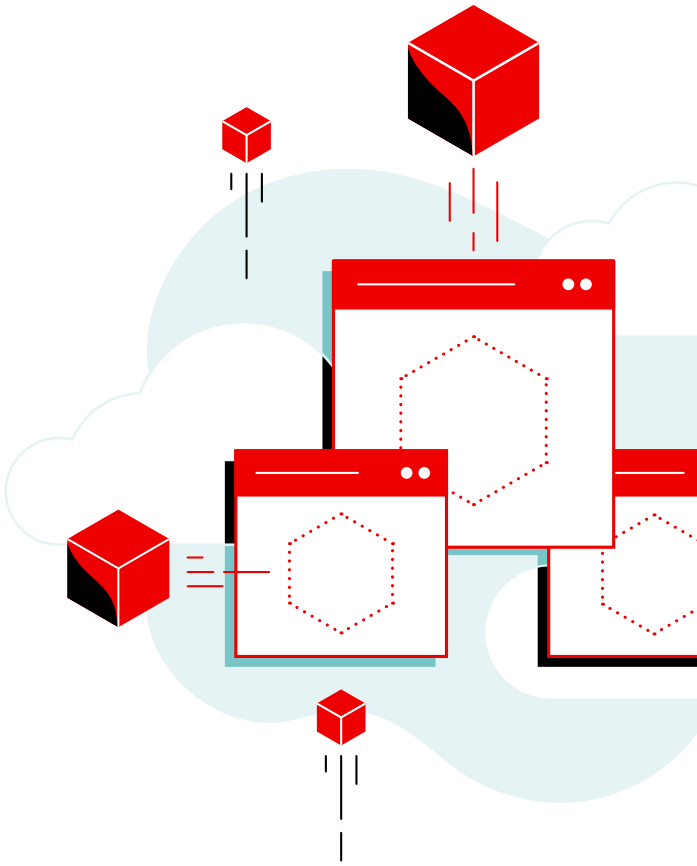
Red Hat

쿠버네티스 보안 현황 리포트

2021



핵심 요약

이번 쿠버네티스 보안 현황 리포트에서는 기업이 중요한 쿠버네티스 애플리케이션 보호 과제를 해결하면서 쿠버네티스, 컨테이너, 클라우드 네이티브 기술을 채택하는 방법을 살펴봅니다. 이 리포트는 500명 이상의 DevOps, 엔지니어링 및 보안 전문가들을 대상으로 한 설문조사 결과를 담고 있으며, 컨테이너 및 쿠버네티스를 수용하는 기업들이 클라우드 네이티브 환경을 보호하기 위해 DevSecOps 이니셔티브를 구현하는 방법에 대한 새로운 조사 결과를 제공합니다. 설문조사는 StackRox가 2021년 초 Red Hat에 인수되기 전에 실시했습니다.

컨테이너 도입 및 보안 문제와 관련된 가장 큰 우려 사항인 보안으로 인해 애플리케이션을 프로덕션 환경에 배포하는 데 계속해서 지연이 발생하기 때문에 쿠버네티스 환경에서 기업이 경험하는 가장 일반적인 보안 인시던트 유형도 살펴봅니다.

설문조사 결과는 Dev, Ops 및 보안 팀 간 협업이 개발 라이프사이클 초기에 보안을 구현하여 쿠버네티스의 가장 큰 이점인 신속한 혁신을 실현하는 데 얼마나 중요한지를 보여줍니다. 많은 조직이 DevSecOps를 도입하고 있다는 사실은 고무적입니다. 조직의 75%가 DevOps 및 보안 팀 간의 협업을 강화하는 이니셔티브를 갖추고 있습니다.

응답자의 94%에 달하는 거의 모든 사람이 지난 12개월 동안 보안 인시던트를 경험했다고 인정했습니다. 대부분의 경우 구성 오류가 그 원인이었습니다. 하지만 상당 부분에서 주요 취약점을 식별하거나 런타임 인시던트가 발생하거나 감사에 실패했습니다. 이러한 결과는 응답자가 프로덕션 환경에 쿠버네티스 워크로드를 배포한 경우에 더욱 중요합니다.

이 리포트의 결과를 벤치마킹하여 컨테이너와 쿠버네티스 전반에 보안 제어를 적용하기 위한 노력을 가속화할 수 있는 방법을 결정하는 것이 좋습니다. 보안이 지연되면 혁신이 지연되며 쿠버네티스의 비즈니스 이점을 저해할 수 있습니다. 컨테이너와 쿠버네티스에 사용할 수 있는 보안 이점은 선언적 구성 및 변경 불가능한 인프라에서 컨테이너화된 애플리케이션에 내재된 격리에 이르기까지 다양합니다. 그러나 조직은 DevOps 기반의 클라우드 네이티브 환경에서 빠르게 실행하여 상당한 이점을 누릴 수 있도록 이러한 기능을 작동시키기 위한 지식, 툴링, 프로세스가 필요합니다.

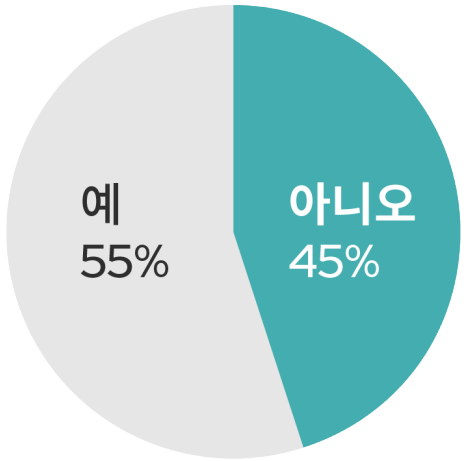
혁신을 지연시키는 보안 우려 사항

응답자의 절반 이상이 보안 문제로 인해 쿠버네티스 애플리케이션의 프로덕션 배포를 연기했습니다.

기업들은 디지털 혁신과 트랜스포메이션을 위한 성장 동력을 촉진하기 위해 쿠버네티스와 컨테이너를 빠르게 도입하고 있습니다. 클라우드에서 탄생한 수많은 신생 기업이 이 기술 스택을 활용하여 성장을 촉진하는 반면, 기존 기업은 기존 워크로드를 하이브리드 클라우드 환경에서 컨테이너 및 쿠버네티스로 마이그레이션하고 있습니다.

신속한 애플리케이션 개발 및 릴리스, 신속한 버그 수정, 향상된 기능 속도는 컨테이너화에서 가장 자주 언급되는 3가지 이점입니다. 그러나 보안을 사후에 고려하게 되면 컨테이너화의 가장 큰 이점인 민첩성이 무색해질 수 있습니다. 설문조사 응답자의 절반 이상(55%)은 보안 문제로 인해 애플리케이션 롤아웃을 연기해야 했습니다. 보안 평가를 통과하지 못한 애플리케이션을 출시하면 비즈니스에 심각한 위험을 초래하게 됩니다. 애플리케이션 배포 지연을 방지하고 컨테이너 및 쿠버네티스의 이점을 실현하기 위해 조직은 보안 수준을 그대로 유지하고 개발 단계로 빌드하여 빌드 단계에서 가능한 한 많은 보안 문제를 해결할 수 있어야 합니다.

