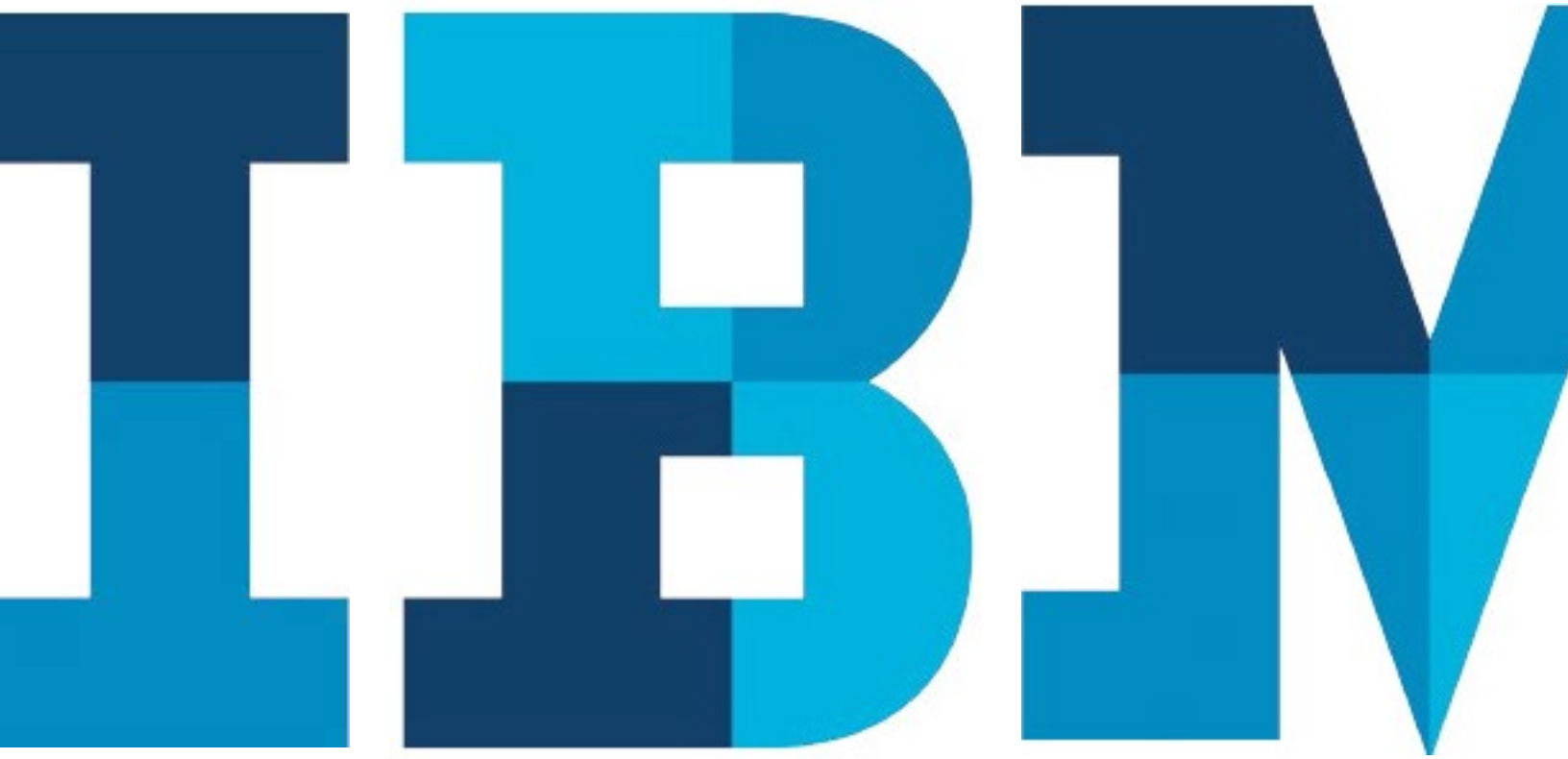
IBM
Thought Leadership 백서

민감한 데이터를 보호하면서 온라인 사용자 경험 향상

IBM Tealeaf Customer Experience on Cloud를 통해 엄격한 보안 및 프라이버시 유지



IBM

개요

온라인 트랜잭션과 상호작용은 많은 조직의 비즈니스에서 큰 부분을 차지합니다. 따라서 이러한 채널을 무시하는 것은 위험한 선택이 될 수 있습니다. 성공적인 조직은 온라인 사용자 경험을 최적화하여 고객을 더 잘 지원하고 경쟁 우위를 유지하는 방법을 끊임없이 모색합니다.

