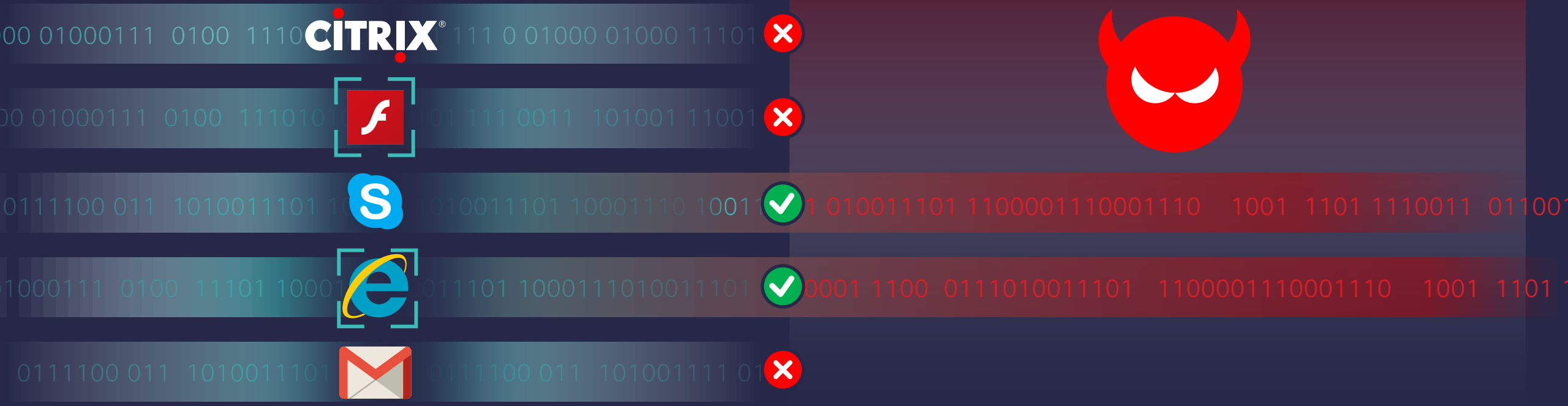
금융망보호를 위한 지능형 차세대 APT 방어 아키텍처

Yong-Ho Kim(yonghkim@cisco.com)
Security Consulting Systems Engineer, Cisco Korea

