데이터 보안 자동화

멀티클라우드 금융 서비스 애플리케이션

데이터 보안 침해 비용은 연간 3조 달러에서 2024년에는 5조 달러 이상으로 증가하거나, 연평균 11% 증가할 것으로 예측됩니다.[1]

Juniper Research

멀티클라우드의 보안 및 컴플라이언스 관리로 리스크 절감

최근 몇 년 동안 금융 서비스 산업에서 클라우드 네이티브 애플리케이션이 민첩성과 탄력성 등의 이점으로 인해 빠르게 도입되고 있습니다. 그러나 클라우드 및 멀티클라우드 배포로 이동하는 경우에는 특히 고객 데이터와 관련한 보안 및 규정 준수 문제를 최우선 과제로 생각해야 합니다. 데이터 보호는 모든 비즈니스에서 중요한 사항이지만, 금융 서비스의 경우 고객의 돈과 직결되는 문제이기에 더욱 중요합니다.

은행, 페이먼트 제공업체, 보험사를 비롯한 금융 서비스 회사에서는 점점 더 엄격해지는 다양한 보안과 개인정보 보호 표준을 준수해야 합니다. 여기에는 결제 카드 산업 데이터 보안 표준(PCI DSS) 및 유럽 연합(EU)의 일반 데이터 보호 규정(GDPR)이 포함됩니다. 이에 따라 다수의 글로벌 기업이 엄격한 트랙킹, 리포트, 문서화 등을 요구하는 GDPR을 준수하기 위해 기준을 높이고 있습니다.

해당 법 규정 중 대다수는 기업이 개인 식별 정보(PII) 데이터를 보호하는 방법과 관련된 특정 요건을 포함합니다. 또한 기업은 데이터 손실 또는 도난으로부터 고객의 데이터를 보호하기 위한 수단을 갖추고 있음을 입증해야 합니다. 예를 들어, 미국의 여러 주에서 채택한 캘리포니아주 보안 침해 정보법(SB-1386)은 보안 침해 사건이 발생한 경우 이를 공개해야 한다고 명시한 최초의 주 법입니다. 이 법에서는 보안 침해가 발생한 경우 "법 집행을 위한 합법적인 요구에 따라 가능한 가장 적절한 시간 내에 불합리한 지연 없이" 영향을 받는 개인에게 이를 알리도록 요구합니다.[2] 그러나 손상된 데이터가 유실되었을 당시 암호화되어 있었음을 입증할 수 있는 경우 면책 조항을 명시하고 있습니다.

금융 서비스 기업에서 이러한 데이터 보호 규제를 준수하지 못하면 더 큰 대가를 치르게 됩니다. 데이터 침해는 여러 측면의 비용을 유발합니다. Juniper Research의 최근 리포트에 따르면, 데이터 보안 침해로 인한 비용은 연간 3조 달러에서 2024년에는 5조 달러 이상으로 증가하거나, 연평균 11% 증가가 예측됩니다.[3] 이러한 증가 추세의 주요 원인은 규제가 엄격해지면서 데이터 침해에 대한 벌금이 높아졌기 때문입니다.

디지털 영역에 대한 기업 의존도가 점점 커지면서 상당한 비즈니스 손실을 입을 위험도 높아집니다. Equifax가 고객의 개인 식별 정보(PII)를 보호하지 못해 비용 손실, 브랜드 이미지 손상은 물론 비즈니스에 큰 차질을 겪었던 일은 대부분의 금융 서비스 업계에서 기억되는 대표적인 사례입니다.

