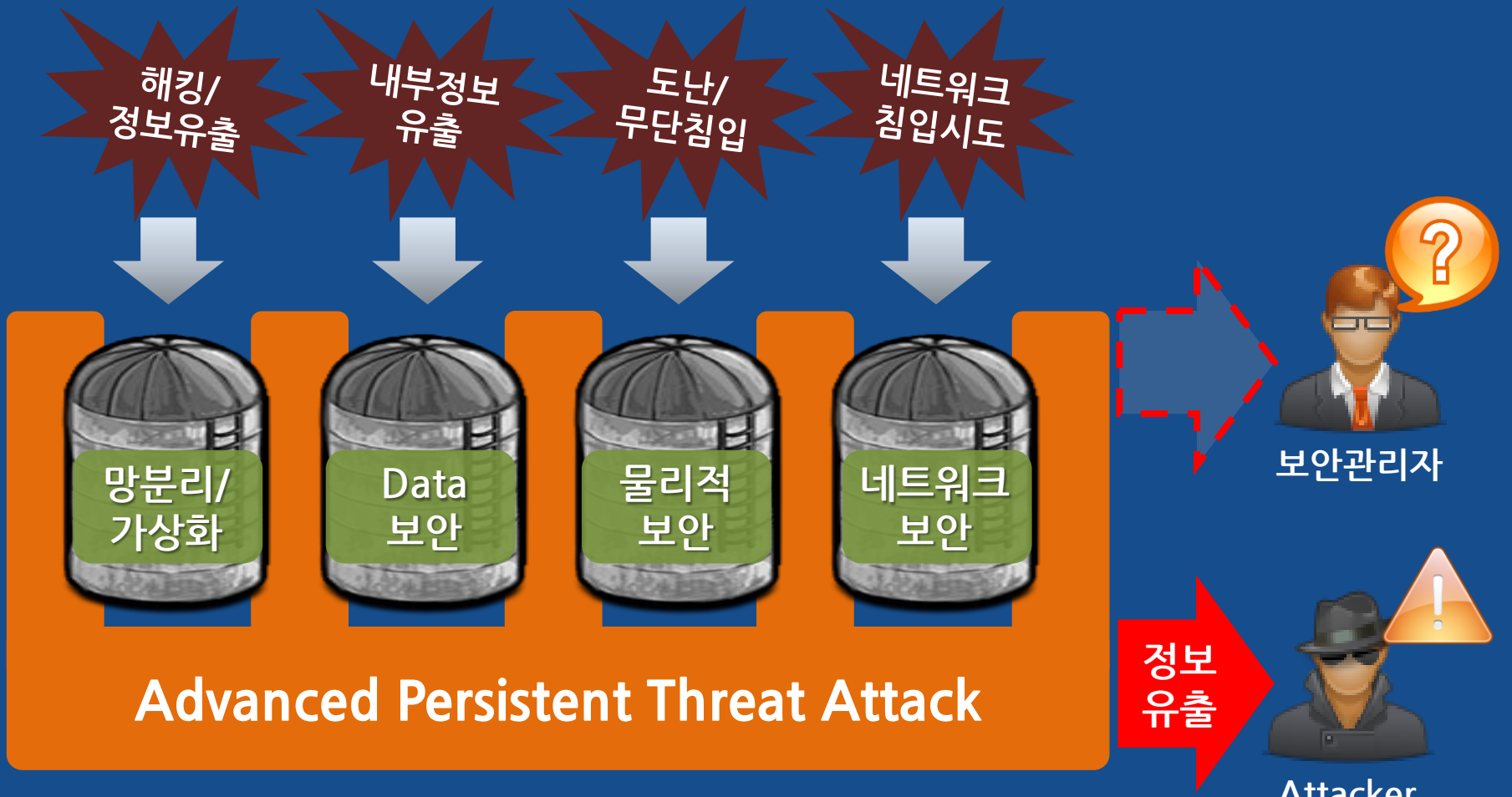
APT 대응,
데이터 거버넌스 확보와 위험관리 전략

주현주 컨설팅팀장

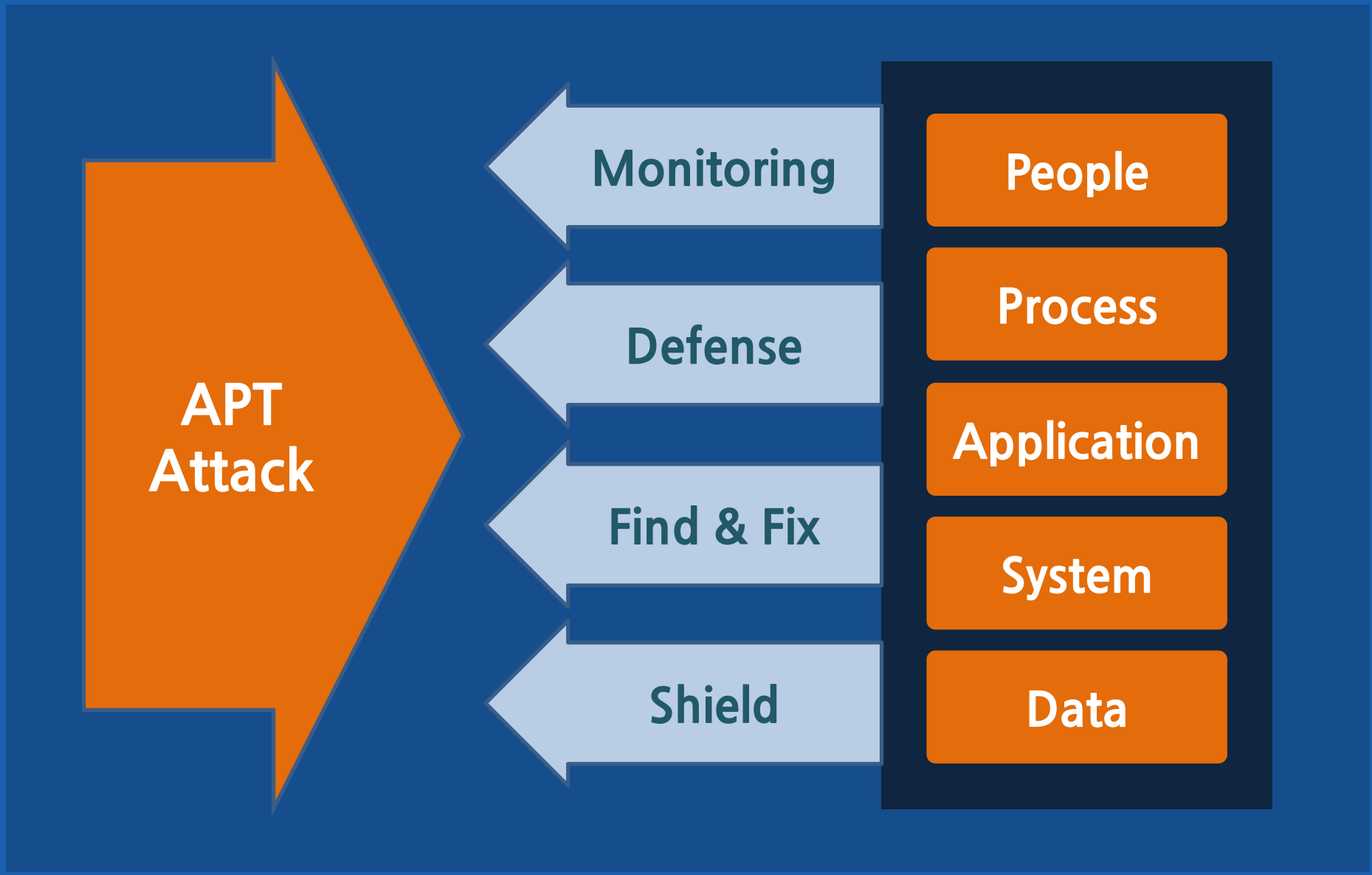
Fasoo

Perimeter-based Security & APT Attack

단위 보안 시스템들은 APT 공격을 효과적으로 방어하고 있을까?

