금융 IT의 핵심 보안 솔루션 및 고객사 운영사례

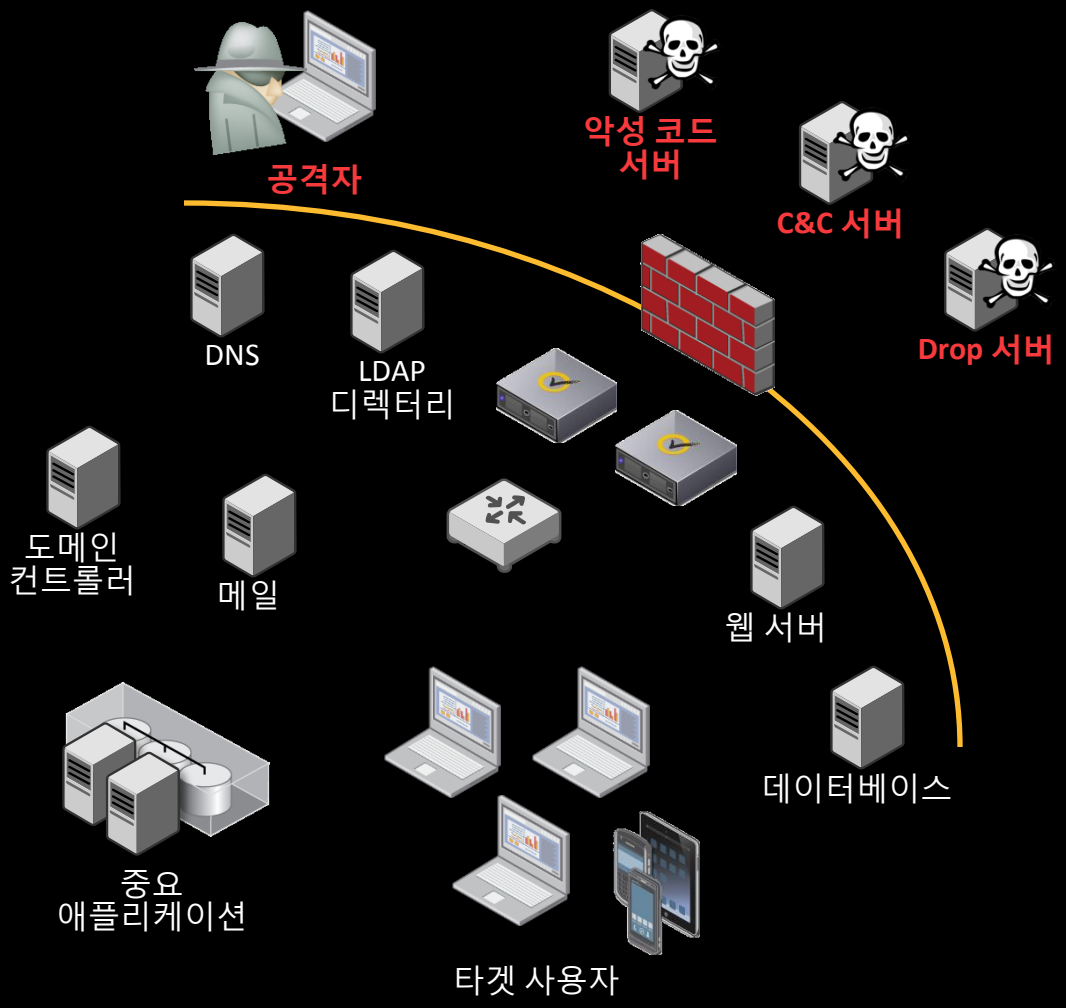
2013년 12월 12일

Symantec Korea

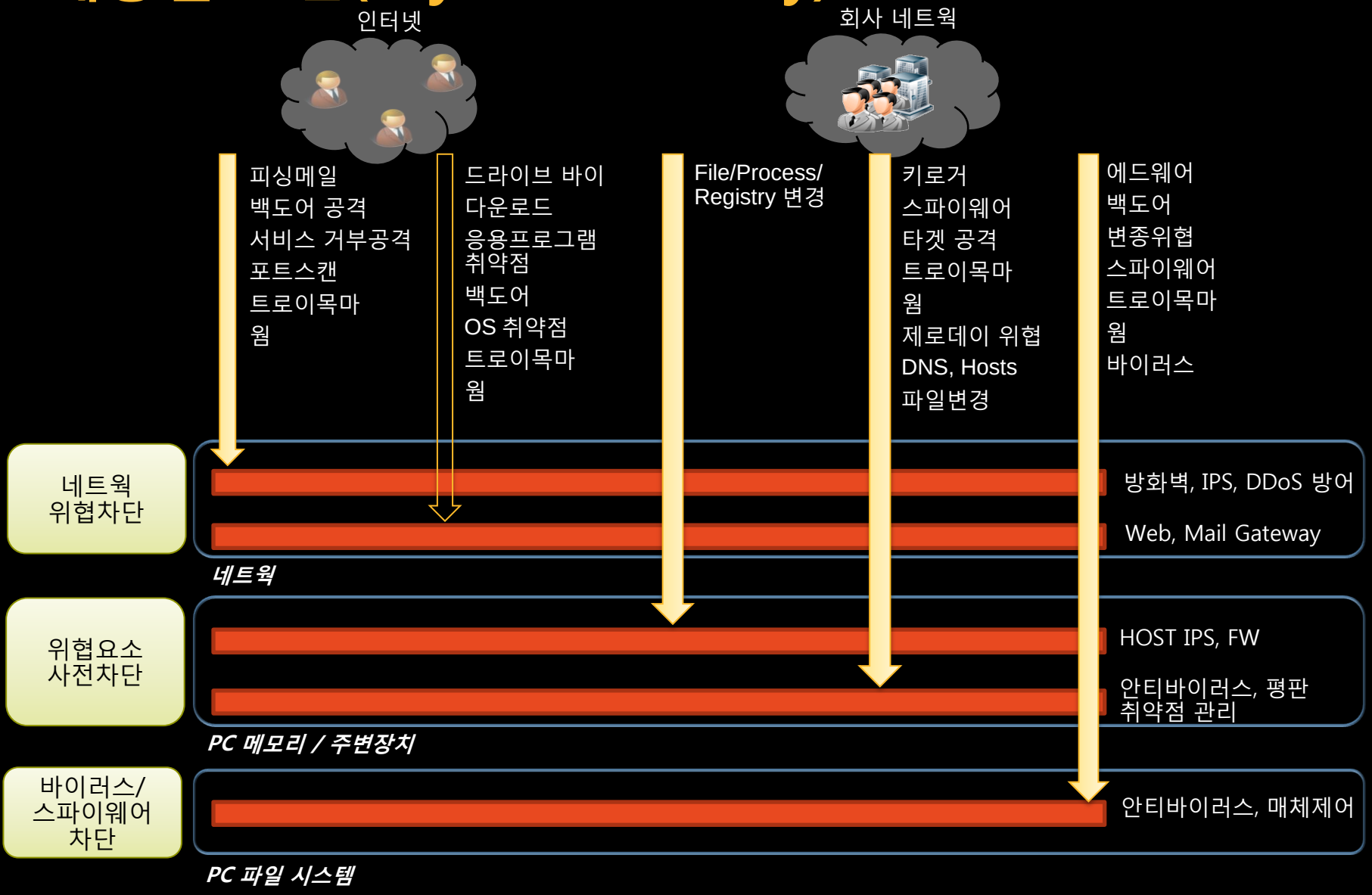

2013년 보안 화두
APT
3.20 Cyber Attack
메모리 해킹
망분리
BYOD
가상화
스미싱
Big Data
개인정보
6.25 Cyber Attack
통합로그관제

현재의 보안 전략

- 위협중심
- 위험관리
- 데이터 중심



계층별 보안(Layered Security)



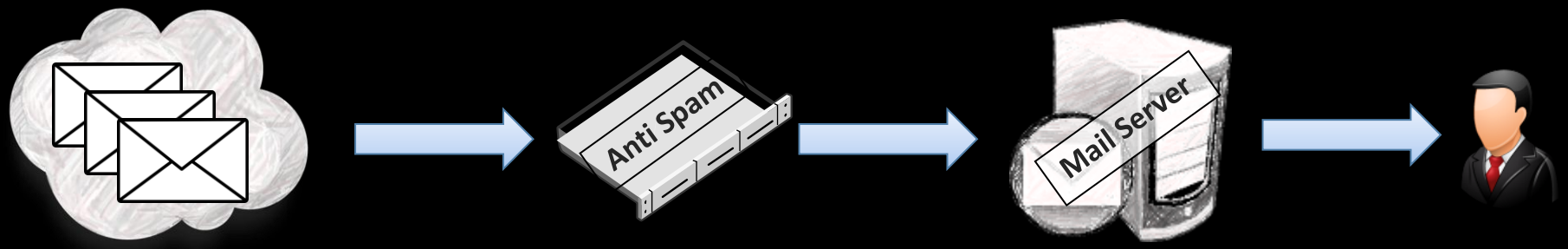
진화하는
보안기술

Solutions

Direction

Symantec

메일 보안 시스템의 진화(Messaging Gateway)

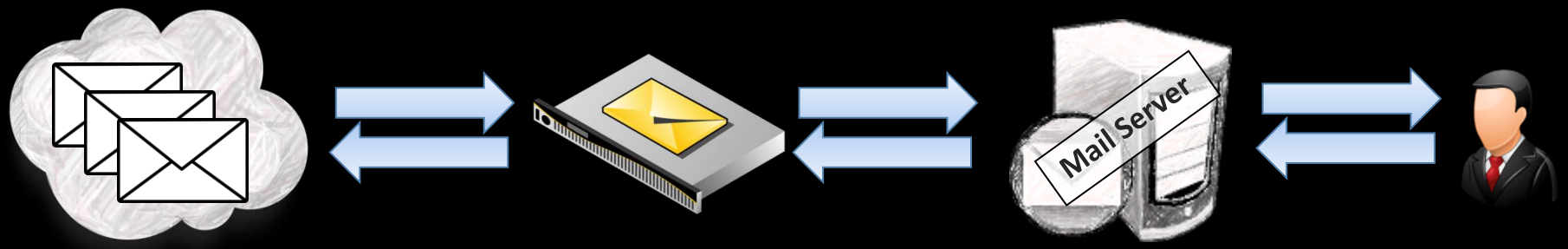


1 Spam 메일 차단
2 첨부된 바이러스 차단(전통적 바이러스 차단엔진)

문제점

1 신종, 변종 악성 첨부 파일에 대한 차단 불가
2 Zero-day 취약점을 이용한 공격에 대한 차단 불가
3 개인정보 보호법, HIPPA, PCI 등의 규제에 위배되는 메일 발송에 대한 차단 불가
