AhnLab
프라이빗 클라우드 안전성 점검

More and More Private

프라이빗 클라우드 안전성 점검은 프라이빗 클라우드 환경의 정보처리시스템 및 클라우드 영역의 기밀성·무결성·가용성에 영향을 주는 다양한 위협 요인을 분석하고 대응 방안을 제시하는 전문 서비스입니다.

서비스 개요

클라우드 서비스 관리와 애플리케이션의 보안성과 신뢰성 향상을 위하여 클라우드 관리 콘솔, 위협 요소 제거, 환경에 대한 특성 분석을 통해 최적화된 진단을 수행합니다.

프라이빗 클라우드 서비스의 보안성 & 신뢰성 향상

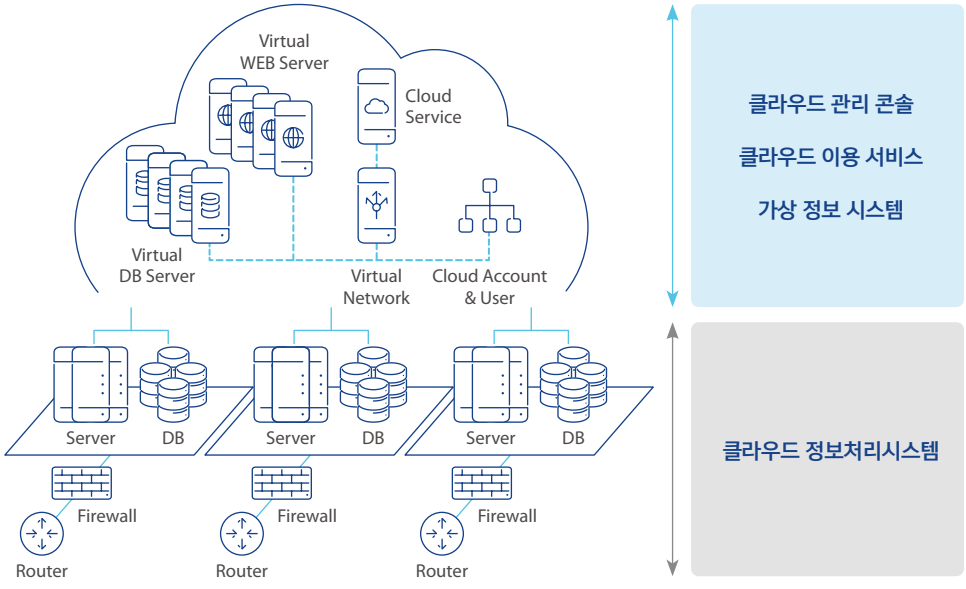
- 클라우드 관리 콘솔의 보안 기능 점검
- 클라우드 및 정보시스템 안전성에 영향을 줄 수 있는 위협요소 제거

프라이빗 클라우드 서비스의 애플리케이션 보안성 향상

- 온프레미스와 클라우드 환경 특성 분석으로 최적화된 진단 수행 및 대응책 제시를 통한 서비스 안전성 향상

특징

프라이빗 클라우드를 자체적으로 구축하여 클라우드서비스를 이용하는 기업을 대상으로 안랩에서 개발한 질의 리스트 기반 분석을 활용하여 클라우드 관리 콘솔, 클라우드 이용 서비스, 가상 정보 시스템, 클라우드 환경의 인프라 자산에 대한 취약점 진단을 수행합니다.



점검항목

프라이빗 클라우드 안전성 점검은 한국인터넷진흥원의 클라우드서비스 보안인증 점검항목 중 IaaS 분야(14개 분야, 117개)를 기반으로 수행합니다.

분야	분류	항목
1. 정보보호 정책 및 조직	1.1 정보보호 정책	3
	1.2 정보보호 조직	2
2. 인적 보안	2.1 내부인력 보안	6
	2.2 외부 인력 보안	3
	2.3 정보보호 교육	3
3. 자산관리	3.1 자산 식별 및 분류	3
	3.2 자산 변경관리	3
	3.3 위험관리	4
4. 서비스 공급망 관리	4.1 공급망 관리 정책	2
	4.2 공급망 변경 관리	2
5. 침해사고관리	5.1 침해사고 대응 절차 및 체계	3
	5.2 침해사고 대응	2
	5.3 사후 관리	2
6. 서비스 연속성 관리	6.1 장애대응	4
	6.2 서비스 가용성	3
7. 준거성	7.1 법 및 정책 준수	2
	7.2 정보시스템 감사	2
8. 물리적 보안	8.1 물리적 보호구역	6
	8.2 정보처리 시설 및 장비 보호	6
9. 가상화 보안	9.1 가상화 인프라	6
	9.2 가상 환경	4
10. 접근 통제	10.1 접근통제 정책	2
	10.2 접근 권한 관리	3
	10.3 사용자 식별 및 인증	5
11. 네트워크 보안	11.1 네트워크 보안	6
12. 데이터 보호 및 암호화	12.1 데이터 보호	6
	12.2 매체 보안	2
	12.3 암호화	2
13. 시스템 개발 및 도입 보안	13.1 시스템 분석 및 설계	5
	13.2 구현 및 시행	4
	13.3 외주 개발 보안	1
	13.4 시스템 도입 보안	2
14. 공공기관 보안요구사항	14.1 관리적 보호조치	4
	14.2 물리적 보호조치	2
	14.3 기술적 보호조치	2
총계		117개

수행절차

프라이빗 클라우드 안전성 점검을 위한 계획 수립, 위험분석, 대책 수립, 이행점검 등 단계별로 세분화된 안랩 정보보호 컨설팅 방법론(ASEM)에 따라 체계적으로 점검합니다.

AhnLab
경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901