


Alert Logic

A NEW APPROACH TO THREAT MANAGEMENT

보안기술본부

openbase 

Complexity Increasing



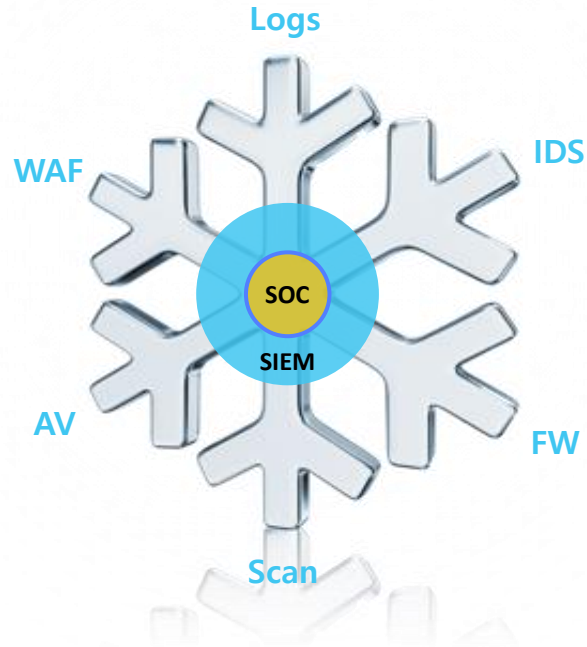
The Risks Are Real

보안은 끝없는 싸움입니다.

- 시스템 패치
- 유지 보수
- 0-day 업데이트
- 보안 교육
- 모범 사례 준수

... 이제 충분히 안전하다고 **확신**할 수 있을까요?





보안 모델 직접 구축

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

"고비용 저효율"



기존 보안 아웃소싱

- 고비용
- 검증된 Incident가 아닌 다량의 Alert
- 중급 규모 고객에겐 B team 정도의 기술 지원
- 통합시스템을 관리하는 부하 가중

