Alert Logic

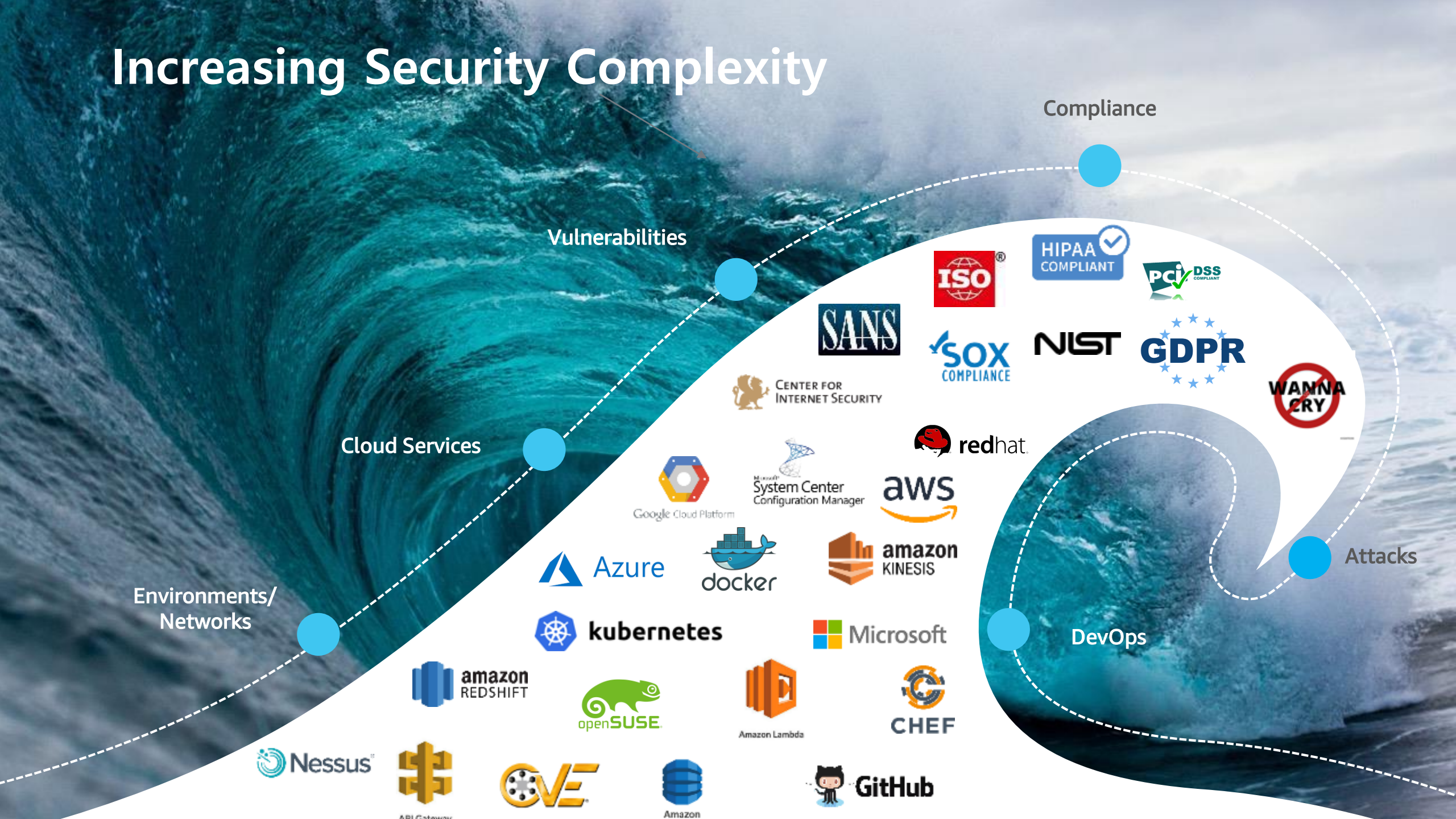
A NEW APPROACH TO THREAT MANAGEMENT

보안기술본부

2019.03.22

openbase

Increasing Security Complexity



The Risks Are Real. Are You Ready?