Dec 11, 2014

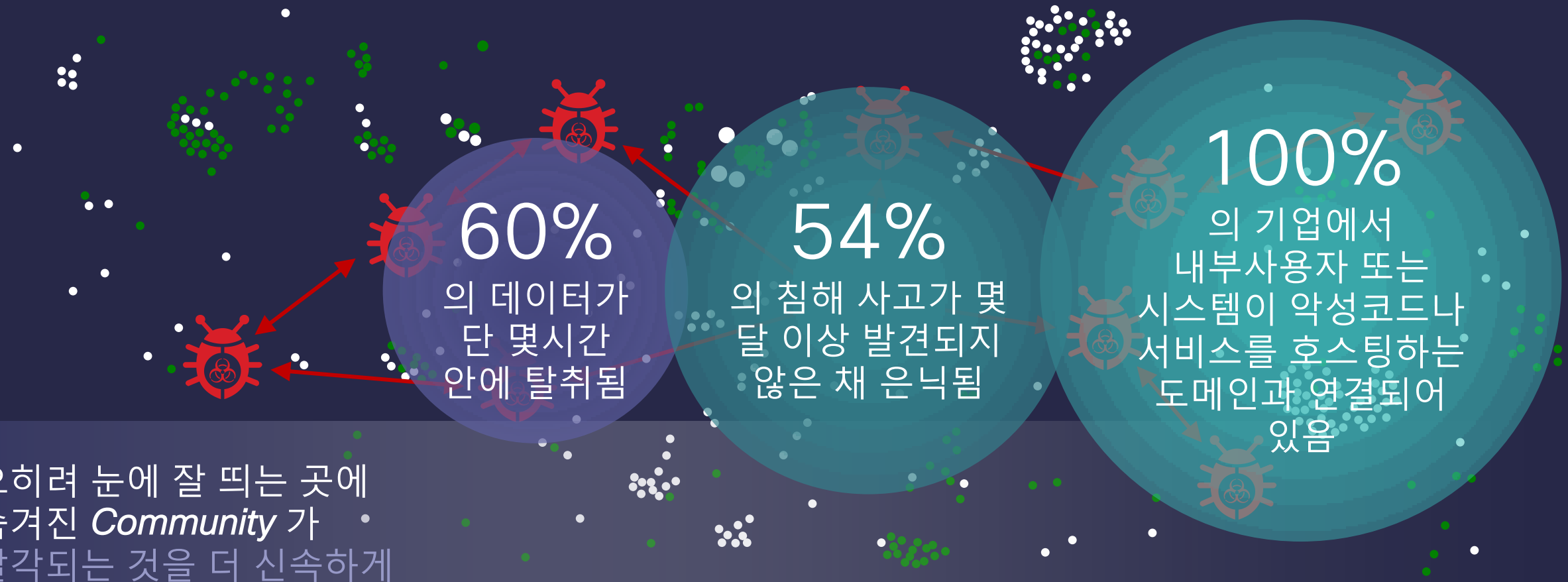
기존 APT 보안 솔루션들의 문제점

특정 공격시점의 차단, 탐지/분석 위주	결국...실제 위협은 놓치는...



기존 APT 보안 솔루션들은 은닉된 공격에 대한 탐지와 분석은 가능하나 특정시점에 국한
더욱 지능화된 공격 및 악성코드들에 의해 쉽게 우회

실제 위협 상황은 바로 가장 흔한 곳에 잠재된……



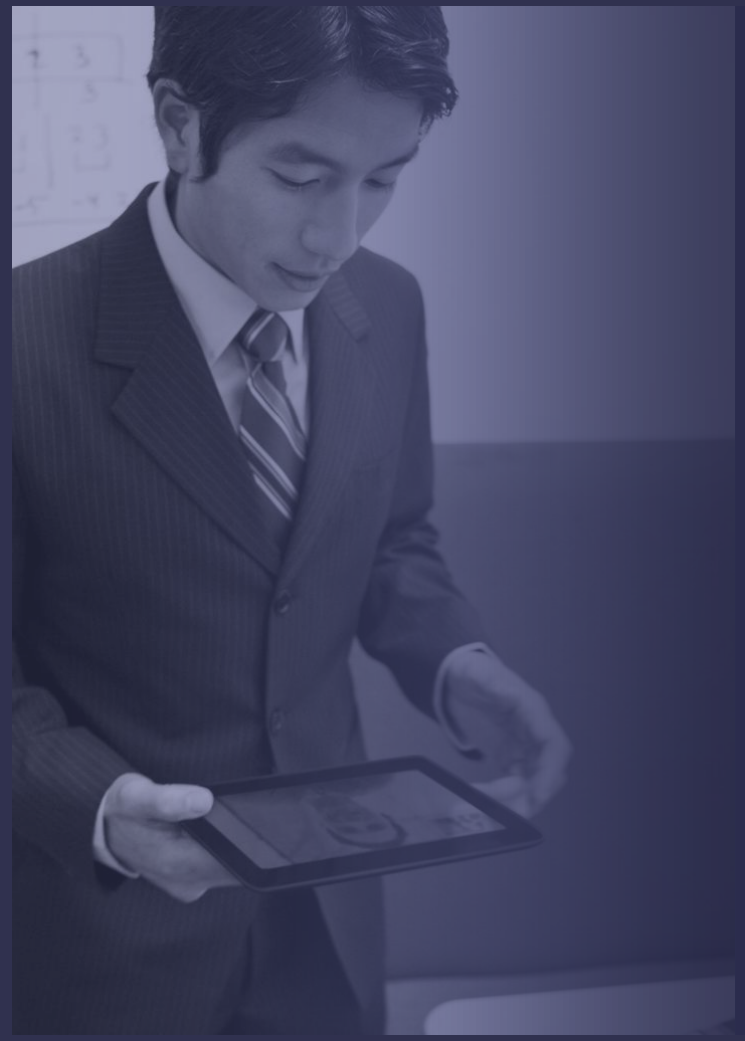
오히려 눈에 잘 띄는 곳에
숨겨진 *Community* 가
발각되는 것을 더 신속하게
탐지하고 피할 수 있음

