클라우드 및 인터넷 환경에서의 안전한 데이터 연계 방안

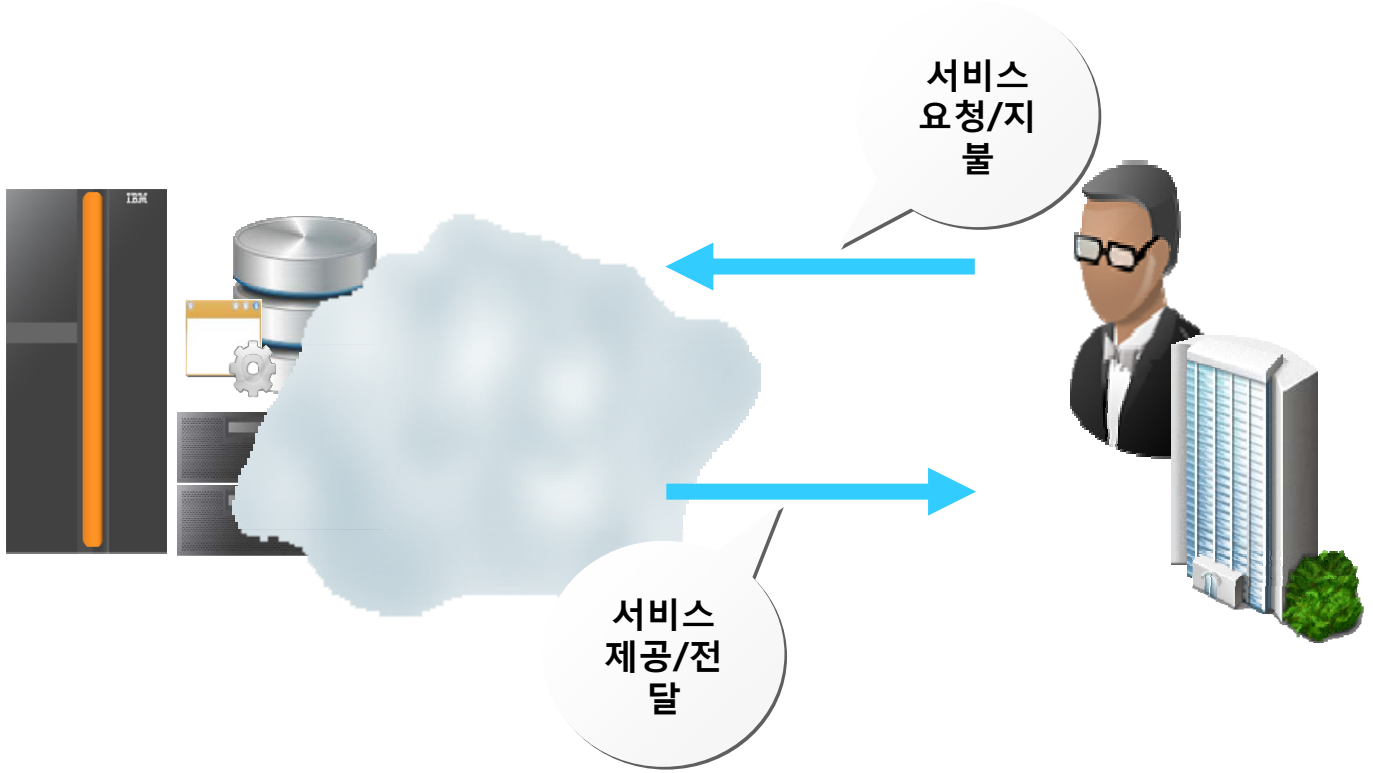
SaaS 통합과 IBM WebSphere DataPower를 중심으로

2011/05/18
한국 IBM 지용득

IBM Security Summit
IBM Security Solutions. Secure By Design.