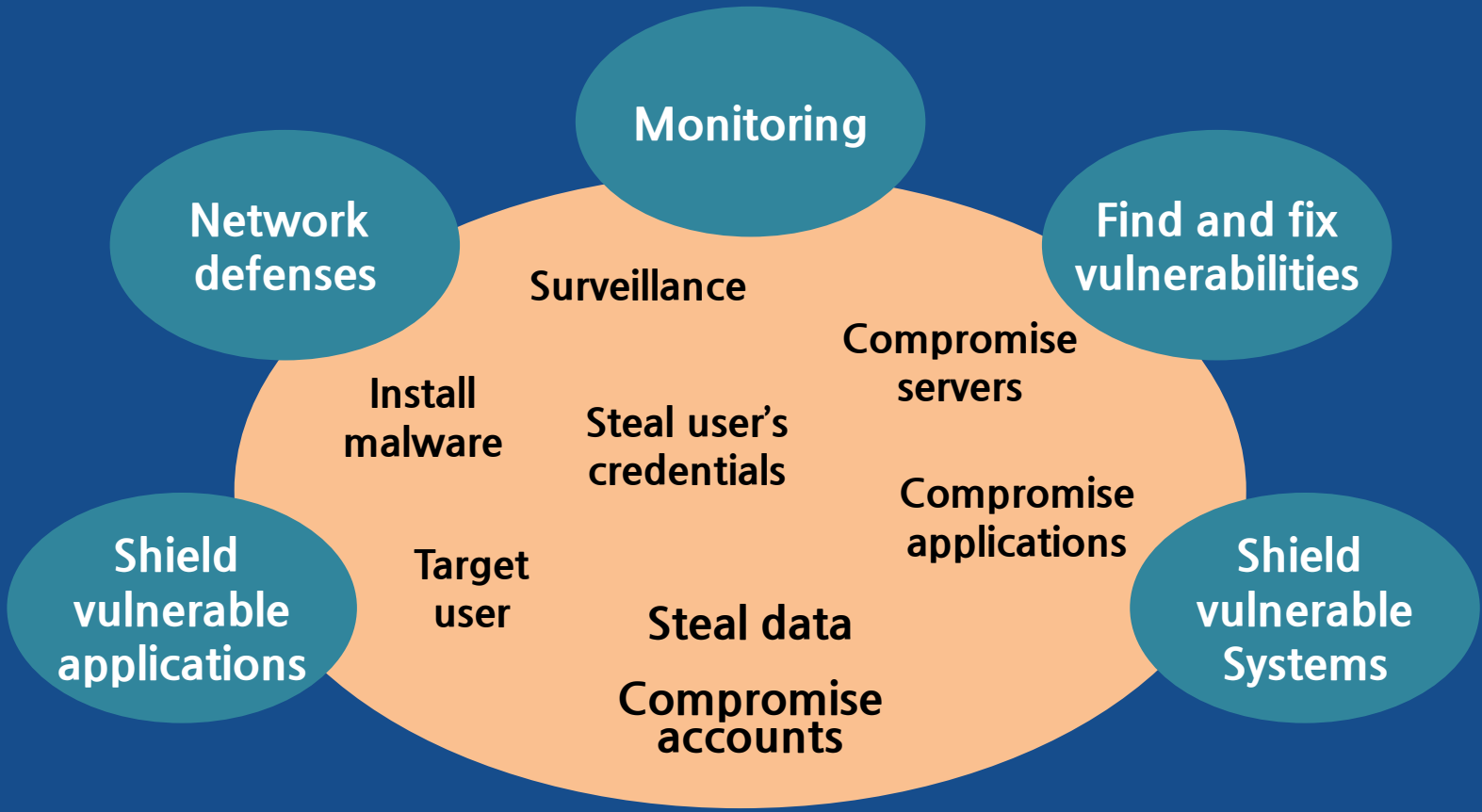


APT 공격 대응 전략


APT
Attack
Monitoring
Defense
Find & Fix
Shield
People
Process
Application
System
Data

Global security trends (Gartner)

“ Perfect defenses are not achievable. ”
“ Data Encryption & better detection is also required. ”

