



보안 및 컴플라이언스 향상

강력한 오픈소스 Linux 플랫폼으로 리스크 감소

목차

1 Linux: 미래를 위한 기반

2 효과적인 보안 및
컴플라이언스 접근 방식 도입

2.1 Linux 환경에서의 취약성
식별 및 문제 해결

2.2 Linux 환경에서의
컴플라이언스 관리

3 모범 사례 및 추천 툴

4 Red Hat을 통한 보안 및
컴플라이언스 강화

5 성공 사례 보기:
영국 기상청

6 지금 시작해 보세요.



Linux: 미래를 위한 기반



Linux®는 세계에서 가장 인기 있는 운영 체제 중 하나로, 현대적이고 혁신적인 IT를 위한 이상적인 플랫폼을 제공합니다. 주로 데이터센터와 클라우드 컴퓨팅 환경에서 가용성이 높은 안정적인 중요 워크로드에 사용되며, 다양한 활용 사례, 타겟 시스템 및 기기를 지원합니다. 모든 주요 퍼블릭 클라우드 공급업체에서는 자사 마켓플레이스에서 Linux의 다양한 배포판을 제공합니다.

그렇지만 선택하는 Linux 배포판과 관리 툴에 따라 효율성, 보안, IT 환경의 상호운용성에 상당한 영향을 미칠 수 있습니다. 이 e-book에서는 Linux 환경에서의 취약점과 컴플라이언스 리스크에 대해 고려할 핵심 사항과 지침을 살펴봅니다.

주요 우려사항인 보안과 컴플라이언스

IT 보안 및 컴플라이언스 리스크 관리는 모든 조직에서 지속적으로 우려하고 있는 부분입니다. 실제로 조직 중 23%가 최근 2년 동안 주요 사이버 보안 공격을 경험했습니다.¹ 보안 침해는 막대한 비용 손실로 이어질 수 있습니다. 데이터 침해로 인해 초래된 비용은 평균 446만 달러에 달합니다.²

끊임없이 바뀌는 산업 및 정부 규제를 지속적으로 파악하기란 어려운 일이며, 컴플라이언스 위반이 발생하는 경우 평균 데이터 침해 비용은 5% 정도 상승합니다.²

비효율적인 보안의 영향 방지

보안 침해 발생 리스크와 영향을 줄이기 위해서는 빠르게 대처해야 합니다.

445만 달러

데이터 침해로 인한 평균 총 비용(2023년)²

277일

데이터 침해를 식별하고 방지하는 데 걸린 평균 시간(2023년)²

102만 달러

200일 이내에 데이터 침해를 식별하고 방지할 수 있는 경우 평균 절감 비용²

¹ Nash Squared, "2023 Nash Squared Digital Leadership Report", 2023년 11월.

² IBM Security, "Cost of a Data Breach Report 2023", 2023년.

일반적인 보안 및 컴플라이언스 과제

보안 취약성 및 컴플라이언스 관리를 어렵게 만드는 요소는 다음과 같습니다.

변화하는 보안 및 컴플라이언스 환경

보안 위협은 빠르게 변화하기 때문에 새로운 위협과 진화하는 규제에 신속하게 대응할 수 있어야 합니다.

23%

규모를 막론하고 모든 조직이 최근 2년 동안 주요 사이버 보안 공격을 경험한 비율.³

82%

2023년에 발생한 데이터 침해 중 클라우드 환경에 저장된 데이터 또는 여러 환경에 분산되어 저장된 데이터와 관련이 있는 비율.⁴

분산형 클라우드 환경

지리적으로, 그리고 논리적으로 분산된 하이브리드 및 멀티클라우드 환경을 사용할 경우 IT 인프라를 한눈에 종합적으로 파악하지 못할 수 있어 모든 시스템에서 일관된 구성을 관리하는 것이 더 어려울 수 있습니다.

크고 복잡한 IT 환경

대규모 인프라는 여러 보안 및 컴플라이언스 툴을 포함하고 있기 때문에, 리스크 관리 운영을 복잡하게 만듭니다.

