Cloud Infrastructure Operations

Day3 Module2 – Azure 보안

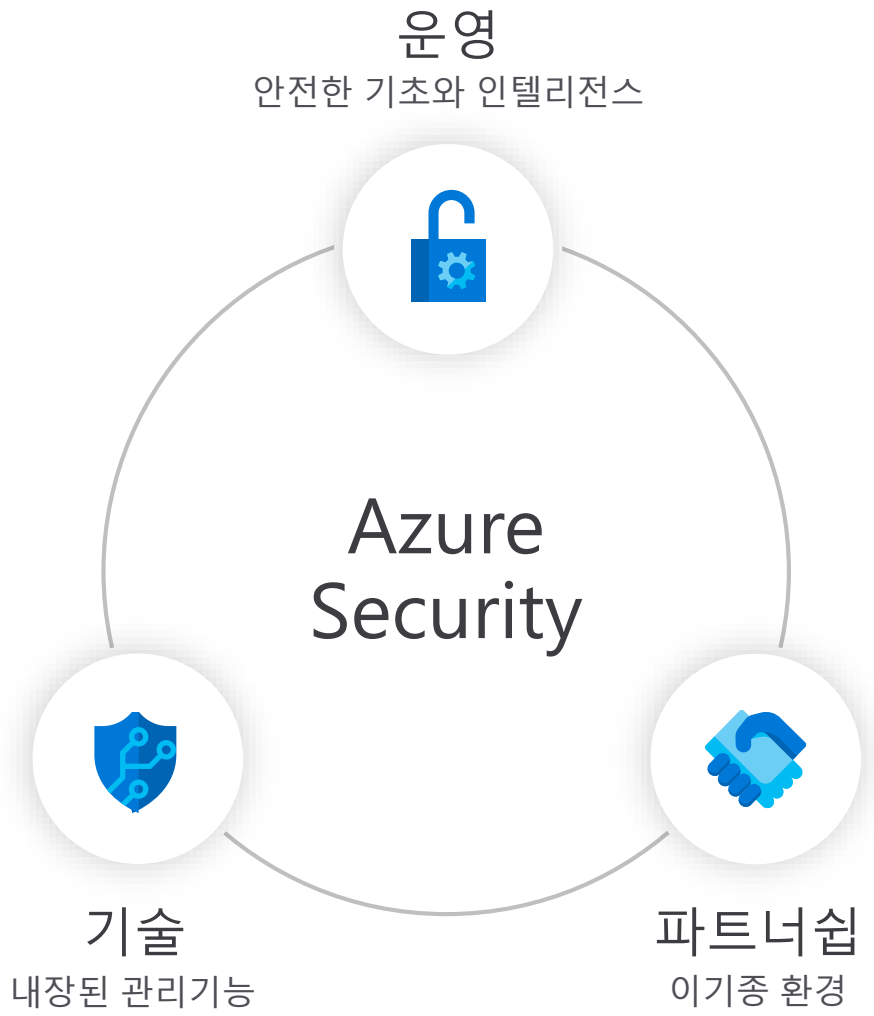
윤혜식 | 2miles CEO
david@2miles.co.kr

Azure 보안 이해하기

Azure 운영, 기술 및 파트너십에서 최고 보안 서비스 제공

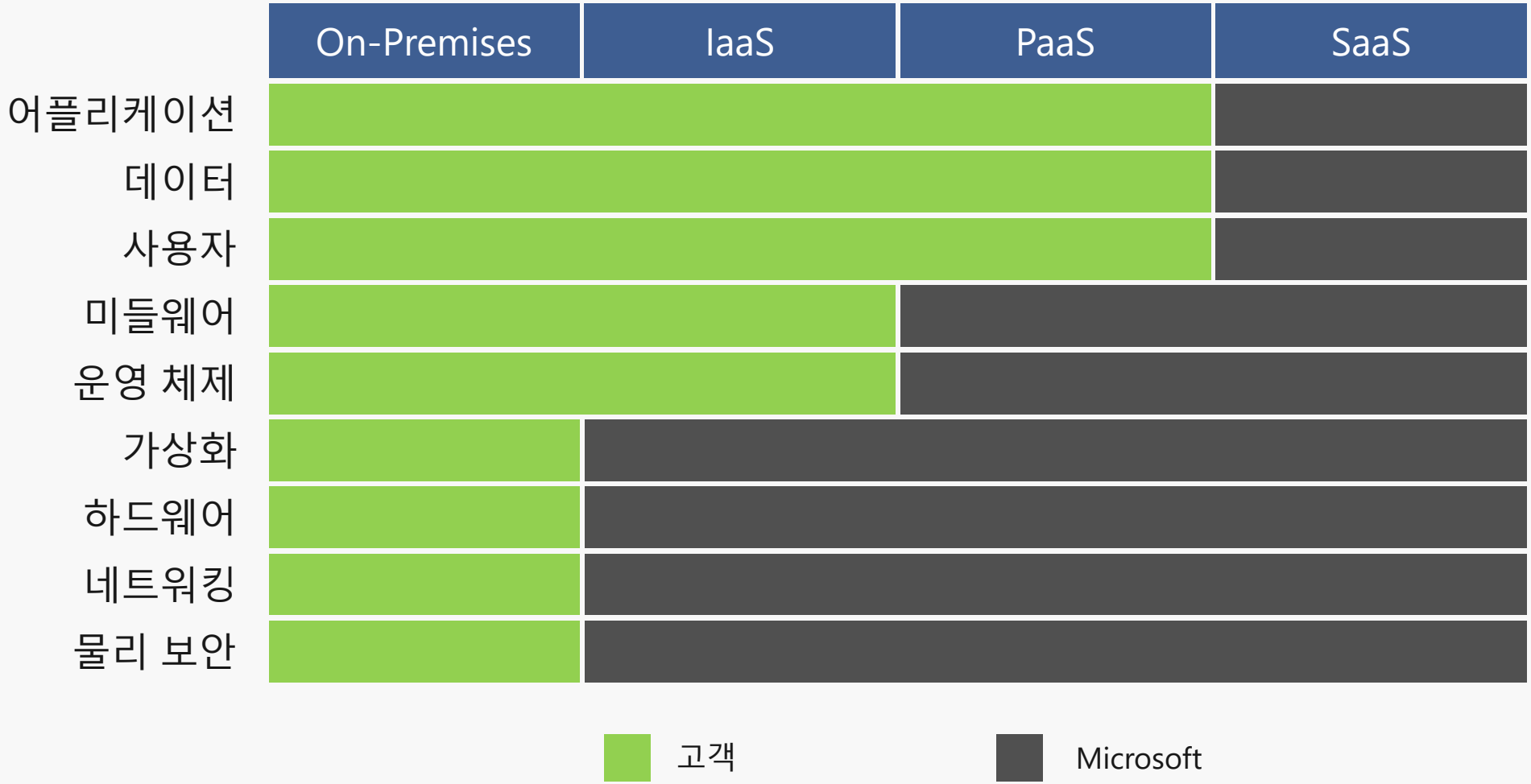
$1B
사이버 보안 연간 투자 금액

3500+
세계적인 보안 전문가



클라우드 보안 - 공유 책임 모델

접근 통제 및 보안 비용 감소



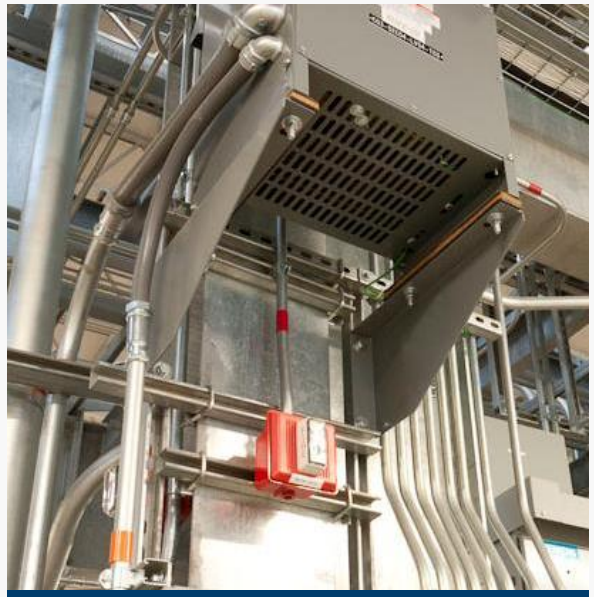
인프라 보호

물리적 & 논리적 보안	시스템 관리& 모니터링	보안 위협 방어
• 데이터 센터 물리 보안 • OS 보안 강화 • 멀티 테넌트 아키텍처	• 패치 및 악성코드 제거 프로그램 제공을 통해 알려진 취약점 조치	• 고급 위협 분석 툴을 통해 신규 위협 제거

데이터 센터 물리 보안

- CCTV 카메라
- 24X7 보안 요원
- 건물 외벽
- 펜스
- 경보 시스템
- 이중 인증 장치
  (생체 인식 + 카드 리더기)
- 보안 운영 센터
- 방진 시스템
- 무정전 시스템

