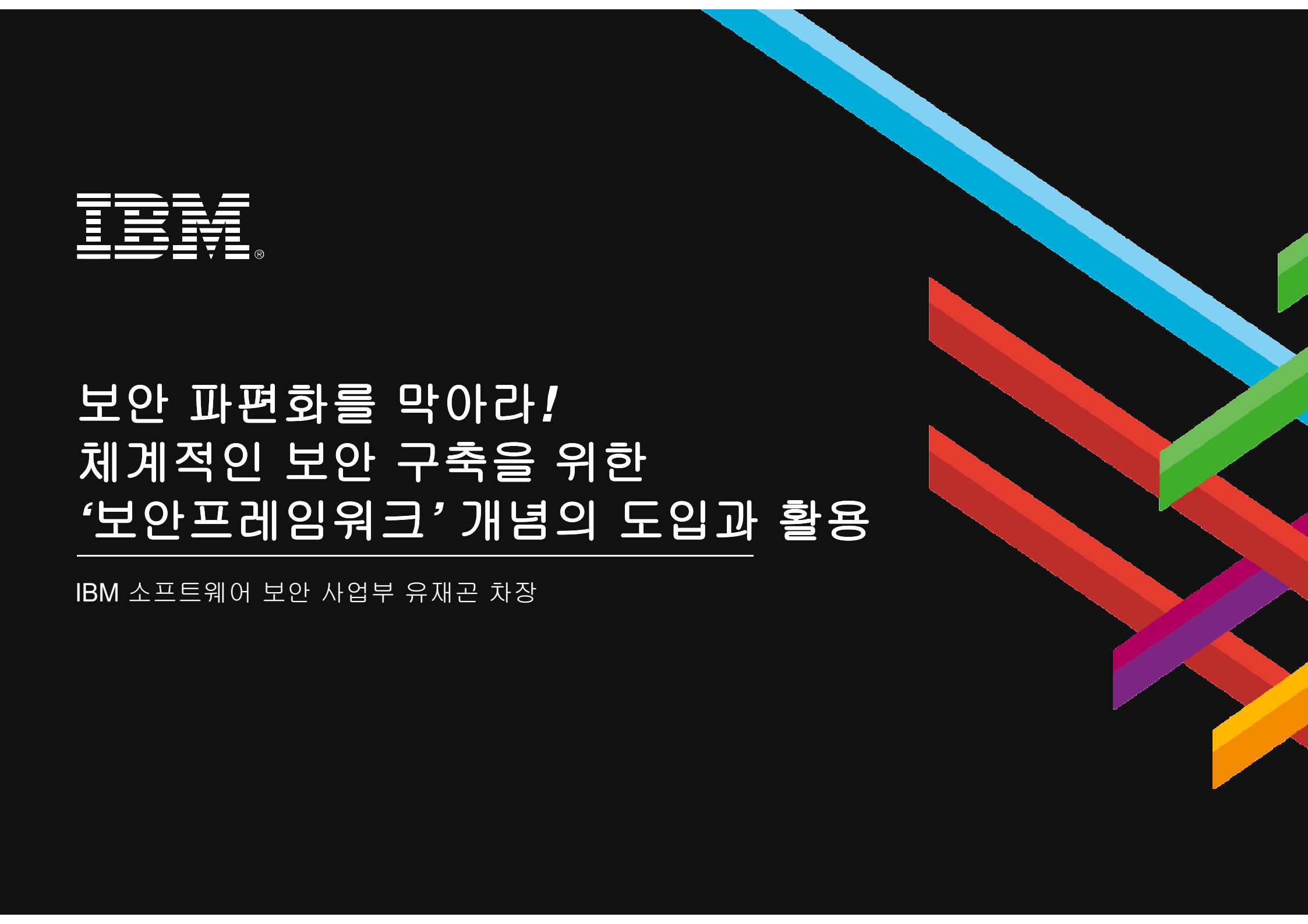


# 보안 파편화를 막아라!
# 체계적인 보안 구축을 위한 '보안프레임워크' 개념의 도입과 활용

IBM 소프트웨어 보안 사업부 유재곤 차장

## Agenda

- 진화하는 위협
- 보안에 대한 새로운 접근법
- ***IBM*** 보안과 함께 위협으로부터 탈출

# 해커들의 동기 및 전문성의 진화

동기

전문화

국가
안보

국가
지원 조직
***Stuxnet***

스파이,
행동주의

경쟁자들과
핵티비스트
***Aurora***

금전적 이득

조직적
범죄
***Zeus***

복수,
호기심


내부자와
스크립키드
***Code Red***

# 보안은 선택이 아닌 임무

| CEO | CFO/COO | CIO | CHRO | CMO |
|---|---|---|---|---|
| 시장 점유율 및 평판 하락<br><br>법적 책임 | 감사 및 벌금<br><br>금전적 손해 | 데이터 기밀성 유지 및 유출 방지 | 직원 기밀 위반 | 고객 신뢰 하락<br><br>브랜드 이미지 실추 |

## 기업 임원 및 이사회 회의의 주된 의제

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

# The Myth: “Our Site Is Safe”

## 우리는 안전하다!

**방화벽과 *IPS* 운영중이다**
80,443 포트는?

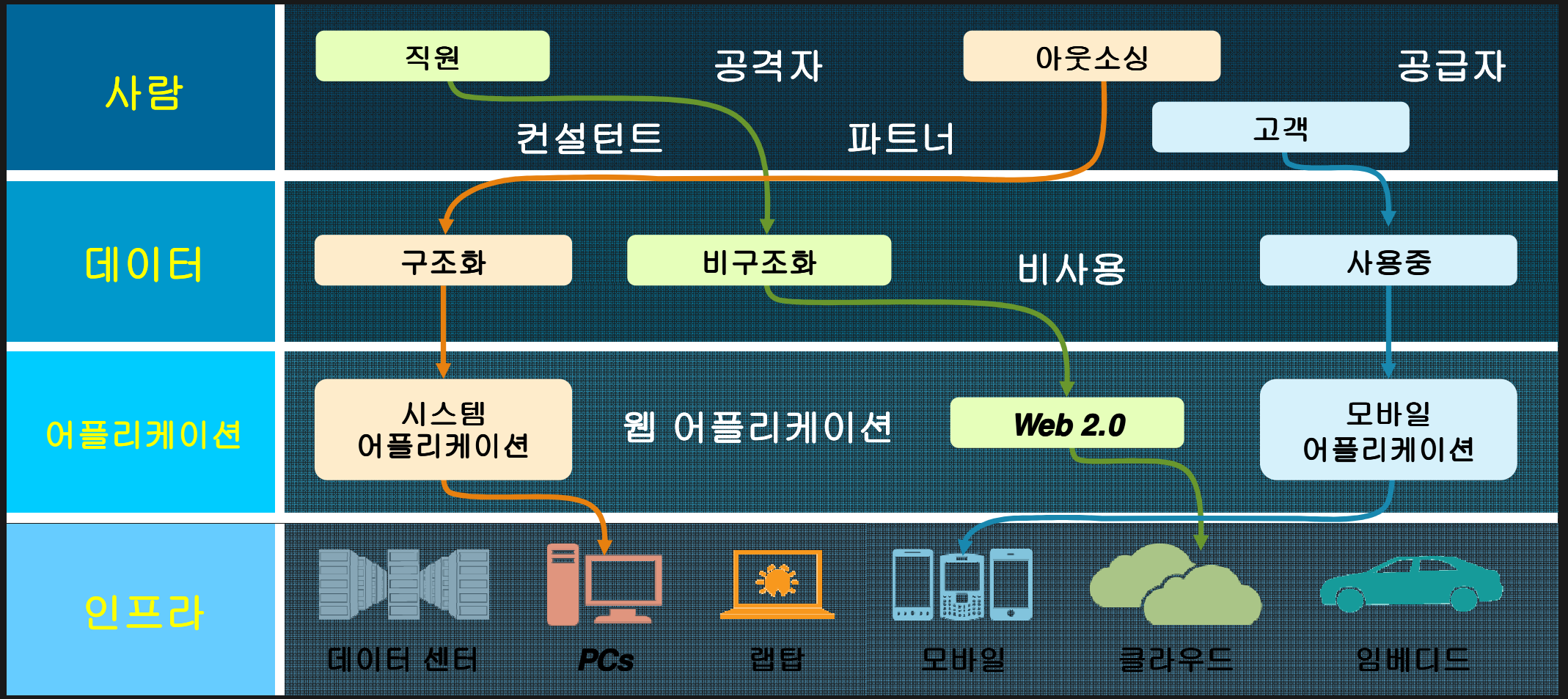
**반기에 한번씩 모의해킹을 한다**
어플리케이션은 반기에 한번 변경되는가?