사용자 경험에 대한 데이터를 캡처함으로써 조직은 효과가 있는 것과 없는 것을 이해하는 데 도움이 되는 행동 정보를 확보하게 됩니다. 경험을 재생함으로써 조직은 사용자가 트랜잭션을 포기하거나, 다른 비즈니스로 전환하거나, 소셜 미디어를 통해 불만을 터트리게 만들 수 있는 문제를 제거할 수 있습니다.

조직이 점점 더 많은 고객 데이터를 분석함에 따라 기본적인 문제, 즉 데이터 수명 주기에 걸쳐 엄격한 데이터 보안을 유지하고 사용자 프라이버시를 보호하는 문제에 직면하게 됩니다. 고객 데이터 수집은 조직이 사기, 소송, 고객 관계 손상 및 평판 손상을 겪게 할 수 있는 데이터 손실 또는 도난의 기회를 창출합니다. 개인 고객 데이터와 상호작용하는 클라우드 기반 솔루션을 사용하면 이러한 우려(민감한 사용자 데이터가 안전한 온프레미스 환경을 벗어나 클라우드로 전송될 것인지, 만약 그렇다면 어떻게 보안을 완벽히 유지하는지 등)가 확대될 수 있습니다.

IBM® Tealeaf® Customer Experience on Cloud(IBM Tealeaf CX on Cloud)는 SaaS 멀티테넌트 솔루션이라는 것이 이러한 질문에 대한 답입니다. 이 솔루션은 온라인 경험을 최적화하면서 사용자 데이터를 보호하고 프라이버시를 유지하며 규정 준수를 계속 유지해야 하는 조직에 고급 분석 기능을 제공합니다. Tealeaf는 민감한 사용자 데이터를 캡처하여 클라우드로 전송하는 것을 방지할 뿐만 아니라 이러한 프로시저의 장애를 처리할 수 있는 추가적인 보안 기능을 제공합니다.

IBM Tealeaf: 탁월한 이력

IBM Tealeaf는 지난 15년간 고객 경험 시장의 선두를 지켜왔습니다. 기능성과 보안성에 대한 명성을 얻었으며 이제 이러한 전문성을 Tealeaf CX on Cloud를 통해 클라우드에 적용하고 있습니다. Tealeaf를 사용하여 고객 관계를 이해하고 강화하는 조직들의 놀라운 명단을 확인해 보십시오.

- 상위 10대 온라인 소매업체 중 7개
- 상위 10대 은행 지주 회사 중 8개
- 북미 최대 규모의 상해보험회사 12개 중 9개
- 주요 미국 항공사 50%
- 모든 주요 북미 무선 서비스 공급자

민감한 고객 데이터를 보호하면서 온라인 사용자 경험을 최적화

Tealeaf CX on Cloud는 조직이 웹 사이트와 모바일 사이트 모두에서 사용성 문제를 해결하고 엄격한 데이터 보안과 사용자 프라이버시를 유지할 수 있도록 설계되었습니다. 조직은 각 방문자 상호작용을 캡처하고 분석하여 고객 경험과 사용자 행동에 대한 명확한 가시성을 제공할 수 있습니다. Tealeaf CX on Cloud에서 제공하는 고급 보고서 및 대시보드 기능을 사용하면 장기 사용 추세에 항시 대비하면서 문제의 근본 원인을 신속하게 식별하고 이러한 문제가 비즈니스에 미치는 영향을 정량화할 수 있습니다.

Tealeaf CX on Cloud 데이터 보안 및 프라이버시 보호 기능은 강력하면서 유연합니다. 이 두 특성은 끊임없이 변화하는 비즈니스 환경에서 꼭 필요한 특성입니다. 이 기능을 사용하면 조직이 고객 경험을 개선하는 데 필요한 데이터만 캡처하고 민감한 정보가 고객의 브라우저를 벗어나지 않도록 방지할 수 있습니다(그림 1). 민감한 데이터가 실수로 수집되고 클라우드로 전송되더라도, Tealeaf CX on Cloud에서 추가적인 프라이버시 기능을 적용하여 해당 데이터가 영구적으로 복구할 수 없게 파괴될 때까지 안전한 IBM SoftLayer® 인프라 내에서 이를 보호할 수 있습니다.