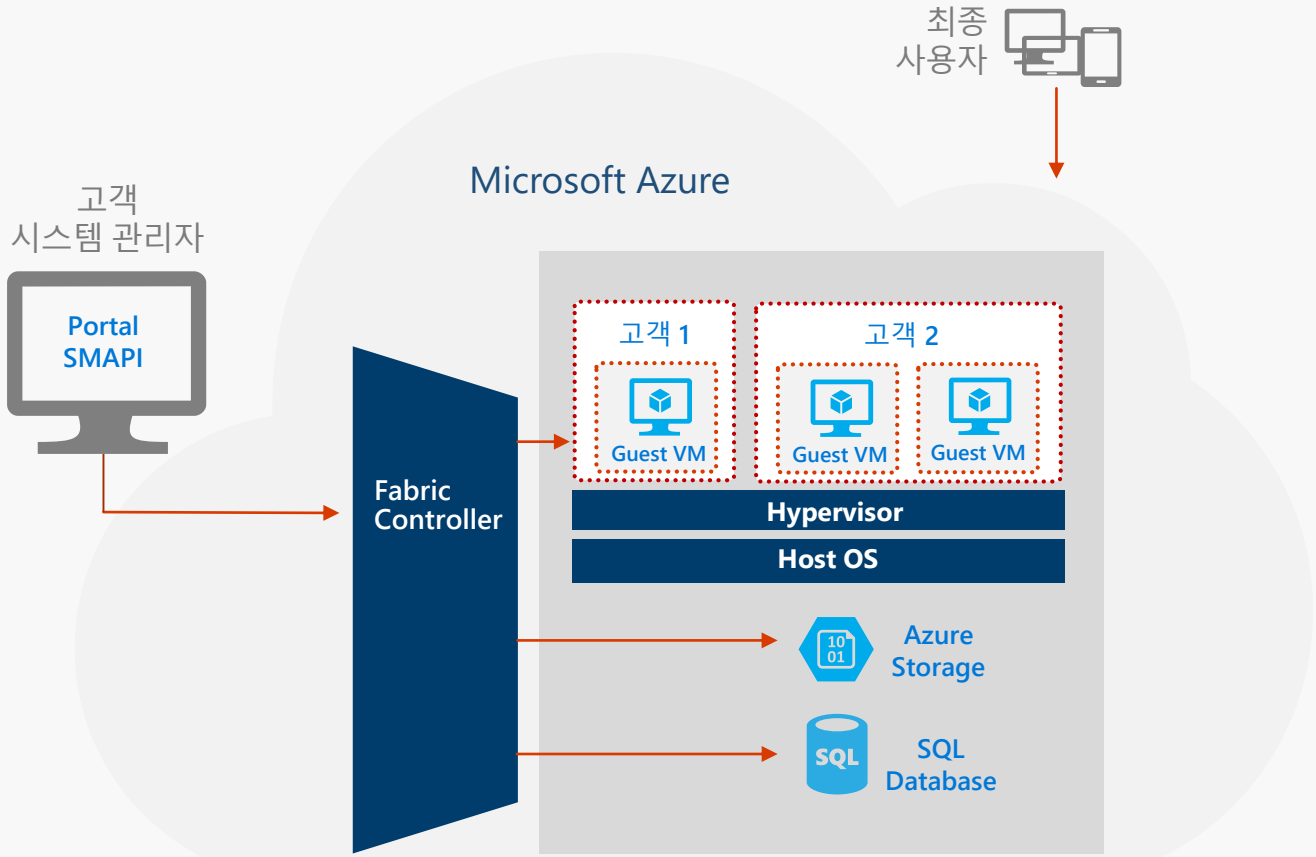
주변 경계



건물

서버 룸

안전한 Multi-Tenant 구조



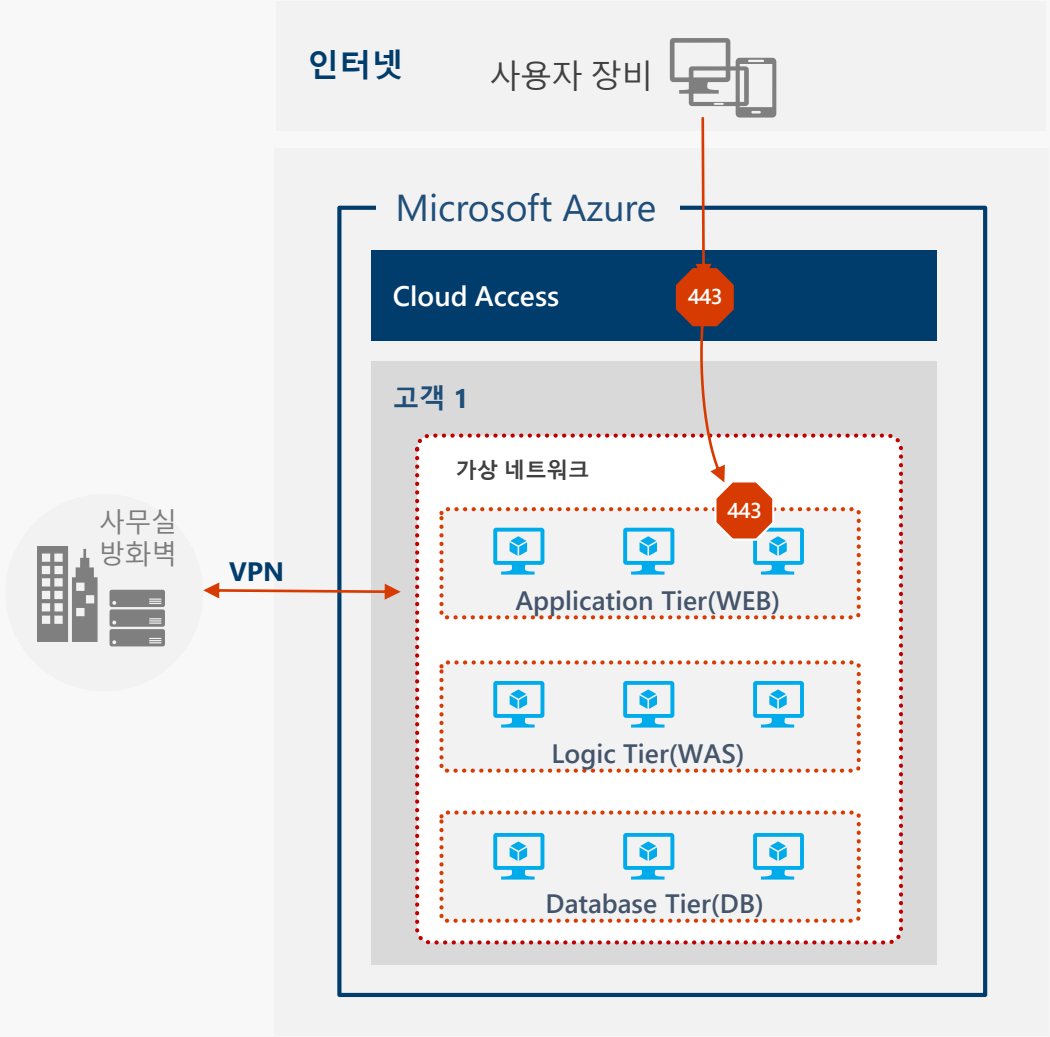
AZURE:

- Fabric Controller을 통해서 중앙에서 고객별 환경을 격리해서 운영
- 클라우드 환경에 최적화된 Windows Server를 Host OS로 운영
- 엔터프라이즈 환경에서 검증 된 Windows Server 2019 상의 Hyper-V
- Guest OS – Windows Server, LINUX 모두 지원

고객:

- 구독 별로 Azure Portal을 통해 고객 자원 관리
- 갤러리 혹은 자체 제작 OS를 통해서 VM 생성

방화벽 보호



AZURE:

- 인터넷으로 직접 접속 차단하고 허용된 경로를 통해서만 접속 허용, 부하 분산 기능 제공 및 NAT 통한 접근
- 분산 방화벽을 통한 침입 방지 서비스 제공 및 고객별 트래픽 분리

고객:

- 사무실 방화벽 통해 Site-to-Site VPN 구성
- 가상 머신 접근을 위한 보안 그룹 설정
- 접근 제어 설정 및 OS 방화벽 구성을 통해 추가적인 보안 조치

패치 관리

매월 MSRC 패치 리뷰	패치 공개	스캐닝	감사 및 평가
• 고객 및 전세계 네트워크, 보안 리서치 기관으로부터 보고된 100,000+ 취약점 리포트 모니터링	• 중요 업데이트 우선순위 설정 • 매월 OS 릴리즈 및 패치	• 모든 Azure VM에 대한 스캐닝 및 리포팅 • 발견된 취약점 및 개선할 부분 처리	• 진상 조사 • 해결 방안 정리

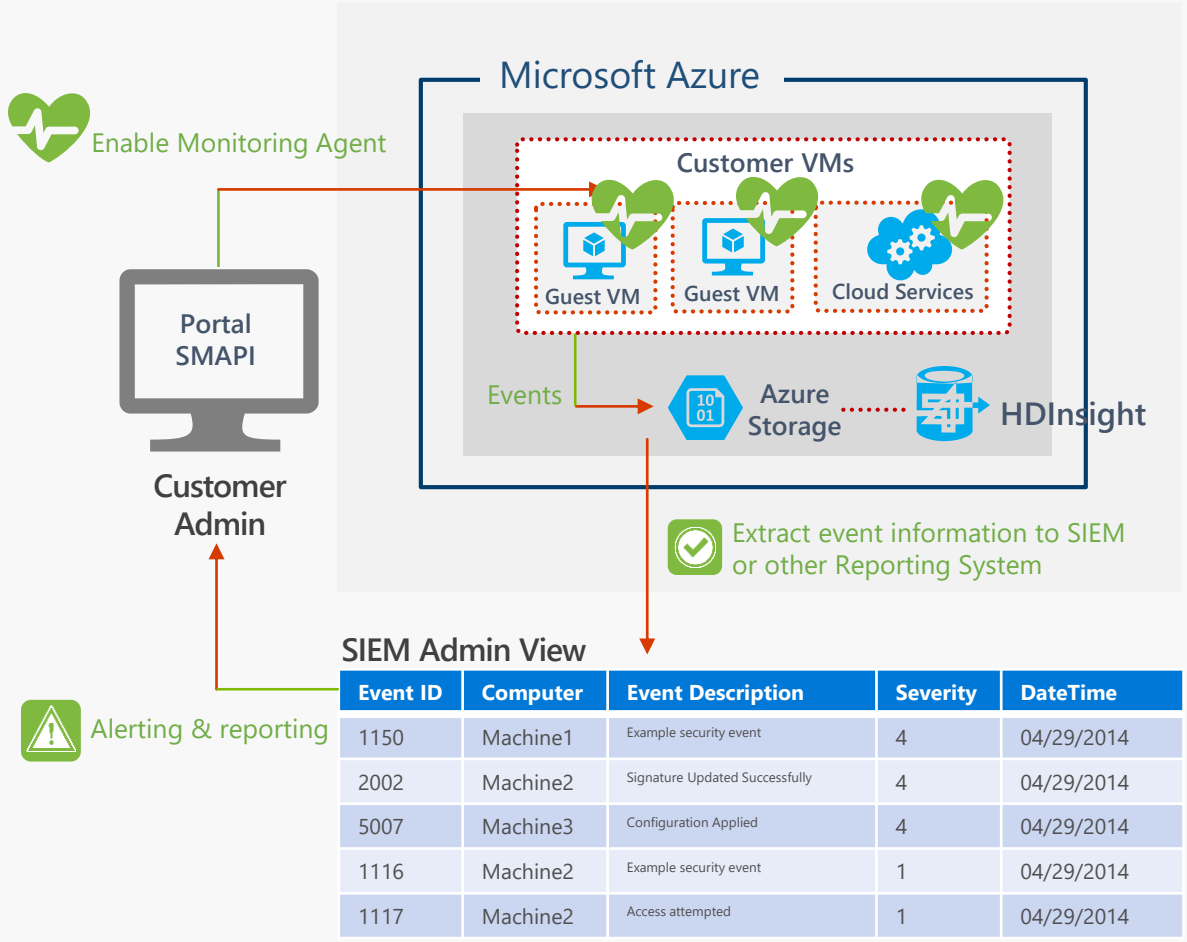
AZURE:

- 정기 업데이트 적용
- 중요 패치의 신속한 적용
- 모든 변경 부분에 대한 엄격한 검토 및 테스트

고객:

- 운영중인 VM에 대해 동일한 수준의 패치 관리 기준 적용
- 보안 센터를 통한 알람기능을 통해 패치가 필요한 서버 확인

모니터링 및 로그 관리



Event ID	Computer	Event Description	Severity	DateTime
1150	Machine1	Example security event	4	04/29/2014
2002	Machine2	Signature Updated Successfully	4	04/29/2014
5007	Machine3	Configuration Applied	4	04/29/2014
1116	Machine2	Example security event	1	04/29/2014
1117	Machine2	Access attempted	1	04/29/2014

AZURE:

