

클라우드의 보안 간소화

여러 환경 전반에서 일관된 보안 기능을 제공하는
Red Hat Enterprise Linux



클라우드 환경 전반에서 일관되게 운영

Red Hat Enterprise Linux는 다양한 최적화 기능을 통해 클라우드에서 신뢰할 수 있는 보안 중심 성능을 보장합니다. 또한 하이브리드와 멀티클라우드 환경을 위한 일관된 운영 기반을 제공하므로 최적의 위치에서 애플리케이션을 실행할 수 있습니다.

클라우드에 배포된 Red Hat Enterprise Linux의 가치에 대해 [자세히 알아보세요](#).

클라우드의 보안은 최우선 과제

클라우드 도입이 늘어나면서 모든 규모의 조직에서 보안은 계속해서 최우선 고려 사항으로 꼽힙니다. 실제로 조직의 85%가 클라우드와 관련한 최우선 과제로 보안을 꼽았습니다.¹ 이러한 우려에는 타당한 이유가 있습니다. 2022년 보안 침해 사례의 45%가 클라우드에서 발생했기 때문입니다.²

일관성은 어떤 환경에서도 보안과 컴플라이언스 모범 사례의 핵심 요소입니다. 비즈니스를 보호하기 위해서는 데이터센터의 온사이트에 보유하고 있는 보안 정책과 액세스 제어를 클라우드에서도 동일하게 유지해야 합니다. 모든 인프라 풋프린트 전반에 일관된 보안 제어를 제공하는 운영 체제를 기반으로 표준화하면 조직의 보안과 컴플라이언스를 개선하는 데 도움이 됩니다. Red Hat® Enterprise Linux®를 모든 환경 전반에서 운영 기반으로 사용하면 클라우드에서 보안과 컴플라이언스를 유지 관리하는 데 필요한 일관성을 확보할 수 있습니다.

환경 전반에서 보안과 컴플라이언스를 위한 일관된 파운데이션 도입

[Red Hat Enterprise Linux](#)를 사용하면 온사이트, 클라우드, 엣지 환경에서 보안과 컴플라이언스를 더욱 간편하게 유지 관리할 수 있습니다. 보안은 Red Hat Enterprise Linux 아키텍처와 라이프사이클의 핵심입니다. 빌트인 보안 기능과 산업 및 정부 규제에 대한 컴플라이언스를 통해 클라우드에서 시스템을 보호합니다. 모범 사례에 기반한 기본 설정은 시스템을 처음부터 더욱 안전하게 구성합니다. 사전 설치된 클라우드 이미지로 구성된 최소화된 패키지 세트를 통해 사이버 보안 위협 공격 표면이 줄어듭니다. 또한 보안 업그레이드와 라이브 패치가 Red Hat Enterprise Linux 서브스크립션의 일부로 제공됩니다.

Red Hat Enterprise Linux를 사용하면 보안 리스크를 완화하고, 계층화된 보안을 구현하고 유지하며, 하이브리드와 멀티클라우드 환경 전반에서 컴플라이언스를 간소화할 수 있습니다. 이 개요에서는 하이브리드와 멀티클라우드 환경 전반에서 일관된 보안 접근 방식을 도입하기 위한 핵심 기능과 역량을 설명합니다.

Red Hat Insights로 규모에 따라 취약점을 감지하고 해결

2022년 데이터 침해를 식별하고 방지하는 데 소요된 평균 시간은 277일이었습니다.² 데이터 침해를 200일 이내에 발견하고 중단하면 이로 인한 비용을 평균 24% 낮출 수 있습니다.² 일관된 일일 모니터링을 통해 비즈니스 운영을 방해하거나 침해로 이어지기 전에 취약점과 컴플라이언스 리스크를 식별할 수 있습니다.

1 Flexera. "Flexera 2022 클라우드 현황 보고서(State of the Cloud Report)." 2022년 3월.

2 IBM Security. "2022년 데이터 침해로 인한 비용 보고서(Cost of a Data Breach Report 2022)." 2022년.



Red Hat Enterprise Linux



보안과 컴플라이언스 운영 가속화

Red Hat Insights는 보안과 컴플라이언스 운영을 가속화하도록 지원합니다.