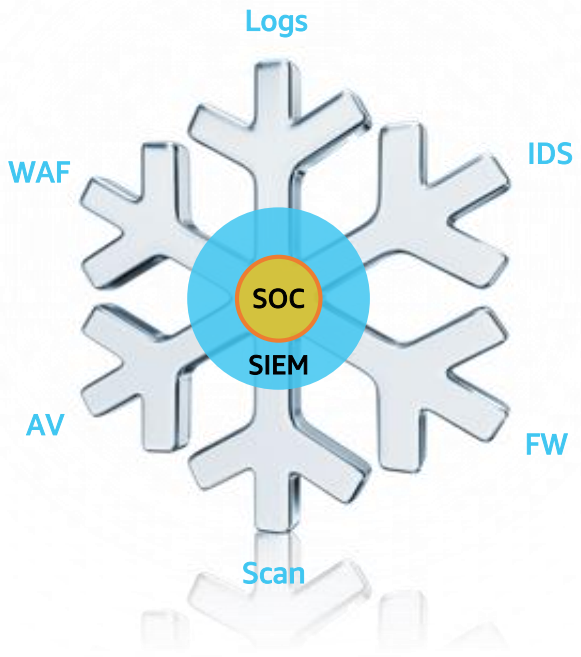
openbase

보안은 끝없는 싸움입니다.

