



# 엔드포인트 시큐리티, 국내환경 적용 완료

Why SGASolutions ?

한성화 부장

에스지에이솔루션즈(주)

# CONTENTS

---

1. Endpoint 보안 환경
2. Endpoint Security 주안점
3. Why SGASolutions ?

# 1. Endpoint 보안 환경

- Network vs. Endpoint
- 다양한 Service
- 다양한 운영환경
- 보안 패치
- 보안 솔루션
- Service Priority

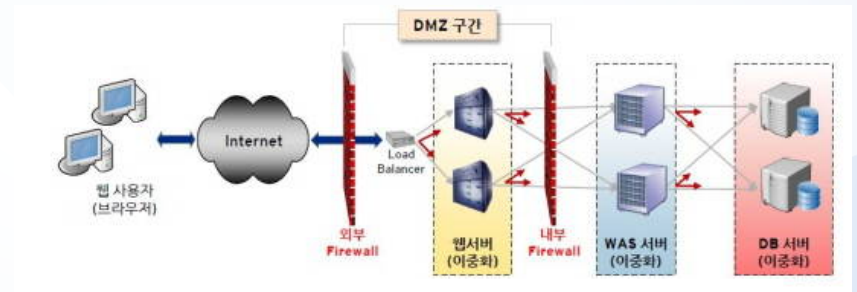
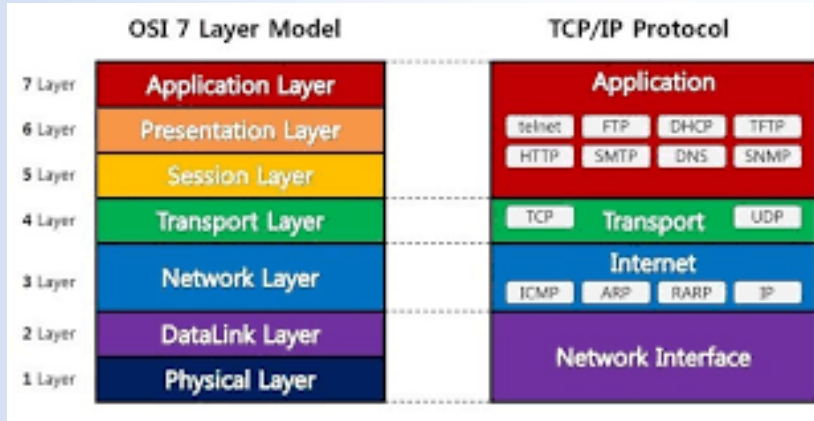
# 1. Network vs. Endpoint

## Network

- Stack 표준 적용
- 관리자의 '의도'에 따른 변화
- 동일 Data 형식(Frame, Packet, Segment)

## Endpoint

- Platform(HW, SW 등) 구성의 높은 자유도
- 목표 달성에 따른 Software 선택
- 관리자의 의도와 무관한 환경 변화



## 2. 다양한 Service



### 3. 다양한 운영환경



# 4. 보안 패치

http://www.cvedetails.com/top-50-vendor

파일(F) 편집(E) 보기(M) 즐겨찾기(A) 도구(T) 도...

X Cookie 641 links on page:

## CVE Details

The ultimate security vulnerability datasourc...

Log In Register Reset Password Activate Account

Switch to https://

### CVSS Score Distribution For

Vendor Name	Number of Total
1 Microsoft	
2 Apple	
3 Oracle	
4 IBM	
5 Cisco	
6 SUN	
7 Adobe	
8 Mozilla	
9 Google	
10 Linux	
11 HP	
12 Redhat	
13 Novell	
14 Apache	
15 Debian	
16 PHP	
17 Symantec	
18 GNU	386 1 5 31 26 57 98 44
19 Wirespark	356 1 2 24 32 110 143 7
20 Canonical	345 10 24 12 87 66 52
21 FreeBSD	327 2 40 8 34 60 23
22 Joomla	321 1 2 46 44 41
23 Drupal	290 1 14 49 57 34 29
24 EMC	282 1 24 16 24 42 23

제어판 홈

업데이트 확인

설정 변경

업데이트 기록 보기

숨겨진 업데이트 복원

업데이트: 질문과 대답

컴퓨터

1개

1개

가능

참고 항목

설치된 업데이트

Windows Anytime Upgrade

Office 업데이트

이 제품은 업데이트되지 않습니다.

현재 분기

버전: 16.0.6366.2062

업데이트 옵션

업데이트 사용

보안, 성능 및 신뢰성에 대한 최신 업데이트를 자동으로 받습니다.

업데이트 보기

이 제품의 업데이트 기록을 표시합니다.

업데이트 정보

자세한 정보

작권 정보에 대해 자세히 알아봅니다.

다음과 같은 업데이트할 제품(1)이

제품 이름	현재 판	최신 판	업데이트(U)
<input checked="" type="checkbox"/> 한컴오피스 업데이트 2010	8.5.6.55	8.5.8.60	닫기

환경 설정(S)... 업데이트 내용(I)



# 5. 보안 솔루션

NH농협은 정부가 추진하는 'ActiveX 없는 전자금융 구현' 및 구글 크롬(NPAP)지원종단으로 2019년 12월 5일부터 ActiveX(플러그인)가 없는 PC에 따라 고객님의 PC에 범용실행파일(exe)형태의 새로운 보안프로그램을 설치합니다.

