금융서비스 업계에서 고객 편리성과 사이버 보안 위협 간의 균형 유지

금융서비스를 안전하게 보호하는 방법

개요

고객 수요가 증가하고 클라우드 효율성이 향상됨에 따라, 혁신적인 금융서비스 애플리케이션의 개발이 가속화되는 동시에 잠재적인 보안 취약점들이 노출되고 있습니다.

민감한 금융 데이터는 공격자들에게 매우 큰 가치가 있기 때문에 금융서비스 업체들은 안전한 애플리케이션 개발과 배포를 보장하는 동시에 거버넌스, 리스크 및 규정준수 관리를 위한 모든 예방 조치를 취해야 합니다.

사이버 범죄자들이 COVID-19 팬데믹 기간 동안 높아진 디지털 의존도와 잠재적으로 취약한 서비스의 사용을 악용하면서, 개인과 기업에 대한 보안이 더욱 시급해졌습니다.[1]

금융서비스 기관들이 진화하는 사이버 보안 위협과 고객 편리성 간의 균형을 맞추려면 어떻게 해야 할까요? 시장 출시 기간을 단축하고 유지하려면, 전문 리스크 관리 인력과 첨단 솔루션들로 지원되는 안전한 애플리케이션 개발 환경이 필요합니다.

모든 것은 발전된 애플리케이션 방법론에서 시작됩니다. 이는 적합한 수준의 자동화와 즉시 구축 가능한 인프라를 활용함으로써 금융서비스 애플리케이션의 개발 및 배포 단계에서 보안과 성능을 극대화해야 한다는 것을 의미합니다.

금융서비스 분야의 보안 위협 현황. 대처 방법

금융서비스 산업은 주요 인프라를 손상시키고 계좌 소유자의 개인식별정보(PII) 등과 같은 귀중한 데이터에 액세스하려는 사이버 범죄자들이 노리는 대표적인 표적입니다. 점차 많은 금융 거래들이 온라인에서 실행되면서, 공격자들은 점차 교묘해진 공격을 통해 악용할 새로운 취약점을 계속해서 찾고 있습니다.

최근, 금융 분야에서 발생한 보안 사고의 대부분은 Brute Force 및 크리덴셜 스터핑(Credential Stuffing) 공격과 DDoS(Distributed Denial-of-Service) 등 2개 범주로 나눌 수 있으며, 모두 증가하는 추세입니다. 웹 공격, 멀웨어, 알려지지 않은(unknown) 공격 및 기타 공격 등은 여전히 상존하는 위협들이지만, 위세는 크게 약화되고 있습니다.[3] 그림 1은 여러 다양한 공격의 빈도가 매년 어떻게 증가하고 있는지를 보여줍니다.

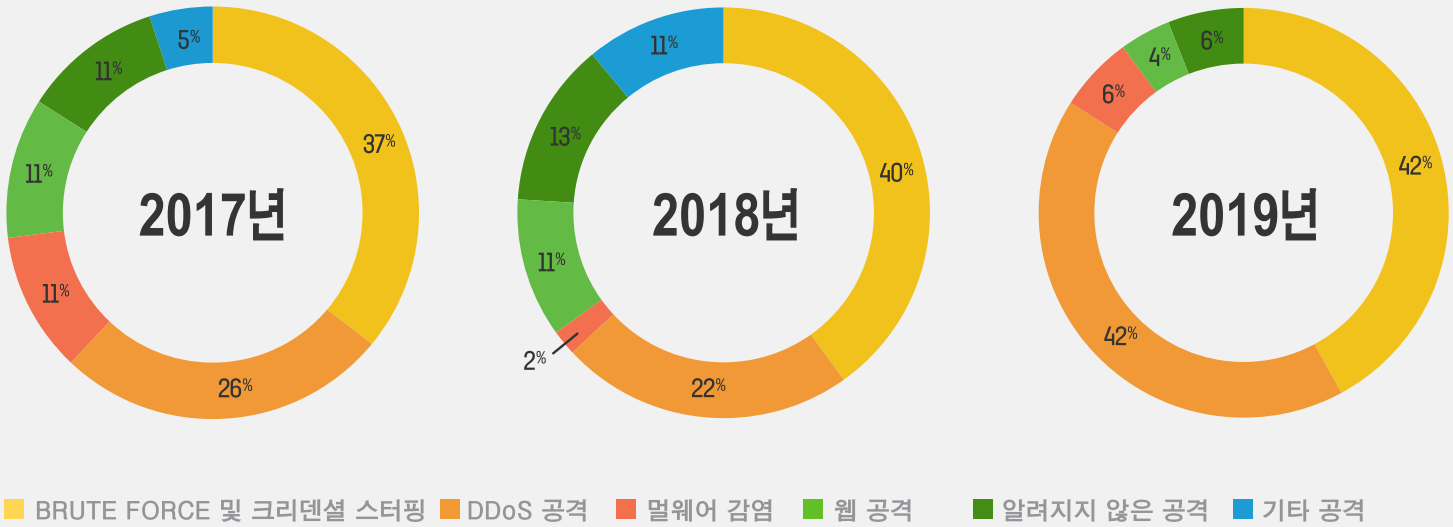


그림 1: 2017년에서 2019년까지 F5 SIRT(F5 Security Incident Response Team)에 신고된 금융서비스 업계의 보안 사고

