FIREEYE™

엔드포인트 시큐리티, 국내환경 적용 완료

Why SGASolutions ?

한 성 화 부장
에스지에이솔루션즈(주)

sga 에스지에이솔루션즈(주)

CONTENTS

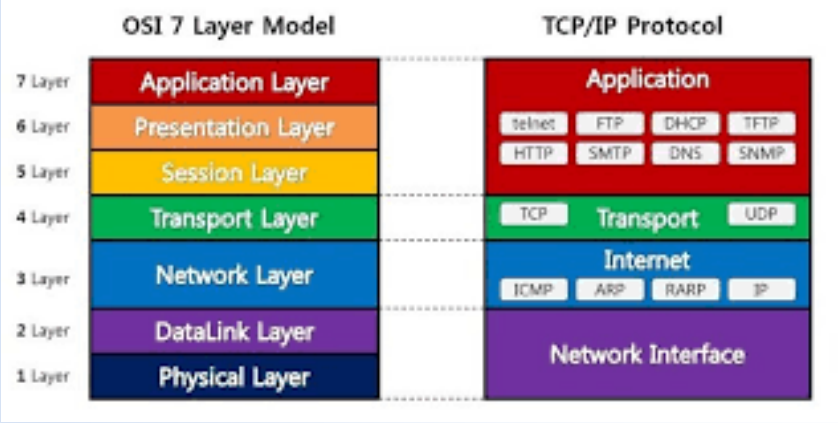
1. Endpoint 보안 환경

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

1. Network vs. Endpoint

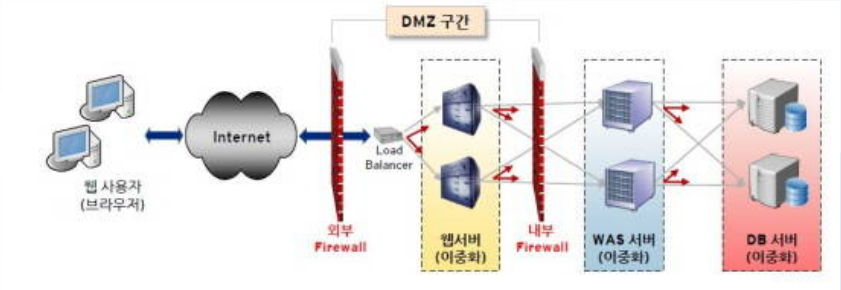