## NH Bank에서 제공하는 보안프로그램을 설치합니다.

고객님의 안전한 서비스 이용을 위한 보안프로그램을 통합관리 할 수 있습니다.

1. [현재설치]를 클릭하시면 자동으로 설치가 진행됩니다.
2. 각 프로그램의 '자세히보기'를 클릭하시어 기능을 확인하시기 바랍니다.

프로그램명	기능	설치상태
통합설치 프로그램(Veraport)	보안프로그램을 한번에 다운로드하기 위한 프로그램입니다.	
공인인증서 보안 (INISAFE CrossWeb EX)	공인인증서 로그인과 거래내역에 대한 전자서명용	
개인PC방화벽(ASTX) (AhnLab Safe Transaction)	비인가된 접근을 차단하고 해킹 및 바이러스를 예방합니다. <a href="#">[자세히보기]</a>	
키보드 보안(TouchEnNdxKey)	키보드를 통해 입력되는 정보가 유출되거나 변조되는 것을 방지합니다. <a href="#">[자세히보기]</a>	
보안 브라우저 (INISAFE SandBox)	악성 프로그램에 의해 웹 페이지가 변조되는 것을 방지합니다. <a href="#">[자세히보기]</a>	

[현재설치](#) [홈페이지로](#)

- WindowsXp 64bit/Windows Server군에서는 [AhnLab Safe Transaction]을 설치합니다.
- 보안프로그램 설치 완료 후에도 계속적인 설치 안내가 나오거나 보안프로그램 오류가 발생하면 보안프로그램 삭제 후 재설치 하시기 바랍니다. [\[오류해결안내 바로가기\]](#)
- 접속PC정보 : [Windows, Win32][MSIE, 11.0] Mozilla/5.0 (Windows NT 10.0; Trident/6.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36
- 설치된 프로그램을 재 설치하고자 할 경우에는 해당 프로그램 [Aosmgr]를 삭제 후 재 설치 하시기 바랍니다.
- 수동설치 후에는 반드시 **새로고침**을 하거나 다시 접속하시기를 바랍니다.
- Firefox, Opera의 경우 [메뉴] - [부가기능] - [확장기능]을 선택하고 INISAFE CrossWebEX를 사용함으로 변경 후 다시 시작하시기를 바랍니다.



