2020 년 클라우드, 커넥티드 카, 의료와 사이버보안의 향후 전망

2019 년 12 월 17 일

피터 갤빈(Peter Galvin) | 최고전략책임자
저자 정보 >

자율주행차. 클라우드 컴퓨팅. 연결된 의료(Connected medicine). 데이터 침해.

이 발명품들과 이용 사례, 도전 과제는 지난 몇 년간 기술 부문에서 주요 화젯거리였습니다. 그리고 이들 모두 다음 한 해 동안 큰 변화를 맞이할 예정입니다.

이러한 변화를 주도하는 것은 최신 지식과 기술의 진보, 체계적인 발전이죠. 그리고 (모두는 아니겠지만) 대부분은 좋은 변화일 겁니다.

그럼, 2020 년에 이 중요한 부문들에 어떤 일이 일어날 거라고 예상할 수 있을까요? 제 예상은 이렇습니다.

자율주행차가 가야 할 길, 더욱 멀어지고 커지는 한계

스스로 주행하는 자동차가 공상 과학 이야기처럼 들린다면, 여러분만 그렇게 생각하는 건 아닙니다. 사람들 대다수에게 자율주행차는 여전히 먼 미래처럼 여겨지죠. 그리고 어떤 면에서 자율주행차는 실제로 먼 미래이기도 합니다.

모두 알다시피 자율주행차는 오늘날 실존하고 있습니다. 하지만 그렇다고 해서 어느 날 곧 길거리에서 수많은 자율주행차를 보게 될 거라는 건 아닙니다. 대신, 성공적으로 시장에 출시될 대부분의 자율주행차는 제한된 범위와 거리에서 운행될 겁니다.

자율주행차를 안전하게 출시하는 방법을 찾는 것은 매우 큰 도전 과제입니다. 그러니 이 과정에 몇 가지 문제가 있을 수 있다는 건 납득할 만합니다. 하지만 자율주행차는 예상보다 훨씬 큰 문제들을 마주했습니다. 치명적인 충돌 사고를 포함해서요.

그 결과로, 자율주행차는 초기 예상보다 훨씬 먼 미래의 일이 되었습니다. 이로 인해 우리는 자율주행차를 이용하는 방식에 일어나는 변화를 마주하게 됩니다. 특정한 도로에서, 특정

속도로, 정해진 거리만큼만 이용하도록 제한됩니다. 스키장 셔틀버스처럼 아주 명확한 구간에서만 이용되며 작은 역할만을 맡게 됩니다.

부메랑 효과, 다중 클라우드와 다중 배포의 도입 확대 주도

IDC(International Data Corporation)는 전 세계 퍼블릭 클라우드 지출이 올해 2,290 억 달러에 이르며, 2023 년에는 거의 5,000 억 달러에 달할 것으로 추산합니다. 또한, 시장 조사 기관인 가트너의 설문조사에 따르면 퍼블릭 클라우드 사용자의 81%가 2 개 이상의 제공업체를 이용하고 있는 것으로 나타납니다. 하지만 IDC 는 물리 서버에서 곧바로 다중 클라우드로 전환하지 않을 것을 조언합니다. 플랫폼 간의 미묘한 차이는 하나 이상의 클라우드 상에 서비스를 구현하는 것을 어렵게 만들기 때문에, 사내 직원들이 충분히 익숙해질 수 있도록 기업들이 충분한 시간을 들여야 한다고 설명합니다.

극복해야 할 문제는 여전히 있지만, 저는 내년 중 다중 클라우드 도입이 더욱 확대될 것이라고 예상합니다. 또한, 2020 년에는 퍼블릭 클라우드뿐만 아니라 물리 서버와 사설 클라우드 환경에도 부합하는 기술에 관심이 더욱 집중되리라고 생각합니다. 부메랑 효과 때문이라고 할 수 있죠.

불과 몇 년 전, 많은 기업은 퍼블릭 클라우드로 100% 전환할 계획이었습니다. 그리고 일부 기업들의 경우, 수많은 애플리케이션을 클라우드로 이전했죠. 이 과정에서 기업들은 퍼블릭 클라우드가 항상 모든 필요를 충족하지는 않는 것을 깨달았습니다. 보안 문제, 애플리케이션 수정 요건을 비롯한 문제점을 발견했기 때문입니다. 그 결과, 일부 앱은 물리 서버 배포 형식으로 복귀됩니다.