컨테이너 또는 쿠버네티스 보안 문제로 인해 애플리케이션의 프로덕션 배포를 미루거나 신속하게 전환했습니까?



응답자의 94%가 지난 12개월 동안 쿠버네티스 환경에서 최소 한 건의 보안 인시던트를 경험

구성 오류는 보안 인시던트의 가장 큰 원인입니다.

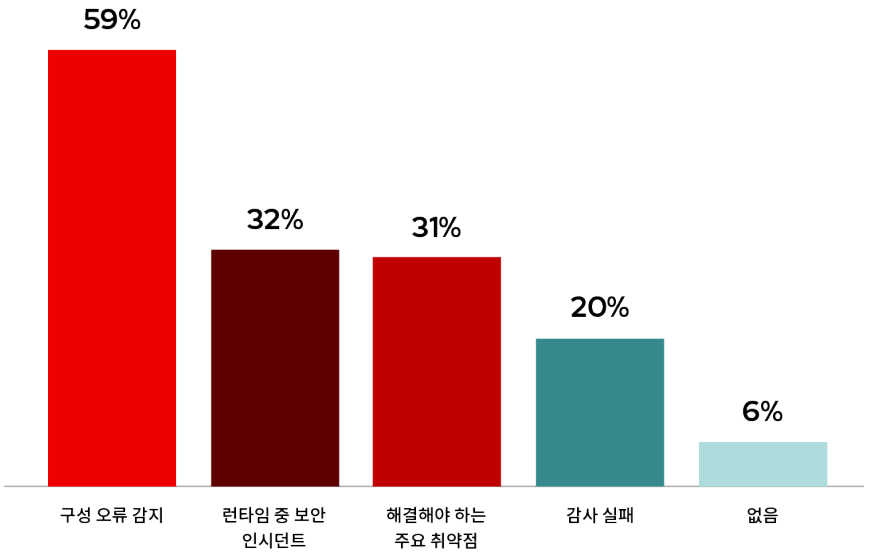
무려 94%에 달하는 설문조사 응답자들이 지난 12개월 동안 쿠버네티스 및 컨테이너 환경에서 보안 인시던트를 경험했습니다.

거의 모든 응답자들이 보안 문제를 겪었다는 사실은 조직의 절반 이상이 보안 문제로 인해 애플리케이션 배포를 미뤘다는 이전의 조사 결과를 설명하는 데 도움이 될 수 있습니다.

인적 오류는 데이터 침해 및 해킹에서 가장 자주 언급되는 원인입니다. 쿠버네티스 및 컨테이너는 강력하지만 이러한 위험을 상당히 증가시킵니다. 쿠버네티스에는 선언적 모델을 통해 적용되는 강력한 기능이 있습니다. 단일 워크로드에는 보다 안전하고 확장 가능한 애플리케이션을 보장하기 위해 상당한 구성이 필요할 수 있습니다. 기술적 부채와 조직의 장애 요소가 추가되면 숙련된 쿠버네티스 전문가라도 항상 모든 것을 올바르게 처리하기란 어려운 일입니다.

60%에 가까운 응답자가 지난 12개월 동안 환경에서 구성 오류로 인한 인시던트를 경험한 것은 놀라운 일이 아닙니다. 거의 3분의 1이 주요 취약점을 발견했으며 또 다른 3분의 1은 런타임 보안 인시던트를 겪었다고 밝혔습니다. 마지막으로, 20%는 감사에 실패했다고 답했습니다.

지난 12개월 동안 컨테이너 및/또는 쿠버네티스와 관련하여 경험한 보안 인시던트 또는 문제는 무엇입니까?



보안은 컨테이너 전략과 관련하여 가장 중요한 고려 사항

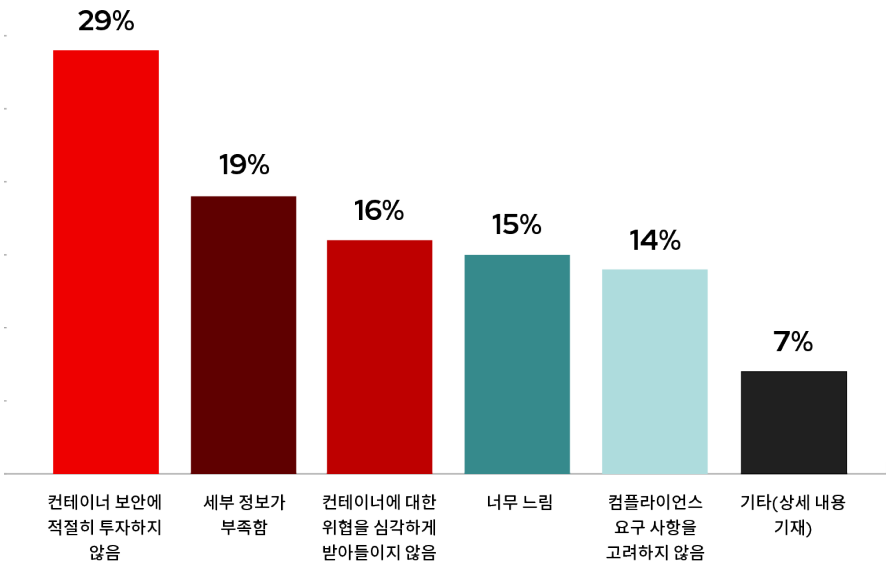
응답자의 59%는 해결되지 않은 보안 및 컴플라이언스 요구 사항 또는 컨테이너에 대한 위협에 대해 가장 크게 우려하고 있습니다.

이러한 환경에서 보안 인시던트가 광범위하게 발생(94%)한다는 사실을 감안할 때 컨테이너 도입과 관련하여 보안이 여전히 최우선 고려 사항이라는 점은 놀라운 일이 아닙니다.

보안에 대한 투자 부족은 응답자 회사의 컨테이너 전략에 대해 가장 많이 언급된 우려 사항입니다(29%). 위협을 심각하게 받아들이지 않고(16%) 컴플라이언스 요구 사항을 고려하지 않을 경우(14%) 응답자의 거의 3분의 2가 보안 및 컴플라이언스를 가장 큰 우려 요인으로 꼽았습니다.

조직은 컨테이너와 쿠버네티스를 적극적으로 도입하고 있습니다. 보안 전략과 툴링에 필요한 투자를 동시에 하지 않으면 크리티컬 애플리케이션의 보안을 위협하고 애플리케이션 롤아웃을 연기해야 할 수도 있습니다.

귀사의 컨테이너 전략에서 가장 큰 우려 사항은 무엇입니까?



