O'REILLY®
Report

Redefining OS Selection

경쟁력 확보를 위한 획기적인 Linux 전략 변화

Ned Bellavance 및 Chris Hayner

Red Hat Enterprise Linux

경쟁 우위의 기반이 되는 OS 선택

현대적인 플랫폼으로 신속한 혁신을 추진하세요. 변화하는 요구에 대응하여 Red Hat Enterprise Linux이 민첩성 및 제어를 구현하는 방법을 알아보세요.

자세히 알아보기

Redefining OS Selection

경쟁력 확보를 위한 획기적인 Linux 전략 변화

Ned Bellavance 및 Chris Hayner

O'REILLY®

Redefining OS Selection
저자: Ned Bellavance 및 Chris Hayner

O'Reilly Media, Inc. 발행(141 Stony Circle, Suite 195, Santa Rosa, CA 95401)

O'Reilly 서적은 교육, 비즈니스 또는 영업 프로모션 용도로 구매할 수 있습니다. 온라인 버전으로도 대부분의 타이틀을 구할 수 있습니다(*http://oreilly.com*). 자세한 내용은 800-998-9938 또는 *corporate@oreilly.com*으로 기업/기관 영업 부서에 문의해 주세요.

기획 편집자: Megan Laddusaw
개발 편집자: Gary O'Brien
프로덕션 편집자: Jonathon Owen
교정 편집자: Stephanie English
표지 디자이너: Ellie Volckhausen
본문 디자이너: David Futato
본문 삽화가: Kate Dullea

2026년 2월: 초판

초판의 개정 이력
2026년 2월 13일: 최초 발행

979-8-341-66786-0

[LSI]

목차

소개

역사적으로 조직은 운영 체제(OS) 배포 전략을 변경하는 데 미온적이었습니다. 기업은 간단한 기술 요구 사항 및 기본 설정에 기반하여 운영되며 절대적으로 필요한 경우에만 여러 OS를 실행합니다. OS 변경은 중요한 애플리케이션의 기술 요구 사항 또는 OS 지원 종료에 따른 강제 업그레이드로 인해 이루어집니다. 이에 따라 조직은 OS 선택은 해결된 논제라고 생각합니다. 즉, 다른 무엇보다 기술적 필요성에 따라 선택한다는 것이죠. 실상은, 최신 글로벌 기술 환경의 급속한 발전에 따라 OS 선택은 전략적 선결 과제가 되고 있습니다.

요즘 기업들은 이전 경험을 크게 뛰어넘는 변화를 놓고 고심하고 있습니다. 최근 몇 년에 걸쳐 컨테이너화 같은 기술이 워크플로우 유연성을 높이고, 애플리케이션 배포 툴셋 및 전략이 획기적으로 바뀌었으며, AI 및 양자 컴퓨팅 같은 기술이 이전에 이해되던 것을 모두 완전히 뒤엎어 놓았습니다. 기업은 기술 요구 사항을 재평가하는 과정에서 OS 선택 전략도 이러한 격변의 시기에 부합하게 조정해야 합니다.

이 리포트는 이러한 새로운 전략적 선결 과제의 동인을 살펴봅니다. 설문조사 및 애널리스트 리포트를 포함한 실증적 연구를 활용하여 현대의 IT 조직이 직면한 구체적인 과제를 파악합니다. 살펴보겠지만, 이러한 변화에는 매우 현대적인 다양한 전략적 트리거가 작용합니다. 새로운 애플리케이션, 하드웨어, 플랫폼은 모두 혁신 가속화를 따라잡는 방향으로 궤를 같이합니다. 혁신 외에도 조직은 불확실한 경제 상황, 정교한 최신 사이버 보안 위협, 데이터 주권 및 공급망 검증과 같은 지정학적 우려에 대처해야 합니다.

이 리포트에서는 기업이 OS 선택을 운영상 필요성의 개념에서 전략적 경쟁 우위 확보의 개념으로 다시 정의하고 있는 방법을 보여 드립니다.

1장

OS 선택의 전략적 변화

최신 IT 환경에 따라 발생한 요구 사항은 엔터프라이즈 OS 인프라 및 애플리케이션 배포 전략에 근본적인 주요 변화를 이끕니다. 변경 없고 검사를 거치지 않는 전통적인 OS 에코시스템의 이점(간소한 관리 및 배포, 낮은 교육 필요성)은 이제 최신 발전 속도를 고려했을 때 마냥 좋다고만은 할 수 없습니다. 조직은 경직된 OS 기본 설정이 강점이기보다는 부담이며 유연성 및 빠른 역량 성장이 현재 상태를 유지하는 것보다 더 중요하다는 것을 느끼고 있습니다. 이러한 추세를 고려하지 않는 기업은 잘 준비되었고 유연성을 발휘할 수 있는 경쟁업체에 뒤처질 리스크가 있습니다. 빠르게 변화하는 기술 환경에 더해, 조달 의사 결정에 직접적인 영향을 미치는 지정학적 요인으로 인해 상황이 더 복잡해집니다.

주요 주제 및 변경 사항

현재 기업 내의 OS 선택 의사 결정의 동인이 되는 몇 가지 주제가 있습니다. 이들 주제는 서로 분리된 트렌드가 아니라 상호 연계되어 조직의 인프라 전략 접근 방식을 재편하는 동력으로 작용합니다. 각각에 대해 이 리포트 뒷부분에서 더 자세히 알아보겠습니다.

*혁신 가속화*는 OS 선택 의사 결정에서 지배적인 요인입니다. 간단히 말하자면 AI, 자동화, 엣지 및 클라우드 컴퓨팅, IoT, 새로운 사용자 정의 하드웨어가 발전하는 속도가 너무 빨라서 일부만 이를 따라잡을 수 있습니다. 기업은 기술이 그 어느

때보다 빠르게 발전함에 딸라 기술 부채를 우려하고 있습니다. 새로운 기술이 프로덕션 레디니스(readiness)에 도달하기까지 전에는 수년이 필요했지만, 이제는 몇 개월이면 아이디어가 배포로 구현됩니다. 바로 이것이 기업의 경쟁력을 뒷받침할 OS를 조사하게 되는 주요 동인입니다.

공급망과 관련한 *글로벌 불확실성*이 수년간 증가해 왔으며, 기업들은 로컬 환경을 넘어 운영 기반 툴, 소프트웨어, 서비스를 제공하는 공급망 전반을 살피게 되었습니다. 많은 기업이 공급망 차질의 가능성이 있는 경우 특히 해외 기업과의 단일 벤더 관계를 잠재적 리스크로 꼽았습니다. 이러한 고려 사항으로 인해 벤더 다변화는 리스크 완화 방법이자 전략적 선결 과제가 되었습니다.

