | 시작 ...

🔍

검색(Ctrl+/)

«

📌 피드백이 있나요?

🚀 시작

🛡️ 보호

🔑 조건부 액세스

👤 Identity Protection

🛡️ 보안 센터

🔑 지속적인 액세스 권한 평가(미리 ...

📄 확인 가능한 자격 증명(미리 보기)

👤 관리

🏆 ID 보안 점수

🔗 명명된 위치

🔑 인증 방법

🛡️ MFA

📄 보고서

👤 위험한 사용자

🔑 위험한 로그인

🚨 위험 검색

🔧 문제 해결 및 지원

👤 새 지원 요청

📄

설명서

Azure Active Directory는 조직을 보호하기 위한 다양한 보안 기능을 제공합니다. 자세한 내용을 보려면 다음 몇 가지 기능으로 시작해 보세요.

- [Azure AD 조건부 액세스](#)
- [Azure AD Identity Protection](#)
- [Azure Security Center](#)
- [ID 보안 점수](#)
- [명명된 위치](#)
- [인증 방법](#)
- [MFA\(다중 요소 인증\)](#)

📘

보안 지침

강력한 보안을 위해 다음을 권장합니다.

- [ID 인프라를 보호하는 5단계](#)
- [Azure AD Password Guidance](#)
- [Azure AD 데이터 보안 백서](#)
- [PHS\(암호 해시 동기화\) 작동 방법](#)

📄

배포 가이드

조직에 위의 기능을 배포하려면 다음을 확인하세요. [Azure AD 배포 플랜입니다.](#)

#YourLocationHashTag

다른 보안은?

스토리지 서비스는 어떤 설정으로 가능할까

공유 액세스 서명 전송 중 암호화 미사용 암호화

...

SAS(공유 액세스 서명)은 Azure Storage 리소스에 대해 제한된 액세스 권한을 제공하는 URI입니다. 스토리지 계정 키로 신뢰하지 않지만 특정 스토리지 계정에 대한 액세스 권한을 위임하려는 클라이언트에 공유 액세스 서명을 제공할 수 있습니다. 이러한 클라이언트에 공유 액세스 서명 URI를 배포함으로써 특정 기간 동안 리소스에 대한 액세스 권한을 부여합니다.

계정 수준 SAS는 여러 스토리지 서비스(예: Blob, 파일, 큐, 테이블)에 대한 액세스 권한을 위임할 수 있습니다. 저장된 액세스 정책은 현재 계정 수준 SAS에서 지원되지 않음을 유의하세요.

자세한 정보

허용되는 서비스 ①

☒ Blob ☒ 파일 ☒ 큐 ☒ 테이블

허용되는 리소스 종류 ①

☐ 서비스 ☐ 컨테이너 ☐ 개체

허용되는 권한 ①

☒ 읽기 ☒ 쓰기 ☒ 삭제 ☒ 목록 ☒ 추가 ☒ 만들기 ☒ 업데이트 ☒ 프로세스

Blob 버전 관리 권한 ①

☒ 버전 삭제 사용

시작 및 만료 날짜/시간 ①

시작 2021. 04. 15. 오후 5:45:42

종료 2021. 04. 16. 오전 1:45:42

(UTC+09:00) 서울

허용되는 IP 주소 ①

예: 168.1.5.65 또는 168.1.5.65-168.1.5.70

허용되는 프로토콜 ①

☒ HTTPS만 사용 ☐ HTTPS 및 HTTP

기본 설정 라우팅 계층 ①

☒ 기본(기본값) ☐ Microsoft 네트워크 라우팅 ☐ 인터넷 라우팅

❗ 엔드포인트가 게시되지 않았기 때문에 일부 라우팅 옵션을 사용할 수 없습니다.