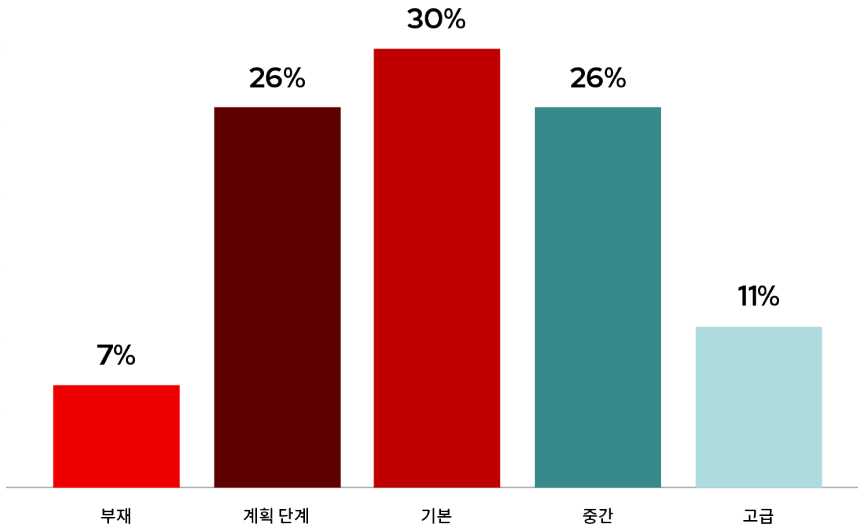
대다수가 컨테이너 보안 전략의 계획 단계를 넘어섬

3분의 1 이상이 중간 또는 고급 보안 전략을 갖추고 있습니다.

컨테이너 도입이 증가함에 따라 조직은 컨테이너 및 쿠버네티스 보안 전략을 계속 발전시키고 있습니다. 기본적인 쿠버네티스 보안 전략을 최소 하나 이상 갖추고 있다고 응답한 비율은 67%입니다. 더 주목할 점은 보안 전략이 전혀 없다고 응답한 비율이 7%에 불과하다는 점입니다.

이 데이터는 유망하지만 컨테이너 전략에 대한 지속적인 보안 우려 사항을 정량화한 이전 결과는 보안 전략이 성숙하고 있는 동안에도 조직이 컨테이너 보안 및 컴플라이언스 요구 사항을 적절히 해결할 수 있도록 더 많은 투자를 해야 한다는 점을 시사합니다.

귀사의 컨테이너 및 쿠버네티스 환경에 대한 보안 전략을 어떻게 설명하시겠습니까?



쿠버네티스 보안에 대한 책임은 고도로 분산되어 있음

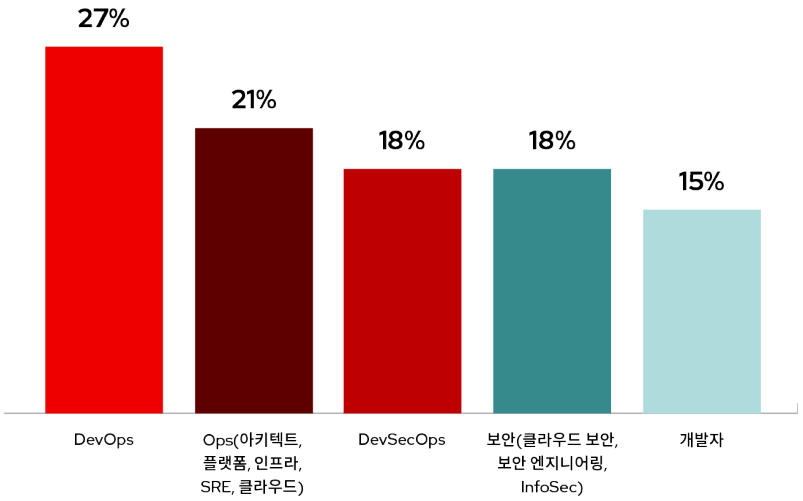
다양한 롤 전반에서 DevOps는 보안을 가장 많이 담당하는 것으로 간주됩니다.

DevOps는 다양한 롤 중에서 컨테이너 및 쿠버네티스 보안을 담당하는 것으로 가장 많이 언급된 단일 롤입니다. 종합하면 응답자 중 무려 66%가 DevOps, Ops, DevSecOps의 수많은 운영 롤을 쿠버네티스 보안의 주요 소유자로 간주합니다.

보안 변화의 필요성을 반영하듯, 응답자의 15%는 개발자들을 쿠버네티스 보안의 주요 소유자로 여기고 있으며 보안 팀을 가장 중요한 책임자로 생각하는 응답자는 18%에 불과했습니다.

이러한 분포는 컨테이너와 쿠버네티스 보안을 실현하기 위해선 많은 노력이 필요하다는 사실을 보여줍니다. 기존에는 보안이 보안 및 컴플라이언스 정책을 적용하는 중앙 제어 지점이었습니다. 컨테이너 및 쿠버네티스 도입은 주로 DevOps에 의해 좌우되는 경우가 많기 때문에 응답자들이 이러한 기술 보안을 담당하는 책임자로 DevOps를 언급하는 것이 놀라운 일은 아닙니다. 이러한 격차를 줄이기 위해 컨테이너 및 쿠버네티스 보안 툴링은 조직에 방해가 될 수 있는 장애 요소를 유지하는 대신 개발자에서 DevOps, 운영, 보안에 이르는 다양한 팀 간의 긴밀한 협업을 촉진해야 합니다.

귀사에서 컨테이너 및 쿠버네티스 보안을 가장 많이 담당하는 롤은 무엇입니까?



대부분의 조직에서 DevSecOps 이니셔티브 추진

응답자 중 단 26%만이 DevOps 및 보안이 분리되어 있다고 답했습니다.

DevSecOps는 더 이상 단순한 유행어가 아니며, 보안을 사후에 고려하는 것이 아니라 애플리케이션 개발 라이프사이클에 구축하는 프로세스와 툴링을 포괄하는 용어입니다. 설문조사 결과, 이 관점에 대해 대부분의 응답자들이 일종의 DevSecOps 이니셔티브를 진행 중이라고 답했습니다. 응답자의 26%만이 보안과 별도로 DevOps를 계속 운영하고 있습니다.

더 주목할만한 점은 응답자의 25%가 DevSecOps 이니셔티브를 통해 전체 라이프사이클에 걸쳐 보안을 통합하고 자동화한다는 점입니다.

귀사에서는 DevSecOps 이니셔티브를 진행하고 있습니까?

- 아니오, DevOps 및 보안은 개별적으로 운영되며 협업은 최소화되어 있습니다.
- 예, 초기 단계에 있으며 DevOps와 보안이 공동 정책을 기반으로 협업합니다.
- 예, 고급 단계에 있으며 보안 통합 및 자동화를 실현하고 있습니다.