금융 서비스 부문이 다른 산업에 비해 효과적인 보안 프로그램을 개발하고 유지하는 데 더 큰 비중을 두고 있기는 하지만, 여전히 사이버 공격과 예측 불허의 상황에 맞서며 만만치 않은 과제에 직면하고 있습니다. 예를 들어, 많은 소비자들은 대부분 유형의 공격을 막는데 매우 효과적인 방법으로 입증되었음에도 불구하고 다단계(MFA: Multi-Factor Authentication) 인증의 사용을 꺼려하고 있습니다.[4]

따라서, 예방 및 탐지 측면 모두에서 엄격한 보안 통제 체제를 구현하는 것은 금융서비스 업체는 물론, 계좌 소유자들을 위험에 빠뜨릴 수 있는 공격을 막는 최선의 방어책입니다.

모범 사례 팁

인젝션(injection) 공격은 웹 애플리케이션들에 심각한 보안 위협을 야기하지만, 이를 완화할 수 있는 효과적인 방법이 있습니다. 이 비디오를 보고 그 대처 방법을 확인해 보십시오.

클라우드의 효율성, 금융 업계 접수

디지털 혁신(digital disruption)이 금융서비스 업체들의 업무 방식을 바꾸어 놓으면서, 애플리케이션은 가장 중요한 요소가 되었습니다. 실제로, F5의 2020년 애플리케이션 서비스 현황(SOAS) 보고서: 금융서비스편에 따르면, 애플리케이션은 모든 금융서비스 업체들에게 매우 중요한 것으로 나타났습니다. 대다수의 응답자들(약 74%)은 애플리케이션이 업무에 필수적이라고 응답했으며, 26%는 애플리케이션이 자체 비즈니스를 지원하고 경쟁 우위를 높이는 데 핵심적인 역할을 수행한다고 응답했습니다.[5]

2020년에는 클라우드의 중요성이 전년도에 비해 11% 증가한 60%를 기록했습니다. 이는 금융서비스 업체들이 더 많은 애플리케이션들을 클라우드 기반 플랫폼에서 실행할 준비가 되어 있다는 것을 시사합니다.[9]

점차 업무에 중요한 애플리케이션들이 클라우드에서 실행되고 있습니다. F5 SOAS 보고서에서, 60%의 응답자들이 클라우드를 향후 2~3년 내에 전략적으로 가장 중요한 기술 트렌드로 평가했습니다. 이는 2019년의 49%에서 증가한 것입니다.[6] 이는 특히, 2~3년 전만 해도 금융서비스 업체들이 클라우드로 전환하는데 회의적이었다는 점에서 매우 주목할 만합니다.[7]

클라우드 컴퓨팅 전환의 배경은 무엇일까요? 우선, 클라우드는 반복적이고 빠른 소규모의 릴리즈를 지원하기 때문에 금융기관들은 혁신적인 신상품과 서비스를 보다 신속하게 시장에 출시할 수 있습니다.[8] 이처럼 빨라진 애플리케이션 제공 속도에 힘입어 금융서비스 업체들은 변화하는 소비자의 기대치에 발맞추고, 기존 경쟁업체 및 핀테크 스타트업들과 차별화된 경험을 제공할 수 있게 됐습니다.

점차 더 많은 금융서비스 업체들이 고객을 위한 디지털 경험을 제공하기 위해 클라우드를 수용하고 있지만, 데이터나 자금을 처리하는 백엔드 애플리케이션들에는 여전히 레거시 기술들을 사용하고 있습니다.

