Database Management
and Security

WARE VALLEY

DB보안의 첫걸음

접근통제와 비정형 쿼리 관리

2019 데이터 그랜드 컨퍼런스

㈜ 웨어밸리 김민경 이사

데이터베이스 보안 위협의 10가지

1. 과도한 권한과 사용하지 않는 권한
2. 권한 남용
3. SQL Injection
4. Malware
5. 약한 감사 추적
6. 저장 매체 노출
7. 취약하고 잘 못 구성된 데이터베이스의 악용
8. 관리되지 않는 민감한 데이터
9. Denial of Service Attack
10. 보안 전문 지식과 교육의 부족

Source : 2015 Verizon Data Breach Report

데이터베이스 취약점과 잘못된 설정 10가지

1. 기본, 공백 및 약한 사용자 이름과 암호
2. SQL Injection
3. 과도한 사용자 및 그룹 권한
4. 불필요하게 활성화 된 데이터베이스 기능
5. 손상된 구성 관리
6. Buffer Overflows
7. 권한 상승
8. Denial of Service Attack
9. 패치되지 않은 데이터베이스
10. 암호화되지 않은 민감한 데이터

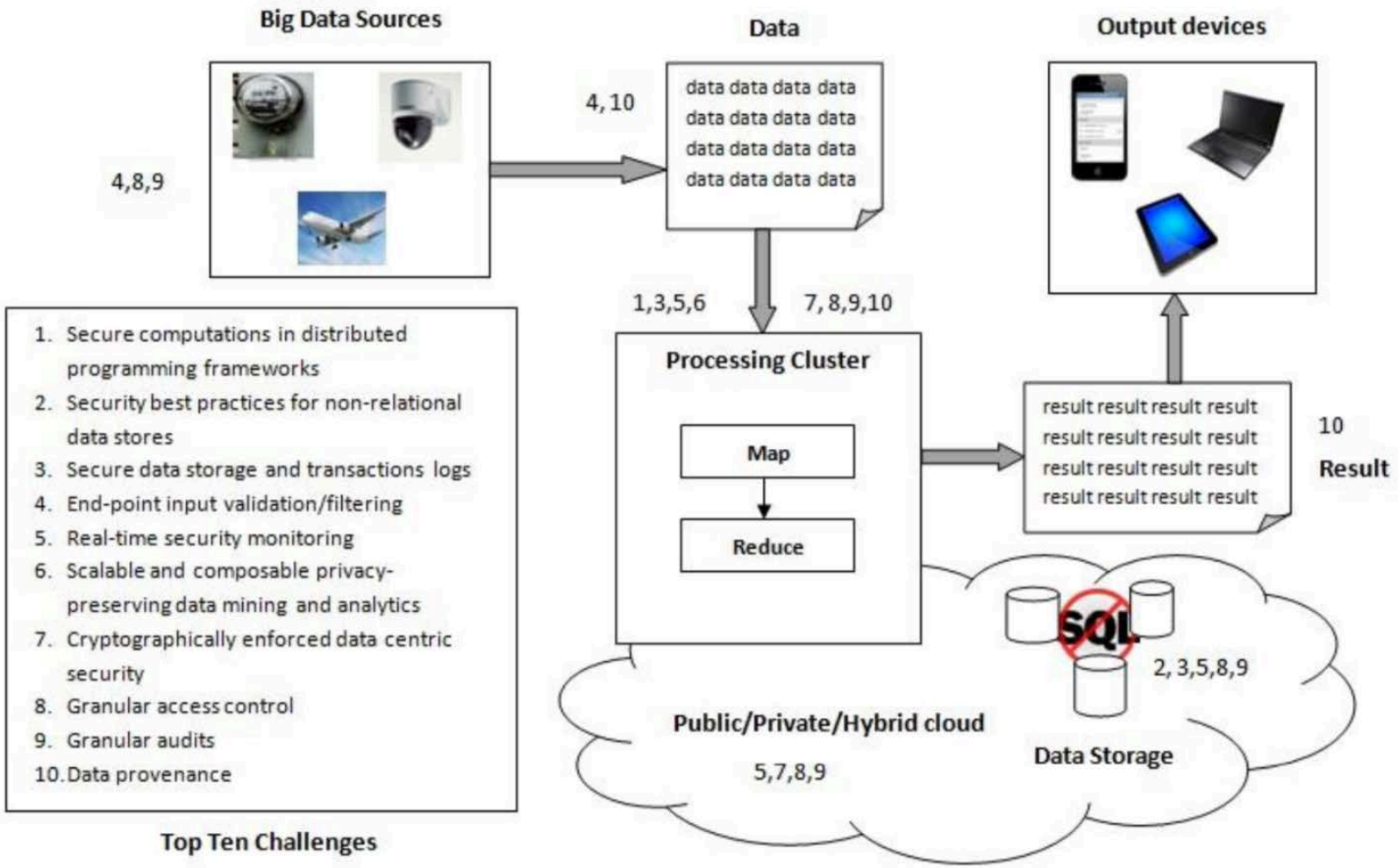
Source : Team SHATTER

Big Data Security Issues

- Vulnerability to fake data generation
- Potential presence of untrusted mappers
- Troubles of cryptographic protection
- Possibility of sensitive information mining
- Struggles of granular access control
- Data provenance difficulties
- High speed of NoSQL databases' evolution and lack of security focus
- Absent security audits