보안 시스템의 복잡성으로 인해 증가한 데이터 침해 비용

\$240,889.⁴

원격 근무 인력으로 인해 증가한 데이터 침해의 평균 비용

\$173,074

원격 근무가 요인이 아닌 데이터 침해와의 비교.⁴

인력 부족 및 원격 업무 지침으로 인한 제한

대부분의 조직은 수동으로 보안 및 컴플라이언스 태스크를 관리하는 데 필요한 인력이 부족합니다. 또한 원격 근무는 기기와 조직의 디지털 자산에 대한 액세스 지점 보호에 대한 부담을 늘릴 수 있습니다.

3 Nash Squared, "2023 Nash Squared Digital Leadership Report", 2023년 11월.

4 IBM Security, "Cost of a Data Breach Report 2023", 2023년.

효과적인

보안 및 컴플라이언스 관리 접근 방식

보안 취약성과 컴플라이언스 관리는 보안 및 규제 정책을 준수하도록 시스템을 모니터링하고 평가하는 작업을 포함합니다. 이상적인 보안 취약성 및 컴플라이언스 관리 방식은 환경 전반에서 다음과 같은 일관되고 반복 가능한 프로세스를 개발할 수 있게 해줍니다.



평가(Assess)

규정을 준수하지 않거나, 취약한 시스템을 식별합니다. 인프라에서 워크로드에 이르기까지 환경의 실제 보안 상태를 평가합니다. 다수의 보안 권고 사항 중 시스템과 환경에 실질적으로 적용 가능한 것이 무엇인지 파악합니다.



우선순위 지정

문제 해결에 필요한 노력, 문제의 영향 및 심각도에 따라 문제 해결 작업을 체계적으로 정리합니다. 리스크 관리 기술을 적용하여 각 문제의 실제 비즈니스 리스크를 파악하고, 그에 따른 해결 방법을 계획합니다. 리스크에는 침해로 이어지는 문제가 발생할 가능성, 침해의 잠재적인 심각성, 문제 해결의 영향 등이 포함됩니다. 개발 및 테스트 시스템에서 특정 문제를 해결한다는 것이 적합하지 않을 수도 있지만, 이 동일한 문제가 프로덕션 시스템에는 매우 중요할 수도 있습니다.



문제 해결(Remediate)

조치가 필요한 시스템에 빠르게 패치를 적용하고 해당 시스템을 재설정합니다. 구성과 패치 프로세스를 자동화하여 문제 해결 속도를 높이고 시스템 전반에서 일관성을 보장하며 인적 오류의 위험을 줄입니다. 자동화 툴이 효과적으로 적용되면 문제를 빠르게 해결할 수 있으므로 환경과 비즈니스의 보안을 개선하는 데 도움이 됩니다.



리포트

변경 사항이 적용되었는지 확인하고 보고를 자동화해 감사를 간소화합니다. 효과적인 보고는 임원급 인력, 감사자, 기술 팀에게 적절한 수준의 세부 사항이 포함된 정보를 제공하여 현재 보안 리스크 및 노출을 파악할 수 있도록 돕습니다.

이러한 방식은 조직이 **DevSecOps**와 같이 현대적이고 빠르게 변화하는 개발 및 관리 기술에 익숙해지는데도 도움이 됩니다. 다음 섹션에서는 보안과 컴플라이언스 리스크를 더욱 효과적으로 관리하기 위한 핵심 고려 사항과 조치에 대해 살펴봅니다.

Linux 환경에서의 취약성 식별 및 문제 해결

취약성 식별 및 문제 해결은 인프라를 평가해 공격에 취약한 시스템을 찾아 문제를 해결하는 프로세스입니다. 이 취약성은 새로운 위협, 오래되거나 누락된 패치, 시스템 구성 오류로 인해 발생합니다. 문제 해결 작업은 패치, 업데이트, 시스템 재설정을 통해 이러한 취약성을 해결하는 과정을 포함합니다.

왜 중요할까요?