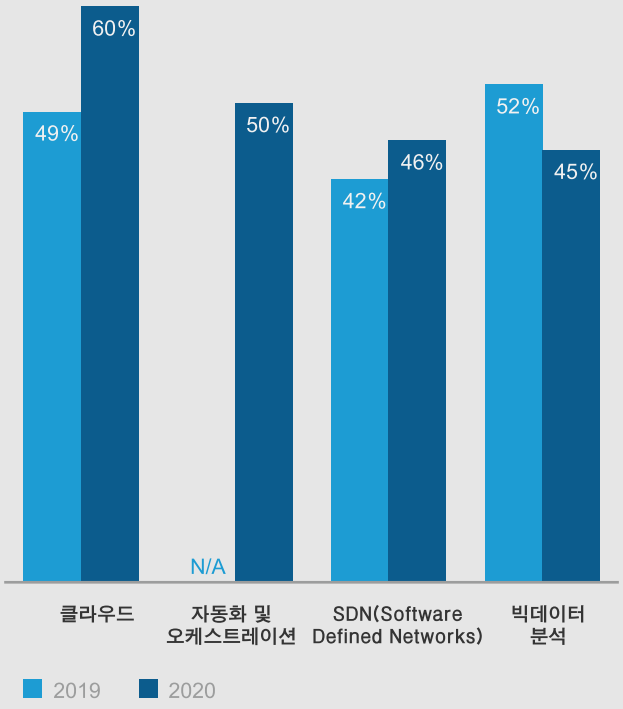
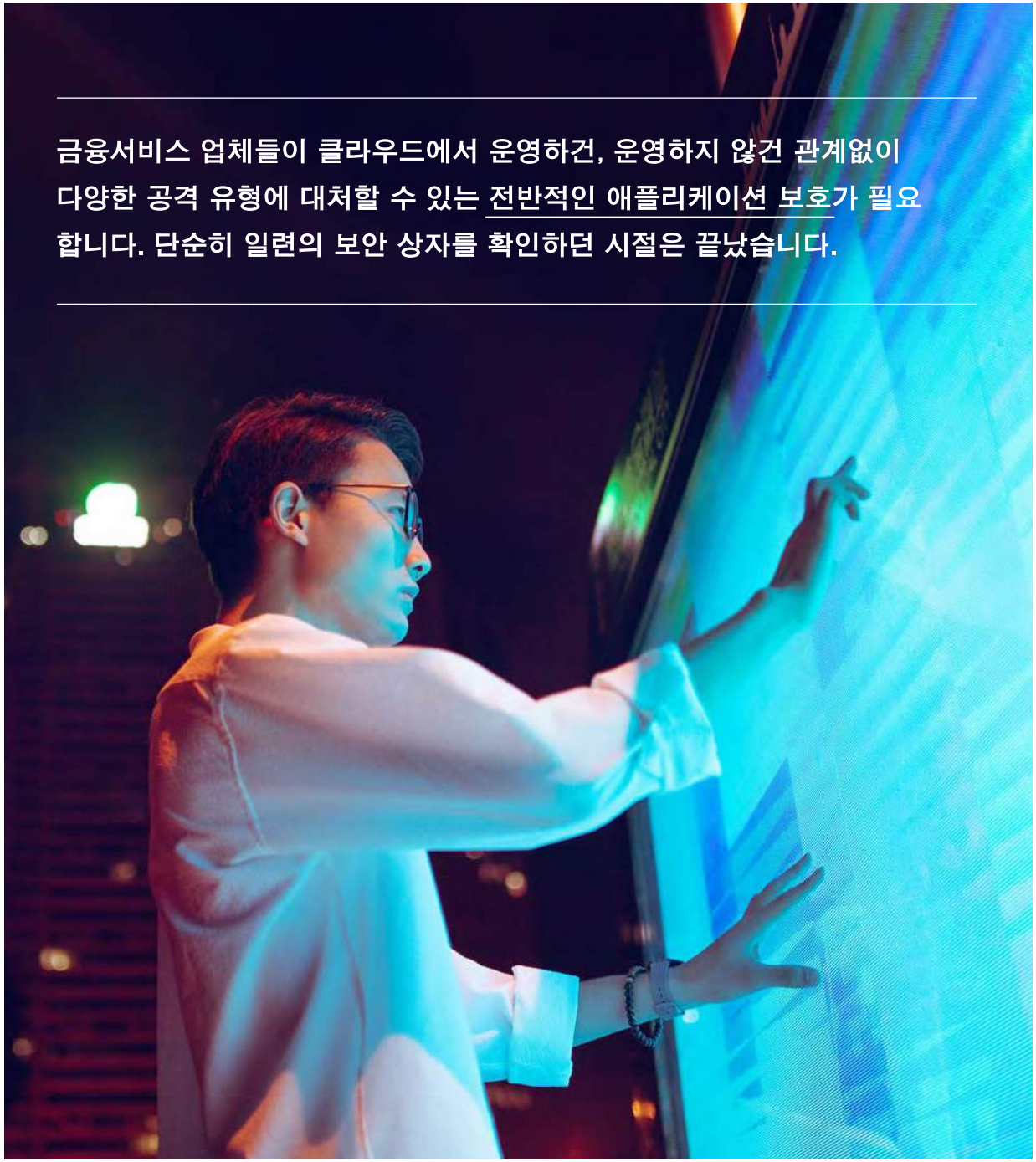


그림 2: F5의 2020년 SOAS 보고서: 금융서비스편에 조사된 향후 2~5년 내 금융서비스 업체들에게 중요해질 기술 트렌드

하지만 COVID-19 팬데믹 동안 배운 교훈은 클라우드로의 보다 전면적인 전환을 가속화하여 이를 통해 금융기관들이 혁신에 박차를 가하도록 할 수 있습니다. 예를 들어, 연방의 급여보호프로그램(Paycheck Protection Program)의 실행으로 수요가 급증하면서 수십 년 전에 개발된 노후 기술 인프라의 한계가 드러났습니다. 이에 따라, 신청자들의 불만이 고조되었으며 현대화의 시급한 필요성이 부상했습니다.[10]

금융기관들이 디지털 방식으로 운영을 고도화하는 데 모든 노력을 기울이고 더 많은 애플리케이션들을 클라우드로 전환함에 따라 보안은 최우선 순위가 되어야 합니다. 널리 만연한 보안 위협에 맞서 클라우드 또는 데이터센터의 모든 애플리케이션을 보호하기 위해서는 입증되고 평판이 좋은 온라인 서비스를 구축하는 것이 필수적입니다.