*경제적 압박*이 심화되어 최적화 및 ROI(투자수익률)에 중점을 두게 되었습니다. ROI는 재무적 사안에 그치지 않습니다. 기술 인력 부족은 예산 제약 못지않게 우려되는 문제로, OS 선택을 복잡하게 만듭니다. 과거에는 관리자 한 명이 다수의 OS의 전문가가 되는 일이 거의 없었습니다. 기업이 고급 전문가 여럿을 정규 직원으로 두는 것은 현실성이 없었고, 이런 이유로 단일 OS 환경을 갖추는 것이 기본이었습니다. 따라서, 실제 입증 가능한 OS 사용 편의성이 우선순위입니다.

이제는 *보안 고려 사항*이 인프라 요구 사항을 새롭게 정의했습니다. 예전보다 배포 속도가 높은 시스템이 많아짐에 따라 기업의 공격 노출 영역도 크게 늘고 있습니다. 이뿐만 아니라 AI 구현, 최신 사이버 위협, 규제 컴플라이언스 등의 새로운 환경은 현대적인 접근 방식을 요구합니다.

마지막으로, *AI*는 기존에 알고 있던 방식의 컴퓨터를 활용한 작업을 송두리째 바꿔 놓았습니다. 관리자나 개발자는 대규모 언어 모델(LLM)을 활용하여 전례 없는 속도로 신규 애플리케이션을 만들 수 있습니다. LLM에 연결해 단순히 질문을 하든, 자체 챗봇을 생성하든, 정교한 에이전틱(Agentic) AI 툴을 구축하든 어떤 경우에도 작업에 가장 적합한 OS가 필요합니다.

OS 선택의 중요성

지금까지 알아본 대로, OS 선택에는 그 어느 때보다 많은 노력이 들어갑니다. OS를 잘못 선택하면 중요 AI 기능 액세스가 제한되거나, 성능이 저해되거나, 조직이 보안 리스크 또는 공급망 취약성에 노출될 수 있습니다. 반대로, 적절한 OS를 선택하면 빠르게 변화하고 생산적인 이 최신 환경으로 발돋움하기 용이합니다. 신중하고 전략적으로 OS를 선택하면 경쟁 우위와 디지털 유연성을 확보할 수 있습니다. 경쟁 우위와 디지털 유연성은 새로운 기술 기회를 활용하려는 기업에게 매우 중요한 요소입니다.

각 선택 요인을 더 자세히 살펴보겠습니다.

혁신 가속화

맹렬한 발전 속도는 인프라 의사 결정을 둘러싼 표준 모델을 근본적으로 바꿨습니다. 이 섹션에서는 이러한 가속화 요인 및 이에 따른 기업의 배포 전략 접근 방식 변화를 살펴봅니다.

빨라진 기술 주기

2025년 McKinsey Technology Trends Outlook 리포트는 "글로벌 기술 환경이 신속한 기술 혁신에 의해 중대한 변화를 겪고 있다."라고 논합니다.[1] 간단히 말하자면 기술 발전은 전례 없는 속도로 이루어지고 있으며, 이 속도는 더욱 높아질 것입니다. 클라우드 도입 속도를 예로 들겠습니다. 대다수의 경우 기업들은 천천히 시작했습니다. 다시 말해, 먼저 클라우드에 개발/검증 환경을 배포한 후에 수년에 걸쳐 점차적으로 전체 프로덕션 워크로드에 적용하는 식입니다. 그런 다음, 생성형 AI나 에이전틱(Agentic) AI를 고려하며, 몇 개월 만에 사고 실험에서 엔터프라이즈 제품으로 구현됐습니다.

---

[1] McKinsey & Company, "McKinsey Technology Trends Outlook 2025," 2025년 7월 22일 *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top- trends-in-tech*.

전통적인 인프라 전략에서는 기업이 기존 OS를 활용하면서 해당 OS 내에서 신규 기술이 작동하도록 만드는 방법을 찾습니다. 최신 글로벌 시장에서 확인되는 속도는 너무 빨라서, 이러한 전통적인 방식은 현실성이 없습니다. 점점 더 많은 개발 팀이 새로운 플랫폼을 실험하면서 오래된 인프라를 끼워 넣어 작동시키는 것이 아니라 최신 기술과 가장 잘 연동하는 플랫폼을 찾고 있습니다. 이런 추세는 OS 실험의 강력한 동인입니다. 개발자와 엔지니어는 기존 OS가 원하는 역량을 발휘하지 못한다고 판단하면 대체 OS를 찾기 시작합니다.

타겟팅 투자

OS 검토와 변경은 다른 무엇보다 신규 기술이 그 동인이 됩니다. 앞에서 추세를 설명한 그대로입니다. 즉, 개발자와 관리자가 익숙한 사내 기존 인프라를 고수하지 않고 동종 최고의 인프라를 찾고 있습니다. 그렇다고 해서 조직들이 리소스를 무제한으로 투입하지는 않습니다. 한정된 자금을 올바른 방식으로 써서 첫 시도에 제대로 하려는 의지가 강합니다. OS 선택은 단순히 서버 한 대와 관련된 의사 결정을 넘어섭니다. 훨씬 더 큰 플랫폼의 일부이므로, 투자 결정이 더욱 중요해집니다.

이러한 투자는 비즈니스 요구 사항을 충족하는 방향으로 이루어집니다. 기술이 진보하면 조직은 그 발전에 발맞춰야 합니다. 예를 들어 조직들은 AI 기능이 작동하려면 특화된 인프라 및 개발 툴이 필요하며 기존의 표준 OS가 태스크를 처리할 수 없음을 인식하고 있습니다. 기업은 AI 툴링의 요구 사항에 부합하기 위해서만으로도 거대한 GPU 기반 서버 팜을 구축해야 했습니다. 미래 지향적인 조직은 혁신의 속도를 인지하고 잠재력을 극대화하는 방향으로 인프라 전략을 조정하고 있습니다. 기업은 기술을 배포해 두고 최상의 성과를 바라는 것이 아니라 자신감 있게 기술 가치의 최대치를 포착할 수 있을 정도로 빠르게 발전하고자 합니다.

글로벌 불확실성

글로벌 불확실성은 기술 전략의 하나의 요인으로 부상했습니다. 경제적 우려를 낳는 지정학적 긴장이 의사 결정에 미치는 영향은 지난 수년에 비해 요즈음 더 커졌습니다. 따라서, 조직들은 기술 공백에서 기존 벤더만 바라볼 수 없게 되었고 이제 지정학적 요소를 고려하여 선택을 평가해야 합니다. 이러한 불확실성에 대해 우려하는 정도는 그 어느 때보다 큽니다.[2] 관세와 규제뿐만 아니라 수출 통제도 걱정해야 합니다. 이러한 지정학적 긴장은 지속적이고 불확실하므로 글로벌 공급망에 위협이 되며, 따라서 기업은 기술 에코시스템을 국경 내에 유지하려는 경향이 생깁니다.