- ▶ **91%** 더 빠르게 보안 취약성 감지³
- ▶ **69%** 더 빠르게 정책 위반 감지³

Red Hat Enterprise Linux를 통한 보안 및 컴플라이언스 관리에 대해 자세히 알아보세요.

- ▶ [Red Hat Insights로 보안 위험 관리 기술 개요](#)
- ▶ [Red Hat Insights로 문제 해결 데모](#)
- ▶ [OpenSCAP을 활용하여 보안 컴플라이언스와 취약성 스캔 라이브 데모](#)

Red Hat Enterprise Linux에 포함된 [Red Hat Insights](#)는 Hybrid Cloud Console에서 호스팅되는 서비스 제품군으로, 플랫폼과 애플리케이션을 지속적으로 분석하여 하이브리드 클라우드 환경을 더 효과적으로 관리하고 최적화할 수 있도록 지원합니다. Red Hat Insights는 예측 분석과 심층적인 도메인 전문 지식을 활용하여 보안과 컴플라이언스 리스크를 비롯하여 기타 운영 리스크를 식별, 평가하고 문제 해결 조치를 권장합니다. 또한 심각도, 위험 유형, 변경의 영향에 따라 문제 해결 우선순위를 지정하는 데 도움을 줍니다. Red Hat Insights는 온사이트와 클라우드 환경에서 작동하므로 단일 인터페이스에서 Red Hat Enterprise Linux를 관리할 수 있습니다. 또한 Red Hat 계정을 클라우드 공급업체 계정에 연결하고 클라우드 기반 시스템과 워크로드를 프로비저닝할 때 Red Hat Insights와 기타 Red Hat 서비스에 자동으로 연결하도록 선택할 수 있습니다.

Red Hat Insights에는 하이브리드와 멀티클라우드 환경을 보호하는 데 도움을 주는 다양한 서비스가 포함되어 있습니다.

- ▶ **취약점 서비스:** CVE(Common Vulnerabilities and Exposures)에 대해 시스템을 스캔하고, 스캔 정보를 수집하고, 단일 인터페이스를 사용해 문제 해결 지침에 액세스할 수 있습니다.
- ▶ **맬웨어 서비스:** 활성 맬웨어 시그니처를 포함한 시스템을 빠르게 식별하여 장기적인 노출을 방지합니다.

내장된 스캔 및 문제 해결 기능으로 컴플라이언스 보장

규정을 준수하지 않으면 보안 위험과 더불어, 벌금 지불, 비즈니스 손상, 인증 상실 등을 유발할 수 있습니다. 2022년 컴플라이언스 실패 수준이 높은 조직이 경험한 데이터 침해로 인한 평균 비용은 557만 달러였습니다.² 높은 컴플라이언스 실패 수준으로 인해 2022년 데이터 침해 비용은 평균 258,293달러 증가했습니다.²

Red Hat Enterprise Linux는 주요 정부 및 산업 표준에 인증되어 규제가 엄격한 환경에서도 확신을 갖고 사용할 수 있습니다. Red Hat Insights에는 하이브리드와 멀티클라우드 환경에서 더욱 쉽게 컴플라이언스를 유지 관리하는 데 도움을 주는 다양한 서비스가 포함되어 있습니다.

- ▶ **컴플라이언스 서비스:** OpenSCAP 정책으로 컴플라이언스를 감사하고, 컴플라이언스 미준수 시스템에 대해 문제 해결을 수행하고, 규정 준수 및 보안 감사에 대한 리포트를 생성합니다. 또한 환경과 운영에 따라 기본 정책을 맞춤 설정하여 더욱 정확한 결과를 생성할 수 있습니다. 내장된 주요 기준은 다음과 같습니다.
 - ▶ 결제 카드 산업 데이터 보안 표준(PCI-DSS)
 - ▶ 향상된 운영 체제 보호 프로파일(공통평가기준)
 - ▶ 호주 사이버 보안 센터(ACSC) Essential Eight
 - ▶ CIS(Center for Internet Security) 벤치마크
 - ▶ 건강보험 정보의 이전 및 그 책임에 관한 법률(HIPAA)
 - ▶ 미국 국방정보시스템연구원 보안 기술 구현 가이드(DISA STIG)
- ▶ **정책 서비스:** 사용자 정의 보안 정책을 정의하고, 시스템의 컴플라이언스를 모니터링하고, 시스템이 컴플라이언스를 준수하지 않는 경우 팀에 알립니다.