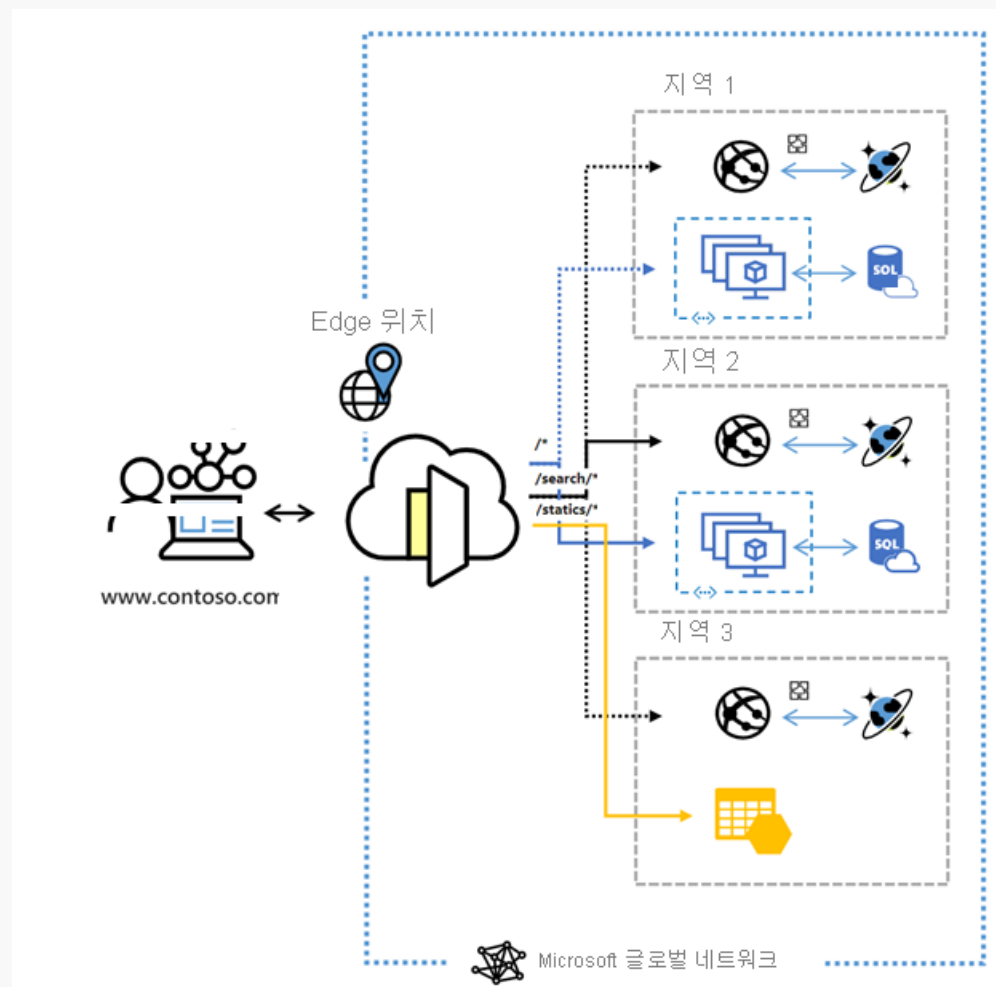
서명 키 ①

key1

알맞은 보안 설정

네트워크 보안 서비스

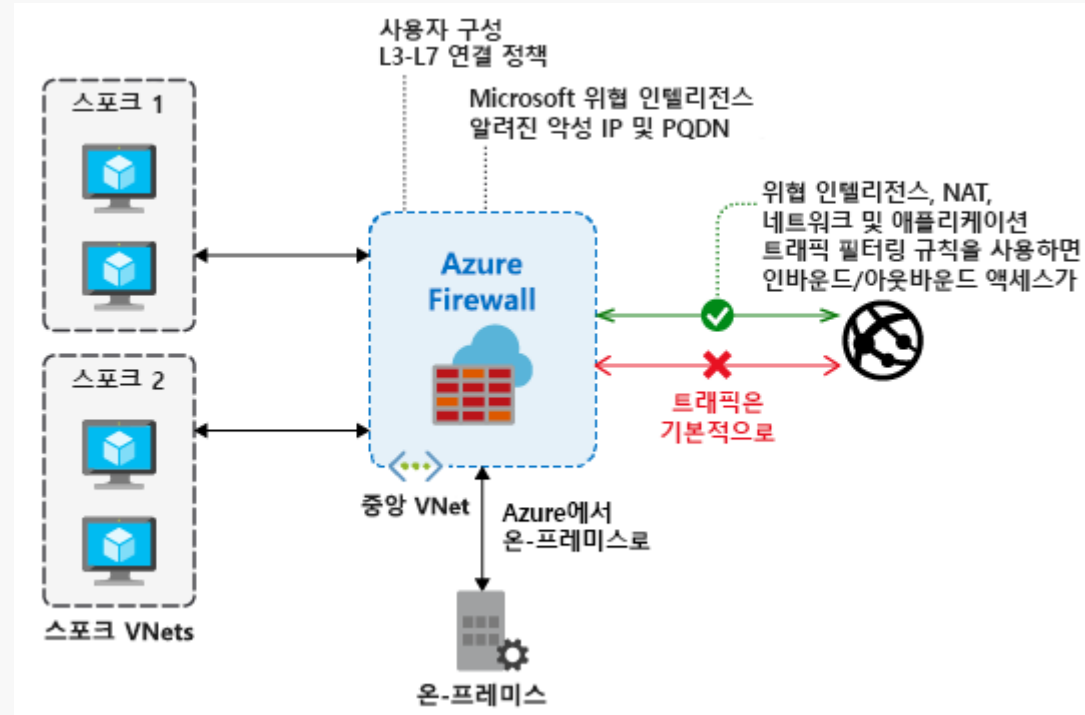
Azure Front Door



알맞은 보안 설정

네트워크 보안 서비스

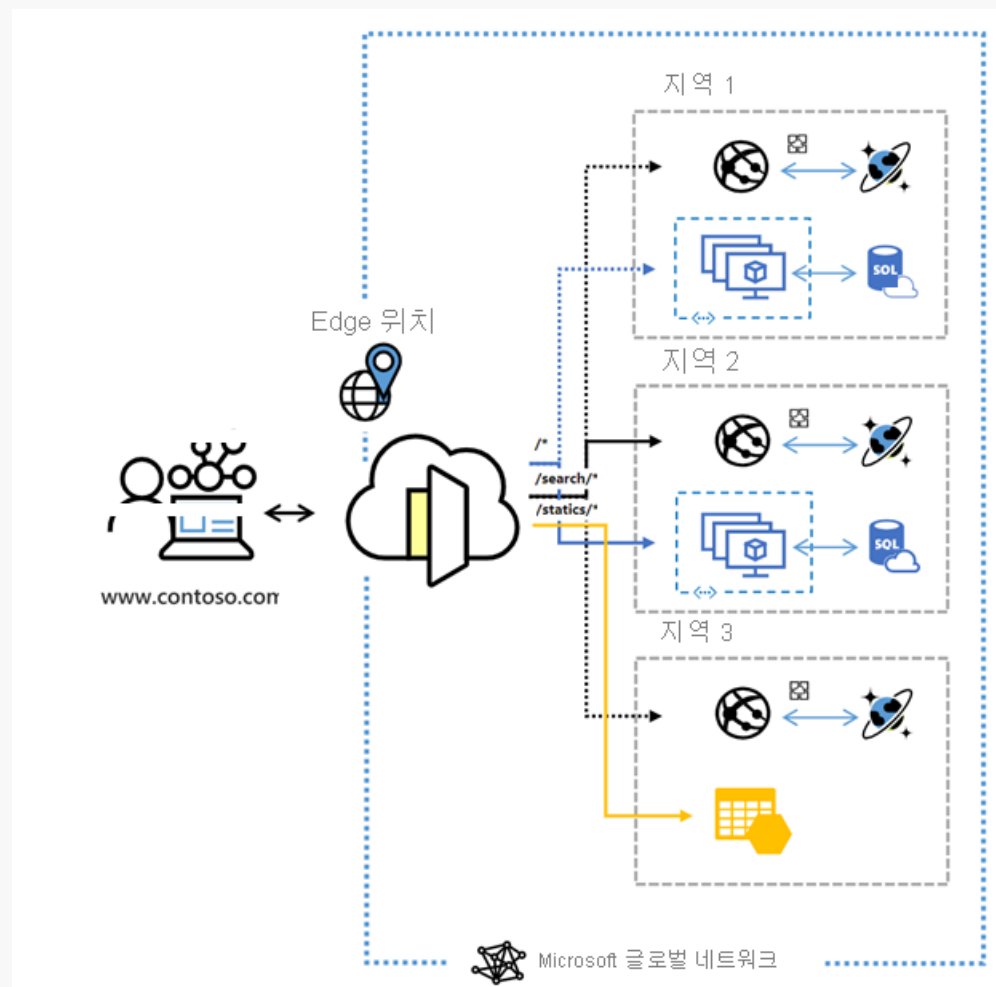
Azure Firewall



알맞은 보안 설정

네트워크 보안 서비스

Azure DDoS Protection



전체 보안 확인

보안 센터

보안 센터를 통한 보안 확인과 설정

홈 > 보안 센터

보안 센터 | 시작 ...

2개 구독 표시 중

검색(Ctrl+F)

일반

개요

시작

권장 사항

보안 경고

인벤토리

통합 문서

커뮤니티

클라우드 보안

보안 준수

규정 준수

Azure Defender

Firewall Manager