- 보안 이벤트에 대한 모니터링 및 알람 기능 제공
- 모니터링 Agent를 통한 보안 데이터 수집 및 보안센터 통한 대시보드 제공

고객:

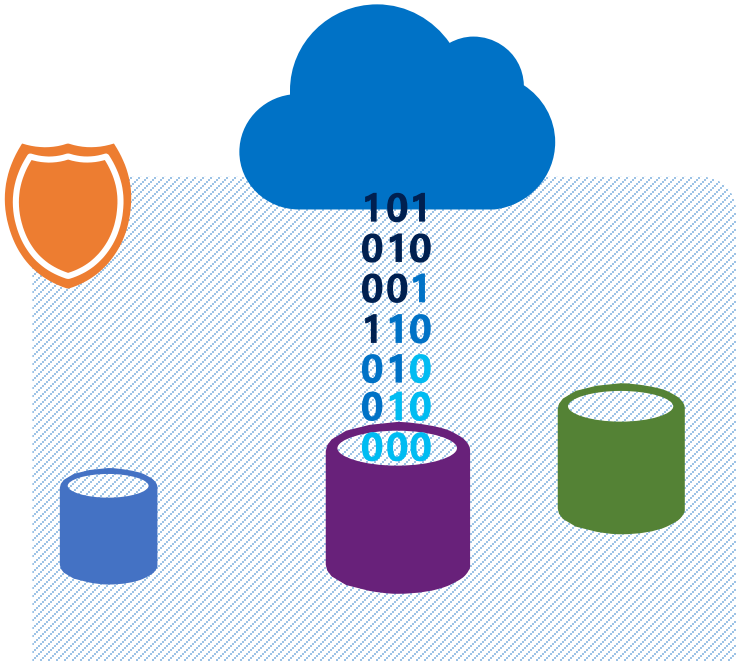
- 모니터링 설정
- 분석을 위해 시스템 이벤트를 SQL DB, HDInsight 혹은 SIEM으로 내보내기
- 시스템 경보 및 리포트 모니터링
- 장애 대응

인증 & 접속

엔터프라이즈 클라우드 인증	모니터 & 접속 보호	Multi-Factor Authentication
Azure AD를 통해 Cloud상에서 엔터프라이즈 규모의 사용자 인증 및 접근 관리	보안 리포트, 접근 패턴 모니터링, 예상 위협 식별	사용자 로긴시 강력한 인증 기능을 통해 추가적 보안 단계 제공

데이터 보호

전송 데이터 암호화	데이터 암호화 기능 제공	데이터 분리
업계 표준 SSL/TLS 프토토콜을 사용하여 전송중 데이터 암호화	가상 서버 및 스토리지에 대해 고객 필요시 암호화 가능 SQL 컬럼 암호화	논리적인 격리 및 접근 제어 기능 제공



개인정보

데이터 저장 위치 제어	제한된 데이터 접근 및 사용	규제 준수
고객이 데이터 저장 위치 및 복제 옵션 선택	고객 데이터는 오직 서비스 제공을 위해서 제한적으로 접근됨 (절대 광고나 마케팅 용도로 사용하지 않음)	Data Processing Agreements, EU Model Clauses, HIPAA BAA

데이터 폐기

데이터 삭제	• Blob, Table등 데이터 삭제시 Index 정보 즉시 삭제 • 지역 중복 복제본은 비동기로 삭제 • 고객은 생성한 디스크 공간에 대해서만 읽기 가능 • Azure 사용 중지 후, 고객 데이터를 90일간 보관
디스크 관리	• NIST 800-88 준수 : 디스크는 분쇄되어 재사용이 불가능

보안 사고 대응

AZURE:

- 총 9단계의 보안 사고 대응 프로세스
- 방지 및 복구에 집중
- 플랫폼 레벨 보안 사고 시 로그 및 VHD 이미지 분석, 필요시 포렌식 정보 고객에게 제공
- 고객 통지에 대해 계약에 명시

Azure Security Services and Capabilities

Network Security

- Virtual Network Service Endpoints
- DDoS Protection
- Network Security Groups
- NSG Service Tags
- NSG Application Security Groups
- NSG Augmented Rules
- Global Virtual Network Peering
- Azure DNS Private Zones
- Site-to-Site VPN
- Point-to-Site VPN
- ExpressRoute
- Azure Virtual Networks
- Virtual Network Appliances
- Azure Load Balancer
- Azure Load Balancer HA Ports
- Azure Application Gateway
- Azure Firewall
- Azure Web Application Firewalls
- Service Endpoints

Monitoring and Logging

- Azure Log Analytics
- Azure Monitor
- Network Watcher
- VS AppCenter Mobile Analytics

Compliance Program

- Microsoft Trust Center
- Service Trust Platform
- Compliance Manager
- Azure IP Advantage (legal)

Identity and Access Management

- Azure Active Directory
- Azure Active Directory B2C
- Azure Active Directory Domain Services
- Azure Active Directory MFA
- Conditional Access
- Azure Active Directory Identity Protection
- Azure Active Directory Privileged Identity Management
- Azure Active Directory App Proxy
- Azure Active Directory Connect
- Azure RBAC
- Azure Active Directory Access Reviews
- Azure Active Directory Managed Service Identity

Security Docs Site

- Azure Security Information Site on Azure.com

DDoS Mitigation

- Azure DDoS Protection
- Azure Traffic Manager
- Autoscaling
- Azure CDN
- Azure Load Balancers
- Fabric level edge protection

Infrastructure Security

- Comes with Azure Data Centers
- Azure Advanced Threat Protection
- Confidential Computing

Pen Testing

- Per AUP
- Per TOS
- No contact required

Data Loss Prevention

- Cloud App Discovery
- Azure Information Protection

Encryption

- Azure Key Vault
- Azure client-side encryption library
- Azure Storage Service Encryption
- Azure Disk Encryption
- SQL Transparent Data Encryption
- SQL Always Encrypted
- SQL Cell/Column Level Encryption
- Azure CosmosDB encrypt by default
- Azure Data Lake encrypt by default
- VPN protocol encryption (ssl/ipsec)
- SMB 3.0 wire encryption

Configuration and Management

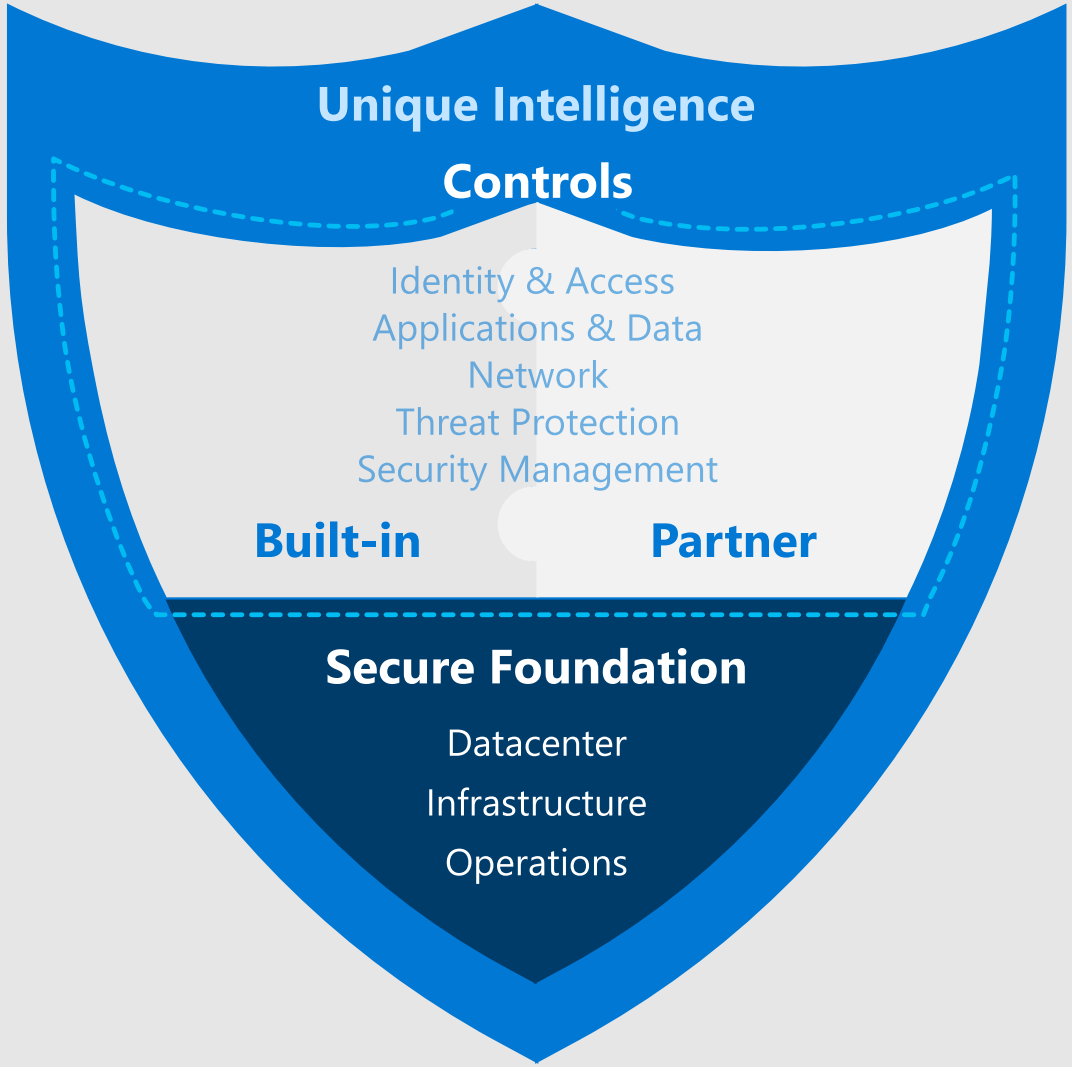
- **Azure Security Center**
- Azure Resource Manager
- ARM Management Groups
- Azure Policy
- Azure Blueprints
- Azure Automation
- Azure Advisor
- Azure API Gateway

Gain Unmatched security

$1B+ annual investments

Over 3500 security experts

Trillions of diverse signals



Cloud Security is a Shared Responsibility

MICROSOFT COMMITMENT

Securing and managing the cloud foundation

Physical assets

Datacenter operations

Cloud infrastructure

JOINT RESPONSIBILITY

Securing and managing your cloud resources

Virtual machines

Applications & workloads

Data

Simplify security management with Azure services

Identity & access management

- Azure Active Directory
- Multi-Factor Authentication
- Role Based Access Control
- Azure Active Directory (Identity Protection)

Data protection

- Encryption (Disks, Storage, SQL)
- Azure Key Vault
- Confidential Computing

Network security

- VNET, VPN, NSG
- Application Gateway (WAF), Azure Firewall
- DDoS Protection Standard
- ExpressRoute

Threat protection

- Azure Security Center
- Microsoft Antimalware for Azure

Security management

- Azure Security Center
- Azure Log Analytics

+ Partner Solutions

Azure Firewall

Cloud native stateful Firewall as a Service

- Built-in High Availability and Auto Scale
- Network and Application traffic filtering
- Centralized policy across VNets and Subscriptions