4 URL 기반의 APT 공격에 대한 대응 불가

메일 보안 시스템의 진화(Messaging Gateway)



1 Spam 메일 차단
2 공격 메일에 대한 스로틀링
3 첨부된 바이러스 차단(Symantec Antivirus 엔진)
4 첨부된 Active Contents 제거
5 메시지 내부의 URL 분석
6 아웃바운드 메일에 대한 Compliance 확인
7 아웃바운드 메일에 대한 개인정보 확인

Disarm 기술 소개

Messaging Gateway 10.5

- 이메일에 첨부된 문서를 통해 악성코드 공격 시도 증가
  - 주로 APT 공격을 위해 Spear Phishing email을 사용
  - 악성행위를 포함하거나 취약점을 이용한 이메일 타겟 공격에 대응필요

Symantec의 새로운 기술 "Disarm" : 첨부된 문서에 대한 재구성을 통해 이메일 기반의 공격 차단

대상 파일 : MS Office documents, PDF documents

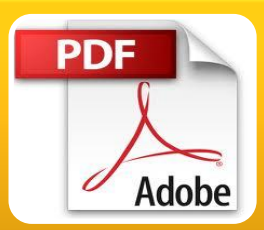
주요 기능

- VBA 코드 제거(매크로 혹은 Active x 컨트롤에 사용됨)
- 악의적으로 삽입된 콘텐트 제거
  - 실행 파일
  - 플래쉬(Flash object)