관세 및 수출 통제

관세 고려 사항 및 그에 따른 잠재적 환율 변동은 기업이 국경을 뛰어넘는 거래를 바라보는 시각을 바꾸고 있습니다. 장기 계약의 경우, 변동성이 발생하여 국가 간 통화 역학이 달라지면 계약 체결 1년 만에도 상황이 크게 바뀔 수 있습니다. 이는 현재 IT 전략에 총체적으로 영향을 주고 있는 중요한 문제입니다. 벤더 선택 시 이러한 경제적 측면을 함께 고려하는 것은 이전의 IT 구매 의사 결정과 크게 달라진 개념입니다.

디지털 주권

지정학적 압력은 경제에 국한되지 않고 확장됩니다. 국가별로 규정 요구 사항이 다르며 이에 따라 고객과 벤더 사이의 다이나믹이 달라집니다. 이를 가장 명확히 확인할 수 있는 부분이 클라우드 컴퓨팅입니다. 클라우드 컴퓨팅 분야에서 기업들은 일반 데이터 보호 규정(General Data Protection Regulation, GDPR) 같은 규제 요건에 따라 데이터를 EU 역내에 유지하는 'EU 전용' 클라우드를 강력하게 요구합니다. 이런 움직임은 수년에 걸친 논쟁 끝에 많은 기업이 특정한 규정 요구 사항에 더 유리한 클라우드 벤더를 적극적으로 찾아 나서면서 생겼습니다.

---

[2] McKinsey & Company, "Navigating the New Geopolitical Uncertainty," 2025년 1월 16일 *https://www.mckinsey.com/capabilities/geopolitics/our-insights/navigating-the-new-geopolitical-uncertainty*.

경제적 불확실성

경제적 압박은 항상 IT에 영향을 줬습니다. 변화의 속도에 글로벌 정세가 주는 압력까지 결합하여 상황이 더 복잡해지고 있습니다. 지출할 자금은 한정적이고 기술 인력도 부족합니다. 경우에 따라서는 새로운 관리자 포지션에 지출할 자금을 확보해도 관리자로 일할 직원이 없을 수도 있습니다.

예산 제약에 따라 비용 최적화는 OS 선택에서 주요 요인이 되었습니다. 기업은 ROI 및 효율적인 지출에 점점 중점을 두고 있습니다. 비용 최적화 위주의 전략은 재정적 지출과 ROI(투자 수익률)의 시각에서 OS 선택을 고려합니다.

보안 및 데이터 침해

IT 자산 보안은 수년 동안 주요 고려 사항이었습니다. Stack Overflow의 2025 Developer Survey 같은 설문조사에서는 개발자가 가장 염두에 두는 측면이 보안, 취약점 분석, 검증이라는 것을 명확히 보여줍니다. 개발자가 특정 기술을 사용 중단한 첫 번째 이유로 '보안 및 개인정보 보호 고려 사항'이 꼽혔습니다.

공급망 공격

소프트웨어의 원산지를 아는 것은 전체의 일부일 뿐입니다. 점차 기업들은 해당 소프트웨어의 디펜던시에 대해서도 출처를 알아야 합니다. 이런 상황은 그 자체로 보안 문제가 될 수 있습니다. 주요 소프트웨어 오퍼링에 필수적인 사소한 패키지의 보안이 침해된다면 조직 전체가 리스크에 노출됩니다. 아마도 가장 많이 언급되는 사례는 2021년 SolarWinds 해킹일 것입니다. 당시 보안이 부실한 SolarWinds 공급망으로 인해 수많은 SolarWinds 고객이 데이터 침해를 당했습니다. 디펜던시 문제는 여전히 만연해 있습니다. 최근, JavaScript 레지스트리인 npm이 공급망 공격을 당해, 사용자 장치에 안전하게 배포할 수 있다고 여겨진 패키지가 암호 화폐 채굴에 사용되었습니다.

AI는 보안 리스크인 동시에 생산성과 비즈니스 기능에 유용한 것으로 입증되었습니다. AI 기반 공격은 지난 수년 동안 폭증했으며 줄어들 기미가 보이지 않습니다. 신용 정보 회사인 Experian의 최근 리포트에 따르면 AI는 2026년에는 인적 오류를 추월해 데이터 침해 원인 1위가 될 정도로 심각한 위협입니다.[3]

양자 암호화 고려 사항

양자 컴퓨팅으로 인한 새로운 위협이 지난 몇 년 동안 파악되었고 그에 대한 연구도 이루어졌습니다. 기존 암호화의 문제에 관해 양자 컴퓨터가 취하는 접근 방식이 완전히 다르기 때문에 결국에는(10년 이내일 가능성이 높지만 이 시기에 관해서는 논란이 있음) 기존의 모든 암호화 알고리즘이 몇 초 안에 깨질 것이라고 합니다. 이렇게 되면 '고전적인 방식으로' 암호화한 모든 파일 및 데이터 저장소가 완전히 취약해집니다. 해커는 이 특징을 알고 지금은 암호화를 해독할 수 없지만 최대한 많은 데이터를 다운로드하고 있습니다. 이 보안 리스크를 '선수집 후해독'이라고 합니다.

PQC(포스트 양자 암호화, Post-Quantum Cryptography)는 양자 컴퓨터의 위력에 저항하는 암호화를 의미합니다. 이 유형의 암호화는 컴퓨터 사이언스 분야에 새롭게 등장하는 연구 토픽으로, 아직 일부 OS만 이 암호화를 활용하고 있습니다. PQC 알고리즘을 활용한 암호화 기술은 해커가 선수집 후해독에 성공하지 못하도록 만듭니다.

AI

AI는 많은 기술 구매 의사 결정의 지배적인 동력으로 부상했습니다. 이 추세는 한동안 명확히 존재해 왔으며, 그 모멘텀은 줄어들지 않을 것으로 보입니다. 특히 AI는 점점 더 OS 선택의 동인으로 작용하고 있으며, AI를 둘러싼 기술도 마찬가지입니다.

---

[3] Experian, 2026 Data Breach Industry Forecast, 2025년 12월 5일, *https://www.experian.com/thought-leadership/business/2026-data-breach-industry-forecast-report*.

바이브 코딩

AI 덕분에 OS의 최신 활용 사례가 바뀌었습니다. 이제 전문성이나 기술적 배경이 없는 사람도 프로그래밍, 데이터 분석, 비즈니스 분석을 활용할 수 있게 되었습니다. 한 가지 예로, 바이브 코딩이 있습니다. 바이브 코딩은 직업이 프로그래머나 애플리케이션 개발자가 아닌 사용자도 애플리케이션을 만들 수 있는 AI 기반 기술입니다. 이런 방식을 가능하게 하는 AI 지원 개발 툴과 연동하는 OS에 대한 시장의 선호는 점점 높아지고 있습니다.