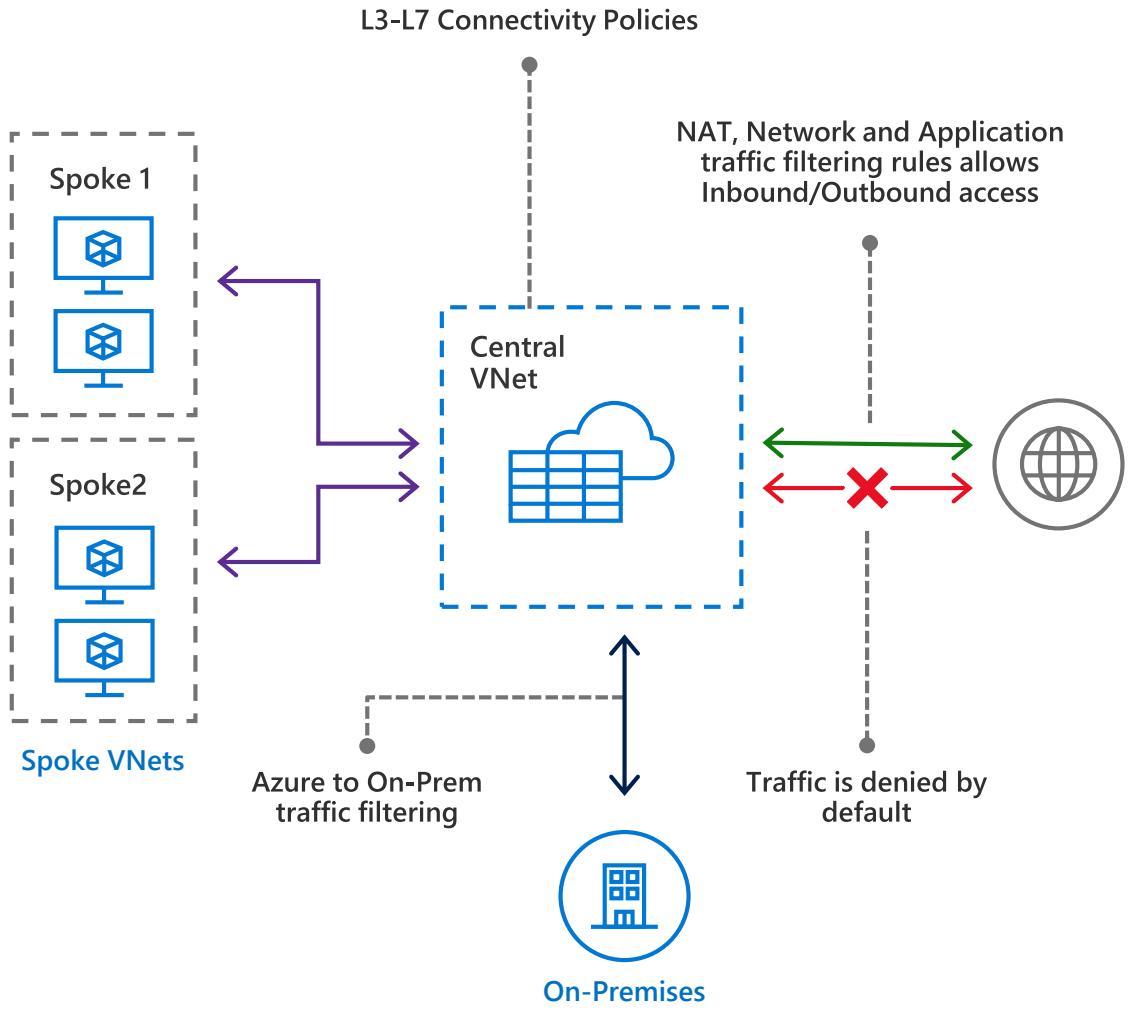
Complete VNET protection

- Filter Outbound, **Inbound**, Spoke-Spoke & **Hybrid Connections traffic** (VPN and ExpressRoute)