IBM Tealeaf CX on Cloud 솔루션을 민감한 데이터를 수집하거나 전송하지 않도록 구성할 수 있으므로, 고객은 개인 정보가 안전한지 의문을 제기하는 대신 정보를 보안하는 브랜드를 사용하고 있음을 확신할 수 있습니다.

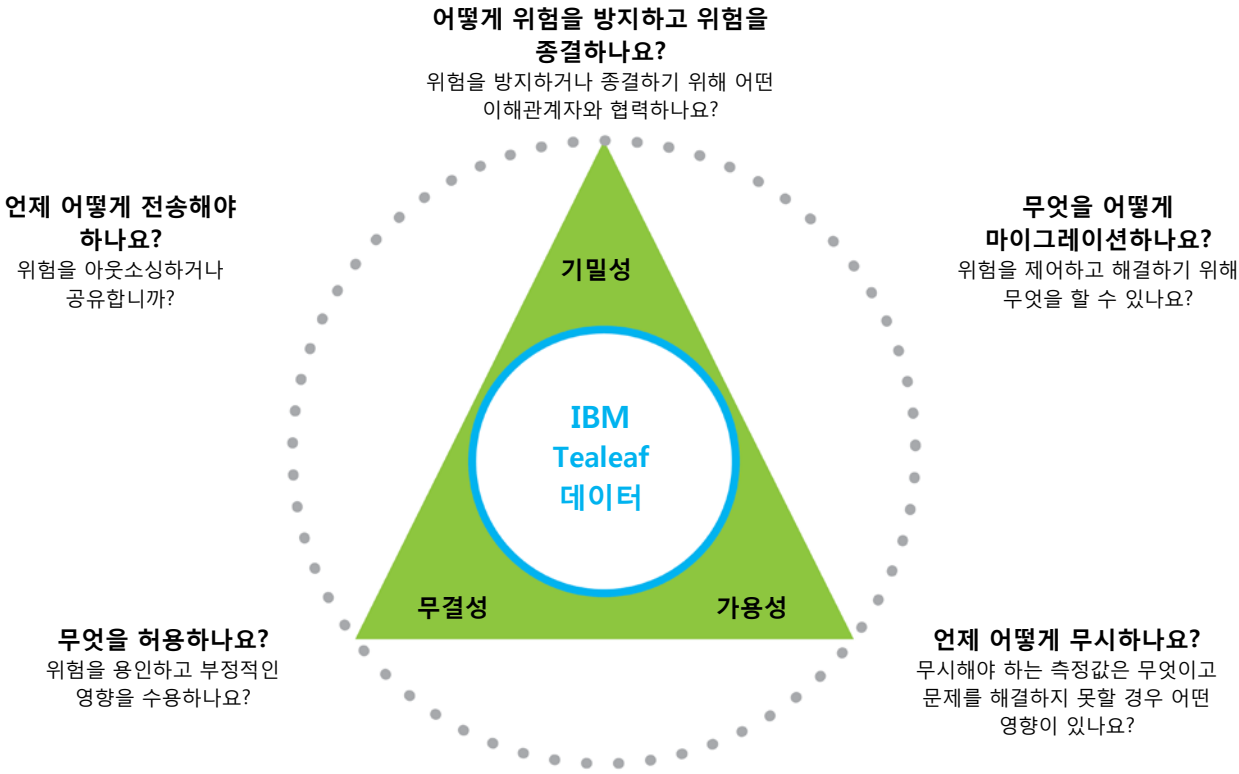


그림 1. SaaS 개발 프로세스 동안 Tealeaf CX on Cloud는 데이터 기밀성, 무결성 및 가용성을 관장하는 지침을 비롯하여 업계 보안 지침을 준수합니다.

엄격한 보안 제어 유지

Tealeaf CX on Cloud는 다양한 데이터(URL, 양식 필드, 사용자 로그인 이름, 쿠키, 애플리케이션, 클라이언트 IP 주소, 기타 원시 데이터 요소)를 캡처하여 조직이 온라인 사용자 경험을 최적화하도록 지원합니다. 하지만 Tealeaf CX on Cloud는 사용자가 사용자 주소, 사회 보장 번호, 신용카드 번호, 의료보험 계정 번호 또는 유사한 데이터(조직의 보안 및 위험 제어 항목에 규정된)와 같이 개인식별정보(PII) 또는 민감한 개인식별정보(SPII)를 캡처하지 않게 구성할 수 있도록 설계되었습니다.