**네트워크 취약점 스캐너를 사용한다.**
네트워크를 사용하는 웹서버의 취약점은?

**우리는 *SSL*암호화를 사용한다**
데이터가 아닌 웹 어플리케이션 자체는?

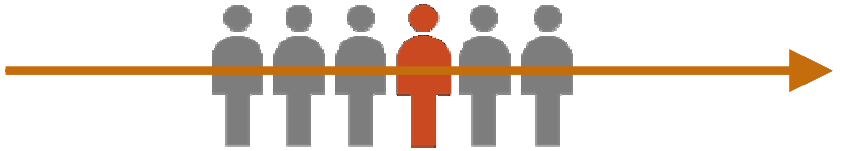
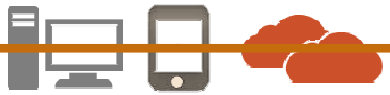
# 보안에 대한 새로운 접근

# 다양화 되고 복잡해진 IT 환경



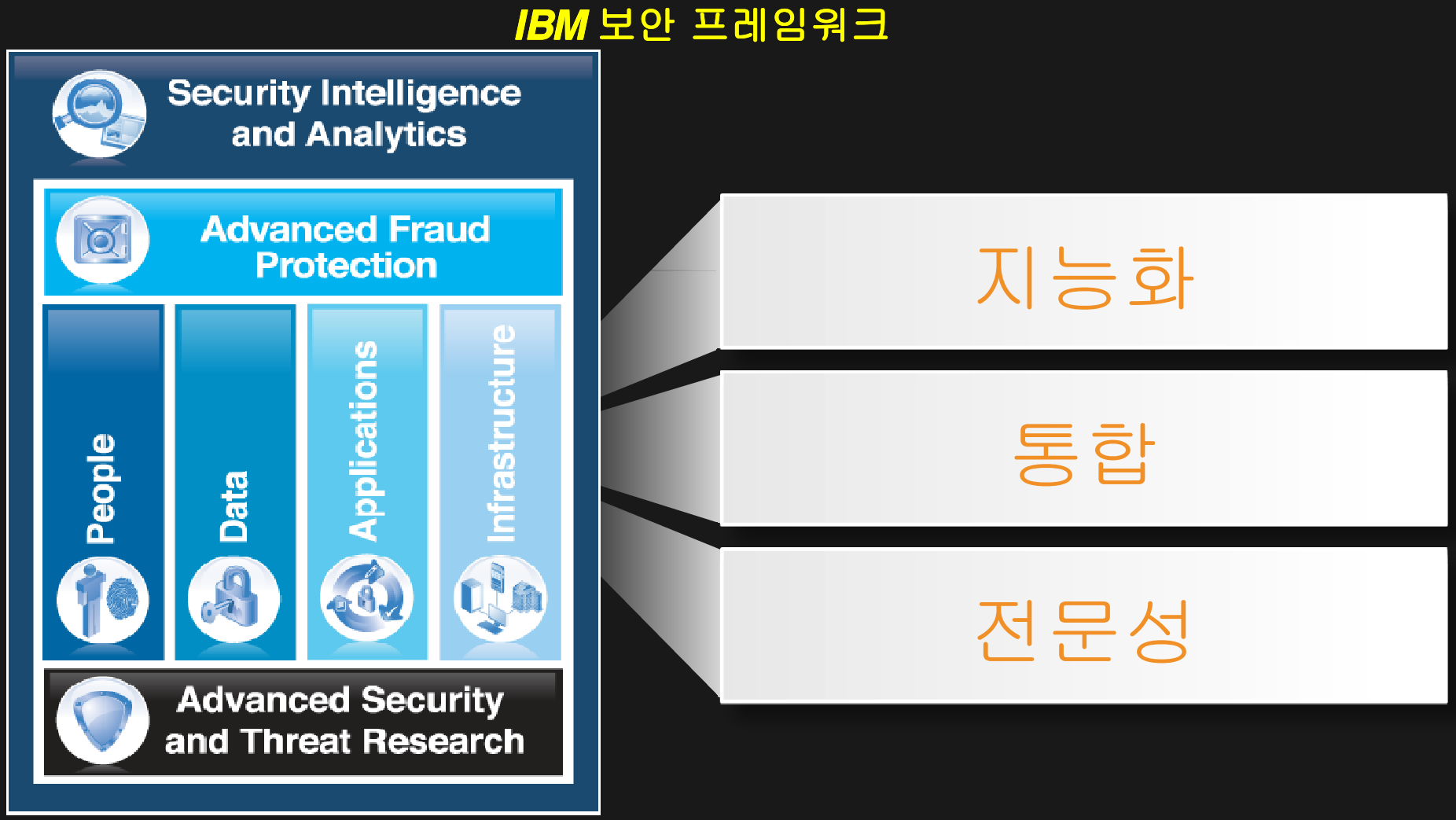

*새로운 접근법이 필요하다*

# 보안에 대한 새로운 접근 필요

| | 현재 | | 미래 |
|---|---|---|---|
| 사람 | 관리 |  | 통찰 |
| 데이터 | 기본 통제 |  | 정밀하게 집중된 통제 |
| 어플리케이션 | 부가적인 보안 |  | 내재된 보안 |
| 인프라스트럭처 | 두꺼운 벽 |  | 더 똑똑한 방어 |

