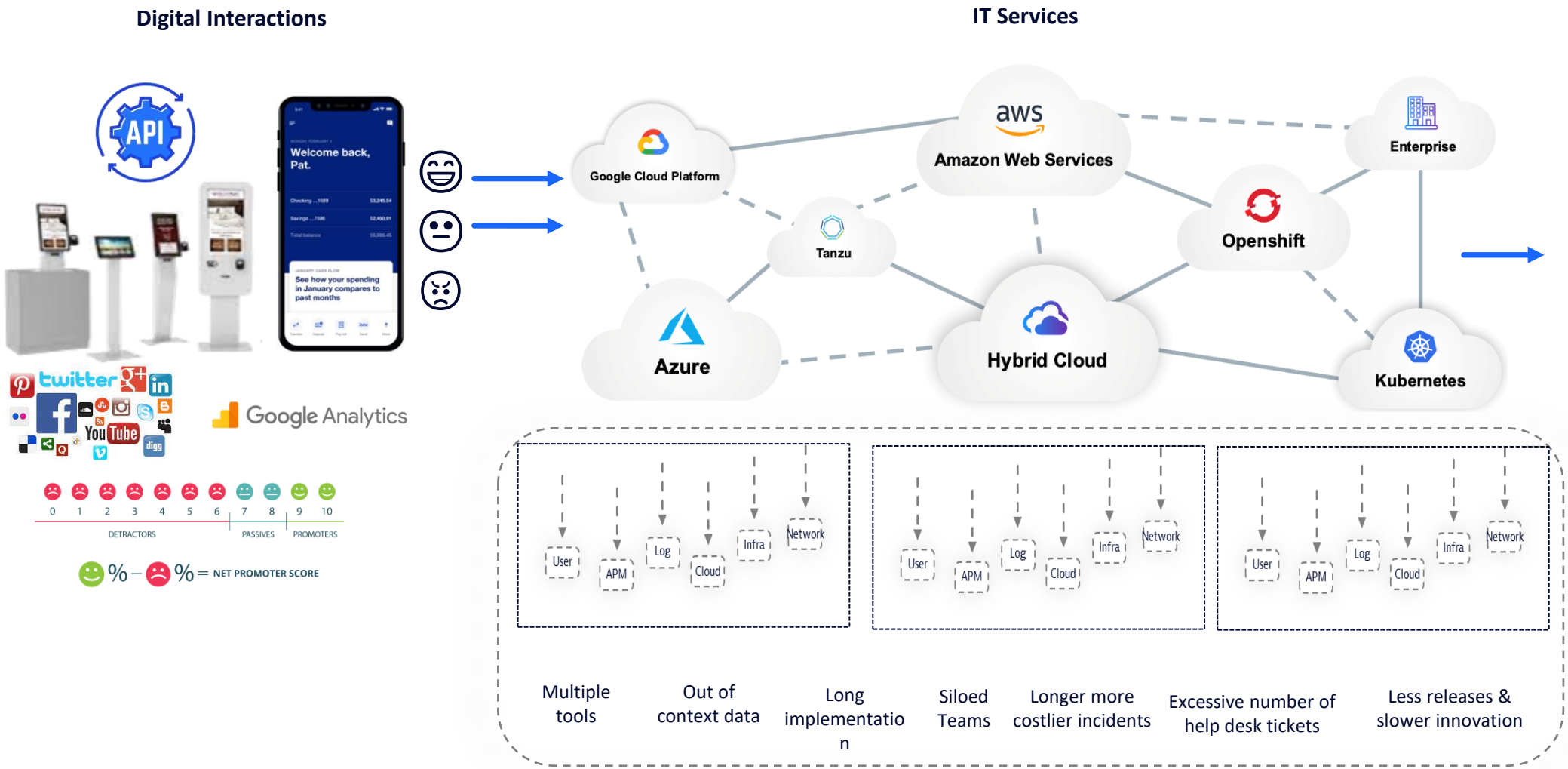
DevOps에서 DevSecOps로

Application Security 관리 자동화

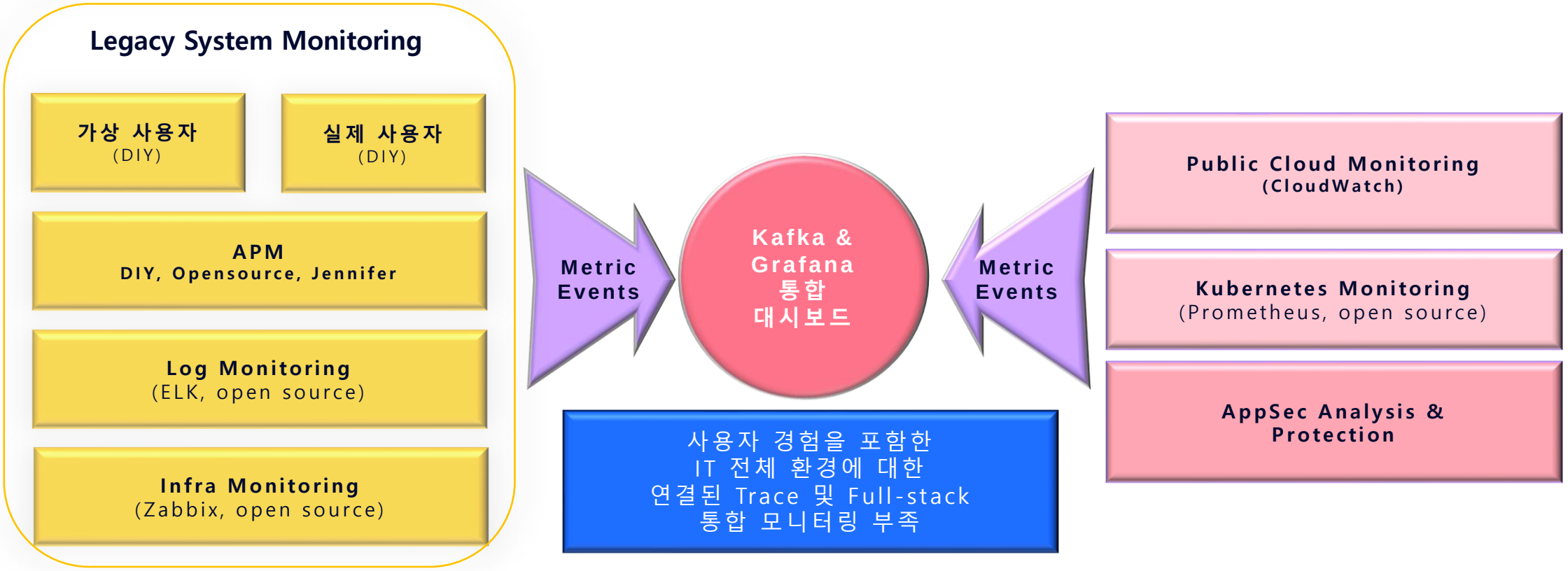
PRESENTER

나 성운 전무
SE Korea
Dynatrace Korea

완벽하고 안전한 엔드-투-엔드 디지털 서비스 관리 체계 구현



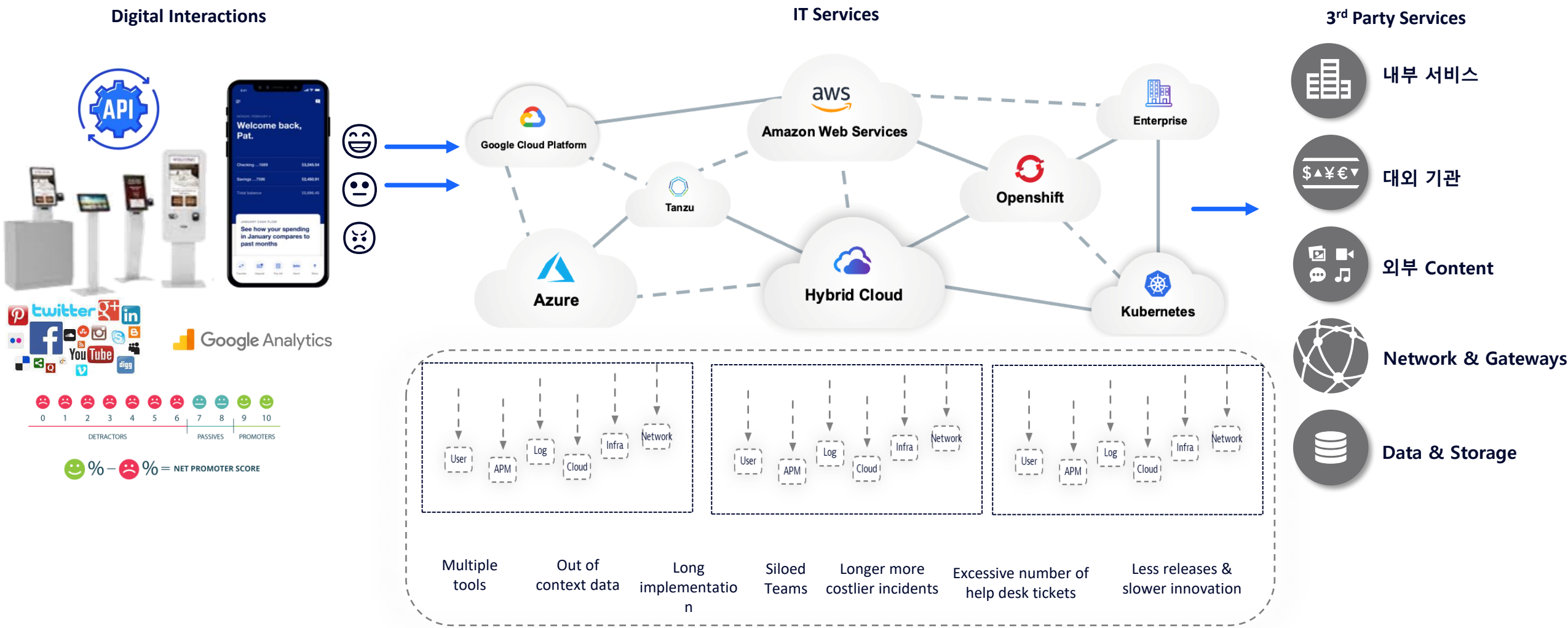
일반적 Silo 모니터링 체계 및 한계



- 팀별 독자적인 Silo 툴 선택, **8개 이상의 모니터링 Tool** 사용
- 각 Tool의 정보를 통합하여 **별도의 통합 Dashboard 구성**
- 담당자는 **개별 Tool을 조합하여 수동으로 원인분석** 수행

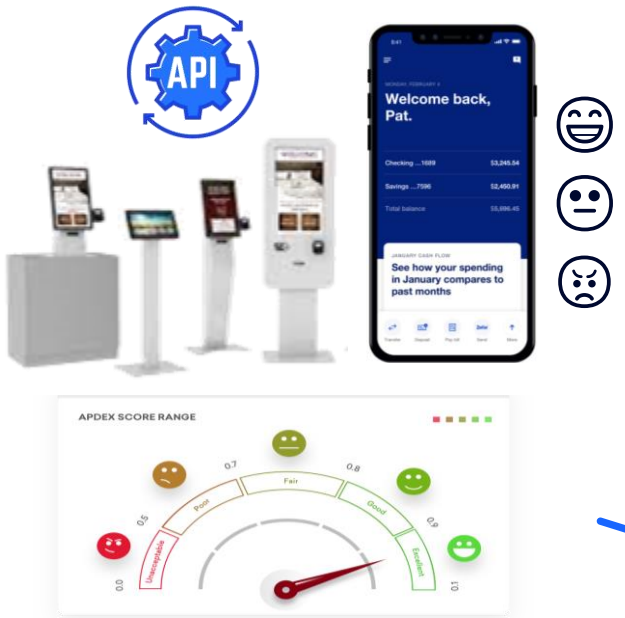
Kubernetes와 AWS 등 새로운 기술 환경으로 인하여 **IT환경이 더욱 복잡**해 지고 있어서, 전체적인 연결/선후 관계 이해 기반 **협업 및 보안 위협 관리에 어려움**이 있음

완벽하고 안전한 엔드-투-엔드 디지털 서비스 관리 체계 구현