하드웨어 가속

이외에, AI는 여전히 포괄적인 OS 기능을 요구하는 전통적인 활용 사례가 있습니다. 추론, 모델 학습 또는 LLM 기반 챗봇 호스팅과 같은 태스크를 수행하려면 OS가 GPU 및 다른 사용자 정의 하드웨어와 효과적으로 상호작용해야 합니다. 특수 칩은 더 빠르고 더 규모가 크며 더 다양한 용도의 AI 기능을 지원하므로, 하드웨어 호환성은 중요한 선택 요인이 됩니다. AI 기반 자동화 및 관리 기능은 OS가 사용할 수 있는 하드웨어 리소스에 지속적으로 부담을 줍니다. 결과적으로, OS가 고급 하드웨어와 상호작용하는 능력은 OS 선택에 영향을 미칩니다.

결론

시장 교란은 조직들이 OS 선택을 평가하게 만들어 새로운 가능성을 모색하는 전략적 기회가 됩니다. 조직들은 이러한 세계적인 혼란과 폭발적인 혁신이 예고하는 전례 없는 기회를 인식하고 있습니다. 지금의 변화를 따라잡을 수 없는 기존 플랫폼을 고수하는 대신, 점점 더 선제적으로 새로운 기회를 탐색하고 있습니다. OS 선택이 이렇게 부담이 아닌 기회로 변모함에 따라 비즈니스 운영 향상을 위한 가장 중요한 기회가 마련되었습니다. 단순히 늘 해 오던 방식으로 처리하지 않고, 격렬한 변화 속에서 작업에 가장 적합한 툴을 찾고 있습니다.

2장

문제부터 해결책까지

1장에서는 OS 선택의 동인이 되는 중요한 요인으로 혁신 가속화, 글로벌 불확실성, 경제적 압박, 보안 고려 사항, AI의 요구 사항을 알아봤습니다. 그러나 IT 분야에서는 최근에서야 이러한 압력을 인식하기 시작했습니다. IT 리더가 직면한 과제는 어떻게 하면 운영상의 새로운 혼란이나 취약점을 낳지 않으면서 이러한 압력에 효율적으로 대응하는가입니다. 이러한 문제를 인식하고 생산적이고 경쟁력 있는 방식으로 대응하는 조직은 성공할 것입니다. 이 장에서는 이러한 과제를 하나씩 살펴보고 문제를 해결하는 방법을 논하겠습니다.

가속화된 혁신 전략

혁신 가속화는 IT 리더에게 원동력이 되어 왔습니다. 단지 경쟁에서 뒤처지지 않으려는 필요에 의해서만이 아닙니다. 선점 우위, 즉 가장 빨리 대응한 조직이 가장 큰 보상을 획득할 수 있다는 개념 덕분입니다. 이런 개념은 OS 선택 전략에서 중요한 의미를 가집니다. OS는 조직이 획득하려는 가속화된 혁신의 기반이 되기 때문입니다. 이런 종류의 혁신을 겪으며 기업은 길을 잃을 수도 있습니다. 따라서 신중한 태도로 식별 가능한 요구 사항과 이익을 기준으로 의사 결정을 내리는 것이 중요합니다. 혁신 가속화는 기분에 따라 즉흥적으로 변경한다는 의미가 아닙니다. 현대적인 OS는 실험이 가능한 동시에 보안, 성능, 신뢰성을 제공해야 합니다.

신속한 구상 실험

기술 혁신 가속화로 인해 전통적인 개발 및 평가 방식으로 따라잡을 수 없는 시장 상황이 되었습니다. 애플리케이션 개발 측면에서 이러한 추세는 한동안 존재해 왔으며, 워터폴 방식 연간 출시 주기에서 애자일 기반 소프트웨어 개발 방식 및 DevOps 기반의 지속적 제공(CD) 방식으로, 그리고 오늘날에는 하루에도 여러 번 업데이트가 이루어지는 초고속 배포 모델로 전환되었습니다. 이러한 추세는 기술 환경 전반에서 관찰됩니다. IT 리더는 앞서가기 위해서는 개발 부문의 방식을 그대로 따라야 함을 인식하고 있습니다.

이 정도의 속도로 혁신하려면 개발 및 검증 주기가 빠르면서도 비즈니스에 리스크를 일으키지 않는 보안 기준을 유지해야 합니다. 효과적인 실험을 수행하려면 회사 데이터(또는 애플리케이션을 호스팅하는 OS)에 리스크를 일으키지 않으면서 프로덕션과 비슷한 조건을 제공하는 정교한 샌드박스 환경이 필요합니다. 이 방법은 실제 프로덕션 조건에서 신속하게 성능을 평가하는 데 사용할 수 있는 현실적인 검증 환경을 제공하기에 가장 효율적입니다.

비슷한 맥락에서, 애플리케이션도 검증에서 프로덕션에 이르는 신속하고 안정적인 경로가 필요합니다. 원활한 프로세스를 통해, 검증 단계에 검증된 애플리케이션이 프로덕션에서 안정적으로 작동하도록 보장해야 합니다. 단순히 편의성의 문제가 아닙니다. 신뢰성 및 반복 가능성은 업그레이드가 최초 테스트 배포만큼 효율적이고 안전하게 이루어진다는 것을 의미합니다.

이런 의미를 고려하면, OS 선택 프로세스에서 신중하고 개방적인 관점을 유지하는 것은 명백한 가치가 있습니다. 혁신이 가속화되는 시기에 애자일해지는 것은 명백한 전략적 이익입니다. OS는 궁극적으로 해당 애플리케이션을 호스팅하며, 애플리케이션 요구 사항이 매우 빠르게 변하기 때문에 조직은 OS가 이러한 변화에 제대로 대처하는지 알아야 합니다. 이러한 미묘한 접근 방식은 IDC 및 McKinsey 같은 기업의 연구와 분석에서 입증되었습니다. 2024년 6월, McKinsey는 "모든 상황에 적합한 만능 접근 방식은 없다는 것이 진실입니다. 대신, 기업들은

혁신을 추구하면서 강력하고 신뢰할 수 있는 기술 인프라를 유지할 필요성을 충족할 수 있습니다."라고 밝혔습니다.[1]

여전히 툴과 기술을 선택할 때는 신중을 기해야 합니다. 변화를 위한 변화는 리스크입니다. OS처럼 기반이 되는 무언가를 전체적인 감독 없이 변경하면 명백한 이익은 없이 복잡성이 더해질 뿐입니다. 이러한 변화를 정당화하는 가장 강력한 근거는 조직 역량의 측면에서 명확한 장점이 입증되었다는 점입니다. 이러한 장점은 입증 가능해야 합니다. 단지 새로운 OS라는 이유만으로 해당 OS를 실행해서는 안 됩니다. 이 점에 있어서 조직들은 현재 역량에 주목할 뿐만 아니라 OS의 향후 잠재성과 안정성도 살펴야 합니다.

보안 중심의 아키텍처

기술 혁신의 속도가 합법적인 비즈니스에게만 이점이 되는 것은 아닙니다. 사이버 보안 위협이 지속적으로 진화하고 있으며, 기업들은 조직 보안을 유지하지 못하면 공격에 취약해집니다. CrowdStrike의 *2025 Global Threat Report*를 비롯한 시장 연구에서는 사이버 위협이 사이버 방어보다 더 빠르게 발전을 지속하고 있음을 명확히 보여줍니다. 최신 위협 환경은 지속적으로 진화하는 전례 없는 도전 과제를 제시하며, 다수의 전통적인 보안 프레임워크 및 IT 툴은 이러한 과제를 해결하도록 설계되지 않았습니다. 이러한 최신 위협에 직면할 준비를 갖추는 것이 전략적 선결 과제가 되었습니다.