구성 오류는 가장 큰 보안 문제를 제기

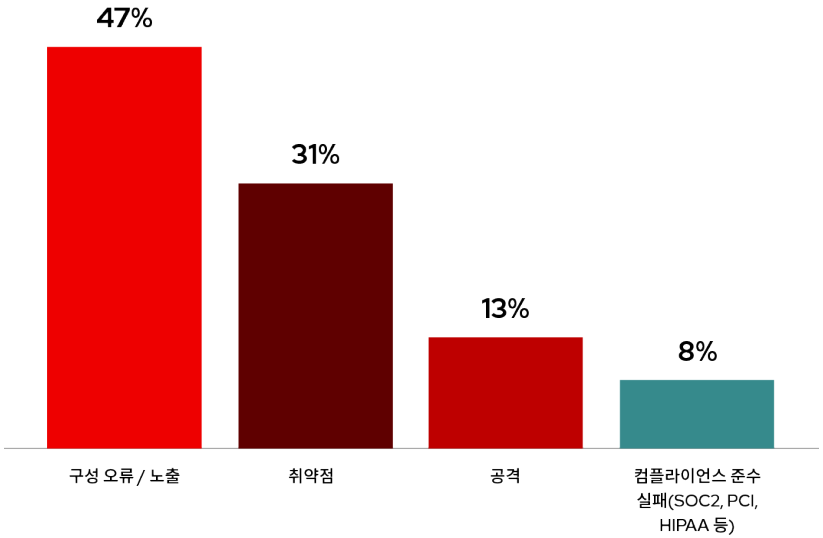
광범위한 구성 오류는 구성 관리 자동화에 대한 필요성을 강조합니다.

설문조사 응답자들은 컨테이너 및 쿠버네티스 환경의 구성 오류로 인한 노출에 대해 가장 크게 우려하고 있습니다(47%). 이는 공격에 대한 우려 수준(13%)의 거의 4배에 달하며, 두 번째 우려 사항으로는 취약점을 꼽았습니다(31%).

구성 관리는 보안 전문가들에게 매우 어려운 과제를 제시합니다. 컨테이너 이미지의 취약성 검사에 사용할 수 있는 툴이 많지만 구성 관리를 위해서는 더 많은 사항을 고려해야 합니다. 사람들은 쿠버네티스 대시보드를 배포해선 안 된다는 사실을 알고있을 수 있지만, 포드의 보안 컨텍스트를 구성하거나 쿠버네티스 롤 기반 접근 제어(RBAC)를 구현하는 것은 팀이 제대로 파악해야 하는 더욱 까다로운 설정의 두 가지 예에 불과합니다.

이 문제를 해결하는 가장 좋은 방법은 구성 관리를 최대한 자동화하여 사람이 아닌 보안 툴을 통해 개발자 및 DevOps 팀이 컨테이너와 쿠버네티스를 안전하게 구성할 수 있도록 지원하는 것입니다.

다음 중 귀사의 컨테이너 및 쿠버네티스 환경에서 가장 염려되는 위험 요소는 무엇입니까?



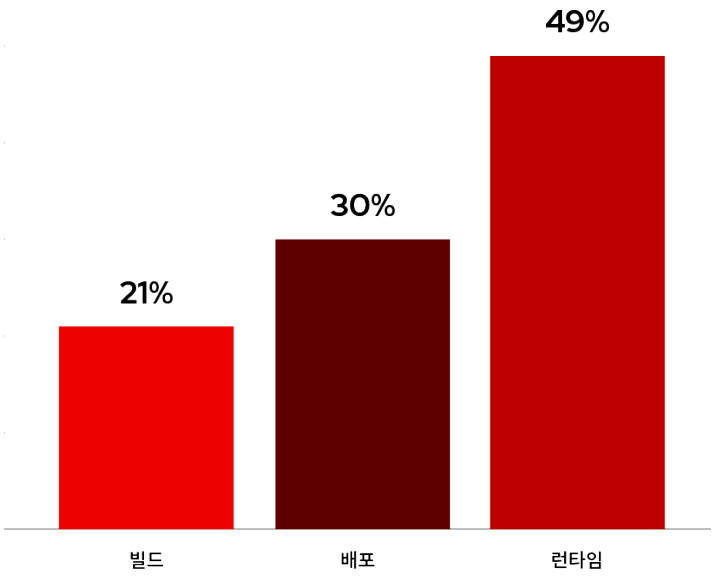
응답자들은 컨테이너 라이프사이클의 런타임 단계에 대해 가장 크게 우려함

거의 절반에 가까운 응답자가 런타임 단계에 대해 가장 걱정하며 런타임 제어의 중요성을 강조하고 있습니다.

런타임은 조직에서 가장 우려하는 컨테이너 라이프사이클 단계입니다. 언뜻 보기에 이 조사 결과는 이전 조사 결과와 반대입니다. 응답자의 압도적인 다수가 구성 오류를 가장 큰 보안 위험의 원인으로 식별하고, 다른 보안 인시던트 유형보다 구성 오류 인시던트를 더 자주 경험했기 때문입니다.

그러나 런타임 보안 문제는 대개 빌드 또는 배포 단계에서 구성 오류와 같은 보안 결함으로 인해 발생한다는 점을 고려하면 이번 조사 결과가 더 큰 의미를 가집니다. 또한 빌드 또는 배포 단계에서 보안 오류가 발생할 경우 애플리케이션이 운영 환경에서 실행될 때에만 부정적인 결과가 나타날 수 있습니다.

보안 측면에서 더욱 우려하고 있는 라이프사이클 단계는 무엇입니까?



하이브리드 클라우드 배포 전략이 가장 일반적

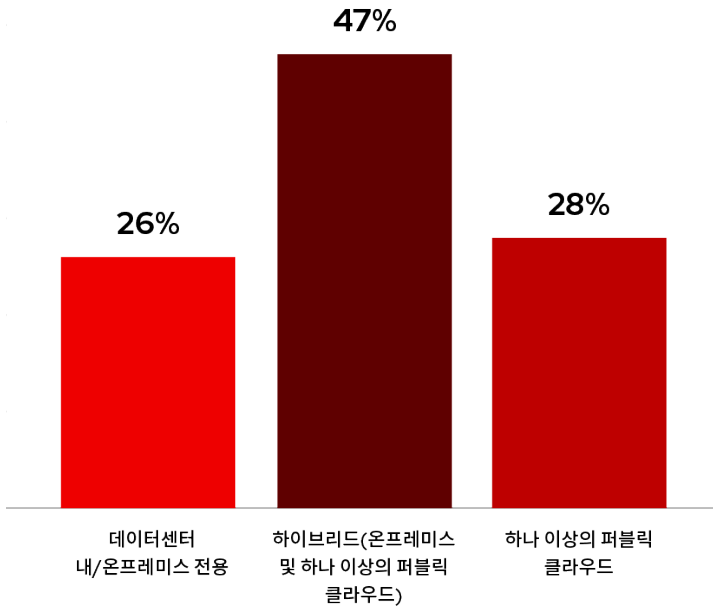
응답자의 47%는 하이브리드 클라우드 모델 전반에 컨테이너를 배포하는 반면 28%는 클라우드 전용 전략을 선택했습니다.