완벽하고 안전한 엔드-투-엔드 디지털 서비스 관리 체계 구현

Digital Interactions



IT Services

Google Cloud Platform
aws
Amazon Web Services
Enterprise
Tanzu
Openshift
Azure
Hybrid Cloud
Kubernetes

3rd Party Services

- 내부 서비스
- 대외 기관
- 외부 Content
- Network & Gateways
- Data & Storage

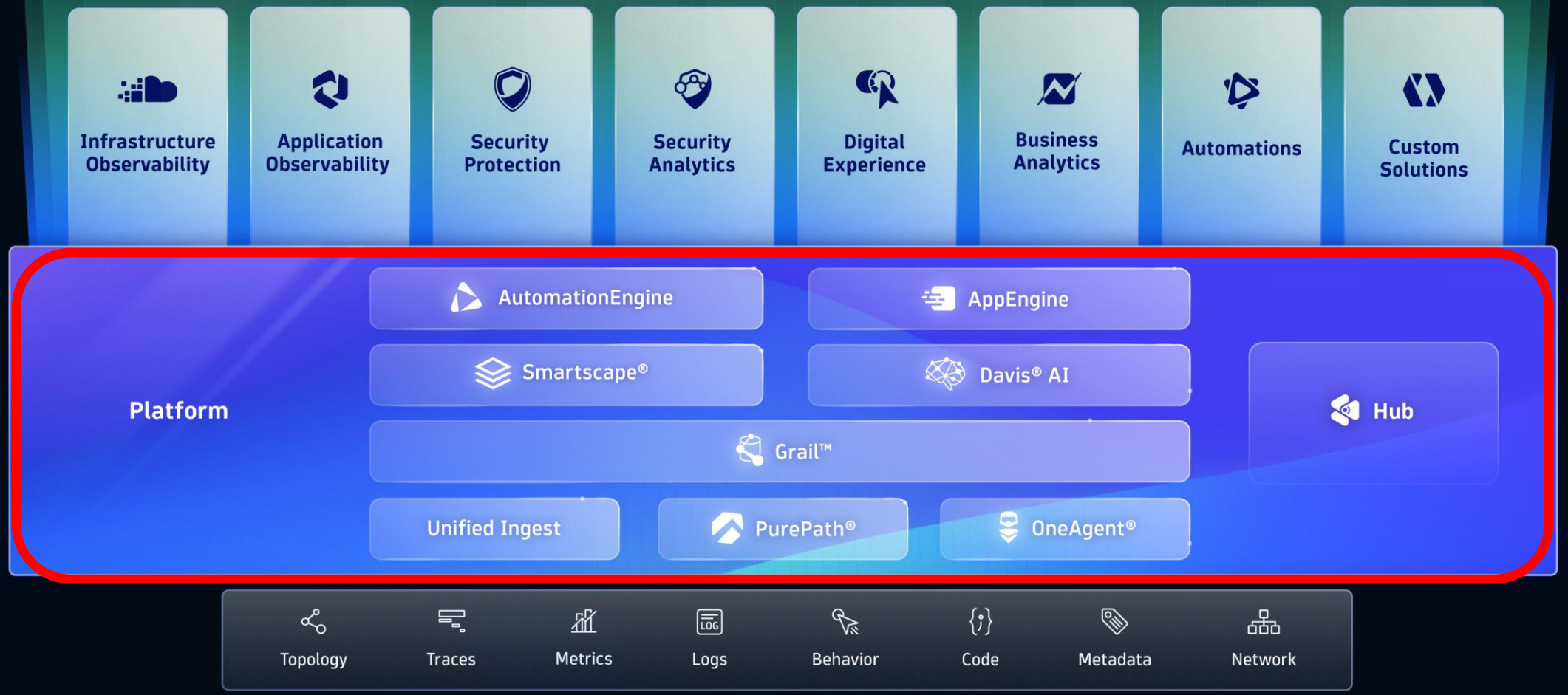
Observability및 App Security를 위한 **자동화된 통합 플랫폼**

비즈니스 context	사용자 경험	Contextual 데이터 연결/통합	AppSec	Intelligent 자동화	Dev + Sec + Ops

자동화 워크플로를 제공하는 데이터 레이크하우스와 Custom App 개발환경

dynatrace

Analytics and Automation for Unified Observability and Security **CLOUD DONE RIGHT.**