³ Principled Technologies, Red Hat 후원. "[Red Hat Insights를 활성화해 모니터링을 자동화하여 관리 시간 및 노력 절감\(Save administrator time and effort by activating Red Hat Insights to automate monitoring\)](#)," 2020년 9월.

이미지 빌더 서비스로 클라우드 전반에 일관되고 강화된 이미지 배포

오늘날 조직의 89%가 멀티클라우드 전략을 시행하고 있습니다.¹ 멀티클라우드 접근 방식을 활용하면 각 워크로드에 적합한 클라우드를 선택할 수 있지만, 동시에 복잡성이 발생하고 비일관성으로 인한 리스크가 증가하여 보안과 컴플라이언스 문제가 발생할 수 있습니다.

[Red Hat Insights 이미지 빌더 서비스](#)를 사용하면 Red Hat Enterprise Linux 운영 체제 이미지를 하이브리드 클라우드 환경 전반에서 더 빠르고 쉽게 생성, 관리, 배포할 수 있습니다. 보안이 강화된 사용자 정의 이미지를 구축하여 템플릿으로 저장한 다음, 여러 클라우드 공급업체 인벤토리로 푸시하여 프로비저닝을 간소화할 수 있습니다. 이를 통해 멀티 클라우드 전반에서 시스템을 일관되게 구성할 수 있습니다.

원격 증명으로 환경 전반에서 시스템 무결성 검증

고도로 분산된 대규모 환경에서 시스템 무결성은 무엇보다 중요합니다. 신뢰할 수 없고 손상된 시스템으로 인해 조직은 악의적인 사용자의 공격에 취약해질 수 있습니다.

Red Hat Enterprise Linux에는 부팅 시 시스템의 상태를 검증하고 원격 시스템의 무결성을 지속적으로 모니터링하는 원격 증명 기능이 포함되어 있습니다. [Keylime](#) 오픈소스 프로젝트를 기반으로 하는 원격 증명은 신뢰할 수 있는 플랫폼 모듈(Trusted Platform Module, TPM)과 Linux 커널 무결성 측정 아키텍처(Integrity Measurement Architecture, IMA)를 사용하여 규모에 맞게 시스템을 모니터링합니다. 또한 모니터링 대상 시스템에 암호화된 파일을 전송하고, 모니터링되는 시스템이 무결성 테스트에 실패할 때마다 수행되는 자동화된 조치를 지정할 수도 있습니다.

네트워크 바운드 디스크 암호화로 클라우드에서 데이터 보호

데이터는 비즈니스의 중요한 자산이며, 클라우드에서 이러한 데이터를 보호하는 것은 매우 중요합니다.

Red Hat Enterprise Linux는 네트워크 바운드 디스크 암호화(Network Bound Disk Encryption, NBDE) 지원을 포함하여 유휴 상태에 있는 데이터를 간편하게 보호할 수 있습니다. NBDE는 하나 이상의 네트워크 서버에 대한 연결을 통해 자동으로 스토리지 볼륨을 해제합니다. 이를 통해 암호화 키를 수동으로 관리하지 않고도 볼륨의 암호를 해독할 수 있으며, 볼륨이 안전하게 보호되는 경우에만 사용할 수 있도록 보장합니다. Red Hat Enterprise Linux는 TPM을 통한 NBDE도 지원하여 암호화된 볼륨을 해제하기 전에 시스템 무결성을 보장합니다.

내장된 Identity 및 액세스 관리 기능으로 더욱 간편하게 제로 트러스트 아키텍처 구현

기존 경계 기반 보안 방식으로는 광범위하게 분산된 새로운 클라우드 기반 환경을 효과적으로 보호할 수 없습니다. [제로 트러스트 아키텍처](#)는 네트워크 경계에만 배타적으로 보안을 적용하는 것이 아니라 각 자산에 보안을 적용하여 도움을 줍니다. 실제로, 제로 트러스트를 구현하면 데이터 침해로 인한 비용을 평균 20.5% 줄일 수 있습니다.² [Identity 및 액세스 관리](#)는 제로 트러스트 아키텍처의 핵심 요소입니다.