- 시스템 패치
- 유지 보수
- 제로데이 업데이트
- 보안 교육
- 모범 사례 준수

Previous Approaches Are Costly and Ineffective

openbase



보안 모델 직접 구축

- 주관적인 솔루션 선택
- 다양한 보안 시스템 통합 부담
- 제한적 가시성
- 전문 인력 확보 어려움
- 큰 유지 보수 부하

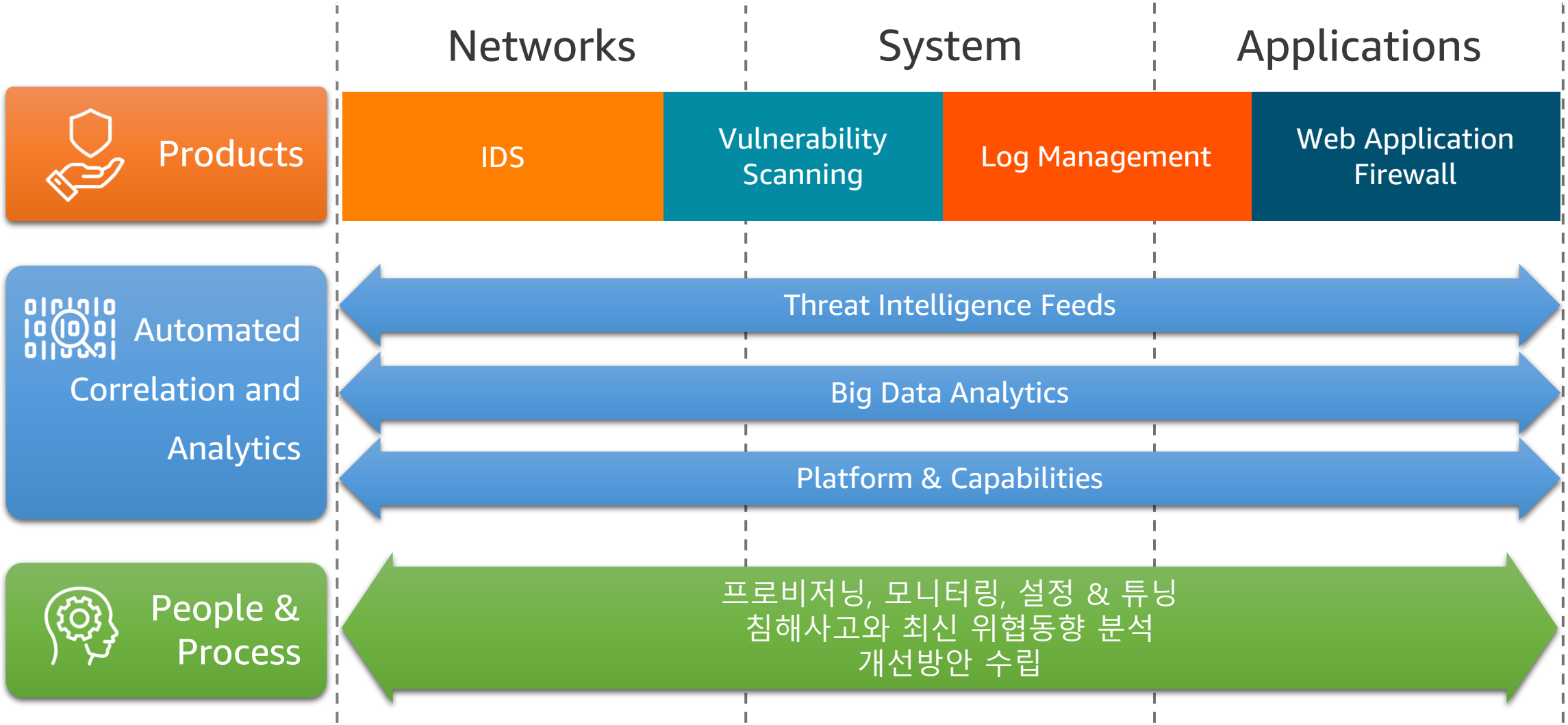
기존 보안 아웃소싱

- 고비용
- 검증된 incident가 아닌 다량의 Alert
- 중급 규모 고객에겐 B team 정도의 수준
- 통합 관리 시스템을 관리하는 부하 가중


New Approach
TO THREAT MANAGEMENT
openbase

Alert Logic - Full Stack, SIEMless Security

openbase

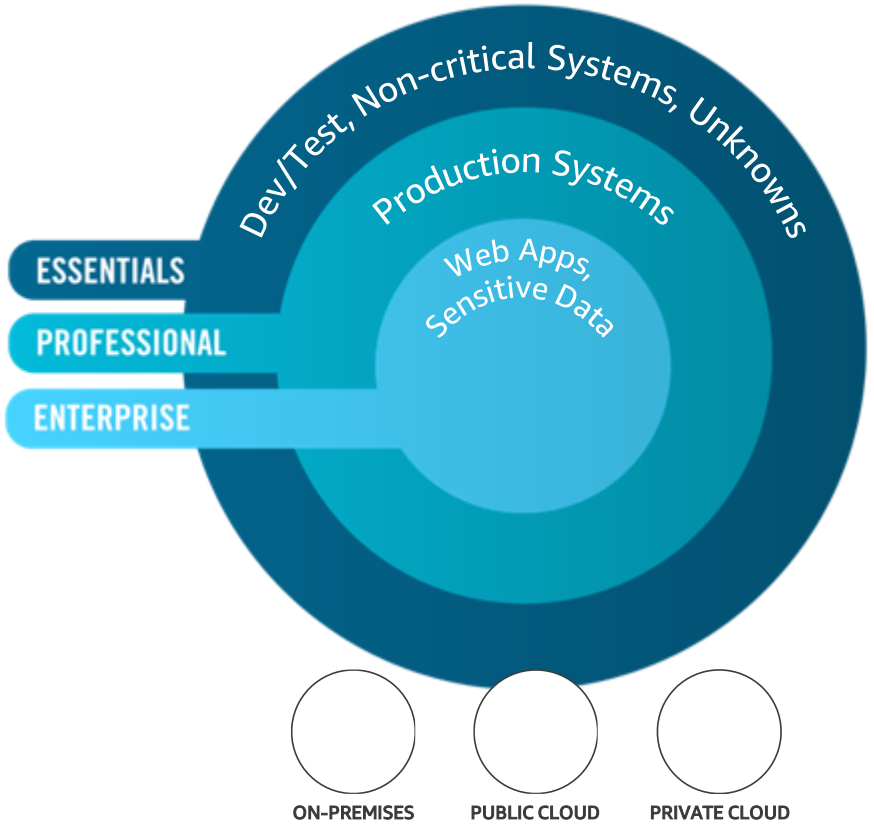


Introducing Alert Logic

openbase

Alert Logic의 SIEMless 보안서비스는,
준비된 보안 플랫폼,
최첨단 위협정보,
보안 전문가가 결합하여
최고의 보안/컴플라이언스를
24시간 경제적인 비용으로 지원하는
서비스입니다.