자동화 부분별 특허 기술 및 비즈니스 효과

데이터 수집

OneAgent 기술

Business impact

- 데이터 수집에 필요한 시간의 95% 이상 절감
- 사람의 실수로 인한 Blind point 생성 최소화
- 동적으로 변화하는 환경 자동 감지 및 관련 데이터 수집

Technical point

- ✓ 서버마다 한 번의 Agent만 설치
- ✓ 이후 인프라, K8S, 프로세스, 컨테이너, 서비스, 사용자 웹 체감 성능까지 자동으로 데이터 수집
- ✓ K8S에서는 Operator를 이용하여 한번만 설정하면 이후 모든 환경에 자동설치됨

연결,선후관계 추적

SmartScape 기술

Business impact

- 다양한 데이터들 간의 연결, 선후 정보 추적에 들어가는 시간의 95% 이상 절감
- 분석 시 자동으로 추적된 선후 연결정보를 이용하여 협업 효율성 증가 및 분석 시간 90% 절감
- 동적으로 변화하는 환경에서도 선후 연결 관계 자동 추적

Technical point

- ✓ 서비스 호출 관계를 추적하기 위해 개발자가 별도이 UUID를 삽입하지 않아도 여러 Tier의 코드레벨까지 자동 추적 가능
- ✓ 서비스 뿐만 아니라 container/process/인프라/사용자 액션까지 360도 선후 연결관계 모델링

이상상황 감지,분석

Davis 인공지능

Business impact

- 다양한 환경의 임계치를 자동으로 판단하여 사전에 문제를 감지하고 원인구간을 확인할 수 있어 MTTR 90% 감소
- 이상 상황 발생시 War room이 필요 없어지고, 투명하게 모든 부분을 확인할 수 있어 생산성 대폭 향상

Technical point

- ✓ 360도 선후 연결 정보를 모델링한 SmartScape 정보를 학습
- ✓ 일반적인 ML이 아닌 IT 성능 분석에 특화된 Deterministic AI 엔진 사용
- ✓ 유사한 패턴을 찾아 문제를 분석하는 방법이 아닌, 실제 호출 관계를 추적하여 최종 원인 구간을 확인하기 때문에 높은 정확성 제공

AppSec 관리

Vulnerability 감지/차단

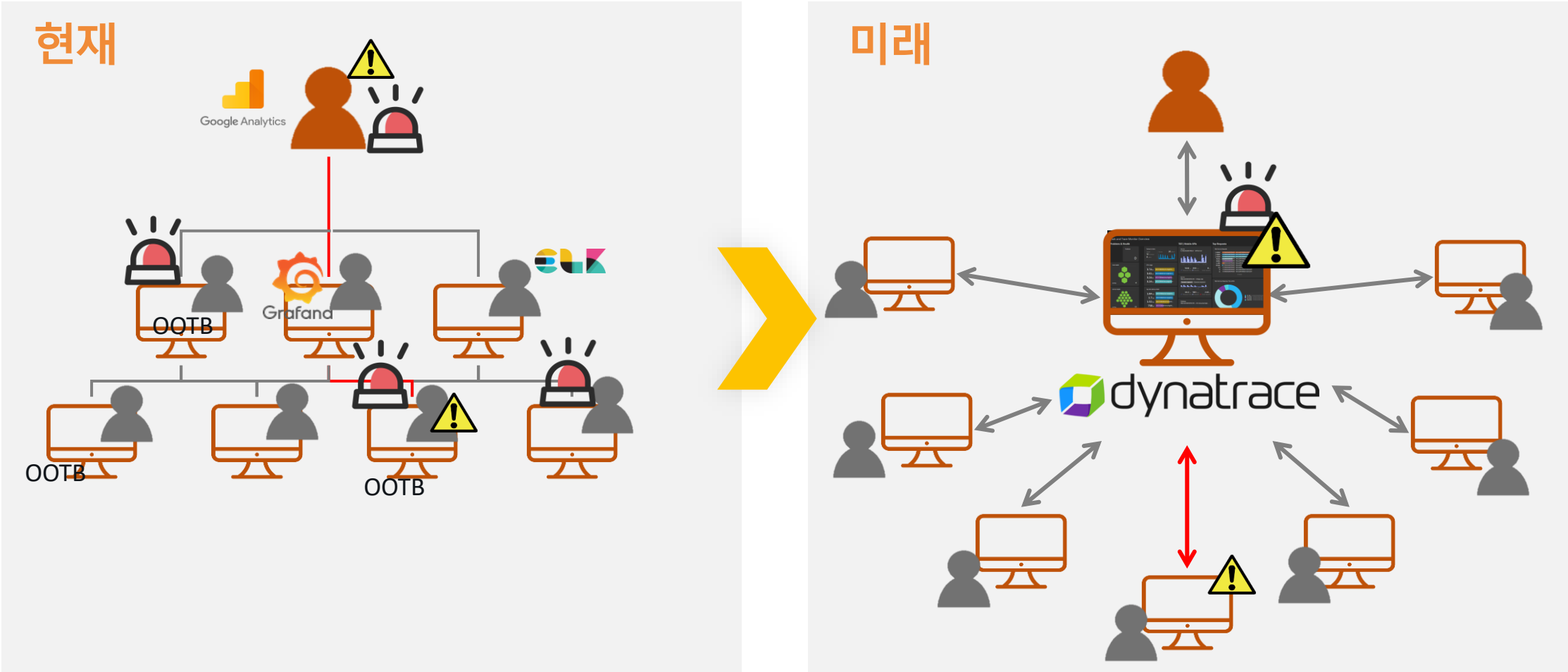
Business impact

- 최근의 Log4Shell 문제와 같이 급증하는 코드 보안 위협을 실시간으로 방어하여 비즈니스 안정성 향상 및 위험 예방
- 보안팀만의 관리가 아닌 개발/운영 담당자까지 모두 보안에 참여하는 협업 체계 구현

