IDG
STRATEGIC
MARKETING SERVICES

namu CITRIX®

IDG Tech Focus

“혁신을 촉진하는 안전한 업무 환경”
디지털 워크스페이스 전략 가이드

- **Executive Viewpoint**
  현대적인 워크스페이스를 위한 동급 최강 보안
- **Special Research**
  차세대 업무 환경 우선순위 조사 : 세대별 역할별 격차와 보안 패러다임
- **Tech Guide**
  디지털 트랜스포메이션에서 보안의 역할
  디지털 트랜스포메이션이 IT 인력에 미치는 영향
- **Technology Review**
  “생산성부터 클라우드, 보안까지” 차세대 업무 환경의 조건과 Citrix Workspace
- **Case Study**
  아시아 최대 복합 리조트 제주신화월드 VDI 도입사례

Executive Viewpoint

현대적인 워크스페이스를 위한 동급 최강 보안

Stan Black | Citrix Chief Security and Information Officer. CISSP인 Stan Black은 사이버 보안, 비즈니스 위험, 위협 인텔리전스, 기업 데이터 보호, 인프라 간소화, 그리고 위기 관리 분야에서 25년 이상의 경력을 가진 베테랑이다.

디지털 워크스페이스의 발전에 따라 변화하는 환경과 사용자 그리고 외부에서 생성되는 데이터를 보호하는 전략 역시 발전해야만 한다. 시트릭스 CISO에게 세계 최강 보안 전략 수립 방안을 물었다.

Q 오늘날의 디지털 워크스페이스를 가장 안전하게 보호할 수 있는 접근방법은 무엇인가?

A 클라우드를 통해서 우리가 소비하는 모든 서비스는 처음부터 끝까지 안전해야만 한다. 클라우드에 연결하는 경우, 누가 클라우드를 통제하고 안전을 책임지고 있는지 생각해야 한다.

클라우드 서비스 업체가 적절한 인증을 받았는지, 서드파티 테스트를 이용하고 있으며, 지속적으로 테스트를 하고 있는지 확인하는 것이 중요하다. 인증을 받는 것은 일회성 프로세스가 아니다. 지속적인 테스트와 개선이 필요하고, 끊임없이 변화하며 수정과 업데이트가 이루어지는 애자일 환경에서는 필수적이다. 보안과 컴플라이언스를 위한 모든 구성요소가 올바로 갖춰져 있는지, 중요한 기업 애플리케이션 및 데이터의 전달과 액세스를 위한 통제 라인을 명확하게 이해하고 있는지 확인해야 한다. 클라우드의 좋은 점은 보안 유효성 검사를 자동화해 적절한 사용 권한이 요구되는지를 확인하고 비정상적인 활동이나 행위가 드러나도록 표시할 수 있다는 것이다.

Q 유연성을 유지하면서 보안도 확보하고 민첩성도 강화하려면 어떻게 해야 하는가?

A 전통적으로 사용해오던 방법과 접근방식을 사용하지 않아야 한다. 이런 방식은 효과가 없었다. 단순화에 우선순위를 두고 유용하지 않은 기술은 제거해야 한다. 단순화와 자동화는 이전에는 불가능했던 수준의 생산성과 사용자 경험, 그리고 보안에 대한 통찰을 얻을 수 있는 역량을 제공한다. IT는 이미 이전에는 불가능했던 방식으로 다듬고 조정할 수 있는 역량이 있으므로 사용자가 좋아하는 경험을 제공하고, 섀도 IT를 제거하며, 보안과 컴플라이언스를 모두 유지하는 데 도움이 될 기술에 자원을 투여하고 있다.

IT는 제공하는 서비스의 근간에서부터 자동화를 구축해야만 한다. 이들 서비스는 자사의 비즈니스와 고객의 비즈니스를 확장하고 요구사항을 만족시키는 데 맞춰 서비스를 제공할 수 있는 깊이 있고 풍부한 정보를 하루 24시간 얻을 수 있다.

Q 경영진이 사용자 ID와 액세스 제어를 잘 관리하려면 어떻게 해야 하는가?

A 우리는 수집하고 기록하는 정보를 표준화함으로써 이 문제를 해결하고 관리하고 있다. 통합 로깅(Unified Logging)을 이용해 불필요한 데이터를 걸러 내기 위해 분석과 머신러닝을 실행할 수 있다. 개인의 행태와 사용 패턴에서 원격 측정을 추가함으로써 변칙적인 활동을 더 잘 식별해낸다. 시간을 들여야 하는 것은 비정상적이거나 변칙적인 행위를 발견해 조사할 때뿐이다.

Q 인적 요소를 다루는 데 대한 조언이 있다면?

A 사이버 이벤트가 진행 중인 경우, 우리는 2가지 방식으로 기준을 잡는다. 첫째, 나와 회사에는 어떤 의미가 있는가? 둘째, 개인과 가족, 그리고 소중한 사람들에게 어떤 의미가 있는가? 하트블리드(Heartbleed)는 대규모 공격이었고 뉴스에 계속 등장했으며, 이는 많은 사람들에게 공포와 불안감을 불러일으켰다. 하지만 반면에 교육의 기회이자 파트너십을 위한 기회이기도 했다. 우리는 안팎의 사람들에게 상황을 설명하고 업무와 개인정보의 보안을 유지하기 위한 베스트 프랙티스를 공유했다. 정보를 연관성 있고 사용할 수 있는 것으로 만들면, 사용자와 파트너십을 구축해 보안을 IT의 임무는 물론, 사용자의 임무로 만들 수 있다. 제공하고 있는 서비스의 경험을 개인화하면, IT는 사용자와 파트너 관계를 맺게 되는 것이다. 이것이 기술에 인간적인 면을 적용하는 방식이다.

Q 디지털 워크스페이스가 어떻게 발전할 것으로 보는가?

A 컴퓨팅 역사상 처음으로 서비스를 제공하는 모두가 거의 전적으로 사용자 경험에 초점을 맞추고 있다. 현재 처리 작업이 일어나는 에지로 콘텐츠와 정보를 보낼 수 있도록 만든 애플리케이션이 대세로 자리잡고 있다. 사용자의 모바일 디바이스에서 상당한 처리 작업을 할 수 있다. 따라서 회사나 클라우드와 연결이 좋지 않아도 필요한 소량의 데이터는 서비스 받을 수 있기 때문에 문제가 되지 않는다.

Special Research

차세대 업무 환경 우선순위 조사
세대별 역할별 격차와 보안 패러다임

IT책임자라면 누구나 산더미 같은 복잡성에 직면해 있다. IT 책임자의 임무, 즉 혁신을 주도하고 생산성을 높이는 일이 레거시 시스템과 섀도 IT, 그리고 클라우드 플랫폼에 의해 도전받고 있다. 이들 역시 하나의 총체적이고 역동적인 환경으로서 함께 동작해야만 하기 때문이다. 이 문제를 더 복잡하게 만드는 것은 숙련된 IT 인력의 부족과 신기술에 대한 서로 다른 지식과 기대를 가지고 있는 여러 세대의 사용자들이다. 설상가상으로, IT는 직원의 업무 몰입도를 희생하지 않으면서 점점 더 정교해지고 있는 사이버 위협으로부터 이 역동적인 환경을 보호해야만 한다.