금융서비스 업체들이 클라우드에서 운영하건, 운영하지 않건 관계없이 다양한 공격 유형에 대처할 수 있는 전반적인 애플리케이션 보호가 필요합니다. 단순히 일련의 보안 상자를 확인하던 시절은 끝났습니다.

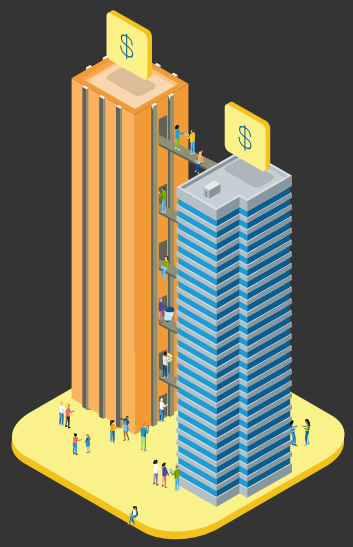
애플리케이션 혁신에 대한 최적의 접근 방식 선택

획일적인(one-size-fits-all) 접근 방식으로는 위험을 최소화하면서 편리성과 혁신에 대한 고객의 요구를 충족할 수 없습니다. 성공적인 애플리케이션 혁신을 위해 다양한 전략들 중에서 선택할 수 있으며, 이들 전략은 저마다 다른 장단점을 가지고 있습니다. 그림 3에 이들 접근 방식 중 일부가 요약되어 있습니다(페이지 8 참조).

오늘날, 매우 경쟁이 치열한 금융서비스 분야에서, 금융기관들은 모던 애플리케이션을 신속하게 시장에 제공하고 고객 요구를 충족할 수 있도록 빠르게 움직이고 민첩해야 합니다. 하지만, 보안을 포기하면서 애플리케이션 개발 속도에 대한 비중을 높이는 경우, 취약점을 노출시키고 계좌 소유주의 데이터와 거래를 위험에 빠뜨리게 됩니다.

금융서비스 업체들이 내부적으로 혁신을 추진하기로 결정한다면, 인프라와 솔루션의 현대화는 애플리케이션 및 API 라이프사이클 전반에서 엔드 투 엔드 자동화를 달성화는 데 필수적입니다. 예를 들어, 금융기관들이 더 많은 소프트웨어 릴리즈를 시장에 내놓으면서 제로터치 방식으로 애플리케이션을 제공할 수 있는 적합한 자동화 툴이 필요합니다. 또한, 매우 빠르고 안전한 네트워크 성능을 위해 보안을 강화하고 지연시간을 줄이며 게이트웨이 복잡성을 최소화하는 모던 API 관리 솔루션이 필요합니다.

그림 3: 금융서비스 분야의 애플리케이션 혁신을 위한 대표적인 모델.



인수합병(M&A)