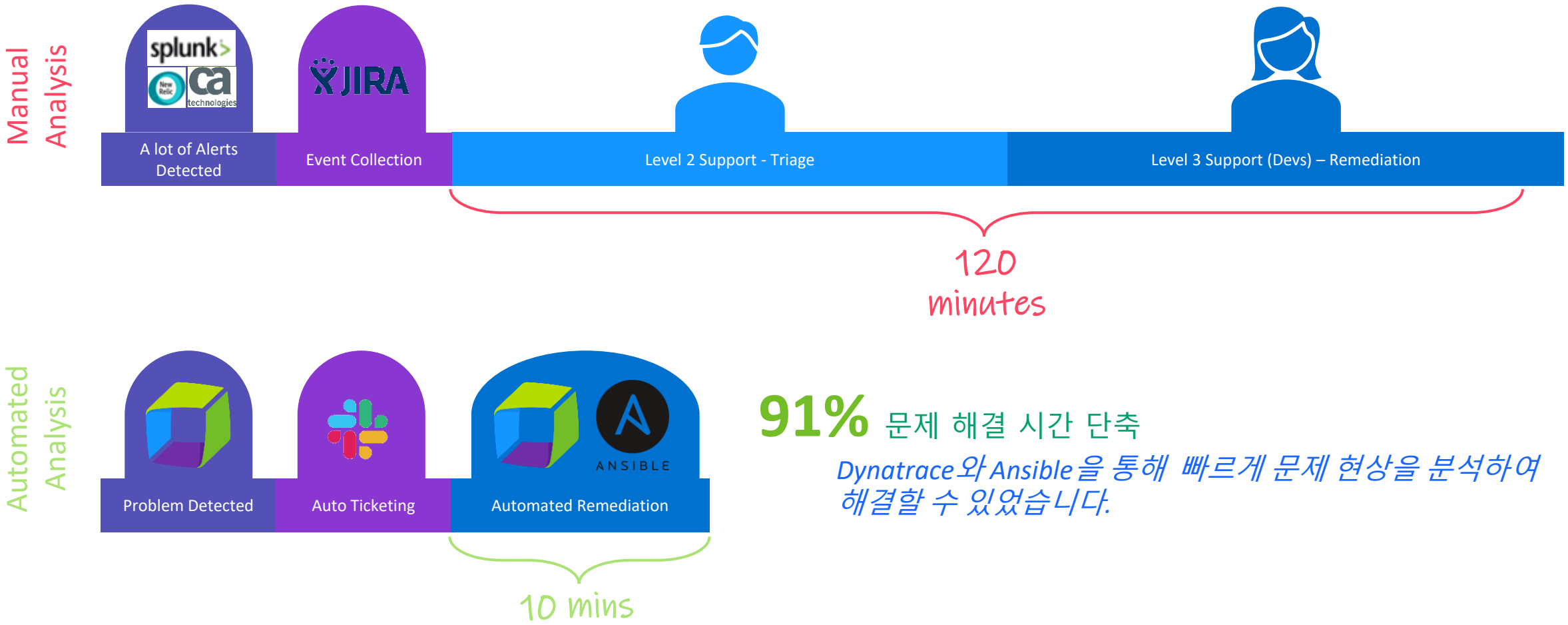
Technical point

- ✓ 별도의 보안 Agent를 설치할 필요 없이, OneAgent가 성능 뿐만 아니라 코드 보안 취약점까지 실시간 감시 및 분석
- ✓ 서버의 코드상에서 감지 및 방어를 수행하기 때문에 최후의 방어선 역할을 수행
- ✓ 영향 받은 모든 부분을 실시간 파악

자동화된 통합 플랫폼을 이용한 새로운 Workflow



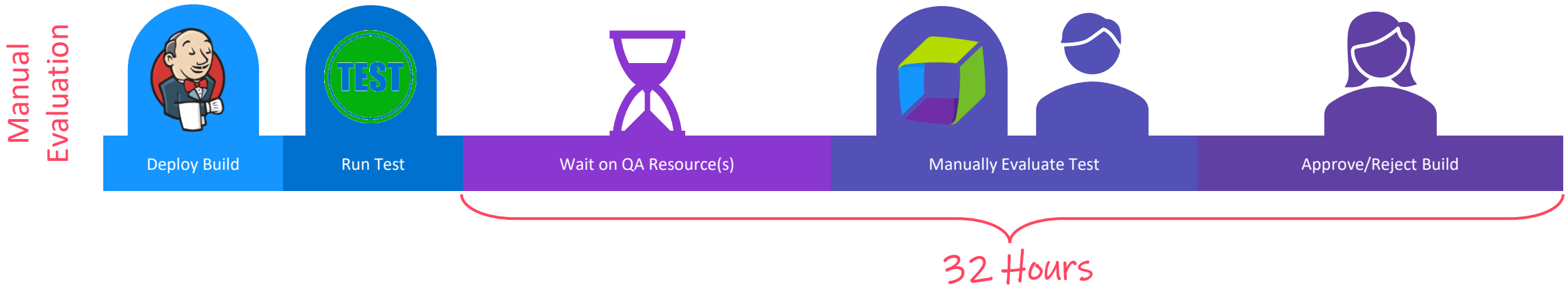
Global 선도 은행 – Problem Auto Analysis 사례

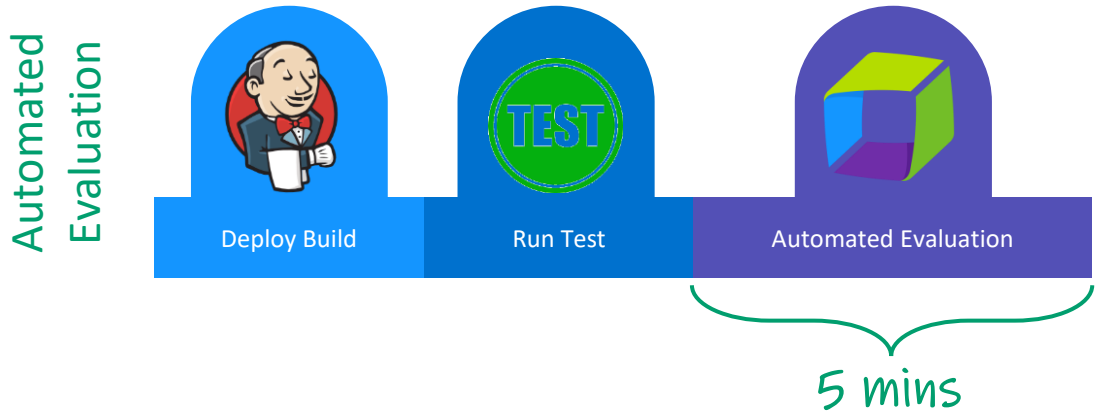


91% 문제 해결 시간 단축

Dynatrace와 Ansible을 통해 빠르게 문제 현상을 분석하여 해결할 수 있었습니다.