단독적인 '심층적인 방어' 전략의 부족성

사일로 형태의
접근 방식

매우 불투명한
가시성

고정적이고
수직화됨



복잡성증가

효율성 저하

미탐된 위협

지능화된 공격

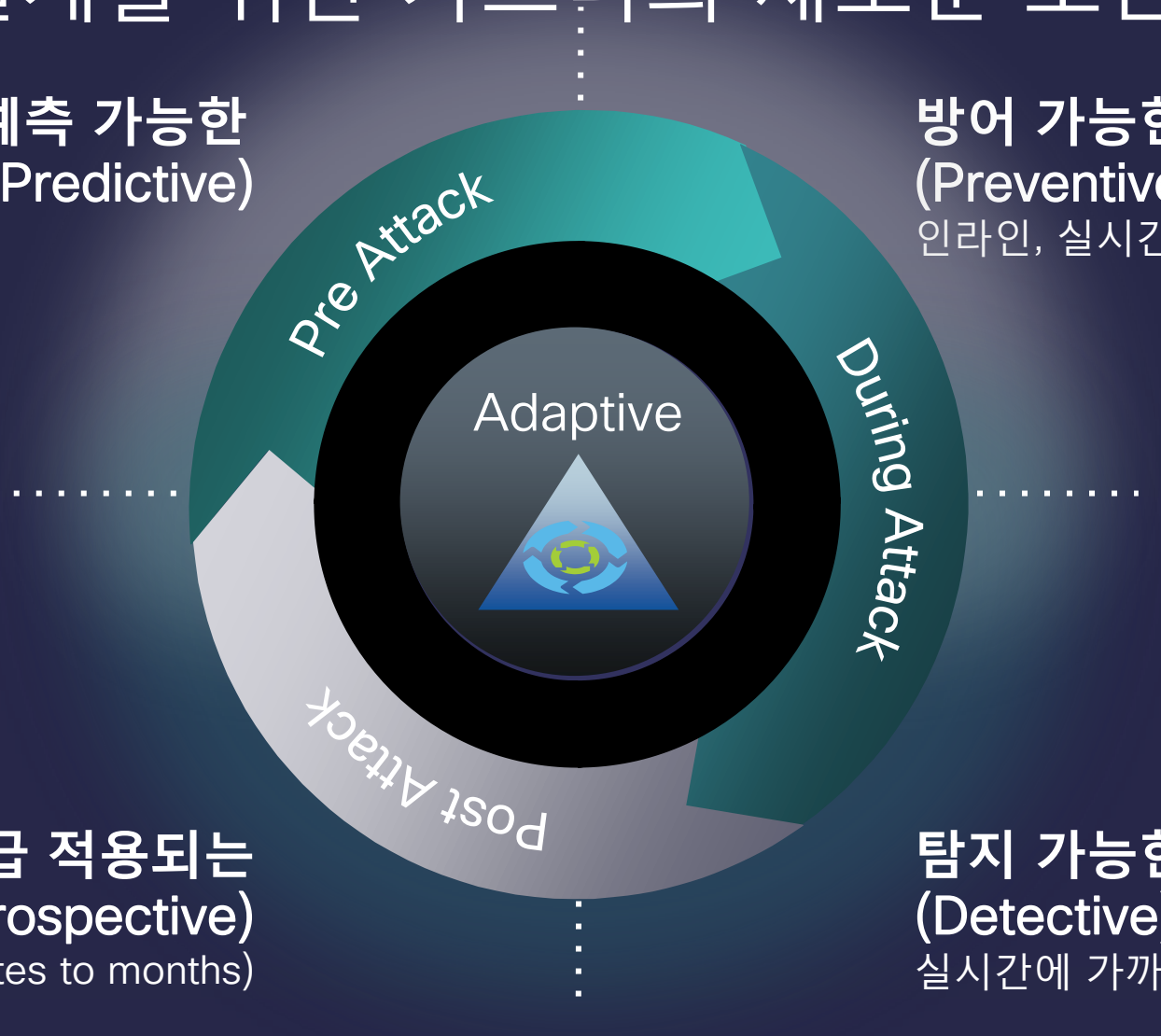
느린 대응

피해 확산

보안 요구 진화의 수렴:
적응형 보안 설계를 위한 가트너의 새로운 보안 모델

예측 가능한
(Predictive)