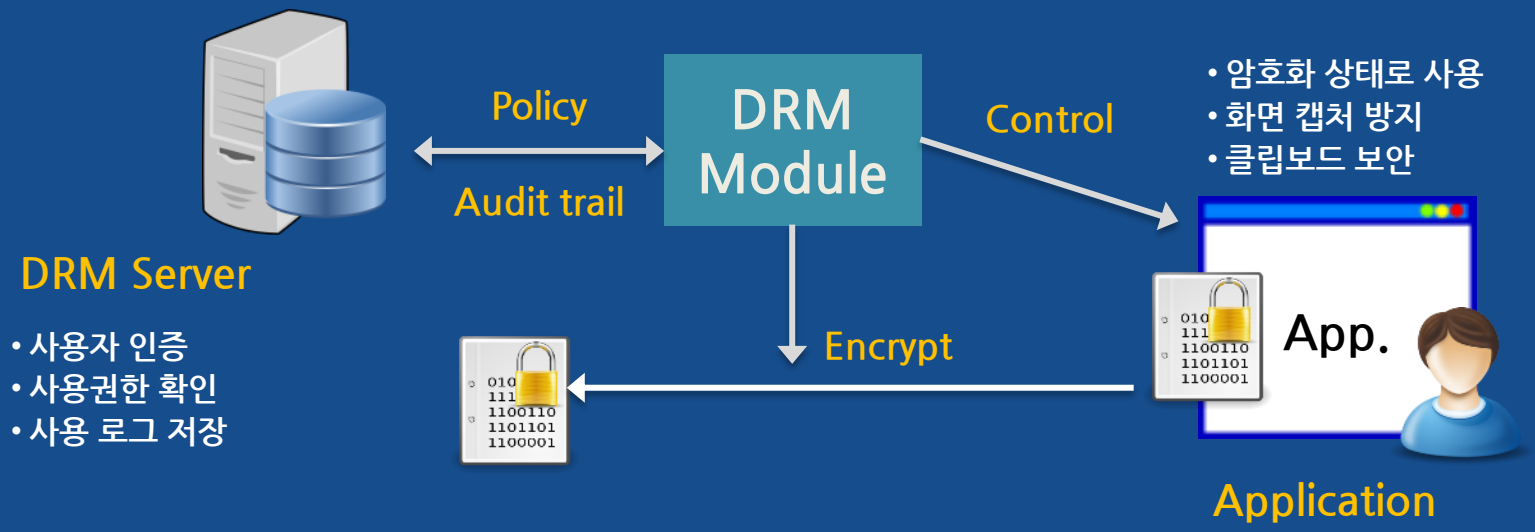


*출처 : Gartner : Top Security Trends and Takeaways for 2014 and 2015

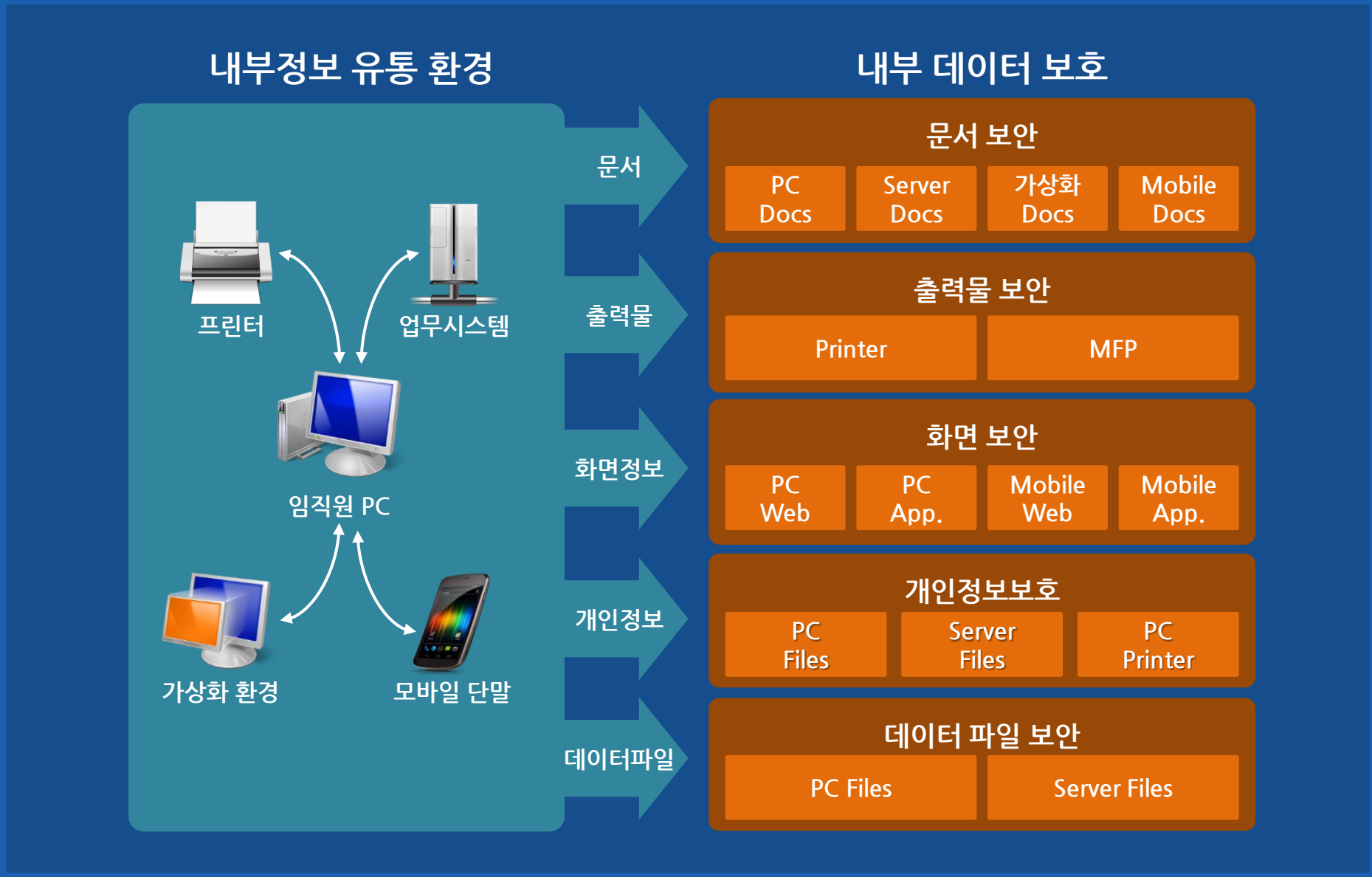
Data Shield & Encrypt = DRM

Fasoo Enterprise DRM

- Encrypt
- Policy
- Control
- Audit trail



DRM 영역 확대


내부정보 유통 환경
프린터
업무시스템
임직원 PC
가상화 환경
모바일 단말
문서
출력물
화면정보
개인정보
데이터파일
내부 데이터 보호
문서 보안
PC Docs
Server Docs
가상화 Docs
Mobile Docs
출력물 보안
Printer
MFP
화면 보안
PC Web
PC App.
Mobile Web
Mobile App.
개인정보보호
PC Files
Server Files
PC Printer
데이터 파일 보안
PC Files
Server Files

데이터 보안 개선 모델

보안 정책의 효과성 검증

Policy	Control	Management
		
Discovery	Authenticate	Logging
Control	Encrypt	Classification
Audit	Revoke	Audit trail

Fasoo

Policy & Data governance

파일 단위 관리 없이 적절한 정책과 규제 준수 한계

임직원

정책 준수 요구

책임자

데이터 생성
및 보관

정책
준수?