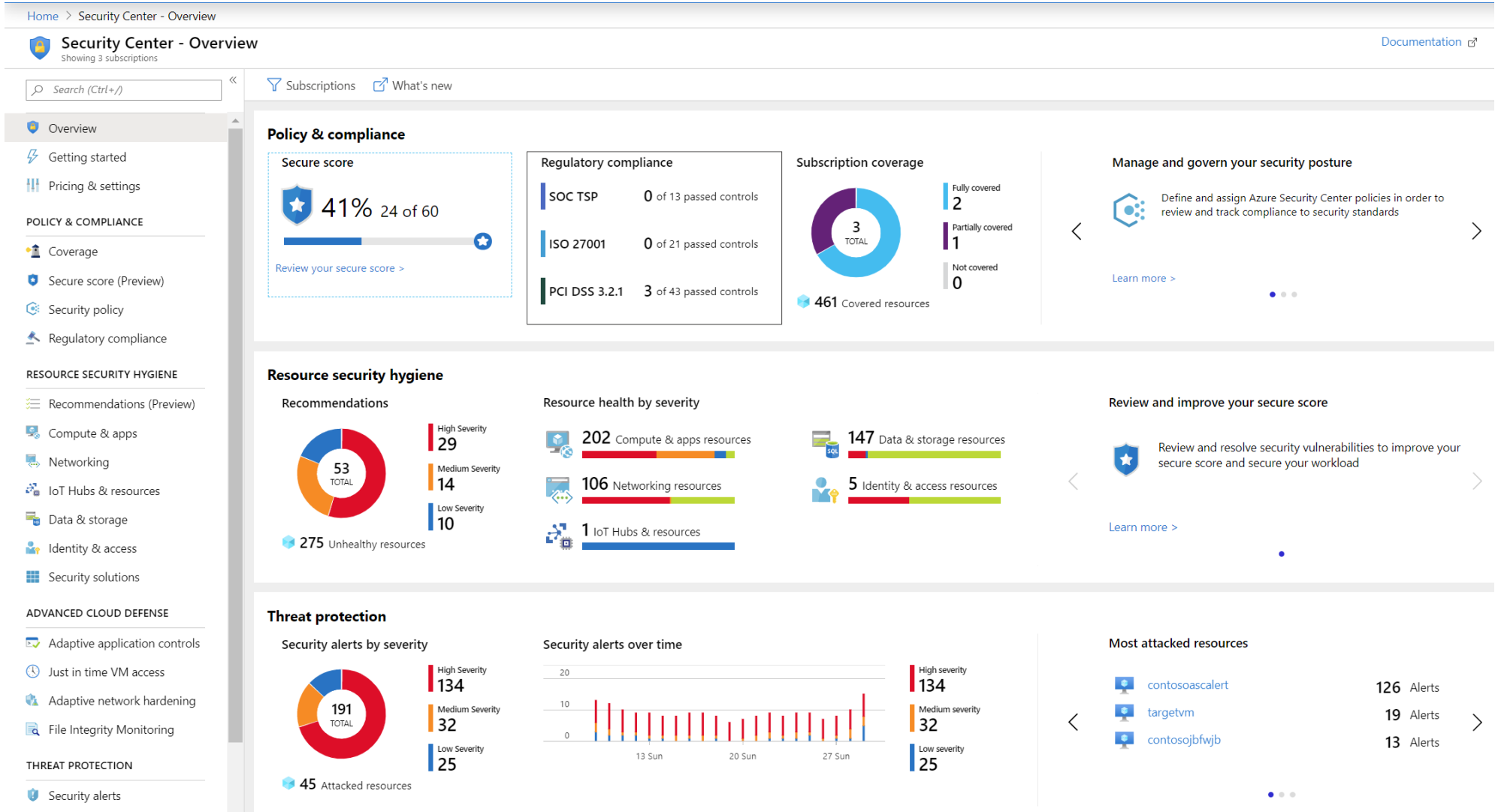
Centralized logging

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or SIEM

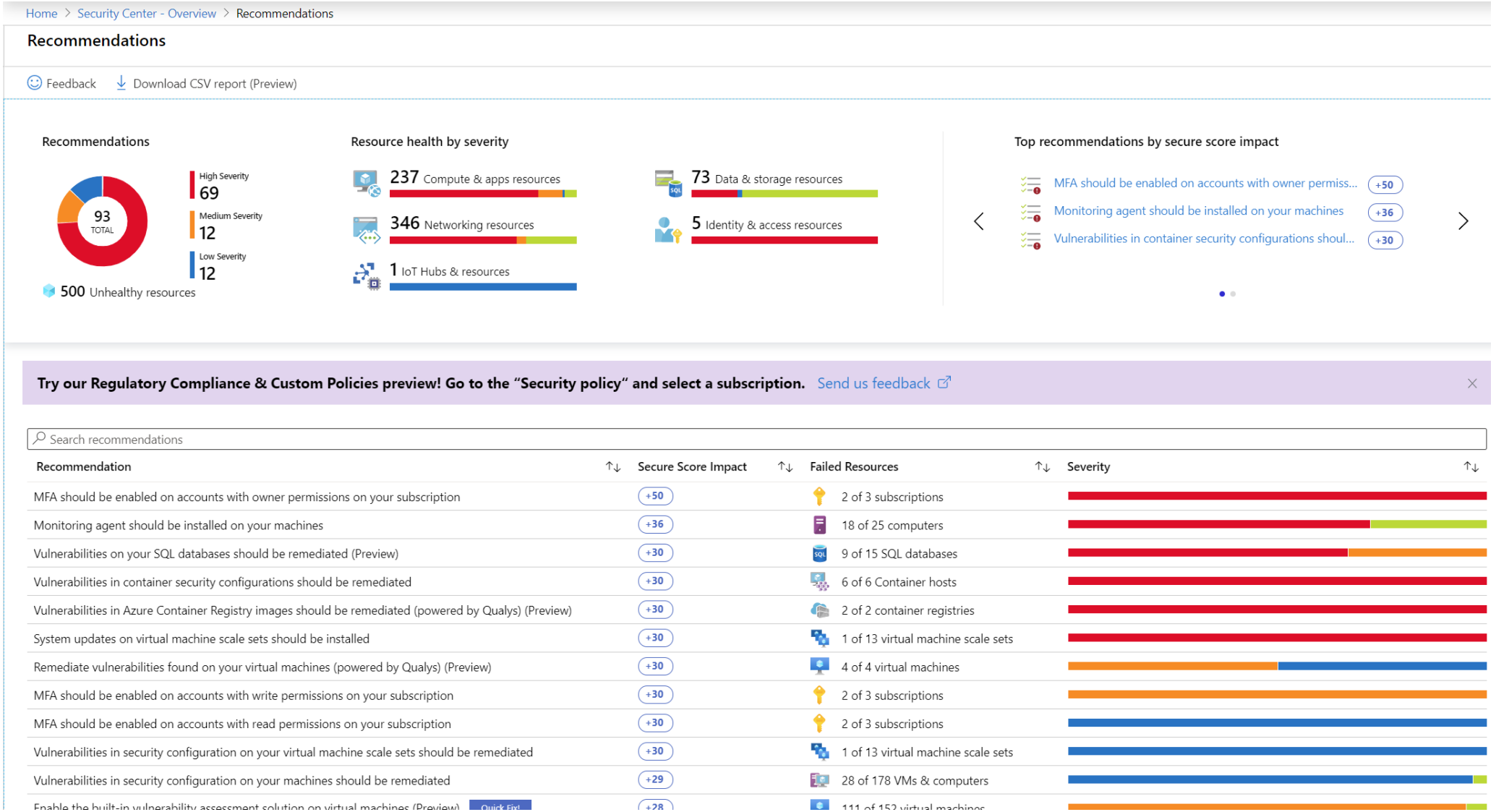
GA



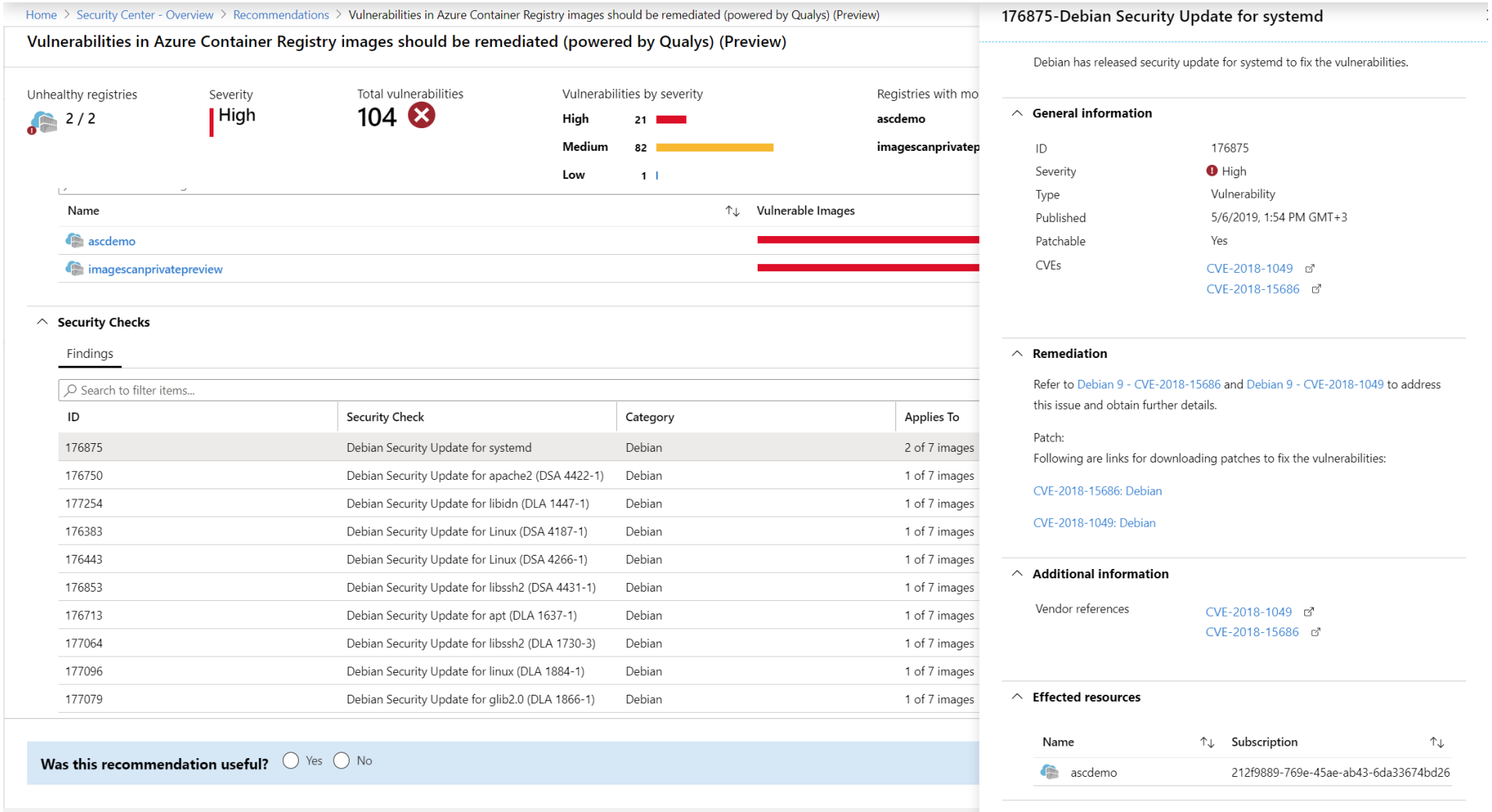
Azure 보안 센터 – 대시보드를 통해 보안 상황 한눈에 파악하기



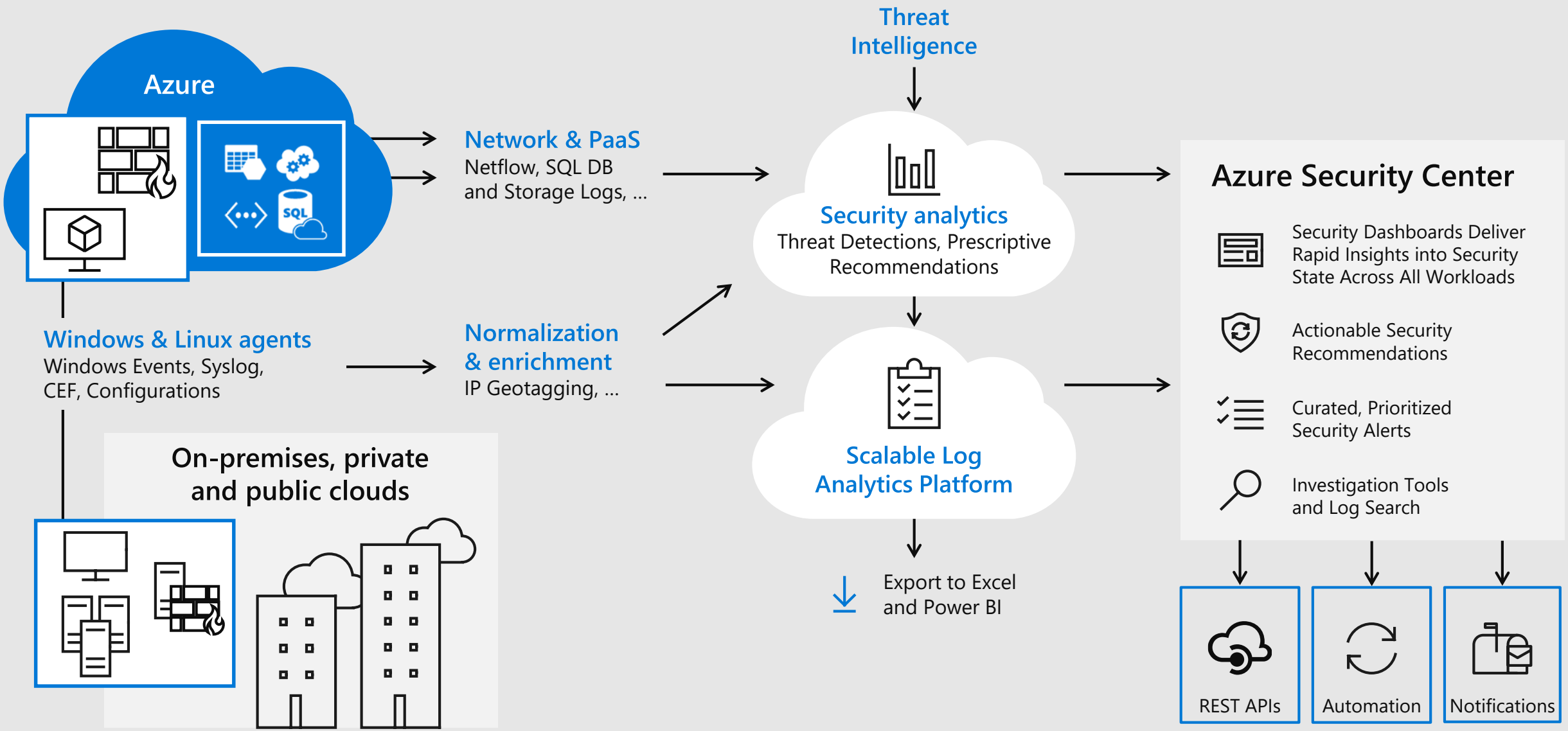
Azure 보안 센터 – 권고 사항과 보안 점수를 통해 안전한 클라우드 관리



Azure 보안 센터 – 취약점 분석과 해결 방안 추천을 통한 안정성 확보



Security Center Architecture



Strengthen security posture

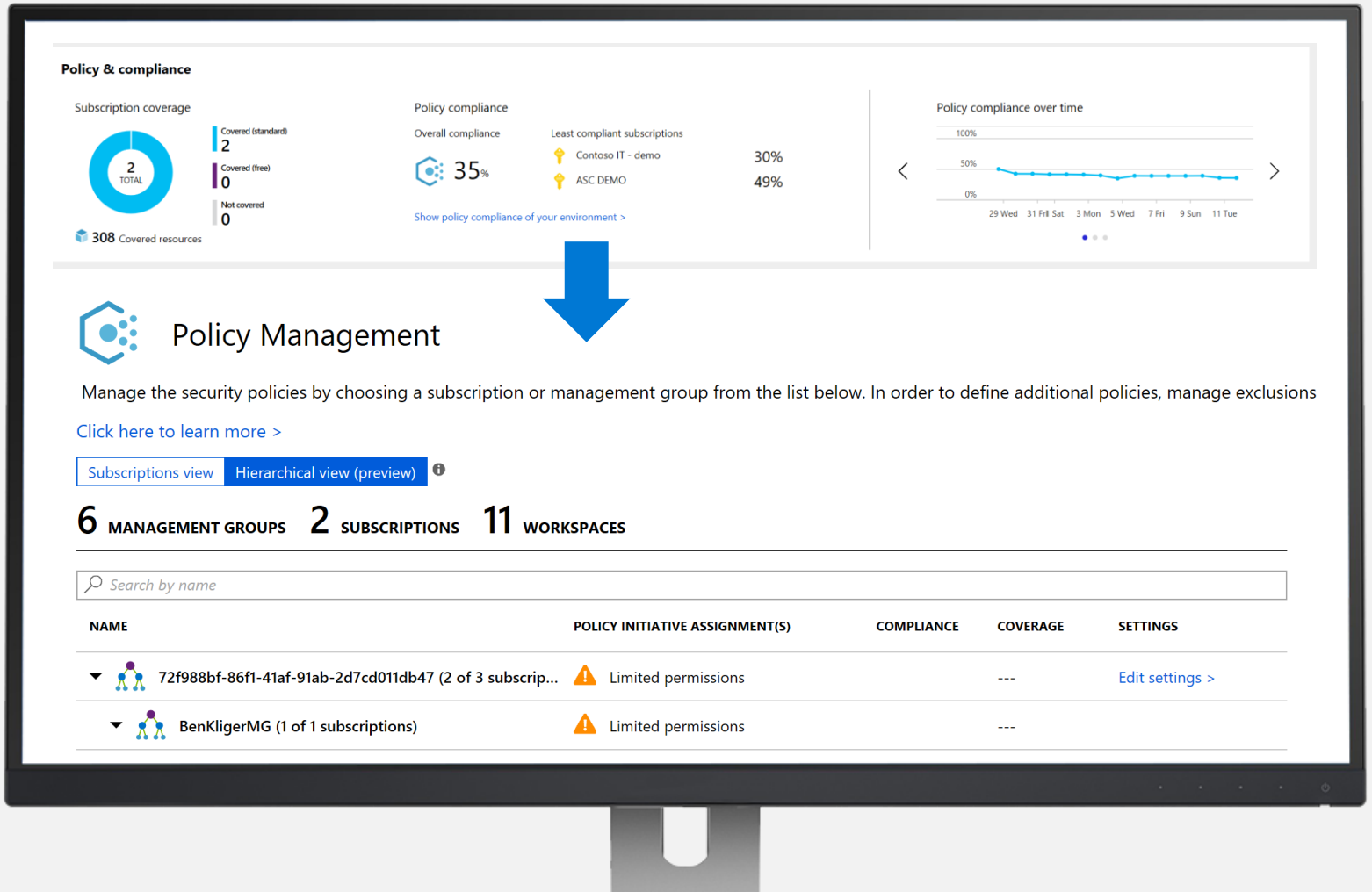
- Manage organizational security policy and compliance
- Continuously assess security state
- Optimize and improve security by configuring recommended controls