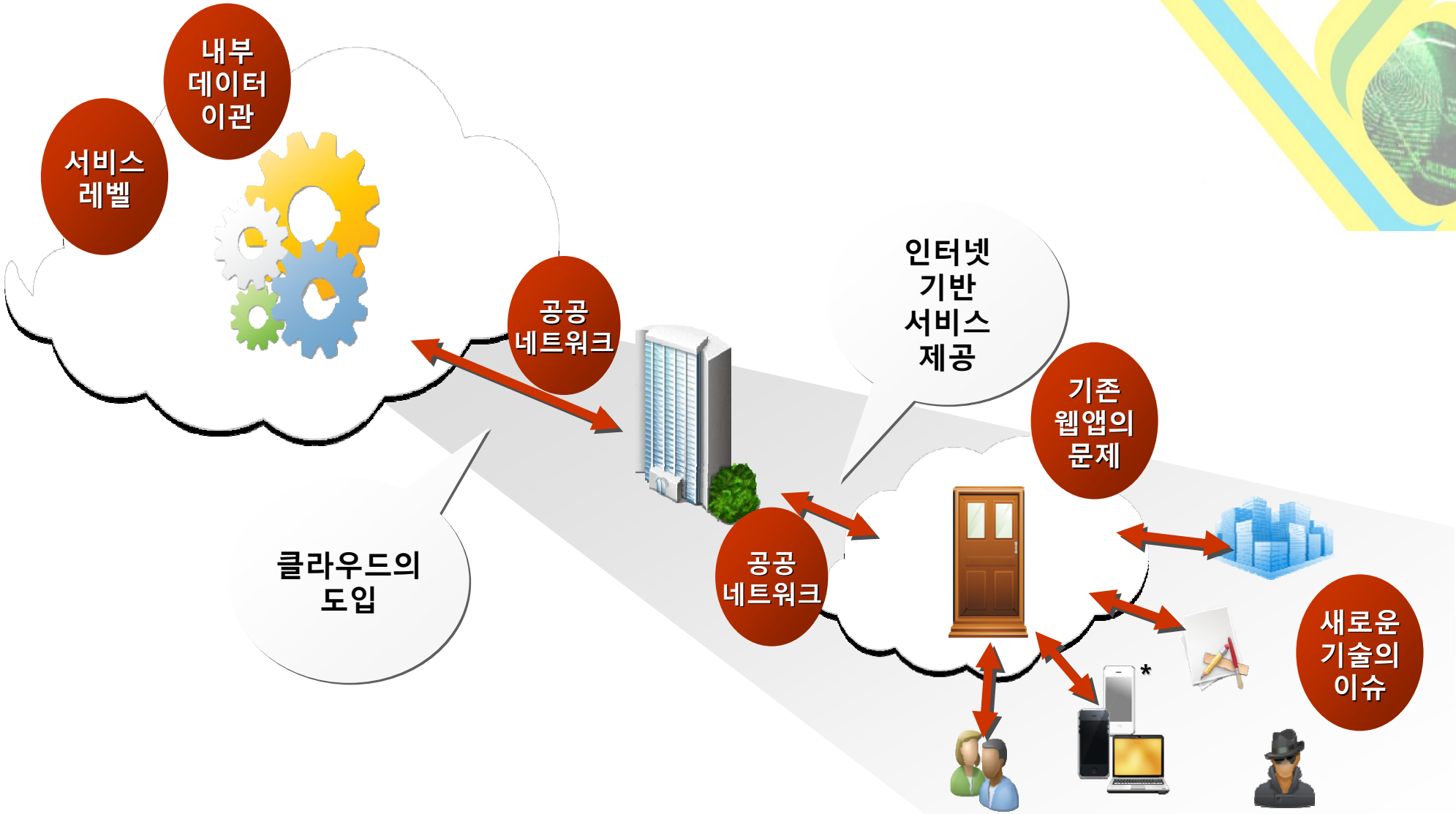
SaaS/클라우드 컴퓨팅 Revisit

- 효율을 높이기 위해 IT 자원의 소유를 피하여 외부로 이전하고
- 신속한 서비스의 제공과 소비에 초점을 둔
- "대체로" 공공 인터넷 망을 경유하는 새로운 IT 서비스 전달 모델



*Icons used by courtesy of Icons Land (http://www.icons-land.com)

클라우드가 가져온 기업 IT 보안의 새로운 지형



*Icons used by courtesy of Sven Vath (http://officinadigitale.forumcommunity.net) and Pixel Mixer (https://www.plimus.com/jsp/buynow.jsp?contractId=2791546)

클라우드가 가져온 기업 IT 보안의 새로운 지형

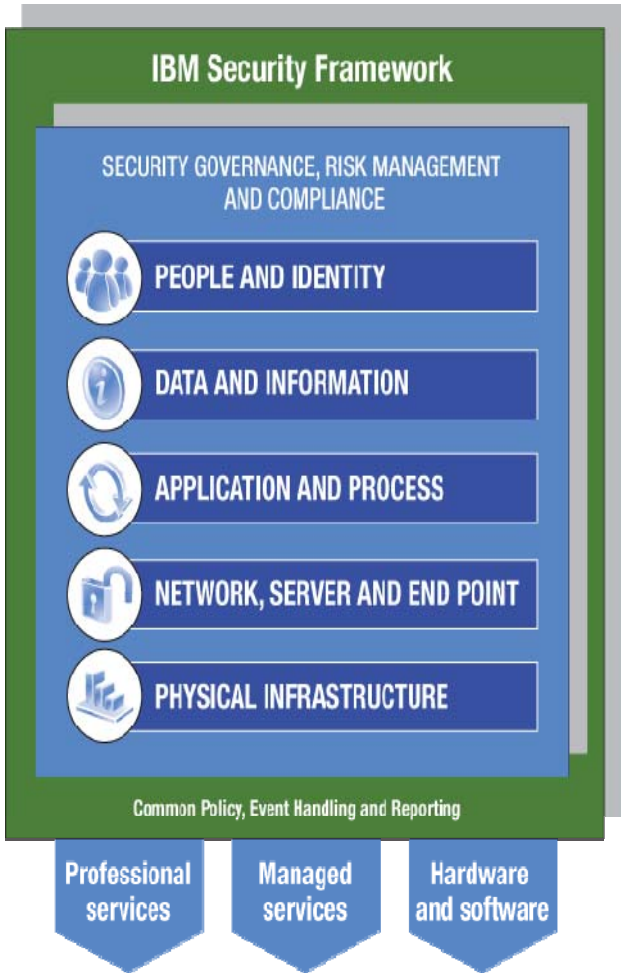
"Cloud/SaaS를 기업에 적용함에 있어서 경영진의 가장 큰 걱정은 데이터 보안과 프라이버시의 문제"

Executive's Top Concerns Regarding SaaS Deployment and Use, Saugatuck Technology

"클라우드를 고려할 때 전체 2/3 이상 기업의 첫 번째 관심사는 바로 보안"

Driving Profitable Growth Through Cloud Computing, IBM

IBM 보안 프레임워크



GRC 거버넌스, 위험 관리와 컴플라이언스

사람과 아이덴터티

데이터와 정보

어플리케이션과 프로세스

네트워크, 서버와 단말 등 IT 인프라

물리적 인프라

안전한 클라우드 서비스 공급과 이용을 위한 노력

클라우드 서비스에 보안 기능이 포함되어 제공되는 영역

클라우드 서비스에 보안 기능이 포함되며 동시에 이용자의 참여가 필요한 영역

SaaS 데이터 전송과 세션에 대한 보안

서비스 수준 모니터링

SLA 부과,
수행, 기록

Granular
접근 제어

접근제어

계정, 토큰, IP,
자격증명
인증

인증

기밀성,
정합성,
데이터
유효성

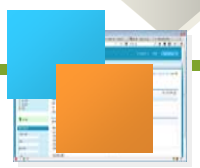
데이터 보안

API(SOAP/RESTFul)

웹 앱(JSP/ASP/HTML)

기타 접근(FTP/SMTP)