보안 취약성으로 인해 침해가 발생하면 큰 비용을 지불해야 할뿐만 아니라 고객의 신뢰와 기업의 평판이 하락하고, 수익이 감소할 수 있습니다. 실제로 사업적 손실이 평균 데이터 침해 비용의 29.2%를 차지하기도 합니다.⁵

효과적인 취약성 식별 및 문제 해결의 장애 요인

대부분의 조직은 대규모 운영을 위한 일관된 보안 전략을 갖추고 있지 않습니다.

- ▶ 완전한 보안 전략을 개발하고 실행하기에는 인력이 부족하거나, 해당 인력의 기술이 부족할 수 있습니다.
- ▶ 일반적인 보안 스캔 툴은 방대한 규모의 잠재적 취약성 목록을 생성하지만, 환경에 따라 적용되는 부분이 다르기 때문에 직원은 적합한 취약성과 문제 해결 작업을 확인하는 데 많은 시간을 들여야 합니다.
- ▶ 수동으로 진행하는 식별, 문제 해결, 추적 프로세스는 운영 속도를 저하시키며, 알려진 취약성이 패치되지 않는 경우도 많습니다.
- ▶ 임시로 문제를 해결하는 경우 패치가 일관성 없게 적용되어 잠재적 보안 리스크가 커집니다.

보안 관리 툴이 핵심적으로 갖춰야 할 기능

효과를 기대할 수 있으려면 보안 침해가 발생하기 전에 시스템의 취약성을 빠르게 식별하고 문제를 해결할 수 있어야 합니다. 그러므로 통합 보안 관리 툴에는 다음과 같은 기능이 필요합니다.



시스템 분석: 환경 전반의 시스템 및 인스턴스에서 운영 체제와 워크로드 수준의 리스크를 식별합니다.



문제 해결 자동화: 식별된 리스크의 문제 해결을 자동화하여 IT 및 보안 팀의 업무 속도, 정확성, 효율성을 개선합니다.



벤더 전문 지식 통합: 해당 벤더 제품에 대한 문제 해결 가이드를 제공합니다. 리스크를 줄이는 데 도움이 될 만한 간단한 작업이 포함될 수 있습니다.



최신 데이터에 정기적으로 액세스: 운영 체제 및 애플리케이션 벤더로부터 알려진 취약성 및 보안 리스크에 대한 최신 데이터를 받습니다.



보고서 생성: 잠재적인 리스크, 문제 해결 작업, 다양한 사용자별로 적절한 수준의 상세 내용을 포함한 보고서를 생성합니다.

Linux 환경에서의 컴플라이언스 관리

컴플라이언스 관리는 시스템이 시간이 지나도 기업 정책, 업계 표준, 적용되는 규제를 준수하도록 보장하는 프로세스입니다. 또한, 인프라 평가를 사용해 규제, 정책 또는 표준의 변화, 설정 오류, 기타 이유로 인해 규정을 준수하지 않는 시스템을 식별합니다.

왜 중요할까요?

규정을 준수하지 않으면 보안 위험과 더불어, 벌금 지불, 비즈니스 손상, 인증 상실 등을 유발할 수 있습니다. 컴플라이언스 위반은 보통 막대한 데이터 침해 비용을 초래합니다.⁶

효과적인 컴플라이언스 관리의 어려움

많은 조직에서는 수동 작업과 사용자 정의 스크립트를 사용하여 컴플라이언스를 관리합니다. 하지만 이러한 프로세스는 너무 느리기 때문에, 빠르게 변화하는 현대적 개발과 운영의 규모가 제한됩니다.

- ▶ 일반적인 표준과 기준이 다양하기 때문에 사용자 환경에 대한 적합성과 영향을 파악하기가 어렵습니다.
- ▶ 수동 프로세스는 컴플라이언스 모니터링, 문제 해결, 감사 운영의 속도를 저하시킵니다. 이로 인해 직원은 효율적으로 시간을 활용하지 못하고, 정책 적용의 일관성이 결여되어, 컴플라이언스 문제의 리스크가 커집니다.
- ▶ 대부분의 조직에서는 보안과 컴플라이언스 관리에 개별 툴을 사용하기 때문에 운영 효율성이 떨어지고, 일관된 사용자 정의 정책을 설정하는 데 어려움이 있습니다.