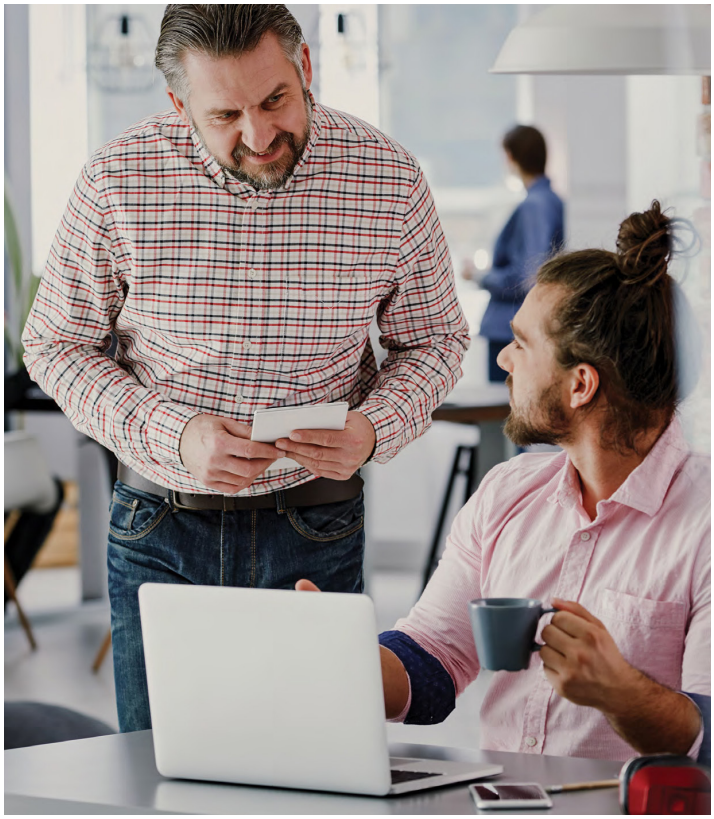
선도적인 CIO와 IT 책임자는 이 복잡한 퍼즐의 해법으로 디지털 워크스페이스를 고려하고 있다. 현대 업무 환경의 핵심 축 중 하나로서, 디지털 워크스페이스는 애플리케이션, 가상 데스크톱, 파일, 그리고 콘텐츠 같은 광범위한 디지털 자산을 아우르고 원격 데스크톱을 확장해 고도로 맥락화되고 개인화된 경험을 제공한다. 디지털 워크스페이스는 위치에 관계없이 특정 워크플로우의 맥락에 따라 콘텐츠와 비즈니스 서비스를 제공하기 위해 이메일부터 협업 앱, 모빌리티, 그리고 보안 기능에 이르기까지 다양한 기술을 활용하며, 한편으로는 적절한 안전장치를 고수한다. 그 결과 보안을 훼손하지 않고 직원의 업무 생산성을 크게 높여줄 수 있는 직관적이고 몰입도가 높은 사용자 경험을 구현한다.

직원 수가 500명 이상인 미국 기업의 IT 임원 201명을 대상으로 IDG와 시트릭스가 실시한 조사에서도 디지털 워크스페이스가 미래 조직의 성공을 위한 핵심 기반으로 인식되고 있음을 확인할 수 있었다. 응답자 10명 중 9명은 디지털 워크스페이스가 생산적인 비즈니스 운영에 중요하거나 핵심적이라고 답했으며, 비슷한 비율의 응답자가 견실한 디지털 워크스페이스 전략이 앞으로의 비즈니스 성과를 달성하는 데 있어 핵심 요소라고 말했다.

디지털 워크스페이스와 보안

보안을 제대로 구현하는 것은 디지털 워크스페이스 배치에 매우 중요하다. 이는 디지털 워크스페이스 보안을 가장 중요한 투자 우선순위라고 평가한 응답자가 86%라는 것으로 쉽게 확인할 수 있다. 77%의 응답자는 한걸음 더 나아가 디지털 워크스페이스 로드맵을 추진하는 데 있어서 보안을 최우선 과제로 꼽았다.

배치 계획에서는 보안 문제의 우선순위가 높았지만, 설문에서는 전통적인 접근방식과 관련된 과제 그리고 기존의 보안 패러다임과 디지털 워크스페이스에



서 영감을 받은 새로운 업무 환경 간의 단절 역시 드러났다. 디지털 워크스페이스의 핵심 원칙인 모빌리티가 보안 문제를 야기하고 있다. 응답자의 41%가 여러 대의 디바이스를 지원해야 한다는 요구조건이 올바른 보안 프랙티스를 방해하고 있다고 답했다.

동시에, 최신 디지털 워크스페이스의 핵심 기술 중 다수가 전통적인 IT 환경에서는 문제가 되지 않았던 보안 허점을 열어놓고 있다. 생체 인식 기반 보안 같은 새로운 방법이 가장 큰 우려사항(66%)으로 조사됐다. 그러나 안정적인 기술도 문제가 있었는데, 응답자들은 와이파이(62%), 이메일(60%), 그리고 노트북 PC(59%)의 사용과 관련한 보안 문제를 제기했다. 결론적으로 IT 조직은 기존의 단편화된 접근방식을 재검토해 전체 환경에 대한 가시성을 제공하는 좀 더 총체적인 보안 패러다임으로 접근해야 한다는 것을 보여준다.

기업이 디지털 워크스페이스의 맥락에서 새로운 보안 접근방식을 도입함에 따라, 새로운 안전장치를 추가하는 것과 긍정적인 사용자 경험을 유지하는 것 사이에서 균형을 잡으려는 움직임도 적지 않다. 응답자의 77%는 사용자 경험을 희생하거나 안전장치의 수준을 낮추지 않고도 보안을 강화하는 것이 가능하다고 자신했다. 하지만 밀레니엄 세대의 생각은 달랐다. 이번 설문조사에서 이런 움직임이 제로섬 게임에 불과하다는 밀레니엄 세대 응답자는 두 배나 많았다.

현재, 대부분 기업(87%)은 디지털 워크스페이스 보안 로드맵의 일환으로 이중인증(Multifactor Authentication) 기법을 채택하고 있다. 그중 30%는 OTP(One-time Passcode)를 사용하고 있고, 나머지 30%는 하드웨어와 소프트웨어 토큰을 사용하는 것으로 나타났다. 좀 더 구체적으로 살펴보면, 응답자의 72%가 디지털 워크스페이스 액세스에 필요한 인증서의 유효성을 검사하는 데 사용자 이름/암호 조합과 SSO(Single Sign-on)를 활용한다. 그러나 신기술 사용도 증가세를 보였는데, 22%의 응답자가 생체 인식을, 17%의 응답자가 푸시 알림을 사용한다고 답했다.

보안에 대한 세대 간 인식 격차

디지털 워크스페이스를 위한 전략을 세울 때 IT 조직은 보안과 관련된 골칫거리를 야기할 세대 차이에 직면할 가능성이 크다. 우선, 각 세대는 정보를 공유하

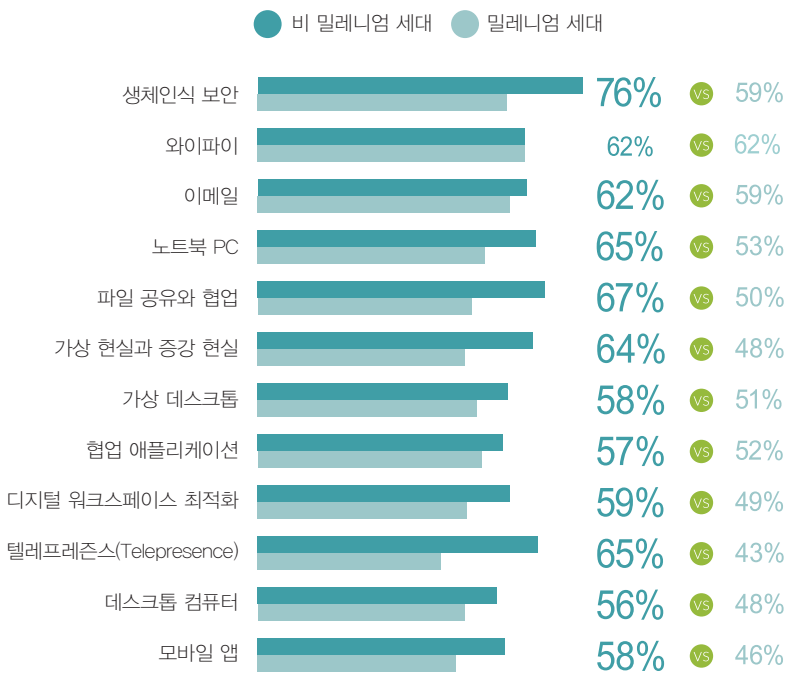
려는 의지와 위험에 대한 욕구에 따라 보안에 다른 우선순위를 부여한다. 비 밀레니엄 세대는 강력한 보안 계획을 기꺼이 받아들인다. 비 밀레니엄 세대 응답자의 87%는 디지털 워크스페이스 전략을 수립할 때 강력한 보안 계획을 최우선 과제로 꼽았다. 이와 대조적으로, 같은 생각을 가진 밀레니엄 세대 IT 임원은 58%에 불과한 것으로 조사됐다.

각 세대가 우려하는 보안 위협의 종류에는 차이가 있다(그림 1 참조). 보안에 부여한 우선순위를 고려할 때, 비 밀레니엄 세대 응답자는 보안 조치로 인한 간섭이 너무 많아 직원이 배제되는 상황에 가장 민감한 것으로 나타났다. 67%에 불과한 밀레니엄 세대 응답자에 비해 비 밀레니엄 세대 응답자의 81%는 보안 조치가 업무 생산성을 저해하지 않는다고 답했다.