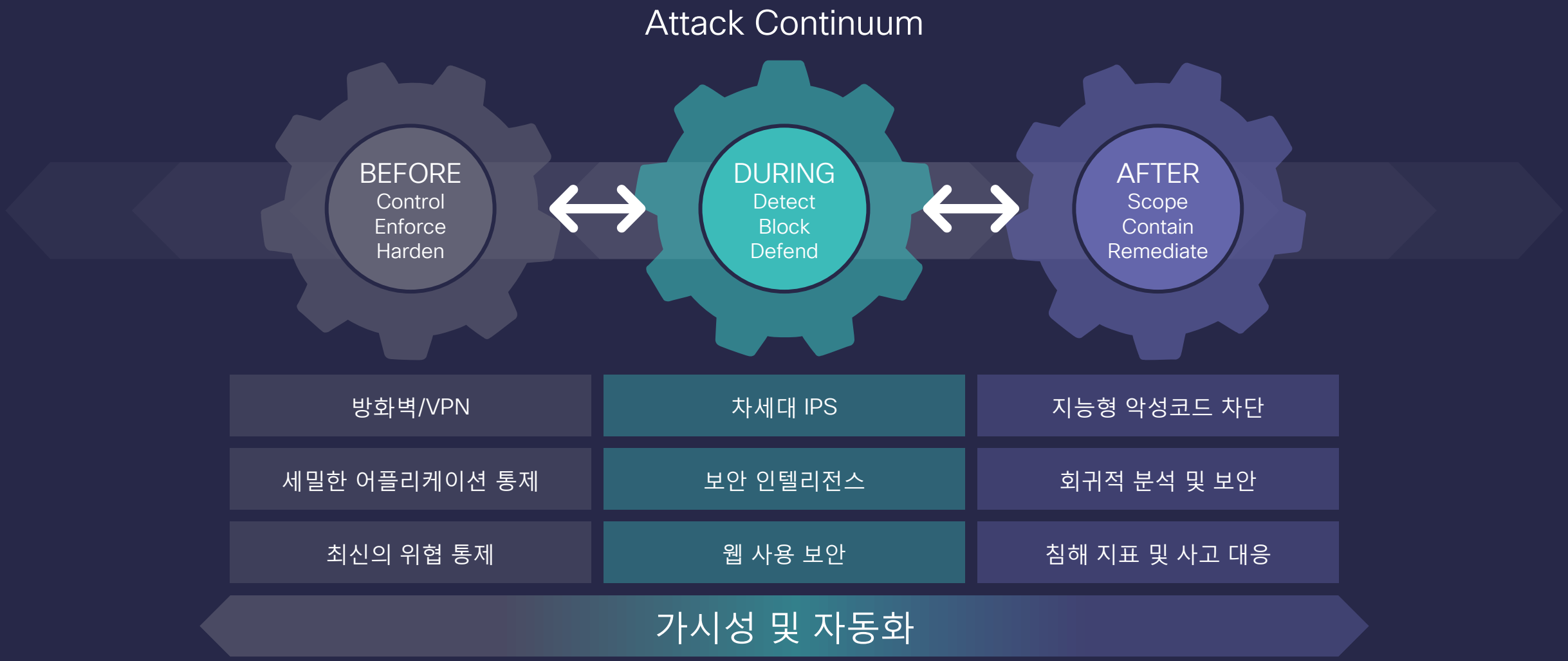
방어 가능한
(Preventive)
인라인, 실시간 (subsecond)



소급 적용되는
(Retrospective)
사후 사건화 (minutes to months)

탐지 가능한
(Detective)
실시간에 가까운 (seconds to minutes)