문서나 도면 생성시 부터 원천 암호화





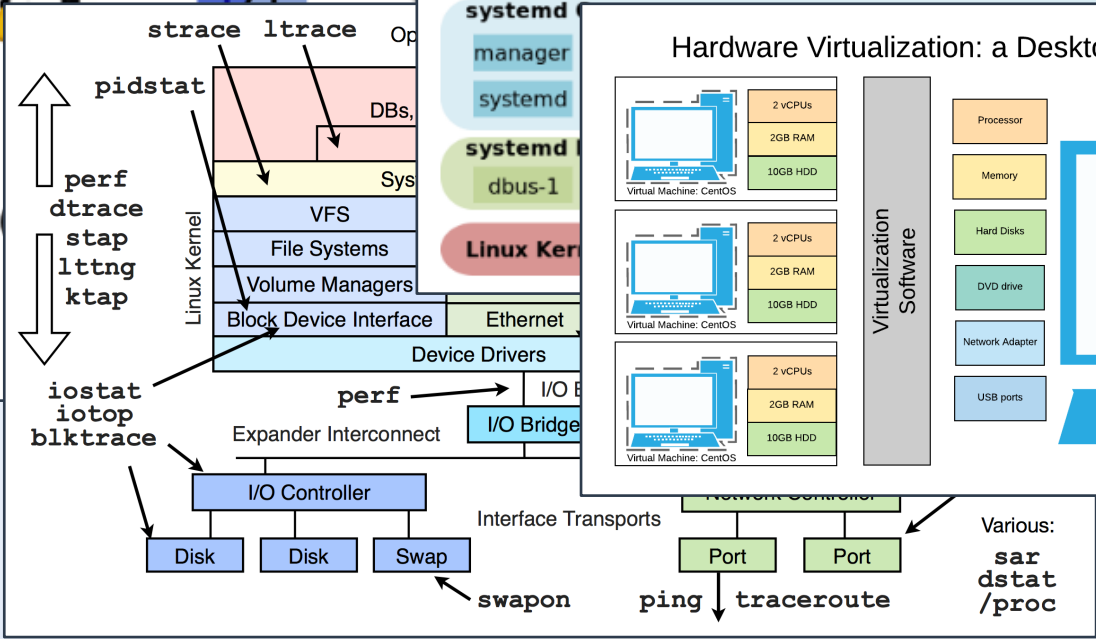
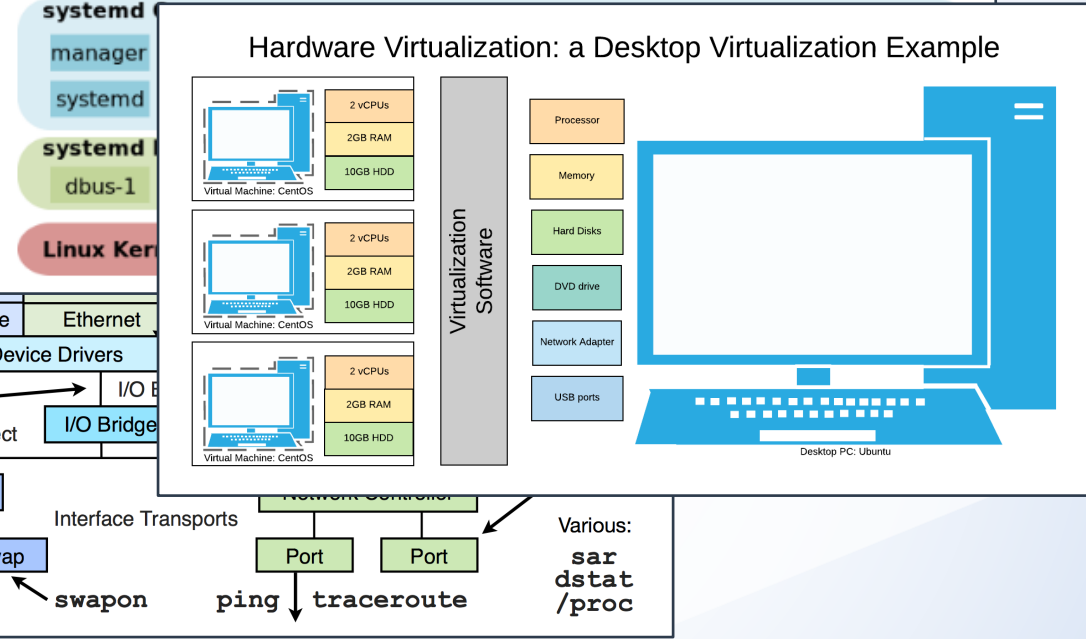
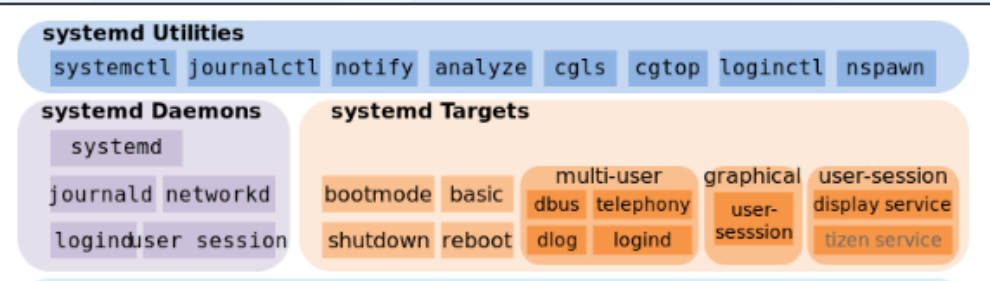
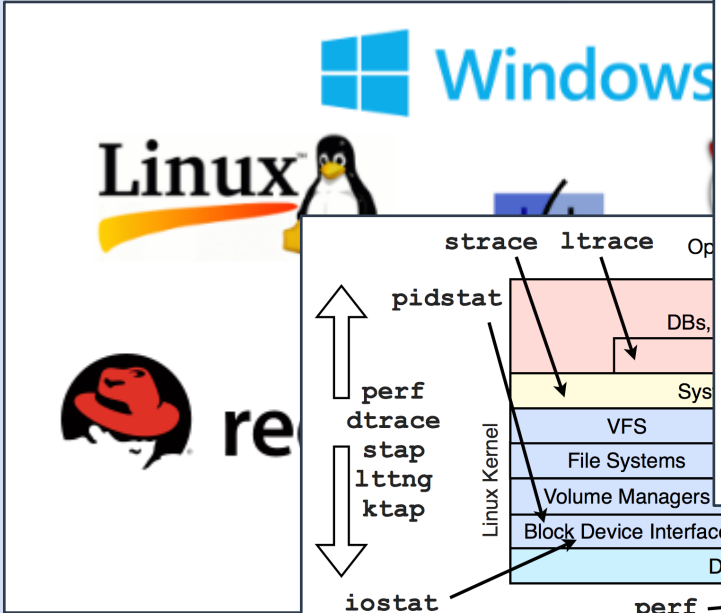
# 6. Service Priority