애플리케이션



UI Mashup

각종 클라이언트
애플리케이션

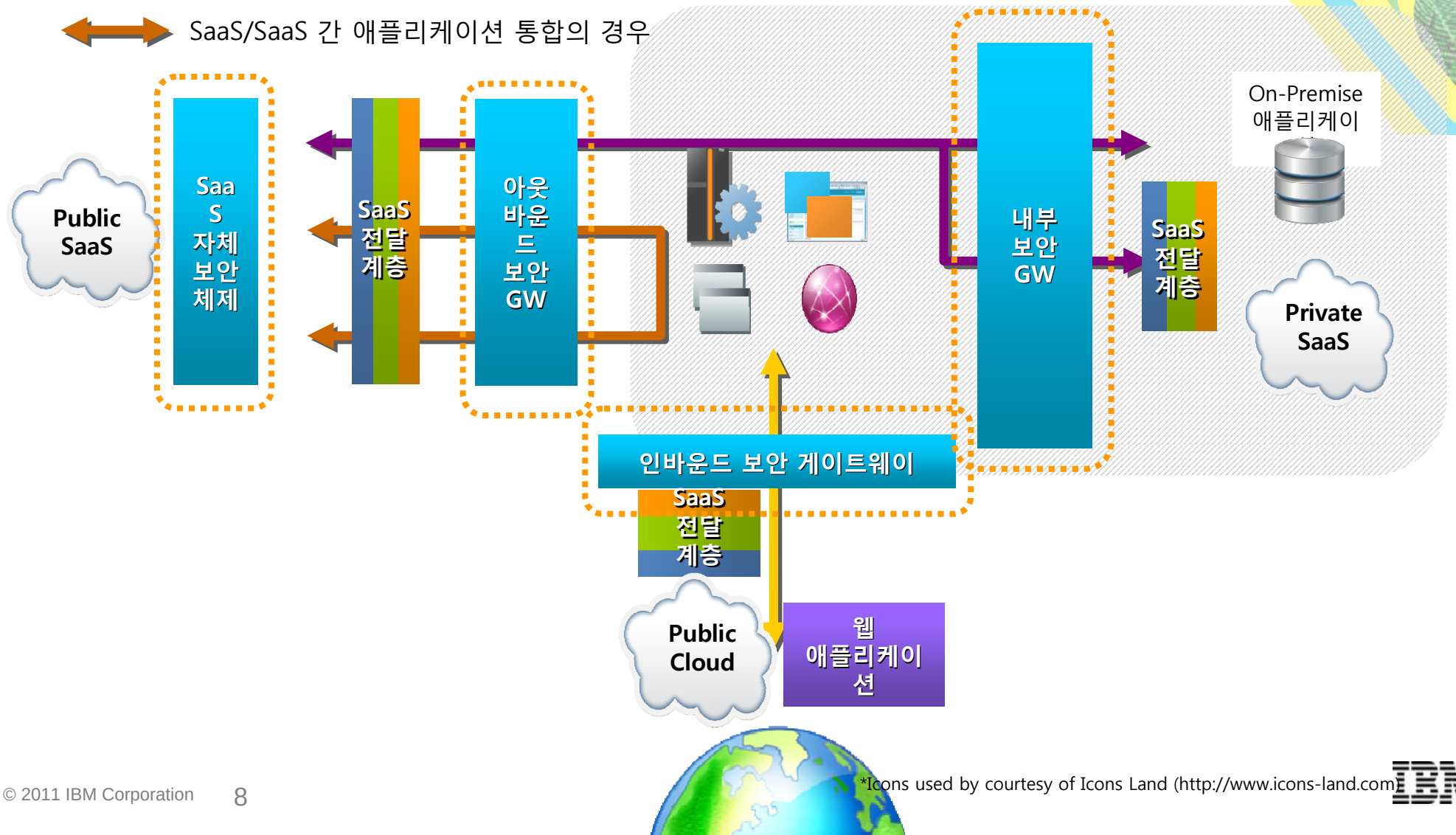
웹 브라우저

SaaS 보안 영역: 엔터프라이즈 관점

SaaS/On-Premise 간 애플리케이션 통합의 경우

On-Premise 애플리케이션의 외부 노출의 경우

SaaS/SaaS 간 애플리케이션 통합의 경우



*Icons used by courtesy of Icons Land (http://www.icons-land.com)

기업 IT에 있어 SaaS로의 이행은...

1. *SaaS와 기업 내부(On-Premise)의 애플리케이션 간의 통합 또는 이전에 요구되는 Connectivity의 구현의 필요*

2. *SaaS와 On-Premise 애플리케이션 간의 통합 또는 이전에 있어서 발생하는 데이터 전송 과정 내 보안성 확보의 필요*

3. *인터넷 기반 Public SaaS 또는 일반적인 웹 애플리케이션을 통해 외부로 서비스함에 있어서 서비스 레벨을 위해 보안성과 동시에 성능 확보의 필요*

기업 IT에 있어 SaaS로의 이행은...

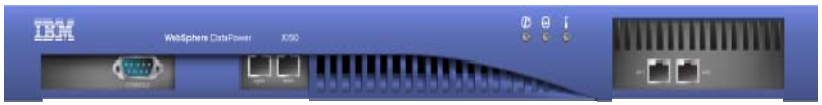
1. *주요 SaaS 공급자는 Web Services/REST와 같은 HTTP 기반의 API나 인터페이스를 제공하여 사용자와 애플리케이션에 접근성 제공*

2. *주요 SaaS 공급자는 공공 네트워크 환경에서의 보안성을 위해 위의 언급된 기술 기반의 데이터 보안과 사용자 인증 체계를 제공*

3. *SaaS 공급자와 더불어 SaaS를 이용하는 사용자 또한 제공된 보안 체제를 따르기 위해 보안 정책을 부과를 목적으로 보안 게이트웨이를 요구*

WebSphere DataPower SOA 어플라이언스

WebSphere DataPower SOA Appliance XI50



WebSphere DataPower SOA Appliance XS40

높은 보안성의 장비

단순한 어플라이언스 접근

특화된 하드웨어 가속기능

서비스 거버넌스

애플리케이션/클라우드 통합

WebSphere DataPower 보안성 하이라이트

- **보안 목적을 위해 디자인된 하드웨어**
  - 밀봉되어 변경이 불가능한 하드웨어 케이스: 자체 파괴 기능 내장
  - USB 포트와 같은 외부 데이터 포트 배제: 외부 데이터 유입 불가능
  - 디폴트 구성은 Lock Down 구조: White List 구조
  - HSM(Hardware Security Module) 지원: 실제 키로 보안성 향상
  - 충실한 감사 로그(Audit Log): 관리 책임 추적

전용 하드웨어로 성능 저감 최소화

- **DataPower의 강력한 보안의 펌웨어 구조**
  - IBM에 의해 서명되고 암호화된 펌웨어 이미지: 위변조 불가능
  - 범용이 아닌 자체 OS: DPOS
  - 소프트웨어나 라이브러리 등 확장 기능 불허: 취약성 원천 차단

DMZ Ready!

써드 파티 보안 인증

Common Criteria EAL4
FIPS 140-2 Level 3 (with optional HSM)
Drummond Group AS2

DataPower SOA 어플라이언스 = XML 방화벽

손쉬운 설정
(Zero Coding)
위주의
데이터 보안

XML/SOAP
위협 감지

- Entity Expansion
- Recursion Attacks
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- Replay Attack
- Message Tampering
- Message Snooping
- XPath/SQL Injection
- XML Encapsulation
- XML Virus
- Schema Validation