Manage organizational security policy and compliance

Review coverage for Azure Security Center across different subscriptions

Easily set centralized security policies across multiple subscriptions

Track and review policy compliance and governance over time

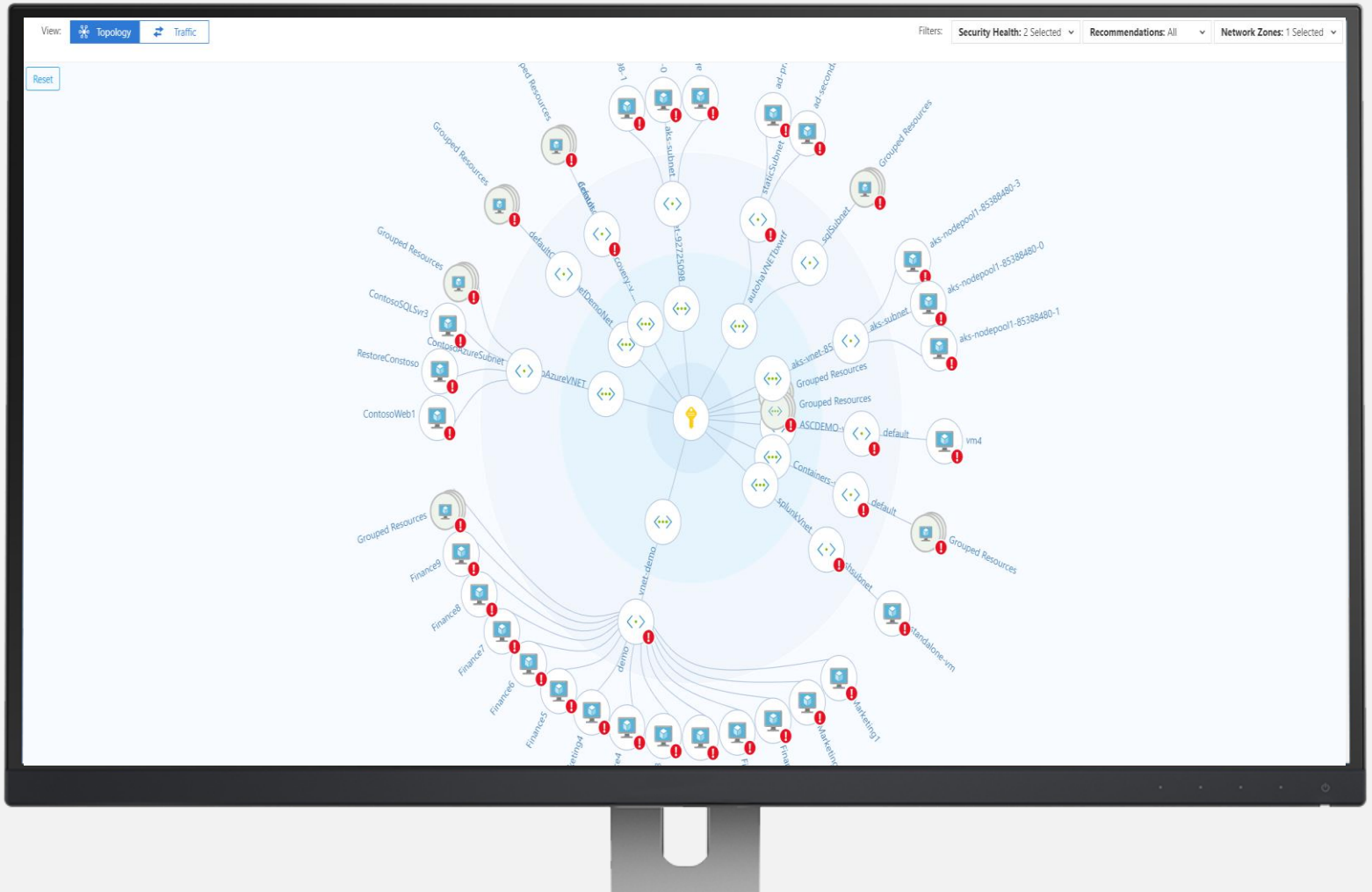


Continuously assess and optimize with Secure Score

Get insights on the security state across your infrastructure

Prioritized recommendations with a security score

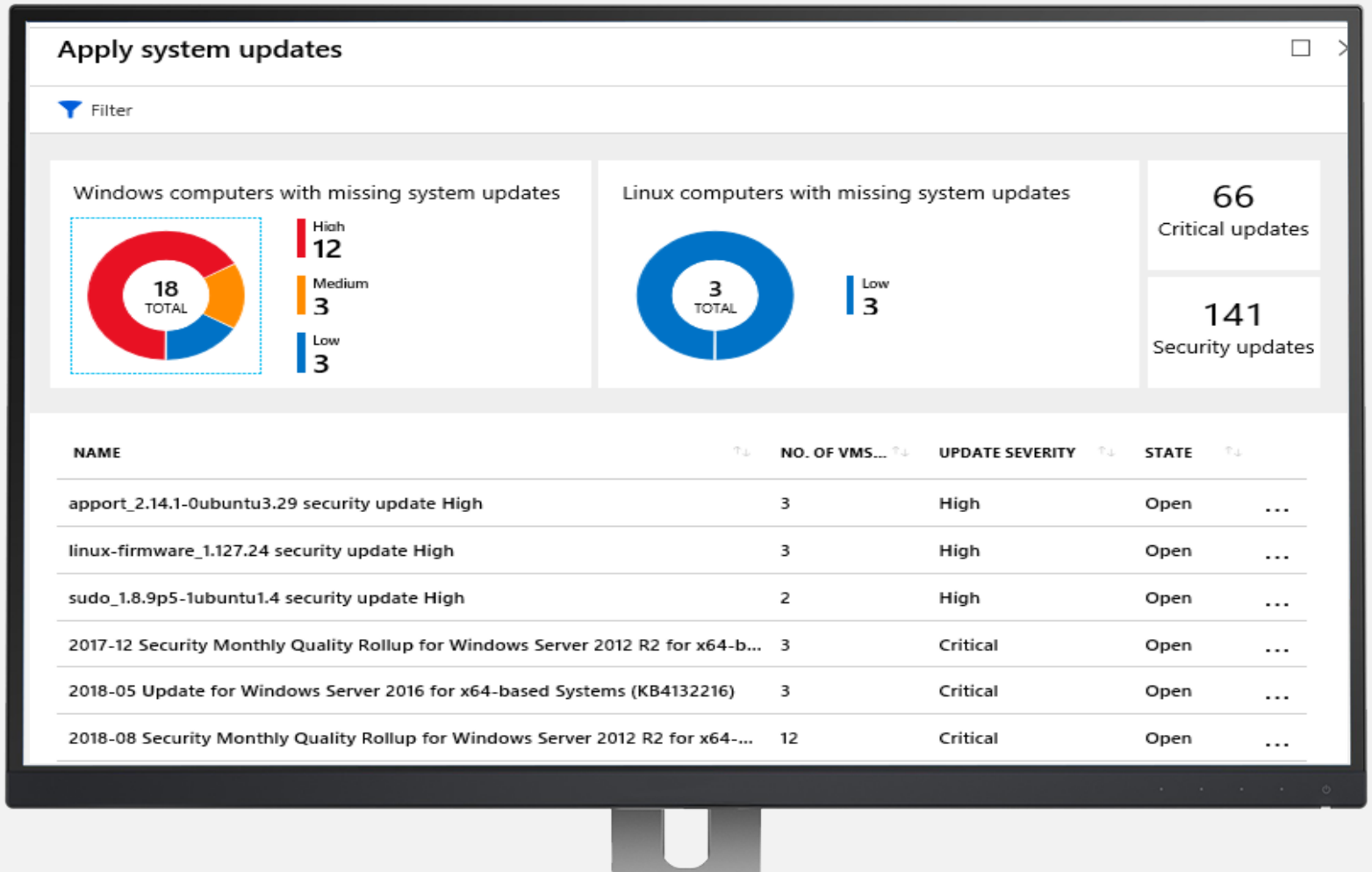
Understand the network topology and visualize configurations



Optimize and improve security by configuring recommended controls

Apply a secure configuration standard with built-in recommendations

Reduce attack surface by applying proactive hygiene measures



Protect against threats

- Detect and block advanced malware and threats for servers
- Detect threats across IaaS and PaaS services using advanced analytics
- Reduce exposure to brute force attacks
- Protect data services against malicious attacks