컴플라이언스 관리 툴의 핵심 기능

효과를 기대할 수 있으려면 상황별 정책을 정의 및 적용하고, 시스템이 이러한 정책을 준수하도록 하며, 감사를 위한 보고서를 신속하게 생성하고 관리해야 합니다. 그러므로 통합 컴플라이언스 관리 툴에는 다음과 같은 기능이 필요합니다.



분석 사용: 시간을 효율적으로 활용하여 컴플라이언스 리스크를 일관적으로 식별할 수 있습니다.



문제 해결 자동화: 규정을 준수하지 않은 시스템에 대한 문제 해결을 자동화합니다.



전체적 파악: 환경 전반의 컴플라이언스 상태를 전체적으로 확인할 수 있어야 합니다.



컴플라이언스 보고서 생성 자동화: 감사 요건 및 보고 대상자에 따라 보고서 생성을 자동화합니다.



전문적 조언 제공: 환경 전반에서 규정을 준수하지 않은 시스템 문제를 해결하기 위한 전문적인 조언과 상황별 지침을 제공합니다.

모범 사례 및 추천 툴

정기적인 시스템 분석

매일 모니터링을 수행하면 비즈니스 운영이 중단되거나 보안 침해 발생 전에 취약성과 컴플라이언스 리스크를 식별하는 데 도움이 됩니다. 운영 체제 및 애플리케이션 벤더의 최신 보안 데이터를 활용하여 분석의 정확도를 높이세요. 또한, 사용자의 환경과 작업에 맞게 사용자 정의 보안 정책을 설정하면 더 정확한 컴플라이언스 결과를 받아볼 수 있습니다.

데이터 침해를

200일

이내에 발견하고 방지하면 비용을 크게 줄일 수 있습니다.⁷

빈번한 패치 적용 및 패치 테스트

시스템을 최신 상태로 유지하면 보안, 신뢰성, 성능, 컴플라이언스를 강화할 수 있습니다. 일반적인 중요 문제를 놓치지 않고 해결할 수 있도록 정기적으로 패치를 적용하세요. 중요 버그 및 결함에 대한 패치는 최대한 빨리 적용해야 합니다. 패치를 프로덕션에 적용하기 전에 제대로 작동하는지 확인하기 위해 패치된 시스템을 테스트할 수 있습니다.

효과적인 관리 툴을 사용하면 시스템 패치 속도를 높일 수 있는 최대 비율

56%.⁸

자동화 배포

인프라의 규모와 복잡성이 커질수록 수동으로 관리하기는 어려워집니다. 자동화를 사용해 모니터링을 간소화하고, 빠르게 문제를 해결하며, 일관성을 개선하며, 정기적인 보고를 보장합니다.

보안 자동화와 인공지능(AI)을 통해 데이터 침해로 인한 비용을 낮출 수 있는 비율

39.3%.⁷

⁷ IBM Security, "Cost of a Data Breach Report 2023", 2023년.

⁸ IDC 백서, Red Hat 후원. "Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools". Document #US46109220. 2021년 8월.

툴을 연결하고 프로세스에 맞게 조정

분산된 환경에서는 각 플랫폼마다 다른 관리 툴이 있는 경우가 많습니다. 애플리케이션 프로그래밍 인터페이스(API)를 통해 이러한 툴을 통합하고, 선호하는 인터페이스를 사용해 다른 툴의 태스크를 수행하세요. 더 적은 수의 인터페이스를 사용해 운영을 간소화하고 환경 내 모든 시스템의 보안 및 컴플라이언스 상태를 더 명확히 확인할 수 있습니다. 또한, 환경 전반에서 프로세스를 조정해 일관성과 신뢰성을 강화합니다.