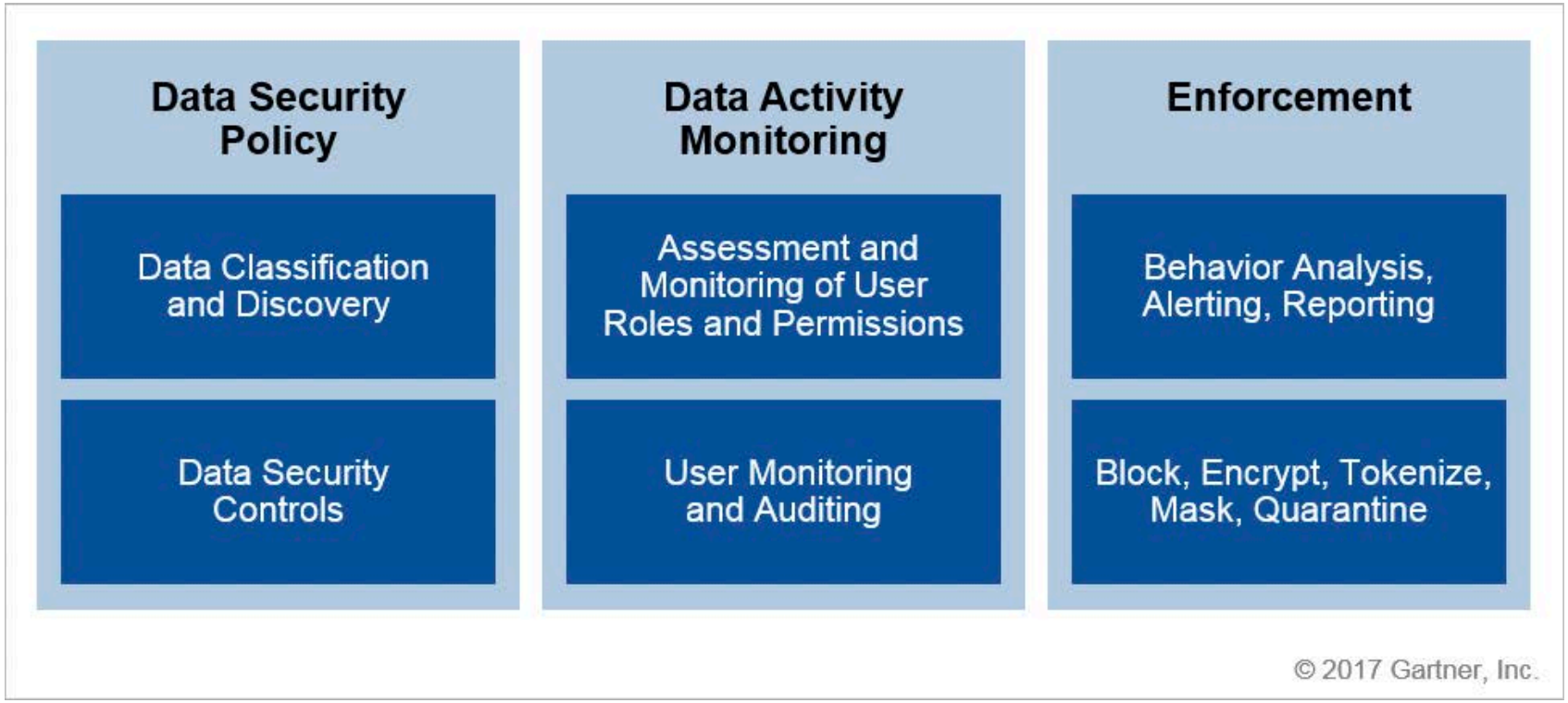
Source : A. Bekker. ScienceSoft

Big Data Security Challenges



Source : S. Rajan. Expanded Top Ten Big Data Security and Privacy Challenges

DCAP Capabilities offered by Vendors



Source : Gartner (Nov. 2017)

DCAP Capabilities

- Data Classification Discovery
  - Terms of speed and false-positive performance
  - A specific DBMS, file type, Hadoop or cloud
  - column/table metadata or within fields
  - a binary large object (BLOB) or character large object (CLOB)
  - unstructured files and rely on tagging
- Data Security Policy Management
  - based on user identities and business roles
  - identify individual users at the application level
- Monitoring User Privileges and Data Access Activity
  - monitor for changes to individual privileges.
  - detect changes and create alerts for privilege escalation or for changes to data
  - be able to intercept access by various administrators

Source : Gartner (Nov. 2017)