새로운 OS를 구현할 때는 이러한 보안 아키텍처를 고려해야 합니다. OS 선택 프로세스에 보안 질문과 검증을 포함하지 않는 조직은 이중 리스크에 처합니다. 즉, 시스템에서 애플리케이션을 호스팅하는 데 따른 리스크와 시스템 자체의 보안 및 신뢰성 리스크입니다. 특히 이 리포트를 작성 중인 지금 시점에 더욱 그렇습니다. OS 벤더는 OS에 AI 기능을 더 많이 추가하고 있으며 AI 기능이 자동화된 방법으로 시스템 관리 태스크를 수행할 수 있도록 다양한 액세스를 허용하고 있기 때문입니다.

---

[1] McKinsey, "Rethinking Conventional Wisdom: Future of Digital Tech Infrastructure," 2024년 6월 26일, *https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/ tech-forward/rethinking-conventional-wisdom-future-of-digital-tech-infrastructure*.

데이터 보안이 핵심

여기에서 핵심 포인트가 포착됩니다. 어떤 OS이든 애플리케이션을 안전하게 실행할 수 있고 데이터를 안전하게 저장할 수 있는 환경을 제공해야 합니다. 기업 입장에서는 OS의 기본 구성 요소든, OS가 호스팅하는 애플리케이션이든 상관없이 실행되는 모든 요소가 안전하게 유지된다는 것이 확실해야 합니다. 다음 세 개 카테고리의 데이터 보안을 고려해야 합니다.

저장 데이터
: 향후 사용할 수 있도록 저장된 데이터입니다.

이동 데이터
: 시스템 간이나 시스템 내에서, 그리고 애플리케이션 간에 전달되는 데이터입니다.

사용 중인 데이터
: 컴퓨팅 플랫폼에서 활발히 처리 중인 데이터입니다.

저장 데이터와 이동 데이터의 보안은 암호화를 통해 처리하는 경우가 많습니다. 사용 중인 데이터의 보안은 더 까다롭습니다. 현대적인 OS 아키텍처는 신뢰 실행 환경(TEE)을 통합하여 이 문제를 해결합니다. TEE는 신뢰도 높은 소프트웨어로 한정되며 엄격하게 통제되는 메커니즘을 통해서만 액세스할 수 있는 시스템 섹션입니다. TEE 내에서 실행되는 모든 요소는 일반적으로 해당 환경 외부에서는 액세스할 수 없습니다. 종종 단일 서버를 넘어 확장되는 하드웨어 및 소프트웨어 기반 솔루션일 수 있으며 기능을 잃지 않으려면 드라이버와 호환성이 최신 상태여야 합니다. 실제로 구현된 모습은 벤더에 따라 다르며 이 리포트가 다루는 범위를 벗어납니다. 하지만 이러한 보안 환경에서 애플리케이션을 실행할 수 있는지 확인하는 것은 매우 중요합니다.

AI 워크로드에는 보호 이상의 관리 필요

모든 종류의 컴퓨팅 워크로드에는 앞서 논의한 데이터 보호 및 데이터 주권 보장 요구 사항이 적용되어야 하지만, AI 워크로드는 추가적인 두 가지 이유, 즉 AI가 새로운 기술이고 데이터 집약적이라는 점, 그리고 컴퓨팅이 복잡하다는 점 때문에 특히 취약합니다.

AI 워크로드의 신규성이란 프로덕션 워크로드가 표준 워크로드만큼 철저히 검증할 시간을 확보하지 못했음을 의미합니다. 보안은 협업을 통한 노력이며, 시장은 개별 벤더가 자체적으로 할 수 있는 것보다 훨씬 더 많은 검증과 QA를 수행합니다. 제품 자체 및 해당 제품의 구성/사용 방식에 모두 해당하는 사실입니다. *Tenable Cloud Security Risk Report 2025*에서 Tenable은 AI를 지원하는 클라우드 워크로드가 다른 워크로드보다 더 취약하다고 밝혔습니다. 워크로드 호스팅 위치에 상관없이, AI의 데이터 집약적 특성은 지속적인 구성 오류 및 취약점과 결합하여 사이버 보안과 관련해 전에 없던 수준의 주의와 노력을 요구합니다.

조직들은 OS를 평가할 때 AI 고유의 리스크를 고려해야 합니다. 그러지 않으면 현재 및 미래의 워크로드를 침해할 수 있는, 알 수 없는 수준의 리스크를 초래하게 됩니다.

결론

OS 의사 결정에서 목적성을 가지고 판단하려면 조직이 기술을 평가하는 방식을 근본적으로 바꿔야 합니다. 이 장에 제시된 도전 과제는 올바른 선택을 함으로써 경쟁력을 극대화하는 데 필요한 체계를 제공합니다. 이 리포트의 결론에서 이러한 모든 의사 결정을 포괄하는 의사 결정 프레임워크를 살펴보겠습니다. 지금은 OS 배포에 관한 새로운 사고를 가져야 할 필요성이 명확합니다. 현대적인 과제에는 현대적인 솔루션이 필요합니다. 그러한 과제를 수용하고 전략적으로 생각하는 조직은 새로운 기술을 활용하고 경쟁 우위를 극대화하기에 더 유리한 입지에 설 수 있습니다.

3장

현대적인 Linux 플랫폼

현대적인 기업은 Linux를 기반으로 서버 운영을 상당 부분 표준화했습니다. 이는 지난 10년 이상에 걸쳐 다양한 연구에서 입증되었습니다. 한 가지 연구만 들자면, 2025년 8월 SQ Magazine은 대기업의 61.4%가 하나 이상의 미션 크리티컬 워크로드를 Linux 기반에서 실행하며 인터넷 연결 웹 서버 중 78.3%가 Linux를 실행한다고 밝혔습니다.[1] 이러한 지배적인 포지션은 수년에 걸친 성장의 결과이며, 이러한 성장 추세는 둔화될 기미가 보이지 않습니다.

그러나 많은 경우 이러한 진술은 개별 배포판에 대해 논하지는 않으므로, 다수의 의사 결정자가 '모든 Linux가 동일'하다고 생각합니다. 모든 Linux가 같지는 않습니다. 모든 Linux 배포판에 기본적인 Linux 커널이 사용되지만, 커널의 배포 방식과 관련 툴 및 애플리케이션 에코시스템은 매우 다릅니다.