XML/SOAP
암/복호화

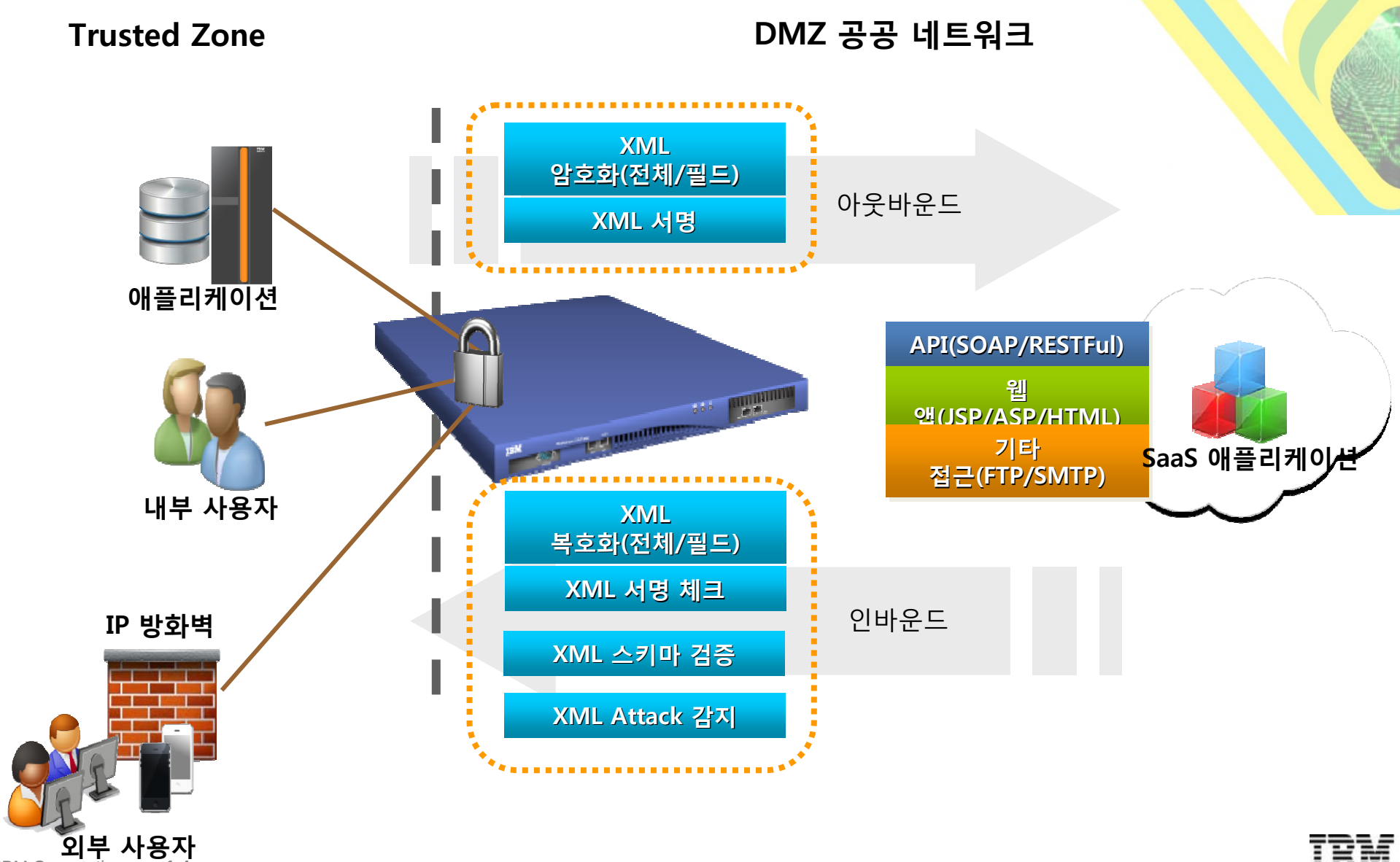
- XML 표준 암/복호화
- WS-Security 지원
- 메시지 전체 암복호화
- 필드 단위의 암복호화
- SSL Initialization
- Termination
- 커스텀 암복호화