- 입증된 솔루션 혁신
- 빠른 시장 출시 속도
- 신규 고객들에 대한 교차 판매 기회
- 막대한 비용이 소요되는 솔루션 통합

사내 애플리케이션 개발

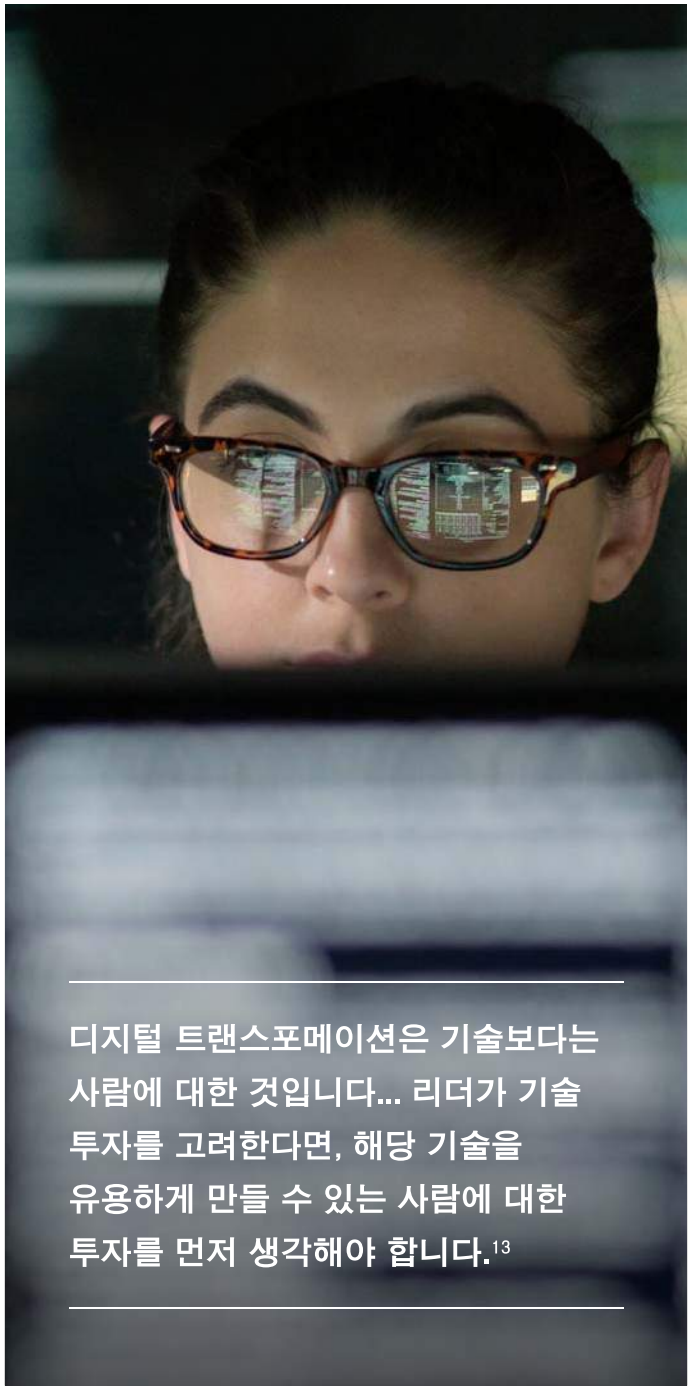
- 완벽한 기술 제어
- 오래된 시스템과 함께 확장하도록 설계 가능
- 느린 시장 출시 속도
- 레거시 통합 문제
- 적합한 인재 유치 필요

핀테크 업체에 대한 투자

- 사내 개발보다 빠른 시장 출시 속도
- 적합한 인재 참여
- 일반적으로 배타적이지 않음
- ROI 달성의 잠재적 어려움
- 데이터 보안 이슈

핀테크 파트너와 협업

- 사내 개발보다 빠른 시장 출시 속도
- 적합한 인재 참여
- 데이터 보안 이슈
- 최소 수준의 제어



디지털 트랜스포메이션은 기술보다는 사람에 대한 것입니다... 리더가 기술 투자를 고려한다면, 해당 기술을 유용하게 만들 수 있는 사람에 대한 투자를 먼저 생각해야 합니다.[13]

보안 위주의 인재 전략 채택

디지털 트랜스포메이션을 계획하는 경우, 기술 그 이상을 봐야 하며 인적 자본에 대해 생각해야 합니다. 결국, 안전한 애플리케이션 개발 및 배포를 위해서는 변화하는 위협에 대해 이해하고 애플리케이션(애플리케이션을 구성하는 코드에서 이를 사용하는 고객에게 이르기까지)을 보호하는 적합한 스킬을 갖춘 적합한 인재가 필요합니다. 이 규칙은 혁신적인 상품 및 서비스를 출시하기 위해 사내에서 개발을 하건, 오픈뱅킹을 통해 핀테크 업체와 협력하건 관계없이 적용됩니다.

금융서비스 업체들이 새로운 클라우드 네이티브 애플리케이션 발표를 가속화하고 오래 전에 구축한 레거시 시스템을 대체하려면, 이들 업무를 수행할 소프트웨어 엔지니어링 및 DevOps 인재를 확보해야 합니다.

디지털 트랜스포메이션이 가속화되면서 금융서비스 임원들은 보안 리스크 관리를 최우선 순위로 삼고 있습니다. 이에 따라, 첨단 위협 관리와 같은 영역에서 인재 경쟁이 치열해지고 있습니다.[11]