비슷한 맥락에서, 비 밀레니엄 세대 응답자의 81%는 직원의 업무 생산성을 위해 보안을 훼손하고 싶지는 않다고 답했다. 밀레니엄 세대 응답자의 비율은 58%였다. 확실히 비 밀레니엄 세대는 디지털 워크스페이스 없이는 SaaS와 클라우드 앱 보안이 불가능하다는 응답이 많았고(81%), 밀레니엄 세대는 절반 정도(58%)에 그쳤다.

디지털 워크스페이스를 보호하는 것이 조직의 최우선 과제라는 것에는 의심의 여지가 없다. 그러나 이 과제는 세대 차이로 인해 복잡해졌으며, IT 조직이 직원 몰입도와 사용자 경험을 떨어뜨리지 않고 보안 위험을 완화할 수 있는 새로운 전략을 마련하도록 압박하고 있다.

그림 1 | 세대별 보안에 대한 우려



최종 사용자와 IT의 보안에 대한 인식 격차

수차에 걸친 설문조사는 IT 의사결정자들 사이에서 보안이 가장 높은 우선순위라는 것을 증명했다. 그렇다면 최종 사용자들은 어떻게 생각하고 있을까?

IT 책임자의 데이터 보안에 대한 걱정은 끊이지 않는다. 공격이 갈수록 더 정교해지면서 해야 할 일도 늘어나고 있다. IDG와 시트릭스가 실시한 설문조사에 따르면, 기업의 미래 계획에서 보안이 가장 중요한 관심사인 이유는 바로 이 때문이다. 최종 사용자도 보안 위협과 회사의 각종 정책을 인지하고 있기는 하지만, 사용자 일부의 행동과 기술 사용은 주목할 가치가 있다.

직원들은 이제 칸막이와 사무실을 넘어 집, 도로, 그리고 해외로까지 이어지는 디지털 직장 생활을 하고 있다. IDG 조사에서 IT 책임자는 이런 트렌드의 영향을 다음과 같이 인식하고 있다.

- 92%는 디지털 워크스페이스 전략이 기업의 성공에 중요하거나 대단히 중요하다고 응답했다.
- 77%는 이런 디지털 워크스페이스의 보안이 최우선 과제라고 답했다.

IT 의사결정권자는 디지털 워크스페이스를 가능케하는 기술 중 다수에 대해 우려하고 있는데, 이러한 우려 목록 제일 위에는 생체인식 보안, 와이파이, 그리고 이메일이 있다.

흥미롭게도, IM(Instant Messaging), 웹 앱, 그리고 모바일 디바이스는 IT 책임자의 우려 목록에서 제일 낮은 순위에 있는 반면, 최종 사용자가 업무를 진행하는 데 가장 선호하는 요소로 나타났다. 사실, 이메일은 최종 사용자가 가장 피하고 싶은 앱 중 하나이며, 그 대신 모바일 디바이스의 문자 메시지, 세일즈포스나 슬랙(Slack) 같은 채팅이 통합된 앱을 좋아한다.

IT 책임자는 조직 내에서 데이터 보안의 중요성을 잘 설명해 왔다. 이번 조사와 관련해 별도로 인터뷰한 8명의 이해당사자는 자신들의 개인정보와 회사의 데이터를 보호하는 일의 중요성을 잘 알고 있었다. 한 물류회사의 영업 관리자(29세)는 “나는 고객 정보를 보호해야만 한다”며, “이건 카드 게임과 같은 것이다. 내 손에 있는 걸 누가 보길 원하지 않는다”고 말했다.

그렇지만, 최종 사용자가 자신의 행동에서 위험을 꼭 인식하고 있다는 것은 아니다. 소셜 미디어에 대한 접근을 제한하는 몇몇 기업의 직원들은 이들 사이트에 접속하기 위해 회사 네트워크를 다소 정기적으로 벗어났다고 인정했다. 한 명을 제외한 모든 이들이 개인적인 이유로 회사 디바이스로 구글의 서비스, 즉 채팅이나 구글 문서도구, 공유 드라이브 등을 이용했다고 답했다.

전반적으로, 직장에서 기술을 사용할 때 보안에 대한 우려가 있느냐는 질문에 최종 사용자들은 자신의 책임이 아니라고 말했다. 한 비즈니스 프로세스 애널리스트(51세)는 “보안은 내 일이 아니라 다른 사람의 문제”라고 말했다.

시트릭스의 최고 보안 전략 임원인 커트 로머는 솔직히, 직원들은 보안 기술을

고려할 필요가 없다는 입장이다. 로머는 "워크스페이스는 사용자에게 보안에 적합한 애플리케이션과 데이터만 제공할 수 있을 정도로 지능적이어야 한다"고 지적했다. 바로 이 부분에서 직원들이 어떻게 일하고 싶은지에 대한 문화적인 이해뿐만 아니라 분석, 머신러닝, 그리고 자동화가 도움이 될 것이다.

로머는 "문화와 코드를 어떻게 표현할 것인가? 이는 미래의 업무 공간을 설계하는 데 있어서 진취적인 사람 모두에게 큰 과제가 될 것이다"라고 강조했다.

업무 공간의 재정의

오늘날의 직원들은 전통적인 물리적 사무실의 경계를 넘어 업무 역량을 확장하는 것을 선호한다. 직원들은 이제 업무용 디바이스를 휴대하고 책상, 회의실, 프로젝트 그룹 사이를 유동적으로 움직인다. 카페에서 점심을 먹으면서 이메일을 확인하고, 집에서도 이동 중에도 심지어 해외에서도 업무를 본다.

한 소비재 회사의 프로젝트 매니저(32세)는 "기술은 물리적 사무실 없이 일을 할 수 있게 해주고, 이 도시에서 저 도시로의 매끄러운 전환을 통해 원격으로 일을 할 수 있게 해 준다"고 말했다. 그는 현재 콜롬비아 보고타에 있는데, 매월 새로운 장소에서 여행하고 일할 수 있도록 해주는 리모트 이어(Remote Year)란 프로그램에 참여하고 있다. 페루와 컬럼비아에서 3개월을 보낸 후, 멕시코시티로 이동할 계획이다. 이 프로젝트 매니저에게 가장 중요한 것은 "고객이나 동료가 연락할 수 있게 하는 것"이다. 하지만 그는 "음성 통화 앱과 관련 기술 덕분에 그리 어렵지 않다. 아무도 내게 '대체 어디에 있느냐?'고 물어보지 않았다"고 말했다.

이것이 새로운 워크스페이스의 특별한 사례일지는 모르지만, 직원들은 훨씬 더 큰 유연성을 가져다주는 디지털 업무 방식을 기대하고 있다. 미국 전역과 다양한 산업에서 근무하고 있는 29세에서 62세 사이의 최종 사용자 8명이 말하는 오늘날 업무를 수행하는 방법에 대해 살펴보자.

정해진 책상에 얽매이는 시대는 저물고 있으며, 이는 오늘날 디지털 작업의 상당한 이점으로 간주되고 있다. 62세의 한 공공서비스 사서는 "너무나 많은 애플리케이션이 이제는 웹 기반이다. 나는 어디서나 그 애플리케이션에 액세스할 수 있다"며, "예전에는, 내 책상에서 해야 할 일이 있었다. 이제는 내가 원한다면, 다른 책상이나 집에서 할 수 있다"고 말했다.

디지털 공간은 또한 직원의 업무 효율성도 개선했다. 예를 들어, 한 물류 회사의 29세 영업 관리자는 자신의 업무용 기술이 "한 번에 12가지 일을 진행하더라도 자신을 조직적이고 집중된 상태로 유지시켜 준다"고 말했다.

어떤 식으로든 서로 연결되어 있지 않으면, 여러 앱을 사용한다는 것은 부담이 될 수 있다. 최종 사용자는 여러 가지 고유 로그인을 사용해야 한다는 것, 그리고 하나의 소스에서 데이터를 추출할 수 없는 것 등의 장애요인을 지적했다. 인터뷰에 참여한 응답자 중 단 한 명, 29세의 영업 관리자만이 IAM(Identity and Access Management) 시스템을 통한 단일 디지털 인터페이스를 사용하고 있었다. 그는 회사가 솔루션을 구축하기 전에는 "정보를 수집하기 위해 이 앱에서 저 앱으로 돌아다녀야만 했다. 일이 두 배나 되었다"고 설명했다.