시스코의 지속적인 공격 전반에 걸친 통합 위협 방어 모델



지능형 지속 위협 공격에 대한 핵심은 *"가시화"*

지능형 지속 위협 공격 방어를 위한 기본 전제

지능형 지속 위협 공격전(Before) 상황 분석 및 조기 경보

주어진 상황과
위협의 상관분석

동적인 보안 통제

다중 벡터 데이터
상관 분석

지속적인
모니터링을 통한
소급 적용

지능형 지속 위협 공격중(During) 동적인 대응

주어진 상황과
위협의 상관분석

동적인 보안 통제

다중 벡터 데이터
상관 분석

지속적인
모니터링을 통한
소급 적용

지능형 지속 위협 공격후(After) 지속적 상황 모니터링 및 추적

주어진 상황과
위협의 상관분석

동적인 보안 통제

다중 벡터 데이터
상관 분석

소급 보안 적용

지능형 지속 위협 공격후(After) 소급적 보안대응

주어진 상황과
위협의 상관분석

동적인 보안 통제

다중 벡터 데이터
상관 분석

소급 보안 적용

시스코 플랫폼 익스체인지 그리드(pxGrid) 아키텍처

다양한 플랫폼간의 상황 정보 교환 및 대응 아키텍처

pxGrid 를 통한 IT 인프라 전반에 걸친 보안 플랫폼화

지능형 지속 위협 공격 전과정에 걸친 대응, 지능형 차세대 보안 아키텍처

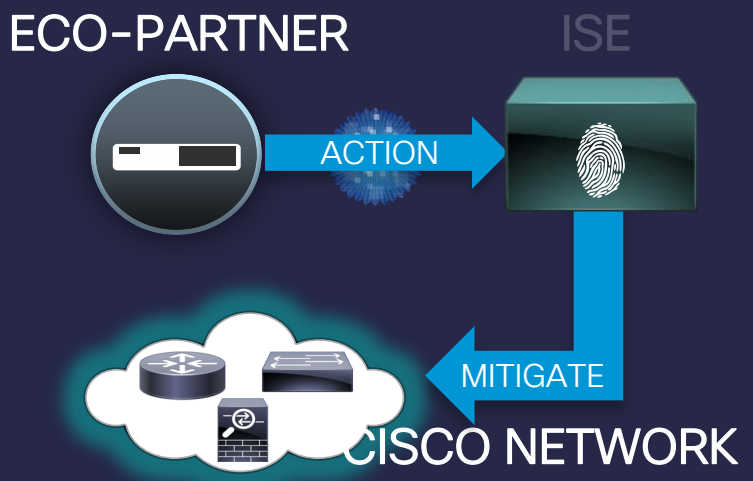
1 개별화된 IT 인프라를 사용자/단말 식별 및 네트워크 인식기반의 IT 보안 플랫폼화