New Approach

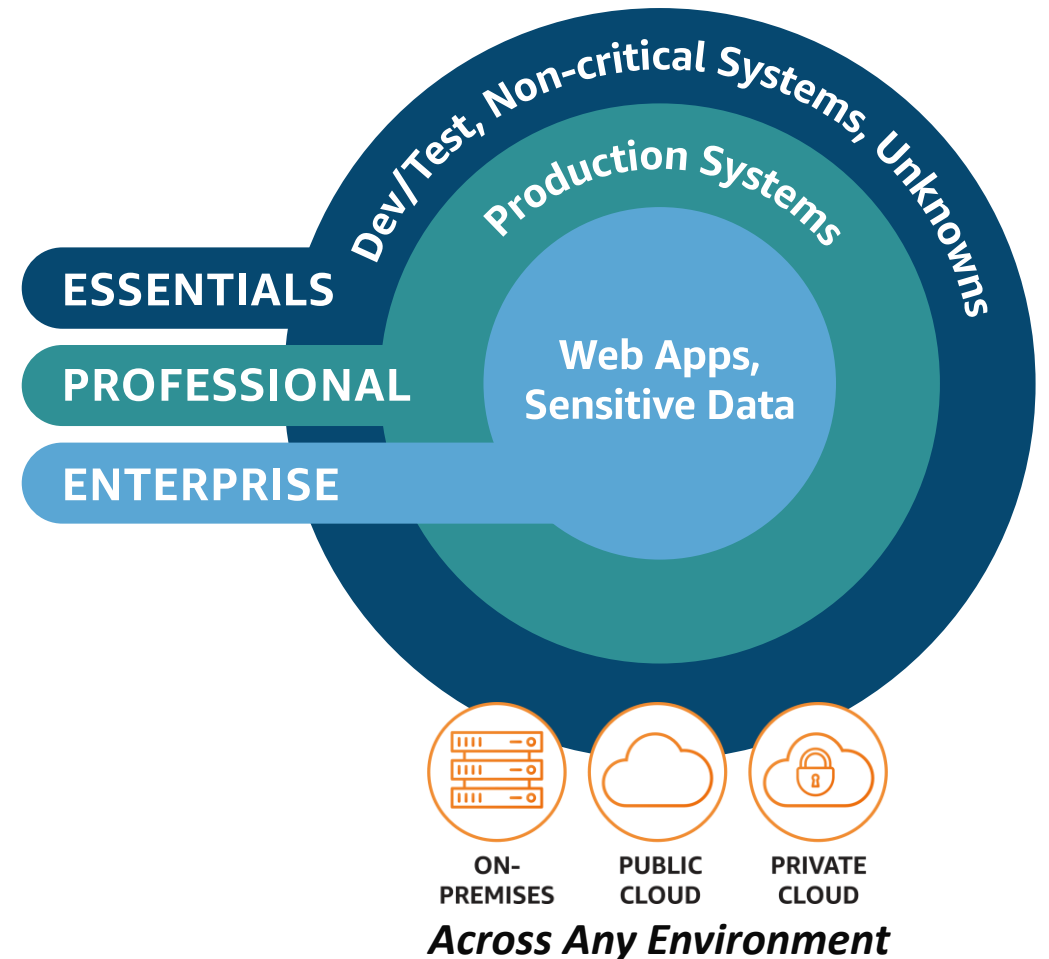
TO THREAT MANAGEMENT

openbase 

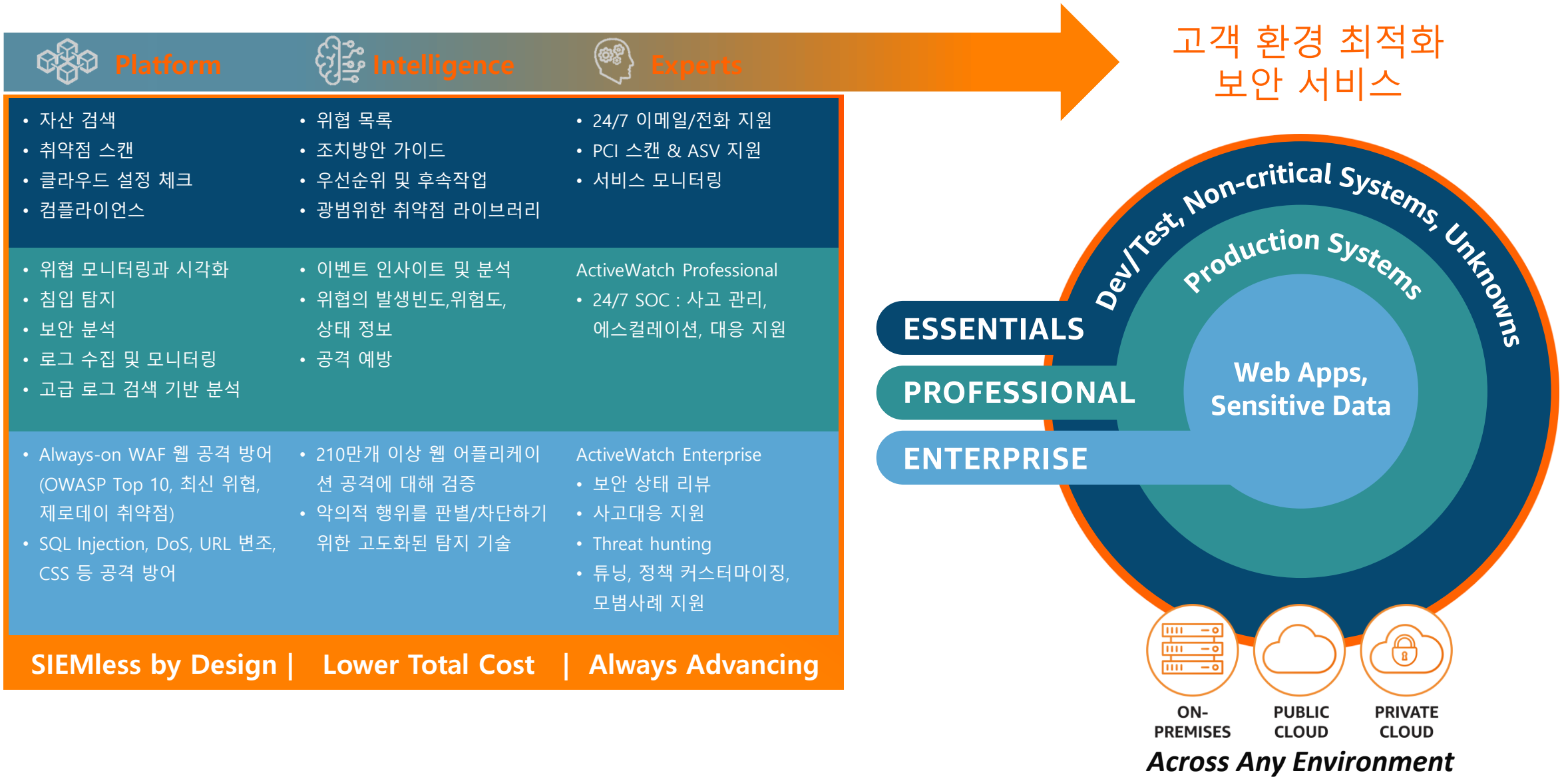
Alert Logic is

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

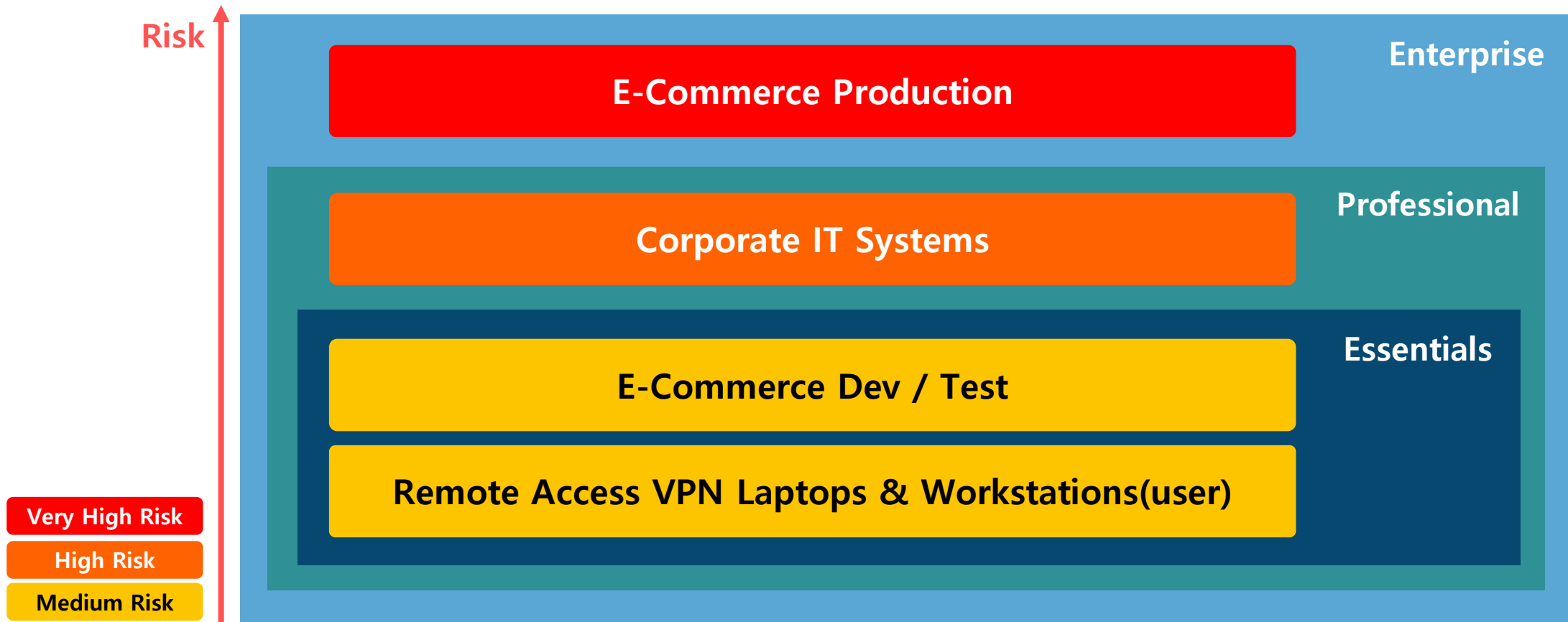
- 클라우드, 온프레미스, 네트워크에서 어플리케이션까지 고객 환경의 전 영역 커버
- 신속한 침해 대응
- 용이한 확장
- 짧은 구축 기간
- 고객 환경에 맞춘 유연한 구성 / 비용 효율 향상



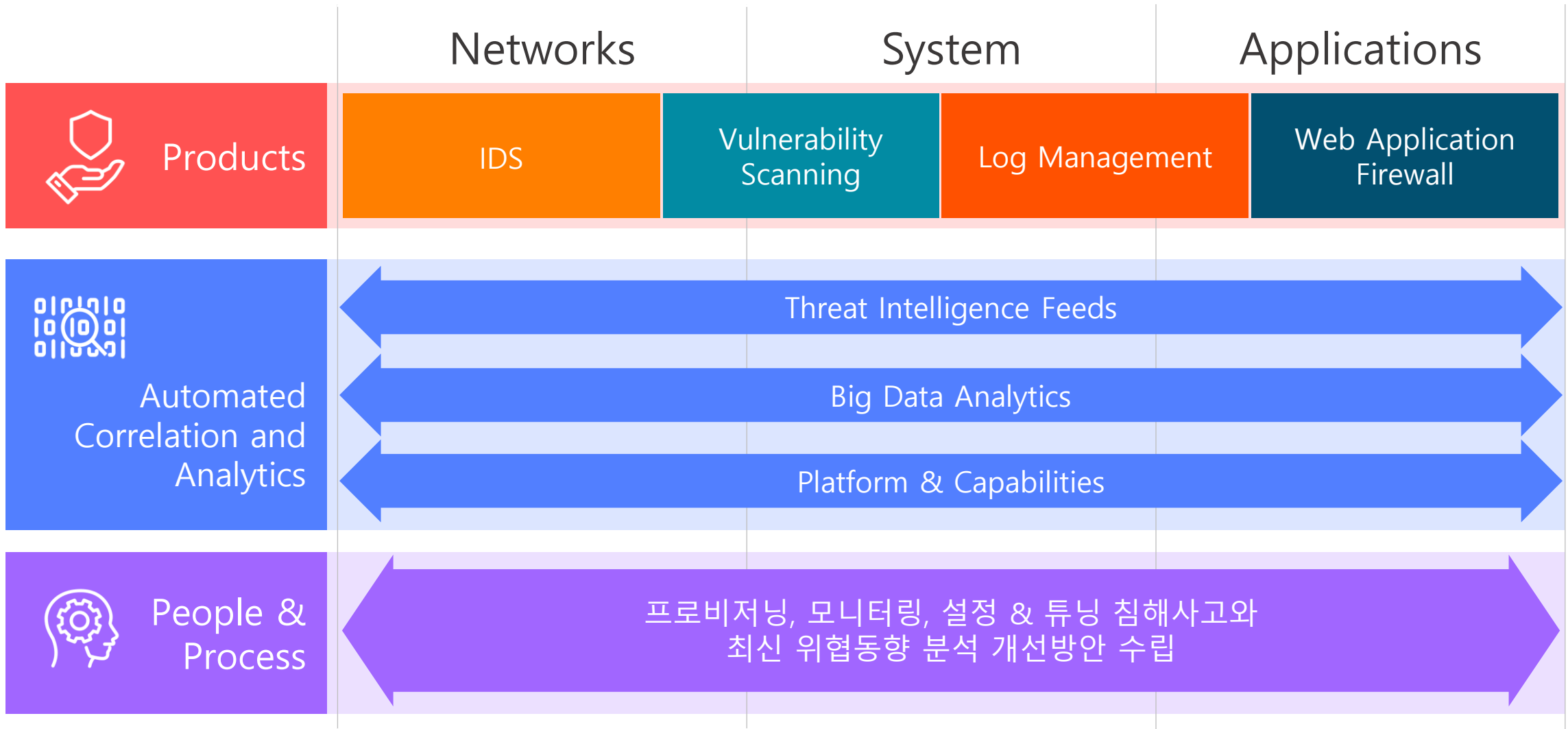
Alert Logic Services



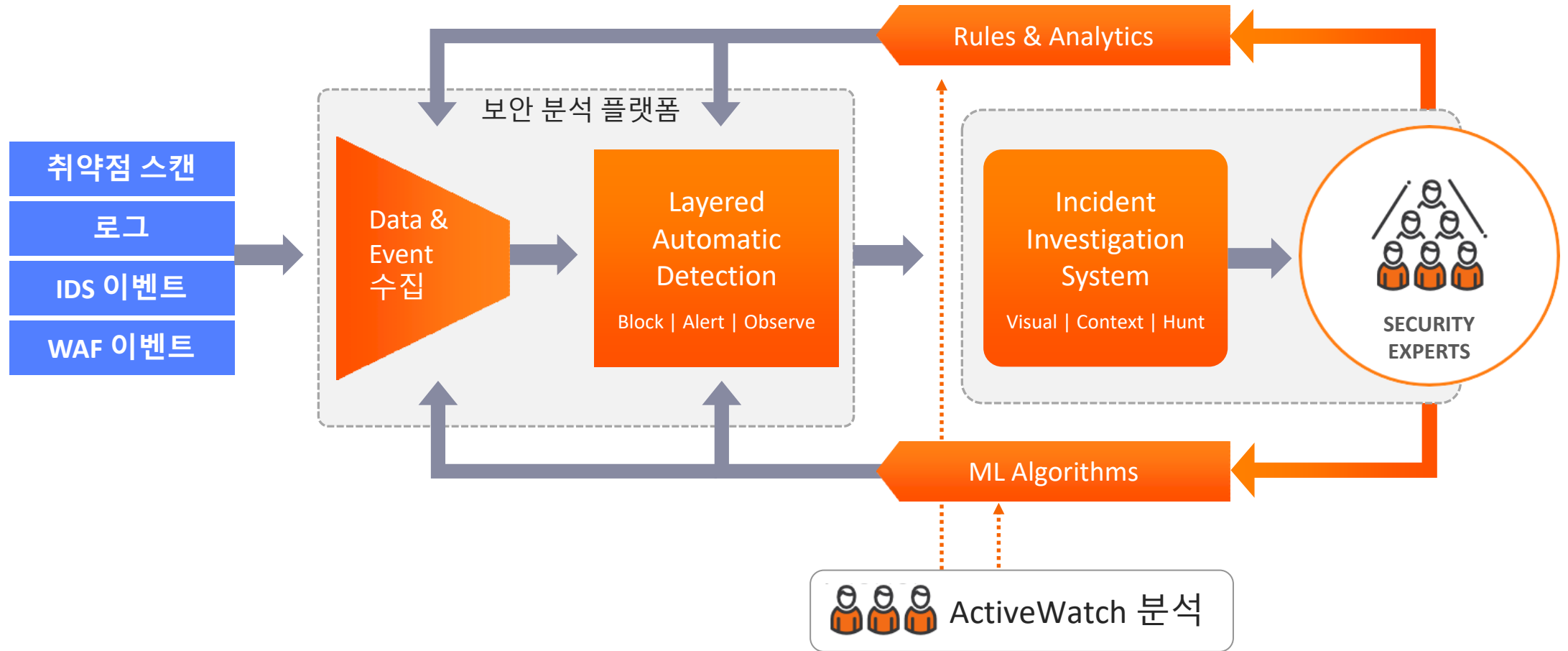
Service Layer



SIEMless Security - Full Stack



Integrated Security Model



Coverage of attack

- 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



Packaged App	ORACLE	SAP	SharePoint				
App Framework	Joomla!	Magento	WordPress	Drupal	dj	CakePHP	spring
Dev Platform	java	Microsoft .NET	php	JS	RAILS		
Database	ORACLE	MySQL	PostgreSQL	SQL Server			
Middleware	APACHE	JBoss	Apache Tomcat	Exchange			

- Provide compliance reports
- Scan for misconfigurations

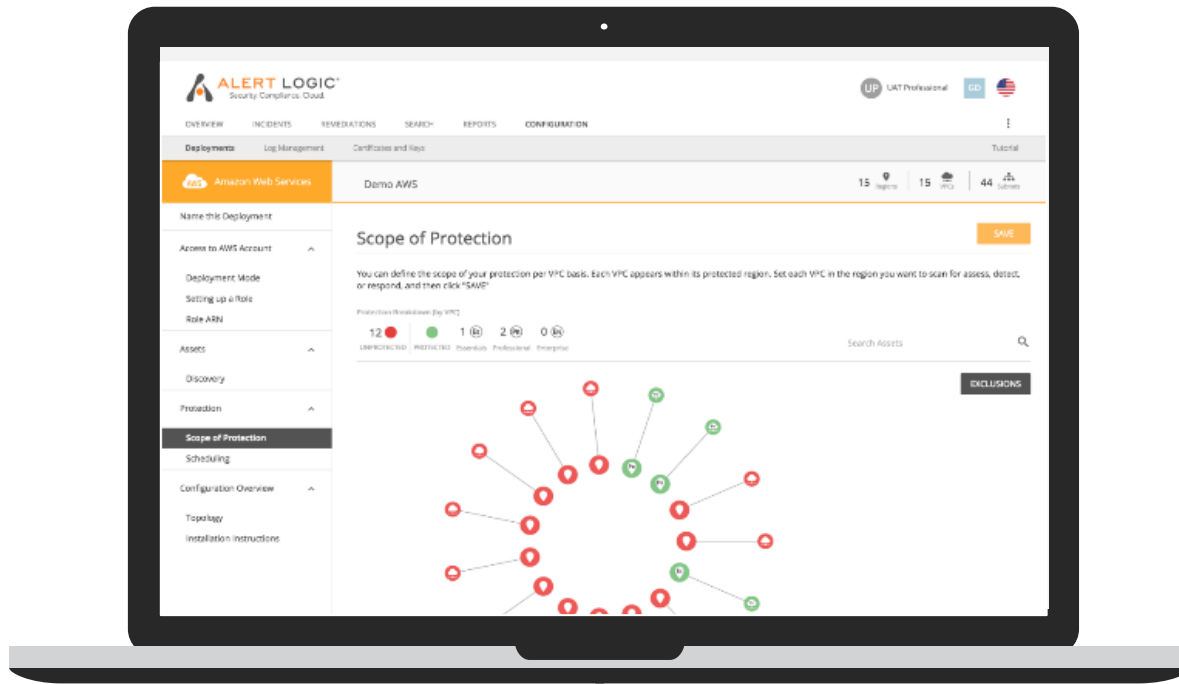


Server OS	redhat	SUSE	ubuntu	Windows Server 2016		
Orchestration	OpenStack	Kubernetes	Docker			
Hypervisor	Xen	Microsoft Hyper-V	vmware			
Network	IPv4	FTP	SSH	SMTP	CISCO	Juniper