MS Office, Adobe Acrobat 취약점

Disarm – 지원 문서 포맷

Messaging Gateway 10.5



- 자바스크립트와 "실행 " 액션 제거
- Flash 와 같은 임베디드 objects/파일을 제거 혹은 대체
- XML Forms Architecture (XFA) objects 제거

- 메크로 제거
- Flash 와 같은 임베디드 objects/파일을 제거 혹은 대체
- PDF, Image 와 같은 지원되는 임베디드 object 에 대한 재구성

- 메크로 제거
- 임베디드 Flash, EXE 제거/대체
- 지원되는 object 에 대한 재구성(PDF, OLE inside OLE, …)

시만텍 보안 연구소에서 113개의 Zero-Day Exploits 에 대한 분석 진행

-Common Vulnerability and Exposure (CVE) database

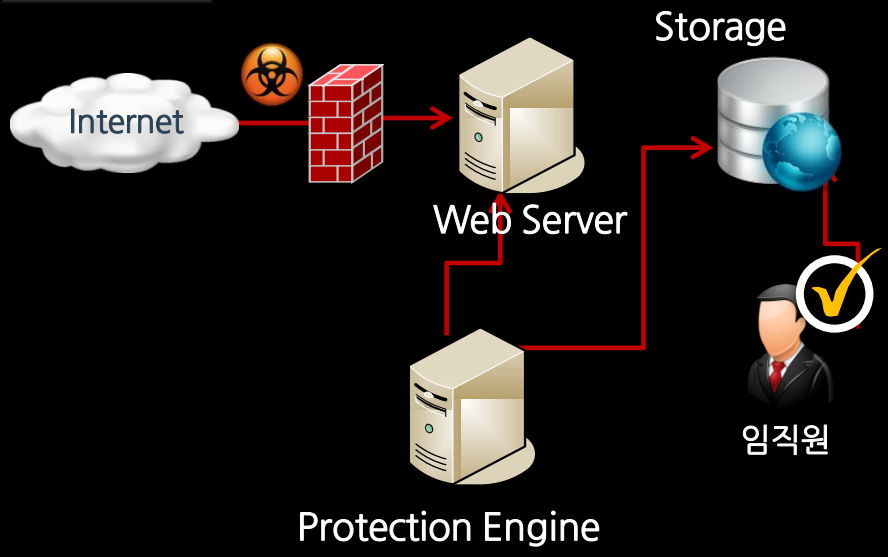
Disarm 98% 의 exploits 차단

클라우드, NAS 보안 시스템의 진화

시만텍 Protection Engine은 고객사의 네트워크를 통하여 클라이언트PC, 스토리지에 유입되는 다양한 악성코드의 감염 위협으로 부터 시스템을 안전하게 보호합니다.

As-Is

To-Be



문제점

시스템의 무결성 여부를 확인할 수 없는 불특정 다수로 부터 파일 유입으로 인한 임직원 PC를 포함한 사내망이 보호되지 않음

1. 웹서버에 저장되는 파일에 대해 **1차 검역**
2. 임직원이 요청하는 파일에 대해 **2차 검역**
3. 임직원 PC에 설치된 백신으로 **3차 검역**

파일의 유입 및 전달 과정에서 다중검역 수행으로 안전한 시스템 및 사내망 유지

Protection Engine 소개

Protection Engine 7.5

내,외부 인프라 환경에 오픈되어 있는 Web, File, NAS, Mail서버 등에 대한 사용자 접근에 따른 파일의 안전성에 대한 검사를 통하여 악성코드로부터 기업 내부의 주요 데이터 및 네트워크를 보호

