SECUVE

Secuve TOS 소개

- 주요 기능 및 특장점 중심 -

2020. 09.

㈜시큐브

SECUVE

CONTENTS

1 Secuve TOS 소개

2 Secuve TOS 특장점 및 경쟁력

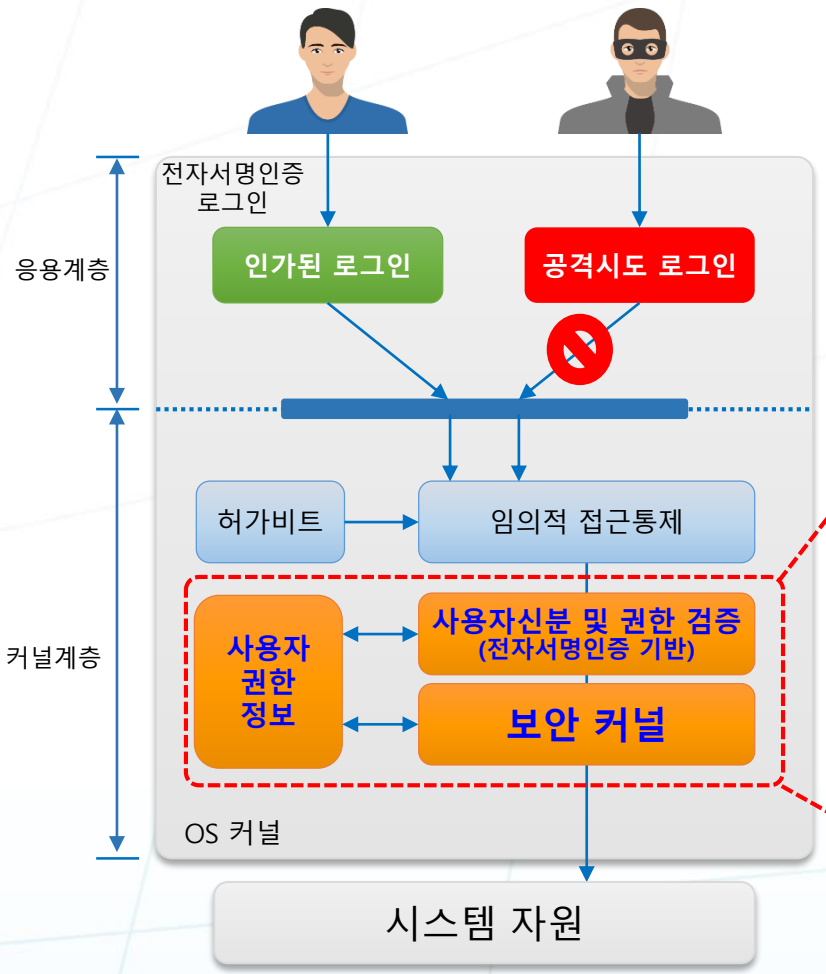
3 Summary

4 주요 고객사

1 Secuve TOS 소개

Secuve TOS Architecture

Core Technology



SECUVE TOS 보안 커널

전자서명 기반 사용자 인증

- X.509 v3 전자서명인증서 기반 사용자 인증

Access Control

- 역할기반접근통제(RBAC),등급기반접근통제(MLS), 접근제어목록(ACL) 등 다양한 접근통제 정책 및 메커니즘 지원

Monitoring & Audit

- 커널레벨 행위감사 (사용자, 프로세스)
- 실행파일 실시간 무결성 검사
- 파일/프로세스/네트워크 접근제어 감사

Prevention Features

- Session Blocking
- 서버 방화벽 (IPv6 지원)