모든 것을 수집하고 분석할 필요가 있습니다

# 지능화,통합,전문성에 기반한 IBM 보안 프레임워크



# IBM 보안 전략

**1** ***CISO*의 관심**

*고객*

| ***CISO*** | ***CIO*** | **현업** |
|---|---|---|


*최근의 추세와 발맞추어가기 위해 다양한 영역의 솔루션을 통합*

**2** **최신 기술로의 혁신**

*트렌드*

| 고도화된 공격 | 클라우드 | 모바일 | 감사 |
|---|---|---|---|

**3** **각각의 영역에서 선두**

*역량*

보안 인텔리전스 및 분석

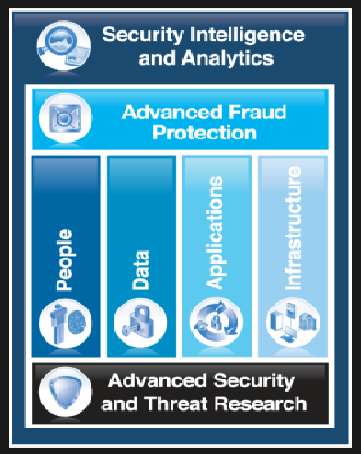
고도화된 사기 방지

| 사람 | 데이터 | 어플리케이션 | 인프라 |
|---|---|---|---|

고도화된 보안 및 위협 연구

# IBM과 함께
# 위협으로부터 탈출

# IBM의 보안에 대한 지속적인 투자




**Mainframe and Server Security**

**1976**
Resource Access Control Facility (RACF) is created, eliminating the need for each application to imbed security

DASCOM

**Access Management**

**1999**
**Dascom** is acquired for access management capabilities

access360

METAMERGE

**Identity Management**

**2002**
**Access360** is acquired for identity management capabilities

**MetaMerge** is acquired for directory integration capabilities

DATAPOWER

INTERNET SECURITY SYSTEMS

**SOA Management and Security**

**2005**
**DataPower** is acquired for SOA management and security capabilities

watchfire

consul

**Network Intrusion Prevention**

**2006**
**Internet Security Systems, Inc.** is acquired for security research and network protection capabilities

ENCENTUATE

princeton softech

Guardium

**Compliance Management**

**2007**
**Watchfire** is acquired for security and compliance capabilities

**Consul** is acquired for risk management capabilities

**Princeton Softech** is acquired for data management capabilities

OUNCE LABS

BIGFIX

**Database Monitoring**

**2008**
**Encentuate** is acquired for enterprise single-sign-on capabilities

NISC

**Application Security**

**2009**
**Ounce Labs** is acquired for application security capabilities

**Guardium** is acquired for enterprise database monitoring and protection capabilities

Q1Labs

**Security Analytics**

**2010**
**Big Fix** is acquired for endpoint security management capabilities

**NISC** is acquired for information and analytics management capabilities

Trusteer

**Security Intelligence**

**2011**
**Q1 Labs** is acquired for security intelligence capabilities

**Advanced Fraud Protection**

**2012**

**2013**
Intent to acquire **Trusteer** for mobile and application security, counter-fraud and malware detection

***IBM* 보안 사업부**

# 치밀한 보안 연구

**11**
보안 관제 센터

**9**
보안 연구 센터

**11**
보안 솔루션 개발 센터

**400**
보안 관제 분석 전문가

**520**
보안 관제 운영 전문가

**941**
보안 전문 컨설턴트

**3,300**
**SO** 보안 운영 서비스 전문가


보안 운영 센터
보안 연구 센터
보안 솔루션 개발 센터
첨단 보안 협회 *(Institute for Advanced Security)* 지사

- 20,000+ 장비 계약 및 운영
- 3,700+ MSS 전세계 고객
- 150억+ 개의 보안 이벤트 모니터링 및 관리
- 1,000+ 보안 관련 특허 보유
- 133개 국가 대상 관제 서비스 (MSS)

# 통합,지능화,전문적인 IBM 보안 프레임워크


| | Today | Tomorrow |
|---|---|---|
| | 기본 | 최적화 |
| People | 애플리케이션 별 계정 관리 | 를 기반 거버넌스 및 특권 사용자 관리 구현 |
| Data | 접근 제어 및 암호화 | 사용 현황 모니터링 및 정보 유출 통제 |
| Application | 취약점 진단 | 통합 및 자동화된 보안 개발 프로세스 수립 |
| Infrastructure | 불필요한 네트워크 및 바이러스 통제 | 실시간 *APT* 탐지 및 포렌식 |

강화된 상관관계 및 정밀화된 분석

– 보안 인텔리전스

사후처리 ●----------▸ 사전예방

# 벽을 허물고 복잡성을 낮추는 통합 프레임워크

## 통합된 지능화


수백 수천 개의 정보를 통합, 상관 관계 분석을 통해 통합 관리

## 통합된 리서치


진화되는 위협을 항상 연구,대응 하며 제품 개발

X-Force Threat Intelligence Cloud

## 통합된 방어


다양한 영역에서 보안 및 취약점에 대한 데이터 연계

JK 2013-04-265

# 모든 분야의 선도자

| Domain | Market Segment / Report | Security Analyst Report Rankings | | |
|---|---|---|---|---|
| | | Gartner Magic Quadrant | Forrester Wave | IDC Market Share |
| Security Intelligence | Security Information and Event Management (SIEM) | **Leader** *2013* | | **Leader** *2011* |
| Anti-Fraud | Web Fraud Detection* | **Leader** *2013* | | |
| People | Identity and Access Governance | **Challenger** *2013* | | **Leader** *2013* |
| | User Provisioning and Administration | **Leader** *2013* | | |
| | Role Management and Access Recertification | | **Contender** *2011* | |
| | Web Access Management (WAM) | **Leader** *2013 MarketScope* | | |
| Data | Database Auditing and Real-Time Protection | | **Leader** *2011* | |
| | Data Masking | **Leader** *2013* | | |
| Applications | Application Security Testing *(dynamic and static)* | **Leader** *2013* | | **Leader** *2013* |
| Infrastructure | Network Intrusion Prevention Systems (NIPS) | **Challenger** *2012* | | |
| | EndPoint Protection Platforms (EPP) | **Visionary** *2013* | **Strong Performer** *2013* | |
| Services | Managed Security Services (MSS) | **Leader** *2012* | **Leader** *2012* | |
| | Information Security Consulting Services | | **Leader** *2013* | |

# 전 방위적인 보안 제품들

## IBM Security Systems Portfolio

| Security Intelligence and Analytics | | | |
|---|---|---|---|
| QRadar<br>Log Manager | QRadar<br>SIEM | QRadar<br>Risk Manager | QRadar<br>Vulnerability Manager |

| Advanced Fraud Protection | | | |
|---|---|---|---|
| Trusteer<br>Rapport | Trusteer Pinpoint<br>Malware Detection | Trusteer Pinpoint<br>ATO Detection | Trusteer Mobile<br>Risk Engine |

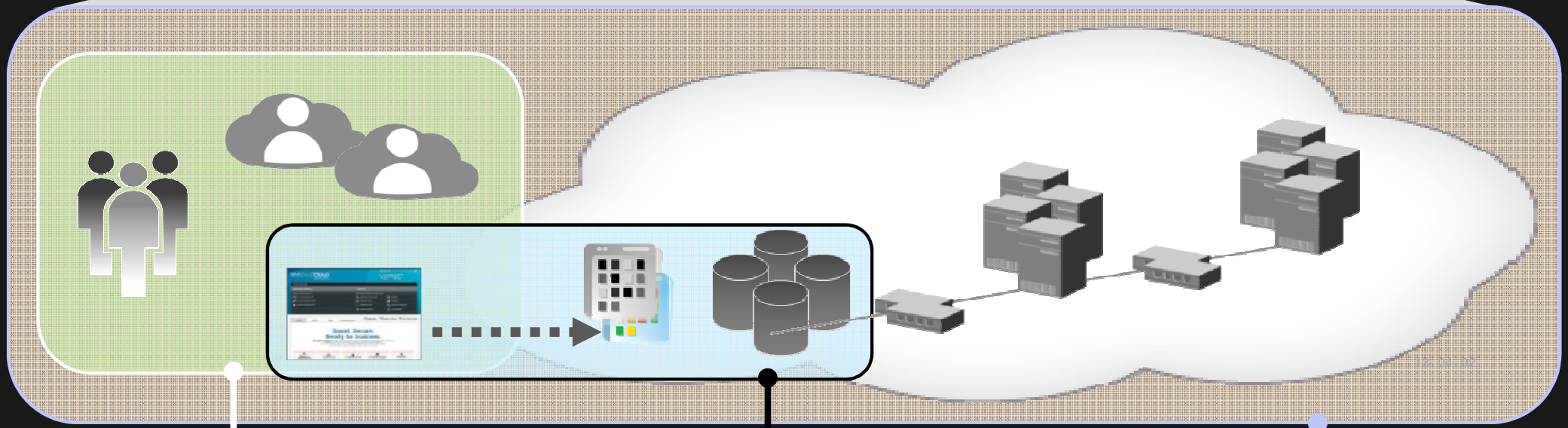
| People | Data | Applications | Network | Infrastructure | Endpoint |
|---|---|---|---|---|---|
| Identity<br>Management | Guardium Data Security and<br>Compliance | AppScan<br>Source | Network<br>Intrusion Prevention | | Trusteer Apex |
| Access<br>Management | Guardium DB Vulnerability<br>Management | AppScan<br>Dynamic | Next Generation<br>Network Protection | | Mobile and Endpoint<br>Management |
| Privileged Identity<br>Manager | Guardium / Optim Data<br>Masking | DataPower Web<br>Security Gateway | SiteProtector<br>Threat Management | | Virtualization and Server<br>Security |
| Federated<br>Access and SSO | Key Lifecycle<br>Manager | Security Policy Manager | Network<br>Anomaly Detection | | Mainframe<br>Security |