서버 기반의 악성코드 검사기능
Symantec Award Winning AntiMalware Engine

응용프로그램,
URL 및
File Access

NAS, Web Proxies, custom application integration

ICAP, RPC Protocol

Protection Engine

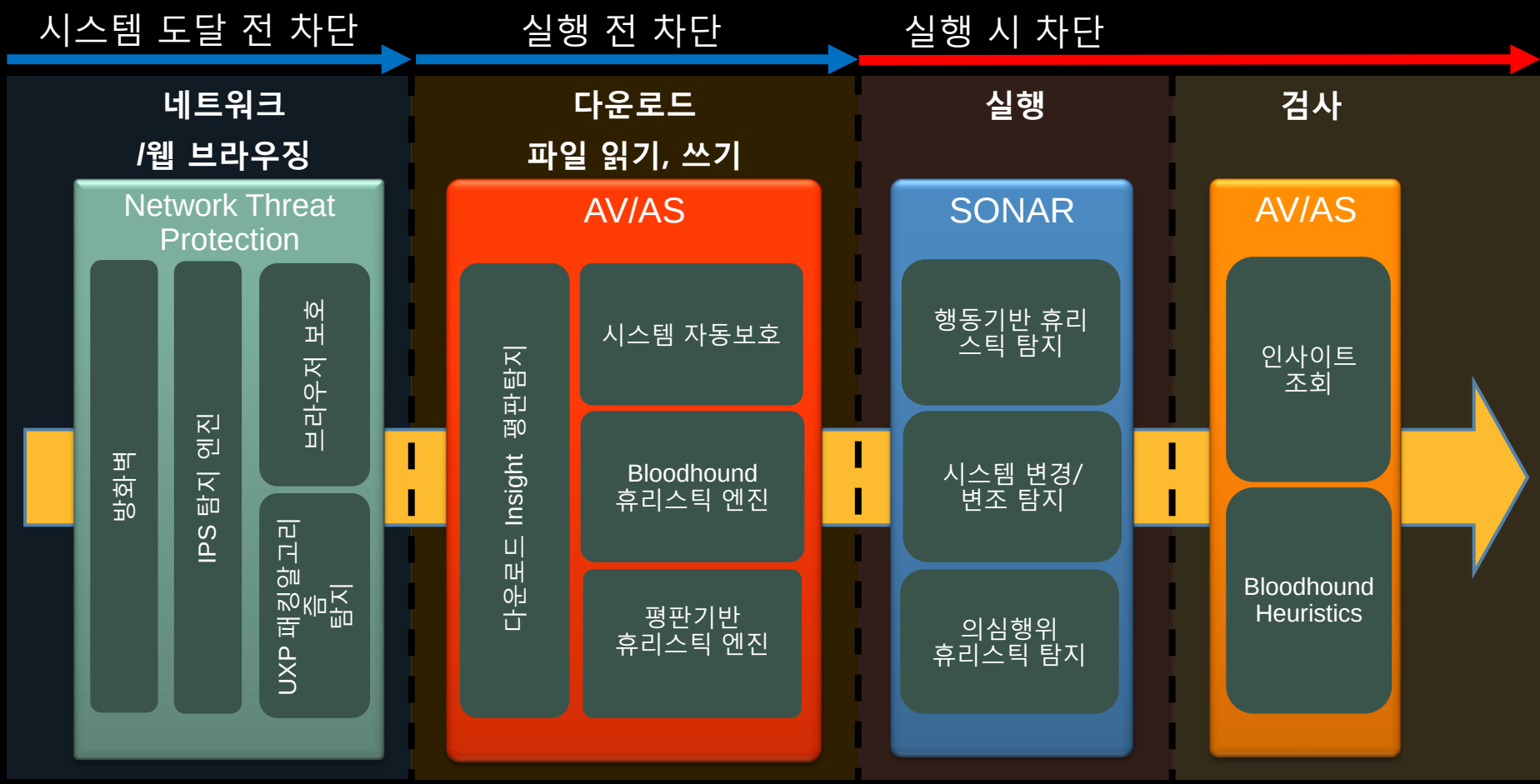
- 감염된 파일/웹 컨텐츠에 대한 결과값 반환
  - 악성코드 이동/격리 및 차단
  - 웹 컨텐츠 차단
- 서버 기반 URL 필터링
  - RuleSpace Engine
- 3rd Party Application과의 연동
  - SDK included for C++, JAVA and .NET

Protection Engine 사용

Protection Engine 7.5

- Example scenarios:
  - 외부망으로 부터 파일이 유입되는 **망연계 솔루션**
  - 인터넷을 통해 외부 사용자로부터 파일이 유입되는 **WEB 서버**
  - 제조사 혹은 파트너사에서 파일이 유입되는 **ERP 시스템**
  - 외부 사용자로부터 파일이 업로드 되는 **FTP 서버**
  - 비 윈도우 기반 시스템에서 제공되는 **파일 공유 시스템 (Samba)**
  - 안티 멀웨어 검색과 같은 더 나은 서비스를 제공하고자 하는 **ISP, 모바일 네트웍 제공업체**
  - **보호되지 않는 기기**에서 접근하는 사용자 보호(Mobile, Home User)

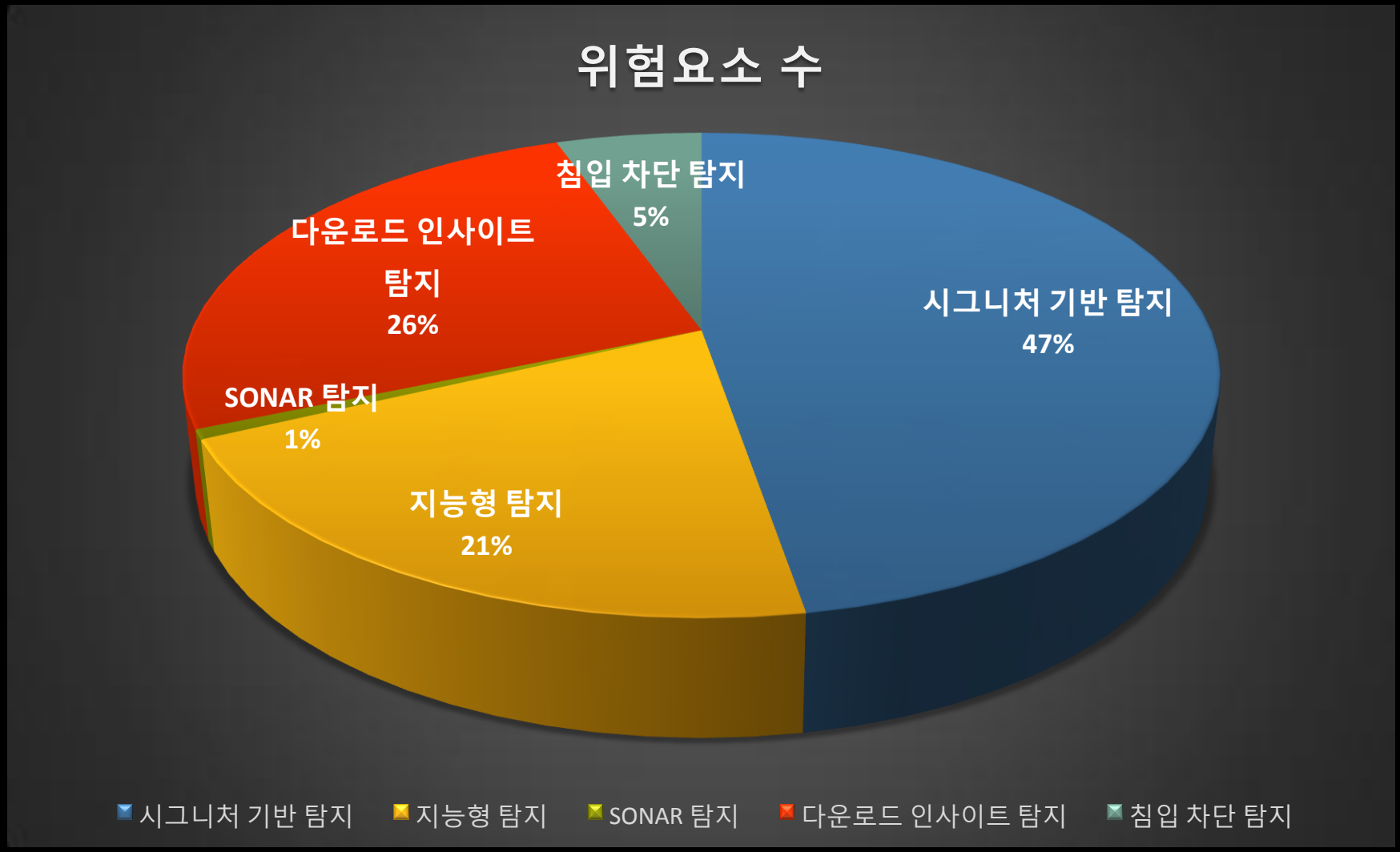
통합 보안 솔루션의 진화(Endpoint Protection)