Network

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



Endpoint

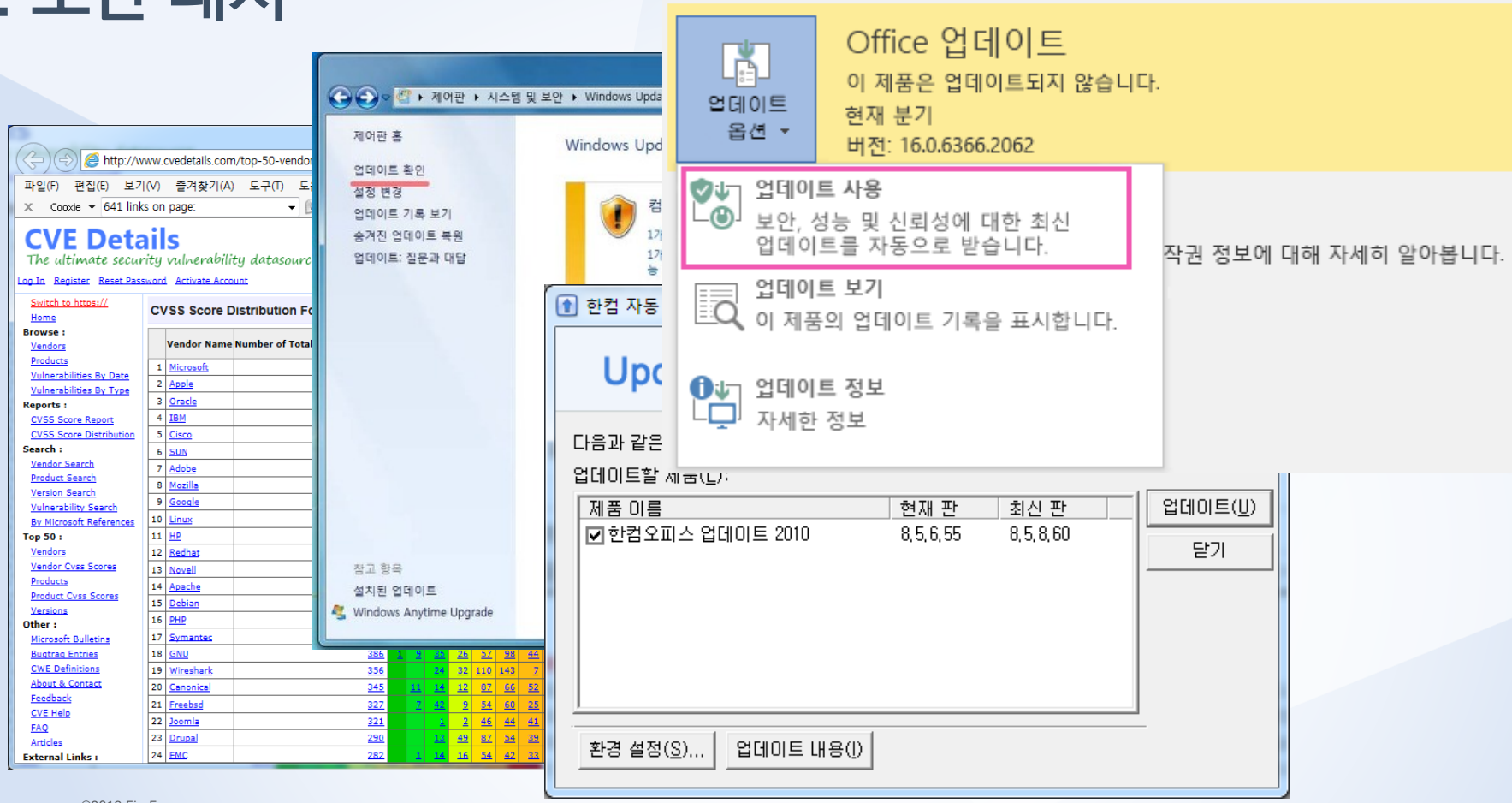
- Platform(HW, SW 등) 구성의 높은 자유도
- 목표 달성에 따른 Software 선택
- 관리자의 의도와 무관한 환경 변화



2. 다양한 Service

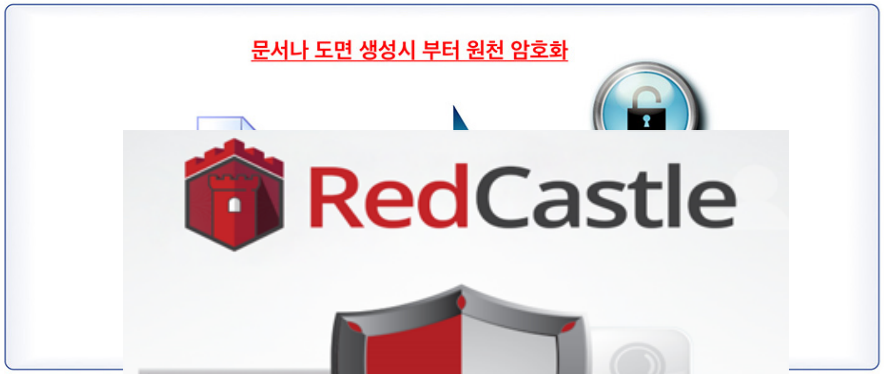
3. 다양한 운영환경

4. 보안 패치



에스지에이솔루션즈(주)