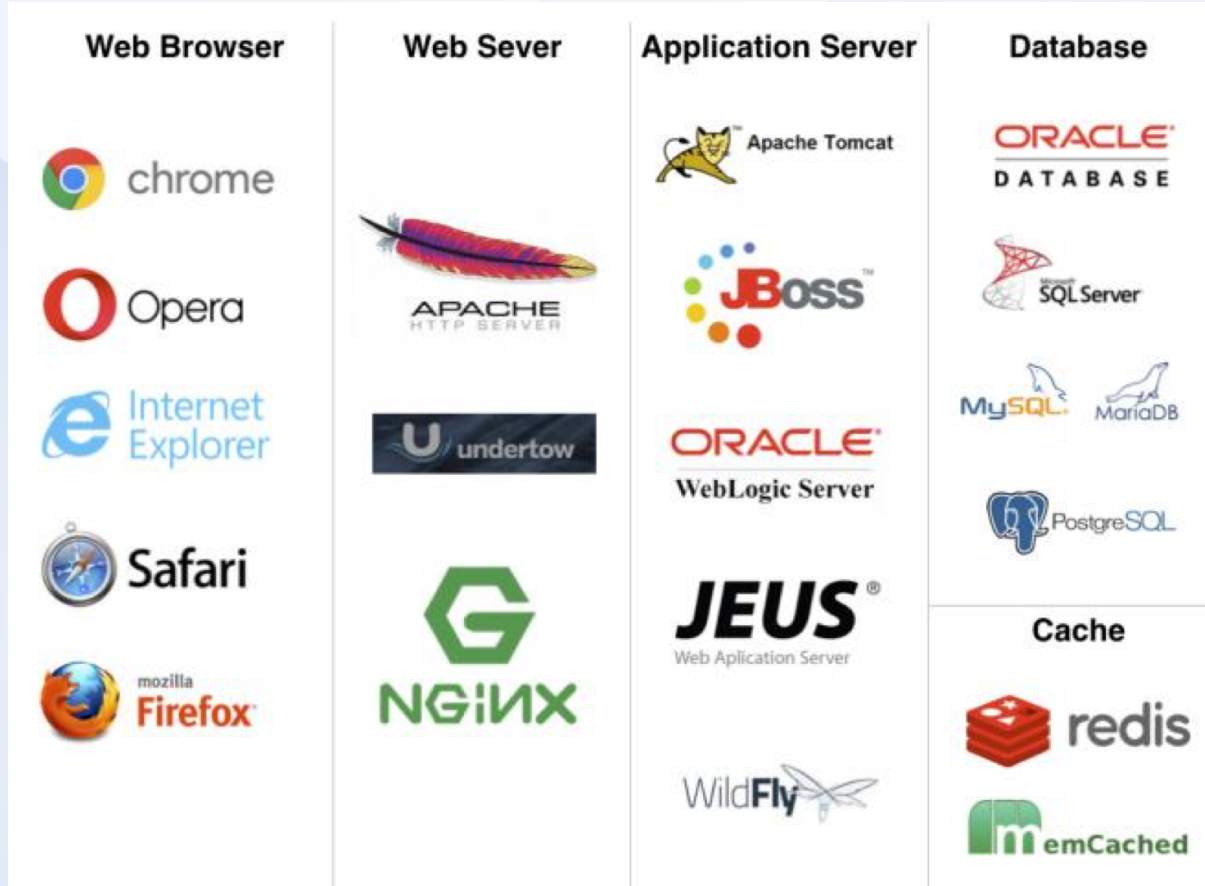
## 2. Endpoint Security 주안점

- OS에 대한 이해
- Application Service에 대한 이해
- Security Pre-Check(호환성 검사)
- 장애 대응
- Security Domain 지식
- 기타