Protection Mechanism

Endpoint Protection 12

고객사례 – 보호 기술별 위험 분포



47.3% / 52.7%

Network threat protection (IPS + Browser IPS)

Endpoint Protection 12

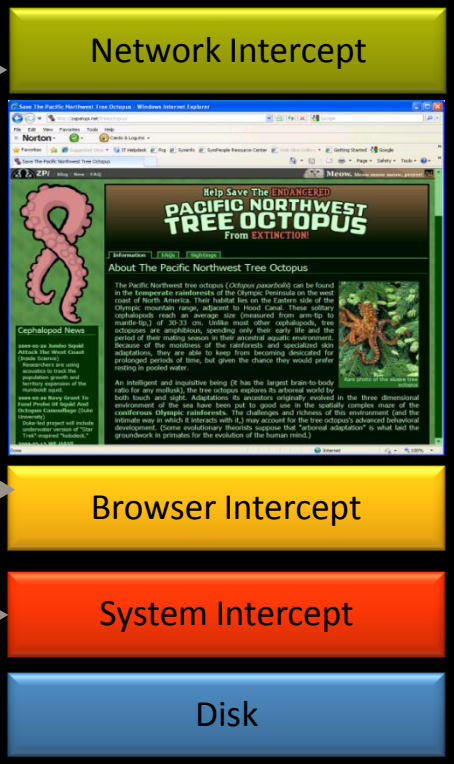
- 네트웍을 통해 시스템에 침투하는 멀웨어의 공격을 탐지하고 차단
- 새로운 취약점이 발견될 때 마다 빠르게 업데이트 하여 대응

Network IPS

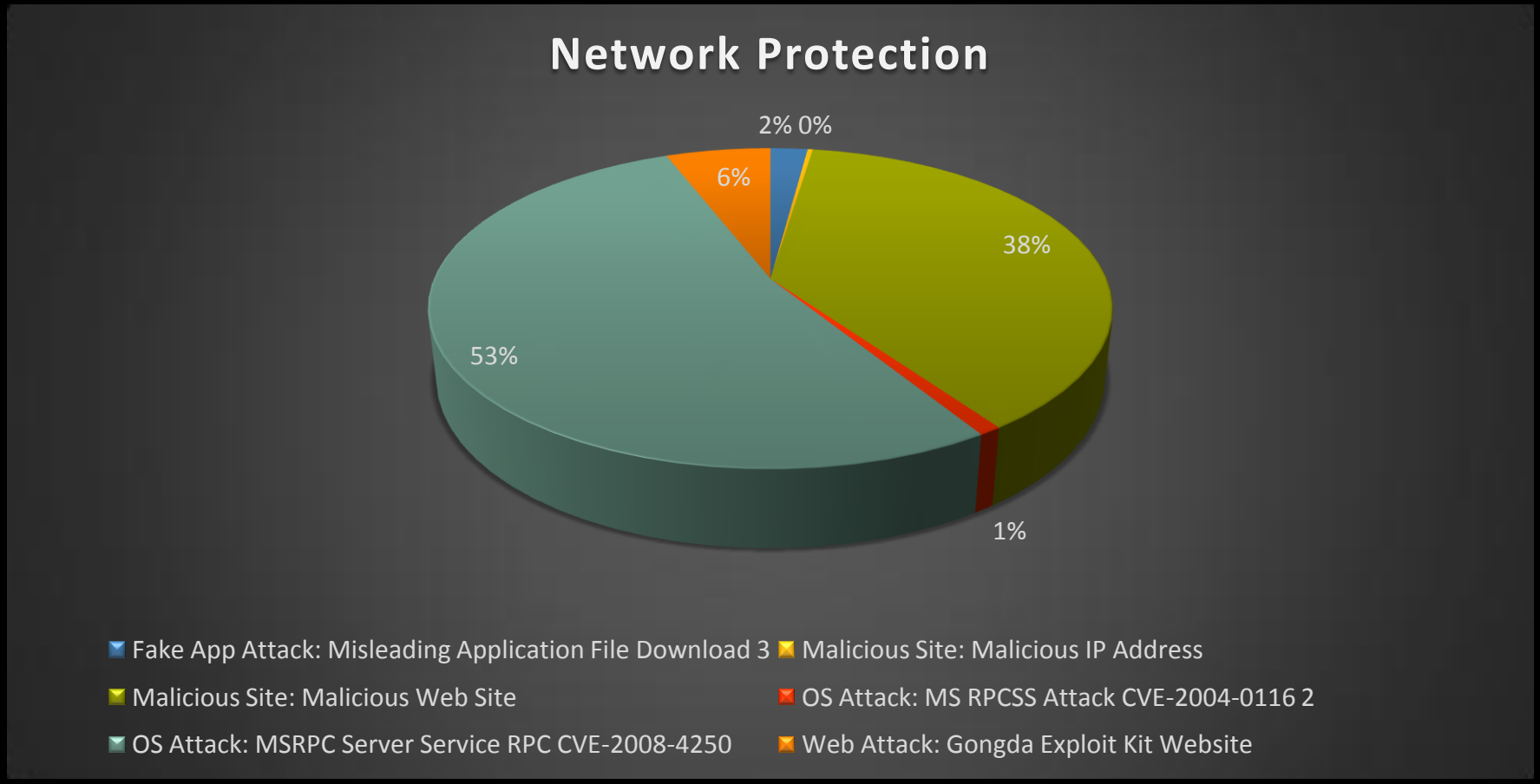
- 모든 네트웍 트레픽에 대한 OS/APP 취약점에 대해 시그니처 기반으로 대응하는 기술
  Intercept: Network traffic
- Example: PDF reader, Windows Media Player, QuickTime, dropbox…