클라우드 전용 전략에 대해 많은 이야기가 있지만 하나 또는 여러 클라우드 제공업체의 실제 배포는 여전히 하이브리드 클라우드 배포보다 뒤처져 있습니다. 응답자의 47%는 컨테이너를 하이브리드 환경에서 실행하는 반면, 28%는 퍼블릭 클라우드에서만 실행합니다.

온프레미스 전용 컨테이너 배포를 격리해도 델타는 여전히 유지되며, 26%는 자체 데이터센터에서만 컨테이너화된 애플리케이션을 실행합니다.

하이브리드 모델이 계속해서 주요 접근 방식으로 사용되기 때문에 조직은 워크로드 배포 위치와 관계없이 동일한 방식으로 실행되는 보안이 필요합니다. 쿠버네티스 네이티브 보안 접근 방식은 온프레미스에서 클라우드 배포에 이르는 환경에 구애받지 않는 제어를 제공할 수 있습니다.

컨테이너를 어디에서 실행하고 있습니까?



하이브리드 클라우드 배포 분야의 리더인 Red Hat OpenShift

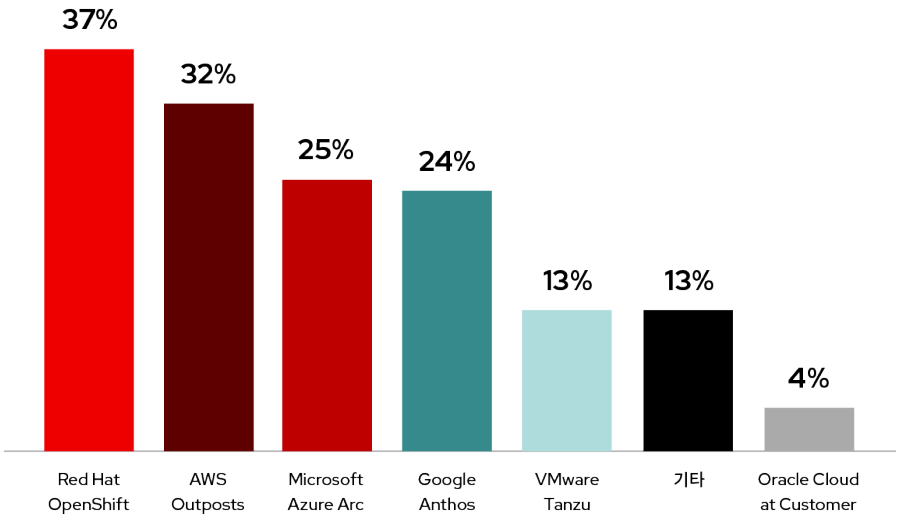
응답자의 37%는 OpenShift를 기반으로 표준화했으며 AWS Outposts 및 Azure Arc가 함께 상위 3위를 차지했습니다.

컨테이너화된 애플리케이션을 실행하는 데 가장 많이 사용되는 모드인 하이브리드 클라우드 배포를 통해 기업이 하이브리드 모드에서 배포하는 방식을 이해하고자 했습니다.

퍼블릭 클라우드 공급업체의 기술이 널리 보급되면서 전반적인 플랫폼 인기도 비슷한 수준으로 상승하고 있습니다. 하지만 설문조사 결과에 따르면 Red Hat® OpenShift®에 비해 뒤처지는 것으로 나타났습니다.

VMware와 Oracle의 하이브리드 오퍼링은 다른 제품들보다 뒤처져 응답자의 13%와 4%가 각각 이 제품을 사용하고 있습니다.

하이브리드 및 멀티클라우드 쿠버네티스 배포를 위한 솔루션을 사용하고 있습니까?



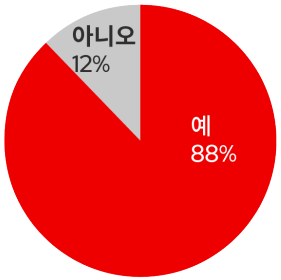
사실상 컨테이너 오케스트레이터 역할을 하는 쿠버네티스는 거의 모든 사람들이 사용

응답자의 88%가 쿠버네티스를 컨테이너 오케스트레이터로 사용하고 있으며 74%가 프로덕션에서 사용하고 있습니다.

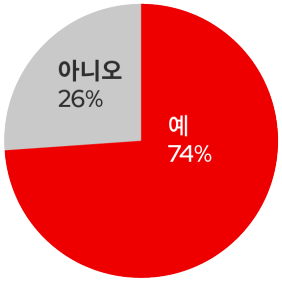
설문조사 결과에 따르면 쿠버네티스의 광범위한 고객 채택률(87%)을 확인할 수 있으며 특히 프로덕션 환경(75%)에서 채택되고 있는 것으로 나타났습니다. 하지만 쿠버네티스의 배포 방식은 계속해서 크게 변화하고 있습니다.

응답자의 51%에 따르면 가장 널리 사용되는 쿠버네티스 플랫폼은 Amazon의 EKS입니다. 다소 놀랍게도 자체 관리되는 쿠버네티스가 두 번째로 가장 많이 선택되는 플랫폼(35%)이며, Red Hat OpenShift가 근소한 차이로 3위(33%)를 차지했습니다. Microsoft의 AKS 및 Google의 GKE가 팽팽히 맞서고 있으며 Azure가 약간의 우위를 점하고 있습니다.

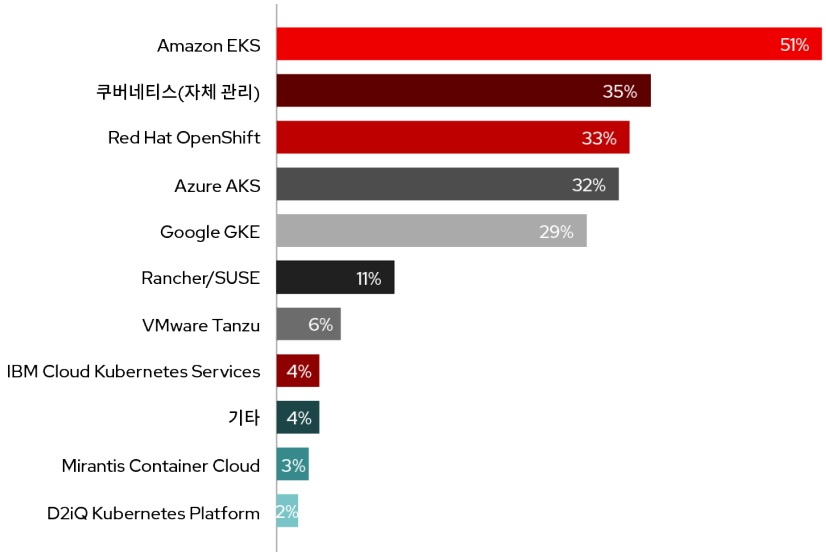
컨테이너 오케스트레이션에 쿠버네티스를 사용하고 있습니까?



쿠버네티스를 사용하는 경우 프로덕션에서 워크로드를 실행하고 있습니까?



컨테이너를 오케스트레이션하기 위해 사용하는 쿠버네티스 플랫폼은 무엇입니까?