**IBM X-Force Research**

# 클라우드 환경을 위한 지능화된 보안

**보안 인텔리전스**

가시성, 감사기능을 확보하여 클라우드 환경을 제어



**계정 보호**

계정 관리, 보호 및 클라우드 접근

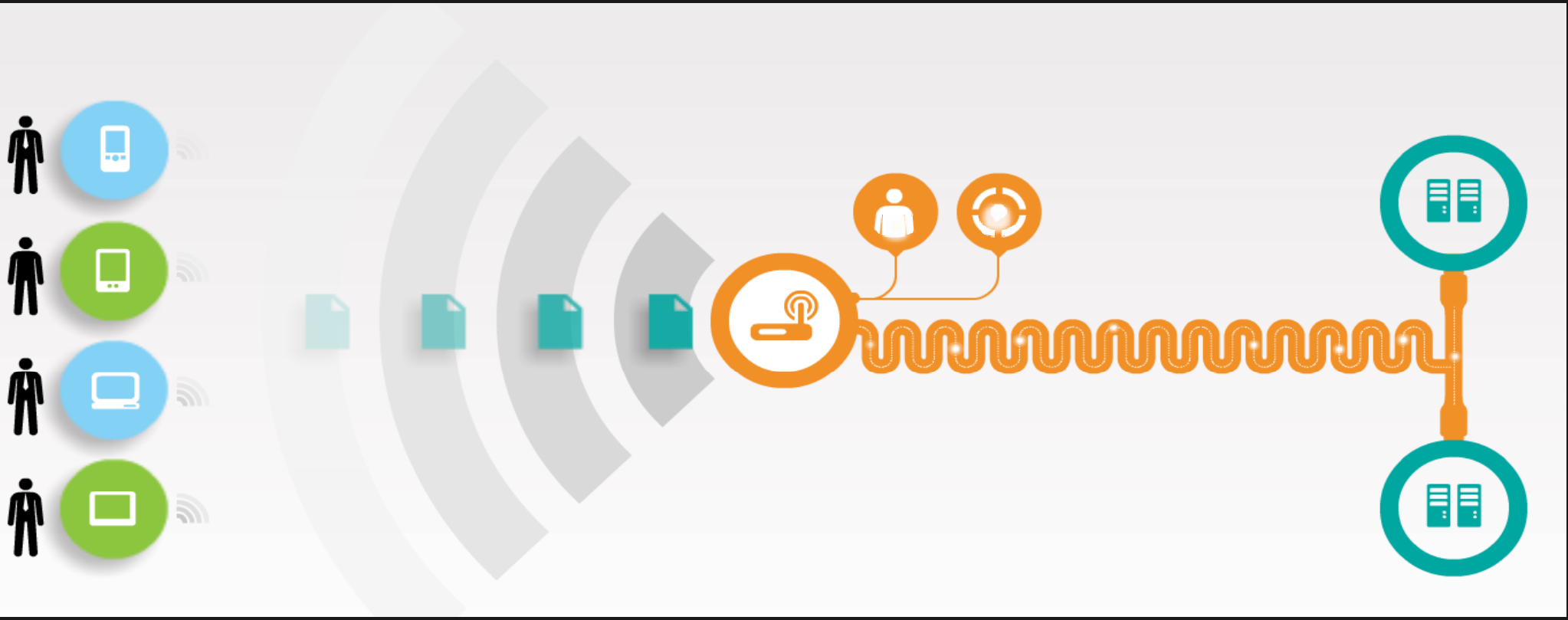
**데이터, 어플리케이션 보호**

기업 데이터를 보호하고 안전한 클라우드 어플리케이션을 빌드, 테스트 및 관리

**위험 보호**

다중 계층과 분석을 통하여 고도화된 위협을 방지

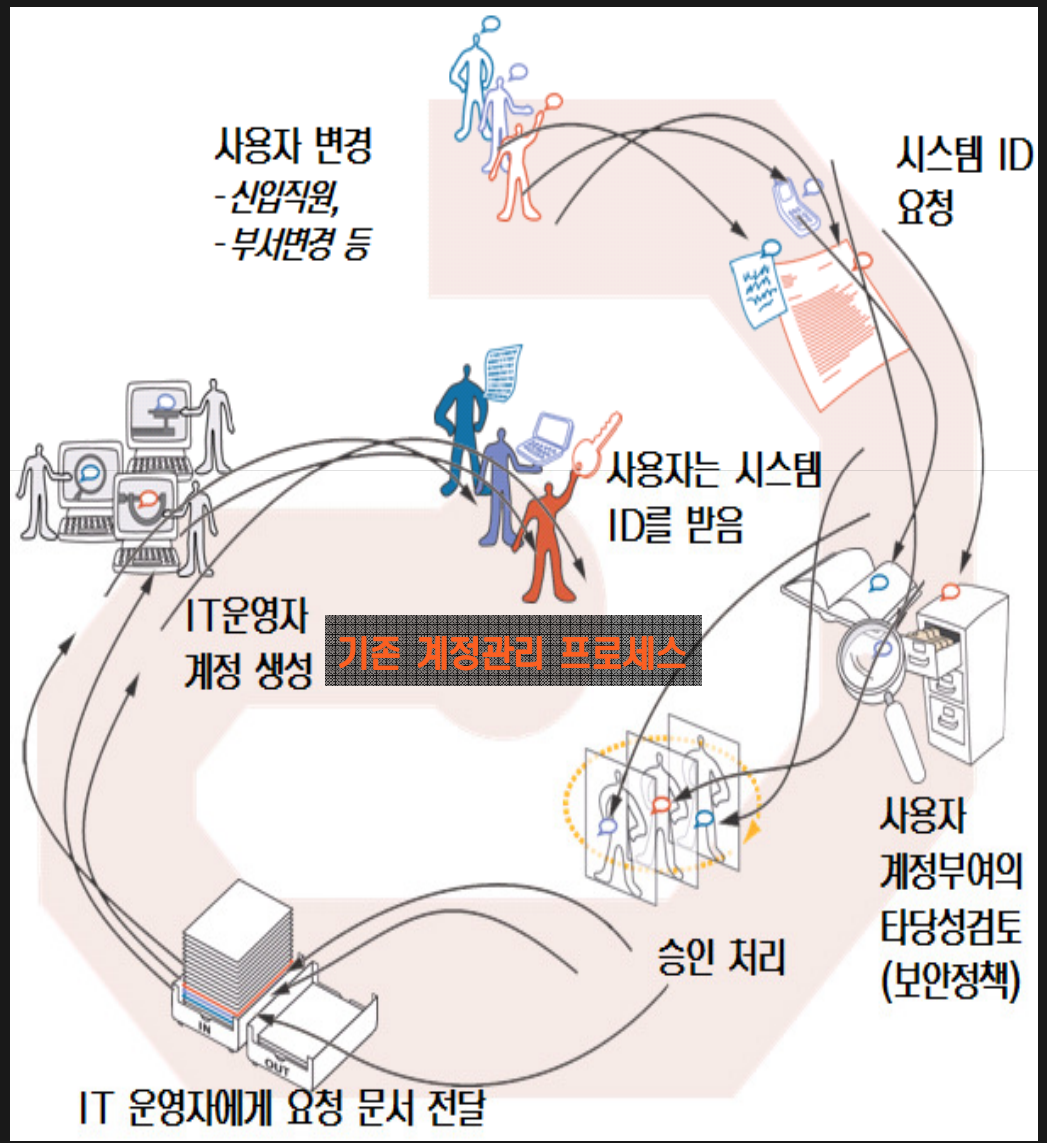
# 모바일 환경의 보안



| 디바이스 관리 | 네트워크, 데이터, 접근 보안 | 어플리케이션 보안 |
| --- | --- | --- |
| 디바이스 및 데이터 보안 | 가시성 확보 및 최적화된 보안 정책 | 안전한 어플리케이션 개발 및 테스트 |