Browser IPS

- 브라우저에 대한 Zero-day 공격에 시그니처리스 기반으로 대응하는 기술
- Intercept: Browser and System API calls
- Example: Flash, Java based exploits



고객사례 - IPS



단 하루동안 2,800여건의 공격을 차단

행동기반 탐지 - SONAR

Endpoint Protection 12

새로운 행동기반의 탐지엔진

- 기존 TruScan 엔진보다 10배이상 향상된 효과

Behaviors
1390

행동기반의 새로운 위협에 적극적 감지

- 제로데이 탐지 : Hydraq/Aurora
- TidServ 와 같은 복잡한 Rootkit

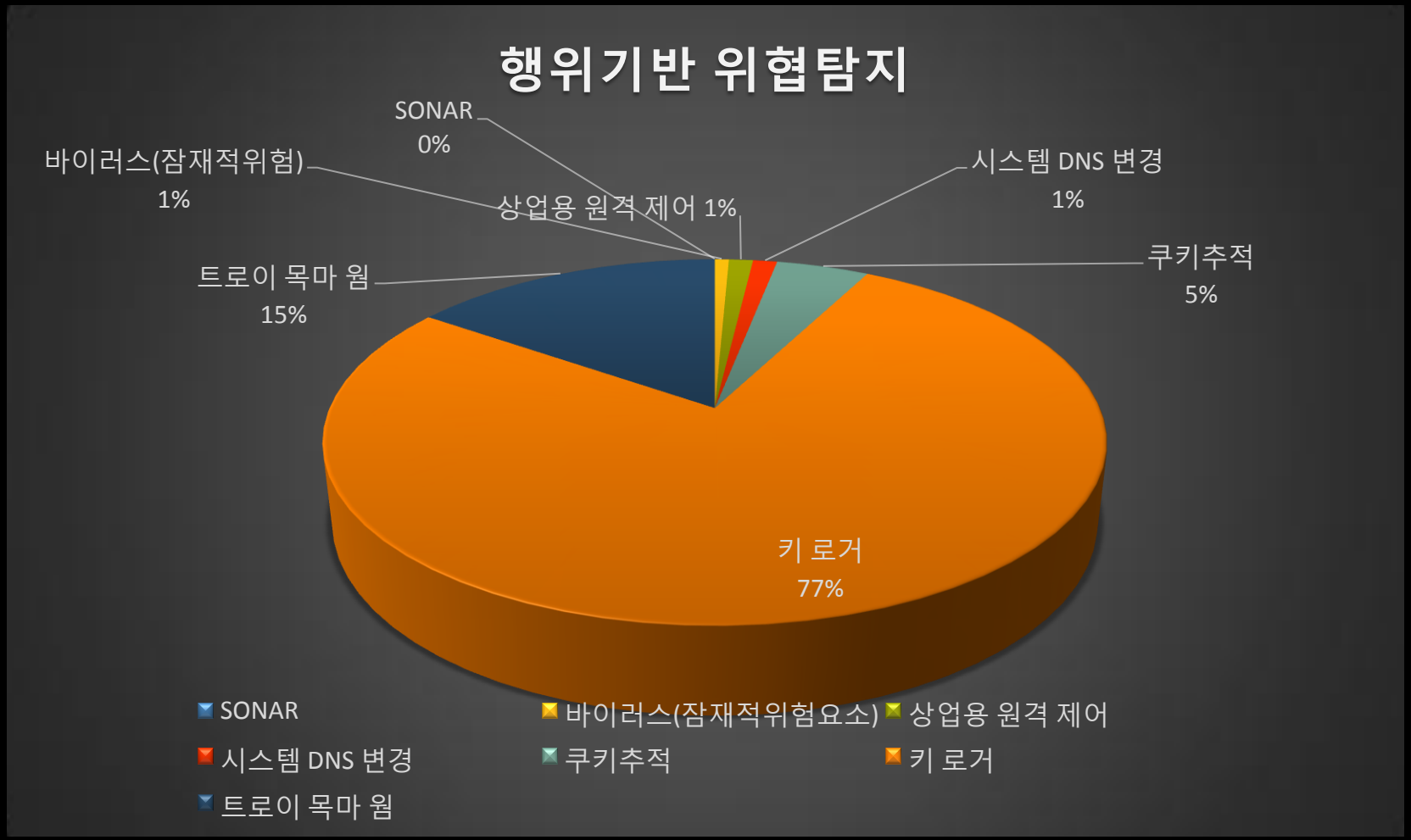
안티바이러스 엔진과 같은 정의파일 기반

- 라이브업데이트를 통한 최신 보호 자동 업데이트

높은 성능의 실시간 엔진

- 발생되는 모든 행위들은 모니터링되고 평가됨
- 퍼포먼스에 영향을 거의 미치지 않음

고객사례 - SONAR



1개월간 16,000 건 발생 – 자동 샘플제출

진화하는
보안기술

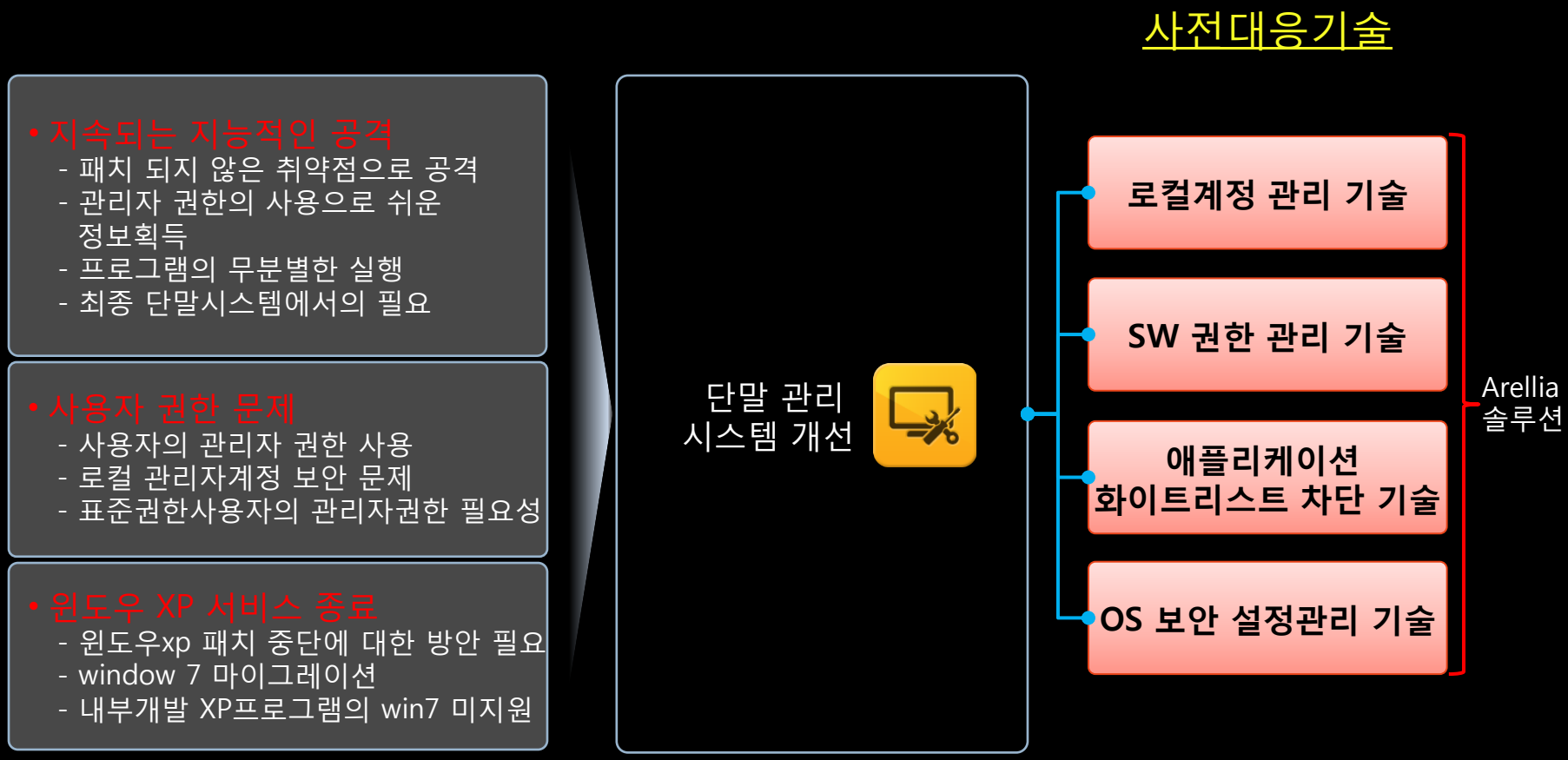
Solutions

Direction

Symantec

공격 사전대응기술

- Zero-Day, APT, 타깃 공격 등 지능적인 보안 위협에 대한 사전통제적인 관리기술이 필요함



Whitelist 기반의 보안 적용 사례 및 특징

1 의료장비등 특수용도의 서버
2 산업용PC, POS등 일부 시스템

*특징
- 설치되어 있는 어플리케이션이 적음
- 파일의 변동이 자주 일어나지 않음
- 가용한 리소스가 적음