오늘날 점점 더 많은 기업이 다중 클라우드와 다중 배포 환경을 받아들이고 있습니다. 기업들이 이렇게 애플리케이션을 배포하는 것은 최고의 기술과 보안성을 제공하기 때문입니다. 물리 서버이든지 클라우드이든지 관계없죠.

제가 보기에 클라우드 환경을 모방하는 비즈니스 애플리케이션은 계속해서 늘어날 것입니다. 엄밀히 말해 애플리케이션이 퍼블릭 클라우드에 속하지 않아도 마찬가지입니다. 기업들은

애플리케이션을 늘리고 확장할 수 있으며, 워크로드를 활성화하고 비활성화할 수 있는 인프라와 아키텍트를 구축합니다. 이런 환경은 퍼블릭 클라우드와 놀랍도록 유사하게 보이지만, 대신 물리 서버나 사설 클라우드상에 구축됩니다.

방문 의료를 촉진하는 연결된 의료

몇 년 전, 와이어드(WIRED)지는 "헬스케어 2020: 이제 진료는 전자 의사가(Healthcare 2020: The e-Doctor Will See You Now)"라는 제목의 기사를 보도했습니다. 이 기사에서는 의료계 내 서류 기반 절차가 줄어들 가능성에 주목했습니다. 시간이 지남에 따라 환자들 스스로가 개인 의료 정보 관리를 더욱 주도하게 될 거라고 했죠. 또한, 웨어러블 기기가 어디에서나 환자의 건강을 모니터링하게 될 것이라고 합니다.

이런 트렌드는 이미 어느 정도 진행되고 있습니다. 내년에는 더욱 보편화될 것으로 예상됩니다.

2020 년에는, 이전에는 의료 시설에서만 볼 수 있던 산소호흡기와 같은 대형 의료 기기를 가정에서도 볼 수 있게 됩니다. 이런 기기들은 작아지고 인터넷에 연결된 기기들로, 가정에서도 이용할 수 있게 됩니다. 네트워크에 연결된 기기들이기 때문이죠. 가정에서 이런 기기들을 사용할 수 있다는 것은 의료업계와 소비자 모두가 시간과 비용을 절약할 수 있다는 의미입니다. 이런 기기들은 건강을 증진하고 생명을 살릴 잠재력 또한 지닙니다.

계속해서 주요 도전과제로 이어지는 데이터 침해

더 많은 연결된 기기, 연결된 시스템으로의 개인 정보 이전은 더욱 큰 위험을 의미하기도 합니다. 그래서 2020 년에는 2019 년만큼이나, 혹은 더 많은 데이터 침해가 발생하게 됩니다.

범법자들은 데이터 침해가 잠재적으로 황금알을 낳는 거위라는 점을 깨달았습니다. 그 결과, 이제는 해커 개인이 아니라 조직범죄 집단이 개인 식별 정보(PII)를 찾아 헤매는 상황이 되었습니다.

귀중한 정보를 제공하는 의료 정보는 특히나 범법자들의 이목을 끄는 정보입니다. 몇몇 보고서에 따르면 전체 의료 기록은 다크웹에서 최대 1,000 달러에 거래될 수 있습니다. 신용카드 정보나 사회보장번호를 훨씬 웃도는 액수죠. 허가받지 않은 사람이 웨어러블 기기와 몸에 이식한 기기 해킹으로 의료 기록에 접근해, 환자의 전자 의료 기록을 담은 의료 시스템에 침입하는 방법을 찾아낼 수 있습니다.

전반적인 사이버보안 문제를 더욱 위태롭게 하는 여러 다른 요인도 있습니다. 인적 과실이나 "겨우 충분한 정도"의 보안과 "불필요하게 높은" 보안 사이에서 균형을 잡지 못하는 기업들이 그 예가 될 수 있습니다.

기업들에는 보안과 개인 정보 통제가 필요하지만, 보안과 통제 수준이 너무 높아 소비자를 몰아내는 정도여서는 안 됩니다. 이 최적 수준을 찾아내는 것이 큰 도전과제입니다. 너무 낮은 수준의 보안을 구축하는 실수를 저지르는 기업들은 향후 데이터 침해의 표적이 될 수 있습니다.

엔트러스트 솔루션에 관해 자세히 알아보려면 엔트러스트 웹사이트를 방문하시기 바랍니다. Twitter, LinkedIn, Facebook 에서도 엔트러스트를 팔로우하실 수 있습니다.