Red Hat Enterprise Linux에 포함된 [Red Hat Identity Management](#)는 전체 환경에서 Identity 관리를 중앙 집중화하고, 보안 제어를 강화하고, 보안 표준을 준수하도록 지원합니다. 제로 트러스트 모범 사례를 구현하고 Identity 관리 인프라를 간소화하는 데 필요한 기능을 제공합니다. 데이터센터 전체에 걸친 확장 가능한 단일 인터페이스를 통해 사용자를 인증하고 정책 기반 또는 역할 기반 액세스 제어(RBAC)를 구현할 수 있습니다. Red Hat Identity Management는 표준 인터페이스를 통해 Microsoft Active Directory, LDAP(Lightweight Directory Access Protocol), 그 외 타사 솔루션과도 통합됩니다. Red Hat Identity Management는 인증서 기반 인증과 권한 부여 기술도 지원합니다.



Linux 환경에서 제로 트러스트 기반 구축

제로 트러스트 아키텍처를 구현하면 IT 환경과 조직을 더 안전하게 보호할 수 있습니다.

- ▶ Red Hat Enterprise Linux로 제로 트러스트를 구현하는 방법에 대해 [자세히 알아보세요](#).
- ▶ Red Hat Enterprise Linux의 사용자 관리에 관한 [라이브 데모를 시청하세요](#).



여러 릴리스 간의 보안 관리 시간 단축

자동화는 수동 오류를 줄이고 시스템을 더욱 빠르게 관리하는데 도움이 됩니다.

Red Hat Enterprise Linux의 시스템 롤에 관한 [라이브 데모를 시청하세요](#).

시스템 롤을 통해 보안 구성과 관리 간소화

인프라의 규모와 복잡성이 커질수록 수동으로 관리하기는 어려워집니다. 클라우드 구성 오류는 데이터 침해 사례 중 15%의 초기 공격 벡터를 차지했으며, 이로 인해 2022년 침해당 평균 414만 달러의 비용이 발생했습니다.² 자동화를 구현하면 더 적은 노력으로도 시스템을 더욱 빠르고 일관되게 구성하고 관리할 수 있습니다.

[Red Hat Ansible® Automation Platform](#)으로 구동되는 Red Hat Enterprise Linux 시스템 롤을 통해 자동화를 사용하여 더 짧은 시간 내에 규모에 맞게 보안 설정을 설치하고 관리할 수 있습니다. 시스템 롤은 인프라 포털에서 여러 Red Hat Enterprise Linux 릴리스와 연동되어 단일 커맨드 또는 워크플로우로 모든 시스템에서 새로운 보안 설정을 구성하고 관리할 수 있습니다.

자세히 알아보기

하이브리드와 멀티클라우드 환경 전반의 보안과 컴플라이언스에 대해 일관된 접근 방식을 취하면 조직을 더욱 효과적으로 보호할 수 있습니다. Red Hat Enterprise Linux는 인프라 포털, 데이터센터, 클라우드, 엣지에서 애플리케이션을 실행하기 위한 보안 중심의 기반을 제공합니다.

하이브리드 클라우드 보안에 대한 Red Hat의 접근 방식에 대해 [자세히 알아보세요](#).



Red Hat 소개

Red Hat은 세계적인 오픈소스 소프트웨어 솔루션 공급업체로서 커뮤니티 기반의 접근 방식을 통해 신뢰도 높은 고성능 Linux, 하이브리드 클라우드, 컨테이너 및 쿠버네티스 기술을 제공합니다. 또한 Red Hat은 고객이 클라우드 네이티브 애플리케이션을 개발하고, 신규 및 기존 IT 애플리케이션을 통합하고, 복잡한 환경을 자동화하고 관리할 수 있도록 지원합니다. [Fortune 선정 500대 기업의 신뢰를 받는 어드바이저](#)인 Red Hat은 전 세계 고객에게 [권위 있는 어워드를 수상](#)한 지원, 교육 및 컨설팅 서비스를 제공하여 모든 산업 분야에서 오픈 혁신의 이점을 실현할 수 있도록 최선을 다하고 있습니다. Red Hat은 기업, 파트너, 커뮤니티로 구성된 글로벌 네트워크의 허브 역할을 하며 고객들이 성장하고, 확장하고, 디지털 미래에 대비할 수 있도록 지원합니다.

한국레드햇 홈페이지 <https://www.redhat.com/ko>

f www.facebook.com/redhatkorea
구매문의 080 708 0880
buy-kr@redhat.com