Policy

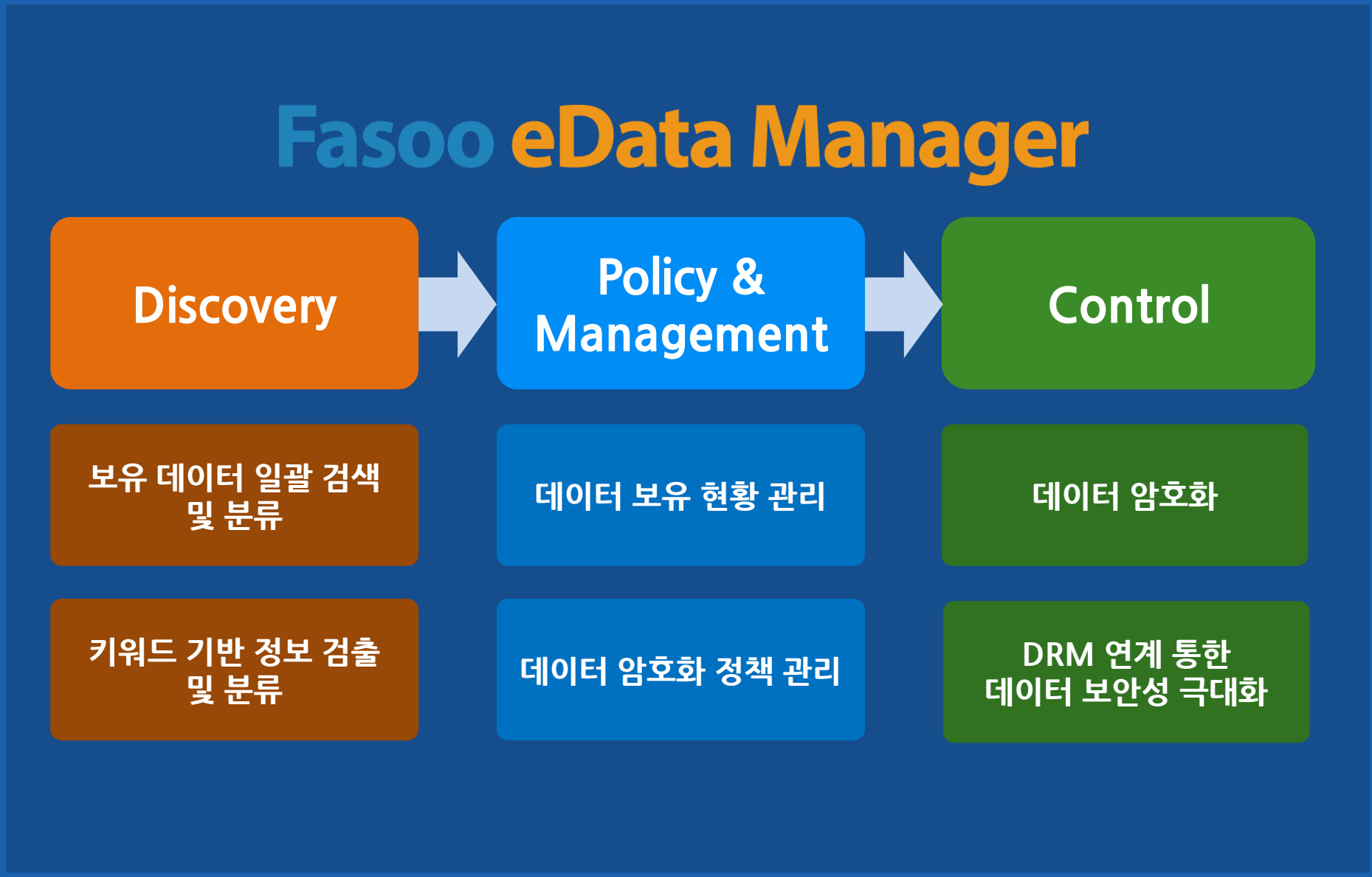
- 데이터 분류/보관
- 암호화 저장
- 보관 기간 종료 시 폐기

정책
수립

데이터 관리 의무

- 보유 현황 파악
- 정책 준수 관리
- 관리/감독/감사