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

Modern and Advancing



- SaaS (Software as a Service) based
- One Agent (plus we manage it)
- Modern UX
- Public/Private Cloud
- On-premises
- Hosting and Co-Location
- Virtual machines
- Containers

Flexible Pricing

The image displays three pricing cards for Alert Logic services, arranged from left to right. Each card has a distinct color: dark blue for Essentials, medium blue for Professional, and light blue for Enterprise. Each card features a logo in a white square (Es, Pr, En), the product name, a description of features, and pricing details. A dashed horizontal line separates the feature descriptions from the pricing information.

Product	Starting Price (Monthly)	Nodes	Term
Alert Logic Essentials	₩630,000	Up to 256	3-year
Alert Logic Professional	₩2,720,000	Up to 25	3-year
Alert Logic Enterprise	₩4,900,000 (with WAF option) / ₩5,100,000 (with ActiveWatch Enterprise)	Up to 25	3-year

Get the Right Mix of Coverage
for Your Environments

At the Optimal Cost

4,000+ Customers and Industry Agree



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

– Lee Ramsey, Co-Founder



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

– Ian Beatty, Director Infrastructure and Information Security



FORRESTER®

*"Alert Logic sets itself apart by **expediting client deployments on any infrastructure**. Alert Logic offers one of the most comprehensive deployments of supervised machine learning among all MSSPs, with SOC analysts continually refining rulesets and detection algorithms."*

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

Gartner®

- "Alert Logic is especially strong in public cloud and virtualized environments where the solution can be deployed quickly and enabled by 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 learning to postprocess IDS event streams."

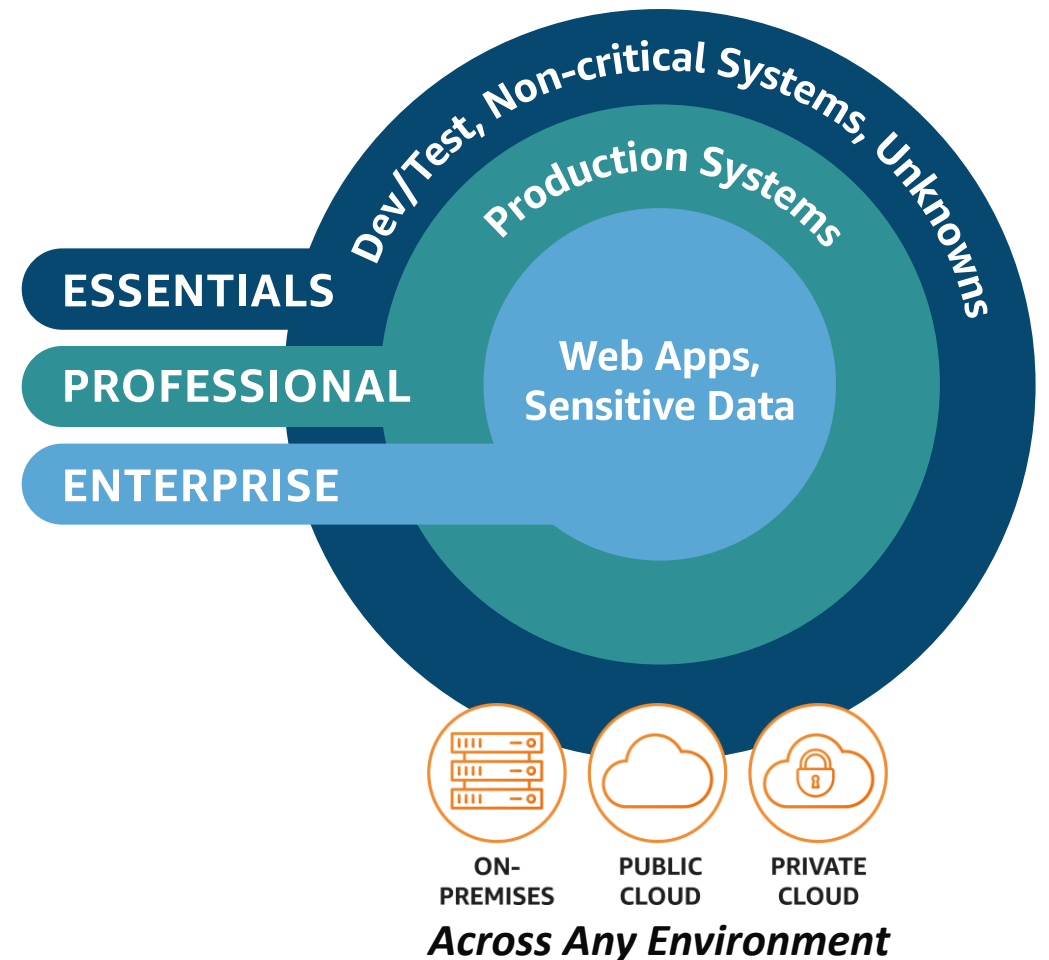


Alert Logic has received more than 60 awards

Summary



- 기업의 중요 자산 보안은 필수
- 기존 방식의 보안은 비효율적이고 비용이 많이 듦
- AlertLogic 보안서비스로
플랫폼, 기술, 보안 전문가를 경제적인 비용으로
활용 가능



WannaCry Threat Management in Action

1. THREAT INTEL

- WannaCry 발생
- 시그니처 개발

2. SECURITY PLATFORM

- WannaCry 탐지 & 고객에게 경고

3. EXPERT DEFENDERS

- 데이터 분석과 Learning자료, 보안 전문지식 결합하여 위협 분석

4. THREAT INTEL

- 변화하는 WannaCry 지속적으로 분석

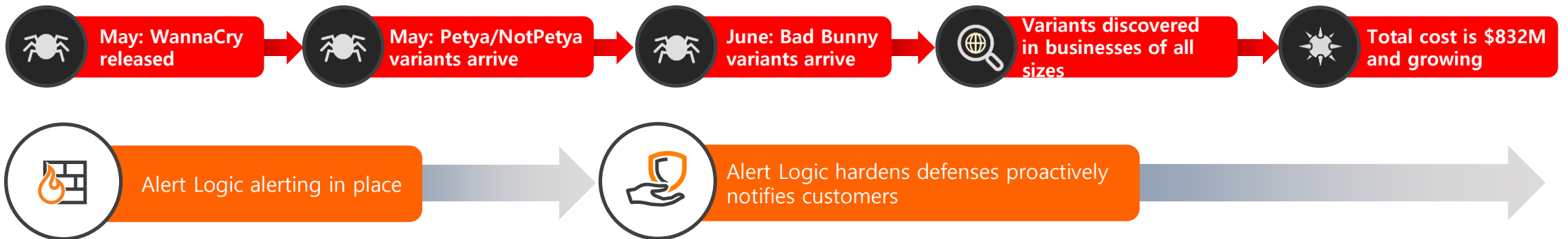
5. SECURITY PLATFORM

- 변화하는 위협에 대응하기 위한 엔진 업데이트

6. THREAT INTEL

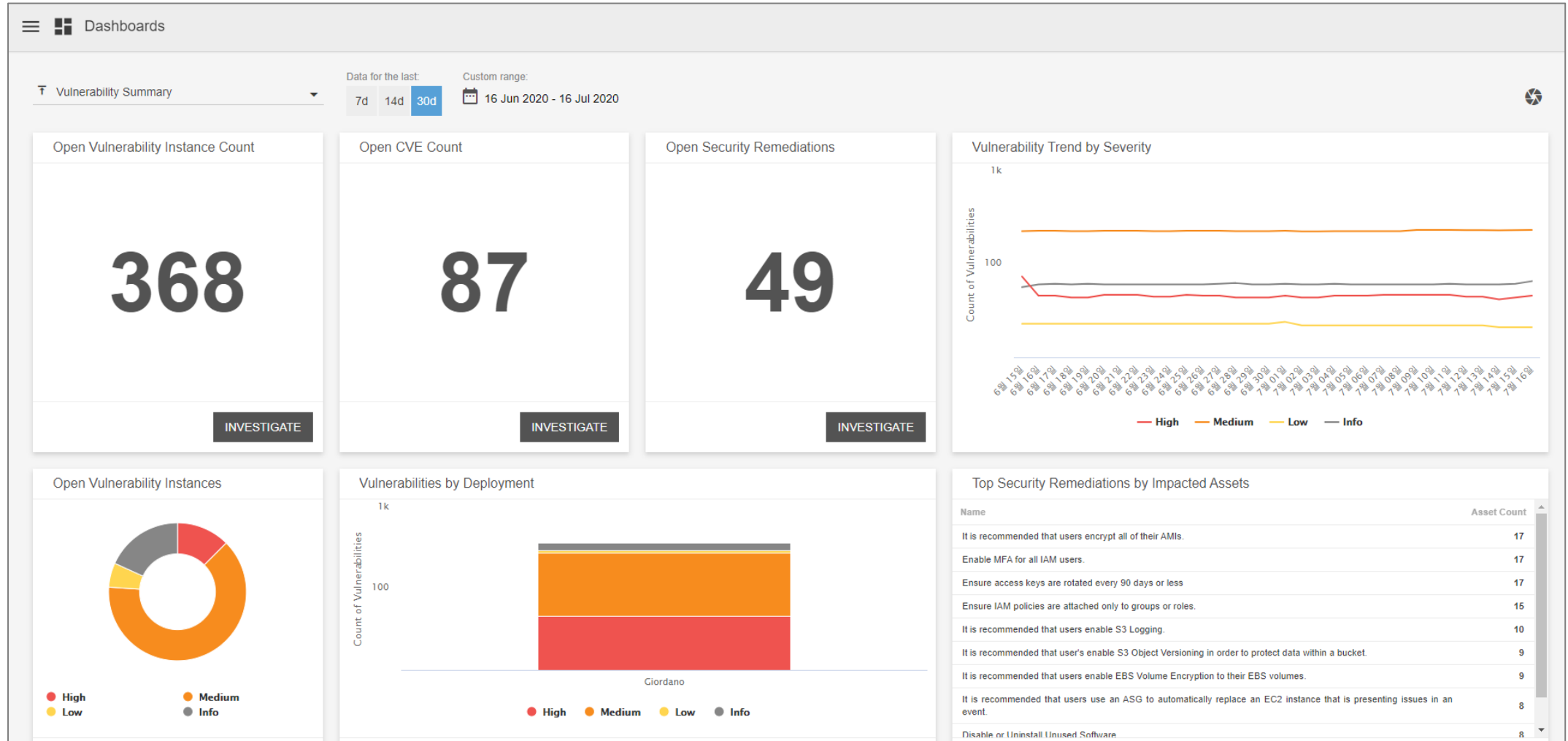
- 새로운 위협마다 고객에게 업데이트 제공

Alert Logic customers protected every step of the way



Alert Logic 주요 화면

Dashboard



Dashboard

The screenshot displays the Alert Logic dashboard for a deployment named "SE Demo - 378762935152". The interface includes a navigation menu on the left with options like "Remediations & Continuous Scan", "Network IDS", "Log Management", "WAF", "Web App IDS", and "Scans". The main content area shows a summary of the deployment's security status:

- Deployment:** SE Demo - 378762935152 (AWS)
- 5 VPCs**
- 28 subnets**
- 67 hosts**
- 60 scoped hosts**
- 60 scanned**
- remediate** button

Below the summary, there are two tabs: "Threat" (selected) and "Scan". The "Threat" tab shows a list of regions with associated threat counts:

- US East (N. Virginia):** 4 threats
- US West (Oregon):** 1 threat

The "Summary Statistics" section includes:

- Deployment Protected by Scope:** 94% (with an "edit" link)
- Credentials Provided to Scope:** (partially visible)

The "Custom Filter Sets" section contains a message: "You do not have any Filter Groups set up yet. You will get a chance to do this in Remediations."

주요 기능

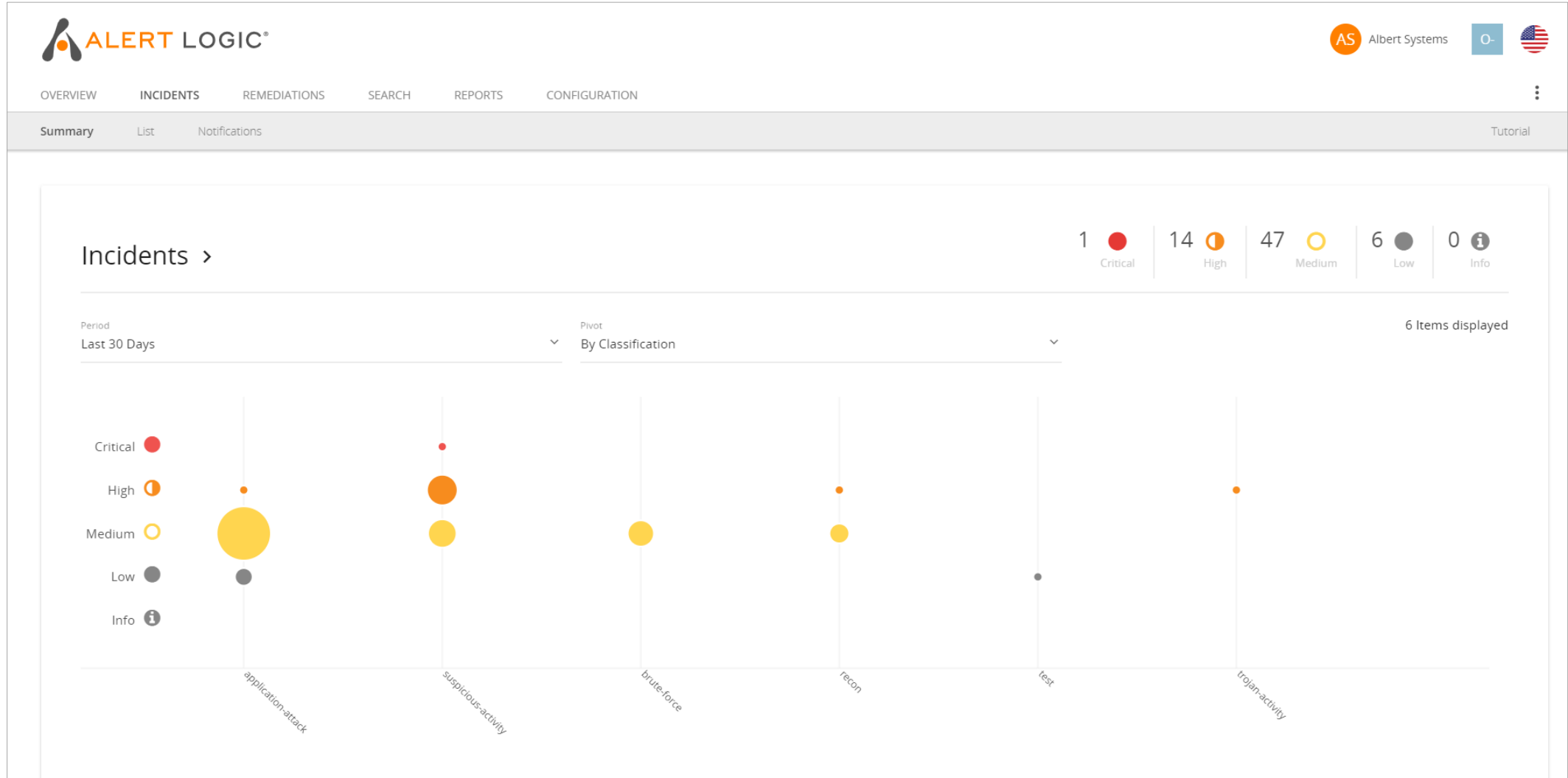
Topology

The screenshot displays the Alert Logic interface for the 'Topology' dashboard. At the top, the 'ALERT LOGIC' logo is on the left, and the user 'AS Albert Systems' is on the right. A navigation bar includes 'OVERVIEW', 'INCIDENTS', 'REMIEDIATIONS', 'SEARCH', 'REPORTS', and 'CONFIGURATION'. Below this, a sub-navigation bar shows 'Dashboards' and 'Topology'. A toolbar contains various icons for search, filters, and actions, along with a 'search asset' input field. The main area features a network diagram with a central globe icon and numerous nodes connected by lines. A right-hand panel provides details for the selected 'us-east-1' region.

Key	Type	Name	Region Endpoint	Created on	Modified on
/aws/us-east-1	Region	us-east-1	ec2.us-east-1.amazonaws.com	Sep 26, 2017 4:26:28 AM	Nov 19, 2018 6:18:59 AM

주요 기능

INCIDENTS




REMEDIATIONS

The screenshot displays the Alert Logic Remediations page for an AWS instance (SE Demo - 378762935152). The interface includes a navigation menu with options like Overview, Incidents, Remediations, Search, Reports, and Configuration. A summary bar shows exposure counts: 715 High, 1.2k Medium, 117 Low, and 174 Info. A left sidebar allows filtering by status (Open, Planned, Disposed, Completed), search filters, saved filter sets, category (Security, Configuration), region (US East, US West, EU), and virtual private cloud. The main content area, titled 'Open Remediations' (193 total), lists three remediations:

- Security**: It is recommended that users upgrade to the latest versions of PHP. This vulnerability has been fixed in the following versions:
 - PHP 5.4.40
 - PHP 5.5.24
 - PHP 5.6.852 High, 52 Medium, 0 Low, 0 Info, 104 total exposures. CVEs include CVE-2015-4599, CVE-2015-4600, CVE-2015-4602, and CVE-2015-4603.
- Security**: It is recommended that users restrict outbound access to IP addresses that are not required. 28 High, 0 Medium, 0 Low, 0 Info, 28 total exposures. Issue: Unrestricted Outbound Access on All Ports.
- Security**: It is recommended that users download and apply the following Microsoft Security Bulletins to fix this vulnerability:

주요 기능

SEARCH

AS Albert SystemsO


OVERVIEW INCIDENTS REMEDIATIONS **SEARCH** REPORTS CONFIGURATION


Log Messages **Events** Blocks Cases Deny Logs

Showing: 1 - 25 of 12,443 events Enable range greater than 1 day Range: 1 Week

Date	Name	#	Share	Source	Port	Destination	Port	Threat	Class	Appliance
<input type="checkbox"/> Nov 13 2018 01:34:03 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		61.184.247.11	47453	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 01:34:44 GMT	ET SCAN NETWORK Incoming Masscan detected [5]	1		80.82.70.118	60000	172.31.1.23	80	50	network-scan	i-076f6da3475311d38
<input type="checkbox"/> Nov 13 2018 01:46:41 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		125.65.42.187	39244	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 03:15:40 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		115.238.245.4	46773	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 03:36:06 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		118.123.15.142	59635	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 03:44:41 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		122.226.181.166	39838	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 03:49:29 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		61.184.247.3	34801	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 03:51:11 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		61.184.247.5	59289	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 04:03:37 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		61.184.247.10	53341	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98
<input type="checkbox"/> Nov 13 2018 04:29:48 GMT	AL IIS6.0 WebDAV Remote Code Execution Attempt [5]	1		203.195.213.123	27317	10.128.0.2	80	0	web-application-attack	al-tm-instance-c-technical-marketing-internal-496
<input type="checkbox"/> Nov 13 2018 04:29:48 GMT	ET WEB_SERVER Microsoft IIS Remote Code Execution (CVE-2017-7269) [5]	1		203.195.213.123	27317	10.128.0.2	80	0	attempted-user	al-tm-instance-c-technical-marketing-internal-496
<input type="checkbox"/> Nov 13 2018 04:29:56 GMT	AL WordPress WPScan Information Disclosure Attack 5 [5]	1		203.195.213.123	27460	10.128.0.2	80	0	web-application-attack	al-tm-instance-c-technical-marketing-internal-496
<input type="checkbox"/> Nov 13 2018 04:31:28 GMT	ET SCAN SSH BruteForce Tool with fake PUTTY version [5]	1		61.184.247.6	54510	10.0.0.6	22	50	network-scan	tm-azure-52-160-90-191-98