보안 시스템이 매우 복잡한 경우 데이터 침해 시 평균 비용이 증가할 수 있는 비율

31.6%⁹

지속적이고 일관된 보안 전략 도입

효과적인 보안을 구축하려면 구성원, 프로세스, 기술을 통합하는 전체적인 접근 방식이 필요합니다. 피드백과 조정을 기반으로 하는 지속적인 보안 전략으로 현대적인 개발 기술, DevSecOps, 디지털 비즈니스의 요구 사항을 지원할 수 있습니다. 계층화된 심층 보안 방식을 도입하여 운영 체제, 컨테이너 플랫폼, 자동화 툴, 서비스로서의 소프트웨어(SaaS) 자산, 클라우드 서비스 등 기업 환경에서 각 계층의 기능을 최대한 활용하세요.

DevSecOps 방식을 도입하여 데이터 침해 시 평균 비용을 낮출 수 있는 비율

38.4%⁹



이상적인 보안 및 컴플라이언스 툴에는 여러 가지 핵심 기능이 포함되어 있습니다.

사전 예방적 분석

개선을 위해서는 보안 및 컴플라이언스 상태를 파악하는 것이 우선입니다. 자동 분석을 제공하는 툴은 시스템을 정기적으로 모니터링하여 문제를 알려주기 때문에, 담당자가 업무 시간 및 노력을 많이 소모하지 않아도 됩니다.

우선순위가 지정된 응답

규범적인 방식으로 문제 해결 단계를 제공하는 툴을 사용하면 필요한 작업을 직접 조사할 필요가 없으므로, 시간을 절하고 실수의 위험을 줄일 수 있습니다. 또한 잠재적인 영향 및 시스템에 미치는 영향을 기준으로 작업의 우선순위를 지정하여 제한된 패치 기간을 최대한 활용할 수 있습니다.

결과 커스터마이징

일부 취약성 및 컴플라이언스 검사는 관련 사용, 구성 또는 워크로드로 인해 특정 시스템에 적용되지 않을 수 있습니다. 이상적인 툴을 사용하면 비즈니스 컨텍스트를 정의하여 거짓 긍정의 수를 줄이고 비즈니스 리스크를 관리하며 보안 및 컴플라이언스의 상태를 사실적으로 파악할 수 있습니다.

직관적인 보고

패치가 적용되었거나, 패치가 필요하거나, 보안 정책을 준수하지 않는 시스템이 무엇인지에 대한 명확하고 직관적인 보고서를 생성하는 툴은 감사에 더욱 잘 대비하고, 환경을 더욱 잘 파악할 수 있도록 도와줍니다.

통합 인터페이스

환경의 단일 구성 요소 또는 계층을 넘어 관리할 수 있는 툴을 사용하면 보안 작업을 간소화하고 보안 및 컴플라이언스 상태를 더욱 정확하게 파악할 수 있습니다. 또한 통합 툴은 스캔 및 문제 해결 지침에 대한 자세한 컨텍스트를 제공합니다.



실행 가능한 인사이트

기업 환경에 맞게 조정된 정보를 제공하는 툴을 통해 잠재적인 보안 취약성 및 컴플라이언스 문제로 어떤 것이 있는지, 영향을 받는 시스템과 예상되는 파급 효과는 무엇인지 등을 더욱 빠르게 파악할 수 있습니다. 이러한 툴은 문제 해결 작업의 우선순위를 정하고 계획하는 데도 도움이 됩니다.



Red Hat을 통한 보안 및 컴플라이언스 강화

Red Hat은 보안 및 컴플라이언스 리스크 관리에 대한 전체적인 접근 방식을 통해 베어 메탈 및 가상 서버에서 프라이빗, 퍼블릭 및 하이브리드 클라우드 인프라와 엣지 배포에 이르는 전체 IT 환경에서 속도, 확장성 및 안정성을 개선합니다. Red Hat® 플랫폼은 구성원과 프로세스, 기술을 모두 통합하여 운영 효율성을 높이고, 혁신을 촉진하며, 직원의 만족도를 높일 수 있도록 도와줍니다.