- 클라우드, 온프라미스, 네트워크에서 어플리케이션까지 고객 환경의 전 영역 커버
- 신속한 침해 대응
- 용이한 확장
- 짧은 구축 기간
- 고객 환경에 맞춘 유연한 구성 / 비용 효율 향상



Across Any Environment

Better Way : SIEMLess Threat Management

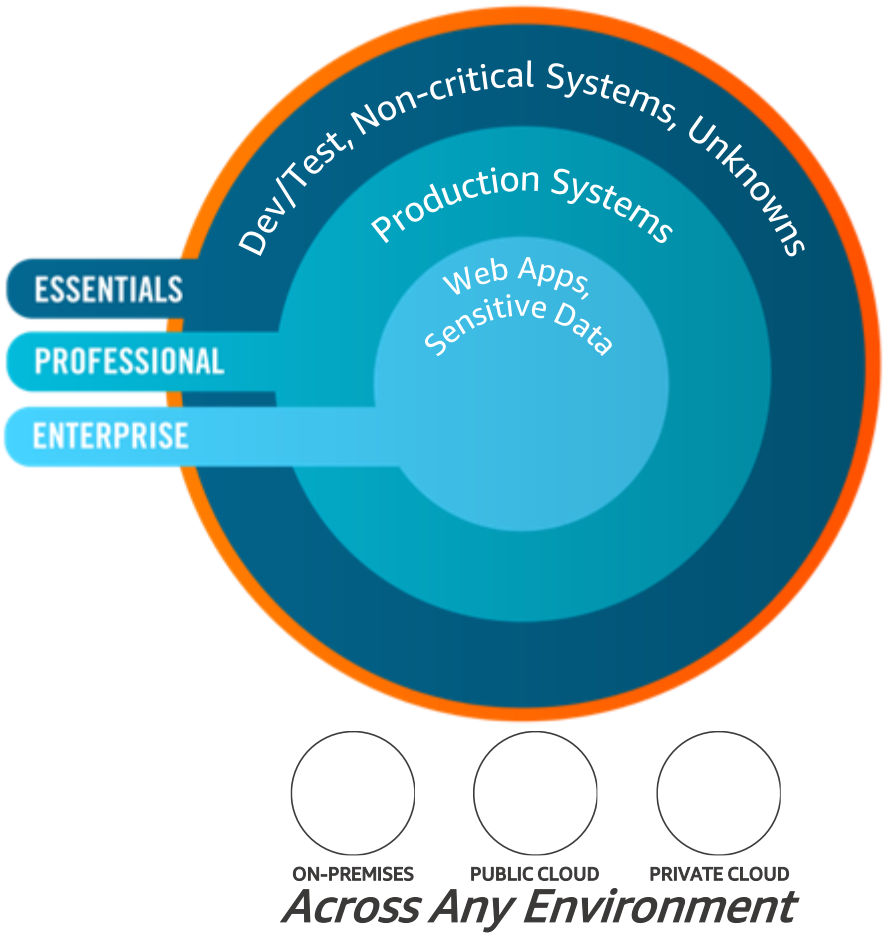
openbase

Alert Logic 서비스

Platform	Intelligence	Experts
• 자산 검색 • 취약점 스캔 • 클라우드 설정 체크 • 컴플라이언스	• 위협 목록 • 조치방안 가이드 • 우선순위 및 후속작업 • 광범위한 취약점 라이브러리	• 24/7 이메일/전화 지원 • PCI 스캔 & ASV 지원 • 서비스 모니터링
• 위협 모니터링과 시각화 • 침입 탐지 • 보안 분석 • 로그 수집 및 모니터링 • 고급 로그 검색 기반 분석	• 이벤트 인사이트 및 분석 • 위협의 발생빈도,위험도, 상태 정보 • 공격 예방	**ActiveWatch Professional** • 24/7 SOC : 사고 관리, 에스컬레이션, 대응 지원
• Always-on WAF 웹 공격 방어 (OWASP Top 10, 최신 위협, 제로데이 취약점) • SQL Injection, DoS, URL 변조, CSS 등 공격 방어	• 210만개 이상 웹 어플리케이션 공격에 대해 검증 • 악의적 행위를 판별/차단하기 위한 고도화된 탐지 기술	**ActiveWatch Enterprise** • 보안 상태 리뷰 • 사고대응 지원 • Threat hunting • 튜닝, 정책 커스터마이징, 모범사례 지원