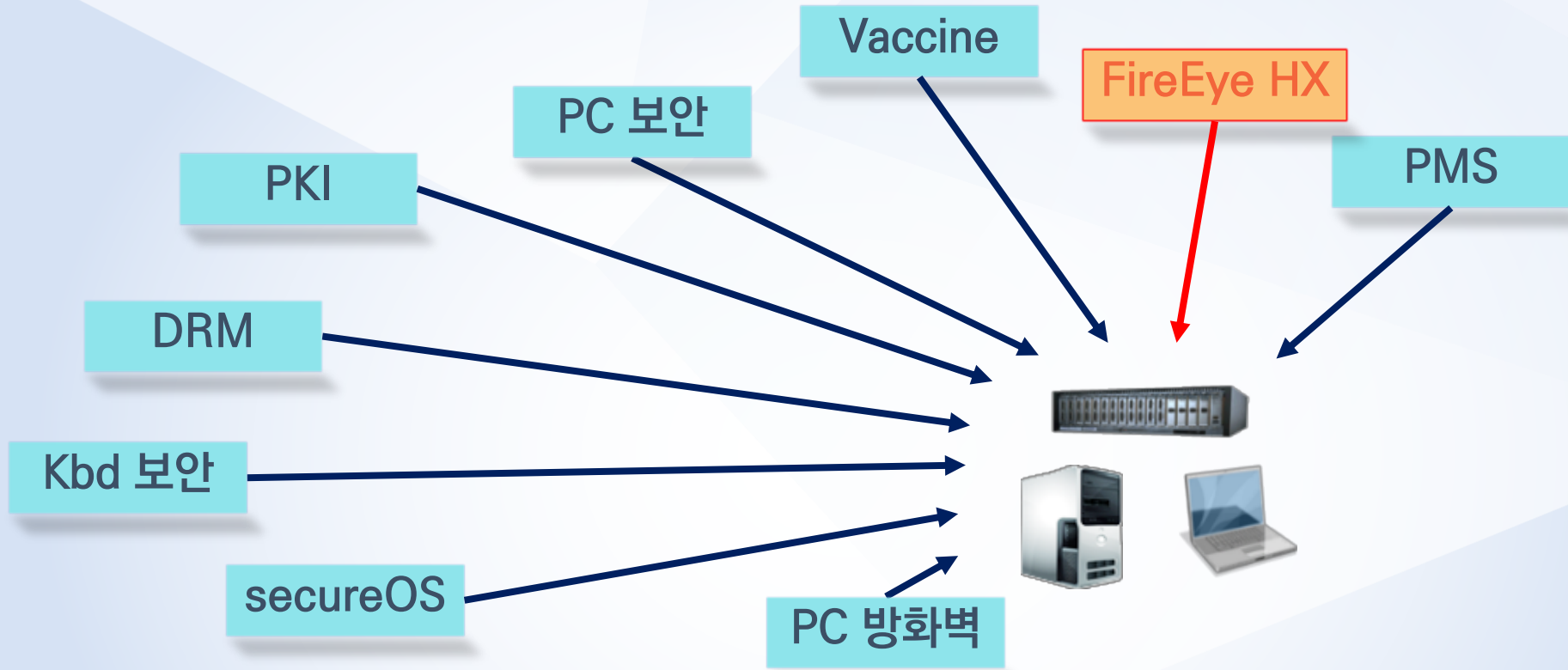
# 1. OS에 대한 이해



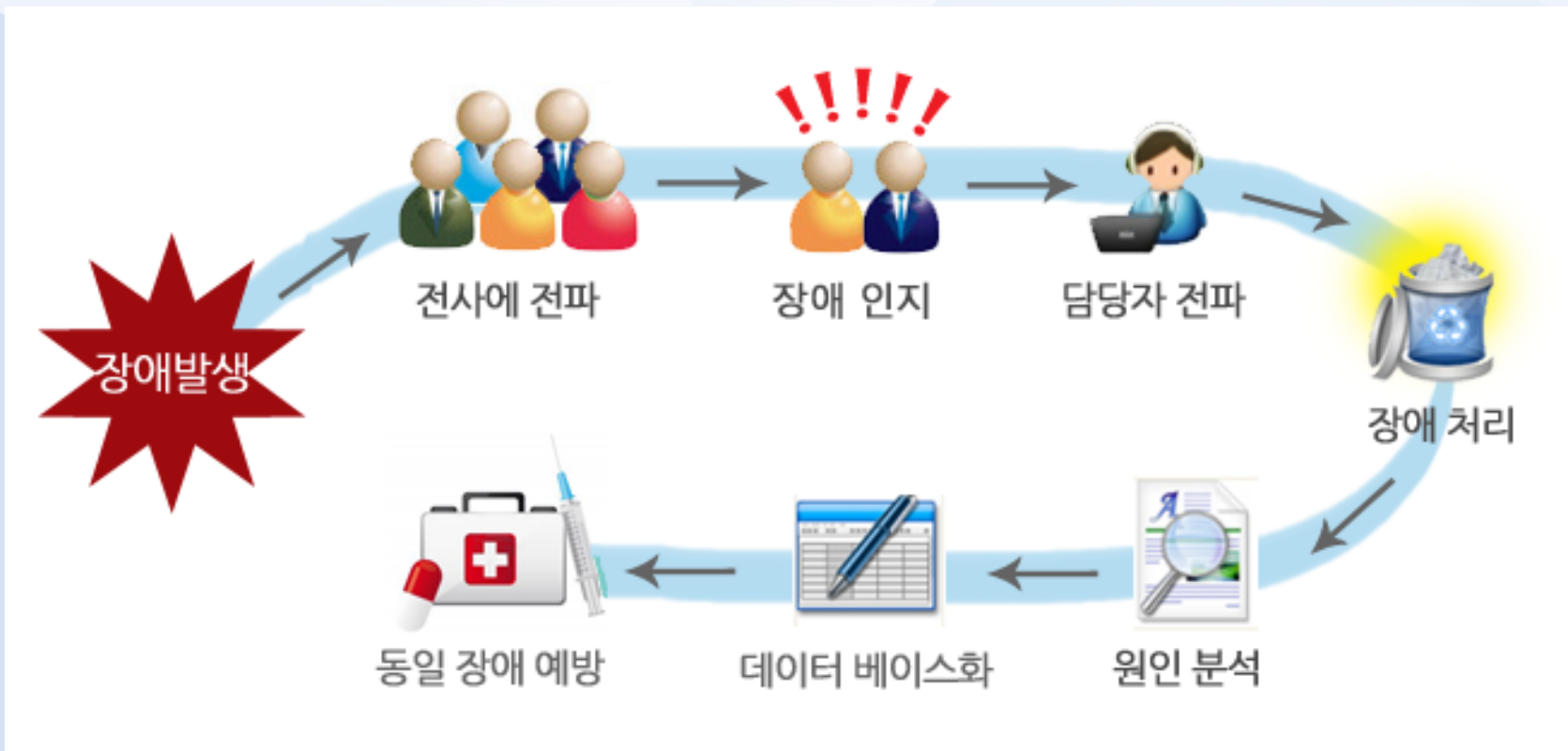
# 2. Application Service에 대한 이해



# 3. Security Pre-Check(호환성 검사)



# 4. 장애 대응



# 5. Security Domain 지식

구분	법	시행령	시행규칙
ICT 산업 진흥 관계법령	인터넷주소자원에 관한 법률	인터넷주소자원에 관한 법률 시행령	-
	정보통신 진흥 및 융합 활성화 등에 관한 특별법	정보통신 진흥 및 융합 활성화 등에 관한 특별법 시행령	정보통신 진흥 및 융합 활성화 등에 관한 특별법 시행규칙
	정보통신산업 진흥법	정보통신산업 진흥법 시행령	정보통신산업 진흥법 시행규칙
	정보보호산업의 진흥에 관한 법률	정보보호산업의 진흥에 관한 법률 시행령	정보보호산업의 진흥에 관한 법률 시행규칙
	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령	-
정보보호 관계법령	정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙
	정보통신기반 보호법	정보통신기반 보호법 시행령	정보통신기반 보호법 시행규칙
	국가정보화 기본법	국가정보화 기본법 시행령	국가정보화 기본법 시행규칙
	전자정부법	전자정부법 시행령	-
개인정보보호 관계법령	개인정보 보호법	개인정보 보호법 시행령	개인정보 보호법 시행규칙
	정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙
	위치정보의 보호 및 이용 등에 관한 법률	위치정보의 보호 및 이용 등에 관한 법률 시행령	-