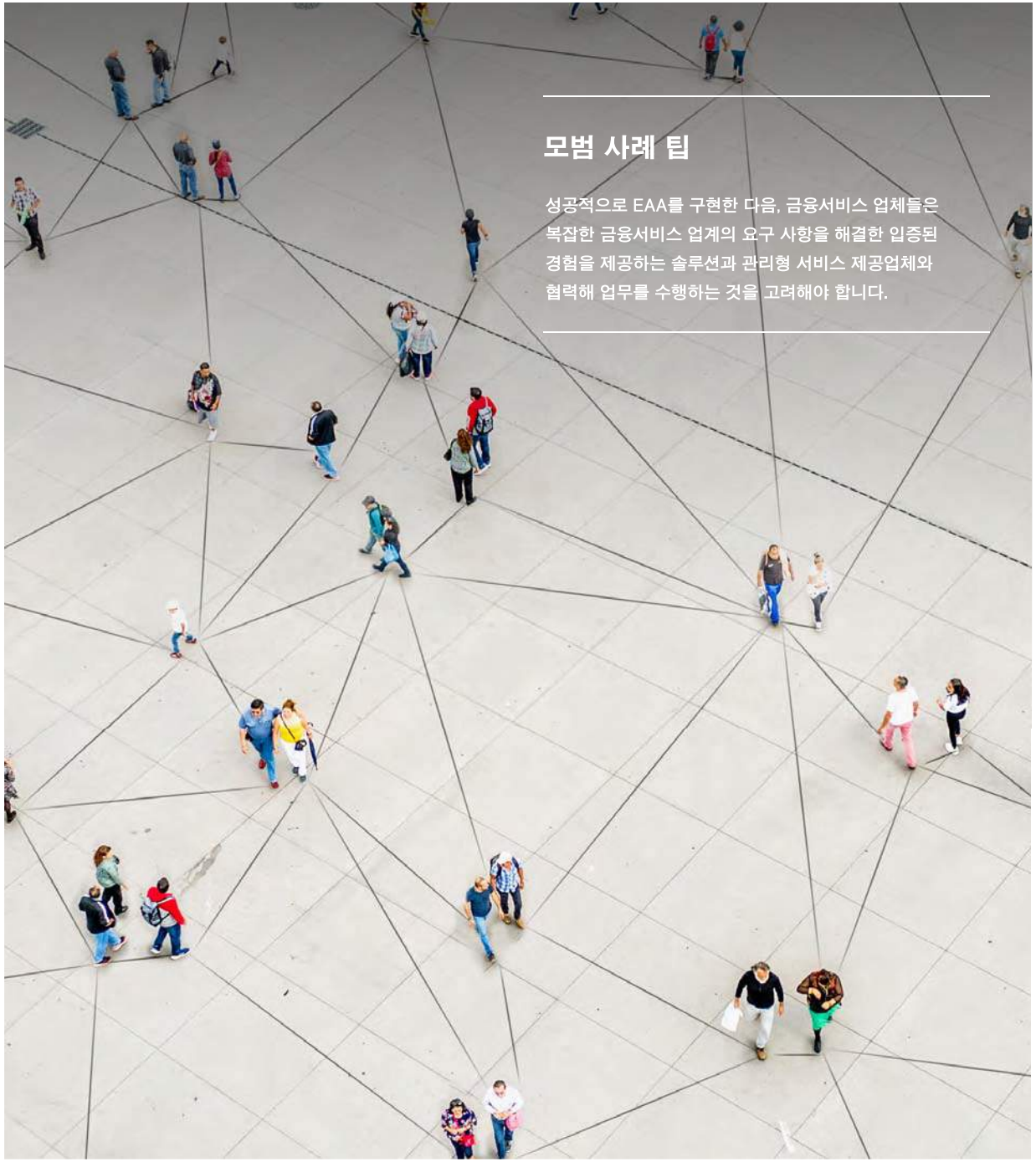
이러한 인재 격차로 인해 금융기관들은 제한된 고급 직원 풀을 두고 Google, Amazon, Facebook 등과 직접 경쟁해야 합니다. 높은 급여, 복리후생제도, 보너스 등은 필수적이지만, 유연한 인간 우선(people-first) 문화, 의미있는 업무, 직업 개발 기회 등을 통해 최고의 인재를 고용하는 데 있어 우위를 확보할 수 있습니다.[12] 가장 유능한 개발자들은 애자일 인프라를 채택하고 최첨단 기술들을 활용해 작업을 수행하기를 원하며, 따라서 기업들은 혁신에 대한 변함없는 의지를 입증해야 합니다.

발전된 애플리케이션 방법론

레거시 인프라를 이용해 편리한 모던 애플리케이션을 개발하려고 하는 경우, 과제와 한계를 겪게 됩니다. 금융기관들이 디지털 트랜스포메이션을 진행하고 있는 상황에서 유연하고 확장성이 뛰어난 EAA(Enterprise Application Architecture)는 일관성과 연계성을 향상시켜 전사적인 결과를 도출해내도록 지원할 수 있으며, 이는 애플리케이션 보안, 성능 및 신뢰성에 대한 기대치를 충족시키는 데 중요한 요구 사항입니다.

발전된 EAA 접근방식은 혁신 노력과 비즈니스 전략을 긴밀히 연계시키고, 새로운 기술과의 손쉬운 통합을 지원함으로써 기업들이 민첩성을 유지할 수 있도록 합니다. 최적의 EAA를 구현함으로써 개발자들은 위치 또는 디바이스에 관계없이, 표준과 규정을 준수하면서 신속하고, 안전하게 모던 애플리케이션을 보다 효과적으로 제공할 수 있습니다.

그림 4 (페이지 11)는 금융서비스 업체들이 EAA를 개선할 수 있도록 돕는 7단계를 보여주고 있습니다.



모범 사례 팁

성공적으로 EAA를 구현한 다음, 금융서비스 업체들은 복잡한 금융서비스 업계의 요구 사항을 해결한 입증된 경험을 제공하는 솔루션과 관리형 서비스 제공업체와 협력해 업무를 수행하는 것을 고려해야 합니다.

발전된 엔터프라이즈 애플리케이션 방법론을 구현하기 위한 단계

단계 1

EAA와 비즈니스 목적을 조정하고 혁신, 민첩성 및 리스크 간의 적절한 균형을 결정합니다.