- 상대적으로 보안성이 높음
- 관리가 어려움

Whitelist 기반의 보안 운영의 어려움

1 신규 프로그램
2 보안 취약점
3 성능향상
4 기능개선
5 사용자마다 다른 프로그램 요구사항

*문제점

- 시스템 업그레이드를 위해 USB등의 장치 사용
- OS, 어플리케이션에 대한 패치 없이 내부 네트웍에 연결됨

애플리케이션 화이트리스트 차단(Arellia)

- 블랙리스트의 반대 개념으로 규정된 화이트리스트에 없는 모든 파일의 실행을 차단 하여 외부 위협으로 부터 시스템을 보호

- 소프트웨어 무단설치/실행 차단
- 등록되지 않은 알려지지 않은 소프트웨어의 차단(화이트리스트)
- 표준 시스템 등 신뢰 할 수 있는 출처에 대해 자동 승인하는 화이트리스트 정책을 적용
- 등록된 애플리케이션 위 변조 시 차단

애플리케이션 화이트리스트 등록 모델

- 유연하게 화이트리스트를 작성

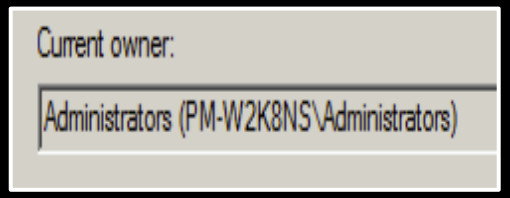
skH4EpLu0pU687dBQ5sb

파일 해쉬값 수집 및 반영

내부 표준 시스템에 설치된
파일의 자동 반영

관리시스템에서 배포되는 소
프트웨어 패키지를 자동반영

디지털 인증서로 서명된
파일의 자동 반영



특정 파일 소유자가 실행
하는 파일을 자동 반영

제조사 이름
또는 파일 속성 값을 등록
하여 반영

사용자 권한 제한(Arellia)

관리자 권한 상승 및 제한 기능

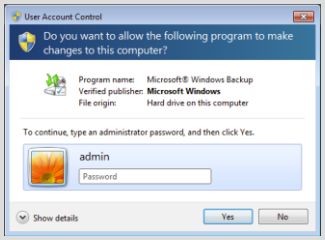
- 웹 브라우저 나 이메일 클라이언트 등 외부에서 공격이 유입되는 프로그램에 대한 권한 제한
- 표준 사용자로 구동 시 관리자 권한이 필요한 기능/애플리케이션을 위한 권한 상승