REPORTS



AS Albert Systems
0-


OVERVIEW
INCIDENTS
REMIEDIATIONS
SEARCH
REPORTS
CONFIGURATION

Threats
Vulnerabilities
Remediations
Compliance
Service
Scheduled
Usage
WAF

Vulnerability Analysis 5

Vulnerability Summary

Vulnerable Hosts Explorer

Vulnerability Distribution Explorer

AWS Exposure Assessment Trends

AWS Vulnerable Host Explorer

Vulnerability List 1

← Undo → Redo ↶ Revert 🔄 Refresh ⏸ Pause
📄 뷰-원본 🔗 Share 📄 Download 🖨 전체 화면

Next: Top 10 Lists →

Vulnerability Summary

Albert Systems
Last Updated Time: 11/19/2018 4:26:43 AM (GMT)

Date Range
Last 60 days

Customer Account
(모두)

Deployment Name
(모두)

Asset Tags
(모두)

Vulnerabilities

7,563
Total

2,074
New

7,098
Fixed

Hosts

732
Total Hosts with Vulnerabilities

Total Vulnerability Trend (Last 4 Months)

Month	Vulnerabilities
8/2018	1,999
9/2018	1,136
10/2018	5,929
11/2018	4,853

Total Host Trend (Last 4 Months)

Month	Hosts
8/2018	197
9/2018	73
10/2018	555
11/2018	690

Vulnerabilities by Age and Severity

	High (7.0-10.0)	Medium (4.0-6.9)	Low (0.1-3.9)	Informational (0.0)	Not Scored
Over 90 Days	467	1,082	153	232	7
46-90 Days	186	405	57	37	5
31-45 Days	23	41	8	22	-
0-30 Days	1,116	2,991	502	1,651	-

주요 기능


CONFIGURATION


The screenshot displays the Alert Logic configuration interface. At the top, the navigation menu includes Overview, Incidents, Remediations, Search, Reports, and Configuration. The Configuration section is further divided into Deployments, Network IDS, Log Management, WAF, Web App IDS, and Notifications. The main content area is titled 'Deployments' and features a search bar and a dropdown menu for filtering by 'Type'. A large purple card labeled 'MANUAL DEPLOYMENTS' with an 'EDIT' button is positioned at the top left. Below it, a grid of deployment cards is shown, each representing a 'Cloud Defender Support Deployment' on various cloud platforms (AWS and Microsoft Azure). Each card includes the deployment name, date, and a unique identifier, along with 'DELETE' and 'EDIT' action buttons.

Platform	Deployment Name	Date	Identifier	Actions
AMAZON WEB SERVICES	Cloud Defender Support Deployment	May 3, 2017	Defender Support Environment for AWS 309018995558	DELETE EDIT
AMAZON WEB SERVICES	Cloud Defender Support Deployment	May 3, 2017	Test/Dev AWS 292196082538	DELETE EDIT
AMAZON WEB SERVICES	Cloud Defender Support Deployment	Jun 9, 2016	T-Vu - 612848318089	DELETE EDIT
AMAZON WEB SERVICES	Cloud Defender Support Deployment	Aug 24, 2018	SE Sandbox - 982509483243	DELETE EDIT
AMAZON WEB SERVICES	Cloud Defender Support Deployment	Apr 13, 2017	Defender Support Environment for AWS 697148468905	DELETE EDIT
AMAZON WEB SERVICES	Cloud Defender Support Deployment	Aug 2, 2016	SE Demo - 378762935152	DELETE EDIT
AMAZON WEB SERVICES	Cloud Insight	Jul 13, 2017	SE Demo - 378762935152	DELETE EDIT
MICROSOFT AZURE	Cloud Defender	Aug 26, 2017	RBAC for SE Demo	DELETE EDIT

Incident 탐지

Event 탐지



Openbase - Production
KY


OVERVIEW
INCIDENTS
REMIEDIATIONS
SEARCH
REPORTS
CONFIGURATION

Dashboards Topology

Remediations & Continuous Scan

Network IDS

Log Management

Web App IDS

Scans

+ Add new
Refresh

Event And Incident Trend

Top 10 Events Signature

- AL CVE-2005-1921 Webservice PHP XML-RPC Remote Code Injection
- AL TELEM OutBound Curl User-Agent Observed From Server
- ET SCAN NMAP OS Detection Probe
- ET SCAN Potential VNC Scan 5800-5820
- ET SCAN Potential VNC Scan 5900-5920
- ET WEB_SERVER ColdFusion adminapi access
- ET WEB_SERVER ColdFusion administrator access
- ET WEB_SERVER ColdFusion componentutils access
- ET WEB_SERVER ColdFusion password.properties access
- ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.

Traffic Trending

Traffic Trending MB

Top 10 Traffic Generating Devices

Device	Name	Traffic
Appliance	alertlogic-tm-ids-1-152	9.49GB
Appliance	i-08557ac1b1613babb	3.47GB
Host	desktop-01ui1vq	2.82GB
Host	i-084a129e6b4423af6	2.50GB
Host	chaehyunju-pc	750.61MB
Host	desktop-d18kaqg	675.47MB
Host	yooinki	429.85MB
Host	desktop-h4q3qoi	429.64MB


Devices Not Collecting

Device	Name
Host	coldfusion
Host	desktop-0h336gf
Host	desktop-d18kaqg
Host	desktop-1c44p95
Host	desktop-mqggtco
Host	hackazon-onprem
Host	se2_suhyunkim

26

Incident 탐지

Event 탐지

Security. Compliance. Cloud.Openbase - ProductionKY

OVERVIEW INCIDENTS REMIEDIATIONS SEARCH REPORTS THREAT LANDSCAPE CONFIGURATION

Events Blocks Log Messages Cases

1 item in Case

Event # Search Search Filters...



Longer time ranges will decrease performance.

Showing: 1 - 100 of 552 events Enable range greater than 1 day Range: 1 Week

Date	Name	#	Share	Source	Port	Destination	Port	Threat	Class	Appliance
<input type="checkbox"/> Aug 30 2018 08:15:16 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	56448	180.76.108.170	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 08:15:45 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	56480	180.76.108.170	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 08:15:54 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	56481	180.76.108.170	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 08:16:29 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	56524	180.76.108.170	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 07:51:02 GMT	INDICATOR-COMPROMISE Suspicious .pw dns query [1]	1		61.82.88.160	60069	168.126.63.1	53	50	trojan-activity	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 08:39:51 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	61436	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 08:39:52 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	61448	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 08:40:03 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	61451	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 09:43:26 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	64492	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 10:51:26 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	52405	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 10:51:49 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	52439	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 10:53:42 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	52558	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 11:23:48 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	54304	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152
<input type="checkbox"/> Aug 30 2018 12:54:53 GMT	AL TELEM OutBound Curl User-Agent Observed From Server [5]	1		61.82.88.160	59807	180.76.159.1	2	0	web-application-attack	alertlogic-tm-ids-1-152

Incident 탐지

Incident 탐지

Security. Compliance. Cloud.OI Openbase, Inc.KY

OVERVIEW **INCIDENTS** SEARCH REPORTS CONFIGURATION

Summary List Notifications Tutorial

Reports(s) (1)

Incident # Search Search Filters...

Longer time ranges will decrease performance.

Showing: 1 - 24 of 24 incidents Type: All | Events | Logs Enable range greater than 1 day Range: 2 Months

ID	Date	Customer	Summary	Events	Threat	Status	Class
<input type="checkbox"/> 627856	Sep 3 2018 08:57:17 GMT	Openbase - Production	61.82.88.244 logged adding ingress rights	4	Medium	Completed Analysis	suspicious-activity
<input type="checkbox"/> 627951	Sep 3 2018 09:03:05 GMT	Openbase - Production	61.82.88.244 logged revoking ingress rights	11	Medium	Completed Analysis	suspicious-activity
<input type="checkbox"/> 627979	Sep 3 2018 09:24:51 GMT	Openbase - Production	61.82.88.244 logged modifying an ACL entry	2	Medium	Completed Analysis	suspicious-activity
<input type="checkbox"/> 629640	Sep 4 2018 04:54:37 GMT	Openbase - Production	61.82.88.244 logged revoking egress rights	6	Medium	Completed Analysis	suspicious-activity
<input type="checkbox"/> 632427	Sep 5 2018 02:25:42 GMT	Openbase - Production	61.82.88.244 logged adding ingress rights	1	Medium	Completed Analysis	suspicious-activity
<input type="checkbox"/> 632813	Sep 5 2018 08:36:56 GMT	Openbase - Production	RCE Attempt From 61.82.88.244	4	Medium	Completed Analysis	application-attack
<input type="checkbox"/> 632816	Sep 5 2018 08:39:20 GMT	Openbase - Production	File Upload Attempt From 61.82.88.244	8	Medium	Completed Analysis	application-attack
<input type="checkbox"/> 632817	Sep 5 2018 08:46:16 GMT	Openbase - Production	Generic vulnerability scan from 61.82.88.244	652	Medium	Completed Analysis	recon
<input type="checkbox"/> 632829	Sep 5 2018 08:54:19 GMT	Openbase - Production	Metasploit obfuscated shell detected from 10.1.1.129	2	Medium	Completed Analysis	suspicious-activity
<input type="checkbox"/> 632830	Sep 5 2018 08:55:00 GMT	Openbase - Production	CVE-2014-3704 Drupal SQL Injection attempt from 61.82.88.244	2	Medium	Completed Analysis	application-attack
<input type="checkbox"/> 632832	Sep 5 2018 08:55:33 GMT	Openbase - Production	Metasploit obfuscated shell detected from 10.1.1.19	2	Medium	Completed Analysis	suspicious-activity
<input type="checkbox"/> 632833	Sep 5 2018 08:56:44 GMT	Openbase - Production	CVE-2016-3081 Apache Struts Dynamic Method Invocation from 61.82.88.244	1	Medium	Completed Analysis	application-attack
<input type="checkbox"/> 633001	Sep 5 2018 08:55:30 GMT	Openbase - Production	Windows Audit Log Cleared on 10.1.1.55	1	Medium	Completed Analysis	suspicious-activity

Incident 탐지

Incident 상세정보

ALERT LOGIC
Security. Compliance. Cloud.

Overview | **INCIDENTS** | Remediations | Search | Reports | Configuration

List | Guardduty | Tutorial

Summary: 61.82.88.244 logged adding ingress rights

Incident
Details | Add to Case

ID:	627856	Customer:	Openbase - Production
Threat Rating:	Medium	Created:	Sep 3 2018 8:57am GMT
Status:	Open Acknowledged by on Sep 3 2018 8:57am GMT	Created By:	System Generated
Sources:	LOG	Timeframe:	86400 Seconds
Proxy Involved:	No	Classification:	suspicious-activity
Tags:	Tags are keywords you can use to describe this entry so you can organize and find it		

Cases
Showing 0 of 0 cases

Date	Case ID	Summary	Status
No Cases could be found.			