단계 2

애플리케이션 인벤토리를 가져옵니다. 엔터프라이즈 포트폴리오 내 모든 애플리케이션의 소재를 확인합니다.

단계 3

포트폴리오 내 각 애플리케이션에 대한 보안 리스크를 평가하고 적합한 솔루션을 배정합니다. 대표적인 예:

- 표준 및 규정 준수에 필요한 하드웨어 및 소프트웨어의 FIPS 인증.
- 기존 및 새로운 OWASP 위협으로부터 보호하기 위한 웹 애플리케이션 및 API 보호
- 동적, 정책 기반 복호화, 암호화 및 다수의 검사 디바이스를 통한 트래픽 스티어링을 적용한 SSL 오케스트레이션.

단계 4

애플리케이션 범주를 정의하고 각 범주에 필요한 애플리케이션 서비스를 지정합니다.

단계 5

애플리케이션 배포 및 관리를 위한 매개변수를 설정합니다.

- 배포 옵션 이해
- 관련 비용. 소비 모델, 규정준수/인증 프로필 평가

단계 6

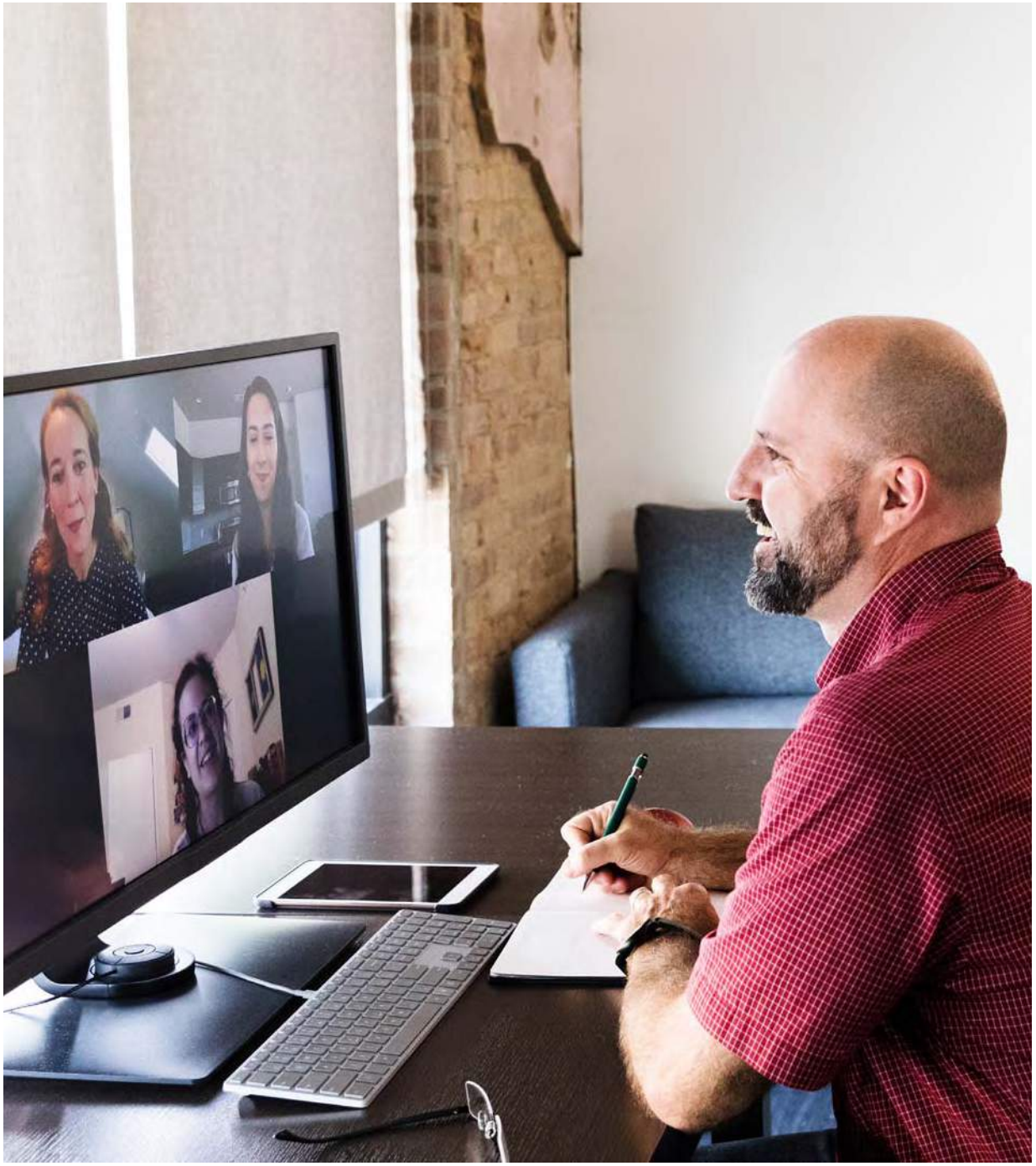
역할 및 책임을 지정합니다.