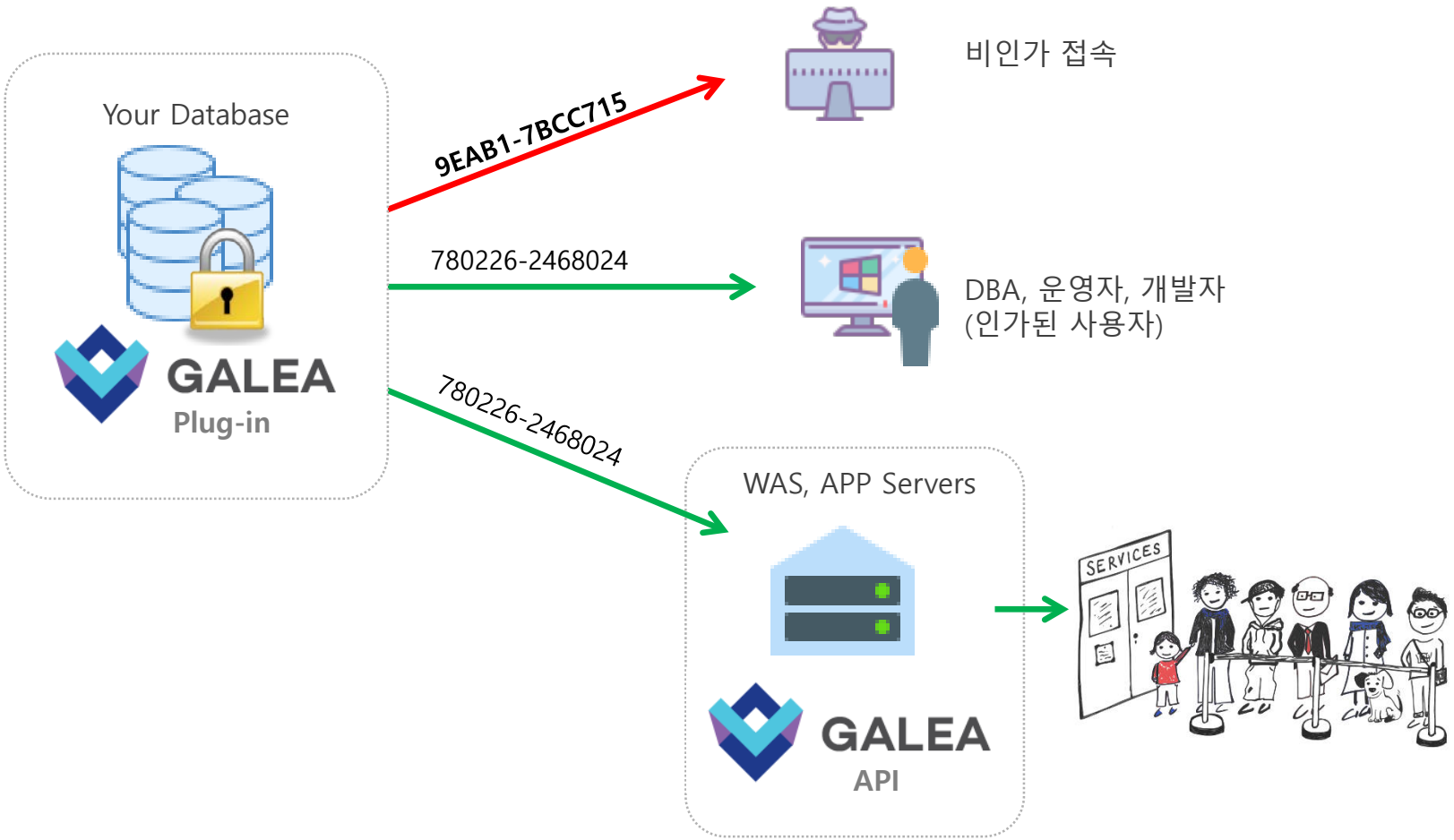
DCAP Capabilities

- Auditing and Reporting
  - require an audit trail, such as unusual user behaviors, changes to data, policy violations or changes to privileges.
  - be able to use the audit logs as a forensic analysis aid to investigate all activities including access, data changes or privileges.
- Behavior Analysis, Alerting and Blocking