XML/SOAP
데이터
검증

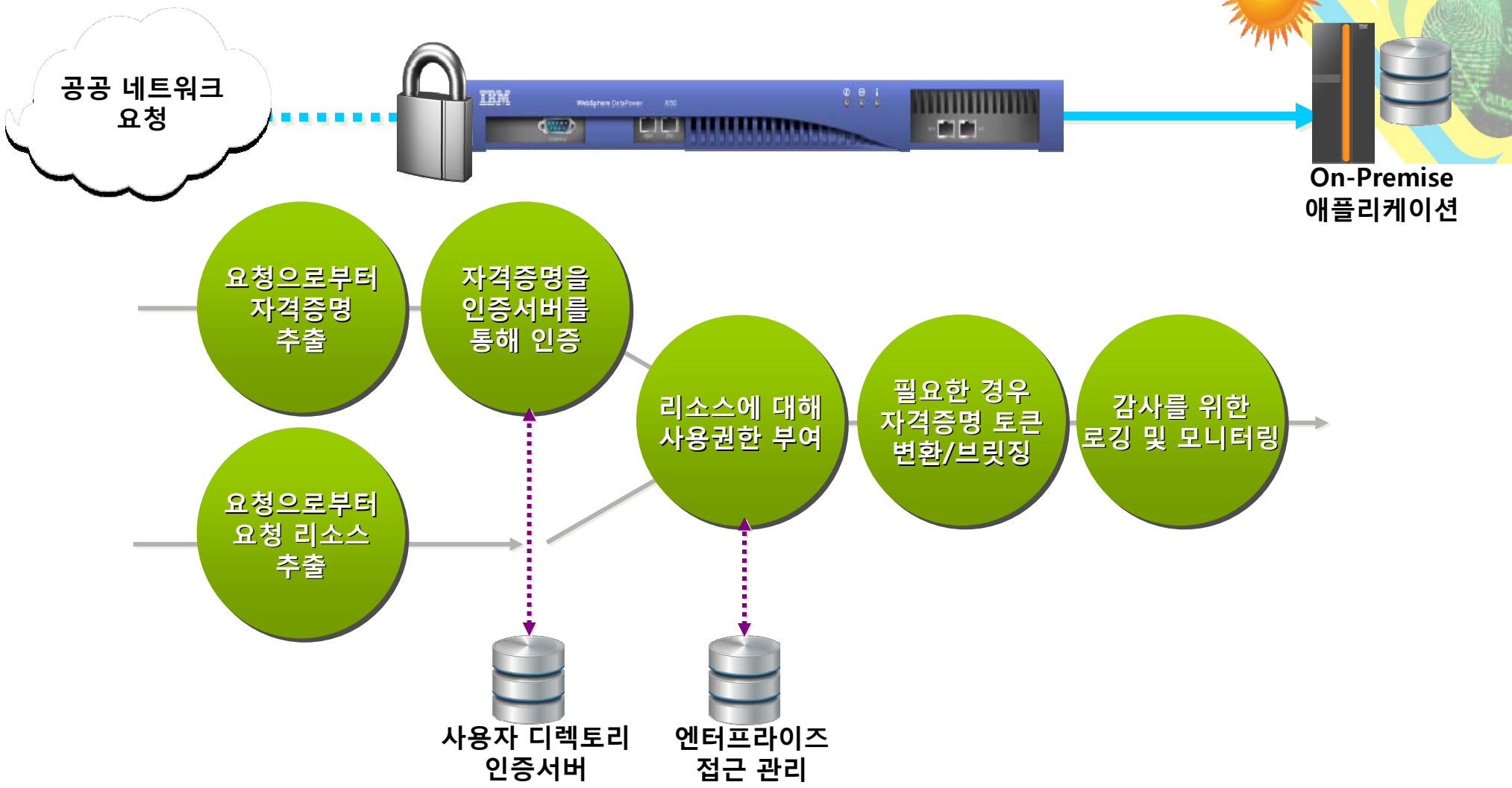
- XML 전자 서명
- XML 전자 서명 검증

DataPower SOA 어플라이언스는 XML 및 데이터를 인식하는 Layer 7 보안 장비

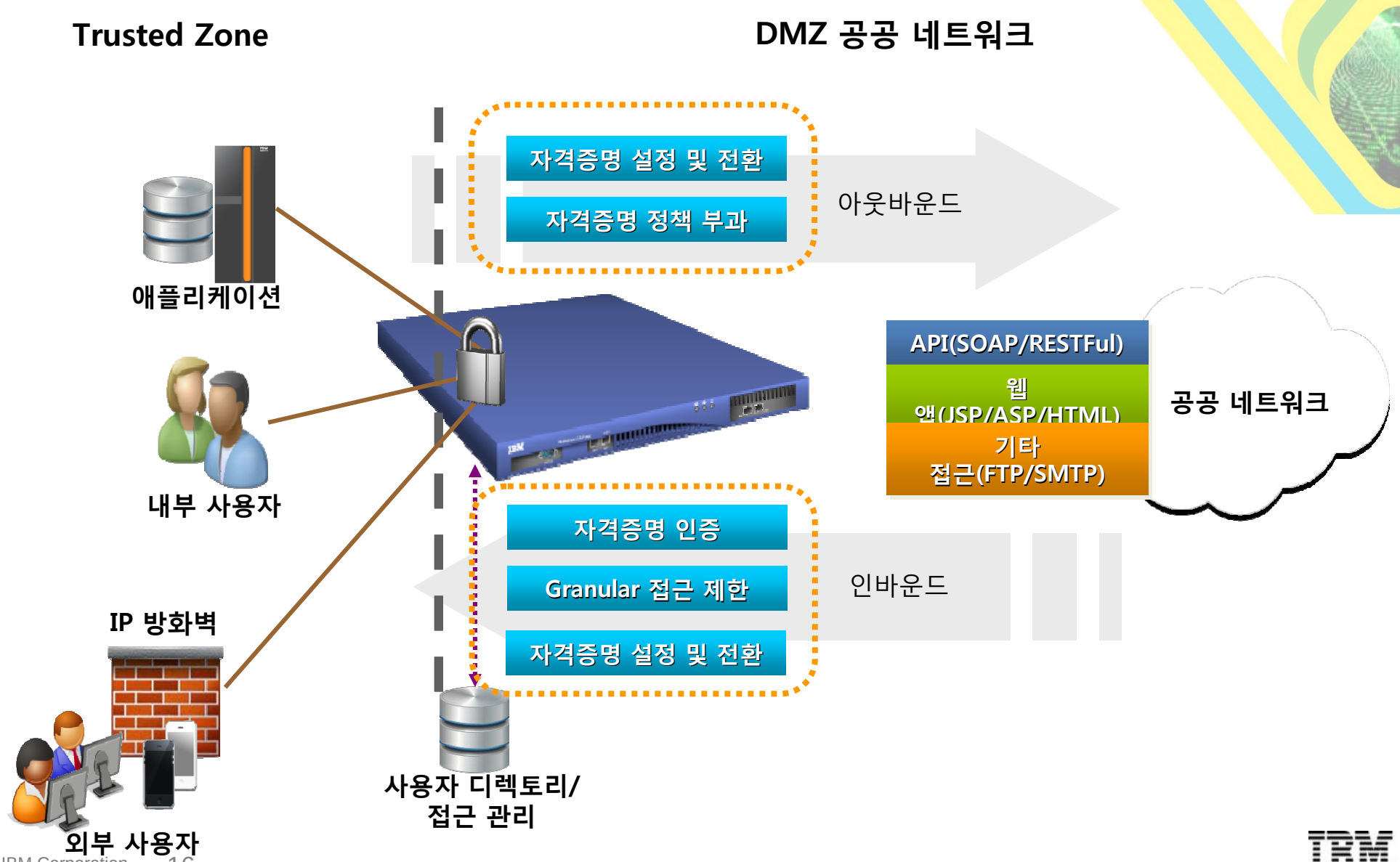
DataPower SOA 어플라이언스 = XML 방화벽



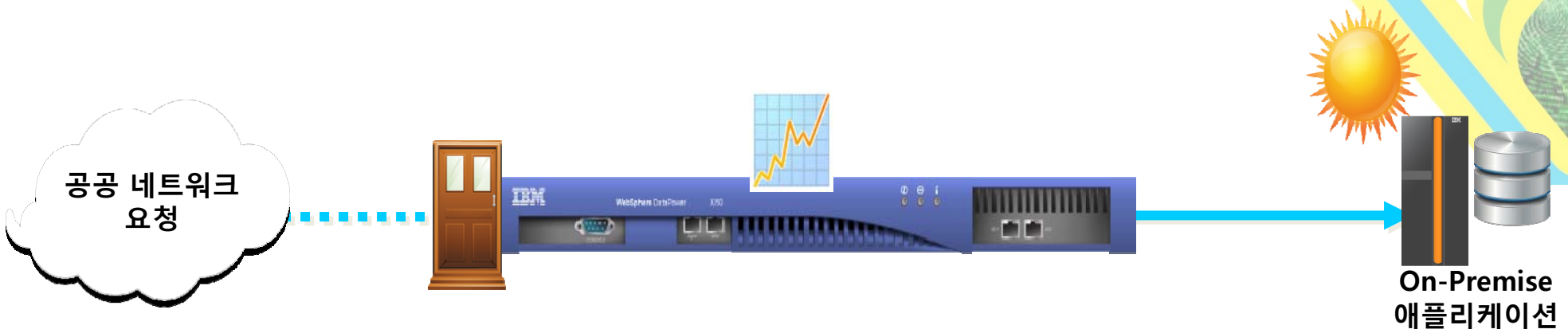
Authenticate, Authorize, Audit(AAA)