이 전략의 핵심에는 **Red Hat Enterprise Linux**가 있습니다. 현대적인 IT 및 엔터프라이즈 하이브리드 클라우드 배포의 일관되고 지능적인 운영 기반인 Red Hat Enterprise Linux는 기업을 위한 최적의 혜택을 제공합니다. 인프라 전반에 일관성이 유지되어 위치에 관계없이 동일한 툴을 사용하여 애플리케이션, 워크로드 및 서비스를 배포할 수 있습니다.

보안은 Red Hat Enterprise Linux 아키텍처와 라이프사이클의 핵심입니다. 다중 계층 침해 방어는 자동화되고 반복적인 보안 제어를 사용해 취약성에 노출될 위험을 완화합니다. 중요 보안 업그레이드와 라이브 패치가 Red Hat Enterprise Linux 서브스크립션의 일부로 제공되므로, 기업의 환경을 더욱 안전한 최신 상태로 유지할 수 있습니다.

66

Red Hat Enterprise Linux로 전환한 이후 당사는 이전에 사용하던 Linux 배포판보다 **더 빠르게 버그와 취약점을 발견하고 조사**할 수 있게 되었습니다.¹⁰

—
Yuki Miyamoto

Square Enix Co., Ltd. Information Technology 부서, IT Infrastructure/Business Online Infrastructure System

Red Hat 관리 툴은 Red Hat Enterprise Linux에 통합되어 보안 취약성 리스크 및 컴플라이언스를 효과적으로 관리하는 데 필요한 기능을 제공합니다.



설정 가능한 툴과 기준이 거짓 긍정의 수를 줄여주어 인프라 상태에 대한 정확한 정보를 제공합니다.



자동화 기능은 설정 및 패치의 정확성을 개선하고 인적 오류를 줄입니다.



사용자 정의 가능한 보기는 적절한 시기에 적합한 대상에게 올바른 정보를 빠르게 제공합니다.



자동화된 사전 예방적 문제 해결 방식 덕분에 지원 팀에 문의하지 않고도 문제를 빠르게 수정할 수 있습니다.



광범위한 리소스 라이브러리는 상세한 타겟 정보를 24시간 연중무휴 제공합니다.



온사이트 및 서비스로서의 소프트웨어(Software-as-a-Service, SaaS) 옵션이 있어 선호하는 툴을 배포할 수 있습니다.



API는 기존 보안과 선호하는 보안, 컴플라이언스 및 관리 툴과 인터페이스를 연결합니다.



취약성 및 맬웨어 감지 기능은 시스템을 검사하여 CVE(Common Vulnerabilities and Exposures) 및 맬웨어 시그니처를 감지합니다.



리소스 최적화 기능을 사용하면 컴퓨팅, 메모리, 네트워크 성능 메트릭을 사용하여 퍼블릭 클라우드 배포 규모를 적절히 조절할 수 있습니다.

통합 툴의 이점 활용

Red Hat 관리 툴은 수년간의 Linux 개발 및 지원 경험을 토대로 개발되었으며, 연동을 통해 IT 관리를 간소화하여 팀의 시간과 노력을 절약하고, 더욱 안전하고 안정적이며 최적화된 환경을 조성합니다.



Red Hat 시스템 분석, 관찰 및 관리

Red Hat Enterprise Linux에 포함되어 서비스로 제공되는 **Red Hat Insights**는 플랫폼과 애플리케이션을 지속적으로 분석하여 위험을 예측하고, 조치를 권장하며, 비용을 추적함으로써 기업이 하이브리드 클라우드 환경을 더 잘 관리할 수 있도록 지원합니다. Insights를 사용하면 IT 효율성, 안정성 및 성능을 모니터링할 수 있고, 보안 및 컴플라이언스 리스크를 관리할 수 있으며, 클라우드 전반에서 지출을 추적하고 최적화할 수 있습니다.