새로운 디지털 작업 방식에 대한 또 다른 도전은 좀 더 철학적이다. 한 부동산 투자회사의 38세 부장은 "플러그를 빼기 어렵다"며, "사람들에게 연락이 닿지 않는다고 말하는 것은 거의 수치로 여겨진다"고 말했다. 공공 서비스 사서의 말대로 "일은 결코 끝나지 않는다."

세대 간 보안 격차를 해소를 위한 패러다임

업무용 기술이 최첨단 기술의 상징이었던 시대는 오래전에 끝났다. 개인 생활에서 애플, 아마존, 구글이 주도하는 원활한 고객 상호작용에 익숙해진 직원은 업무 환경에서도 비슷하고 제약 없는 경험을 기대한다. 하지만 보안이나 다른 장벽이 이런 모빌리티에 방해가 되면서 좌절하게 된다.

생산성과 보안을 향상시키는 발판 역할을 하는 동시에 현대적인 작업 환경을 재정의하는 기술인 디지털 워크스페이스를 적극적으로 고려해야 할 시점이다. 디지털 워크스페이스는 앱이나 원격 데스크톱 모음이 아니다. 디지털 워크스페이스는 직원들이 어디서나 모든 디바이스에서 안전하게 작업할 수 있도록 하는 상황별 맞춤형 경험을 제공해 업무를 수행하는 데 필요한 도구, 시스템 그리고 콘텐츠의 완벽한 보완체에 쉽게 액세스할 수 있도록 한다.

디지털 워크스페이스는 궁극적으로 몰입도와 더 나은 의사결정을 촉진한다. 시트릭스의 최고 보안 전략가인 커트 로머는 "사용자가 업무란 맥락 안에서의 동적인 역할을 이해하고 최대한 생산적이고 몰입할 수 있도록 권한을 부여하는 데 도움을 준다"고 설명했다.

디지털 워크스페이스에 대한 기업의 관심이 빠르게 증가하고 있다. IDG/시트릭스 설문조사에 따르면, 응답자의 92%가 건전한 디지털 워크스페이스 전략을 성공의 열쇠로 꼽았고, 93%는 직원의 생산성을 향상시키는 이 기술의 역량을 긍

정적으로 평가했다. 말로만 디지털 워크스페이스 개념을 칭찬하는 것은 아니다. 응답자의 96%가 디지털 워크스페이스 최적화를 현재 또는 가까운 미래에 대다수 직원이 사용할 수 있다고 확인했다.

보다 유연하고 고도로 직관적인 업무 방식을 추진하게 된 데는 증가한 밀레니엄 세대가 한몫한다. 이들 밀레니엄 세대는 2025년까지 전 세계 노동력의 약 3/4를 차지할 것으로 추산된다. 디지털 세계에서 성년이 된 밀레니엄 세대는 직업적인 환경에서 유연하고 통합된 경험을 기대하지만, 베이비붐 세대와 X 세대 직원 역시 다양한 업무 방식에 대한 지원을 요구하고 있다. 그리고 모든 세대는 여러 디바이스를 지원하는 모빌리티 솔루션에 굶주려 있다. IDC는 2020년까지 모바일 인력이 미국 노동력의 거의 3/4(72.3%)을 차지할 것으로 추정하고 있다.

새롭게 조명 받는 보안

디지털 워크스페이스가 직원 생산성에는 긍정적인 요소가 되겠지만, IT 조직, 특히 기업 보안에는 심각한 과제를 제시한다. 기존의 기업 시스템과 업무 환경은 생산성을 제한하고 유연성을 저해하는 구식 보안 프레임워크가 부담으로 작용하기 때문이다.

IDG/시트릭스 조사에 따르면, 대부분 조직은 OTP(30%)와 하드웨어 및 소프트웨어 토큰(30%)을 포함한 일종의 이중 인증(87%)을 사용하고 있다. 그러나 사용자 경험의 컨슈머라이제이션이란 요소가 남아있다. 서로 다른 디바이스별로 토큰을 작동시키거나 여러 개의 암호를 기억해야 한다는 생각은 최종 사용자를 지치게 만들고, 이 때문에 많은 사용자가 번거로운 기업 보안 프랙티스를 피하기 위해 섀도 IT로 눈을 돌리고 있다.

IT 의사 결정권자의 41%가 여러 디바이스를 지원하는 것이 보안 전략에 부정적인 영향을 미친다고 답한 것은 놀랄 일이 아니다. 특히, 이들은 여러 가지 문제를 나열했는데, 엔터프라이즈 데이터 액세스에 대한 통제력이 떨어지는 것을 가장 우려스러운 문제(40%)로 지목했으며, BYOD(Bring Your Own Device) 환경에서 매우 다양한 개인 디바이스와 플랫폼을 지원하는 데 어려움을 겪고 있다 (39%)는 점, 그리고 주요 과제로 사이버 공격을 범죄과학적으로 조사하는 능력에 대한 한계(37%)를 언급했다. 응답자의 37%는 아웃바운드 필터(Outbound Filter)를 우회하도록 설정된 디바이스가 또 다른 장애물이라고 언급했는데, 이는 이런 디바이스가 데이터 프라이버시 보호 법률과 다른 규제 요건을 준수하지 못할 위험성을 높이기 때문이다.

여러 세대 직원의 다양한 기대사항은 디지털 워크스페이스 확보에 또 다른 고민거리를 더하고 있다. 나이 든 직원들은 번거로운 보안 정책과 프랙티스를 기꺼이 참아낼 수 있지만, X 세대와 밀레니엄 세대 직원들은 그렇지 않아서, IT 부서가 최신 디지털 워크스페이스에 대한 보안을 재고해야 한다는 압력이 가중되고 있다. 또한, 보안 문제는 밀레니엄 세대의 지나친 공유 성향 때문에 더욱 심각한 문제가 되고 있다. 단순히 P2P(Peer-to-Peer) 피드백을 원하는 경우 깃허브(GitHub) 같은 사이트에서 IP를 공유하는 것처럼 의도치 않게 기업 보안의 경계를 넘을 수 있다.

그 결과 디지털 워크스페이스의 자유와 전통적인 보안 프레임워크 간의 단절 심화로, 전반적인 업무 경험을 향상시키기보다는 방해가 되는 경향이 있다. 시트릭스 수석 부사장 겸 CISO인 스탠 블랙은 "지금까지는 가정에서의 개인과 직장에서의 개인이 존재해 왔는데, 이 두 가지 환경을 혼합할 수는 없었다"면서 "우리는 사람들이 방해를 받지 않고 빠르고 쉽게 일을 할 수 있도록 하고 나머지 생활도 누릴 수 있도록 해야 한다"고 말했다.

그림 2 | 멀티 디바이스 지원에 있어서의 보안 과제

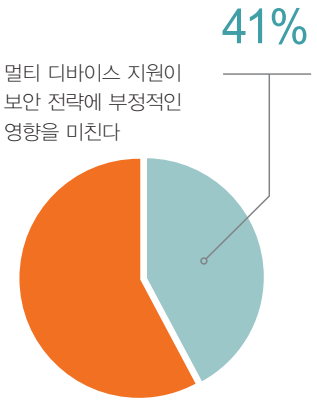
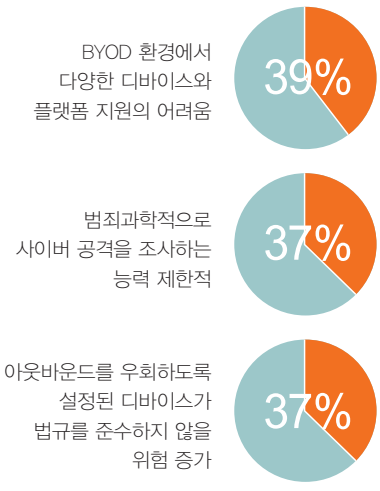


그림 3 | 세부 과제



사람 지향적인 보안 패러다임

이런 과제를 해결하기 위해 디지털 워크스페이스는 보안에 대한 새로운 사고 방식을 필요로 한다. 디지털 워크스페이스는 오래된 디바이스 중심 모델보다는 사용자를 보안 프레임워크의 중심에 두는 사람 중심의 접근방식으로 진화해야 한다.