5. 보안 솔루션



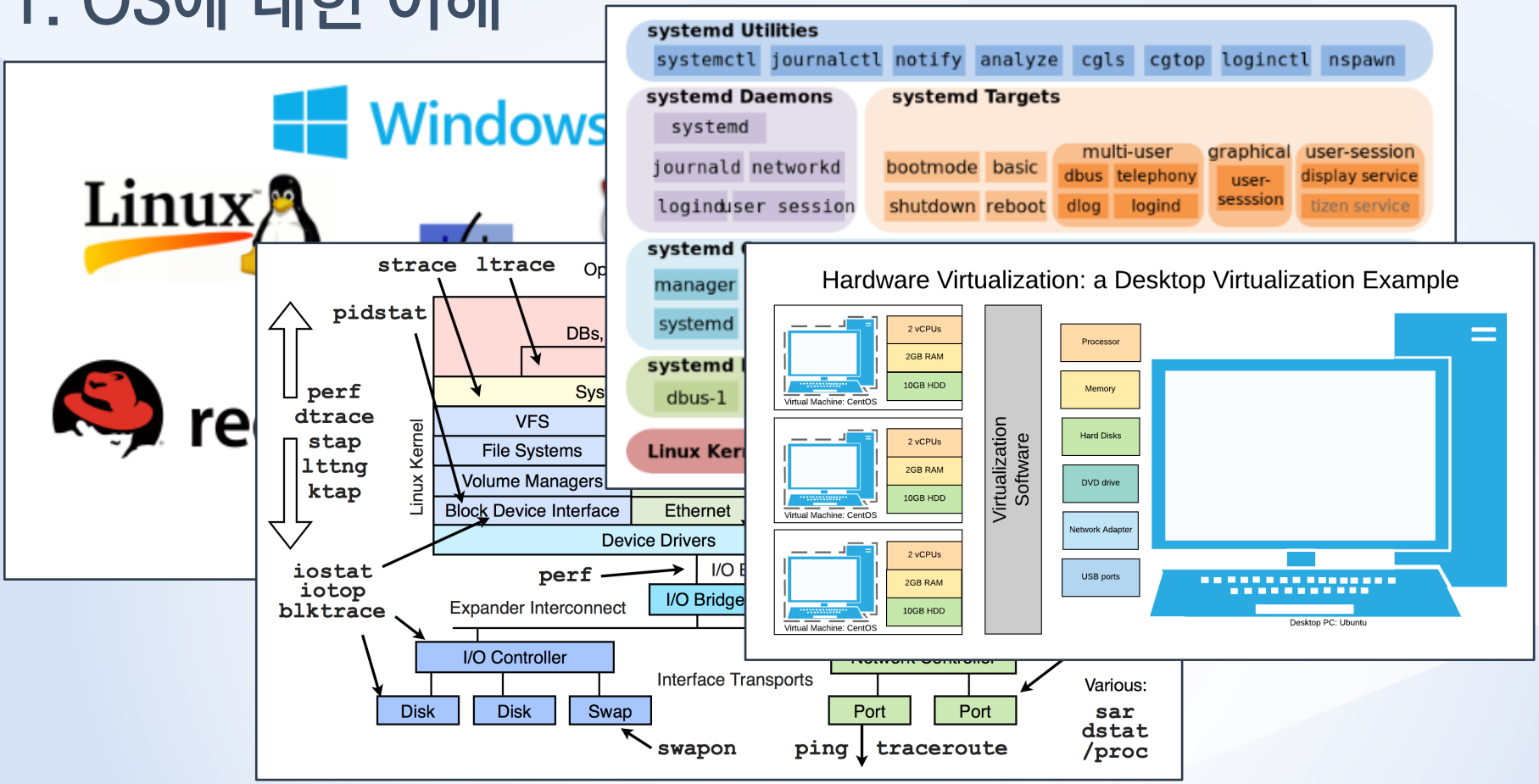
6. Service Priority

에스지에이솔루션즈(주)