조직이 해야 하는 일은 평가 대상 OS의 주요 차별화 요소를 찾는 것입니다. 다수의 현대적인 OS는 최첨단 기능을 발전시켜 왔지만, OS에 따라 이들 기능이 서로 다르게 처리되며 일부 기능은 일부 OS에서만 사용 가능합니다. 찾아볼 만한 가장 유용한 기능에는 현대적인 보안 배포 모델, AI 통합 시스템 툴, 플릿 관리 툴, 엔터프라이즈급 보안, 확장 지원 및 파트너 인증이 포함됩니다. 또한 OS의 기능은 OS가 호스팅하여 실행할 워크로드 요구 사항에 비추어 고려해야 합니다. 현대적인 요구 사항에 부합하는 동종 최고의 기능인지 판단해야 합니다.

---

[1] Robert A. Lee, "Linux Statistics 2025: Desktop, Server, Cloud & Community Trends," *SQ Magazine*, 2025년 11월 18일 업데이트, *https://sqmagazine.co.uk/linux-statistics*.

OS 배포 혁신

OS 배포는 지난 몇 년간 크게 변하지 않았습니다. 전통적인 배포에서는 모종의 설치 프로그램이 개입하여 커널 및 다른 툴을 하드 디스크에 설치했고 그 후에 사용자가 애플리케이션을 설치했습니다. 패키지 관리의 등장은 애플리케이션 관리 및 시스템 관리 측면에서 큰 도약입니다. 사용자가 애플리케이션을 설치하거나 업데이트할 때마다 코드를 처음부터 컴파일할 필요가 없어졌기 때문입니다.

현대적인 Linux 배포판은 시스템이 기본적으로 필요에 따라 교체 가능하며 변경 불가능한 컨테이너로서 역할을 하는 배포 모드를 제공해야 합니다. 새 이미지를 다운로드할 수 있으며, 간단히 재부팅하기만 하면 변경하려는 모든 시스템 구성 요소를 업그레이드 또는 다운그레이드할 수 있습니다. 이 방식은 보안과 신뢰성을 제공하며 플릿의 모든 시스템이 모든 바이너리 및 라이브러리의 규정된 버전을 실행 중이라는 확신을 줍니다.

생성된 이미지는 애플리케이션 컨테이너(또는 이미지)와 동일한 방식으로 관리할 수 있지만, 바이너리 및 OS 커널 자체에 이르기까지 훨씬 더 작은 규모로 이루어집니다. 이것이 이전의 패키지 기반 업데이트 모델과 비교한 주요 개선 사항입니다. 패키지는 소스에서 컴파일하는 방식에 비해 탁월한 배포 모델이지만 호환성, 패키지 요구 사항, 잠재적 버전 충돌 측면에서 자체적인 문제가 있습니다. 컨테이너 기반 모델의 경우 모든 요소가 이미지에 포함되기 때문에 이러한 문제가 사라집니다. 컨테이너 내 항목의 버전은 일관되게 유지되어, 많은 시스템 관리자가 가지는 구성 드리프트 관련 우려가 크게 줄어듭니다. 또한 이미지 설치가 훨씬 더 빠르고 용이합니다. 간단히 이미지를 다운로드하고 적용한 후 재부팅하면 됩니다.

이미지는 변경 불가능하기 때문에 보안 이점도 제공합니다. 다시 말해서, 악의적인 사용자나 맬웨어가 가동 중인 이미지를 수정할 수 없으며 교체할 수도 없습니다. 이러한 이미지는 애플리케이션 컨테이너와 동일한 방식으로 관리되기 때문에, Podman 같은 표준 컨테이너 툴이나 다양한 다른 컨테이너

플랫폼을 활용하여 이미지를 살펴볼 수 있습니다. 툴에 대한 이러한 지식 덕분에 애플리케이션 컨테이너에 익숙한 관리자는 신속하고 자신 있게 OS 이미지를 배포할 수 있습니다.

마지막으로, 직접 생성한 이미지를 어디서나 사용할 수 있습니다. 물리, 가상화, 클라우드 또는 엣지 환경 등 어느 곳에 배포하든 상관없습니다. 이미지가 배포되고 어느 위치에서나 동일한 방식으로 실행됩니다. 또한 이미지를 처음부터 끝까지 더 손쉽게 관리할 수 있습니다. 그림 3-1은 샘플 이미지 모드 프로세스를 이미지 빌드, 이미지 배포, 배포 후 이미지 관리의 간단한 세 단계로 보여줍니다.

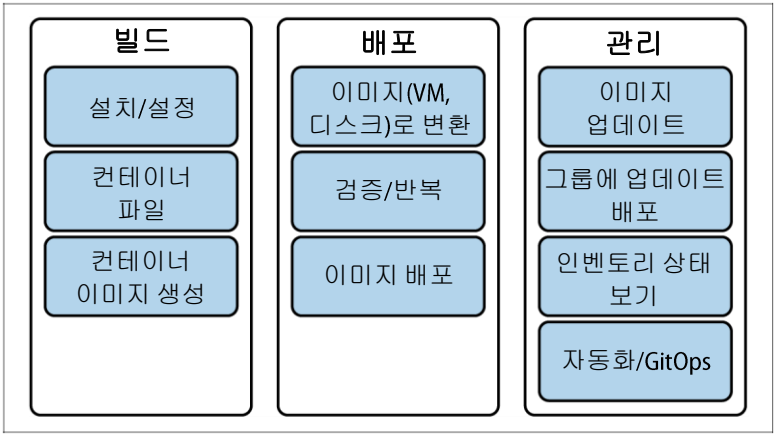

그림 3-1. 샘플 컨테이너화된(이미지 모드) OS 배포 모델

AI 지원 시스템 관리

많은 애플리케이션 제작자가 터미널 에뮬레이터(커맨드라인 액세스 제공) 같은 시스템 관리 툴에 직접 AI를 통합하기 시작했습니다. 이렇게 하면 관리자가 브라우저 창이나 별도의 애플리케이션을 열 필요 없이 원하는 LLM에 쿼리할 수 있기 때문에 특히 유용합니다. 다음 논리적 단계는 OS 제조업체가 동일한 방식을 따르는 것입니다. 즉, OS 자체에 직접 AI를 통합합니다. 그런 다음, 최종 사용자가 선택하는 터미널에

상관없이 커맨드라인에서 AI 어시스턴트를 호출할 수 있습니다. 이 기능은 기술 수준에 상관없이 모든 관리자에게 크게 도움이 됩니다. 특히 주니어 관리자는 커맨드라인에서 직접 AI 어시스턴트에게 질문할 수 있는 기능을 활용하고 즉석에서 재평가하고 적합한 일을 올바른 방식으로 하고 있는지 확인할 수 있습니다.

모든 AI 툴과 마찬가지로, 커맨드라인 어시스턴트를 사용할 때는 주의해야 합니다. 정확한 답변을 얻기 위해서는 커맨드라인 어시스턴트에게 제기하는 질문을 다듬어야 하는 경우도 있습니다. 특히 셸 스크립트 같은 코드를 생성하도록 어시스턴트에게 요청하는 경우 더욱 그렇습니다.