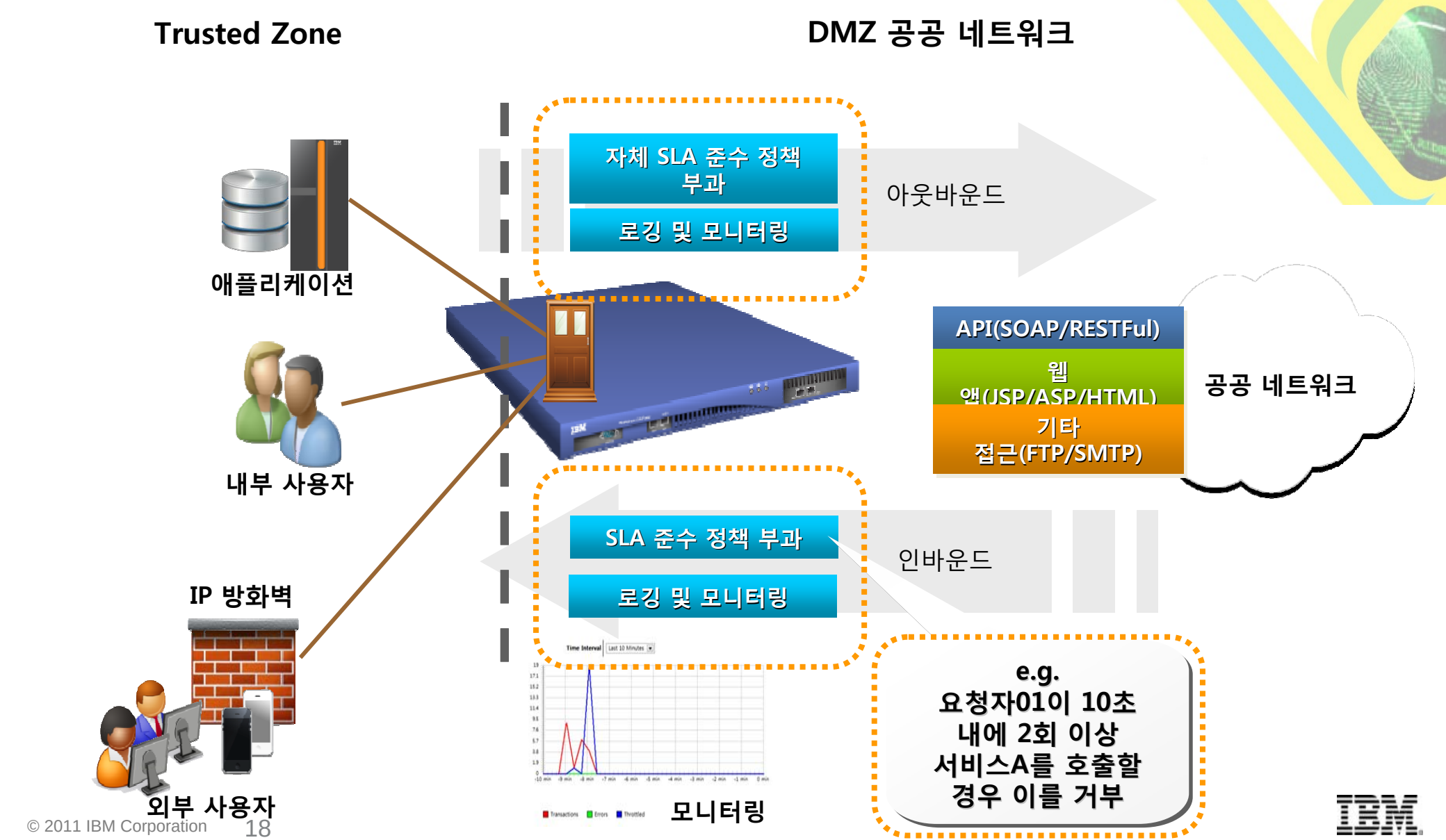
Authenticate, Authorize, Audit(AAA)



서비스 수준 모니터링(Service Level Monitoring)



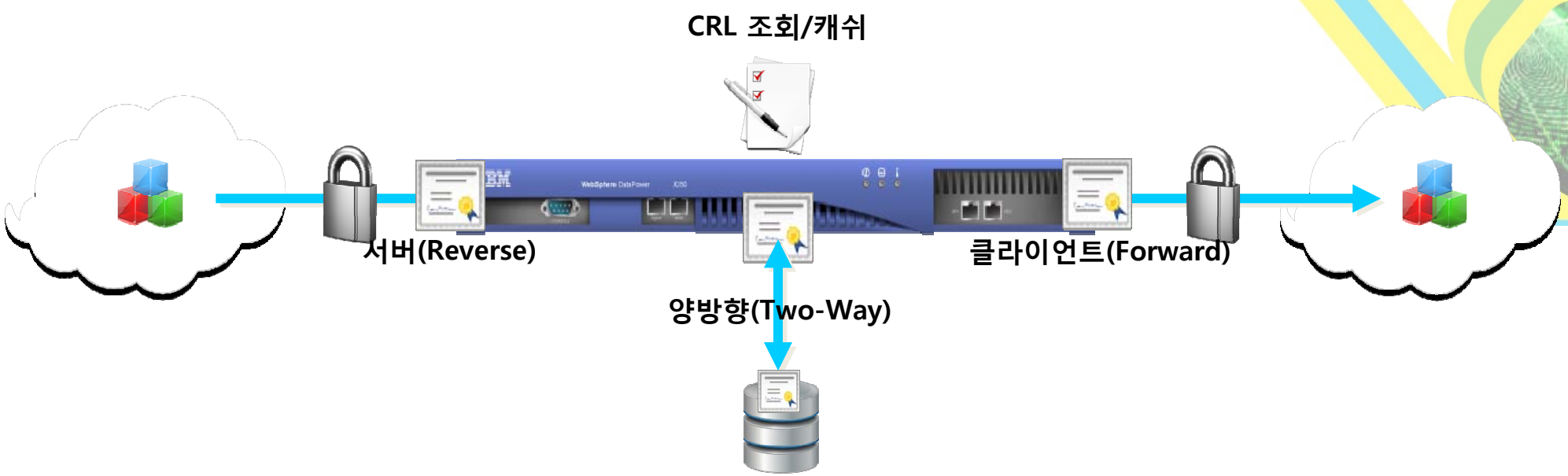
서비스 수준 모니터링(Service Level Monitoring)



DataPower Secure Cloud Connector

- On-Premise 영역과 클라우드 간의 보안 채널 생성
- 대부분의 클라우드 공급자에 적용 가능한 표준 프로토콜 기반(SSH)
- 생성된 단일 채널에 위에 다중의 양방향 연결 생성
- 전송 계층에서의 트래픽에 대한 암복호화
- 다른 DataPower 보안 기능과 병용으로 보안성 극대화
- Application Optimization 옵션의 기능 중 하나로 제공

DataPower SSL 지원



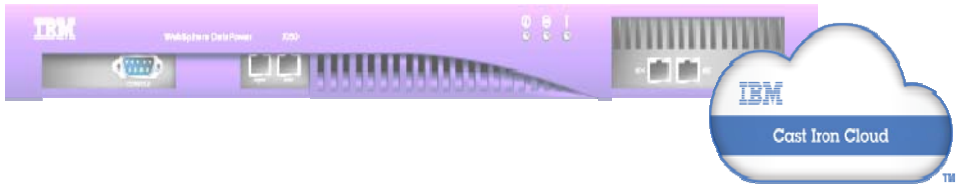
- SSL Proxy 서비스로 Forward/Reverse/Two-Way 모드 모두 지원
- 빠른 속도로 데이터 기밀성, 정합성, 서버/클라이언트 상호 인증 실행
- 중간 참조 서버(e.g. 인증 서버)와의 연결에도 사용
- 웹 애플리케이션에서 범용적으로 쓰이는 접근성