2. Endpoint Security 주안점

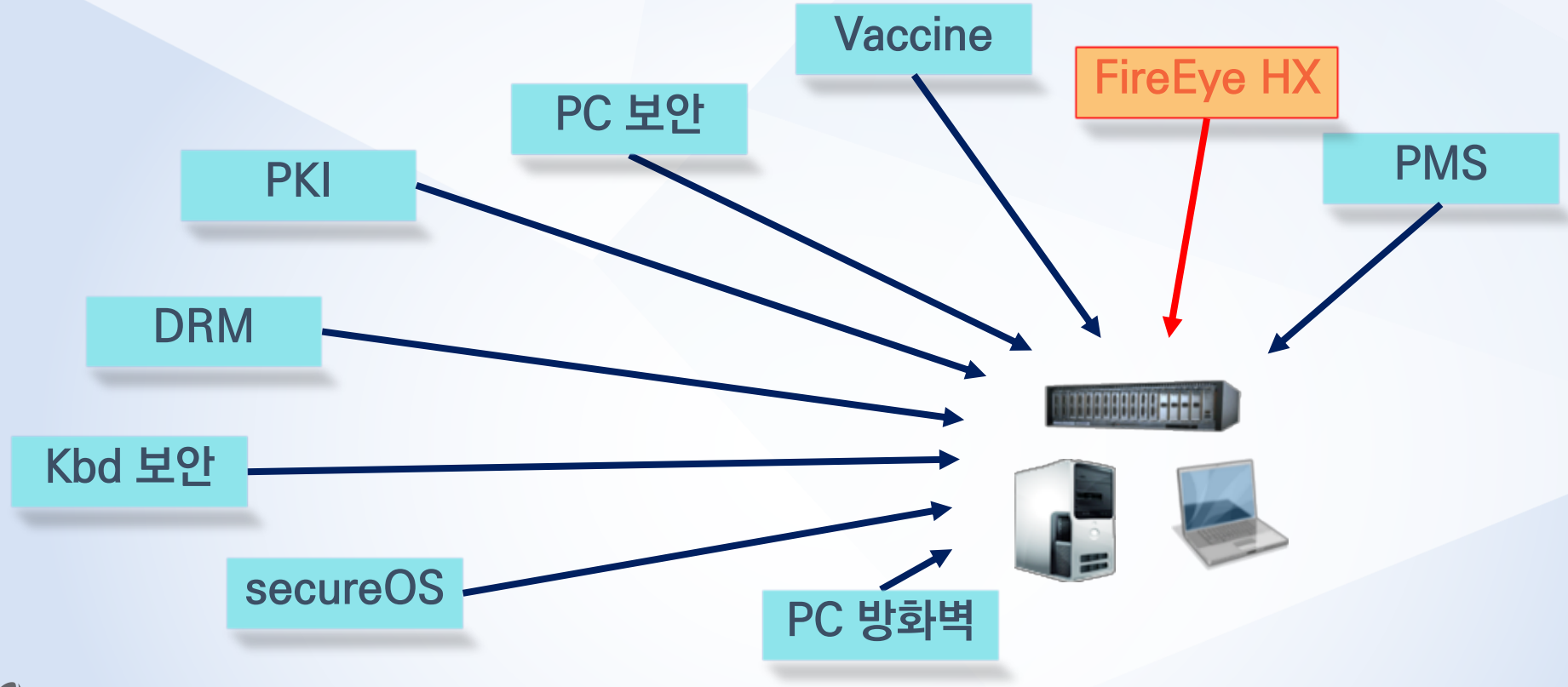
- OS에 대한 이해
- Application Service에 대한 이해
- Security Pre-Check(호환성 검사)
- 장애 대응
- Security Domain 지식
- 기타