26% 보안 인시던트 해결 시간 단축¹¹

24% 더 효율적인 IT 보안 팀¹¹

76% 예기치 못한 다운타임 감소¹¹



시스템 관리 간소화 및 자동화

Red Hat Satellite는 물리, 가상 또는 클라우드 또는 엣지 환경 등 어디에서나 Red Hat Enterprise Linux 시스템을 프로비저닝하고 유지 관리하도록 설계된 인프라 관리 솔루션입니다. Satellite는 프로비저닝, 패치 및 기타 반복적인 시스템 관리 태스크를 규모에 맞게 간소화하여 운영 효율성을 높이면서 시스템 보안, 가용성 및 정책 컴플라이언스를 유지 관리합니다.

56% 패치 작업 효율성 향상¹²

56% IT 인프라 효율성 향상¹²

28% 총 운영 비용 절감¹²

¹¹ IDC Business Value Snapshot, Red Hat 후원. "The Business Value of Red Hat Insights". Document #US51795124. 2024년 2월.

¹² IDC 백서, Red Hat 후원. "Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools". Document #US46109220. 2021년 8월.

실제 고객 사례

영국 기상청

영국 기상청은 매일 전 세계 사람들에게 날씨 및 기후 관련 서비스를 제공합니다. 영국 기상청은 서버 관리를 위한 포괄적 접근 방식을 확립하는 것을 목표로 Red Hat Satellite 사용을 보완하기 위해 Red Hat Insights를 도입했습니다. 영국 기상청은 Red Hat 기술 계정 관리자의 도움을 받아 서버 환경에 대한 가시성을 상당히 개선했습니다.

먼저 여러 시스템에서 알려진 문제에 관해 Insights를 테스트하는 것으로 시작했습니다. 문제는 즉시 표면화되었으며, IT 팀은 더 광범위한 배포를 진행하기로 했습니다. IT 팀은 내부 변경 관리 프로세스에 따라 Satellite를 사용하여 전체 자산에서 Insights 설치를 간소화했습니다.

IT 팀은 Insights를 사용한 후 훨씬 손쉽게 태스크의 우선순위를 정하고, 문제가 있는지 여부를 확인하며, 문제의 영향을 받는 시스템과 문제의 심각도를 파악할 수 있게 되었습니다. 또한 영국 기상청은 구성 문제를 식별하고 해결하여 원하는 표준에 맞는 서버 자산을 구축할 수 있었습니다.

영국 기상청은 앞으로도 계속 Insights와 Satellite를 사용하여 전체 환경을 관리하고 더욱 선제적인 방식으로 보안 태세를 개선하려고 합니다.

66

Red Hat Insights는 하향식 개요를 제공하고 **자산 관리에 대한 더욱 전체적인 접근 방식**을 도입하는 데 도움이 될 수 있음을 확인했습니다. Red Hat Satellite는 개별 시스템에서 문제를 표면화하는 능력이 매우 탁월한 반면, Red Hat Insights는 개별 시스템 수준에서 문제를 다루는 대신 자산 전체에서 공통적인 문제를 연결하는 데 강점을 갖고 있습니다.

Chris Wilkinson

영국 기상청 수석 시스템 엔지니어

지금 시작해 보세요.

기업의 비즈니스는 자체 IT 인프라 및 애플리케이션에 의존합니다. 효과적인 보안 취약성 및 컴플라이언스 관리 방식과 툴로 기업을 보호할 수 있습니다.

Red Hat은 보안 중심 운영과 혁신에 필요한 신뢰할 수 있는 Linux 플랫폼과 통합 관리 툴 및 서비스를 제공합니다.



Red Hat Insights를 사용하여 리스크 분석

- ▶ Red Hat Insights [알아보기](#)
- ▶ Red Hat Insights에 대한 [애널리스트 의견 확인하기](#)

Red Hat Satellite를 사용하여 규모에 맞게 관리

- ▶ Red Hat Satellite [알아보기](#)
- ▶ Red Hat Satellite에 대한 [애널리스트 의견 확인하기](#)