ISE에서 파악된 사용자/단말 그리고 네트워크 상황 정보를 기존 IT 인프라스트럭처에 공유

2 IT인프라 상황정보 기반의 동적인 네트워크 보안 정책 플랫폼화

에코파트너사 솔루션으로 부터 획득된 보다 다양한 상황 정보를 토대로 정확하고 효과적인 네트워크 접근제어 정책 수립

3 보안/네트워크 인프라스트럭처를 활용한 지속/능동적인 방어체계화



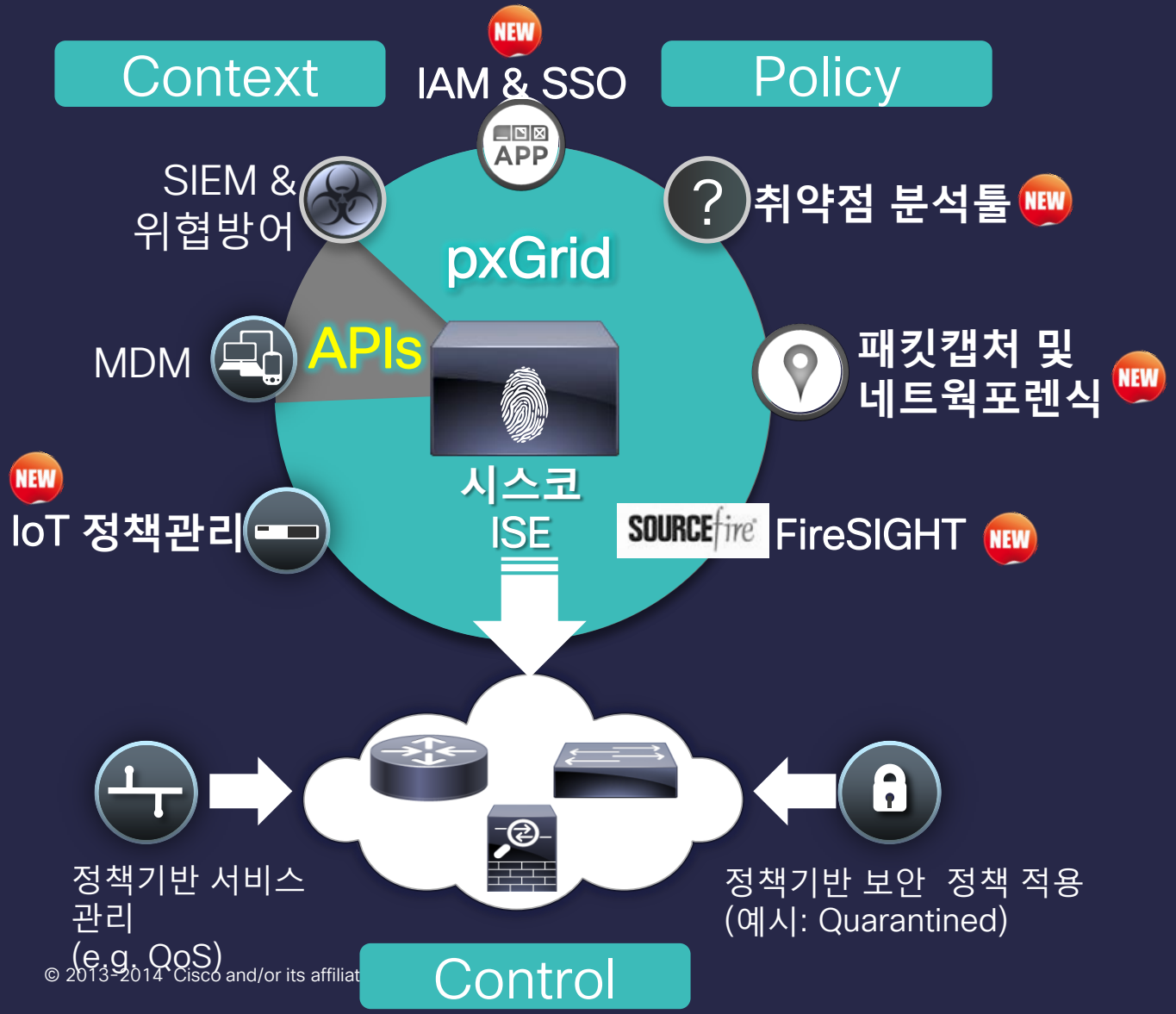
WHY CUSTOMERS CARE

"누가, 어떤 단말이, 어떤 방식으로의 접근인지" 에 대한 상황 정보의 입력으로 단순한 IP정보기반 정보보다 ***정확하고 효율적인 관리체계 제공***