Global 보험사 - DevOps 성능 관리 자동화



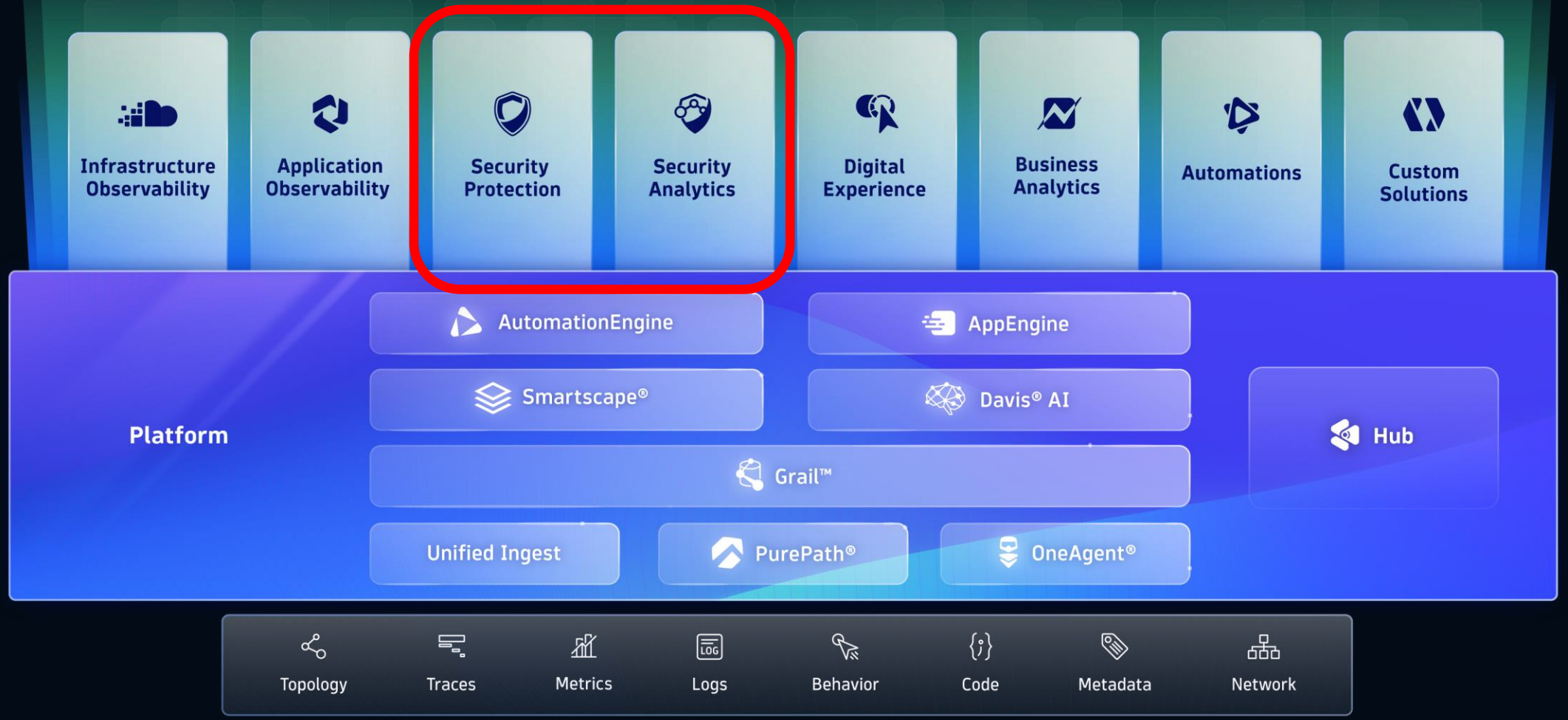


400x 성능 평가 기간 단축

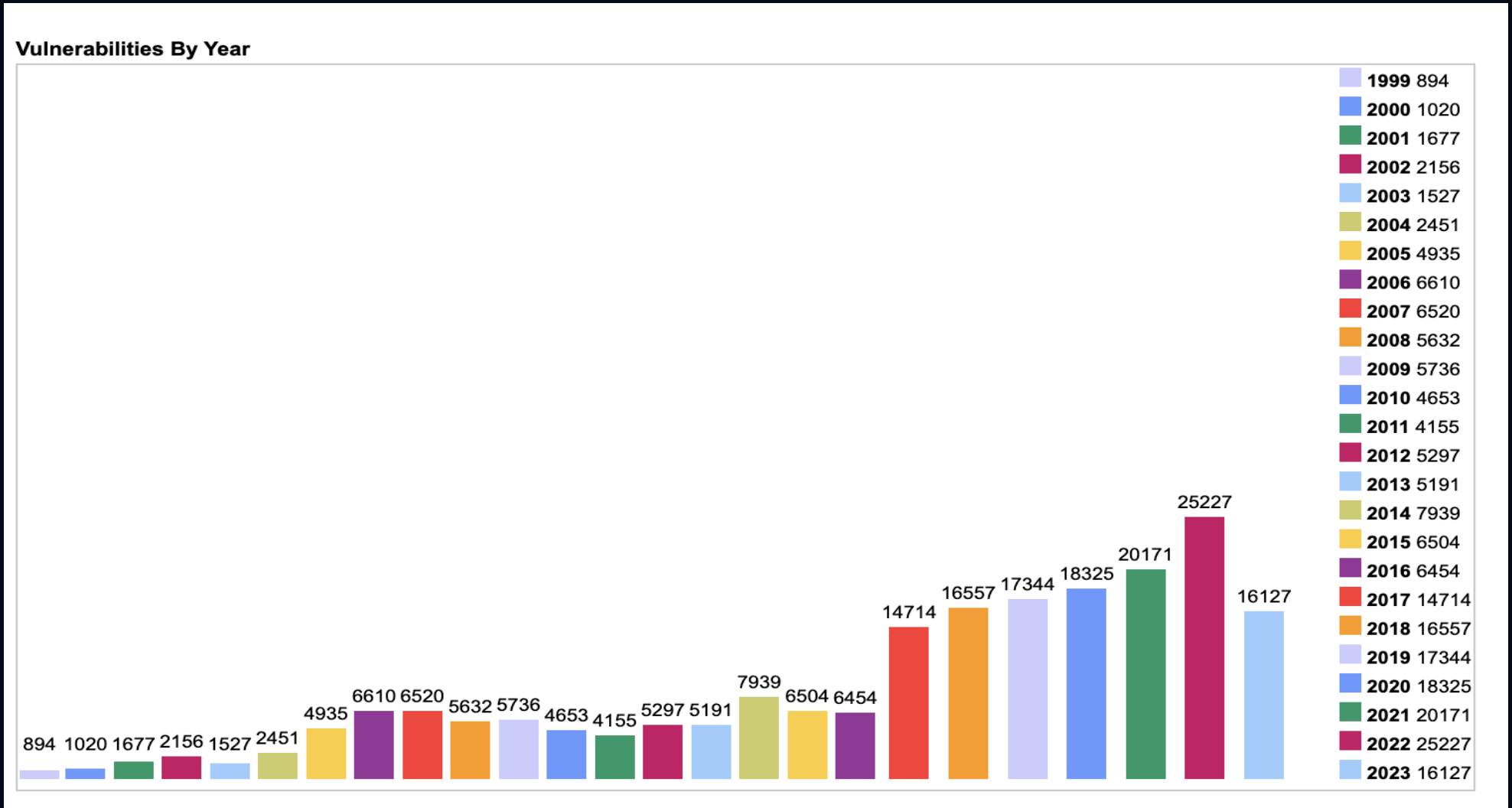
Dynatrace 를 통해 "You Build It, You Own It" 조직을 구축할 수 있습니다.

dynatrace

Analytics and Automation for Unified Observability and Security **CLOUD DONE RIGHT.**



Cloud-native 어플리케이션 위험 관리 어려움 증가



Source: https://www.cvedetails.com/browse-by-date.php

Cloud-native 어플리케이션 위험 관리 어려움 증가

3X

2017~21년 애플리케이션 취약점에 대한 공격 증가

75%

애플리케이션 취약점이 운영환경에 유출되는 것을 걱정하는 CISO

67%

개발자가 취약점을 검사하고 수정할 시간이 없다고 말하는 CISO

80

고위험 애플리케이션 취약점을 수정하는 데 걸리는 평균 일수

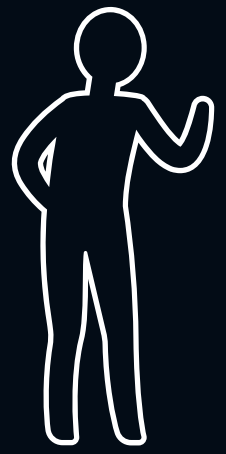
https://www.dynatrace.com/info/ciso-report/

Cloud-native 어플리케이션 보안은 기업 전체의 핵심 업무

어디에서 어떻게 영향 받지?

Dev

우리는 취약한가?

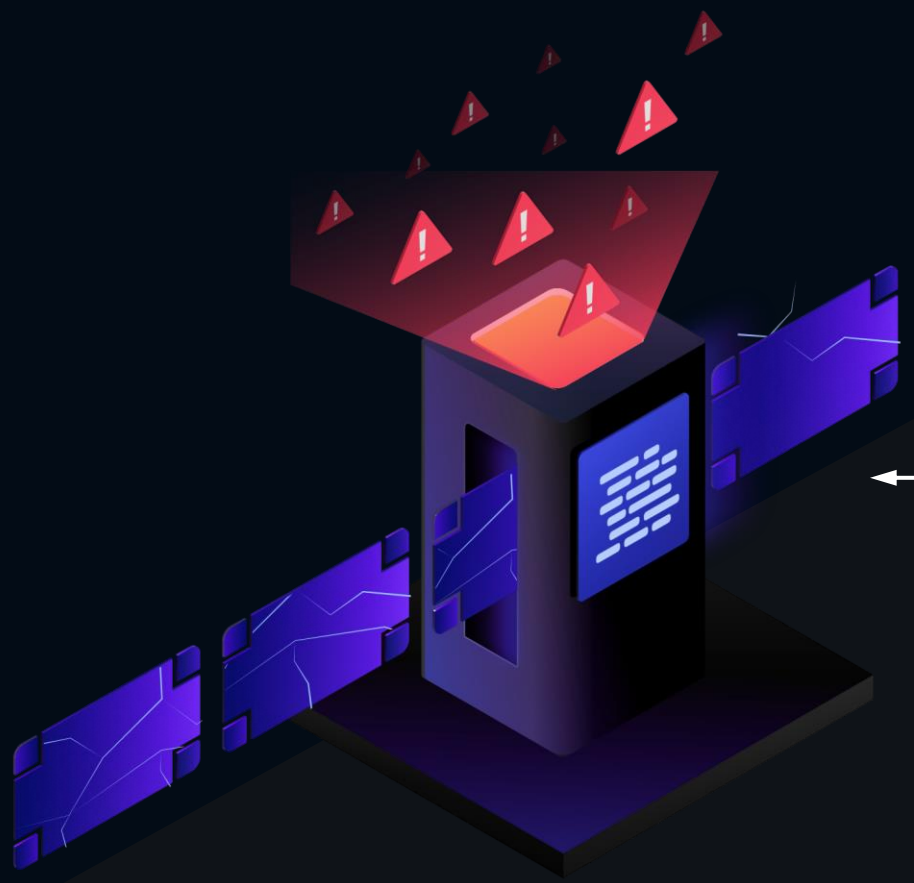


Sec

위험은 무엇이지?