Detect and block advanced malware for Windows and Linux servers

Detect threats on servers with behavior analytics and machine learning

Get Windows server EDR with the integration of Windows Defender ATP

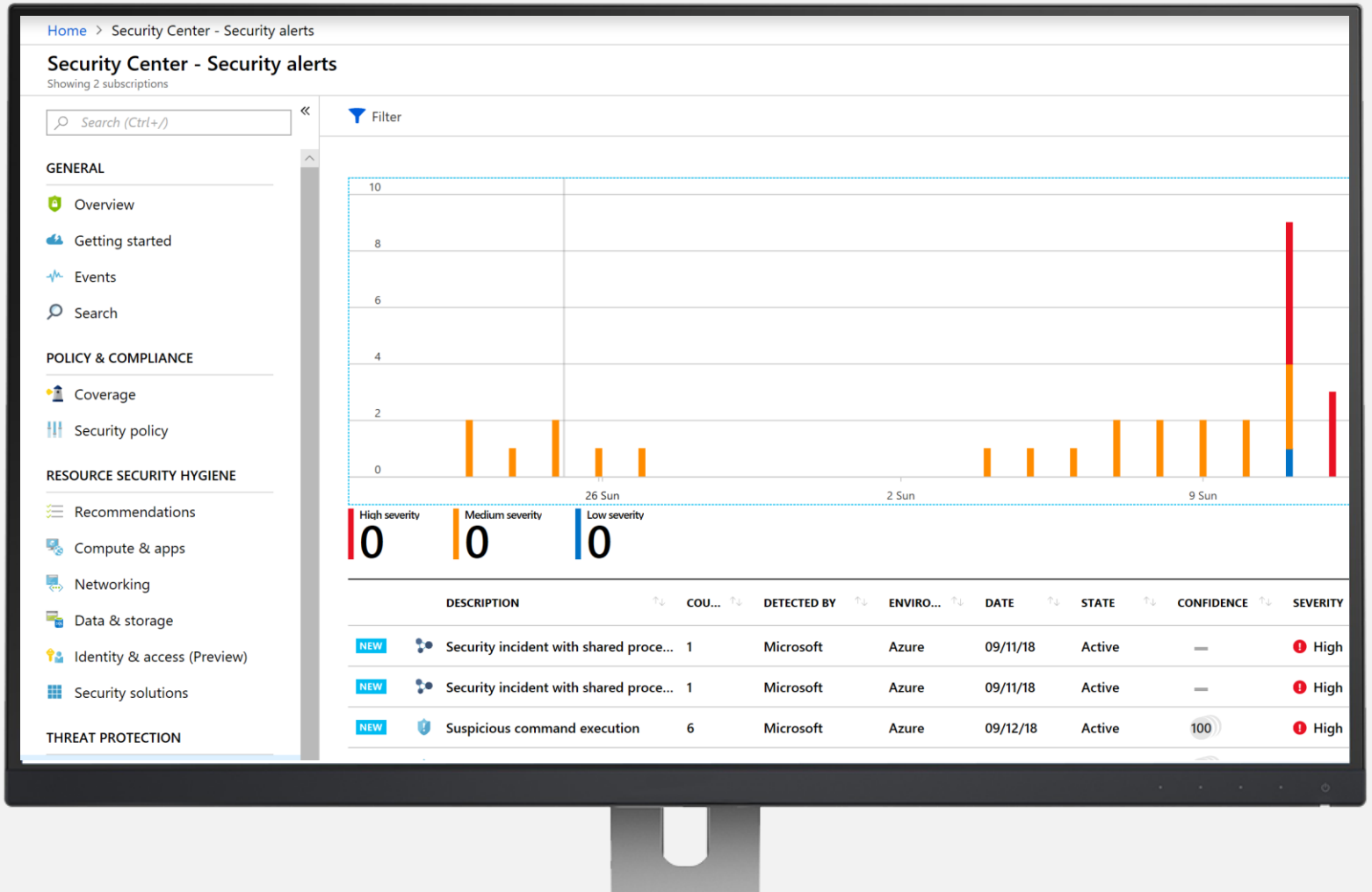
Automate application whitelisting with a ML based solution

Detect threats across services

Detect threats targeting Azure services such as Azure App Services, Azure SQL, Storage services and more

Get Azure UEBA with the integration of Microsoft Cloud App Security

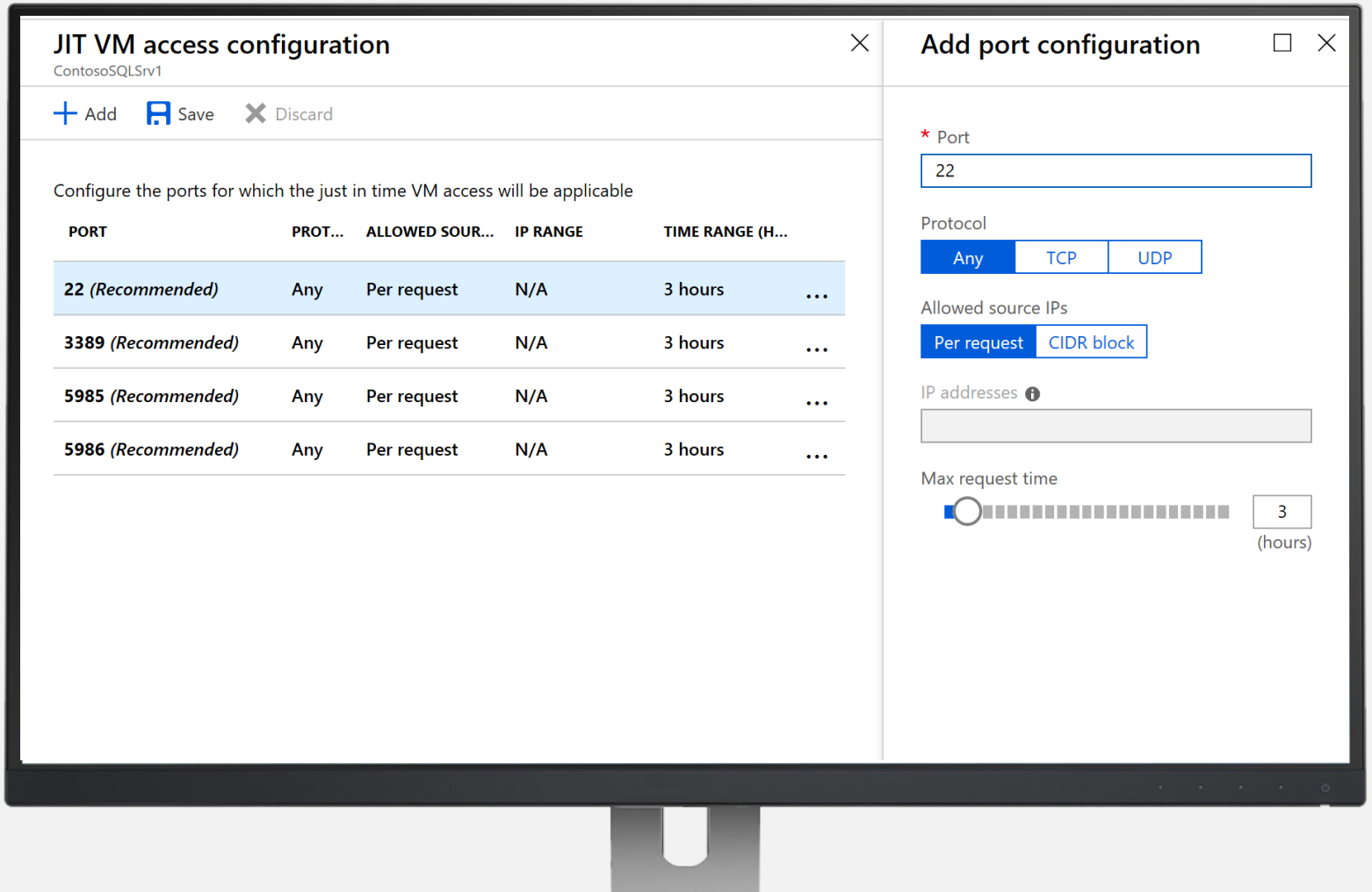
Investigate and respond to an attack with ASC Fusion kill chain analysis



Limit exposure to brute force attacks

Reduce access to VM ports only when it is needed with Just-in-Time VM Access

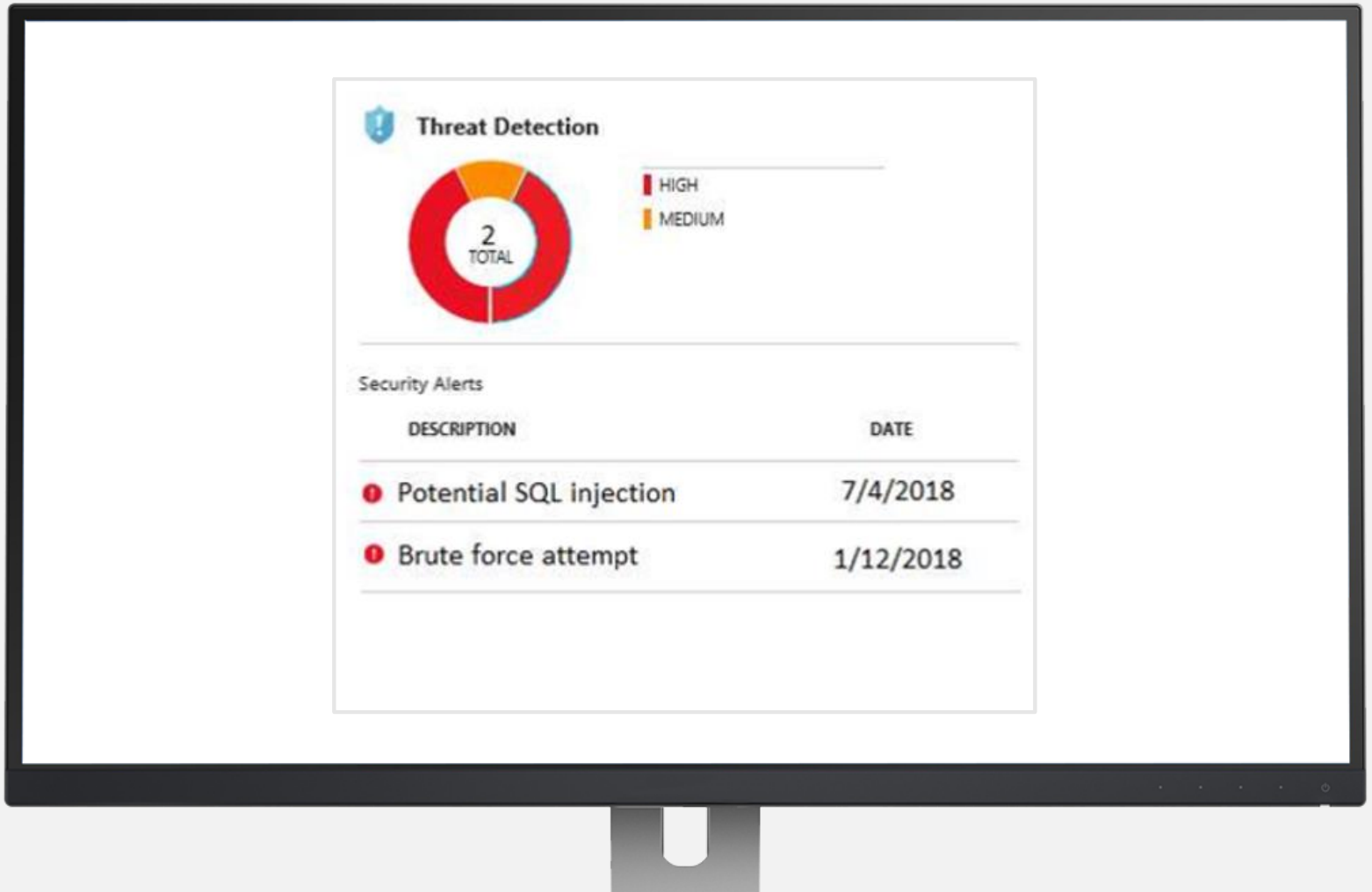
Access automatically granted
for selected ports, and for limited time, approved users and source IPs