구분	법	시행령	시행규칙
기타 참고 법령	전자문서 및 전자거래 기본법	전자문서 및 전자거래 기본법 시행령	전자문서 및 전자거래 기본법 시행규칙
	전자서명법	전자서명법 시행령	전자서명법 시행규칙
	전자금융거래법	전자금융거래법 시행령	-
	전기통신사업법	전기통신사업법 시행령	-
	전기통신기본법	전기통신기본법 시행령	-
	통신비밀보호법	통신비밀보호법 시행령	통신제한조치 등 허가규칙
	-	국가사이버안전관리규정	-
	-	보안업무규정	보안업무규정 시행규칙
	방송통신발전 기본법	방송통신발전 기본법 시행령	-
	전자상거래 등에서의 소비자보호에 관한 법률	전자상거래 등에서의 소비자보호에 관한 법률 시행령	전자상거래 등에서의 소비자보호에 관한 법률 시행규칙
기타 참고 법령	신용정보의 이용 및 보호에 관한 법률	신용정보의 이용 및 보호에 관한 법률 시행령	신용정보의 이용 및 보호에 관한 법률 시행규칙
	스마트도시 조성 및 산업진흥 등에 관한 법률	스마트도시 조성 및 산업진흥 등에 관한 법률 시행령	-
	국가공간정보 기본법	국가공간정보 기본법 시행령	-
	소비자기본법	소비자기본법 시행령	-

※ 출처: 한국인터넷진흥원





# 6. 기타



## Enter the Configuration Command

You can use the Cisco IOS CLI to enter the configuration commands manually.

1. Log on to the switch through the Console port.
2. If you use the Console port, and no network is configured on the switch, the Setup command Facility appears.

---System Configuration Dialog---

Continue with configuration dialog?

Enter no so that you can enter Cisco commands directly.

If the Setup Command Facility does not appear, go to the next section.

3. When the user EXEC mode prompt appears, enter the enable password, if one is configured. For example:

```
Switch> enable
```

```
password: password
```

4. Enter config mode by entering the configuration command. For example:

```
Switch> config terminal
```

```
Switch(config)#
```

**2.1.3 Mac**

SentryAPT V1.0  
normal and abnormal

**4.2.1 Security log policy settings**

Security Set log collection policy for each agent.

Depending on the security agent, select the type of log to collect logs and then select 'Apply' at the bottom. Log collection policy will be applied.

Log Type	Description
FTP	On the system where Security Agent is installed, it saves the FTP user log of ordinary user.
TTY	On the system where security agent is installed, TTY access log such as Telnet, SSH, rLogin of general user is saved.
TTY I/O	Stores the Input Message and Output Message generated by the normal user's TTY session on the system where Security Agent is installed.

The log types that can be set are as follows.

sga SGA Solutions Co., Ltd.

74 / 170

## 04. Why SGASolutions ?

- Endpoint 보안 기술 확보
- Endpoint 보안 솔루션 보유
- 장애 대응 Process
- QA
- Etc.
- Endpoint Security 기술 확보