Ops

전통적인 접근 방식의 한계



정적 코드 스캐너 (SCAT)

- 파이프 라인 초기의 정적 코드에서는 잘 작동
- 사용자 정의 가능, 수동 설정 및 업데이트
- 운영 Context에 대한 미반영
- 과도한 경보 및 오탐지

일부 취약점이 Production 단계에 도달

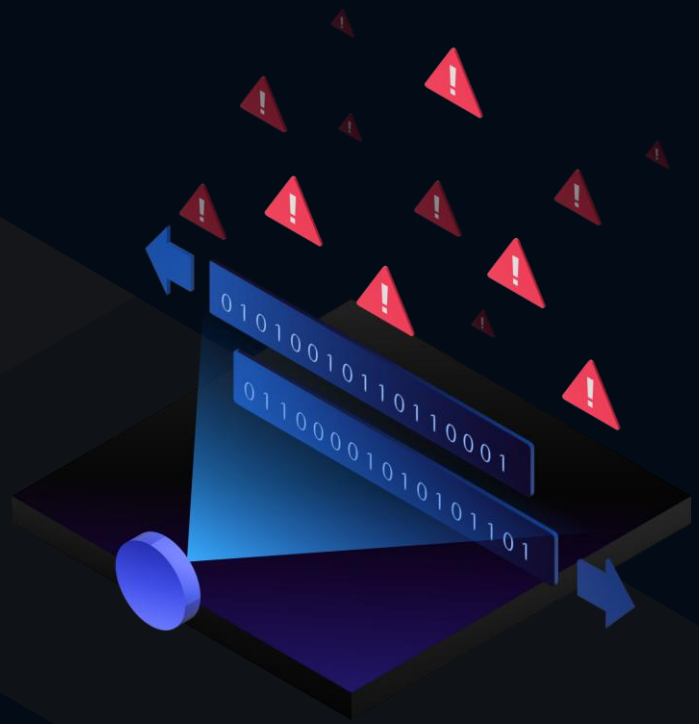
Pre-Production

Production

전통적인 접근 방식의 한계

네트워크 트래픽 스캐너

- 네트워크 주요 지점에서 다양한 공격 탐지
- 잦은 업데이트 필요
- 어플리케이션 컨텍스트가 없음
- 과도한 경보 및 오탐

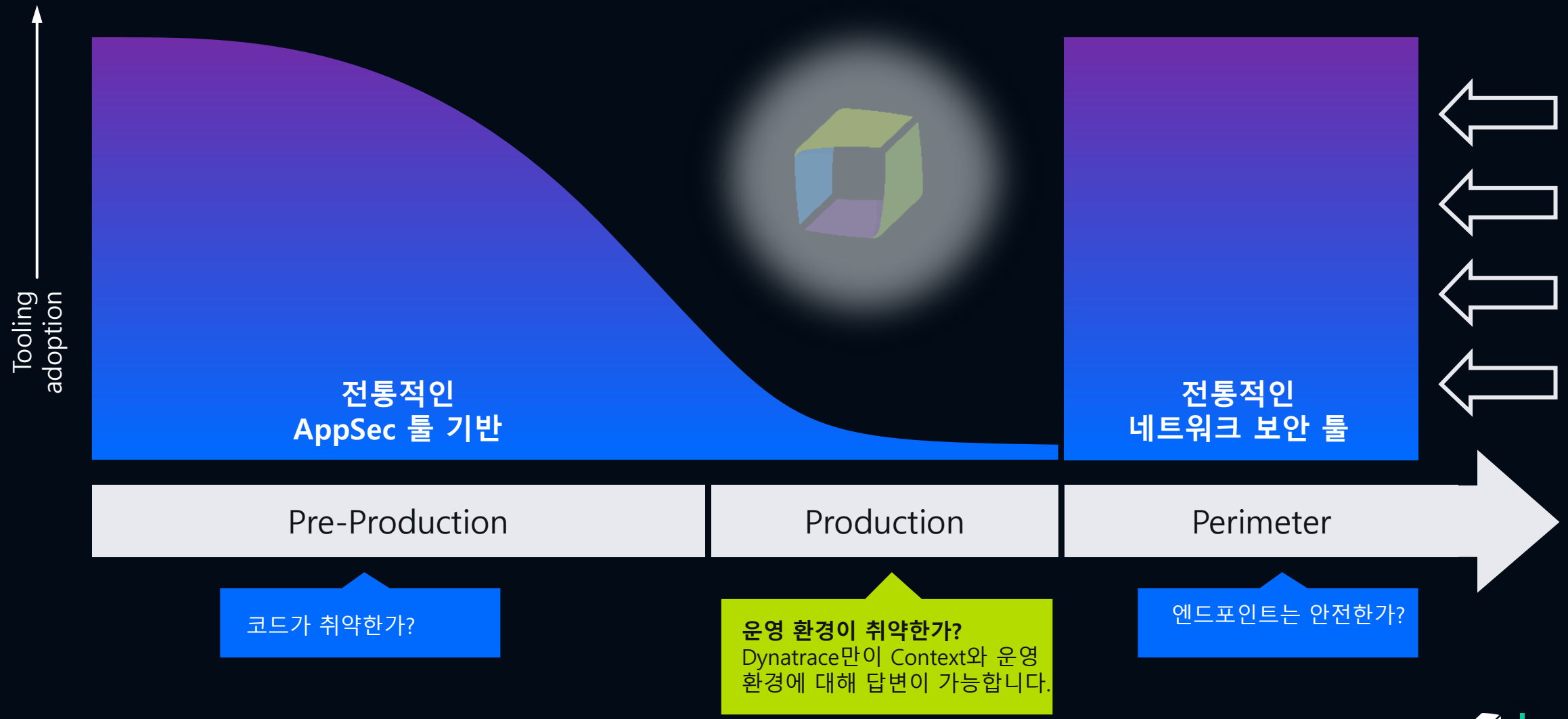


Pre-Production | Production | Network

전통적인 접근 방식의 한계

Pre-Production | Production | Network

운영 환경의 runtime vulnerabilities 위험 최소화



Log4Shell이 알려지고 몇 분 후 바로 자동 탐지 후 최우선 순위 배정 – Dynatrace AppSec

GitHub에 등록

NVD Vulnerability 등록

Snyk Vulnerability 등록

Dynatrace AppSec Vulnerability catalog 갱신

고객 환경 vulnerability 감지 Davis Security Score

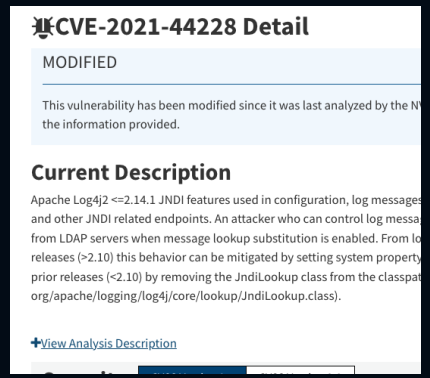
12월 10일, 00:40am