핵심은 Tealeaf CX on Cloud에서 제공하는 SDK(Software Development Kit) 또는 UI 캡처 메소드에 있습니다(그림 2). 이 메소드가 적절하게 구성되면 특정 양식 필드에 입력되는 데이터를 Tealeaf 솔루션이 캡처하는 것을 자동으로 차단할 수 있습니다. 9개의 숫자와 2개의 대시로 구성된 사회 보장 번호가 차단되는 경우 개인 정보를 완전히 제거하여 "xxxxxxxxxx"로 만들기 위해서는 문자를 하나씩 대체해야 합니다.

또한 Tealeaf CX on Cloud에서는 데이터를 마스킹하는 기능을 제공하며 이 기능은 데이터 차단과는 전혀 다릅니다.

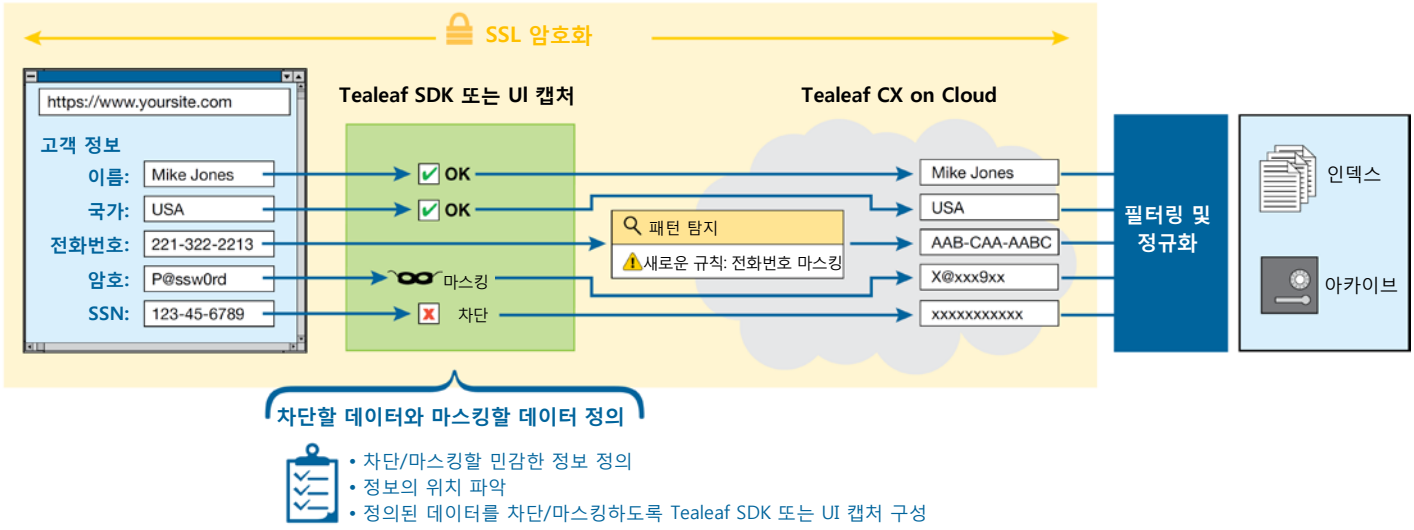


그림 2. 마스킹되거나 차단되어야 하는 데이터를 정의하고 이에 따라 SDK 또는 UI 캡처 메소드를 구성하는 작업은 Tealeaf CX on Cloud 솔루션의 핵심 요소입니다. Tealeaf CX on Cloud는 이 지침과 규칙을 통해 민감한 데이터가 캡처되기 전에 이를 차단하거나 마스킹할 수 있습니다. SDK로 코딩될 수 없는 프라이버시 업데이트가 이루어지는 경우 보호 계층 추가를 위해 추가적인 프라이버시 기능이 클라우드에 적용됩니다.