SIEMless by Design | Lower Total Cost | Always Advancing

고객 환경 최적화 보안 서비스



Coverage of attack surface

openbase

Defend Every Layer of Environments

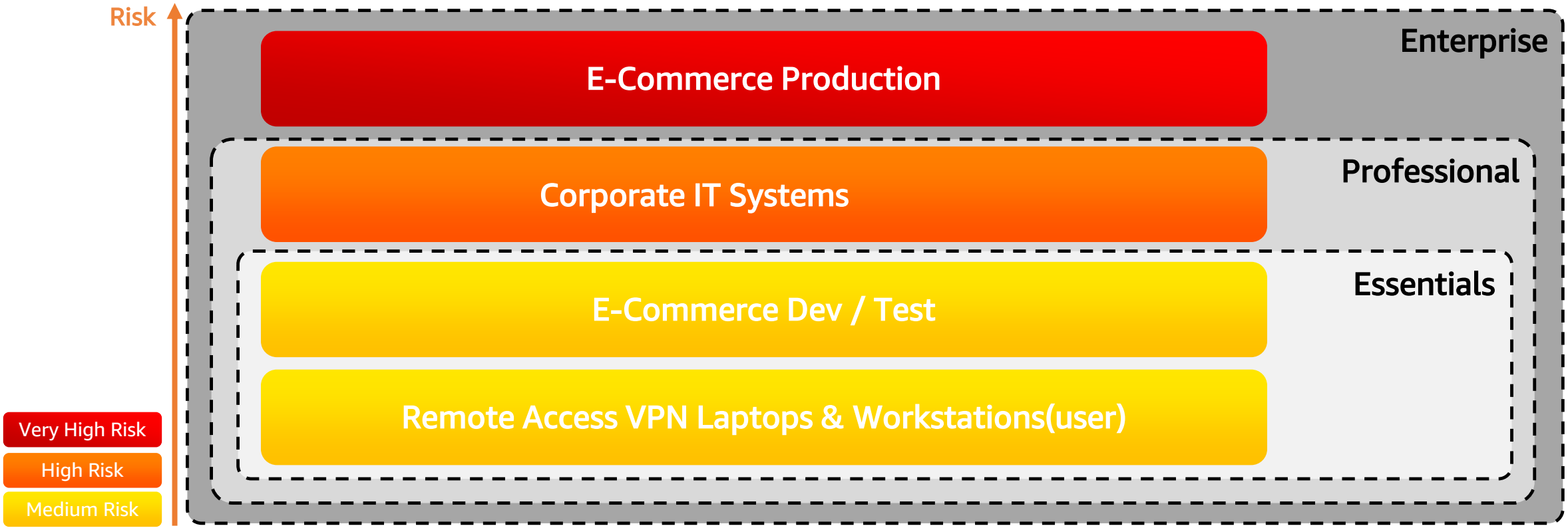
- 최신 공격과 오래된 공격 모두 커버
- 높은 정확도
- 맥락에 기반한 대응

- Web Application Firewall
- HTTP anomaly detection
- Machine learning algorithms for SQL injection
- Signatures for riskiest web plug-ins, servlets & libraries