1. OS에 대한 이해

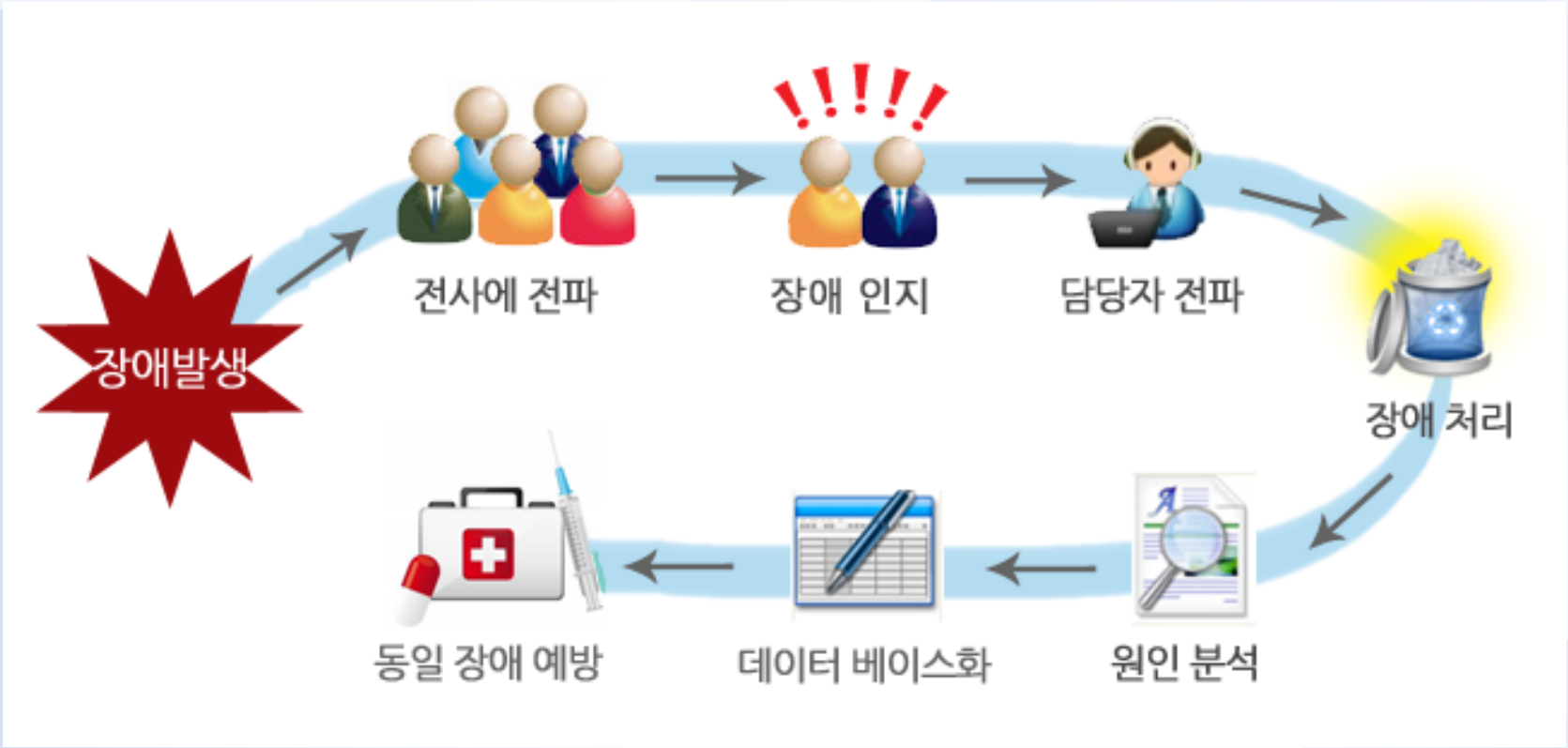


2. Application Service에 대한 이해

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
	정보통신산업 진흥법	정보통신산업 진흥법 시행령	정보통신산업 진흥법 시행규
	정보보호산업의 진흥에 관한 법률	정보보호산업의 진흥에 관한 법률 시행령	정보보호산업의 진흥에 관한 법률
	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 등 법률 시행규칙
	정보통신기반 보호법	정보통신기반 보호법 시행령	정보통신기반 보호법 시행규
	국가정보화 기본법	국가정보화 기본법 시행령	국가정보화 기본법 시행규
	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 등 법률 시행규칙
	위치정보의 보호 및 이용 등에 관한 법률	위치정보의 보호 및 이용 등에 관한 법률 시행령	-
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
	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 Comma

You can use the Cisco IOS CLI to enter the
To enter the Cisco IOS commands manuall

1. Log on to the switch through the Con
   port.

   See Connect a Terminal or Compute
   more information.
2. If you use the Console port, and no ru
   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
   configuration is present, go to the ne
3. When the user EXEC mode prompt a
   and the enable password, if one is c
   example:

   Switch> enable

   password: *password*
4. Enter config mode by entering the co
   the following example.

   Switch> config terminal

   Switch(config)#

SentryAPT

2.1.3 Mac

SentryAPT V1.0
normal and abnor

Process #1

Process #1

[Figure

As shown in the
systems and sy
Continuously lear
system. If you id
behavior, it is c
considered an AP

In addition to the
program, user's h
network traffic a
systems are prov

sga SGA Solutions Co., Ltd.

SentryAPT

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.

The log types that can be set are as follows.

Log Type		Description
Unix Log	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.

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, 내PC지키미
- 통합 에이전트 및 통합 PC보안 제품