예를 들어 최종 사용자가 암호 복잡도 요구 사항을 지키기를 바라지만 실제 암호 값을 수집하길 원하지 않는 조직에서는 암호 필드를 마스킹하도록 SDK를 구성하여 암호 값 P@ssw0rd를 X@xxx9xx로 대체할 수 있습니다.

각 조직은 먼저 차단하거나 마스킹할 데이터를 정의해야 합니다. 조직의 위험 또는 보안 부서 담당자들은 적절한 기업, 산업 및 정부 규제를 검토하고 캡처하거나 마스킹해서는 안 되는 데이터 유형을 파악합니다. 그리고 이 팀에서는 차단하거나 마스킹해야 하는 데이터를 포함하는 모든 사이트 또는 앱 페이지가 표시된 요구 사항 문서를 작성합니다. 그런 다음 IBM Tealeaf 팀이 조직의 IT 그룹과 협력하여 Tealeaf SDK 또는 UI 캡처를 구성하고 필요한 테스트를 수행합니다.

모든 캡처된 데이터는 고객의 브라우저에서 Tealeaf CX on Cloud로 전송될 때 SSL 암호화로 안전하게 유지됩니다. 민감한 데이터가 차단되거나 마스킹되는 경우 Tealeaf CX on Cloud에서 분석하지 않고 브라우저 수준에서 즉시 차단되거나 마스킹됩니다. 따라서 Tealeaf 세션 데이터에 액세스할 때는 그 누구도 차단되거나 마스킹된 데이터는 볼 수 없습니다. 무단으로 데이터에 액세스할 가능성을 최소화하기 위해 Tealeaf CX on Cloud는 누구에게도 민감한 데이터에 대한 특별 액세스를 허용하지 않습니다.

UI SDK를 통해 프라이버시 기능을 브라우저 수준에서 적용하는 것이 이상적입니다. 민감한 데이터가 클라우드에 도달하기 전에 차단되거나 암호화되기 때문입니다. 하지만 데이터 수집 규칙이 변경되어 SDK 코드가 업데이트될 때까지 민감한 정보가 노출될 위험에 놓일 상황이 있을 수 있습니다. 이러한 경우 Tealeaf CX on Cloud는 중요한 장점을 제공합니다. 바로 이 솔루션은 보호 계층 추가를 위해 클라우드 수준에서 프라이버시 기능을 적용할 수 있다는 것입니다. 예를 들어 복잡한 패턴 탐지 기능을 사용하면 캡처 프로세스에서 제대로 차단되지 않은 민감한 정보를 파악하고 차단할 수 있습니다(예를 들어 SDK를 다시 구성하지 않은 상태에서 새로운 필드가 추가된 경우).

Tealeaf CX on Cloud에서는 데이터를 수신하면서 데이터를 정규화하고 보호하도록 특정 필터링 및 조작 함수를 수행하는 프로세스를 통해 데이터를 간소화합니다. 데이터가 정규화되면, 인덱싱되고, 아카이브되며, 이후 액세스 및 분석에 사용할 수 있게 됩니다. (보안 주제에 대한 추가 FAQ는 부록 A 참조)

SoftLayer로 클라우드 위험 줄이기

IBM SoftLayer는 전용 서버, 관리형 호스팅 및 클라우드 컴퓨팅 업계의 선두주자입니다. Tealeaf CX on Cloud를 현존하는 최고 성능의 클라우드 인프라 중 하나인 SoftLayer 클라우드 인프라에 배포하면 기본 인프라 수준에서 제공되는 추가 보안 조치를 활용하여 사용자 정보 보호를 강화할 수 있습니다.

IBM: 심층적인 보안이 최우선

IBM에서는 데이터 프라이버시 및 보안을 나중에 추가하거나 단순히 "비즈니스를 수행하는 비용"의 일부로 간주하지 않습니다. 전 세계적으로 거의 4,000개에 가까운 고객사를 위해 매일 150억 건의 보안 이벤트를 관리 및 모니터링하는[1] IBM은 알려진 사이버 보안 위협이 저장된 전 세계에서 가장 큰 단일 데이터베이스 중 하나를 유지 관리합니다. 최근 생겨난 위협을 파악하고 분석하며, 아직 대중에게 알려지기 전인 경우도 많습니다. IBM은 프라이버시 및 보안 분야의 리더로서 깊은 지식을 바탕으로 운영하며, 보안 데이터베이스 정보를 분석 및 사용하여 사이버 위협 환경에 대한 매우 중요한 인사이트를 도출합니다.