확실치 않은 경우 주니어 관리자는 시니어 동료에게 문의하여 AI 어시스턴트가 제시한 답변이 자신이 수행하려는 작업을 실제로 실행해 낼지 확인하는 것이 좋습니다.

이 툴은 기본 Bash 스크립트 등을 단순히 이해하는 것에 비해 더 강력합니다. 커맨드라인 어시스턴트는 애플리케이션 및 서비스를 구성하고 OS 기능을 활용해 트러블슈팅하는 방법에 관한 편리한 팁을 제공할 수 있습니다. 중요한 것은 이 어시스턴트가 Linux 전반에 관해서뿐만 아니라 배포판의 세부 요점 및 특정 요구 사항과 요건에 대해서도 구체적으로 학습했다는 점입니다. 이러한 미세 조정(fine-tuning)은 AI 분야에서 이미 잘 알려져 있습니다. 일반 LLM과 달리, 적합한 종류의 도큐멘테이션만을 기반으로 학습시켜 환각을 최소화하도록 구축한 사용자 정의 모델은 이런 종류의 툴을 기본 툴의 중요한 차별화 요소로 만듭니다.

커맨드라인 어시스턴트는 SELinux(Security-Enhanced Linux) 및 기본 방화벽 같은 툴에 특히 유용합니다. 이 둘은 모두 시스템 운영에 매우 중요하지만 복잡하며 대부분의 경우 그 구성이 아주 가끔 변경됩니다. 시스템 관리자는 커맨드라인 어시스턴트를 활용해 도움을 받으면 훨씬 더 빠르고 손쉽게 이 툴을 구성할 수 있음을 알게 됩니다. 또한 AI 툴은 검증된 다양한 사례를 비교할 수 있으므로 모범 사례를 잘 파악하고 숙련된 관리자에게도 명확하지 않을 수 있는 구성 오류를 명시할 수 있습니다.

마지막으로, 커맨드라인 어시스턴트는 사용 중인 툴의 구조를 파악하는 데 활용할 수 있습니다. 예를 들어 현대적인 호스트 기반 방화벽을 이해하고 싶으면 단순히 어시스턴트에게 질문하면 됩니다. 어시스턴트는 관련 도큐멘테이션 리소스를 쿼리하여 사용자가 제출한 내용을 기반으로 모범 사례와 예시를 도출하며 구성 또는 소스 코드 변경을 보충하여 추천 내용과 이유를 파악하는 데 도움을 주는, 쉬운 영어로 된 답변을 생성합니다.

플릿 관리 툴

우리가 논의한 두 가지 툴은 강력하며 개별 시스템 수준에서 시스템 관리를 크게 단순화합니다. 다음 툴은 한 차원 높여 사용자가 전체 Linux 배포 환경을 선제적으로 관리할 수 있도록 지원합니다. 이러한 툴은 OS 제조업체가 제공하는 모든 요소와 깊이 연계되어 있습니다. 다시 말해서, 플랫폼 전체를 한곳에서 관리할 수 있어, 관리 및 감사 요구를 단순화합니다. 이상적으로는, 조직이 배포된 애플리케이션 라이프사이클 및 이에 따라 환경 내 실행 중인 시스템에 미치는 영향을 이해하는 데 도움이 되는 계획 기능도 포함됩니다. 이러한 통합에 의해 조직 전반의 실시간 보안 및 구성 검증이 가능합니다.

로드맵 기능은 예정된 애플리케이션/OS 릴리스에 관한 자세한 정보를 제공하므로, 조직은 새로운 기능이 릴리스된 후에 대응하는 것이 아니라, 예상되는 새 기능을 기반으로 업그레이드를 미리 계획할 수 있습니다.

플릿 관리 툴은 시스템 최신 상태를 유지하는 데에도 사용할 수 있습니다. 조율된 패치 적용(자동 또는 예약 실행되어 성공 확인), 기능/소프트웨어 업데이트 또는 롤아웃, 중앙화된 구성 관리 등을 통해 1,000개에 달하는 서버를 관리하는 것도 단일 서버 관리만큼 간편합니다.

엔터프라이즈급 보안

보안을 중심으로 설계한 OS는 앞서 논의한 변경 불가능한 이미지, 구성 관리 등과 같은 보안 이점 그 이상을 포함해야 합니다.

가장 많이 언급되는 향후의 공격 중 하나는 포스트 양자 암호화를 둘러싸고 일어납니다. 이전 장에서 설명한 대로, PQC는 키, 암호화, 디지털 서명용 양자 내성 알고리즘을 제공합니다. 데이터와 애플리케이션이 미래의 기술 발전에 대비하도록 해주며 OS 배포판을 비교할 때 꼭 확인해야 할 중요한 기능입니다.

엔터프라이즈급 OS 플랫폼은 강력한 공급망 보안 기능도 제공합니다. 단순히 OS에 국한되지 않고, DevSecOps 방식으로 배포하려는 개발자와 조직의 역량을 강화하는 플랫폼 접근 방식입니다. 이 예시로 가장 간단한 것은 알려진 양호한 애플리케이션 디펜던시를 호스팅할 신뢰할 수 있는 위치이지만, 훨씬 더 심도 있는 기능까지 가능합니다. 이상적인 DevSecOps 플랫폼이라면 개발 팀에 모든 애플리케이션 및 디펜던시를 위한 엔드 투 엔드 보안 파이프라인을 제공합니다.

PQC 보호, 관리자와 개발자를 위한 자동화된 보안 툴, 선제적인 소프트웨어 관리가 조합되어 지속적으로 업데이트되고 정교한 최신 위협 환경에 대처하는 계층화된 방어 체계를 조성합니다. 중요한 것은 이러한 보안 체계는 조직이 사용하는 툴과 OS를 통해 제공되어 모든 기능을 갖춘 플랫폼 체계가 되므로 조직은 광범위한 외부 제3사 보안 투자에 의존하지 않아도 된다는 점입니다.

확장된 하드웨어 및 소프트웨어 지원 및 인증

OS 플랫폼이 강력하기는 하지만 조직은 여전히 운영을 위한 외부 호환성이 필요합니다. OS 실행 기반이 되는 하드웨어 및 실행 시스템 자체에서 활동되는 제3사 소프트웨어의 경우도 마찬가지입니다.

현대 환경에서 하드웨어 호환성 분야는 빠르게 변화하는 시장입니다. 특히 AI 하드웨어는 매우 빠르게 변화하고 있어, OS 드라이버와 호환성이 이에 발맞춰 발전해야 합니다. 선택하는 배포판이 이런 면에서 탁월한지 확인하는 것이 중요합니다. 최신 AI 라이브러리, 드라이버, 애플리케이션을 제공할 뿐만 아니라 NVIDIA, Intel, AMD 같은 제조업체를 위한 하드웨어 최적화도 지원해야 합니다. 하지만 이들 세 개 주요 업체 외에도, OS 제조업체는 빠르고 안전하며 신뢰할 수 있는 방식으로 최종 사용자에게 최신 기능을 제공하는 강력한 제3사 에코시스템을 갖춰야 합니다.