- Provide compliance reports
- Scan for misconfigurations

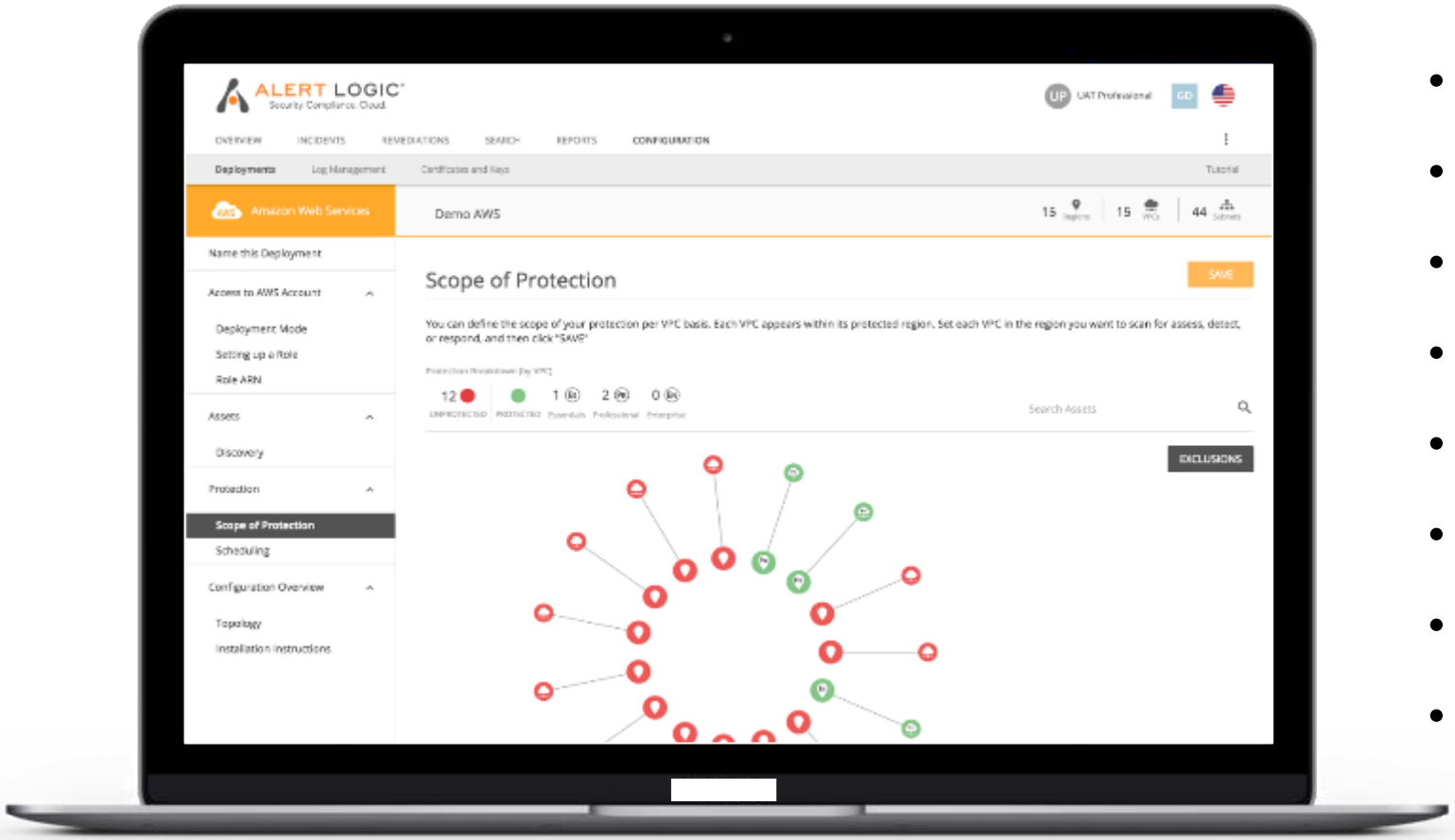
- Scan for asset-level vulnerabilities
- Collect log & network data
- Identify lateral movement, brute force, privilege escalation, command and control…

Coverage Applied



Modern and Always Advancing

openbase



- SaaS(Software as a Service) based
- One Agent(plus we manage it)
- Modern UX
- AWS, Azure, Google Cloud
- On-premises
- Hosting and Co-Lo
- Virtual machines
- Containers

Flexible Pricing

openbase

Get the Right Mix of Coverage for Your Environments

At the Optimal Cost

4,000+ Customers and Industry Observers Agree

openbase

*"We **would have needed multiple vendors** to be ab le to do what we are doing with just Alert Logic."*

– Lee Ramsey, Co-Founder

Pre-Fi

*"**Alert logic frees up company resources**, so we don't have to dedicate people to security."*

– Ian Beatty, Director Infrastructure and Information Security

CHESS

Real Evidence. Real Recovery.