데이터 거버넌스 솔루션, Fasoo eData Manager



Big data security Analytics

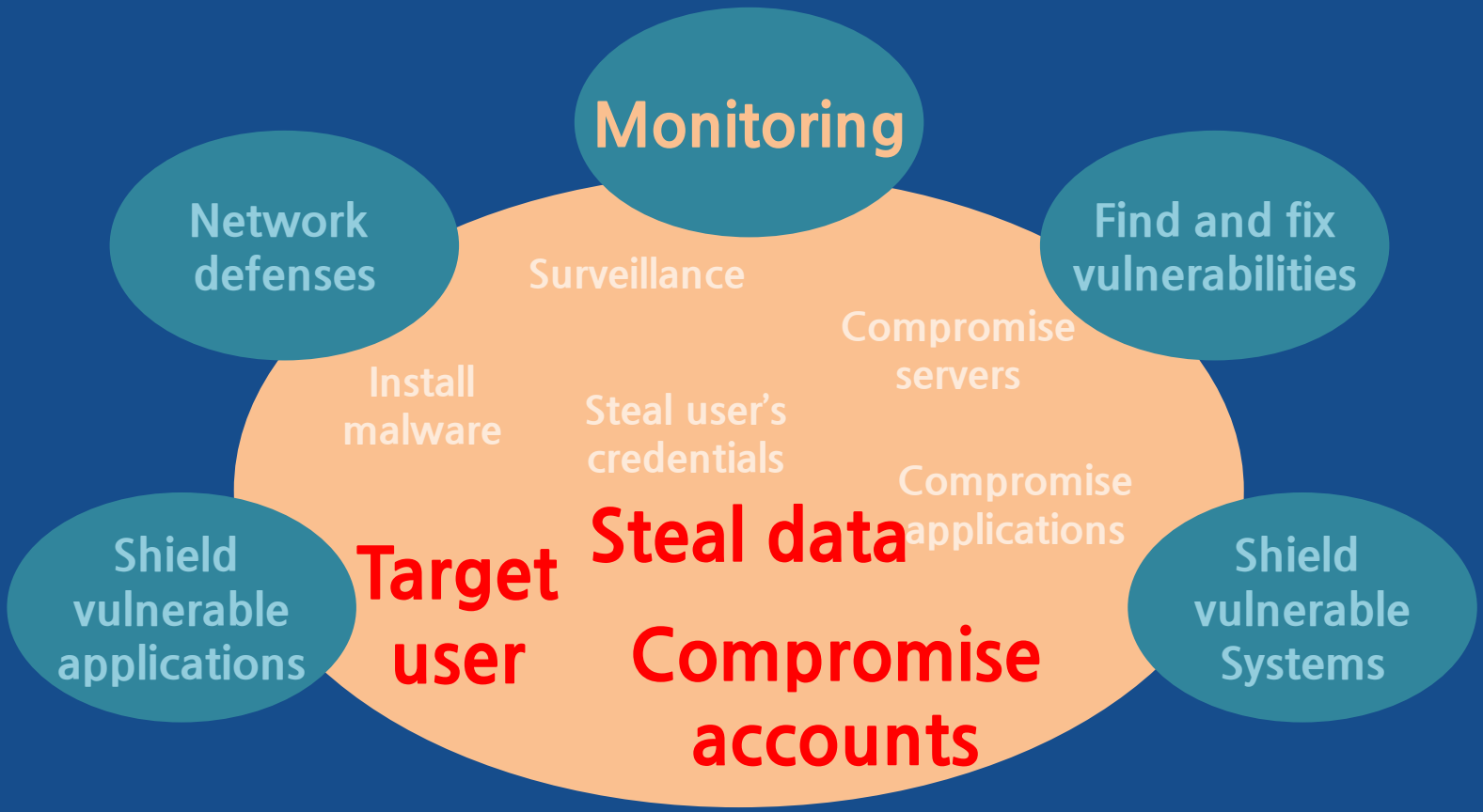
Top Digital Security Trends for 2014 by Gartner