다양한 솔루션으로부터의 정보 통합으로 포괄적인 네트워크 접근정책을 위한 ***단일화된 정책 관리 기능 확보***

보안 및 네트워크상의 위협 이벤트에 대한 대응 리소스 감소로 ***비용 효과적인 APT 방어 체계 구축***

시스코 pxGrid에 새롭게 합류한 솔루션

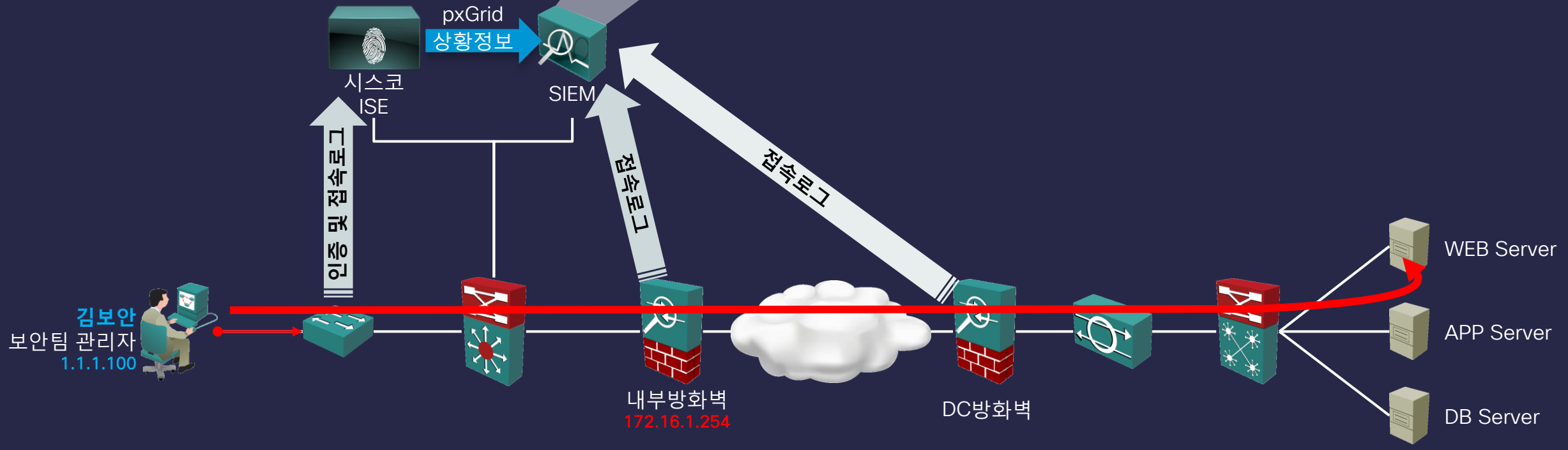


- CISCO (Source)Fire + ISE (TD)
- Ping Identity (IAM/SSO)
- tenable network security Tenable Nessus (취약점분석)
- EMULEX Emulex (패킷캡처)
- BAYSHORE Bayshore (IoT 정책/ DLP)
- NetIQ NetIQ (SIEM & IAM)
- splunk> Splunk (SIEM/위협방어)
- Lancope Lancope (SIEM/위협방어)

적용 1단계 : 상황 가시화

개별화된 IT 인프라를 상황 인식기반의 IT 보안 플랫폼화

접속일시	사용자	사용자IP	장비명	출발지	출발지 포트	목적지	목적지 포트	액션
12/8 11:30	김보안	1.1.1.100	내부방화벽	1.1.1.100	56844	10.1.1.200	80	허용
12/8 11:30	김보안	1.1.1.100	DC방화벽	172.16.1.254	56844	10.1.1.200	80	허용



적용 2단계 : 동적인 보안 정책

IT인프라 상황정보 기반의 동적인 네트워크 보안 정책 플랫폼화

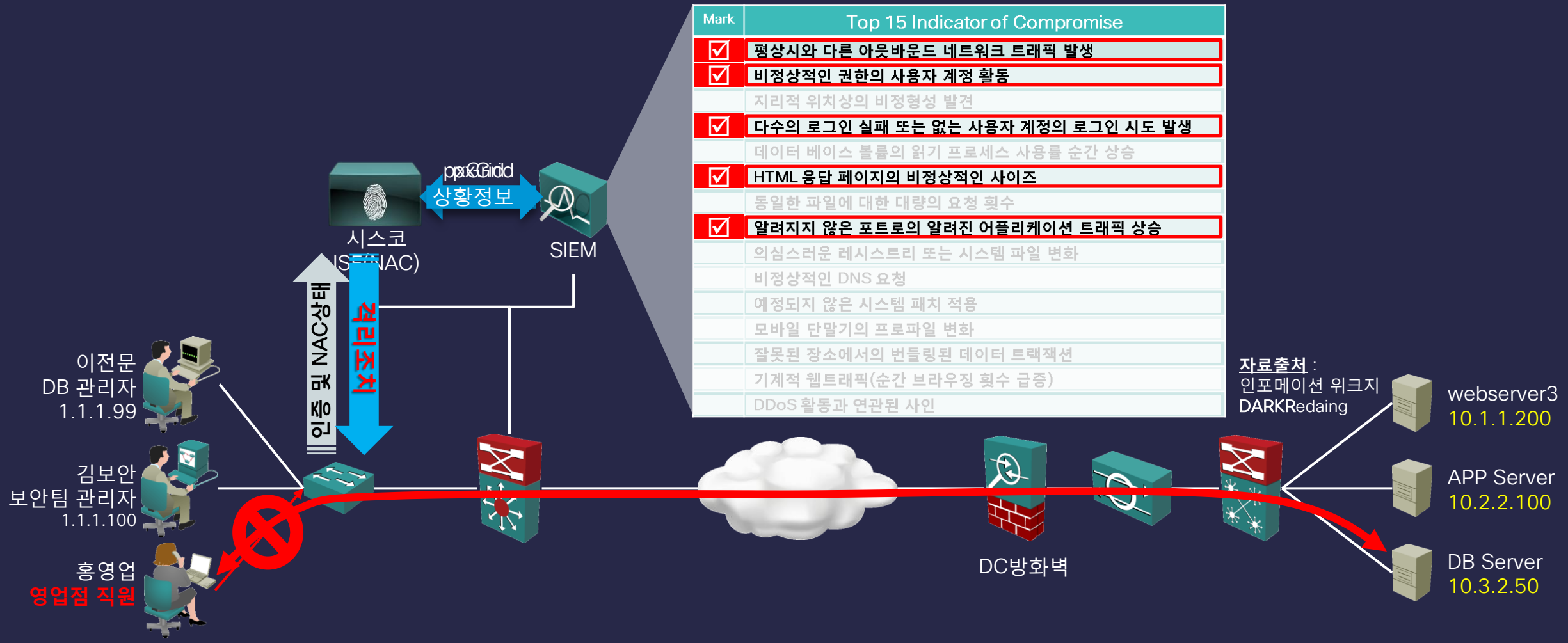
접속일시	사용자	사용자IP	장비명	출발지 객체 그룹(SGT)	출발지 IP	출발지 포트	목적지 객체 그룹(SGT)	목적지 IP	목적지 포트	액션
12/8 11:30	김보안	1.1.1.100	DC방화벽	InfoProtect	1.1.1.100	56844	webserver3	10.1.1.200	80	허용
12/8 11:30	이전문	1.1.1.99	DC방화벽	Nac_Fail	1.1.1.99	56844	DB_Server	10.3.2.50	80	차단