Protect data services

Assess potential vulnerabilities across Azure SQL and Storage services

Classify and audit access to sensitive data in Azure SQL



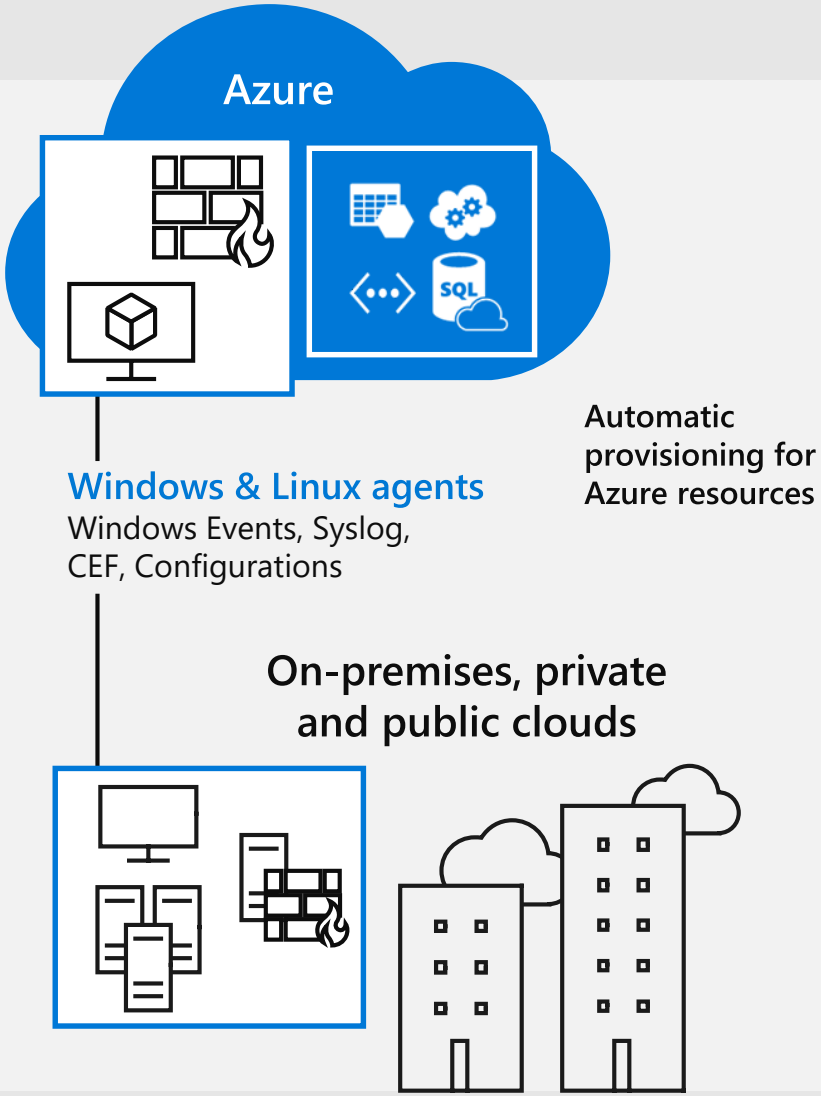
Get secure faster

Automatically discover and onboard Azure resources

Extend to server workloads running in other clouds and on-premises datacenter

Integrate with existing workflows and tools (SIEM, NG Firewall..)

Automatic onboarding & extending to hybrid cloud



Seamless Azure integration

Automatically discovers and monitors security of Azure resources

Extensive log collection

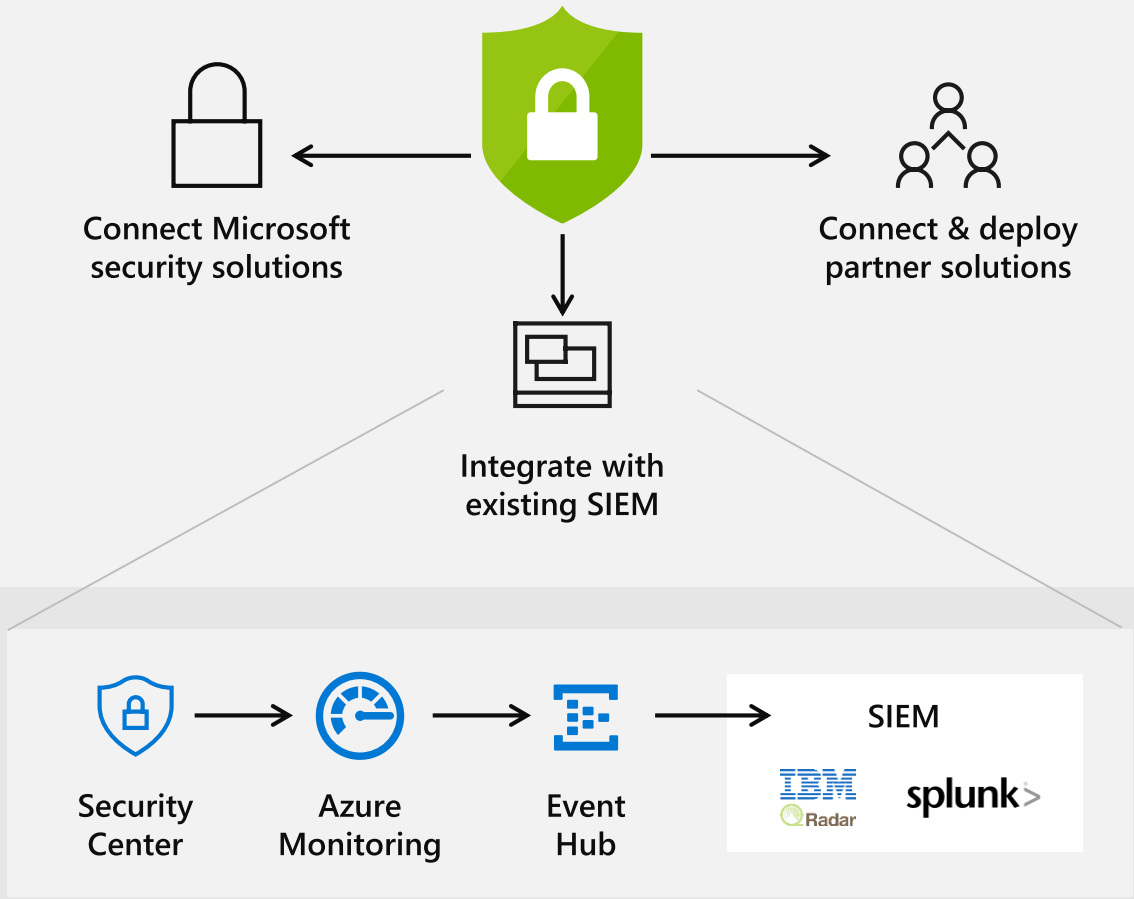
Protect servers running on other clouds and on-premise

Integrating with existing workflows and tools

Respond quickly to threats with automated workflows

Automation support with REST APIs and PowerShell cmdlts

Consolidate SOC insights by integrating with existing SIEM solution

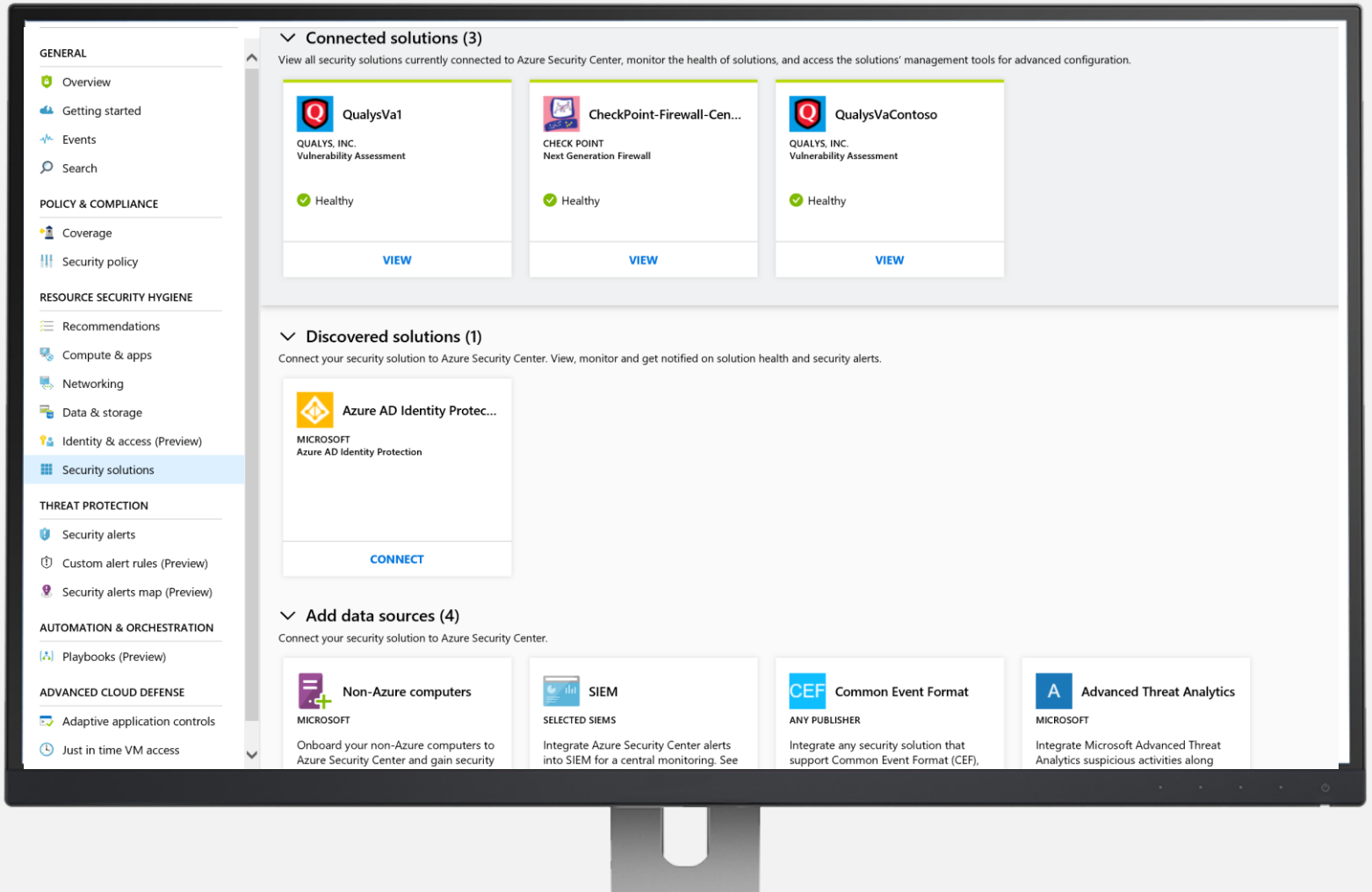


Integrating with security partners

Recommends and streamlines provisioning of partner solutions

Integrates signals for centralized alerting and advanced detection

Enables monitoring and basic management



감사합니다