WebSphere DataPower Cast Iron 어플라이언스

WebSphere DataPower Cast Iron XH40

WebSphere DataPower Cast Iron XH40 Hypervisor Edition

WebSphere DataPower Cast Iron Live on Cloud

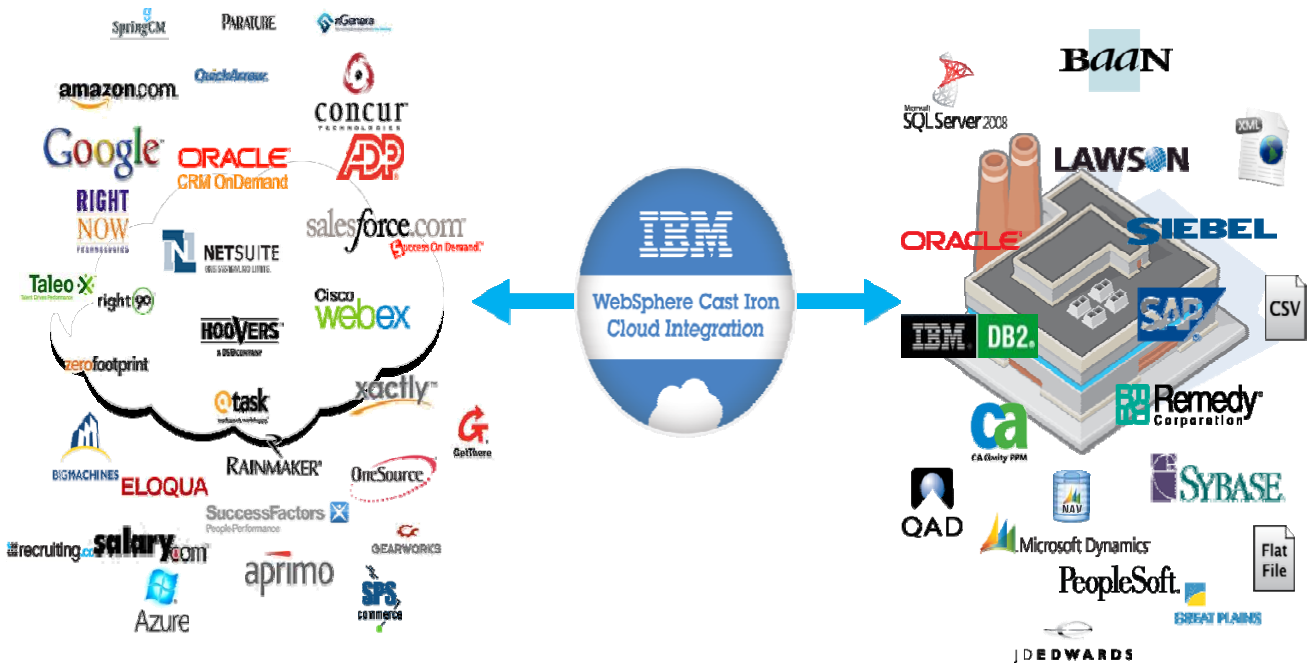


On-Premise 애플리케이션/
SaaS 애플리케이션 통합

WebSphere DataPower Cast Iron 하이라이트

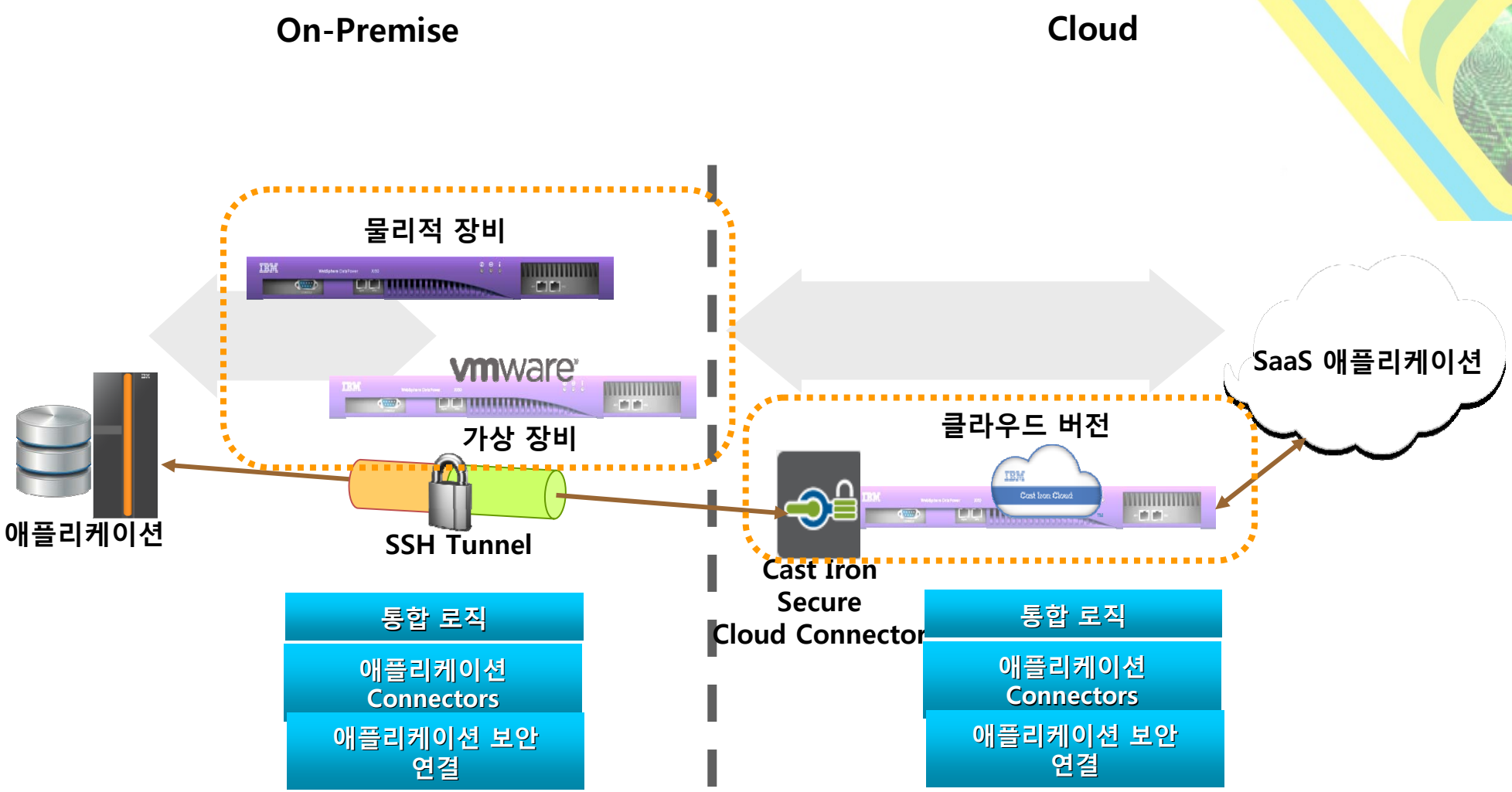
- **SaaS/클라우드와 On-Premise 애플리케이션 간의 신속하고 쉬운 통합을 위한 어플라이언스**
  - 주요한 SaaS/클라우드 서비스에 대한 Connector 제공: Salesforce.com, NetSuite, Google Apps, Taleo…
  - 주요한 On-Premise 애플리케이션에 대한 Connector 제공: SAP, Oracle, PeopleSoft, Siebel…
  - 통합 패턴에 대한 템플릿 제공으로 신속하고 용이한 통합 로직 작성