# 1. Endpoint 보안 기술 확보

## Targeted Security Domain

### 엔드포인트 보안 솔루션 개발 및 공급

10여년 간 엔드포인트 보안 솔루션 개발 및 공급, 기술지원

- 백신, PMS, WhiteLoc, DeviceLoc
- DaLoc, 내PC지킴이
- 통합 에이전트 및 통합 PC보안 제품

### 국내 다양한 System 환경 지원

다양한 Svr, PC 에이전트 환경에 대한 지원

- Windows Server/Desktop OS
- Linux/Unix 등
- 개발제품에 대한 타 보안솔루션과의 충돌 대응 경험

### 자체 악성코드 분석팀 운영

개발팀과 독립적인 자체 악성코드 분석팀 운영

- 악성코드 수집, 분석
- 악성코드 테스트 및 행위분석
- 악성코드 DB 등록 및 제품 반영

### 위협분석, 대응을 위한 인텔리전스팀 운영

위협분석/대응의 인텔리전스팀 운영

- 악성코드 분석 외에 지능형 침해위협 분석
- 악성행위 정형화, 모델링, 능동형 차세대 보안위협 탐지, 대응방안 연구



## 2. Endpoint 보안솔루션 보유

### 서버 보안

#### RedCastle

- › 정확하고 강력한 사용자 행위기반 서버 접근통제 제품

#### AuthCastle

- › 서버 접근(접속) 시 기본 ID / Password 외에 추가 인증을 제공하는 2차 인증 솔루션

#### AuditCastle

- › 서버 접근에 대해서 이상 또는 비정상 행위에 대한 로그 수집, 저장 및 분석할 수 있는 제품

### 응용보안

#### TrustChannel FIDO

- › 사용자의 생체정보 등을 통하여 사용자 인증을 수행할 수 있는 차세대 인증 솔루션

#### TrustCertificate

- › 증명서 등의 문서에 대해 법적 효력이 있는 문서를 생성하며, 이를 검증할 수 있는 솔루션

#### TrustDocument

- › 종이문서의 소모 비용을 절감하고, Paperless 비즈니스 환경을 구축할 수 있는 솔루션

### 시스템보안

#### VirusChaser

- › 사용자PC 및 서버에 대해 바이러스 및 악성코드, 웜 등을 탐지하고 치료하는 백신 솔루션

#### PatchChaser

- › Windows 기반의 사용자 PC에 대한 보안 패치를 일괄 적용하는 제품

#### DaLoc

- › 인터넷 PC의 사용자 작업에 의하여 생성된 문서 자료의 강제 삭제 솔루션

### Infra 보안

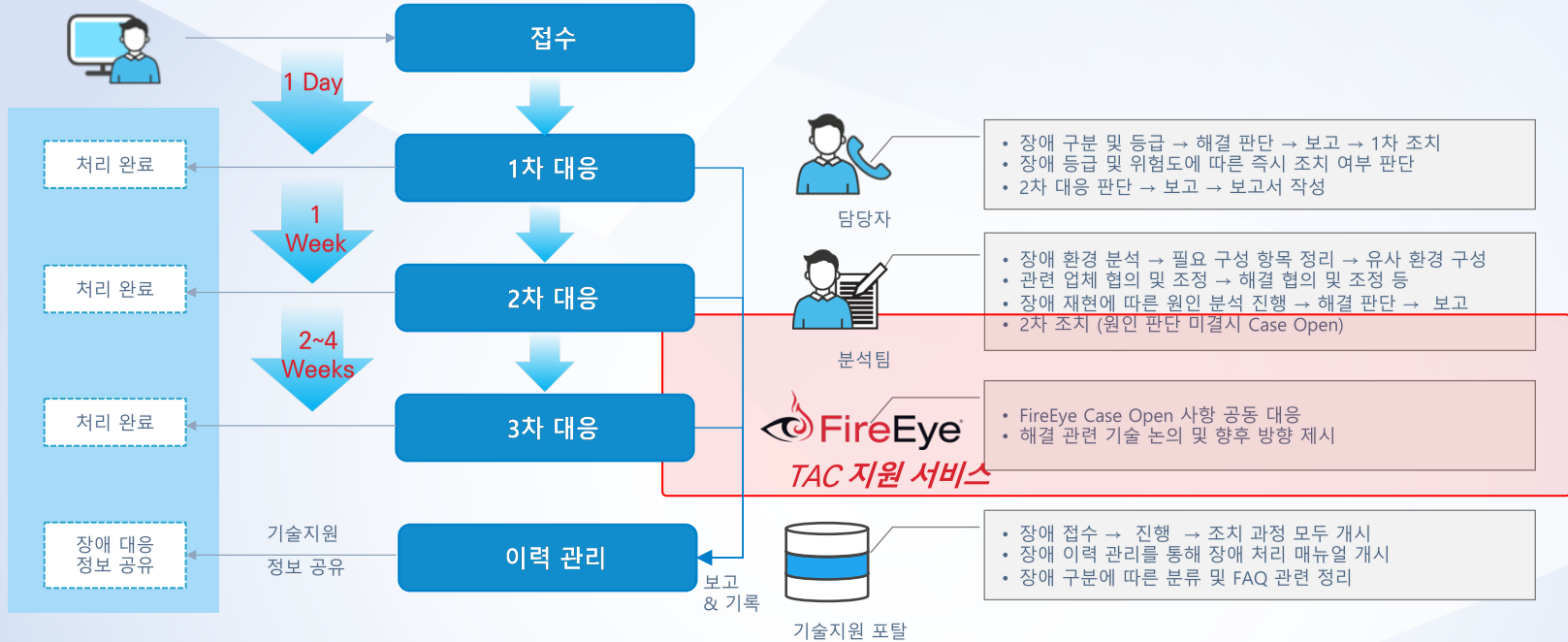
#### SentryAPT

- › Bigdata 및 Machine Learning 기반의 APT 공격 탐지 시스템

#### SentryIntelligence

- › Cloud, DNN 기반의 악성코드 분석 시스템

# 3. 장애 대응 Process



# 4. QA(Quality Assurance)

## 1. QA Role



### 제품 검증

- 설치 절차와 운영을 통하여 발생 가능한 문제들에 대하여 사전 예방
- 제조사와의 업무 협업 체계 활용으로 제품 안정성 확보
- 기술팀 및 인텔리전스팀 인력으로 소프트웨어 상시 충돌 여부 검증
- 고객사 소프트웨어와 호환성 테스트
- 충분한 모의테스트를 통한 안정성 확보

금융.공공.기업의 다양한 내부 환경의 보안 제품 간 QA 검증으로 고객사 운영 시 사용자의 업무 연속성 확보, 제품의 내고장성, 업데이트 업무 공수의 최소화를 발휘합니다.