결론

OS의 보안, 에코시스템, 기능 세트는 서로 연동함으로써 이 리포트 시작 부분에서 언급한 과제, 즉 다른 OS를 탐색하는 전략적 선결 과제를 해결할 수 있습니다. 이번 장에서 제시한 주요 기능이 충족된다면 해당 OS는 기능과 관리 용이성 측면 모두에서 경쟁업체와 차별화됩니다. 기술의 진보는 강력한 파트너 프로그램과 결합하여 신규 OS 플랫폼 선택 시 간과할 수 없는 중요한 전략적 차별화 요소가 됩니다.

4장

다음 단계

조직의 OS 선택은 경쟁력 및 내부 인프라 관리 측면에 영향을 미치는 근본적인 의사 결정입니다. 혁신 가속화, 글로벌 불확실성, 경제적 제약, 현대적인 보안 요구 사항, AI 등이 주는 압력에 대응하려면 통합된 방식으로 이러한 과제를 해결하도록 특별히 설계한 플랫폼이 필요합니다.

이 선택은 가볍게 다룰 의사 결정이 아닙니다. 향후 OS 및 플랫폼과 관련한 의사 결정을 내릴 때 고려해야 할 4가지 주요 평가 단계가 있습니다.

- 조직에 가장 중요한 압력 식별하기
- 워크로드와 기능 요구 사항 매핑하기
- 비즈니스가 얻는 전체 가치 평가하기
- 공급망 보안 및 장기적 실행 가능성 검증하기

조직에 가장 중요한 압력 식별하기

조직은 여러 팀들이 서로 다른 조합의 압력을 받고 있음을 알게 됩니다. AI 제품 팀은 혁신과 하드웨어 요구 사항을 최우선으로 하고, 규제 산업은 보안 및 컴플라이언스 역량에 더 크게 중점을 둡니다. 조직은 압력을 주는 각 분야(혁신 가속화, 글로벌 불확실성, 경제적 제약, 보안 요구 사항, AI)를 현재의 중요성 및 미래의 예상 중요성을 기준으로 평가하고 해당 목록을 활용해 미래에 대비한 평가를 거쳐 '필수 사항'과 '선택 사항'으로 나눠 목록을 작성합니다.

워크로드와 기능 요구 사항 매핑하기

요구 사항을 좌우하는 한 가지 요인은 바로 조직에 가장 중요한 워크로드입니다. 워크로드를 분석하면 조직에 워크로드별 최적화가 유리한지 아니면 더 큰 규모의 표준화 접근 방식이 더 적절한지 알 수 있습니다. 이러한 분석은 규모에 상관없이 모든 조직에 도움이 됩니다. 워크로드의 수량과 중요성이 반드시 회사 크기에 비례하지는 않기 때문입니다.

비즈니스 가치 평가

워크로드를 분석하고 나면 조직은 서버 수, 직원 수(그리고 기술 수준), 관리 중인 총 워크로드 수량을 제대로 파악하게 됩니다. 이러한 수치는 OS 라이센스, 지원 및 인프라 요구 사항과 같은 직접 비용을 산정하는 데 도움이 됩니다. 또한 사내 전문성 수준, 예상치 못한 제약에 따른 워크로드 배포 지연, 인프라 경직성으로 인해 놓친 비즈니스 기회 등과 같은 간접 비용을 추산하는 데에도 도움이 됩니다. 이 데이터를 수집하고 나면 기업은 운영 효율을 향상하고 경쟁력을 높이는 더욱 합리적인 전략적 의사 결정을 정보에 입각하여 내릴 수 있습니다.

공급망 보안 및 장기적 실행 가능성 검증하기

OS 또는 플랫폼 의사 결정을 내리는 조직은 해당 OS 또는 플랫폼을 오랜 기간 동안 사용할 것임을 염두에 둬야 합니다. 회사의 역사를 이해하는 것이 중요하지만 회사의 애플리케이션, 파트너 포트폴리오의 깊이와 폭, 규제 컴플라이언스 및 최첨단 기능(예: AI) 같은 중요한 측면에서의 경험과 역량 등을 검증하는 방법을 아는 것도 중요합니다. 조직은 워크로드 배포의 다년간 라이프사이클이 보장되기를 기대하며, 플랫폼이 현재만이 아닌 미래의 워크로드도 처리할 수 있는지 확인하는 것이 중요합니다.

결론

이 프로세스에서 성공의 핵심은 인프라 의사 결정에 따라 디펜던시가 만들어진다는 점을 이해하는 것입니다. 지금 내리는 선택이 조직의 성공을 가능하게 할 수도, 역량을 제약하고 향후 수년 동안 프로세스를 지연시킬 수도 있습니다. 명확한 요구 사항 및 평가 프레임워크를 염두에 두고 전략적으로 OS 선택 의사 결정에 접근하는 조직은 공격적으로 혁신을 추구하고, 불확실성에 성공적으로 대처하고, 현재만이 아닌 미래에도 생산성과 보안을 최적할 수 있는 기반을 마련할 수 있습니다.

작성자 소개

Ned Bellavance는 20년이 넘는 해당 분야 경력을 보유한 IT 전문가이자 기술 교육자입니다. 헬프 데스크 운영자, 시스템 관리자, 클라우드 아키텍트, 제품 관리자로 활약했습니다. 최근에 Ned는 Ned in the Cloud LLC를 운영하며 교육 과정을 개발하고, 다양한 팟캐스트를 운영하며, 책을 저술하고, 기술 벤더를 위한 오리지널 콘텐츠를 제작하고 있습니다. Ned는 2017년부터 Microsoft MVP를 역임했고 2020년부터 HashiCorp Ambassador로 활동했습니다. 불편함을 받아들이기, 실패에 대비하기, 친절하기라는 세 가지 신조를 가지고 있습니다.

Chris Hayner는 운영 체제, 인프라, 클라우드 컴퓨팅, 사이버 보안에서 수십 년의 경력을 보유한 숙련된 IT 전문가입니다. 커리어의 시작은 데이터센터이며 그는 해당 분야에서 메인프레임, AlphaServer, 화이트박스 x86 서버 등 다양한 시스템을 관리했습니다. 이후 가상화, 클라우드 기술, 포괄적인 사이버 보안 및 IT 전략 분야까지 다뤘습니다. 지난 15년 동안 Chris는 컨설팅 분야에서 일하며 serving as a 분야별 전문가(SME), 아키텍트, 애널리스트로 활동했습니다. 이러한 활동을 통해 수백 개 조직이 비즈니스 목표와 IT 솔루션 사이의 격차를 줄이고 혁신 및 운영 성공을 추진하도록 지원했습니다. Chris는 CISSP 인증 및 다수의 벤더 및 산업 인증을 보유했을 뿐만 아니라 Temple University에서 MBA를 취득하여 기술 전문성과 비즈니스 안목을 고루 갖추었습니다.