  - An ability to create security alerts based upon preselected monitoring
  - Future products may even correlate rules to detect unusual behaviors.
  - The ability to analyze historical access trends will provide increasingly important forensic insights to detect inappropriate behaviors.
- Data Protection
  - encryption, tokenization or data masking

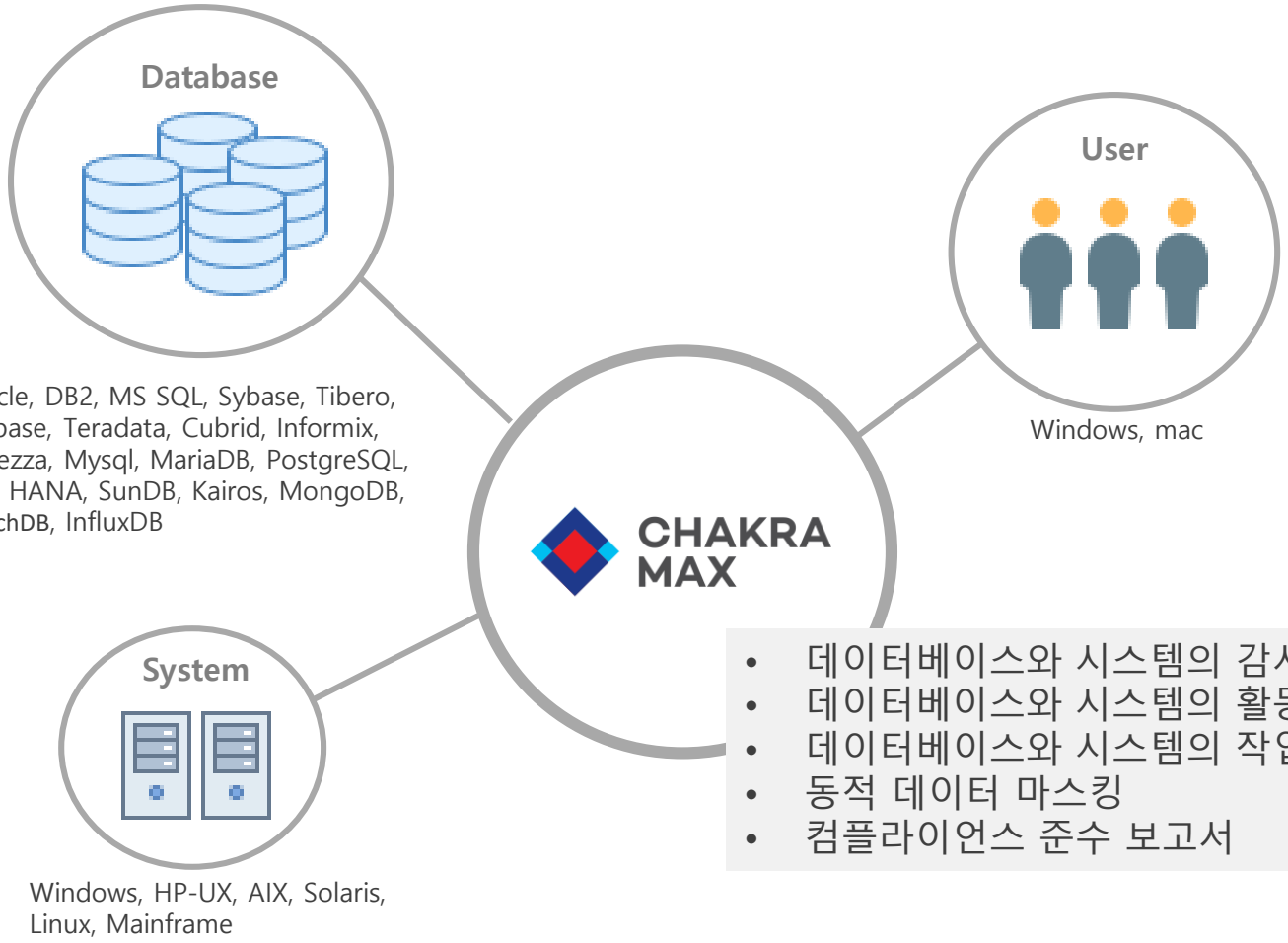
Source : Gartner (Nov. 2017)