NAC 상태	계정권한	소속부서	결정된객체 그룹(SGT)
정상	Root	보안팀	InfoProtect
비정상	DB관리자	IT운영팀	NAC_Fail

객체그룹(SGT)	IP주소
InfoProtect(200)	1.1.1.100
NAC_Fail(100)	1.1.1.99

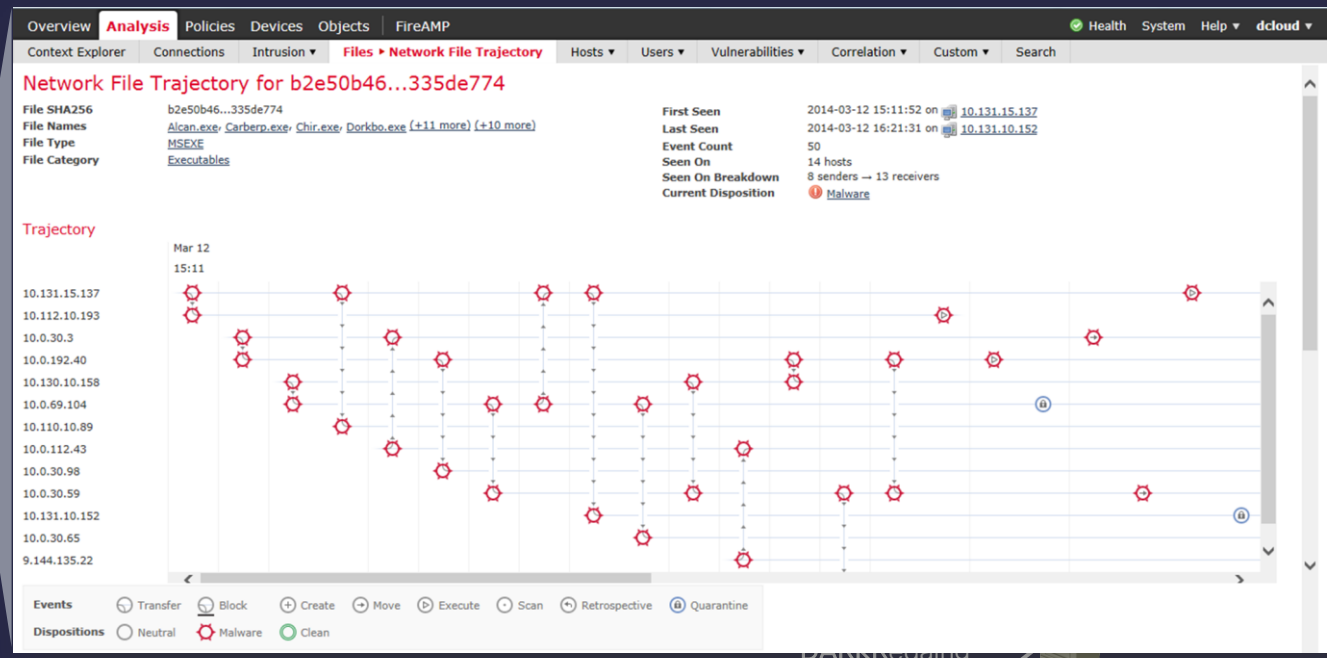
적용 3단계 : 소급 보안 적용

보안/네트워크 인프라스트럭처를 활용한 지속/능동적인 방어체계화



적용 3단계 : 소급 보안 적용

보안/네트워크 인프라스트럭처를 활용한 지속/능동적인 방어체계화



금융망보호를 위한 지능형 차세대 APT 방어 아키텍처
시스코 pxGrid 를 활용한 상황인식 기반의 지속, 능동, 소급 보안 대응

Thank you.