관리

가격 책정 및 설정


보안 정책

보안 솔루션


워크플로 자동화

적용 범위


클라우드 커넥터




서버
Security Center는 Windows 및 Linux 머신의 클라우드 네이티브 보호를 제공하여 공격 표면 줄이기, 취약성 검색, 실시간 위협 검색 등을 제공합니다.
[자세한 정보 >](#)




App Service
Security Center에서는 App Service에서 실행 중인 애플리케이션에 대한 권장 사항 및 위협 감지를 제공할 수 있습니다.
[자세한 정보 >](#)




Kubernetes 서비스
Security Center는 비정상적인 활동을 검색하고 컨테이너 환경을 위한 Azure 네이티브 런타임 위협 보호를 제공하여 Kubernetes 배포 및 워크로드를 보호할 수 있습니다.
[자세한 정보 >](#)




Key Vault
Security Center는 Key Vault 계정을 악용하고 이전 암호를 추출하려는 비정상적이고 잠재적으로 유해한 시도를 검색하여 Azure Key Vault를 보호할 수 있습니다.
[자세한 정보 >](#)




Azure SQL 데이터베이스
Security Center에서는 데이터베이스 및 취약성 평가에서 위협 및 공격을 탐지하여 보안 구성 오류를 파악하고 수정하는 Advanced Threat Protection을 통해 클라우드에서 SQL을 보호할 수 있습니다.
[자세한 정보 >](#)



스토리지 계정
Security Center는 스토리지 계정에 액세스하거나 악용하려는 비정상적이고 유해한 시도를 탐지하여 스토리지 계정을 보호할 수 있습니다.
[자세한 정보 >](#)



컨테이너 레지스트리
Security Center는 컨테이너 레지스트리의 Azure 네이티브 취약성 관리를 제공하여 컨테이너의 위협으로부터 보호할 수 있습니다.
[자세한 정보 >](#)