1 *Juniper Research. 2019~2024년 사이버 범죄 및 사이버 보안 전망: 위협 분석, 영향 평가 및 완화 전략(The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024), 2019년 8월.*

2 *캘리포니아 상원 법안 1386, SEC. 2. 섹션 1798.29, 2002년 9월 제정.*

3 *Juniper Research. 2019~2024년 사이버 범죄 및 사이버 보안 전망: 위협 분석, 영향 평가 및 완화 전략(The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024), 2019년 8월.*

멀티클라우드 환경에 필요한 컴플라이언스 자동화 전략

금융 서비스 회사에서는 하이브리드 및 멀티클라우드 환경이 점점 더 빠른 속도로 표준으로 자리잡고 있습니다. 최근 Enterprise Cloud Index 리포트에 따르면 금융 서비스 업계는 하이브리드 클라우드 도입 측면에서 전 세계 평균인 18%에 비해 시장의 21%에 도달하여 대부분의 업계를 앞지르고 있습니다.[5] 이렇게 혼합된 환경에서 시스템 컴플라이언스를 수동으로 모니터링하는 것은 어려울 뿐 아니라 거의 불가능한 일입니다.

최근 SANS Institute 리포트는 설문조사에 참여한 조직 중 절반 이상(54%)이 진화하는 규제를 충족하기 위해 클라우드 전략을 조정하고 있다고 밝혔습니다.[6] 그럼에도 불구하고, 금융 기관은 경쟁력을 유지하기 위해 클라우드로 마이그레이션해야 합니다.

설문조사에 참여한 54%의 조직이 진화하는 규제를 충족하기 위해 클라우드 전략을 조정하고 있다고 답했습니다.[4]

SANS Institute

효과적인 자동화 전략이 없다면, IT 팀은 보안 및 컴플라이언스 시스템을 수동으로 확인하는 데 있어 여러 가지 잠재적인 위험을 겪게 됩니다. 수동 프로세스는 부적절한 작업을 초래하거나 구성 변경 시 컴플라이언스의 핵심 요소인 감사 추적 정보를 누락하는 문제로 이어질 수 있습니다.

이러한 수동 프로세스의 특징은 다음과 같습니다.

- 시간이 많이 소요되는 지루한 작업
- 인적 오류에 취약
- 반복 및 공유가 불가능하거나 확인 불가능한 작업
- 불완전하거나 일관되지 않은 변경 로그 정보로 인한 감사 실패 취약성
- 운영팀 및 보안팀 간에 원활하지 않은 커뮤니케이션

다행스럽게도 건전한 자동화 전략을 구축하면 조직이 보안 및 컴플라이언스를 개선하여 전반적인 비즈니스 위험을 줄이는 데 도움이 됩니다. 효과적인 자동화 전략을 통해 복잡한 멀티클라우드 환경을 관리하고 간소화할 수도 있습니다.

자동화를 활용하면 금융 기관은 보안 및 컴플라이언스를 더욱 종합적이고 효율적으로 관리할 수 있습니다. 또한 소프트웨어 패치와 시스템 구성을 자동화하면 인적 오류를 줄일 수 있습니다. Verizon이 2019년 발행한 보안 침해 조사 리포트에 따르면, "사이버 범죄자들은 인적 오류를 악용"하는 경우가 많습니다.[7] 이 부분에서도 자동화가 컴플라이언스와 전반적인 보안을 강화하는 데 도움이 될 수 있습니다.

---

4 *SANS Institute. SANS 2019 클라우드 보안 설문조사(SANS 2019 Cloud Security Survey), 2019년.*

5 *Nutanix. 엔터프라이즈 클라우드 인덱스(Enterprise Cloud Index), 2019년.*

6 *SANS Institute. SANS 2019 클라우드 보안 설문조사(SANS 2019 Cloud Security Survey), 2019년.*

7 *Verizon. 2019 데이터 침해 조사 리포트(2019 Data Breach Investigations Report), 2019년.*

코드로서의 컴플라이언스: 클라우드 기반 보안 자동화

자동화 전략은 컴플라이언스를 프로세스의 일부로 자동화하여 DevSecOps를 논리적인 다음 단계로 진행합니다. 최근 IT 조직에서는 모든 프로세스를 코드로 구현하고 있으며 컴플라이언스 구현도 마찬가지입니다. DevOps가 여러 가지 보안 검증을 자동화하며 DevSecOps로 진화한 것과 비슷한 방식으로 컴플라이언스를 구현하는 것입니다. 금융 서비스의 상당히 많은 컴플라이언스 요건을 감안하면 금융 서비스 업계에서 DevSecOps로 보안을 코드화한 것처럼 컴플라이언스도 자동화해야 한다는 점은 놀라운 일이 아닙니다. 그 결과가 바로 DevSecComplianceOps입니다.