- ✓ Software-defined security
- ✓ **Big data security analytics**
- ✓ Intelligent/Context-aware security controls
- ✓ Application isolation
- ✓ Endpoint threat detection and response
- ✓ Website protection
- ✓ Adaptive access
- ✓ Securing the Internet of Things

*출처 : Gartner : Top Security Trends and Takeaways for 2014 and 2015

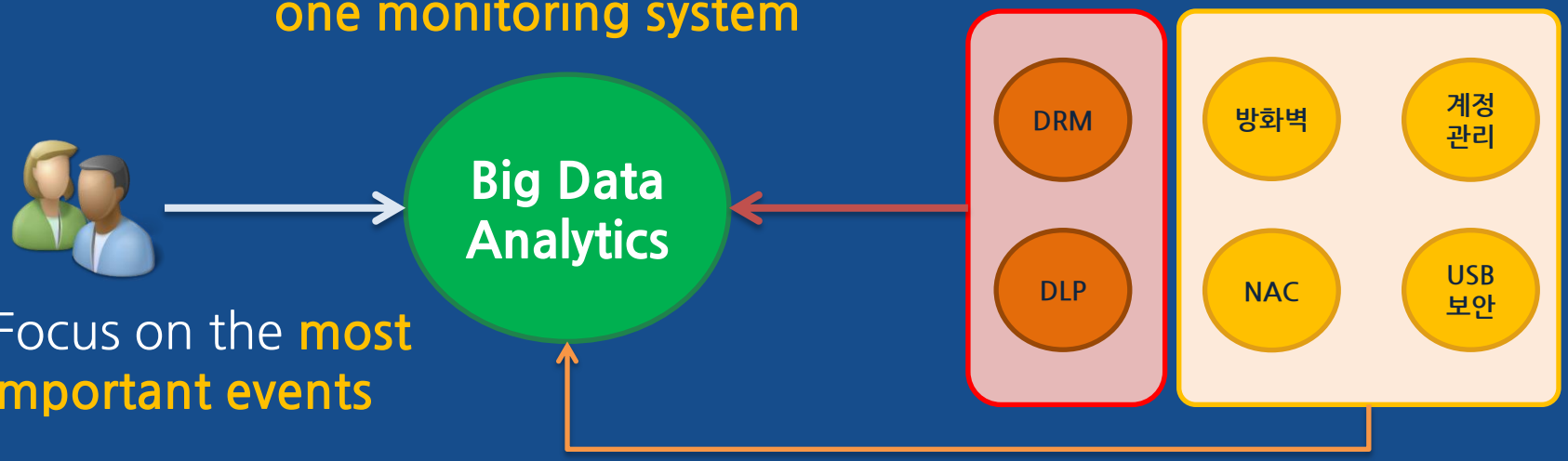
Big Data Analytics & DRM

Security for Targeted Attacks