- 보안을 비롯해 EAA 내 각 구성 요소에 대한 책임자 명시
- 개별 기여자, 부서 또는 기능별 위원회(cross-functional committee)에게 책임이 있음을 인식

단계 7

EAA 접근방식을 조직 전반에 적용해 보안을 최적화합니다.

- 사용자 액세스 제어 또는 코드 취약점 검색 등과 같은 자동화된 방식 활용
- 직원 교육과 커뮤니케이션을 통한 조직 온보딩



자신있게 혁신 추진

혁신은 가치와 취약점 모두를 위한 훌륭한 소스가 될 수 있습니다. 금융서비스는 계속해서 진화하는 공격 방식을 사용하는 사이버 범죄자들에게 여전히 매력적인 공격 표적이기 때문에 신종 위협으로부터 고객 애플리케이션, 백엔드 시스템을 보호하기 위해서는 보다 신속하게 움직여야 합니다.

다행스러운 것은 애플리케이션 혁신과 보안이 반드시 상충될 필요는 없다는 것입니다. 체계적으로 설계된 엔터프라이즈 애플리케이션 인프라의 일부로서 적합한 인재를 고용하고 안전한 저지연 환경을 구축함으로써 애플리케이션 라이프사이클의 모든 단계에서 보안이나 성능을 저하시키지 않으면서, 시장 출시 속도를 높일 수 있습니다.

F5의 뱅킹 및 금융 서비스 부문에 대한 자세한 내용을 확인해 보십시오.

부록

[1] CISA(Cybersecurity & Infrastructure Security Agency), 경고 (AA20-099A): 악의적인 사이버 공격자에 의해 악용되는 COVID-19, 국토안보부(2020년4월8일), https://www.us-cert.gov/ncas/alerts/aa20-099a 참조.

[2] NortonLifeLock, 사이버 안전 통찰력 보고서 글로벌 결과(2020년3월30일), 6페이지, https://now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf?promocode=DEFAULTWEB 참조

[3] Raymond Pompon, Malcolm Heath 및 Sander Vinberg, 2017년-2019년의 금융서비스 업체들에 대한 주요 공격, F5 Labs 애플리케이션 위협 인텔리전스(2020년4월27일), https://www.f5.com/labs/articles/threat-intelligence/top-attacks-against-financial-services-organizations-2017-2019 참조

[4] 상동

[5] F5 Networks, Inc., 2020년 애플리케이션 서비스 현황 보고서 – 금융서비스편, 8페이지.

[6] 상동, 8페이지

[7] 상동, 8페이지

[8] Deloitte, 클라우드 필수 요소: 은행들이 클라우드 기반 트랜스포메이션을 통해 비즈니스 민첩성을 향상시키는 방법, 5페이지, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/financial-services/ca-financial-services--cloud-imperative-en.pdf 참조

[9] F5 Networks, Inc., 2020년 애플리케이션 서비스 현황 보고서 – 금융서비스편, 7페이지.

[10] Tom Krazit, 스트리트, 오랫동안 클라우드 추이 주시; 그리고 다가온 코로나바이러스, Protocol (2020년4월29일), https://www.protocol.com/financial-services-cloud-transformation-coronavirus 참조

[11] Dan Butcher, 은행들, 충분한 사이버 보안 인재 구인난, eFinancialCareers (2017년3월14일), https://www.efinancialcareers.com/news/2017/03/deloitte-banks-are-engaging-in-a-recruitment-war-for-cybersecurity-talent 참조.

[12] Jeff Hyman, 대형 기술 업체들과의 인재 경쟁? 돈의 문제가 아님, Forbes (2018년5월30일), https://www.forbes.com/sites/jeffhyman/2018/05/30/giants/#49e2cb9a1d43 참조

[13] Becky Frankiewicz 및 Tomas Chamorro-Premuzic, 디지털 트랜스포메이션에서 중요한 것은 자금이 아닌 인재, Harvard Business Review (2020년5월6일), https://hbr.org/2020/05/digital-transformation-is-about-talent-not-technology?ab=hero-subleft-1 참조

F5 소개

F5는 개발부터 전체 라이프사이클 전반에 이르기까지 애플리케이션을 지원하므로, 차별화된 고성능 보안 디지털 경험을 제공할 수 있습니다.

F5.com/solutions에서 뱅킹 및 금융 서비스 리소스에 대한 자세한 내용을 확인해 보십시오.

US Headquarters: 801 5th Ave, Seattle, WA 98104 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2020 F5 Networks, Inc. All rights reserved. F5, F5 Networks 및 F5 로고는 미국 및 기타 특정 국가에서 F5 Networks, Inc.의 상표입니다. 기타 F5 상표는 f5.com에서 확인할 수 있습니다. 본 자료에 언급된 기타 모든 제품, 서비스 또는 회사 이름은 각 소유권자의 상표이며, F5의 그 어떠한 명시적 또는 암묵적 보증이나 제휴도 부인합니다. EBOOK-BFSI_505109142