자체 악성코드 분석팀 운영

개발팀과 독립적인 자체 악성코드 분석팀 운영

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

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

위협분석, 대응을 위한 인텔리전스팀 운영

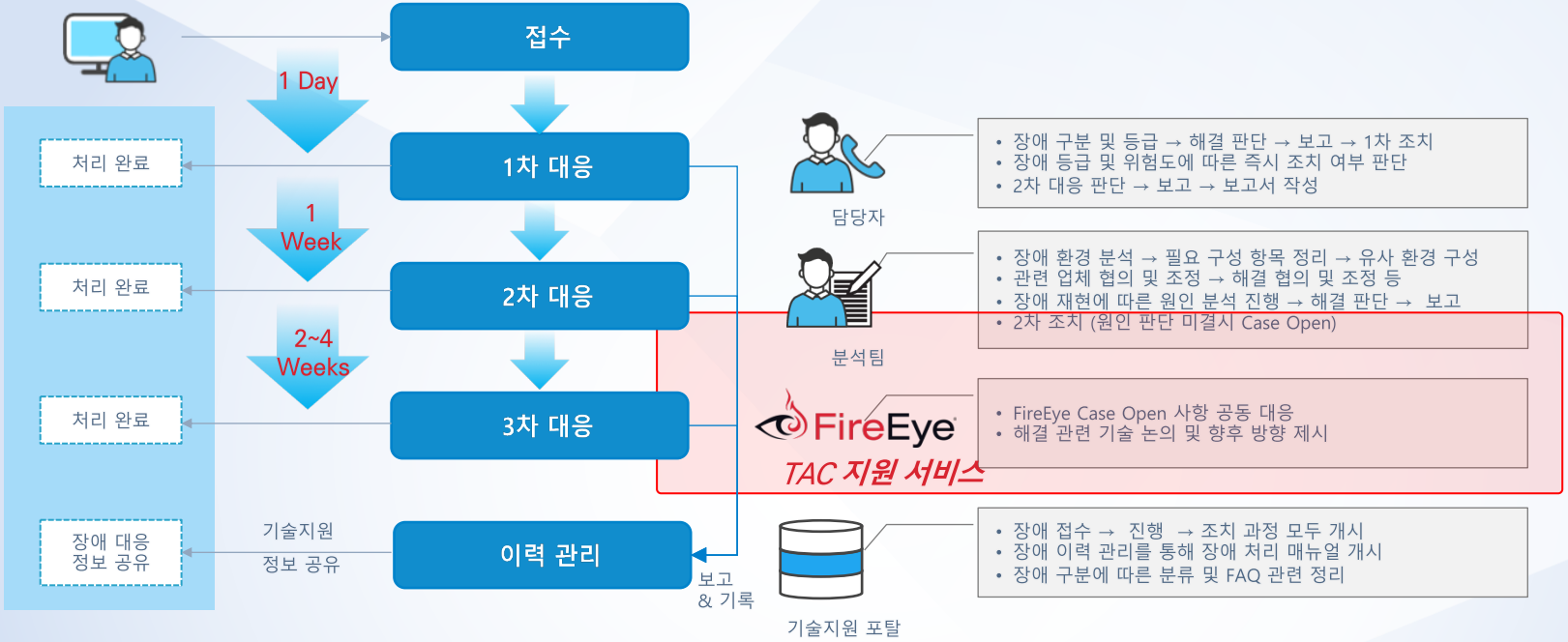
위협분석/대응의 인텔리전스팀 운영

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

2. Endpoint 보안솔루션 보유

서버 보안	응용보안	시스템보안	Infra 보안
RedCastle › 정확하고 강력한 사용자 행위기반 서버 접근통제 제품	**TrustChannel FIDO** › 사용자의 생체정보 등을 통하여 사용자 인증을 수행할 수 있는 차세대 인증 솔루션	**VirusChaser** › 사용자PC 및 서버에 대해 바이러스 및 악성코드, 웜 등을 탐지하고 치료하는 백신 솔루션	**SentryAPT** › Bigdata 및 Machine Learning 기반의 APT 공격 탐지 시스템
AuthCastle › 서버 접근(접속) 시 기본 ID / Password 외에 추가 인증을 제공하는 2차 인증 솔루션	**TrustCertificate** › 증명서 등의 문서에 대해 법적 효력이 있는 문서를 생성하며, 이를 검증할 수 있는 솔루션	**PatchChaser** › Windows 기반의 사용자 PC에 대한 보안 패치를 일괄 적용하는 제품	**SentryIntelligence** › Cloud, DNN 기반의 악성코드 분석 시스템
AuditCastle › 서버 접근에 대해서 이상 또는 비정상 행위에 대한 로그 수집, 저장 및 분석할 수 있는 제품	**TrustDocument** › 종이문서의 소모 비용을 절감하고, Paperless 비즈니스 환경을 구축할 수 있는 솔루션	**DaLoc** › 인터넷 PC의 사용자 작업에 의하여 생성된 문서 자료의 강제 삭제 솔루션	

3. 장애 대응 Process



에스지에이솔루션즈(주)