Notes
Showing 1 of 1 notes

Date	User	Description
Sep 4 2018 4:54am GMT	system	Attack Detail: Attacker Location: 61.82.88.244, Korea, Republic of Target: aws.amazon.com User: uhurue

Attack Detail:
Attacker Location: 61.82.88.244, Korea, Republic of
Target: aws.amazon.com
User: uhurue

```
{ "ipProtocol": "udp", "fromPort": 161, "toPort": 162, "groups": {}, "ipRanges": { "items": [ { "cidrIp": "61.82.88.0/24" } ] }, "ipv6Ranges": {}, "prefixListIds": {} }
```

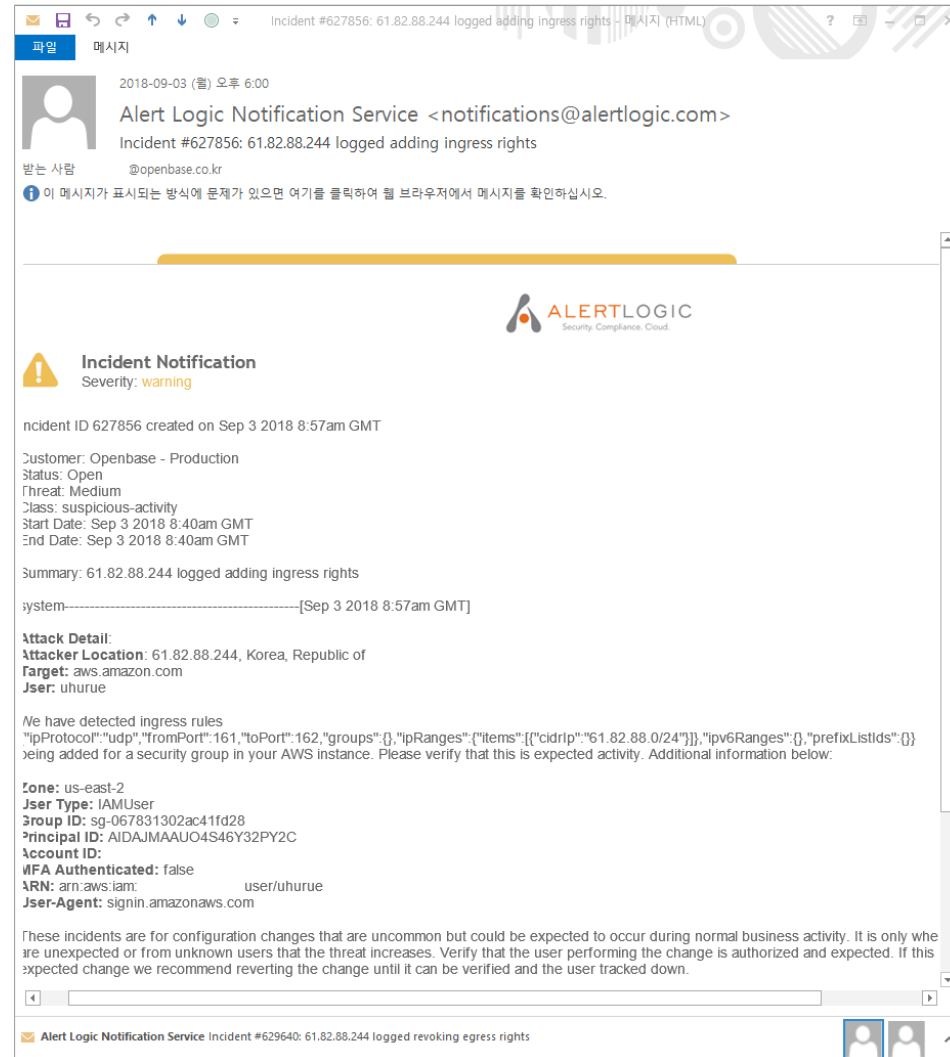
being added for a security group in your AWS instance. Please verify that this is expected activity.

Zone: us-east-2
User Type: IAMUser
Group ID: sg-067831302ac41fd28
Principal ID: AIDAJMAAU04S46Y32PY2C
Account ID:
MFA Authenticated: false
ARN: arn:aws:iam:::user/uhurue
User-Agent: signin.amazonaws.com

These incidents are for configuration changes that are uncommon but could be expected to occur during normal business activity. It is only when they are unexpected or from unknown users that the threat increases. Verify that the user performing the change is authorized and expected. If this is not an expected change we recommend reverting the change until it can be verified and the user tracked down.

Incident 탐지

Incident 알람 - 이메일



컴플라이언스 및 취약점 관리

모니터링 중인 자산 구성 및 위험도 현황

The screenshot displays the Alert Logic dashboard for an AWS deployment named "SE Demo - 378762935152". The dashboard provides a comprehensive overview of the asset composition and their security status. At the top, a navigation menu includes Overview, Incidents, Remediations, Search, Reports, and Configuration. The main content area features a summary of asset counts: 5 VPCs, 28 subnets, 63 hosts, 58 scoped hosts, and 58 scanned assets. A "remediate" button is available for actions. Below this, a table lists specific assets, such as "vpc-aad162cd", with associated metrics like 6 subnets, 26 hosts, and 23 scoped hosts scanned. The dashboard also includes a regional risk heatmap for "US East (N. Virginia)" and "US West (Oregon)", where colors indicate the severity of threats. Additional sections for "Summary Statistics" and "Custom Filter Sets" are visible at the bottom.

Asset Type	Count
VPCs	5
subnets	28
hosts	63
scoped hosts	58
scanned	58

Asset ID	Subnets	Hosts	Scoped Hosts	Scanned
vpc-aad162cd	6	26	23	23

유형별 자산 분포

영역별 위험도를 색깔로 표시

컴플라이언스 및 취약점 관리

발견된 위험 및 취약점

ALERT LOGIC
Security. Compliance. Cloud.

OVERVIEW INCIDENTS REMEDIATIONS SEARCH REPORTS CONFIGURATION

List Tutorial

AWS OpenbasePSDInsight Exposure Count

25	High	49	Medium	6	Low	8	Info
----	------	----	--------	---	-----	---	------

add to my plan

Open

- + Planned
- Disposed
- ✓ Completed

Search filters

Saved Filter Sets

Category

- Alert Logic Configuration
- Security

Region

- US East (Ohio)
- US East (N. Virginia)

Virtual Private Cloud

- vpc-07d7d513d06abf893 (vpc-07d7d513d06abf893)
- vpc-1688a77e (vpc-1688a77e)

CLEAR FILTERS SAVE FILTER SET

Remediation Steps

31

Alert Logic Configuration

It is recommended that you install Cloud Insight collectors for GuardDuty.

- Amazon GuardDuty Collector for Cloud Insight is not Installed 99

Open details

Security

Determine if privileged access is needed.

- Dangerous IAM Role for DDB 7.6
- Dangerous IAM Role for IAM 7.5
- Dangerous IAM Role for RDS 7.6
- Dangerous IAM Role for S3 7.6

+ 12 other exposures

Open details

위험도별 이슈 개수

조회 필터

컴플라이언스 및 취약점 관리

이슈 조치 - Initial Access Key

The screenshot displays a list of compliance issues for user Kim Younkyung. Each issue includes a title, a description, a score, and an 'Added to Plan' date. The third issue, 'Disable Automatic Access Key Creation', is highlighted with a blue box and a callout.

Issue Title	Description	Score	Added to Plan
Unrestricted Outbound Access on All Ports	Unrestricted Outbound Access on All Ports	10	Added to Plan on Sep 4, 2018
Unencrypted EBS Volume	It is recommended that users enable EBS Volume Encryption to their EBS volumes.	5.7	Added to Plan on Sep 4, 2018
Ensure VPC Default Security Groups Restrict All Traffic	Ensure the default security group of every VPC restricts all traffic.	6.3	Added to Plan on Sep 4, 2018
Disable Automatic Access Key Creation	Do not setup access keys during initial user setup for all IAM users that have a console password.	6.3	Added to Plan on Sep 4, 2018

IAM 사용자를 초기 생성할 때 Access Key가 자동으로 부여되지 않게 하라.
(위배 3건 발견)

컴플라이언스 및 취약점 관리

이슈 조치 - Initial Access Key

Do not setup access keys during initial user setup for all IAM users that have a console password. Added to plan On 13:23 - 2018-09-04

remove from plan | dispose | mark as complete

AWS 콘솔 조치 방법

Perform the following to delete access keys that do not pass the audit:

1. Login to the AWS Management Console:
2. Click Services
3. Click IAM
4. Click on Users
5. Click on Security Credentials
6. As an Administrator
 - Click on Delete for keys that were created at the same time as the user profile but have not been used.
7. As an IAM User
 - Click on Delete for keys that were created at the same time as the user profile but have not been used.

Via CLI
aws iam delete-access-key

Filters Used

No applied filters were found.

Exposures 0 | 3 | 0 | 0 Affected Assets 2 Evidence 3

Disable Automatic Access Key Creation 6.3

Affected Assets	Evidence
hyeink	{access_key_last_used,"hyeink", "..."}
chaehyunju	{access_key_last_used,"chaehyunju", "..."}

AWS 콘솔 조치 방법

관련 계정

컴플라이언스 및 취약점 관리

이슈 조치 – Initial Access Key

The screenshot shows the AWS IAM console for user 'chaehyunju'. The 'Security credentials' tab is selected, showing 'Sign-in credentials' and 'Access keys'. The 'Access keys' section contains a table with two inactive keys. A callout box points to the first key, indicating it should be deleted as it is not being used.