권한 제한 필요

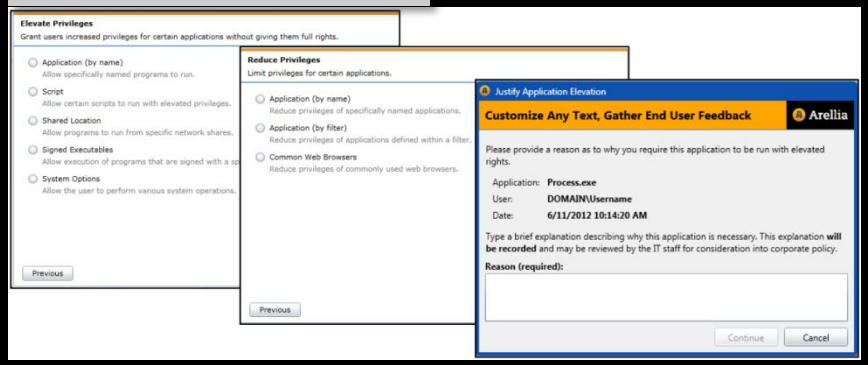
- 관리자 권한을 통해 외부공격의 유입수단이 되는 경우, 관리자 권한으로 실행됨
  - 웹브라우저
  - 이메일클라이언트
- 시스템의 설정값 등의 변경

권한 상승 필요

- 표준 사용자로 할 수 없는 작업
  - 컴퓨터백업
  - 시간 변경
  - HDD 조각모음
  - 언어 설치
  - 드라이버설치
  - 실행에 관리자 권한이 필요한 SW
  - 관리자권한이 필요한 소프트웨어 설치(Adobe Reader, java, WinZip등)



권한상승/제한/사용자피드백



이점	내용
보안강화	• 악성코드가 관리자 권한으로 실행되지 않음 • 사용자가 보안 설정을 변경 할 수 없음
운영 비용 감소	• 시스템 안정성 강화로 helpdesk등 지원비용 감소 • 애플리케이션 권한 상승은 IT지원 요구를 감소 시킴
책임 감소	• Software compliance 준수

진화하는
보안기술

Solutions

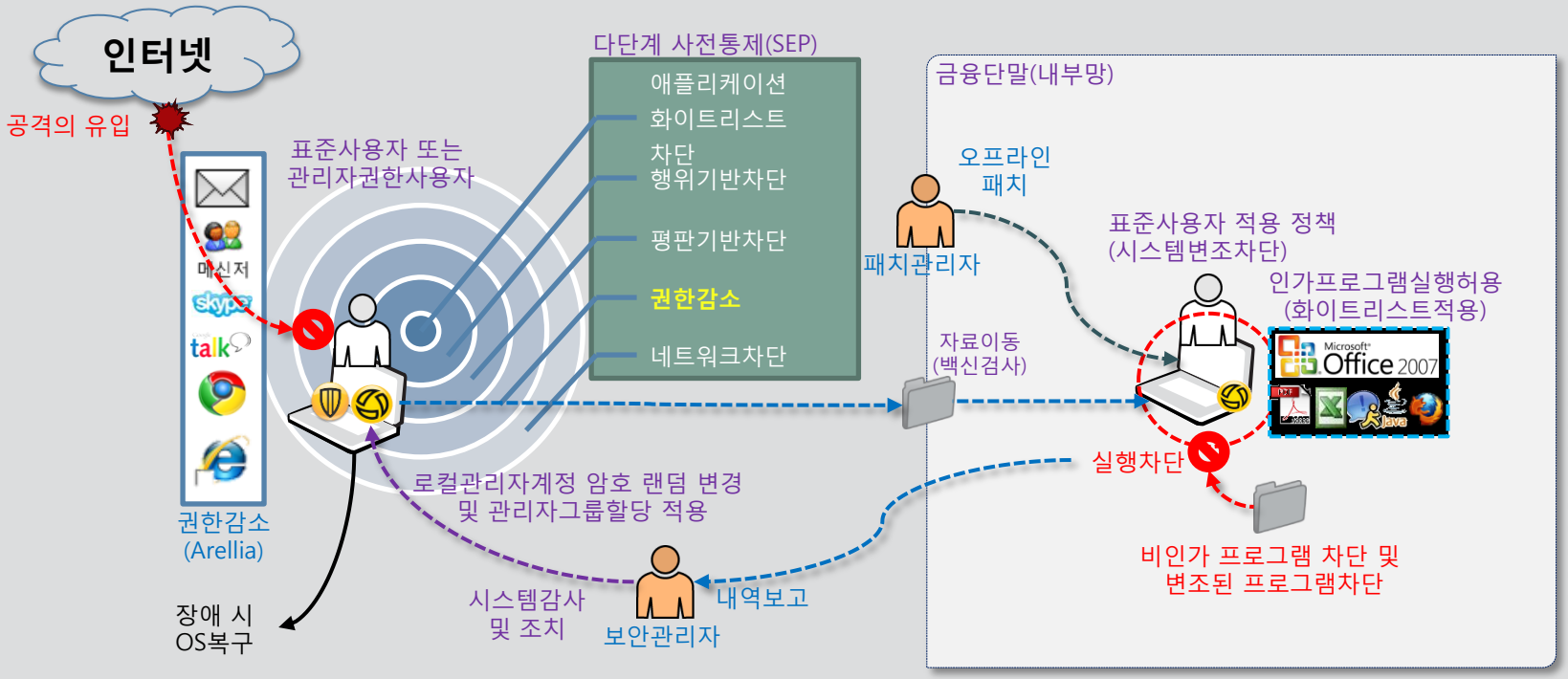
Direction

Symantec

금융단말 보안 적용방안

- 인터넷 시스템은 다양한 사전 보호 수단의 적용
- 단말 환경에서는 표준환경 유지 및 보호 적용

금융단말 보안 구성 사례



감사합니다!