4. QA(Quality Assualance)

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

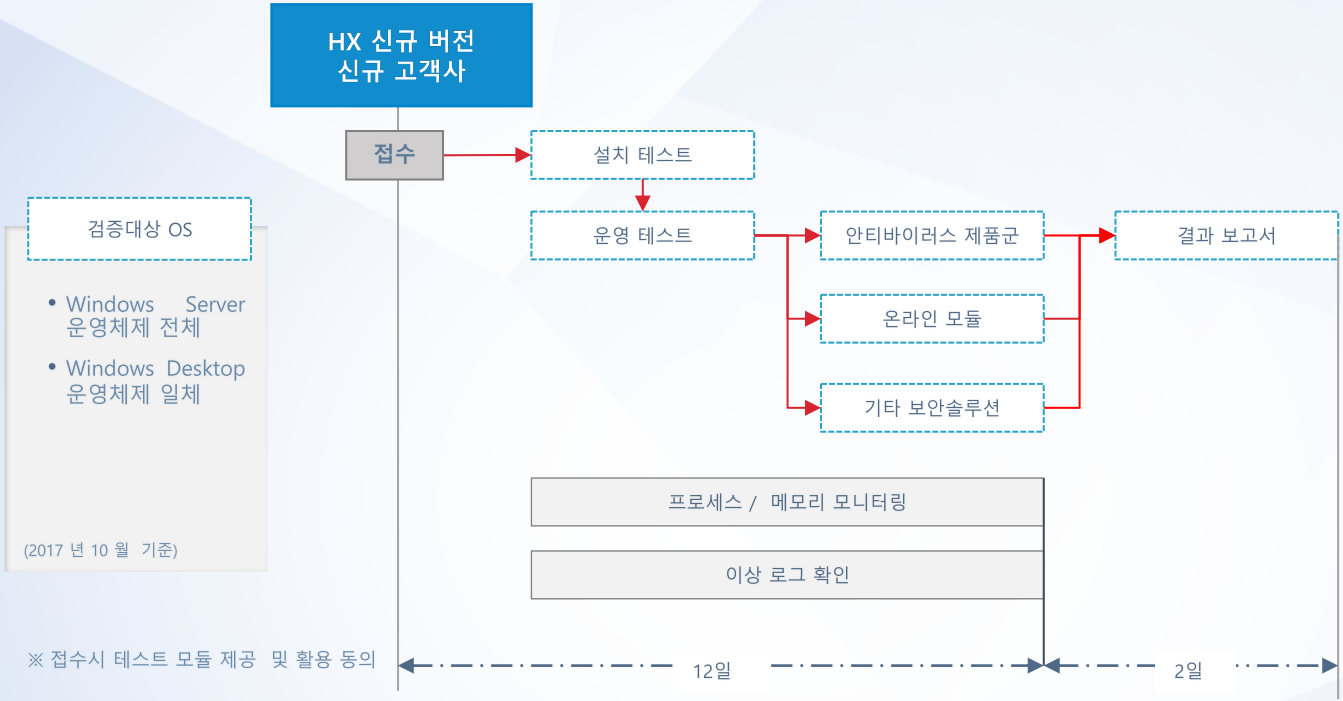
- 이상유무 판단
- 시험결과서 작성
- 배포 협의

배포

- 단계별 배포 진행

4. QA(Quality Assualance)

2.QA Process



에스지에이솔루션즈(주)

4. Etc.

SGA SOLUTIONS CC CERTIFICATION

CC 인증

인증제품명	인증일
Redcastle V4.0 for Redhat Enterprise Linux 7	2015-10-16
Patch Chaser 2.1	2015-10-16
RedCastle V4.0 for Solaris 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 Solaris 10	2014-07-31

SGA SOLUTIONS GS CERTIFICATION

GS인증

Korea's first operating system authentication security check

국내최초 운영체제 보안시스템 인증을 확인하세요

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 Solaris	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
• Administration Guide - System Administration Guide - System Security Guide - User Guide • Reference Guide • Release Note	• Administration Guide • Deployment Guide • Support Guide • Release Note

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

5. Endpoint 보안 기술 확보

Base Security Technology

기술력

다양한 영역의
보안 **원천기술** 보유

- **시스템 보안**: 커널핸들링, 다양한 OS, 감사/추적
- **응용 보안**: PKI, FIDO, 전자문서
- **PC 보안**: Agent 기술, 파일핸들링, Agent 통합
- **통합 보안**: 통합관리, 서버연계, 대용량처리

신기술 선도

보유 기술 기반의
신기술 대응
및 적극적 **사업 창출**

지능형 위협 대응	Security Intelligence
차세대 인증	Security Integration
Cloud / IoT	Platform

성장성

기술 기반의
신성장 동력의
미래 동반자

- **고객의 자산 보호**
- **파트너 동반성장 극대화**
- **Business based Technical Partnership**

Thank You !