빅 데이터 기반 데이터 위험관리 모델

1. Use Big Data Analytics as **one monitoring system**

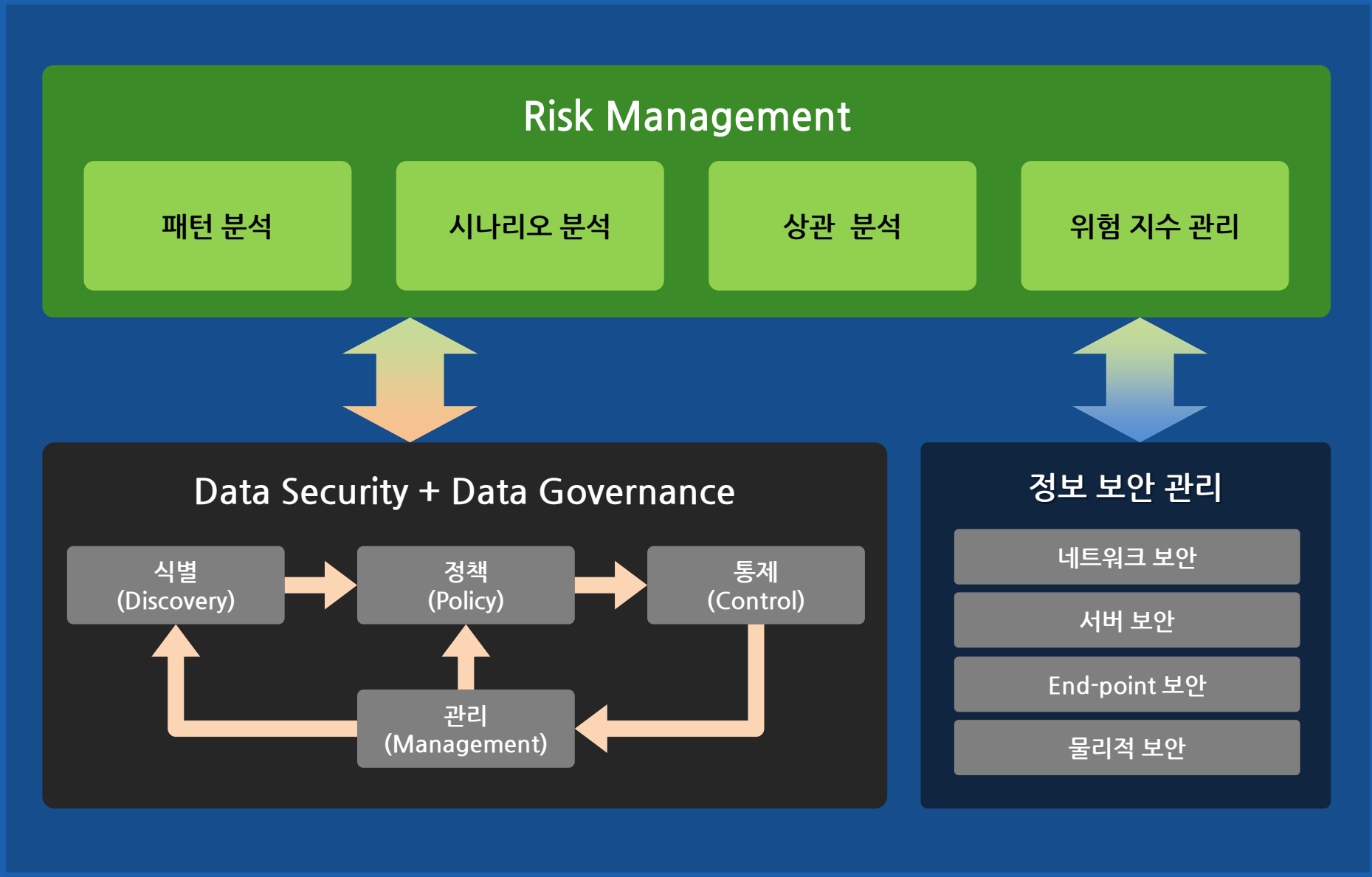


2. Focus on the **most important events**

3. Broaden adoption across **multiple applications and use case**

4. Use intelligence from vendors that use their own big data analytics

신개념 데이터 위험관리 솔루션, Fasoo RiskView



Fasoo

시나리오에 기반한 Critical Case 검출

- 각 조직에 특화된 시나리오에 따른 이상징후 탐지 Rule 적용

데이터 위험관리 방법

사용 패턴, 이상 행위, 중요 정보 등