특히, 규제 요구 사항은 지역별로 다른 경우가 많으므로, 글로벌 규모로 컴플라이언스를 구축하는 것은 쉽지 않은 일입니다. 글로벌 은행은 전 세계의 규제 요건은 물론 지역별 규제까지 충족해야 합니다. 예를 들어, 유럽 지역의 은행은 독일 지점에 적용되는 추가 컴플라이언스 표준도 준수해야 합니다. 보안을 위해 작성된 코드가 독일에서처럼 말레이시아에서도 적용되던 DevSecOps 상황과 달리, 대부분의 금융 서비스 조직에서는 글로벌 컴플라이언스와 지역 컴플라이언스 요건을 모두 준수해야 합니다.

은행은 여러 지역에 걸쳐 위치하기 때문에, 같은 은행이라도 방화벽으로 데이터를 보호하기 위해 다른 요건이 적용될 수 있습니다. 향후 규제에서 비즈니스의 연속성과 탄력성을 보장하기 위해 둘 이상의 퍼블릭 클라우드에 데이터를 보관하도록 요구하는 경우 이에 대한 대비가 필요할 수 있습니다. 규제 요건이 변화하면서 여러 지역과 클라우드 유형 전반의 복잡성을 관리하기 위해 컴플라이언스 자동화의 중요성이 더욱 강조되고 있습니다.

효과적으로 위험을 줄이고 컴플라이언스를 간소화하려면 처음부터 애플리케이션 코드에 컴플라이언스 규정을 포함하여 구축해야 합니다. 이 새로운 DevSecComplianceOps 접근 방식을 통해 IT팀은 글로벌 프레임워크 내에서 현지화된 자동화를 달성할 수 있고, 이 모든 것을 확장 가능하며 강화된 환경에서 실현할 수 있습니다.

Red Hat과 Intel의 보안 및 컴플라이언스 자동화 지원

Red Hat과 Intel은 함께 자동화에 필요한 보완적인 하드웨어 및 소프트웨어를 제공합니다. 이들 혁신 기업은 협력을 통해 코드형 인프라(IaC) 기술을 결합한 공동 솔루션도 만들었습니다. 몇 년 동안 심층적인 파트너 이니셔티브를 개발했고, 그 결과 더 많은 이점을 갖추고 긴밀하게 통합된 솔루션이 탄생했습니다.

Red Hat® Ansible® Automation Platform은 Red Hat OpenShift® 컨테이너 애플리케이션 플랫폼 기술을 사용해 모든 클라우드 환경에서 인프라와 코드 배포를 자동화합니다. 하드웨어 기반 격리 및 메모리 암호화를 지원하는 Intel SGX(Intel Software Guard Extensions)와 결합하여 메모리에서 신뢰할 수 있는 보호 영역인 '엔클레이브(enclaves)'에 데이터를 저장합니다. 로컬 지역에 일관적으로 자동 배포할 수도 있습니다. 이 자동화되고 일관적이며 보안이 강화된 데이터 환경을 디지털 비즈니스의 기반으로 사용해 코드 보호를 강화하고, 개발자가 더 안전한 솔루션을 제공할 수 있도록 지원합니다.

일반적으로 규제가 적용되는 워크로드는 신뢰할 수 있는 전용 환경에서 실행해야 했으며, 대체로 은행 내부에 전용 인프라가 필요했습니다. 사용 중인 데이터를 보호하는 기술을 활용하여 워크로드는 하나 이상의 클라우드에서 서버를 공유할 수 있습니다. 즉, 신뢰할 수 없는 환경에서도 신뢰할 수 있는 방식으로 워크로드를 실행할 수 있다는 의미입니다.