응답자들은 기능이 풍부한 보안 솔루션을 필요로 함

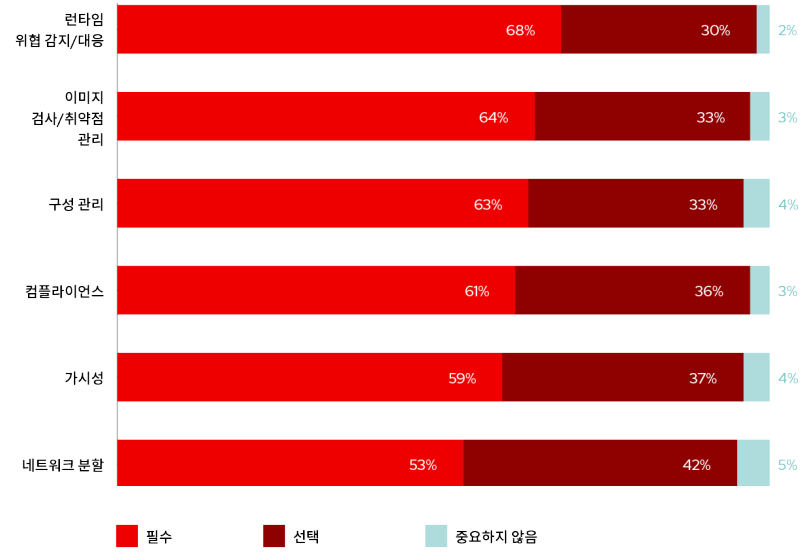
응답자의 68%는 런타임 위협 탐지 및 인시던트 대응을 필수 기능으로 꼽았습니다.

응답자들은 쿠버네티스 보안 플랫폼으로부터 많은 것을 기대하고 있으며, 응답자 중 3분의 2는 네트워크 세분화를 필수 기능으로 꼽았습니다. 이 기능은 DevOps 및 보안 활동을 포괄하며 컨테이너 및 쿠버네티스 보안 플랫폼의 광범위하고 심층적인 기능에 대한 요구를 뒷받침합니다.

또한 쿠버네티스와 컨테이너를 안전하게 보호하기 위해서는 개발, 운영 및 보안 팀의 참여가 필요하다는 사실도 강조합니다.

응답자들은 이미지 검사/취약성 관리(64%) 및 구성 관리(64%)를 반드시 보유해야 하는 3대 보안 기능 중 2가지로 꼽았습니다. 응답자의 절반 이상이 이러한 각 보안 기능이 필수적이라고 답했습니다.

다음 쿠버네티스 보안 기능의 중요성을 어떻게 평가하시겠습니까?



응답자들은 광범위한 오픈소스 보안 툴을 사용

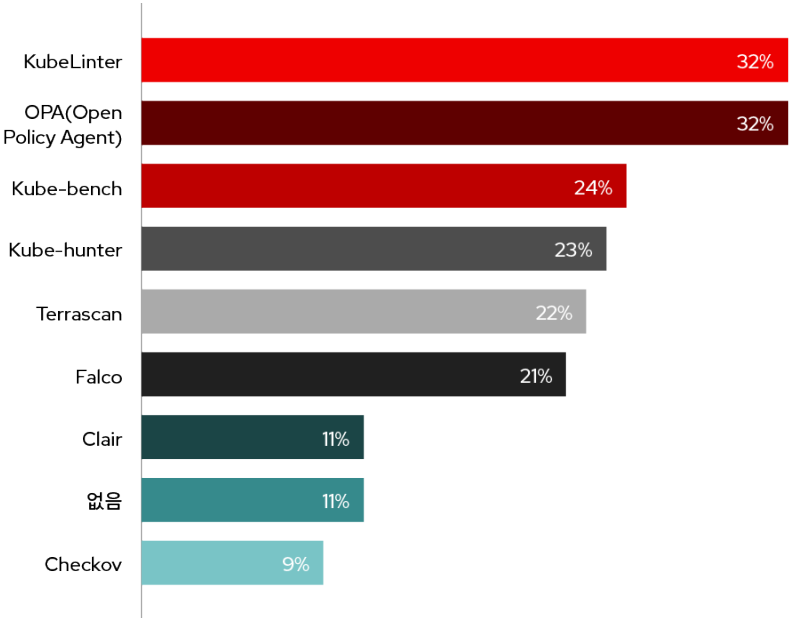
응답자의 20% 이상이 6가지 오픈소스 보안 툴을 사용하고 있으며, KubeLinter 및 OPA가 상위 2개 툴로 꼽힙니다.

쿠버네티스는 무엇보다도 개발 및 DevOps 팀이 컨테이너화된 애플리케이션 개발, 배포 및 관리를 가속화하고 확장하기 위한 툴입니다. Red Hat, Amazon, Microsoft 및 Google과 같은 공급업체는 쿠버네티스의 기본 기능을 향상시키기 위해 보안 기능을 추가했습니다. 동시에 상용 보안 벤더는 고급 활용 사례에 적합한 엔터프라이즈 레디 보안 솔루션을 제공하기 위해 한 단계 더 나아갔습니다.

이와 동시에 쿠버네티스 커뮤니티는 쿠버네티스의 보안 격차를 해소하기 위해 오픈소스 보안 툴을 출시하는 데 매우 적극적으로 참여하고 있습니다. 고객들이 선택할 수 있는 다양한 오픈소스 보안 툴이 있으며, 설문조사 결과에 따르면 쿠버네티스 보안 시장을 지배하는 단일 오픈소스 보안 툴은 없습니다.

KubeLinter 및 OPA는 보안 분야에서 가장 인기 있는 두 OSS이지만 3위를 차지한 Kube-bench(24%)와 6위의 Falco(21%) 간 차이는 3% 포인트에 불과합니다.

쿠버네티스 보안에 사용하는 오픈소스 툴은 무엇입니까?



컨테이너 및 쿠버네티스 보안 여정의 주요 사항

500명 이상의 응답자를 대상으로 실시한 이 설문조사 결과, 조직이 클라우드 네이티브 환경을 안전하게 구축, 배포, 관리하지 않음으로써 애플리케이션 개발 및 릴리스를 가속화할 수 있는 핵심 이점을 놓치고 있다는 사실을 알 수 있었습니다. 조직 전반에 구성 오류와 취약성이 만연함에 따라, 애플리케이션을 프로덕션에 배포하려고 할 때 보안을 "추가"하는 대신 DevOps 워크플로우에 내장하여 제공하도록 전환해야 합니다. 응답자의 절반 이상이 보안 문제로 인해 프로덕션 배포를 미루고 있기 때문에 보안 제어 기능이 부족하면 비즈니스 가속화 및 혁신을 저해할 수 있습니다.