Access key ID	Created	Last used	Status
[Redacted]	2018-07-16 15:49 UTC+0900	N/A	Inactive Make active Delete
[Redacted]	2018-07-19 13:04 UTC+0900	N/A	Inactive Make active Delete

삭제할 access key : 사용되지 않음

컴플라이언스 및 취약점 관리

컴플라이언스 관리 - 보고서

OVERVIEW
INCIDENTS
REMEDIATIONS
SEARCH
REPORTS
CONFIGURATION

Interactive
Scheduled
Usage

Service Review 2

Incident Analysis 5

AWS Incident Analysis 6

CIS Benchmarks 1

CIS AWS Foundations Benchmark

Environment Exposure Trends 2

Vulnerability Analysis 2

Vulnerability Reports 1

Product Usage 3

← Undo → Redo ← Revert ↻ Refresh ⏸ Pause
* 山 뷰: 원본 ⚙ Share ⏴ Download [] 전체 화면

CIS AWS Foundations Benchmark

Deployment Name: (All) Section: (모두)

Openbase - Production

Last Updated Time: 9/4/2018 10:02:53 AM

Passed Checks

27.7% (13)

Partially Passed Checks

2.1% (1)

Failed Checks

70.2% (33)

CIS Check Name List (Select Check Name to view asset level info)

Section	Check Name	Passed/Total	Status
1 Identity and Access	Avoid the use of the "root" account	1/1	Passed
	Do not setup access keys during initial user setup for all IAM users that have a console password	3/3	Passed
	Enable detailed billing	0/1	Failed
	Ensure a support role has been created to manage incidents with AWS Support	0/1	Failed
	Ensure access keys are rotated every 90 days or less	3/3	Passed
	Ensure credentials unused for 90 days or greater are disabled	3/3	Passed
	Ensure hardware MFA is enabled for the "root" account	1/1	Passed
	Ensure IAM instance roles are used for AWS resource access from instances	1/1	Passed
	Ensure IAM Master and IAM Manager roles are active	0/1	Failed
	Ensure IAM password policy expires passwords within 90 days or less	0/1	Failed
	Ensure IAM password policy prevents password reuse	0/1	Failed
	Ensure IAM password policy require at least one lowercase letter	0/1	Failed
	Ensure IAM password policy require at least one number	0/1	Failed
	Ensure IAM password policy require at least one symbol	0/1	Failed
	Ensure IAM password policy require at least one uppercase letter	0/1	Failed
Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	0/3	Failed	
Ensure no root account access key exists	1/1	Passed	
2 Logging	Ensure AWS Config is enabled in all regions	0/1	Failed
	Ensure CloudTrail is enabled in all regions	1/1	Passed

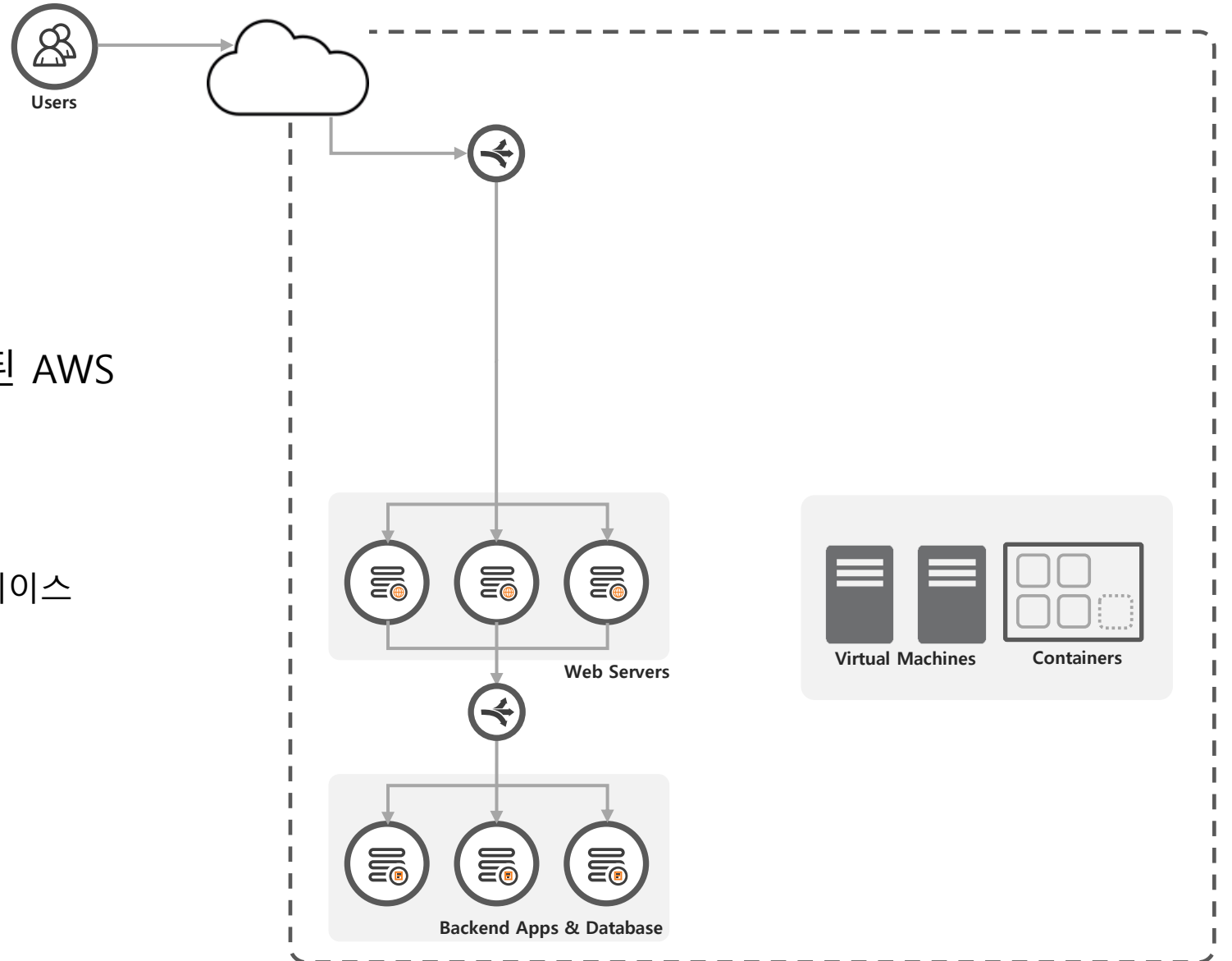
Do not setup access keys during initial user setup for all IAM users that have a console password