# 계정 및 접근 관리

People



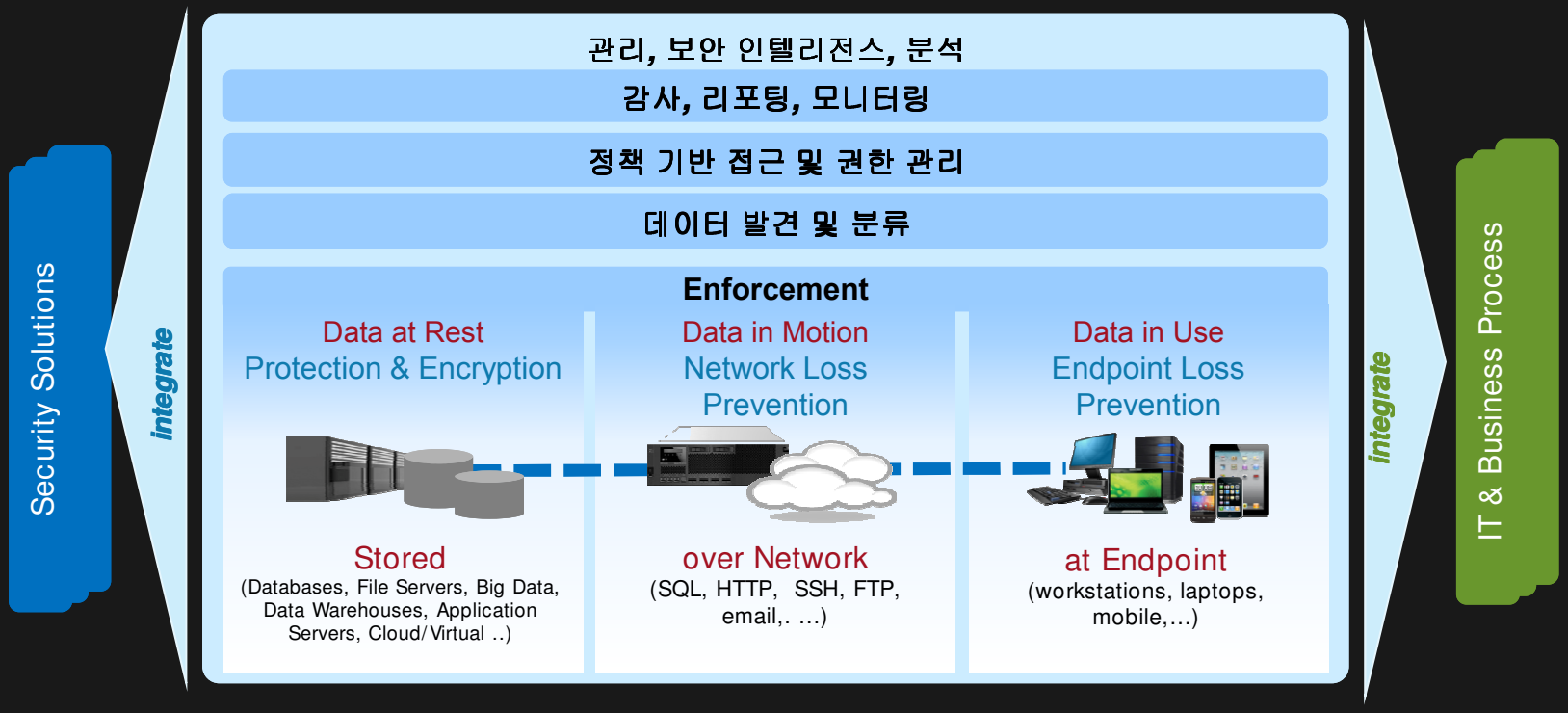

- ***30~60%***의 계정은 불필요한 계정
- 처리 소요시간 ***:*** 사용자당 약 ***5***일
- 한 사람의 운영자는 ***300~500***명의 요구사항만을 처리

- 중앙 집중화된 계정/권한관리 시스템의 운영을 통한 투명성 증대
- 체계적 계정/권한 관리 및 통합 인증을 통해 관리 비용 절감 및 업무 효율 향상
- 사용자 별로 역할과 책임에 맞게 접근 권한 및 자격을 부여하는 프로비저닝을 통한 보안성 강화

# 데이터 보안

Data

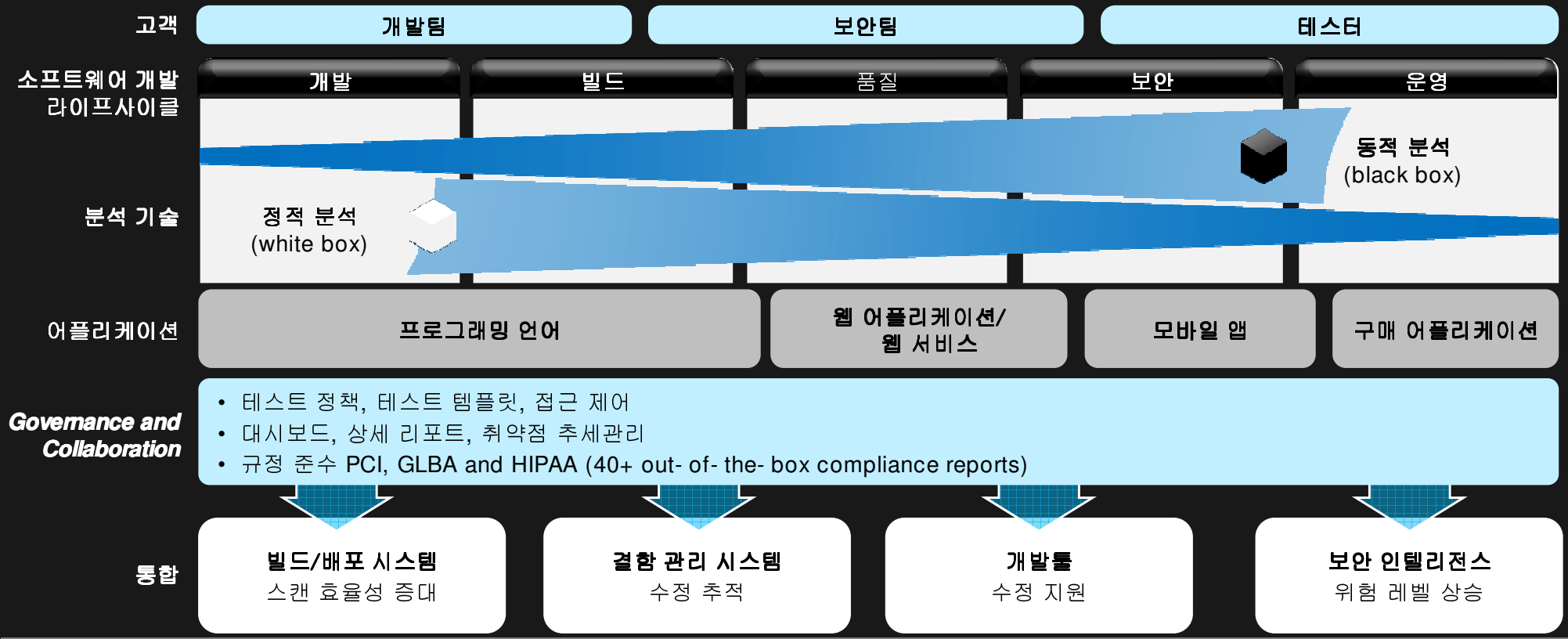
- 전 방위 접속경로 모니터링 및 제어
- 규정 준수 프로세스 준수
- 데이터 보호를 위한 운영 비용 절감




| 핵심 주제 | | |
|---|---|---|
| 새로운 플랫폼 확대 | 새로운 데이터 보안 역량 개발 | 확장성 및 낮은 유지 비용 |

# 어플리케이션 보안

Applications




## 핵심 주제

모바일 어플리케이션 역량 및 새로운 취약점 분석

단순화된 인터페이스 및 증가된 ***ROI***

보안 인텔리전스 통합

# 인프라 보안

Infrastructure

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***Security Intelligence Platform*** | Log Manager | SIEM | Network Activity Monitor | Risk Manager | Vulnerability Manager | *Future* | IBM X-Force Labs |
| ***Threat Intelligence and Research*** | Vulnerability Data | Malicious Websites | Malware Information | IP Reputation | | *Future* | IBM X-Force |
| ***Advanced Threat Platform*** | Intrusion Prevention | Content and Data Security | Web Application Protection | Network Anomaly Detection | Application Control | *Future* | ***IBM Network Security*** |