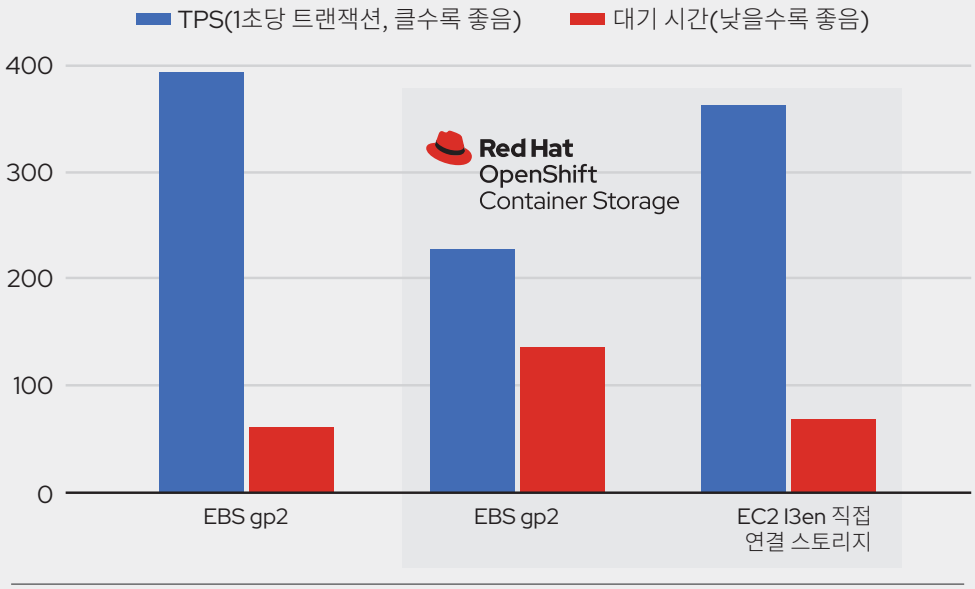

그림 1. Intel SGX 지원 시스템

예를 들어, GDPR을 위한 컴플라이언스 요건이 매우 엄격하다는 점을 고려하면, 유럽과 미국에서 각기 다른 데이터 보호 방식을 사용하는 것은 효과적이지 않습니다. Intel SGX를 사용하면 개발자가 메모리에 보다 안전한 엔클레이브를 만들 수 있으므로 공격자가 서버에 물리적으로 액세스하거나 악의를 가지고 관리 권한을 높이더라도 메모리에서 실행 중인 항목을 볼 수 없습니다.

개발자는 Red Hat Ansible Automation Platform을 통해 Red Hat OpenShift에서 코드로 자동화된 시스템을 만들 수 있습니다. 이 접근 방식은 서버의 공격으로 인해 악의적인 사용자가 해당 엔클레이브에서 실행되고 있는 것을 볼 수 없다는 증거를 제시합니다. 마찬가지로, 다른 기업의 솔루션을 신뢰해야 하는 모든 클라우드에서 이 엔클레이브는 환경을 완전히 신뢰할 수 없는 경우에도 신뢰를 강화해줍니다

GDPR 이전에는 은행에서 데이터센터로 이동하여 고장난 물리적 디스크를 폐기하는 것이 가능했습니다. 하지만 GDPR 시행 후에는 고객이 데이터 삭제를 요구할 수 있으며, 기업은 해당 데이터가 삭제 또는 파기되었음을 감사 가능한 방식으로 증명해야 합니다. 일반적인 사례는 데이터가 암호화되었기 때문에 더 이상 해당 데이터를 사용할 수 없음을 증명하는 증거를 규제 기관에 제공하는 보상 메커니즘을 구축하는 것입니다.

예를 들어, 한 커피 회사의 직원이 고객 수백만 명의 신용카드 정보가 들어 있는 노트북을 택시에 놓고 내렸다고 가정해 봅시다. 대부분의 개인정보보호법에 따라, 은행은 피해자들에게 보상하고 보안 침해 사실을 일반에 공개해야 합니다. 하지만 노트북에 하드디스크를 암호화하는 엔드포인트 보호 소프트웨어가 설치되어 있다면 보상 및 공개를 하지 않아도 됩니다. 보충 메커니즘에 따라 해당 소프트웨어는 암호화의 증거를 제공합니다.

