

네트워크 보안을 위한 NIST 컴플라이언스

어떤 성공 사례를 채택하셨습니까?

네트워크 보안을 위한 NIST 지침

NIST(국립표준기술원)는 다음을 포함하여 다양한 미국, 국제, 산업별 사이버 보안, 데이터 개인 정보 보호, 위험 관리 규정 및 프로그램의 기초를 형성하는 권장 기술 표준 및 지침을 발표합니다.¹

FedRAMP	FISMA (연방 정보 보안 관리법)	HIPAA(건강 보험 양도 및 책임에 관한 법)	GDPR(개인정보 데이터 보호 규정)	C2C (Comply to Connect)	ISO 표준
---------	-------------------------	----------------------------	----------------------	----------------------------	--------

네트워크 보안을 위해 어떤 NIST 지침을 채택했습니까?







사이버 보안^{2,3}

어떤 사이버 보안 관행을 시행하고 있습니까?

<h4>제로 트러스트 보안 관행</h4> <ul style="list-style-type: none"> IoT를 포함한 네트워크의 장치에 대한 가시성 ID를 기반으로 정책을 정의하고 할당하는 일관된 방법 네트워크 전체에서 리소스에 대한 최소 권한 액세스 시행 사용자 및 장치 보안 상태에 대한 지속적인 모니터링 공격이 의심되는 경우 액세스를 제한하거나 취소하는 프로토콜 	<h4>데이터 보호 관행</h4> <ul style="list-style-type: none"> 조직 내에서 사용 중인 애플리케이션 식별 패치, 업데이트, 수정 사항을 모니터링하고 시기적절하게 구현 장치에 대한 보안 태세 표준 시행 사이버 위협 식별, 회피 및 보고에 대한 작업자 교육
---	---

위험 관리⁴

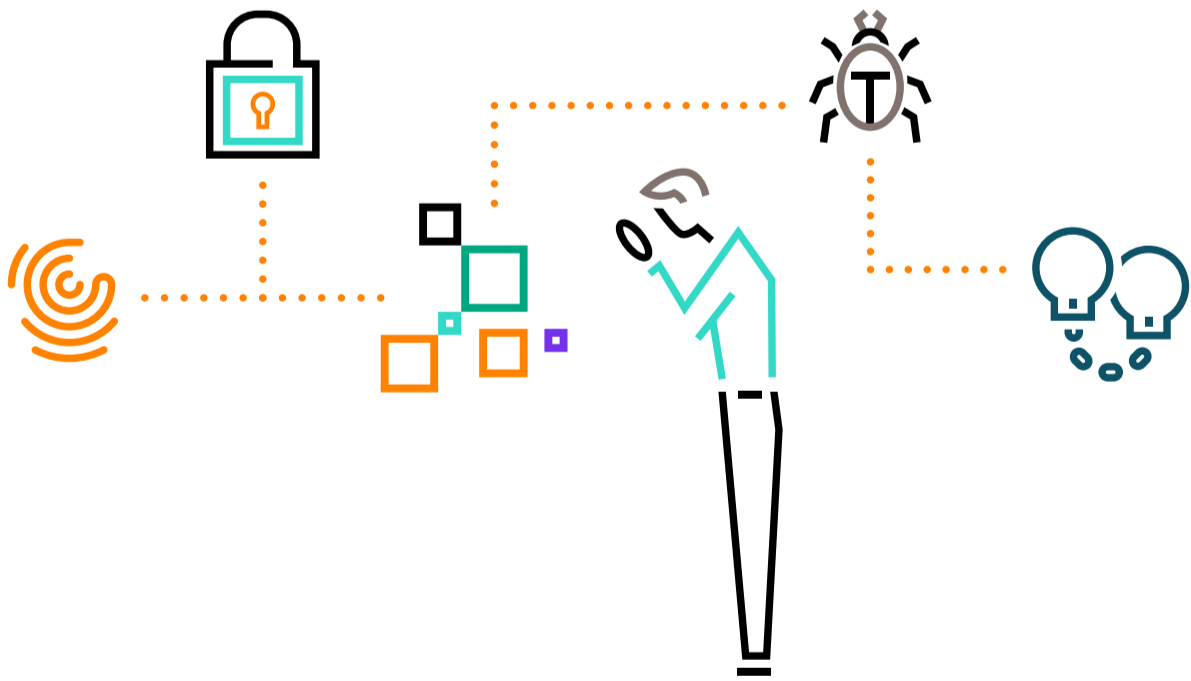
귀사 환경의 솔루션 요건은 무엇입니까?

 <h4>보안 소프트웨어 개발</h4> <p>SSDF(보안 소프트웨어 개발 프레임워크) 및 SDLC(소프트웨어 개발 수명 주기) 성공 사례를 통해 개발되었습니다</p>	 <h4>SBOM(Software Bill of Materials)</h4> <p>SBOM(Software Bill of Materials)과 함께 제공됩니다</p>	 <h4>하드웨어 인증</h4> <p>악성 부팅 코드 및 장치 가장 공격에 대한 기본 보호 기능을 포함합니다</p>
 <h4>공급망 보안</h4> <p>공급망 전반에 걸쳐 자체 무결성을 보호하도록 설계된 프로세스 및 표준으로 개발되었습니다</p>	 <h4>암호화</h4> <p>민감 데이터의 개인 정보 및 무결성을 보호합니다</p>	 <h4>취약점 해결</h4> <p>제품의 취약점을 식별, 보고, 해결하는 프로세스를 갖추고 있습니다</p>

참고: 이 목록은 완전한 것이 아니며 해당 주, 국가 및 업계의 규정 준수 요건이 다를 수 있습니다. 귀사의 요구 사항에 맞는 상세한 네트워크 보안 및 위험 관리 평가를 제공하는 HPE Aruba 네트워킹 전문가와 상의하십시오.

HPE Aruba Networking으로 NIST 성공 사례 채택 가속화

보안 우선의 AI 기반 네트워크가 보안, 개인 정보 및 위험 관리에 대한 NIST 지침을 준수하는 데 어떻게 도움이 되는지 알아보십시오.



¹ Crosswalks. 국립표준기술원. <https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks>. 2023년 11월

² 중요 인프라 사이버 보안 개선을 위한 프레임워크. 버전 1.1 국립표준기술원. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP04162018.pdf>. 2018년 4월

³ Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. 제로 트러스트 아키텍처. NIST 특별 간행물 800-207. 국립표준기술원. <https://doi.org/10.6028/NIST.SP800-207>. 2020년 8월

⁴ 합동 테스크 포스. 정보 시스템 및 조직을 위한 위험 관리 프레임워크: 보안 및 개인 정보 보호를 위한 시스템 수명 주기 접근 방식. NIST 특별 간행물 800-53. 국립표준기술원. <https://doi.org/10.6028/NIST.SP800-53r5>. 2020년 9월

보안 컴플라이언스 요건을 충족하는 더 스마트한 방법

고성을 보장하면서 엣지부터 클라우드까지 비즈니스를 연결하고 보호하는 보안 중심의 포괄적인 AI 기반 네트워킹을 통해 혁신적인 비즈니스 성과를 달성하십시오.

올바른 구매 결정을 위해 HPE 프리세일즈 담당자와 상의하십시오.



자세히 알아보기

arubanetworks.com/products/security/