1. 쿠버네티스 네이티브 보안 아키텍처 및 제어 기능 사용

쿠버네티스 네이티브 보안은 쿠버네티스의 풍부한 선언적 데이터 및 기본 제어를 사용하여 몇 가지 주요 보안 이점을 제공합니다. 쿠버네티스에서 사용 가능한 선언적 데이터를 분석하면 구성 관리, 컴플라이언스, 세분화, 쿠버네티스 관련 취약성에 대한 위험 기반 인사이트를 통해 보안을 강화할 수 있습니다. 애플리케이션 개발 및 보안을 위해 동일한 인프라와 해당 제어 기능을 사용하면 학습 곡선이 줄어들고 더 빠른 분석 및 문제 해결이 가능합니다. 또한 쿠버네티스가 인프라로 확장하는 것과 동일한 자동화 및 확장성 이점을 얻도록 하여 운영 충돌을 방지합니다.

2. 빌드/배포에서 런타임에 이르는 전체 라이프사이클 보안 구현

보안은 특히 코드를 빠르게 제공하는 것이 핵심인 개발자와 DevOps 팀에서 오랫동안 비즈니스 저해 요인으로 간주되어 왔습니다. 컨테이너와 쿠버네티스를 사용하면 개발자가 처음부터 자산에 강력한 보안을 구축할 수 있도록 지원함으로써 보안이 비즈니스 액셀러레이터 역할을 해야 합니다. 구성 확인의 일부로 DevOps 모범 사례와 내부 제어 기능을 통합하는 컨테이너와 쿠버네티스 보안 플랫폼을 찾아보세요. 또한 개발자가 기능 제공에 집중할 수 있도록 쿠버네티스 자체 구성의 보안 상태를 평가해야 합니다.

3. 쿠버네티스 환경 전반에 이식성 필요

대부분의 조직에서 온프레미스 및 퍼블릭 클라우드 환경(때로는 멀티클라우드에서) 모두에 컨테이너를 배포하므로 자산이 실행되는 어느 위치에서든 보안이 일관되게 적용되어야 합니다. 공통된 기반은 쿠버네티스이므로 쿠버네티스를 정보 소스(SOT), 실행 지점, 범용 가시성 계층으로 만들어 일관된 보안을 유지할 수 있습니다. 관리형 쿠버네티스 서비스는 조직의 쿠버네티스 도입 능력을 가속화할 수 있지만 클라우드 공급업체별 툴링 및 서비스에 종속되지 않도록 주의해야 합니다.

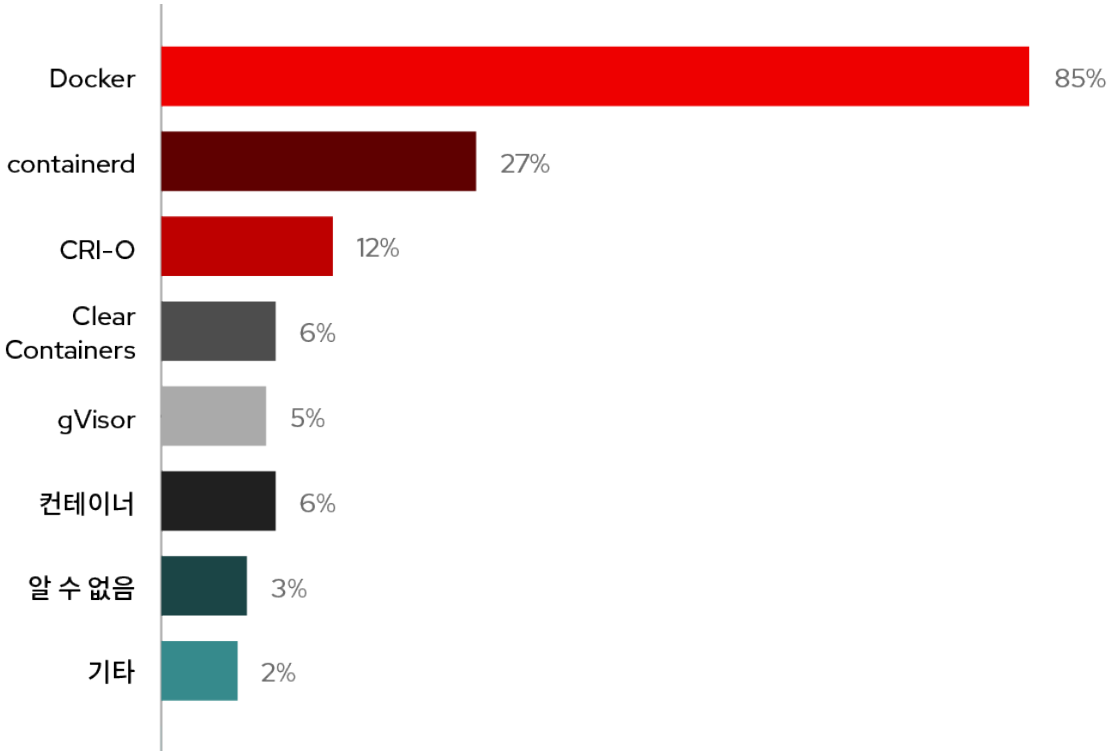
4. DevOps과 보안 연결

대부분의 조직에서 DevOps 또는 보안 팀이 컨테이너 보안 플랫폼을 실행하기를 기대하기 때문에 보안 툴링이 보안과 DevOps를 연결하는 데 도움이 되어야 합니다. 이 플랫폼을 효과적으로 사용하려면 컨테이너화된 쿠버네티스 기반 환경에서 적절한 보안 제어를 구축해야 합니다. 또한 위험을 적절히 평가해야 합니다. 개발자에게 CVSS 점수가 7 이상인 발견된 취약점 39개를 모두 수정하도록 지시하는 것은 비효율적입니다. 담당 개발자에 대해 해당 취약점에 노출된 세 가지 배포를 식별하고 이러한 배포가 위험한 이유를 제시하면 보안 상태를 진정으로 개선할 수 있는 조치를 취할 수 있습니다.

응답자 정보 – 컨테이너 런타임 기술

Docker 런타임 엔진은 여전히 우세를 유지하고 containerd가 큰 차이로 2위를 차지했습니다.