어떤 클라우드에서든 코드로서의 컴플라이언스를 통해 유사한 보상 메커니즘을 제공할 수 있습니다. 개발 과정에서 Intel SGX 및 Ansible Automation Platform을 사용하는 클라우드 네이티브 애플리케이션은 Red Hat OpenShift에 대한 컴플라이언스 자동화 래퍼를 제공합니다.

결론

Red Hat과 Intel은 고객이 지속적인 통합 및 배포(CI/CD) 파이프라인을 연결하고 코드로서의 컴플라이언스 설계를 통합할 수 있도록 지원합니다. 이를 통해 DevOps 환경에서 인적 오류의 위험을 줄일 수 있습니다. DevSecComplianceOps 접근 방식은 애플리케이션 구축, 테스트, 배포를 자동화하여 개발팀과 운영팀 간 격차를 해소해줍니다.

DevSecComplianceOps로 지원되는 일관된 자동화는 가이드의 반복 가능성을 공유 및 검증할 수 있는 능력은 물론, 여러 팀 및 클라우드 전반에 일반적인 자동화 플랫폼을 제공합니다. 이러한 기능을 함께 사용하면 보안, 네트워킹, Windows, Linux® 및 기타 팀에게 코드로서의 컴플라이언스로 보안을 강화하기 위해 필요한 역할에 대한 정보를 제공할 수 있습니다.

코드로서의 컴플라이언스는 다음과 같은 다양한 이점을 제공합니다.

- 컴플라이언스를 위한 추적 및 반복 기능
- 반복적인 태스크에 소요되는 시간 단축
- 일관된 인프라 관리 접근 방식을 통해 다운타임 위험 감소
- 문제에 대한 분석, 감지, 해결을 자동화함으로써 시스템적 오류 최소화
- 인적 오류로 인한 위험 감소
- IT 프로세스 가속화(며칠에서 몇 분 단위로 단축)
- 멀티클라우드 환경 전반에 일관된 설정 및 관리 구현

자세히 알아보기

앞의 예시에서 금융 서비스 회사가 코드로서의 컴플라이언스를 활용하여 오늘날 멀티클라우드 워크로드의 데이터와 개인정보를 어떻게 보호하는지에 대한 간략한 시나리오 몇 가지를 살펴보았습니다. Red Hat과 Intel이 보안 또는 컴플라이언스를 유지하면서 CI/CD 파이프라인 자동화를 실현하는 방법에 대해 자세히 알아보세요.

한국레드햇 홈페이지 https://www.redhat.com/ko

RED HAT 정보

Red Hat은 세계적인 엔터프라이즈 오픈소스 솔루션 공급업체로서 커뮤니티 기반 접근 방식을 통해 신뢰도 높은 고성능 Linux, 하이브리드 클라우드, 컨테이너, 쿠버네티스 기술을 제공합니다. 또한 고객으로 하여금 신규 및 기존 IT 애플리케이션을 통합하고, 클라우드 네이티브 애플리케이션을 개발하며, 업계를 선도하는 Red Hat의 운영 체제를 기반으로 표준화하는 동시에 복잡한 환경의 자동화, 보안 및 관리를 실현할 수 있도록 지원합니다. Red Hat은 전세계 고객에게 높은 수준의 지원과 교육 및 컨설팅 서비스를 제공하여 권위있는 어워드를 다수 수상한 바 있으며, Fortune 선정 500대 기업의 신뢰를 받는 어드바이저로 인정받고 있습니다. 또한 기업, 파트너, 오픈소스 커뮤니티의 전략적인 파트너로서 고객들이 디지털 미래에 대비할 수 있도록 지원하고 있습니다.

www.facebook.com/redhatkorea
구매문의 080 708 0880
buy-kr@redhat.com