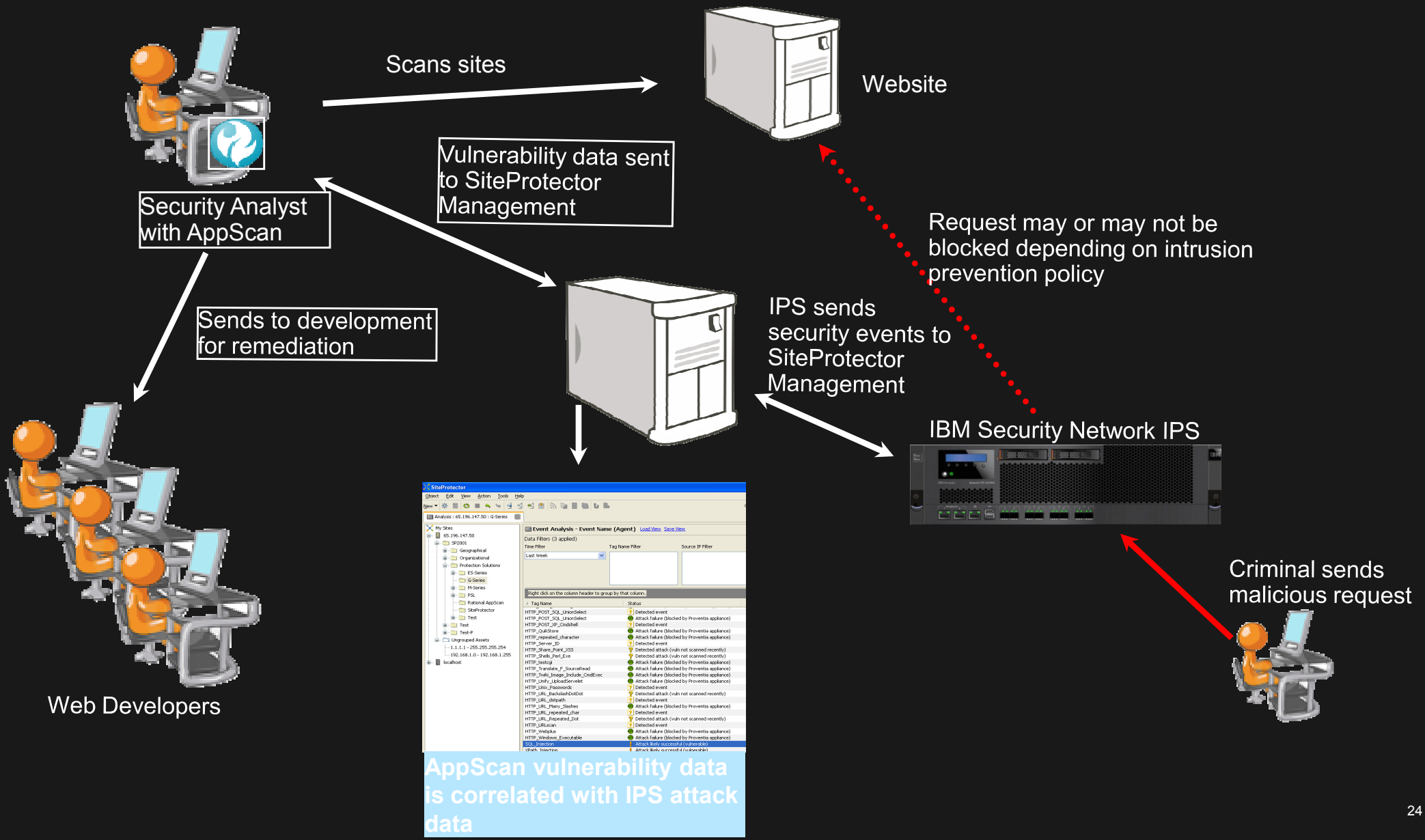
## 핵심 주제

고도화된 위협 보호 플랫폼

***X- Force*** 위험 인텔리전스 확대

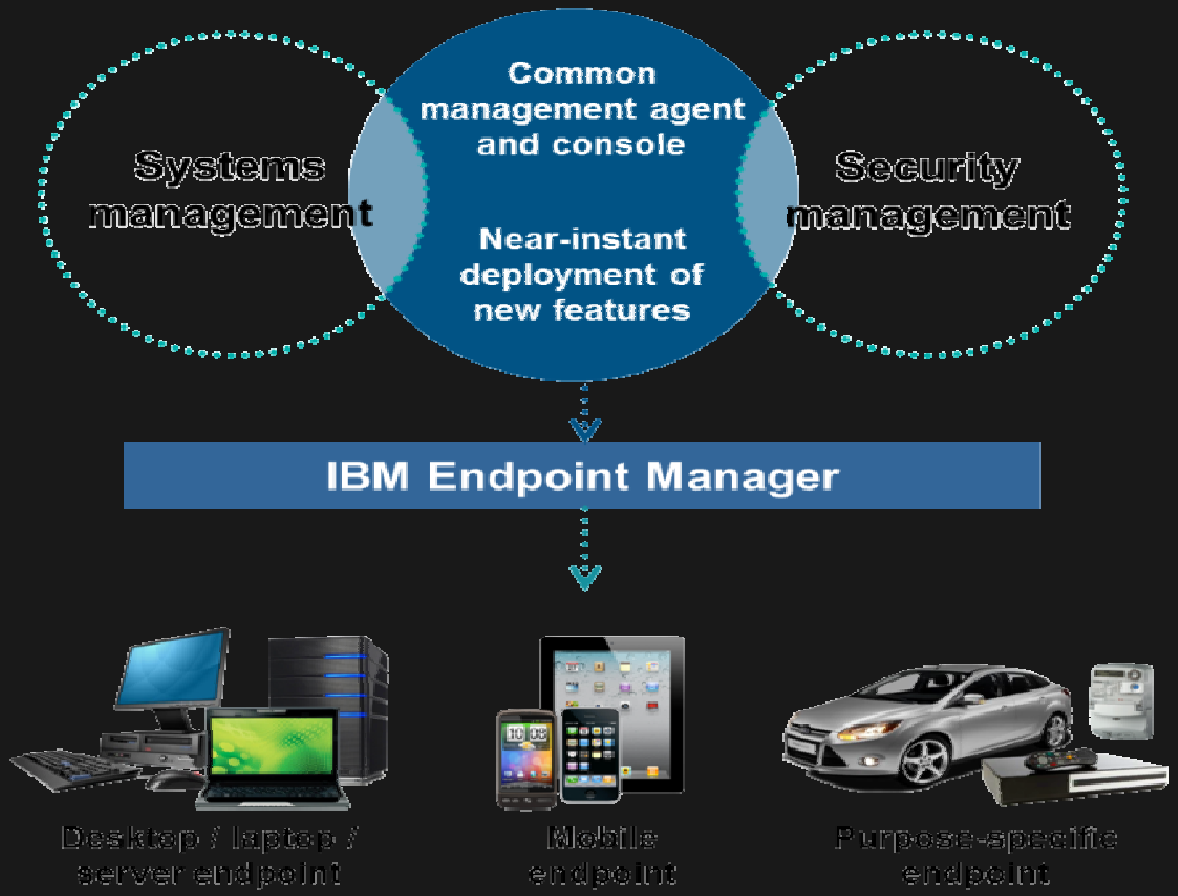
보안 인텔리전스 통합

# 어플리케이션 취약점 정보와 데이터 연계



# 인프라 보안 : 엔드포인트

Infrastructure




| 핵심 주제 | | |
|---|---|---|
| 모바일 디바이스 보안 | 보안 내용 확장 | 지능화된 보안 통합 |

# 사기방지 멀웨어 방지

Advanced Fraud Protection

## 보다 향상된 위협 방어

**제로데이 공격과 데이터 유출에 대한 전체적인 보호**

***Trusteer Apex*과 함께**

- IBM QRadar Security Intelligence Platform
- IBM Network IPS
- IBM Endpoint Manager

## 보다 향상된 위협 인텔리전스

**빠른 악성코드와 최신 위협에 대응**

***Trusteer Cyber Intelligence*와 함께**

- IBM X- Force Research & Development
- IBM X- Force Global Threat Intelligence

## 통합된 사기 방지

***IAM*과 *E- commerce*로 사기 탐지 확장**

***Trusteer Pinpoint*와 함께**

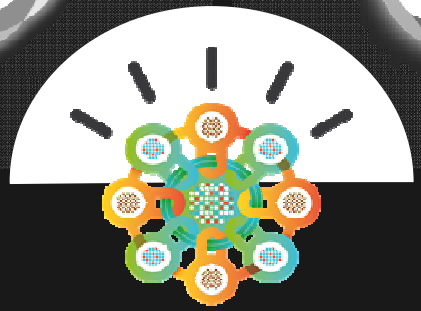
- IBM Security Access Manager
- IBM WebSphere Application Server


## 안전한 모바일 트랜잭션

**모바일 디바이스와 어플리케이션을 위한 내장된 보안**

***Trusteer Rapport*와 *Mobile*과 함께**

- IBM Endpoint Manager for Mobile Devices
- IBM Worklight Mobile Application Platform