이 새로운 보안 모델은 상황별 액세스와 보안 제어를 제공하기 위해 인공지능, 머신러닝, 가상화, 분석 같은 기술을 사용해 사용자와 사용자의 행동에 대해 알려진 모든 것을 수집하고 조합한다. 이를 통해 올바른 수준의 보안을 제공하면서, 사용자 경험에는 방해가 되지 않도록 보장한다. 사용자 행태 분석을 적용함으로써 새로운 보안 패러다임은 진일보하는데, 행동 패턴을 모니터링하고 정교한 알고리즘으로 이를 분석해 잠재적 위협이나 남용 징후 같은 이상 징후를 감지하고 위험을 완화하기 위해 사전 예방적 대응을 시작한다.

새로운 보안 모델은 ID와 액세스 제어를 비즈니스 프로세스를 소유하고 있는 비즈니스 담당자에게 넘겨줘 보안 관점에서 요구되는 사항을 더 잘 규정하도록 한다. 예를 들어, 사용 중인 디바이스, 액세스 위치 그리고 해당 시점에서 사용자 활동 같은 다른 요인을 고려하는 것은 추가적인 맥락화(Contextualization)과 개인화를 제공해 사용자 경험의 유연성을 방해하지 않고 보안을 강화한다.

시트릭스 CTO 크리스찬 레일리는 "IT는 더 이상 병목현상이 아니며, 누가 무엇에 접근해야 할지를 결정하는 대부도 아니다"라며, "보안은 동적으로 조정되며 그러한 상황 전반에 걸쳐 적절한 수준으로 경감된다"고 강조했다.

직원들은 안전하지만 방해받지 않고 작업할 수 있는 유연하고 고도로 개인화된 디지털 워크스페이스를 요구하고 있다. 현대 인력의 필요사항을 수용하기 위해 IT 조직은 강제적인 보안 모델에서 몰입을 조장하고 혁신과 생산성을 높이는 사람 중심 모델로 전환해야 한다.

Tech Guide

디지털 트랜스포메이션에서 보안의 역할

Doug Drinkwater | CSO.com

디지털 트랜스포메이션(Digital Transformation)은 프로세스와 서비스를 디지털화하여 고객 서비스 제공부터 공급망 파트너와의 프로세스 개선까지 비즈니스가 보다 민첩하고 효율적으로 운영될 수 있도록 하는 것이다. 마케팅팀은 제품 홍보 방식을 바꾸고 싶고, HR 부서는 채용 프로세스를 개선하고 싶으며, IT팀은 온라인 서비스를 즉석에서 자동화하고 싶다.

디지털 트랜스포메이션 프로젝트를 시작하기 위해 조직은 계획과 전략 단계에서 인력, 프로세스 및 기술을 합쳐서 데이터 분석, 사물 인터넷(Internet of Things), 모바일 그리고 소셜 같은 기술이 차이를 만들어 낼 수 있는 부분을 확인해야 한다. 하지만 이 과정에서 정보 보안은 너무 쉽게 배제되고 있다.

보안 없는 디지털 트랜스포메이션의 위험

IT와 비즈니스가 시장 출시 속도를 향상시키기 위해 애자일(Agile)과 데브옵스(DevOps) 같은 이니셔티브를 신속하게 처리함에 따라, 이후 보안의 역할은 위험과 보안에 미치는 연쇄적 영향에 대한 질문으로만 국한되었다. 간단히 말해, 디지털 트랜스포메이션은 고객(또는 이와 동등한 대상)에게 가치를 부여하는 데 너무 몰두한 나머지, 핵심 보안 기능에 대한 영향을 거의 고려하지 않고 있다.

데이터 침해와 취약점 수치가 증가함에 따라 일각에서는 보안 없는 디지털 트랜스포메이션이 조직을 더 큰 위험에 빠뜨리고 있다고 지적한다. 가트너는 최근 2020년에는 디지털 비즈니스의 60%가 디지털 위협 관리에 대한 보안팀의 무능으로 커다란 서비스 장애를 겪을 것으로 전망했다. 가트너는 "디지털 비즈니스는 기존 비즈니스보다 빠른 속도로 움직이며, 최대한의 통제를 위해 설계된 기존의 보안 접근방식은 디지털 혁신의 새로운 시대에 더 이상 효과가 없을 것"이라고 밝혔다.

디지털 트랜스포메이션 때문에 지연되는 보안

기존 디지털 트랜스포메이션 프로젝트는 뒤늦은 보안이나 보안 부재로 실패하는 경우가 많다. 델과 디멘셔널 리서치(Dimensional Research)의 연구에 따르면, 비즈니스 임원들은 보안팀의 개입으로 인해 디지털 트랜스포메이션이 방해를 받거나 무산될 수 있다는 것을 가장 큰 우려사항 중 하나로 꼽았다.

하지만 흐름이 바뀌고 있음을 나타내는 작은 조짐들이 있다. 기록적인 수의 침해, 버그가 많은 IoT 소프트웨어 그리고 EU의 GDPR 때문에 강화된 것으로 보

이는 설계 단계부터의 보안 움직임은 전반적으로 보안의 비중이 커지고 있음을 보여준다. CCS 인사이트에서 기업 리서치 프랙티스를 맡고 있는 애널리스트 닉 맥콰이어는 "오늘날 우리는 보안이 모든 조직과 CIO의 최우선 의제가 되었다고 본다"고 말했다.

맥콰이어는 "미국과 유럽 전역에서 조사 대상 기업의 70% 이상이 자사의 보안 예산이 증가하고 있다고 밝혔으며, 절반 정도는 향후 몇 년 안에 사이버 공격을 당할 가능성이 높다고 말했다. 데이터 보안은 디지털 워크스페이스에서 가장 중요한 투자 우선순위이며, 종종 디지털 트랜스포메이션 전략에서 가장 두드러진 부분인 모바일 애플리케이션을 구축하는 데 필수적인 요소이다"라고 설명했다. 또 "확실히 달라진 점은 오늘날 보안이 핵심 기술 우선순위일 뿐만 아니라 비즈니스 우선순위가 되었다는 것이다"라고 덧붙였다.

이 견해에 모든 사람이 동조하는 것이 아니다. J. 골드 어소시에이츠의 대표 애널리스트 잭 골드는 "많은 기업들과 대화한 경험에 따르면, 보안에 대해 입에 발린 말을 하고 있지만 보안이 디지털 트랜스포메이션 프로세스의 주요 구성요소는 아니다"라고 지적했다. 중요하다고 생각은 하지만 진정한 의미를 모르고 있는 CEO도 문제이지만, 여러 공급업체의 다양한 솔루션을 연결하는 이른바 "기술적 짜깁기"도 과제라는 것. 골드는 "이 모든 것을 한데 모으는 것은 정말 어렵다"고 강조했다.

맥콰이어는 기업이 기술 진보를 따라잡기 위해 고군분투하고 있다는 것을 인정한다. 맥콰이어는 "많은 기업이 그저 급격한 기술 변화를 따라가지 못하고 있을 뿐이다. 맬웨어, 랜섬웨어, 피싱 공격이 빠르게 증가하면서 위협 지형도가 우리 눈앞에서 변하고 있다"고 말했다. 또 "GDPR의 형태로 상당한 규제 변화가 일어

나고 있는데, 이는 새로운 압력을 가중시키고 있다. 보안과 프라이버시 프로세스가 취약한 기업은 재정적으로 책임을 져야 한다"고 덧붙였다.

이에 더해 대부분 기업에서는 보안 인재가 부족하고, 다양한 디바이스와 클라우드 앱이 혼재하는 환경에서 업무 정보에 액세스하는 직원들을 제대로 보호하지 못하는 기존의 복잡한 보안 기술을 운영하고 있다는 사실이 결합되어, 보안 시장이 호황을 누리고 있다. 맥콰이어는 "클라우드 액세스 보안, 사용자 행태 분석 및 머신러닝, IDaaS(Identity as a Service), 이중인증, 모바일 위협 방어 등의 새로운 보안 기술이 등장하는 이유가 여기에 있다. 이들 기술은 점점 더 많은 데이터를 보호 장벽 외부에 저장해야 하는 기업을 보호하기 위한 최신 보안 스택의 새로운 계층을 보여주고 있다"고 말했다.