주요 리스크에 대한 위험수준

전일대비 리스크지수 Top 5 부서

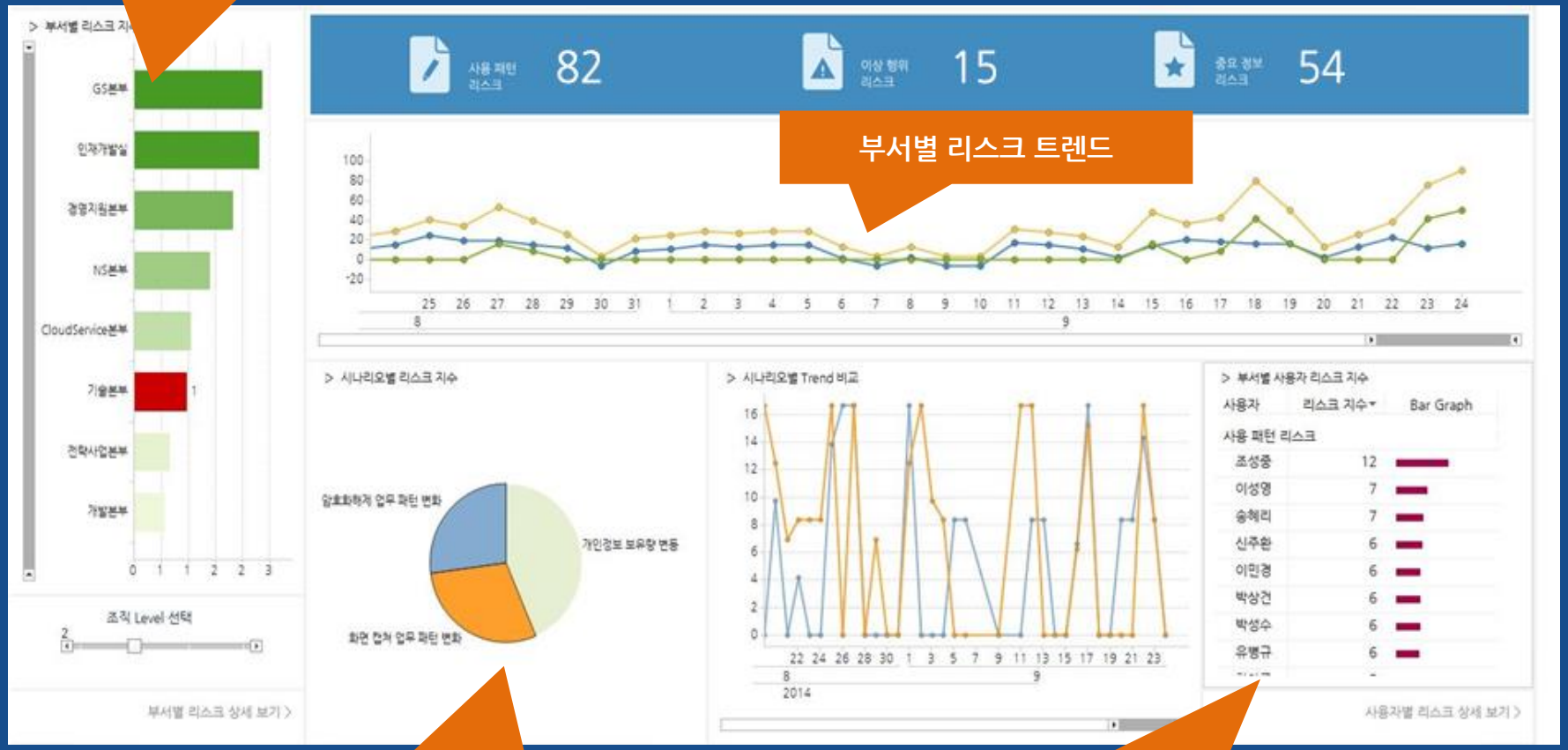
전일대비 리스크지수 Top 5 사용자

전일 시나리오별 리스크지수

Fasoo

데이터 위험관리 방법

부서별 주요 리스크에 대한 위험수준



부서별 리스크 트렌드

리스크 시나리오와 트렌드

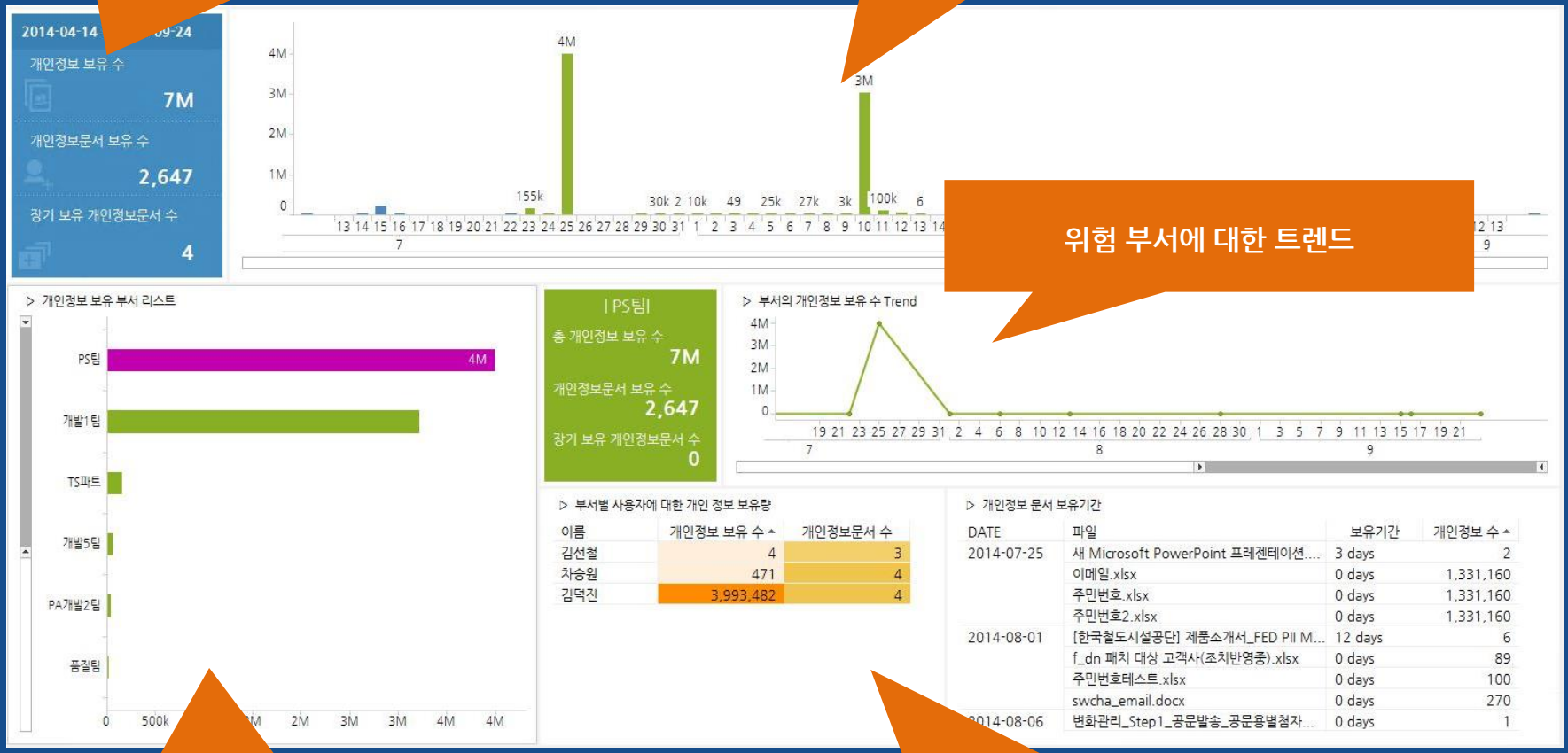
부서에 대한 사용자 별 리스크

Fasoo

데이터 위험관리 방법

사내 개인 정보 / 중요 정보 사용량 / 보유량

사내 보유량 트렌드 및 위험도



중요 정보를 많이 보유하거나 사용하는 부서

선택 부서 사용자에 대한 보유량 및 보유 문서 정보 확인

Fasoo

FASOO 2015

Data Security

Data Governance

Risk Management

Fasoo