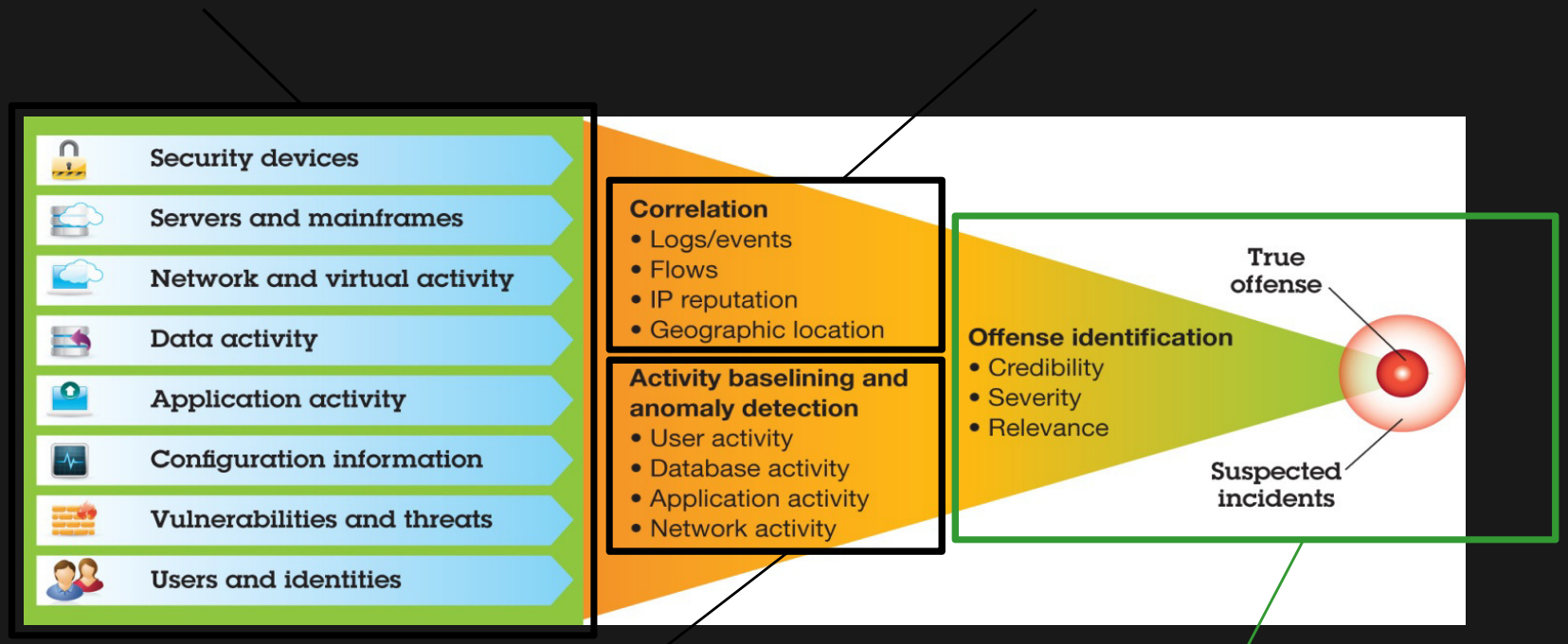


# 통합화된 지능화된 보안

Security Intelligence and Analytics

## 모든 것을 모니터링 함
로그, 네트워크 트래픽, 사용자 행위 등

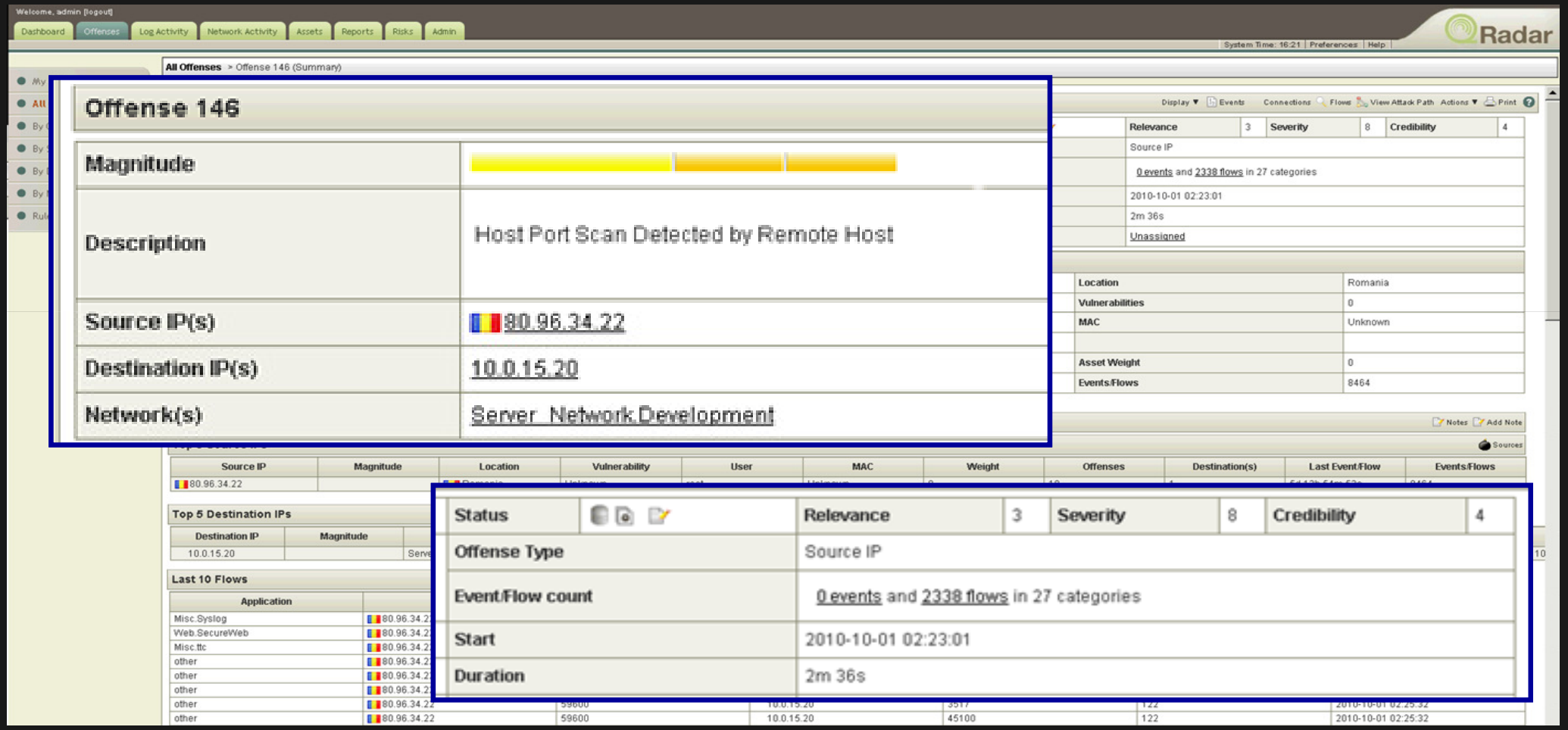
## 지능형 상관관계 분석
서로 다른 데이터 소스로부터 공통 분모를 찾아냄