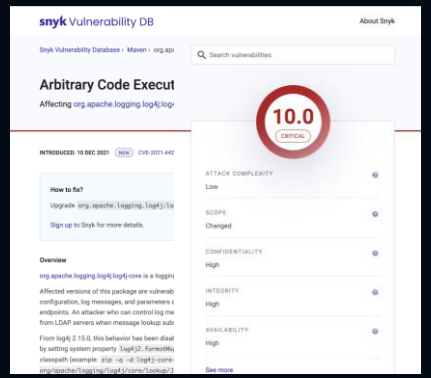
12월 10일, 10:15am

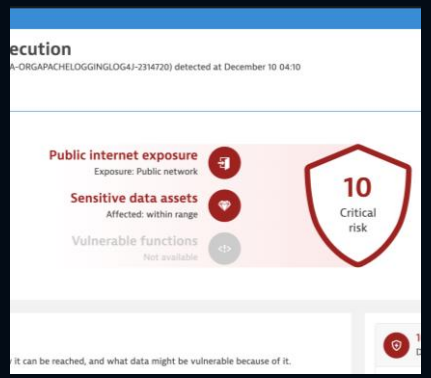
12월 10일, 10:45am

12월 10일, 10:50am

12월 10일, 11:05am







애플리케이션 코드 보안 취약성 실시간 감지, 우선순위 지정 및 보호

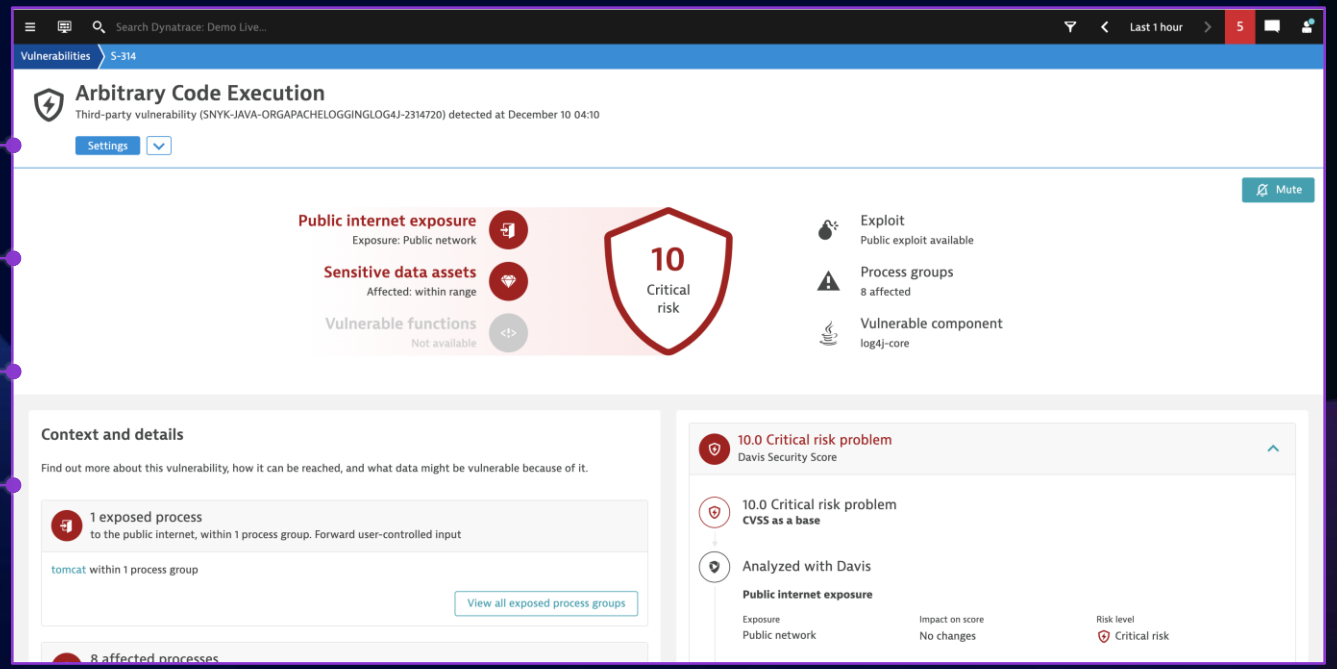
- Dynatrace는 복잡한 클라우드 네이티브 환경에서 어플리케이션에 대한 코드 취약성 문제(Vulnerability) 방지
- 전체적인 Full-stack 가시성을 제공하면서 동시에 DevSecOps로의 발전 지원

vulnerability 문제 발견

DAVIS가 우선 순위 평가

Topology를 활용하여 문제가 심각해 지기 전에 사전 조치

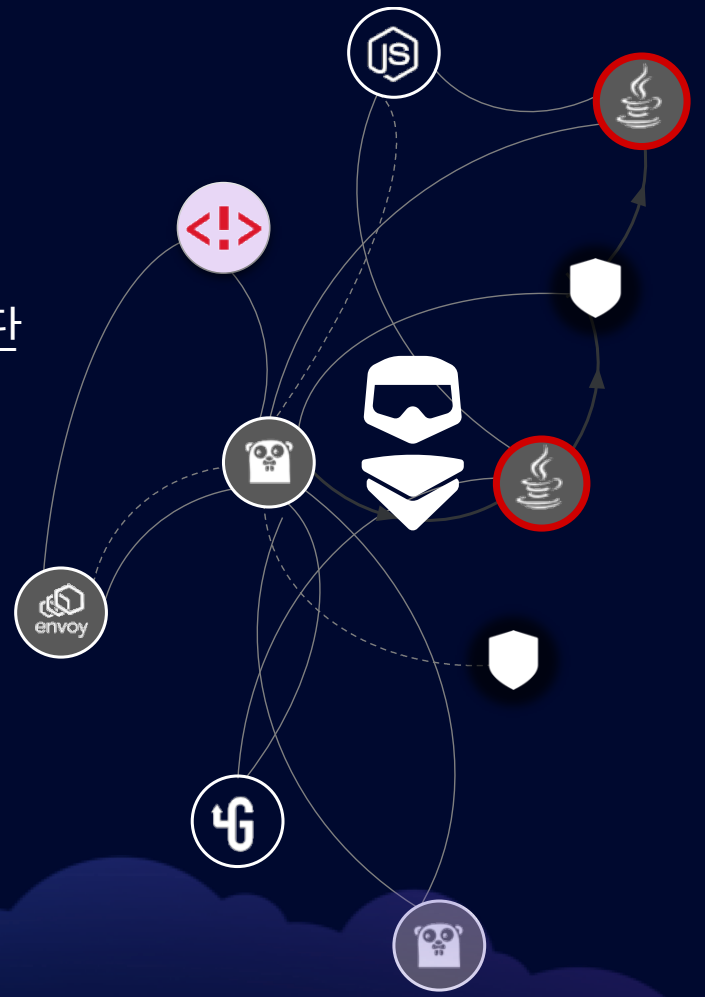
실시간 공격 탐지 및 차단



코드 취약성 탐지 후 런타임 응용프로그램 보호

코드 취약성(Vulnerability)로 인한 위험 감소

- SQLi 및 JNDI, Command Injection 형태의 공격 탐지 및 차단
- 오탐율 0%, 100% 정확
- OneAgent 활용, 쉽게 Enable/Disable 가능
- 사용자 경험에 대한 부정적인 영향 최소화



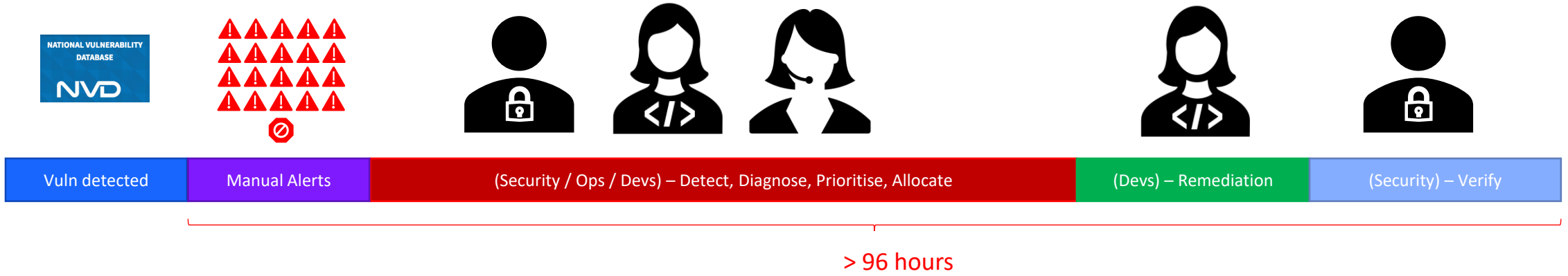
** Results from OWASP benchmark project test suite*