WAREVALLEY : Database Security and Management

Galea : Column Level Database Encryption

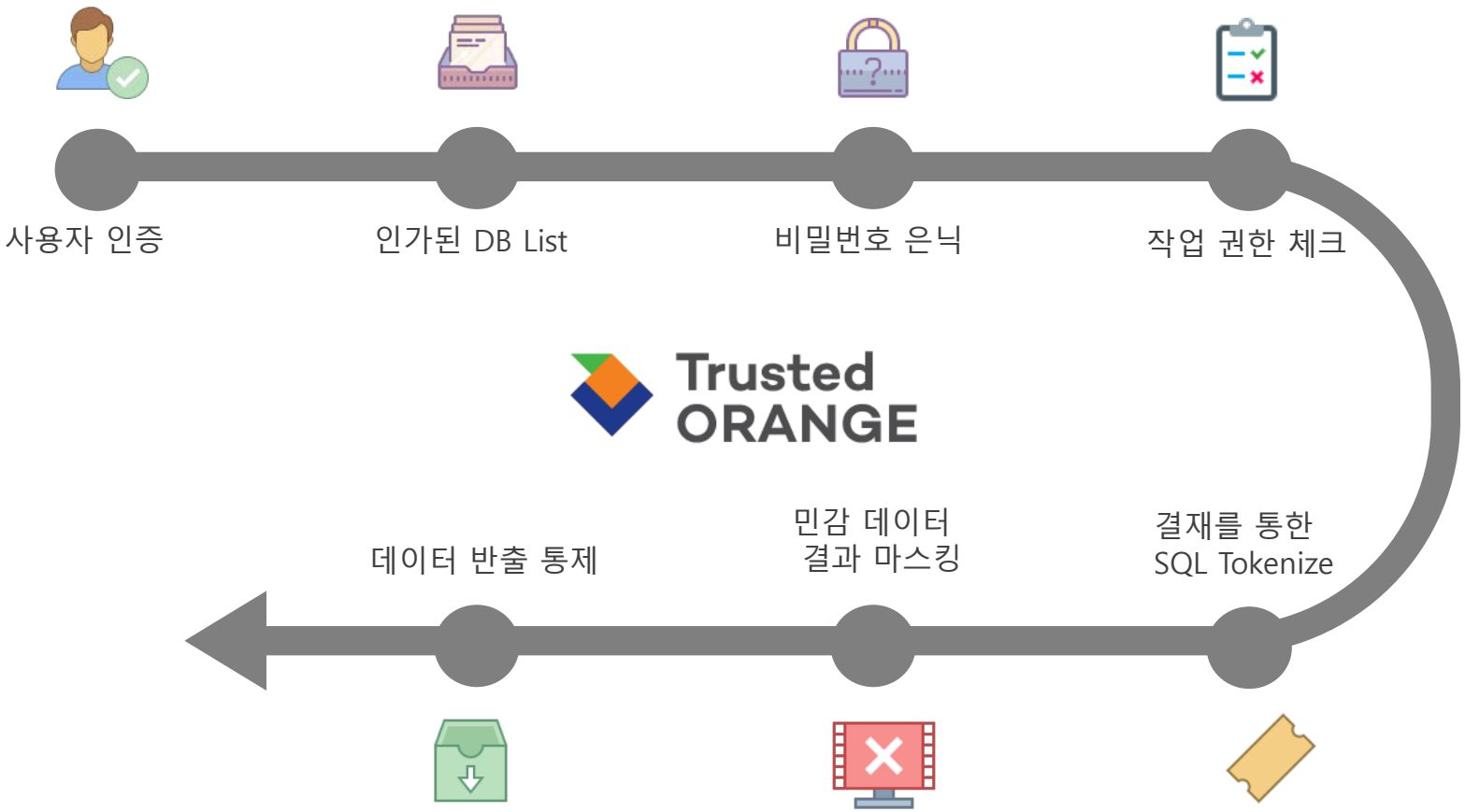


Chakra MAX : Database, System Audit and Protection

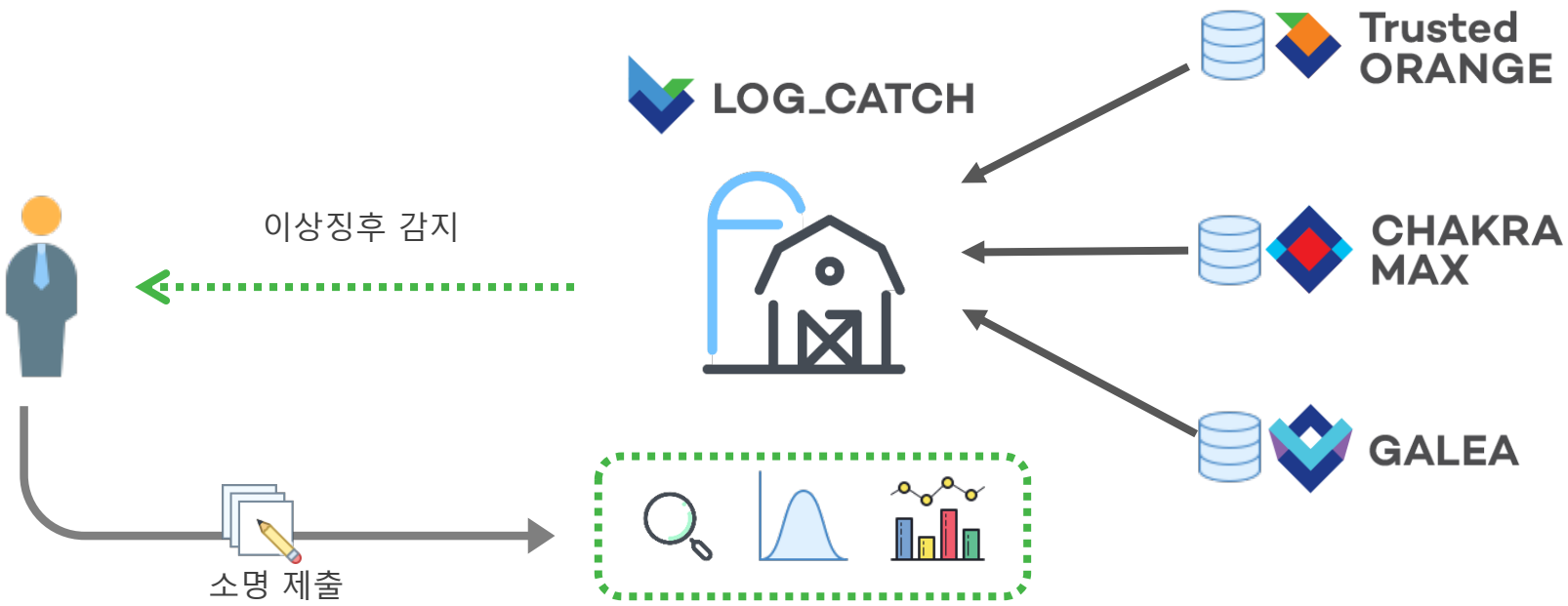


- 데이터베이스와 시스템의 감사와 차단
- 데이터베이스와 시스템의 활동 모니터링
- 데이터베이스와 시스템의 작업 결재 프로세스
- 동적 데이터 마스킹
- 컴플라이언스 준수 보고서

Trusted Orange : Database Privilege



LogCatch : Behavior Analysis



Thank you!

mkkim@warevalley.com
http://www.warevalley.com

(주) 웨어밸리