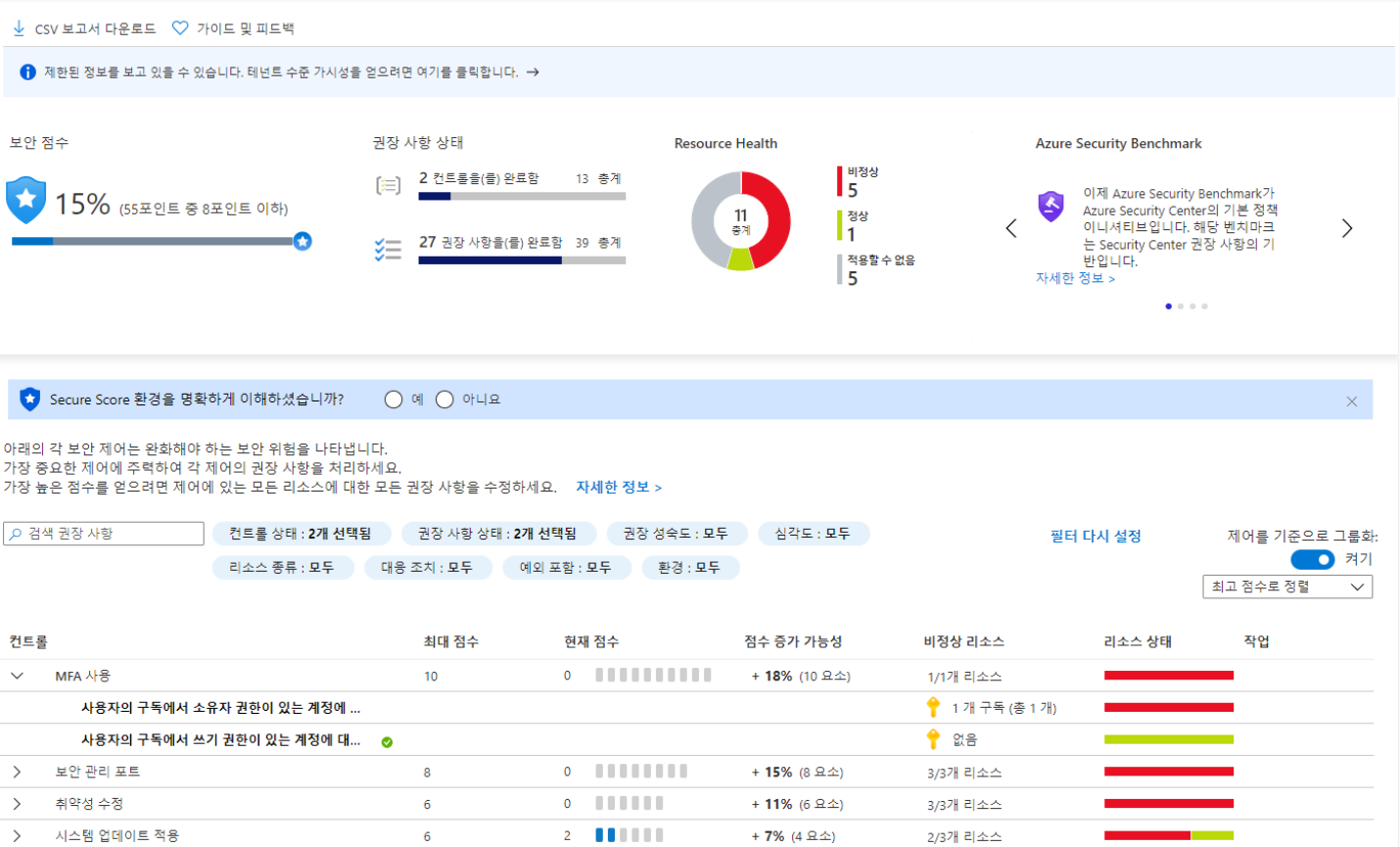


SQL Server
Security Center에서는 데이터베이스 및 취약성 평가에서 위협 및 공격을 탐지하여 보안 구성 오류를 파악하고 수정하는 Advanced Threat Protection을 통해 온-프레미스 및 기타 클라우드에서 SQL Server를 보호할 수 있습니다.
[자세한 정보 >](#)

전체 보안 확인

보안 센터

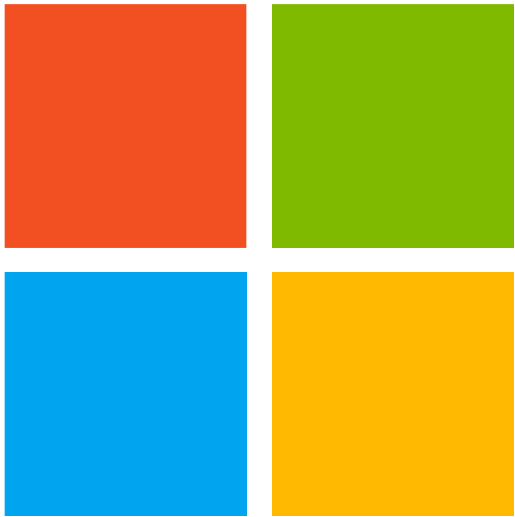
보안 센터를 통한 보안 확인과 설정





CLOUDMATE

Azure Expert Group



Microsoft