클라우드 (Internet)

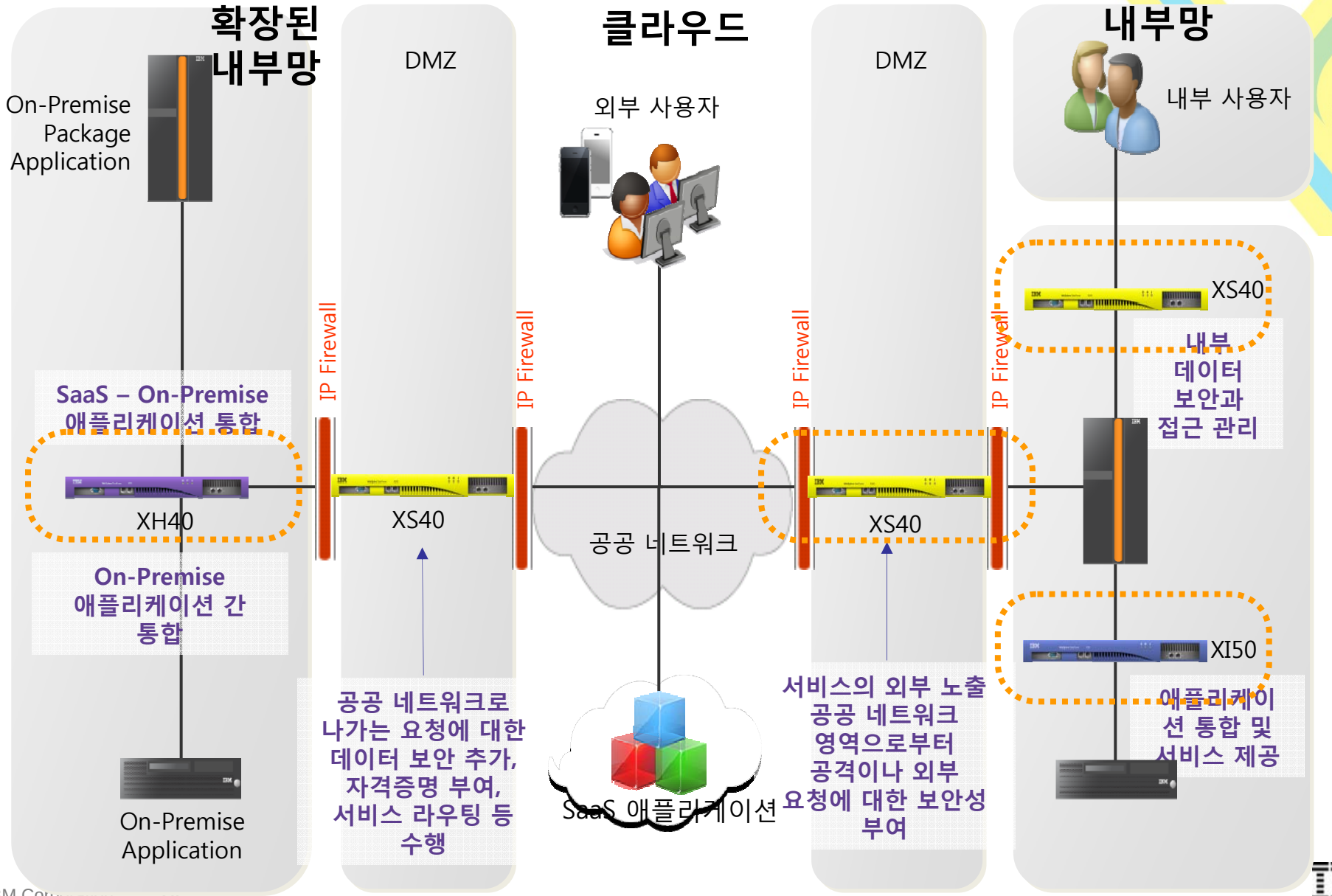


엔터프라이즈 (On-Premise)

WebSphere DataPower Cast Iron 통합 모델



DataPower SOA 어플라이언스 + Cast Iron

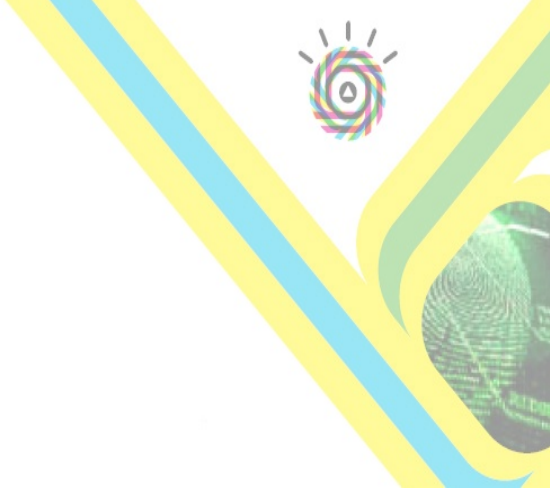


요약

1. SaaS의 도입은 기존의 IT 환경에 연결(Connectivity)와 보안이라는 새로운 요건을 초래하게 됨

2. IBM WebSphere DataPower 어플라이언스 제품군은 SaaS의 도입에 있어 애플리케이션들 간의 연결과 보안성을 위해 디자인된 전용 하드웨어

3. IBM WebSphere DataPower 어플라이언스 제품군은 클라우드/SaaS의 제공자/이용자 모두를 위한 보안성을 확보하면서도 성능 저감은 최소화



고맙습니다