디지털 트랜스포메이션에서 보안의 역할

디지털 트랜스포메이션에는 여러 단계가 있지만, 보안이 자연스럽게 들어갈 부분이 어디인지는 불분명하다. 알티미터 그룹(Altimeter Group)의 디지털 트랜스포메이션 6단계를 기준으로 하면, 보안은 모든 단계에, 아니면 최소한 후반 단계에라도 넣을 수 있고, 넣어야 한다.

CISO는 디지털 트랜스포메이션 프로세스 전체에 걸쳐 보안을 적용하려는 듯하다. 예를 들면, 최근 로스앤젤레스시 CISO인 티모시 리는 디지털 트랜스포메이션을 수용하는 CISO는 조직이 급변하는 글로벌 시장에 적응하기 쉽도록 도움을 줄 수 있다고 말했다. 리는 "우리의 일은 단순히 기회와 위험을 관리하는 것만이 아니다. 우리의 역할은 사이버 보안을 비즈니스 원동력이자 디지털 트랜스포메이션의 기반 중 일부가 되도록 하는 것이다"고 말했다.

한편, 제록스의 CISO 앨리사 존슨(전 백악관 부 CIO)도 CISO는 "보안을 설계 프로세스의 제일 앞에 두어야 한다"며, 개혁을 가로막고 있다면 바로 그런 CISO가 "회사의 경쟁력과 대응 능력을 저해할 수 있다"고 말했다.

듀오 시큐리티(Duo Security)의 전 CISO 겸 최고 개인정보보호 책임자를 역임하고, 현재 대표 애널리스트인 덕 코플리는 CISO는 IaaS, 마이크로서비스, API가 지배하고 있는 정보화 시대의 새로운 '구성 요소'에 문화적으로나 기술적으로 대응해야 한다고 제시함으로써 디지털 트랜스포메이션이 처한 진퇴양난 상황을 잘 표현했다. 코플리는 "CISO나 이와 유사한 역할을 하는 사람에게 조직에서 새로운 비즈니스 모델과 새로운 기술을 채택할 수 있도록 하는 것이 새로운 표준이며, 이것이 CISO의 역할에 대한 기본 요건이다"라고 강조했다.

보안이 개입해야 할 단계에 대해 맥콰이어는 맨 처음부터 개입해야 한다는 데 의견을 같이 했다. 맥콰이어는 "보안은 모든 디지털 트랜스포메이션 계획의 선두에 있어야 한다, 맨 처음에 있는 기획과 설계 단계부터 있는 것이 이상적이다. 설계 단계에서 보안을 염두에 두지 않거나 처음부터 맞는 원칙을 적용하지 않아서 프로젝트가 지연되거나 실패하는 경우를 너무 많이 본다. 따라서 보안팀이 마지막에 개입하면, 프로젝트 전체에 적신호가 내려진다"며, "보안이 처음부터 디지

털 트랜스포메이션의 일부가 되도록 한 기업들은 장기적으로 성공할 뿐 아니라 오늘날의 환경에서 시장에 더 빨리 진출하는 것을 봐 왔다"라고 말했다.

디지털 트랜스포메이션을 위한 새로운 보안 솔루션

보안에서는 대응이 예방만큼 중요하다고 알려진 디지털 시대에 맥콰이어가 보안을 강화할 신기술의 수요를 감지한 것은 놀랄 일이 아니다. 그는 "장벽이 사라짐에 따라 보안 요건이 변화하고 있다"고 말했다. 맥콰이어는 많은 경우 서로 말을 하지 않으며, 주로 방어적인 보안 제품을 복합적으로 혼용하고 있는 고객들로부터 탐지와 대응도 가능케하는 보다 통합되고 완전한 보안 플랫폼을 요구하는 쪽으로 초점이 바뀌고 있다고 분석했다.

맥콰이어는 "보안 대응 방안이 방어에서 탐지, 대응으로 빠르게 변화하면서 인프라 전반에 대한 가시성의 중요성이 커졌다. 온프레미스와 클라우드에 있는 디바이스, 네트워크, 그리고 앱 전반에 대한 가시성이 필요하다"고 강조했다. 또 "이는 기업이 더 넓은 공격 표면에서 위협을 탐지할 수 있어야 하기 때문에 엄청난 변화"라고 덧붙였다.

Tech Guide

디지털 트랜스포메이션이 IT 인력에 미치는 영향

Zeus Kerravala | CIO.com

디지털 트랜스포메이션의 확산과 함께 다양한 기술의 필요성 또한 커지고 있다. 새삼스러운 일은 아니지만, 이번에는 변화가 너무 빠르게 일어나고 있다.

애널리스트가 되기 전에 필자는 기업 IT 부서에서 일했고, 기술 발전이 사람들에게 미칠 수 있는 영향을 직접 목격했다. 필자는 전세계의 90%가 IBM 메인프레임 상에서 운용되고 있던 시기에 유닉스와 윈도우 관리자로 경력을 시작했다. 필자는 100명 이상의 메인프레임 관리자가 있는 회사에 고용된 네 번째 개방형 시스템 담당자였다. 3년 만에 윈도우/유닉스 담당자는 200명으로 늘어났고, 거의 모든 메인프레임과 기존 메인프레임 담당자는 새로운 세계로 도약하지 못했다.

VoIP가 등장했을 때도 비슷한 일이 있었다. "레거시(Legacy)" 팀은 네트워킹을 이해하지 못했고, 직원들은 빠르게 새로운 인재로 교체되었다. 이런 상황은 여러 가지 다른 기술 시장에서도 반복해서 일어났고, 우리는 디지털 트랜스포메이션의 부상과 함께 이런 일을 다시 겪고 있다.

디지털 트랜스포메이션이 IT 부서에 미치는 영향

하지만 이번에는 IT에 미치는 영향이 다를 것으로 본다. 기술이 변화하고 있을 뿐만 아니라, IT 통제 대상 자체가 달라졌다. 필자가 IT에 몸담고 있을 때, 모든 기술은 IT가 보유하고 있었다. 글자 그대로 모든 것이었다. 여기에는 엔드포인트, 운영체제, 조달, 애플리케이션 그리고 보안이 포함되었다. 오늘날, 더 많은 통제 대상이 LoB(Line of Business)로 옮겨감에 따라, 패러다임이 바뀌었다. IT의 역할은 회사 기능보다는 비즈니스를 지원하는 서비스 조직이 되었다.

이런 IT의 역할 변화는 기술 전문가에게 여러 가지 새로운 기술을 배울 것을 요구한다. 다음은 현재 인재 부족을 경험하고 있거나 가까운 미래에 발생할 것으로 예상하는 몇 가지 분야에 대한 예이다.

데이터 분석. IT 인프라는 엄청난 양의 데이터를 생성하고 있다. 이런 데이터는 LoB가 업무를 조정하는 데 도움이 되는 비즈니스 통찰력으로 변환되어야 한다.

머신러닝/인공 지능. 데이터 분석과 마찬가지로, 데이터로부터 통찰력을

생성하는 프로세스이기는 하지만, 전혀 다른 방식으로 수행된다. 수작업으로 "단편적 데이터를 가지고 어떤 결론을 도출하기"보다는, 머신이 그런 일을 하도록 학습시키는 것이 더 빠르고 더 효율적이다.

비즈니스 연락 담당(Business Liaison). 현업 부서는 IT 자금을 지출하는 데 대해 더 많은 통제권을 요구하고 있다. 그렇지만, 대부분의 현업 담당자는 자신들이 어떤 것을 모르고 있는지를 정말로 모르고 있다. IT 전문가는 모든 요건이 충족되고 있는지를 확인하기 위해 비즈니스에 대해서 더 배운 다음, 이런 요구사항들을 클라우드 서비스나 다른 기술로 매핑하는 데 도움을 줘야 한다.

사이버 보안. 늘 인기있는 분야였지만, 보안 전문가가 해야 할 일도 변하고 있다. 방화벽과 IPS를 프로그래밍하는 것보다, 비즈니스 위험을 이해하고 이를 최소화하는 방법을 이해하는 것이 중요하다. 회사 책임자들과의 긴밀한 조율이 필요하다.

소프트웨어 기량. 이 주제에 관해서는 정의를 분명히 하고 싶다. 모든 사람이 프로그래머가 되어야 한다는 수사를 덧붙이고 싶지 않다. 사실이 아니기 때문이다. 그러나 모든 엔지니어는 클라우드 서비스를 포함해서, 소프트웨어 작업에 익숙해야 한다. 이는 오케스트레이션 도구를 사용해서 작업하고, 기본적인 스크립팅을 이해하고 있으며, API 호출을 하는 것을 의미한다. 명령줄에서 독수리 타법으로 입력하는 것은 과거의 유물이어야 하며 최신 소프트웨어 기술로 대체되어야 한다.