Alert Logic 구성

Alert Logic Architecture - AWS

서비스 시스템 및 내부 자산으로 구성된 AWS 환경

- public 네트워크에 구성된 웹 서비스
- private 네트워크 백엔드 시스템 및 데이터베이스
- 가상 서버/호스트 및 컨테이너



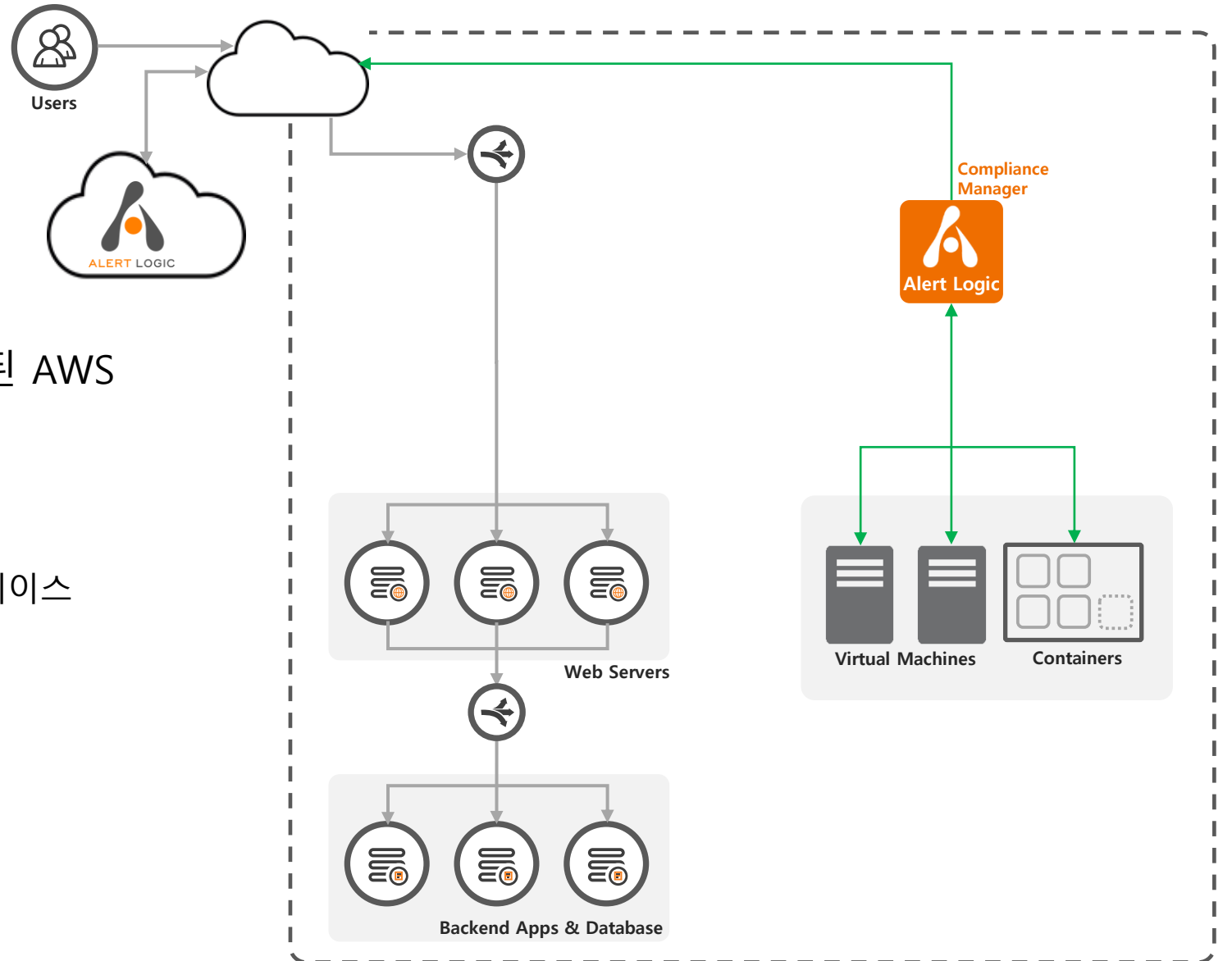
Alert Logic Architecture - AWS

서비스 시스템 및 내부 자산으로 구성된 AWS 환경

- public 네트워크에 구성된 웹 서비스
- private 네트워크 백엔드 시스템 및 데이터베이스
- 가상 서버/호스트 및 컨테이너

Alert Logic Essential

- Compliance 관리 어플라이언스



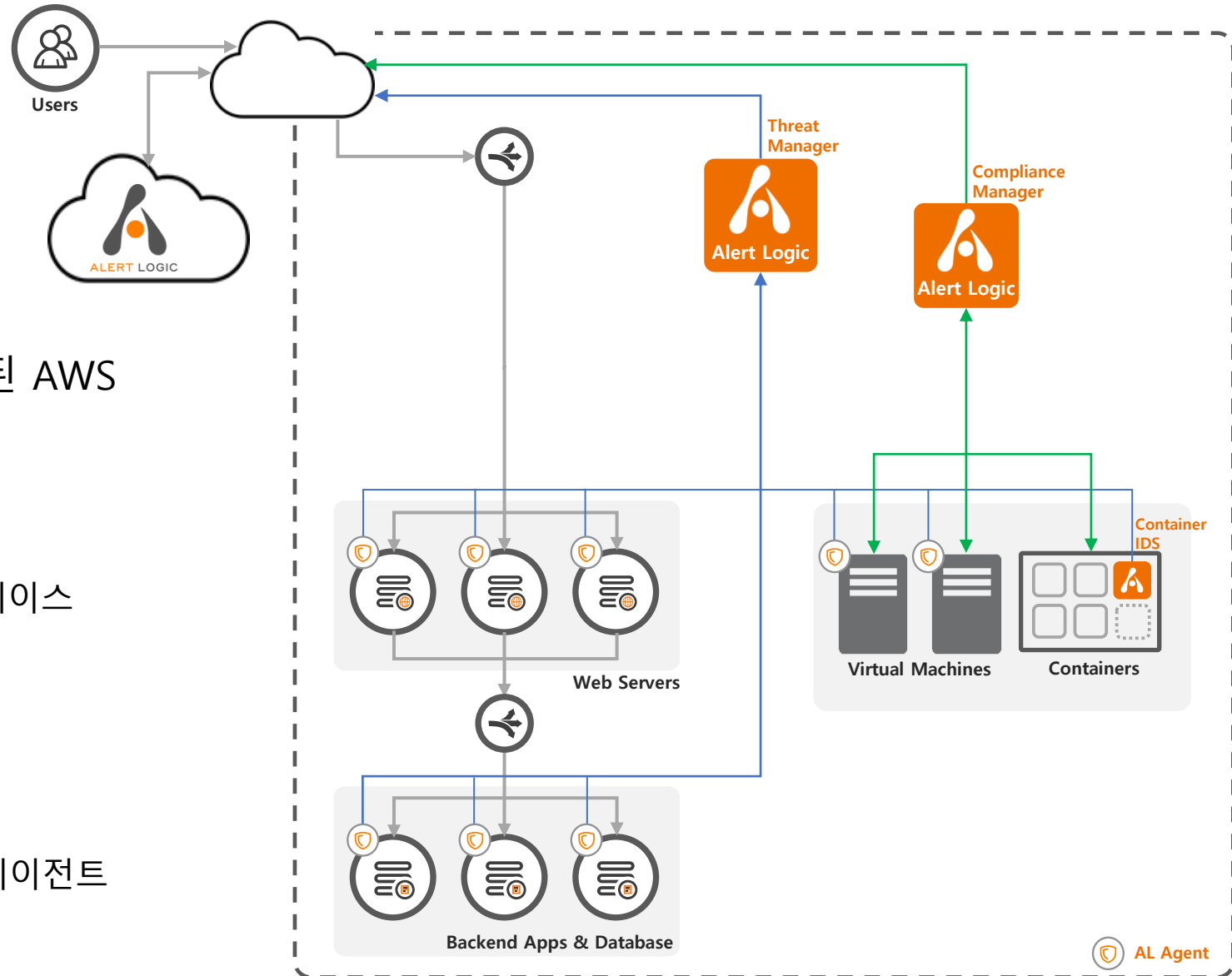
Alert Logic Architecture - AWS

서비스 시스템 및 내부 자산으로 구성된 AWS 환경

- public 네트워크에 구성된 웹 서비스
- private 네트워크 백엔드 시스템 및 데이터베이스
- 가상 서버/호스트 및 컨테이너

Alert Logic Professional

- Compliance 관리 어플라이언스
- 위협 관리 어플라이언스 및 컨테이너 IDS, 에이전트



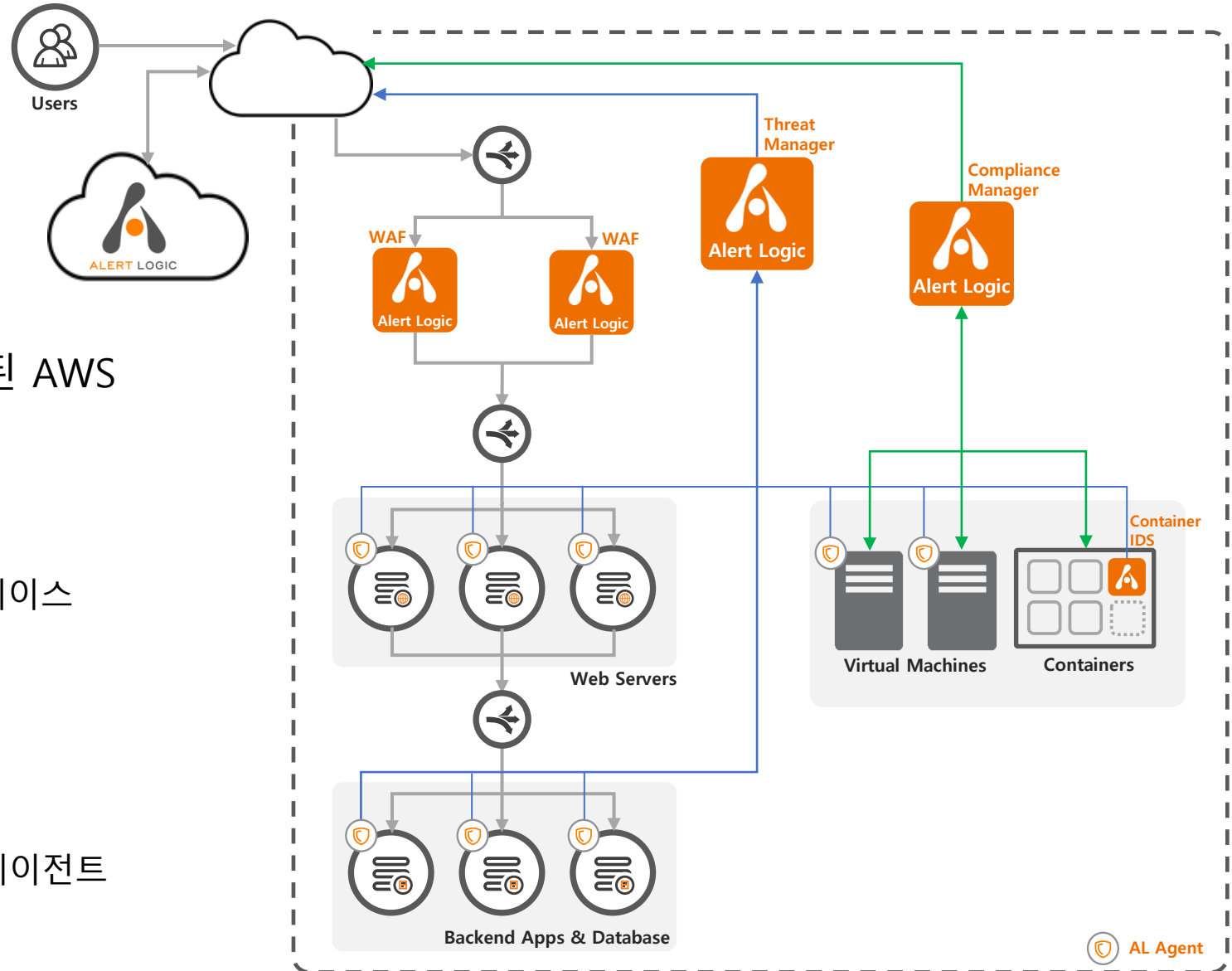
Alert Logic Architecture - AWS

서비스 시스템 및 내부 자산으로 구성된 AWS 환경

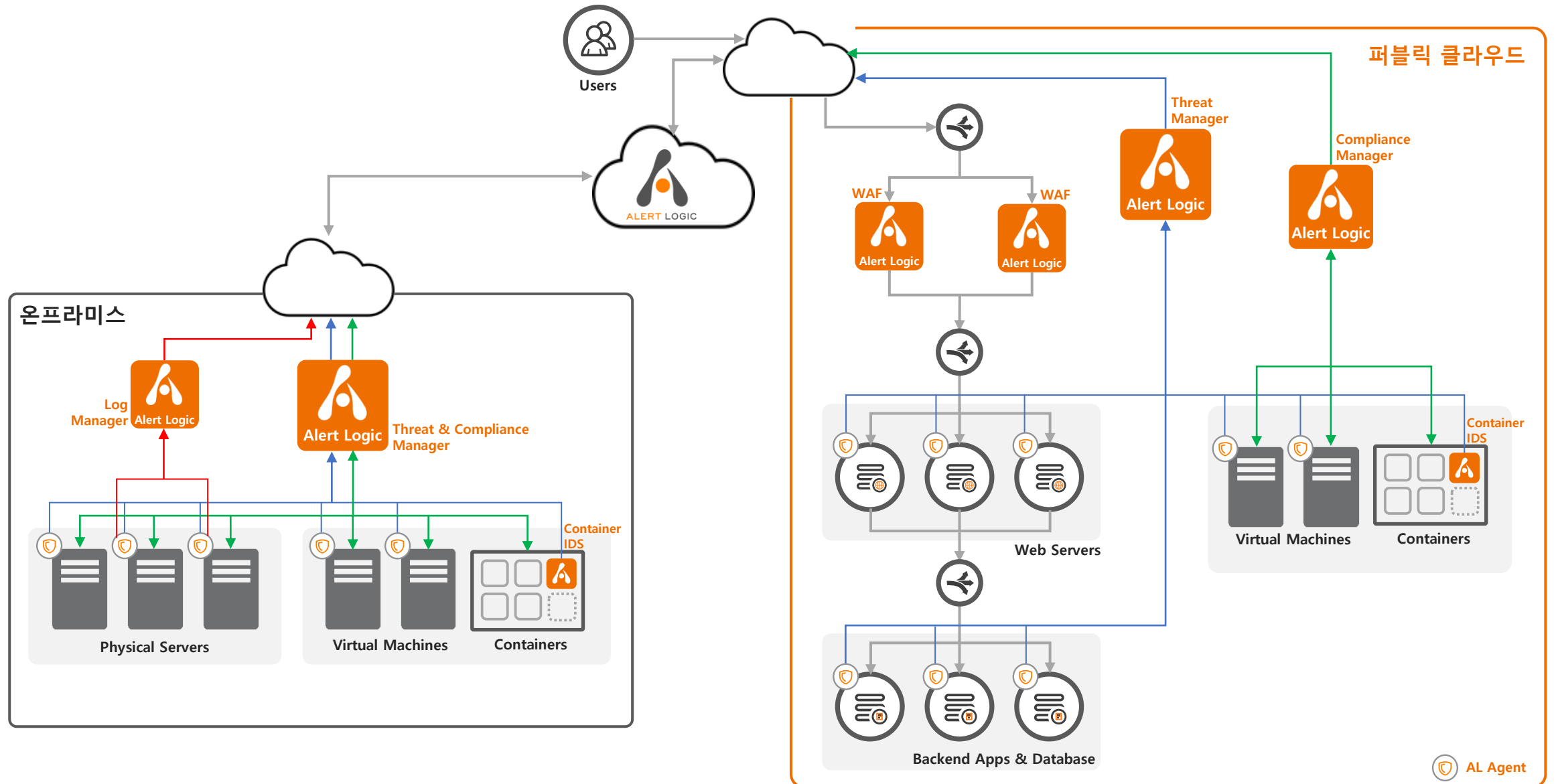
- public 네트워크에 구성된 웹 서비스
- private 네트워크 백엔드 시스템 및 데이터베이스
- 가상 서버/호스트 및 컨테이너

Alert Logic Professional & WAF

- Compliance 관리 어플라이언스
- 위협 관리 어플라이언스 및 컨테이너 IDS, 에이전트
- Alert Logic WAF



Alert Logic Architecture - Hybrid



감사합니다.