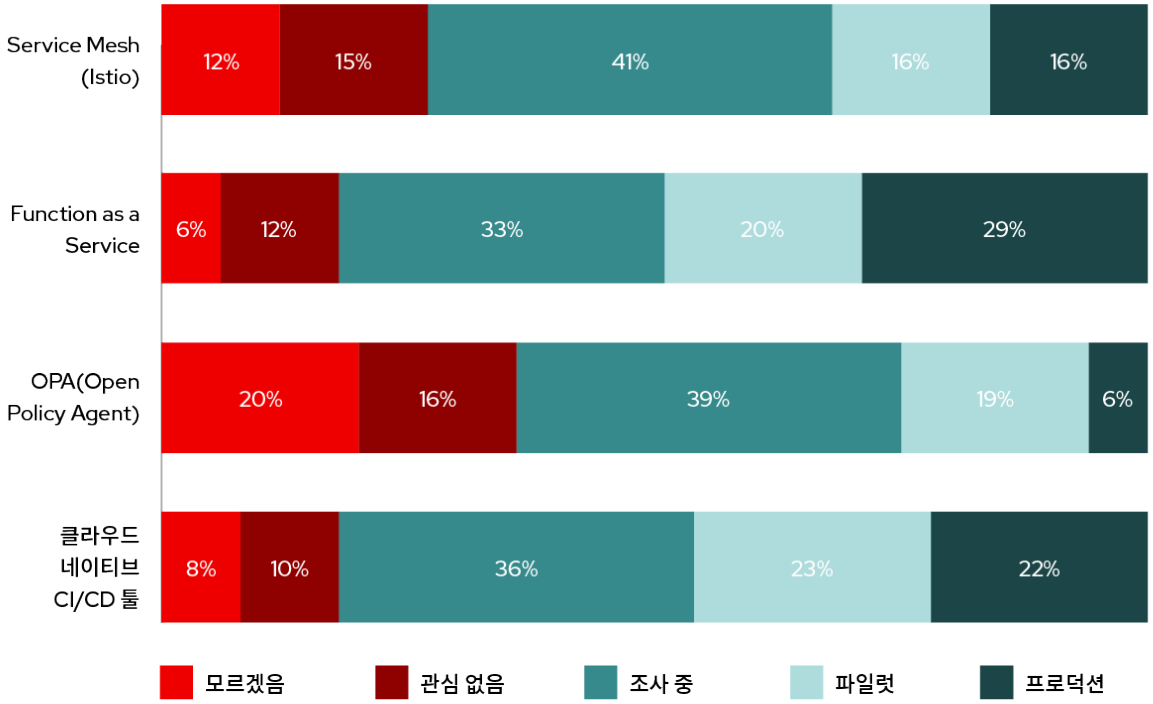
어떤 컨테이너 런타임을 사용합니까?



응답자 정보 - 기타 클라우드 네이티브 기술

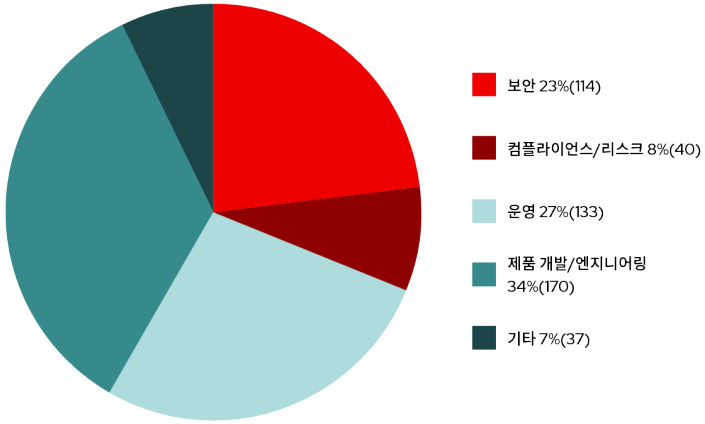
이머징 클라우드 네이티브 기술은 여전히 초기 도입 단계에 있습니다. 파일럿 또는 프로덕션 환경에서 서비스로서의 기능(FaaS) 및 클라우드 네이티브 CI/CD 툴만 상당 수준 사용되고 있습니다.

고려 중이거나 사용 중인 기타 클라우드 네이티브 기술은 무엇입니까?

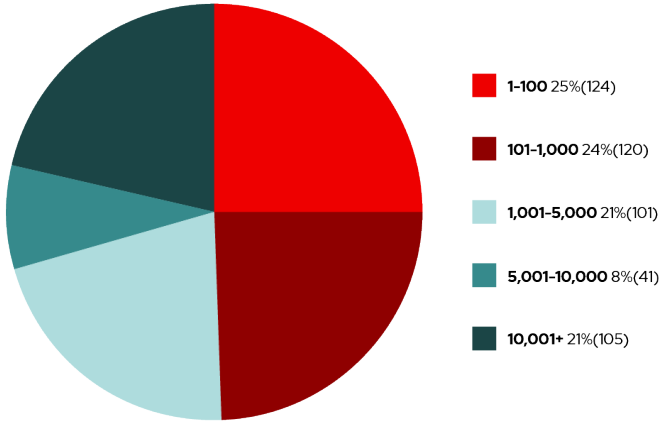


응답자 정보 – 핵심 인구 구성

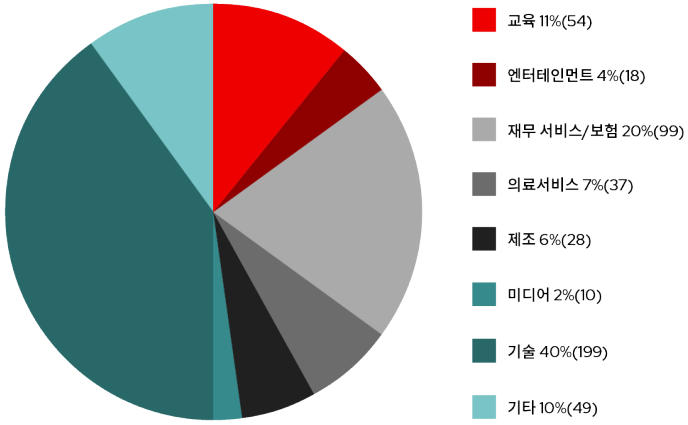
귀하의 직무 영역은 무엇입니까?



귀사의 규모는 어떻게 됩니까?



어떤 산업에 종사하십니까?



Red Hat Advanced Cluster Security for Kubernetes에 대해 자세히 알아보기

Red Hat Advanced Cluster Security for Kubernetes는 컨테이너 여정을 진행하면서 구축, 배포, 런타임 전반에 걸쳐 애플리케이션을 보호하는 쿠버네티스 네이티브 컨테이너 보안 플랫폼입니다. 환경이 더욱 복잡해지고 자동화에 대한 의존도가 높아짐에 따라 Red Hat 플랫폼은 보다 정교한 환경에서 보안을 운영하면서 DevOps의 속도에 보조를 맞출 수 있도록 지원합니다.

쿠버네티스 네이티브 보안은 다음과 같은 중요한 이점을 제공합니다.

- **운영 리스크 최소화:** 쿠버네티스 네이티브 제어를 사용하여 위협을 완화하고 애플리케이션에 대한 운영상의 리스크를 최소화하는 보안 정책을 실행하여 DevOps에 맞게 보안을 조정합니다.
- **운영 비용 절감:** 공통 정보 소스(SOT)를 사용하여 시간, 노력 및 직원에 대한 전반적인 투자를 줄이고 보안 분석, 조사 및 문제 해결을 간소화합니다.
- **DevOps 생산성 가속화:** 개발자 속도를 지원하는 기존 워크플로우 및 툴링에 포함된 실행 가능하고 컨텍스트가 풍부한 가드레일을 개발자에게 제공하여 혁신 속도를 가속화합니다.

Red Hat Advanced Cluster Security for Kubernetes의 실제를 확인해 볼 준비가 되셨습니까? 비즈니스 및 요구 사항에 맞는 맞춤형 데모를 사용해 보세요.

데모 요청