해외 대형 보험사

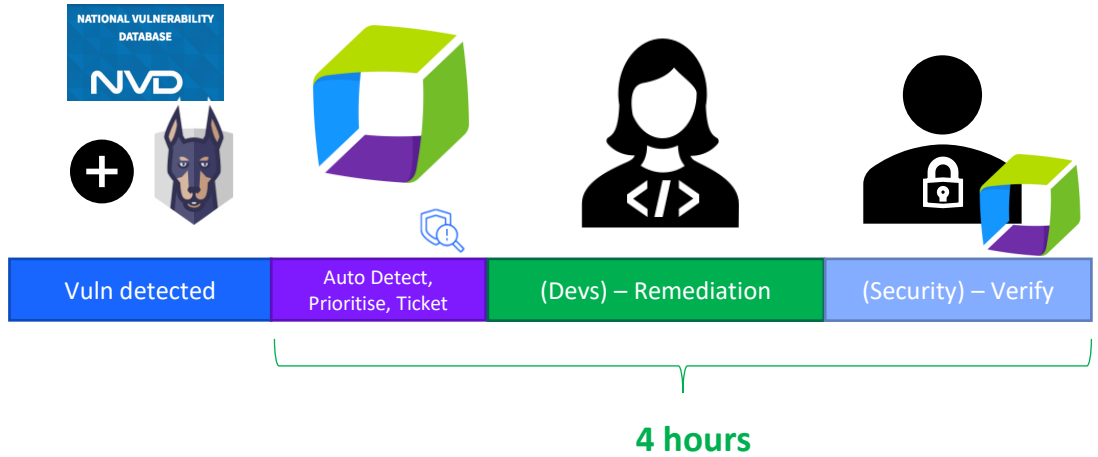
dynatrace

Application Security Runtime Vulnerability 분석

Before AppSec



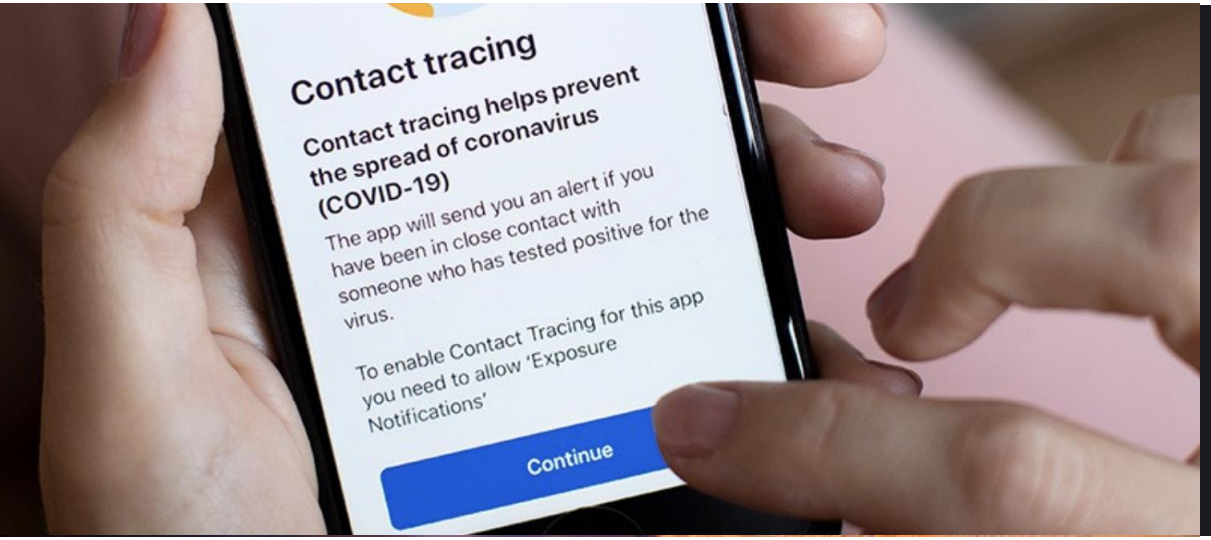
After AppSec



취약점 위험 해결 시간 95% 단축

"Dynatrace의 AppSec 솔루션을 통해 중요한 취약성 문제 해결 시간을 96시간에서 4시간으로 개선했습니다."

고객 사례: 3rd party application 보안 관리



"우리는 긴급 상황 발생 시 새로운 클라우드 애플리케이션을 즉각적으로 구축해야 하는 상황에 직면했습니다. 성능과 보안은 모두 매우 중요했습니다. 앱에는 PII가 로드되어 있었고 데이터 침해는 치명적일 수 있습니다. Dynatrace는 클라우드 앱의 보안을 보장하는 데 도움이 되는 유일한 솔루션이었습니다."

상황

- 정부 기관 - 3rd Party 업체에서 개발한 앱을 구매.
- 앱은 시민들에게 코로나19 안전에 대한 공지 및 접촉 추적 기능을 제공합니다.
- 민감한' 개인정보가 앱에 저장되었음.

문제점

- 이 앱은 3rd party 업체가 개발했기 때문에 소스 코드가 없음.
- Vulnerability를 평가할 능력이 없었음.

Dynatrace 효과

- Dynatrace는 정적 소스 코드가 아닌 런타임 애플리케이션을 모니터링.
- 앱에서 거의 100개의 취약점을 발견.

고객 사례 : 실시간 감지 및 분석

"보안 코드 스캔이 운영환경에 미치는 영향으로 인해 Vulnerability 스캐너는 일주일에 한 번만 실행됩니다. 즉, 새 버전의 소프트웨어를 출시하면 다음 주까지 보안 문제에 대해 알 수 없으며, 이는 사각지대이며 심각한 위험입니다! Dynatrace의 실시간 가시성은 이러한 사각지대를 제거하고 클라우드 기반 애플리케이션의 보안에 대한 더 큰 확신을 줍니다."

상황

- 대형 은행 – 모바일 앱 제공.

문제점

- 운영환경에서 VA 스캐너는 매주 실행됨.
- 6일간의 사각지대가 발생하며 심각한 위험 요소임.

Dynatrace 효과

- Dynatrace는 실시간 결과를 제공.
- 이전에 알려지지 않았던 운영 환경의 60여개 취약점을 감지.

고객 사례 : 더욱 향상된 정확성과 자동화된 우선순위 지정으로 시간 절약

"우리는 최근 소프트웨어 구성 분석(SCA) 툴을 최신 버전으로 업그레이드했지만 실제로는 문제를 더욱 악화시켰습니다. 우리는 감지 목록에 있는 모든 취약점을 해결할 수 없었고 어디서부터 시작해야 할지 몰랐습니다. Dynatrace는 어떤 취약점이 진짜인지, 어떤 취약점을 먼저 해결해야 하는지 자동으로 분석하여 제공함으로써 우리의 삶을 크게 개선했습니다."

상황

- 중견 보험 Agency 기업
- 기존 정적 어플리케이션 보안 테스트(SAST) 및 소프트웨어 구성 분석(SCA) 툴이 제공하는 많은 취약점을 모두 해결하기에는 절대적 시간이 부족함.

문제점

- 어떤 취약점이 실제로 중요한지 확인하는 데 매우 많은 시간이 소요됨.
- 애플리케이션 보안 테스트의 단편적인 정보로는 전반적인 비즈니스 위험을 평가하기가 어려움.

Dynatrace 효과

- Dynatrace 런타임 분석에 의해 취약점의 거의 절반이 오탐(false positive)인 것으로 나타났음.
- Davis Security Advisor는 모든 취약점을 분석하여 어떤 라이브러리를 먼저 교정할지 권장함.

Demo

deep dive

ASK & Next Steps

Use Case Workshop

주요 활용 사례 소개 및 공유

- increase service quality by continuously improving reliability and stability
- Represent monitoring information in multidimensional, simplified and customized dashboards
- apply predictive analytics to enable automated actions for incident handling and prevention
- improve root cause analysis and incident resolution time by correlating all components
- centrally consolidate all monitoring information and connect to the CMDB

PoC Review

PoC를 통한 검증

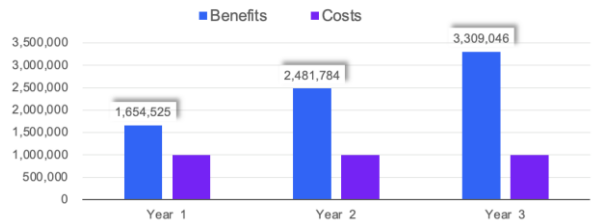
ROI 협의

Dynatrace 적용방안 및 ROI 협의

Potential Impact
(Benefits over the next three years)

$7.4M Total Benefits	148% 3 Year ROI
$827.3K Cost of Delay (3 Months)	7 Months Payback Period

Benefit vs. Cost



korea.info@dynatrace.com

CLOUD DONE RIGHT