기술 혁신을 위해 일상적인 작업을 없애라

CIO는 이러한 변화의 인간적인 측면을 염두에 두고 현재의 IT 전문가 그룹이 자신의 역량을 전환할 수 있도록 보장해야 한다. 그러나 IT 구현과 관련된 많은 일상적인 작업을 없앨 수 있는 방법을 먼저 찾아내지 않으면 안된다. 자동화는 확실히 도움이 될 수 있지만, 그것만이 유일한 해결책은 아니다.

또 다른 접근 방식은 클라우드를 활용해 IT 운영 방식을 완전히 바꾸는 것이다. 예를 들어, 지스케일러(Zscaler) 같은 서비스를 사용하여 보안을 간소화할 수 있다. 다수의 사내 보안 장비를 관리하는 대신, 그런 기능의 일부 또는 전체를 클라우드에서 수행할 수 있으므로, 보안 팀은 기술을 전환하기 위해 필요한 시간을 확보할 수 있다.

비즈니스가 빠르게 움직여야 한다는 것은 누구나 알고 있다. 그것이 디지털 시대의 성공 비결이기 때문이다. 그렇지만, CIO는 IT 직원을 어떻게 이끌어야 할지도 고려해야만 한다. 옛날 방식으로 하지만 더 빠르게 일을 하려 시도하는 것은 효과가 없을 것이다. 클라우드를 활용하는 것처럼 새로운 운영 방법을 찾는 것은 기업뿐 아니라 직원들에게도 성공을 가져다줄 수 있다.

Technology Review

"생산성부터 클라우드, 보안까지" 차세대 업무 환경의 조건과 Citrix Workspace

자료 | Citrix

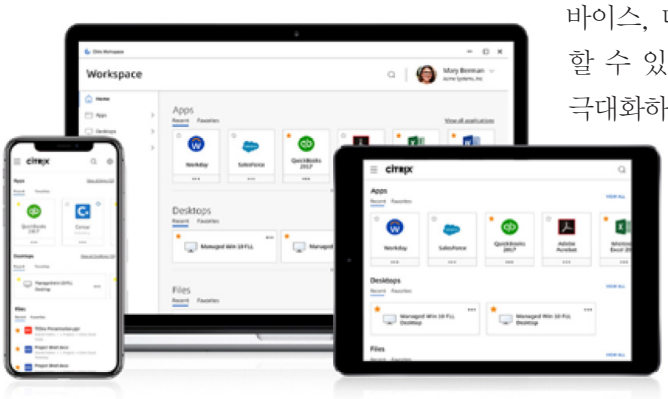
신세대 직원은 자신에게 친숙한 디바이스와 애플리케이션을 그대로 사용하면서도 끊김없는 매끄러운 경험을 기대한다. 또한 이들 디바이스와 애플리케이션이 네트워크 조건에 관계없이 잘 동작하기를 기대한다. 현재 연결된 네트워크의 대역폭이 어떤 지 정확하게 모를 수도 있고, 아니면 신경 쓰지 않는 것일 수도 있다. 최종 사용자는 그저 원하는 것이 제대로 동작하기만을 바란다.

하지만 이를 지원해야 하는 IT는 비즈니스의 요구사항을 지원하고 업무 생산성을 향상할 수 있는 방식으로 이런 엄청난 사용자 경험을 제공해야만 한다. 즉 최종 사용자에게 기업의 자원에 액세스할 수 있고 협업할 수 있는 유연성을 제공해야 한다. 한편으로는 인프라를 민첩하게 관리해 신속하고 비용 효율적으로 확장할 수 있어야 한다.

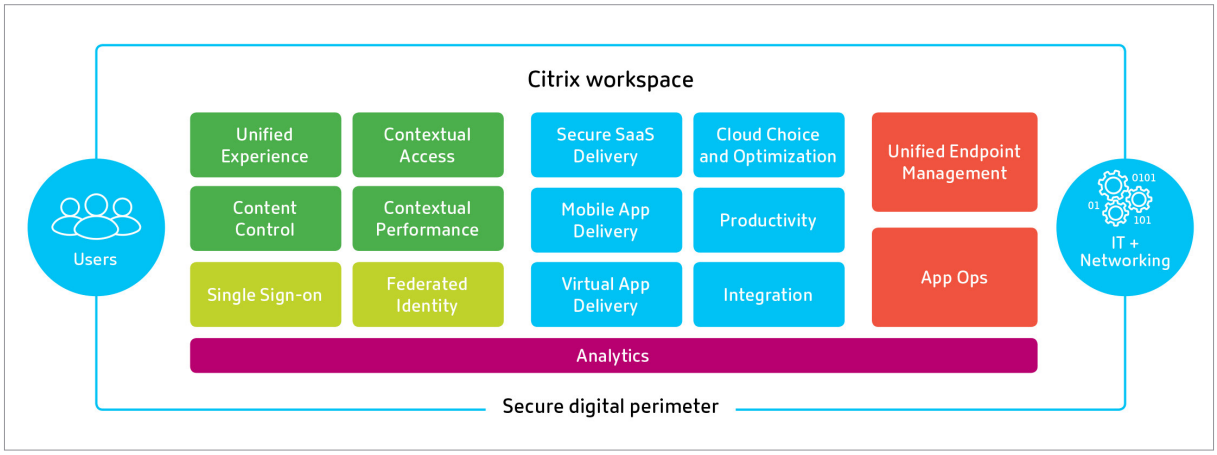
디지털 워크스페이스는 일상적인 작업의 속도를 높이고 최적화해 준다. 이메일 첨부파일을 열고, 다른 저장소에 있는 파일에 액세스하는 작업을 빠르고 간편하게 수행할 수 있는 것은 물론, 애플리케이션을 열고 서로 다른 디바이스 간을 전환하는 것도 쉽고 편리해진다.

클라우드는 디지털 워크스페이스를 완성하는 핵심 축이다. 선택권이 많을수록 클라우드 트랜스포메이션을 완성할 수 있다는 자신감도 커지는 법. 따라서 온프레미스부터 퍼블릭 클라우드, 프라이빗 클라우드까지 다양한 딜리버리 모델의 조합을 수용할 수 있는 유연성이 필요하다. 이를 통해 사용자가 선호하는 어떤 모바일 디바이스라도 지원할 수 있으며, 더 많은 장소에서 업무를 수행하고 작업한 파일을 저장하고 액세스할 수 있는 위치도 더 많이 제공할 수 있다. 당연히 동료와의 협업도 끊김없이 매끄럽게 진행할 수 있다.

하지만 선택권이 늘어나는 만큼 통제에 드는 비용도 증가한다. 사용자부터 디바이스, 데이터, 워크로드, 네트워크까지 중앙에서 관리할 수 있어야 하며, 이를 위해서는 기존 투자의 효과를 극대화하는 한편, 현대화도 추진해야 한다. 디지털 워크스페이스는 IT 부서에 더 많은 선택권을 가져다주는 한편, 관리를 최적화해 디지털 환경으로의 매끄러운 전환을 가능하게 한다. 이를 통해 기존 비즈니스를 혼란에 빠뜨리지 않고도 디지털 트랜스포메이션을 완성할 수 있다.



이제 기업 보안팀은 언제 어디서나 접속하



는 디바이스를 공개 네트워크를 통해 지원하면서도 기업 데이터 자산을 보호해야만 한다. 보안에 대한 우려는 애플리케이션과 데이터를 중앙 데이터센터에 저장하는 가상 데스크톱을 사용하는 것으로도 일부 해소할 수 있다. 하지만 어디까지나 부분적인 해법일 뿐이다. 직원들은 여전히 SaaS 애플리케이션에 접속해야 하고 안전하지 않은 웹사이트를 방문한다. 또한 보안 모델은 민감한 데이터를 휴대형 저장장치에 복사하거나 피싱 이메일을 여는 등의 위험한 행동도 감시해야 한다. 이들 행위는 기업을 데이터 절취나 기타 컴플라이언스 위험에 노출시킬 수 있다.