### 사전 테스트

- 사내 환경 테스트
- 사전 영향도 평가
- 상용 소프트웨어와 충돌테스트
- 기능 동작 테스트

### 그룹 테스트

- 고객사 테스트 그룹 선정 후 해당 그룹 테스트 진행
- 영향도 검증

### 시험결과

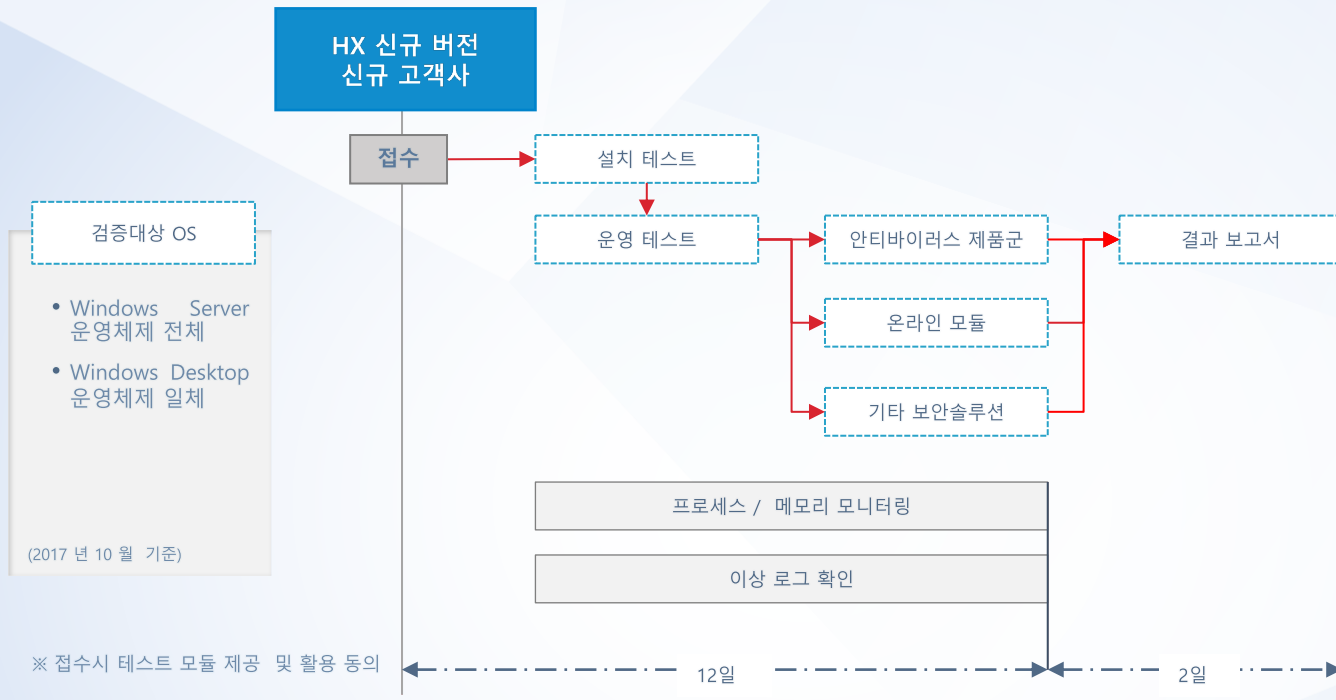
- 이상유무 판단
- 시험결과서 작성
- 배포 협의

### 배포

- 단계별 배포 진행

# 4. QA(Quality Assurance)

## 2. QA Process





# 4. Etc.



ITSC

SGA SOLUTIONS CC CERTIFICATION

## CC 인증



GOOD Software

SGA SOLUTIONS GS CERTIFICATION

## GS인증

Korea's first operating system authentication security check  
국내최초 운영체제 보안시스템 인증을 확인하세요

인증제품명	인증일
RedCastle V4.0 for Redhat Enterprise Linux 7	2015-10-16
Patch Chaser 2.1	2015-10-16
RedCastle V4.0 for Solsis 11	2015-10-01
RedCastle V4.0 for HP-UX11.31	2015-09-20
RedCastle V4.0 for RedHat Linux 6	2015-07-23
RedCastle V4.0 for AIX7.1	2015-06-19
Virus Chaser 9.0 Enterprise	2014-12-16
RedCastle V4.0 for Solsis 10	2014-07-31

분류	인증제품명	인증일	
Trust	TrustCertificate V2.5	2016-02-22	
Trust	TrustPKI Toolkit V4.0	2015-12-07	
DeLoc	DeLoc v2.0	2015-09-10	
Virus Chaser	Virus Chaser For Linux/Unix v2	2014-11-10	
WhiteLoc	WhiteLoc v2.1	2014-10-20	
RedCastle	RedCastle V4.0 for Solsis	2014-04-07	14-0077
RedCastle	RedCastle V4.0 for HP-UX	2014-04-07	14-0078
RedCastle	RedCastle V4.0 for Linux	2014-04-07	14-0079

- FireEye HX 및 Agent 관련 한글 기술자료 파트너 및 고객사 배포

HX Series	HX Agent
<ul style="list-style-type: none"> <li>• Administration Guide                             <ul style="list-style-type: none"> <li>- System Administration Guide</li> <li>- System Security Guide</li> <li>- User Guide</li> </ul> </li> <li>• Reference Guide</li> <li>• Release Note</li> </ul>	<ul style="list-style-type: none"> <li>• Administration Guide</li> <li>• Deployment Guide</li> <li>• Support Guide</li> <li>• Release Note</li> </ul>

- 최신 기술 지원 문서 릴리즈 발생 시 한글화 작업 후 2~4주 이내 배포



# 5. Endpoint 보안 기술 확보

## Base Security Technology



# Thank You !