## 비정상 행위(*Anomaly*)를 감지
숨겨져 있던 비정상 상황을 탐지

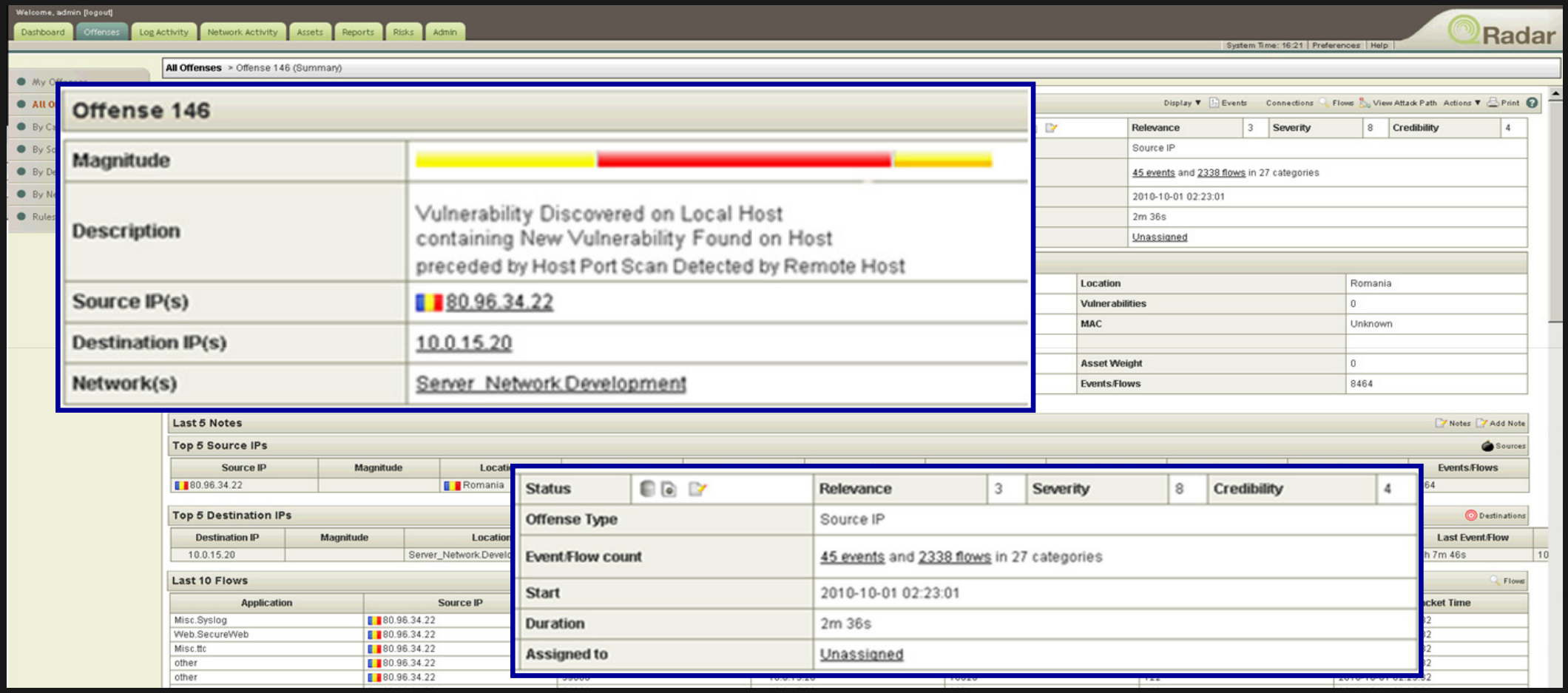
## 위협의 우선순위 결정
가장 위험하고 시급한 상황 확인

# 어플리케이션 취약점 정보 없이 Offense 스코어링




- 어플리케이션 취약점 데이터와 연계 전에는, Offense 우선순위가 낮음

# 어플리케이션 취약점 정보와 연계

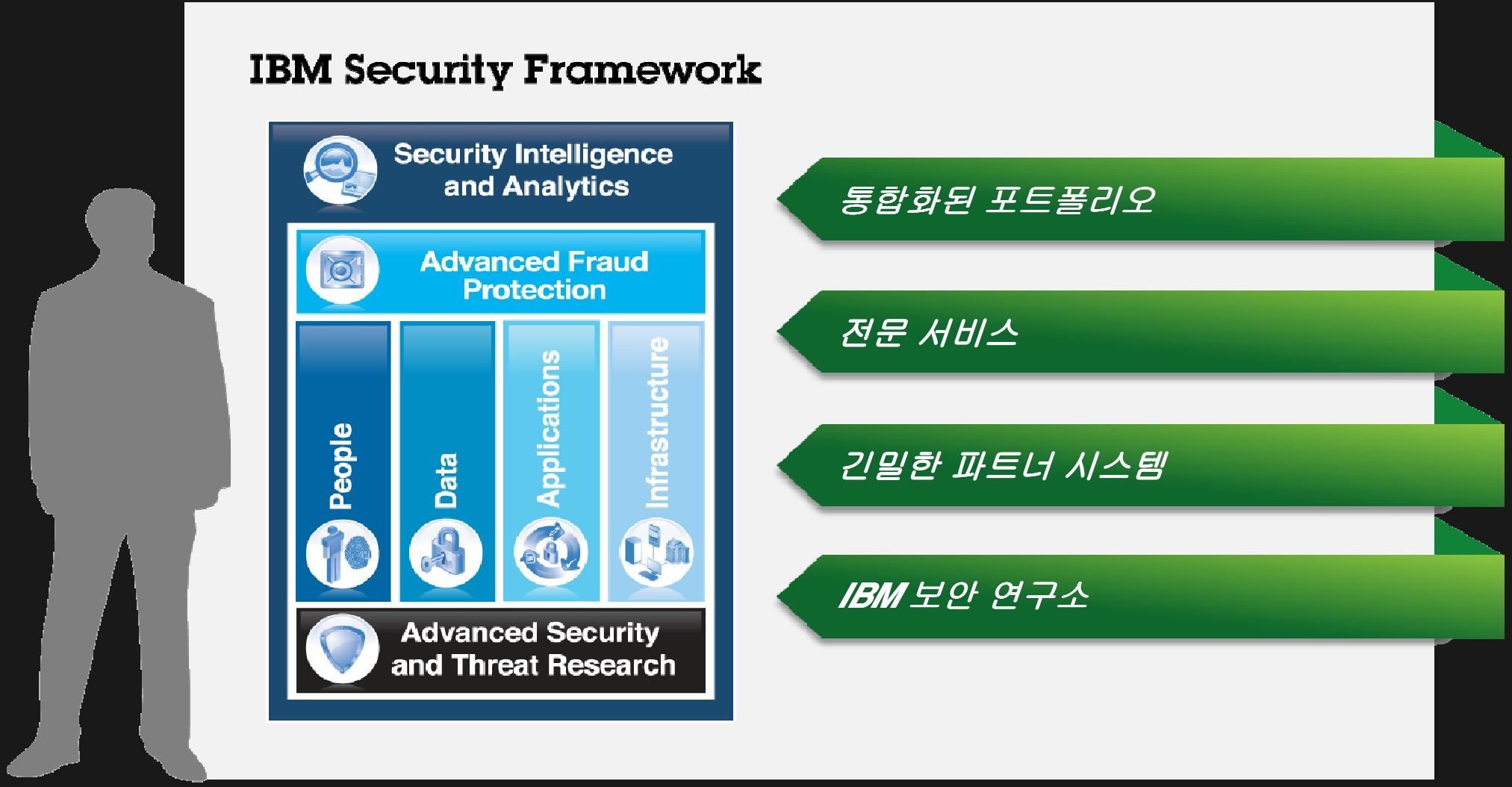



- 어플리케이션 취약점 정보와 연계하여 **Offense** 스코어링
- 알려진 취약점을 통해 공격 받고 있는 서버

# 고객 사례로 본 효과

| | | |
|---|---|---|
| 보안 지능화 및 분석 | 보안 및 규정 준수 향상 | 고객은 잠재적인 보안 위협에 대한 비용 증가를 최소화 하며 가시성을 높이고 *PCI* 규정 준수 달성 |
| 고도화 사기 방지 | 금융 사기 및 고도화된 보안 위협 방지 | 고객은 단계별 보안 규정을 준수하며 단계별 온라인 금융 사기를 제로 수준으로 낮춤 |
| 사람 | 비용을 절감하며 사용자 접근을 관리 | 고객은 헬프 데스크 비용을 ***30%*** 절감 하였으며 그 결과로 수십억 절감 |
| 데이터 | 데이터 무결성 유지 및 유출 방지 | 고객은 데이터 저장 공간 및 규제 준수 비용 수십억 절감 |
| 어플리케이션 | 웹 어플리케이션의 자동화된 보안 테스트 | 고객은 ***225***개의 새로운 어플리케이션을 추가 하였으며 매년 보안 사고 없이 ***1000***조건의 트랜잭션 처리 |
| 인프라 | 적극적인 경고, 단순화된 모니터링 및 관리 환경 | 고객은 모든 디바이스 및 네트워크를 모니터링 하여 모든 사이트의 정상적인 트래픽 중지 없이 제로 수준의 오탐 처리 |

# IBM 보안 프레임워크와 함께 IT 자산을 지키세요!




IBM