장벽을 보호하는 구식 접근법은 엔드 투 엔드 보안을 보장해야 한다는 요구에 밀려나고 있다. 이제 날로 증가하는 디바이스와 서비스를 지원하면서도 앱과 데이터를 보호하고 사용자 액세스를 통제해야 한다. 디지털 워크스페이스는 공통의 위협에 대한 한층 강화된 보안 통제를 구현한다. 여기에는 악성코드나 DoS 공격은 물론 피싱공격이나 사용자 오류로 포함한다.

완전히 통합된 디지털 업무 공간을 통해 비즈니스 생산성 향상

Citrix Workspace는 시트릭스의 디지털 워크스페이스 관련 핵심 솔루션을 하나로 통합한 것으로, 조직 내 모든 사용자에게 안전한 디지털 업무 공간을 제공한다. 완벽하게 통합된 업무 공간을 통해 어디에서든 앱, 데스크톱 및 데이터에 안전하게 액세스할 수 있다. Citrix Workspace를 사용하면 기업 자체의 SaaS 및 웹 앱을 사용하는 것보다 더욱 강력한 IT 보안 및 제어 기능을 유지할 수 있으며, 특히 디바이스, 클라우드, 네트워크에 대한 선택권을 완벽하게 보장한다.

Citrix Workspace를 구성하는 주요 솔루션은 다음과 같다.

앱 및 데스크톱 딜리버리. 현재 전 세계 1억 명이 넘는 사용자가 사용하고 있는 업계 최고의 가상화 솔루션인 Citrix Virtual Apps 및 Citrix Virtual Desktops를 제공한다. Citrix Workspace를 사용하면 윈도우 앱 및 데스크톱뿐만 아니라 모든 유형의 디바이스 및 네트워크를 통해 리눅스, 웹 및 SaaS 애플리케이션에 안전하게 원격 액세스할 수 있다.

엔터프라이즈 모빌리티 관리. Citrix Endpoint Management 기술을 통해 하나의 포괄적인 솔루션에서 모바일 디바이스 관리(MDM), 모바일 애플리케이션 관리(MAM), 모바일 콘텐츠 관리(MCM), 보안 네트워크 게이트웨이 및 엔터프라이즈급 모바일 생산성 앱에 대한 모든 액세스 권한을 얻을 수 있다.

파일 동기화 및 공유. Citrix Workspace는 전체 IT 컨트롤을 유지하면서 모든 기업 및 개인용 모바일 디바이스에서 엔터프라이즈급 데이터 서비스를 제공한다. Citrix Content Collaboration을 사용하여 모든 기기에서 파일을 액세스하고, 동기화하고 안전하게 공유할 수 있다. 오프라인 액세스는 이동 중에도 직원의 생산성을 끌어 올린다.

지점 네트워킹 및 WAN. Citrix Workspace에는 애플리케이션 가속화, 전송 데이터 감소 및 프로토콜 제어를 제공하여 WAN에서 애플리케이션을 최적화하는 Citrix SD-WAN WANOP 에디션이 포함되어 있다.

보안 원격 액세스. Citrix Workspace에는 Citrix Gateway가 포함되어 있어 원격 액세스 인프라를 통합하고 데이터센터, 클라우드 또는 SaaS로 제공되는 모든 애플리케이션에서 싱글사인온을 제공한다.

분석 및 통찰력. Citrix Analytics는 인공 지능 및 머신러닝을 사용하여 Citrix Workspace 전반의 사용자 동작을 기반으로 위협을 탐지하고 분석한다. 사용자, 기기, 네트워크, 앱 및 파일에서 데이터를 수집하고 상호연관시키는 어려운 작업을 자동화한다. Citrix Analytics는 악의적인 내부자의 데이터 유출을 방지하고, 의심스러운 랜섬웨어 활동을 발견하고, 비준수 기기를 탐지하는 등의 작업을 지원하도록 설계되었다.

Case Study

아시아 최대 복합 리조트
제주신화월드 VDI 도입사례

자료 | Citrix

제주신화월드는 아시아 최대 복합 리조트로, 제주신화역사공원 내 조성되어 여러 대형 호텔과 카지노, 대규모 쇼핑 및 다이닝 시설, 고급 스파, 컨퍼런스 시설 등을 갖추고 있다.

핵심 비즈니스의 성장을 지원하는 강력한 디지털 토대

제주신화월드는 장기적 성장을 위해 VDI(Virtual Desktops Infrastructure) 솔루션인 Citrix Virtual Apps & Desktops를 선택했다. 정식 개장과 함께 대표부터 신입 직원까지 약 2,000명의 직원이 VDI 환경에서 일할 수 있도록 IT 인프라 환경을 구축했다.

처음부터 VDI 환경을 구축한 것은 보안과 효율성 때문이다. 제주신화월드의 사업은 고객 데이터가 중요하고, 그만큼 모든 직원에게 보안을 강조하고 있다. VDI는 모든 데이터를 직원의 PC가 아니라 중앙의 서버팜에 저장한다. 모든 데이터를 중앙에서 관리하기 때문에 외부에서 데이터에 접근하는 것과 직원이 무단으로 데이터를 복사하는 것을 통제할 수 있다. 그만큼 고객의 데이터가 유출될 위험을 줄일 수 있다.

VDI는 기업 IT 관리자의 고민도 효율적으로 해결할 수 있다. PC의 신규 설치와 교체, 업그레이드, 소프트웨어 문제 해결 등을 IT 담당자가 직접 찾아가 처리하는 기존 방식으로는 2,000명을 지원을 효과적으로 지원할 수 없다. 물리 PC 자체가 없는 VDI 환경은 이런 사용자 PC 지원이 서버팜에서 이루어지기 때문에 업무 효율을 극대화할 수 있다. 또한 장기적으로도 데이터 및 보안 중심의 구조는

상당한 비용 절감은 물론 비즈니스 연속성 강화로 이어질 수 있다.

첫 단계로는 필수 데이터센터 인프라 및 프라이빗 클라우드 환경을 구축했다. 마이크로소프트 애저 클라우드에서 실행하는 마이크로소프트 오피스 365를 Citrix Virtual Apps & Desktops에 연결해 하이브리드 클라우드 기반 업무 환경을 구현했다.

그 결과, 현재 제주신화월드는 중요 데이터를 내부 데이터센터에 안전하게 저장하는 동시에 효율성이 뛰어난 외부 협업 도구를 사용하고 있다. 데이터는 직원 PC가 아닌, 중앙 서버 팜으로 저장하고 제어한다. 당연히 데이터의 외부 접근 및 직원의 무단 복제는 금지된다.

효율적 운영 및 비용 절감

Citrix Virtual Apps & Desktops는 제주신화월드의 신입 사원 관리, 구형 하드웨어 교체, 새 프로그램 설치, 시스템 업그레이드 등 업무 효율성 또한 크게 향상시켰다.

고정성이 큰 다른 VDI 환경과는 달리, 제주신화월드의 Citrix Virtual Apps & Desktops는 최적의 유연성을 확보하도록 설계되었다. 예를 들어 직원이 유용한 앱을 설치하여 작업 효율성을 더 높일 수 있다. 회사 외부에서 작업하는 경우, 직원은 가상 데스크톱에 접속하기만 하면 된다.

더 나아가 Citrix Virtual Apps & Desktops는 물리적 수명에 따른 구형 PC 교체 필요성도 크게 줄었다. 그리고 데이터 보안이 훨씬 더 강화되었다. Citrix Virtual Apps & Desktops에서 진행한 작업은 모두 회사의 중앙 서버에 저장되어, 무단 접근 및 정보 유출을 차단했다. 숙박 기록 및 카지노 시설 이용 내용을 포함한 매우 민감한 고객 데이터를 다루는 제주신화월드로서는 이 부분이 특별히 더 중요하다. 제주신화월드 김창수 시니어 IT 디렉터는 "Citrix Virtual Apps & Desktops 솔루션에 매우 만족한다. IT 관리 효율성이 크게 높아졌고, 비용 절감이 기대된다"고 밝혔다.

제주신화월드

- **분야** : 엔터테인먼트, 카지노, 레저
- **규모** : 직원 2,000명 이상
- **주요 이점** : 데이터 보안 강화 / 운영 효율성 향상 / 비용 절감
- **고객사 프로필** : 제주신화월드는 아시아 최대 규모의 복합 리조트로, 여러 메이저 호텔과 카지노, 대형 쇼핑 및 다이닝 시설, 고급 스파, 컨퍼런스 시설 등을 갖추고 있다.
- **소프트웨어 및 서비스** : Citrix Virtual Apps & Desktops 7.11 / Microsoft Office 365