물리적 보안 및 운영 보안

SoftLayer는 광범위한 물리적 보안 옵션과 조직의 요구와 수요에 맞게 조정된 여러 중첩된 계층의 보호를 제공합니다. 예를 들어 SoftLayer 호스팅 위치는 물리적 침입에 대비한 보안을 갖추고 있으며, 서버실은 인증 받은 직원만 액세스할 수 있습니다. 시스템의 경우 관리 직원은 모두 액세스할 수 있지만 다른 사람들의 접근은 금지되어 있습니다.

SoftLayer 인프라에는 마이크로칩 수준에 이르기까지 보안 조치가 포함되어 있습니다. ISO 27001 및 SSAE 16(Statement on Standards for Attestation Engagements No. 16) 표준에 대한 인증을 받았습니다. ISO 27001 인증은 사람, 프로세스 및 IT 시스템이 포함된 위험 관리 프로세스를 적용함으로써, 민감한 정보 관리에 대한 체계적인 접근 방식인 ISMS(Information Security Management System)에 대한 요구 사항을 지원합니다. SSAE 16은 새로운 ISAE 3402 보고서 표준을 반영 및 준수하기 위해 미국 서비스 조직 표준을 업데이트하도록 설계되었습니다. SoftLayer는 추가적인 하드웨어 지원 보안 옵션을 온디맨드로 제공하므로 조직은 요구 사항의 변화에 따라 보안 프로파일을 커스터마이징할 수 있습니다.

네트워크 보안

혁신적인 SoftLayer 네트워크 아키텍처와 첨단 하드웨어 기술을 사용하려는 노력은 네트워크 수준에서 외부 위협에 노출되는 것을 획기적으로 최소화합니다. 이 네트워크는 3개의 개별적이고 중복적인 아키텍처를 멀티티어 네트워크 토폴로지로 통합합니다. 데이터는 캡처되어 SoftLayer 클라우드 인프라로 수집되면서 SSL/HTTPS 보안을 사용하여 암호화됩니다. 고객이 HTTPS를 통해 애플리케이션에 로그인할 때도 이와 유사하게 암호화됩니다. SoftLayer 환경의 방화벽은 데이터베이스에서 애플리케이션까지 솔루션을 분리 및 보호합니다.

사용자 데이터 보호 및 온라인 경험 개선

Tealeaf CX on Cloud에서 온라인 고객 경험에 대해 그 어느 때보다 뛰어난 가시성을 제공하므로 조직은 개별 사용자의 눈을 통해 웹 사이트, 모바일 사이트 및 모바일 애플리케이션이 어떻게 동작하는지 보고 주도적으로 개선해갈 수 있습니다. Tealeaf CX on Cloud를 업계 표준 보안 기능과 연동하면 업계 최고 보안 기술로 민감한 데이터를 보호하면서 실행 가능한 인사이트를 제공할 수 있습니다. 그 결과로 조직은 큰 비용으로 이어질 수 있는 데이터 손실을 방지하고, 가장 엄격한 규정을 준수하면서 브랜드 평판을 보호하며, 고객에게 좀 더 자신 있고 좀 더 나은 온라인 경험을 제공할 수 있습니다.

IBM Tealeaf CX on Cloud는 정보 보안 관리 모범 사례에 대한 프레임워크를 제공하며 국제적으로 인정받는 정보 보안 관리 표준인 ISO 27001 표준에 대한 인증을 획득했습니다. ISO 27001에 따라 IBM Tealeaf CX on Cloud는 정보 보안 위험을 지속적으로 평가하고 이를 해결하도록 적절한 통제와 정책을 구현해야 합니다. 이 인증은 고객의 정보와 데이터를 안전하게 유지하려는 IBM Tealeaf의 약정을 보강합니다. ISO 27001 인증서 보기.

ibm.com/tealeafoncloud를 방문하여 IBM Tealeaf Customer Experience on Cloud에 대해 자세히 알아보십시오.

IBM
Route 100
Somers, NY 10589

Produced in the United States of America
2016년 8월

[1] "IBM Security Named a Leader in Gartner Magic Quadrant for Security Information and Event Management." July 29, 2015. ibm.com/press/us/ en/pressrelease/47397.wss

재활용하십시오.

IMW14864-KRKO-01