FORRESTER®

"Alert Logic sets itself apart by expediting client deployment s on any infrastructure. Alert Logic offers one of the most co mprehensive deployments of supervised machine learning a mong all MSSPs, with SOC analysts continually refining rules ets and detection algorithms."

Forrester Wave™: Global Managed Security Services Providers, Q3 2018

Gartner®

- "Alert Logic is especially strong in public cloud and virtualized envir onments where the solution can be deployed quickly and enabled b y prebuilt integrations via Chef/Puppet/Ansible.
- **Customers value Alert Logic's ease of use.**
- Alert Logic is one of the first vendors to use analytics and machine l earning to postprocess IDS event streams."

CYBER SECURITY EXCELLENCE AWARDS WINNER 2018

the techies 2018 Best Security Technology of the Year WINNER

Info Security Products Guide 2017 GLOBAL EXCELLENCE GOLD

TOP 100 MSSPs

NETWORK PRODUCTS GUIDE IT World Awards 2017 GOLD

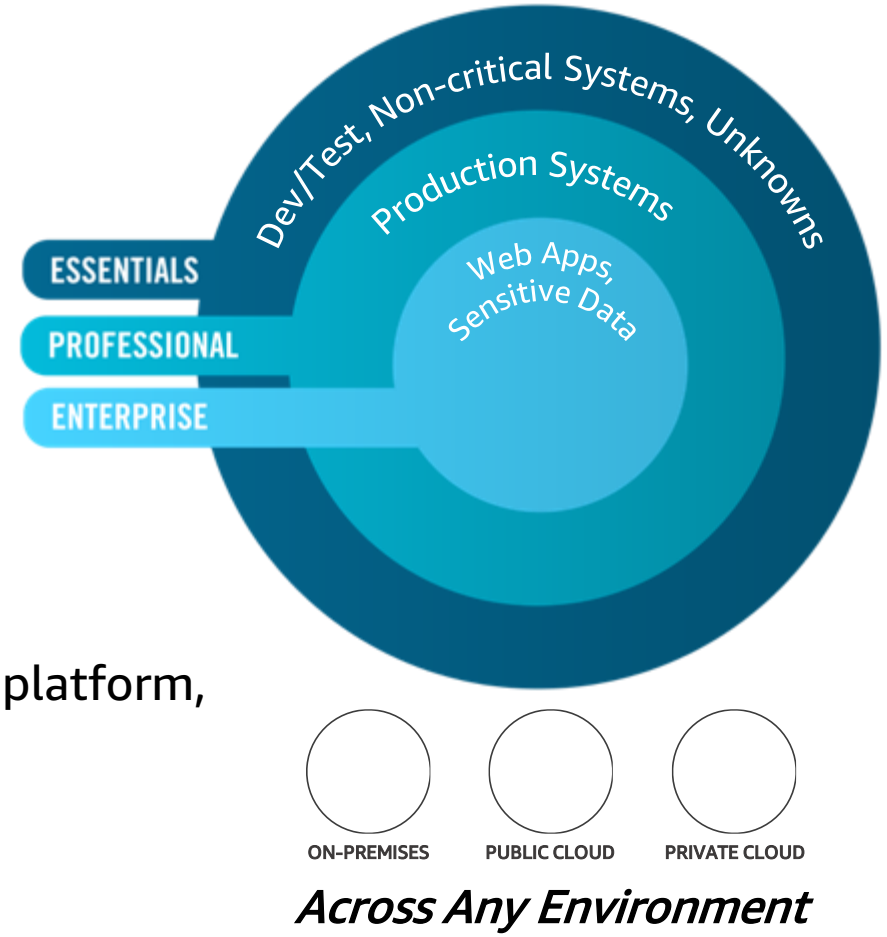
Alert Logic has received more than 60 awards

Summary

openbase

- 기업의 중요 자산 보안은 필수
- 기존 방식의 보안은 비효율적이고 비용이 많이 듦
- AlertLogic 보안서비스로 플랫폼, 기술, 보안 전문가를 경제적인 비용으로 활용 가능
- Your enterprise needs protection
- A DIY approach is expensive and challenging
- Alert Logic provides a way forward with the right mix of platform, technology and experts for a lower total cost

When can we start?




감사합니다.
openbase