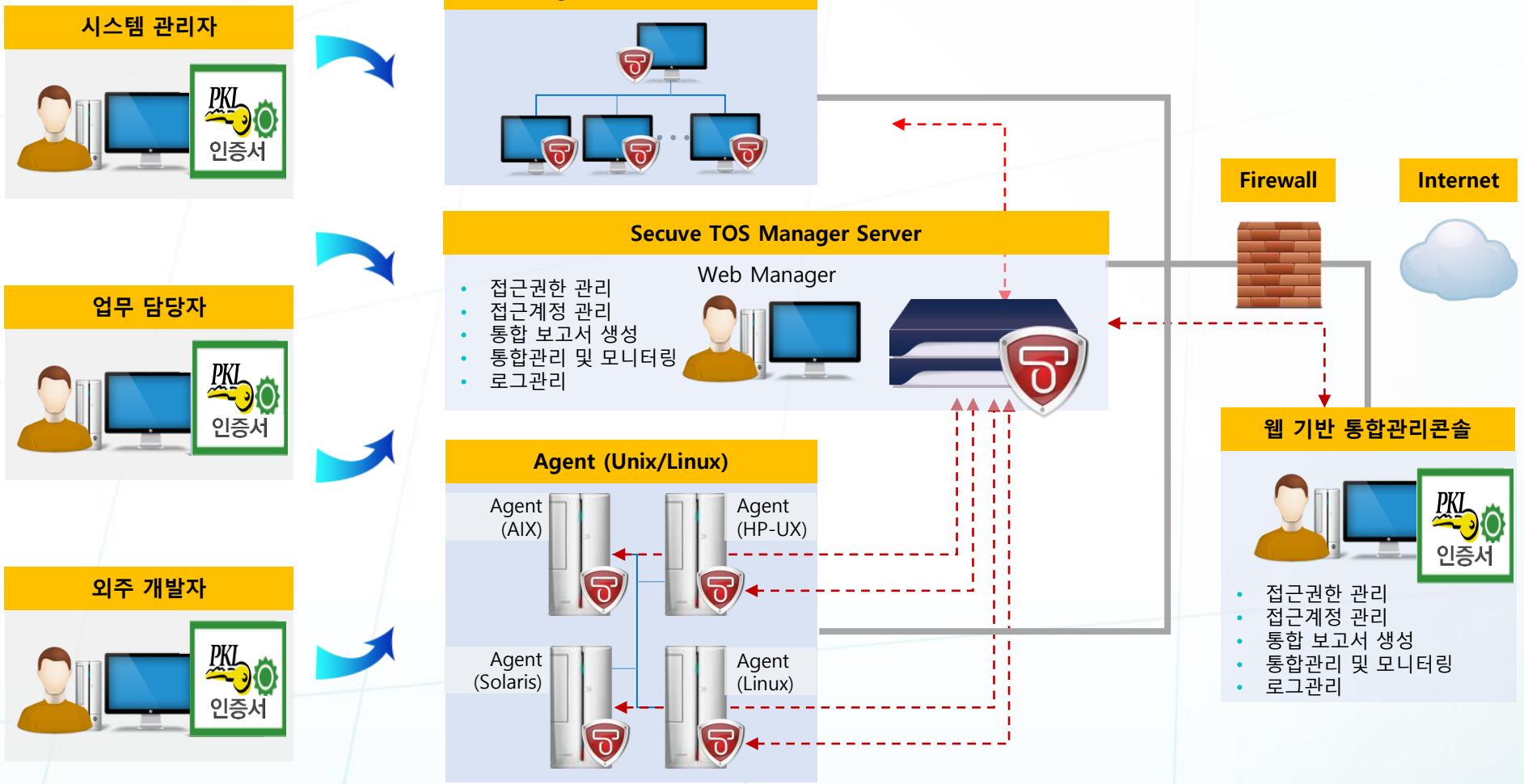
Self-Protection

- Kernel Sealing
- 제품 프로세스 및 설치디렉터리 보호

- 고도의 암호기술이 적용된 전자서명 인증 수행(2048 bits강도)
- OS 커널 레벨에서 사용자권한 정보를 검증하여 접근 및 행위를 통제 (불법 권한 획득 불가)

SECUVE

Secuve TOS Configuration



범례 Secuve TOS Agent

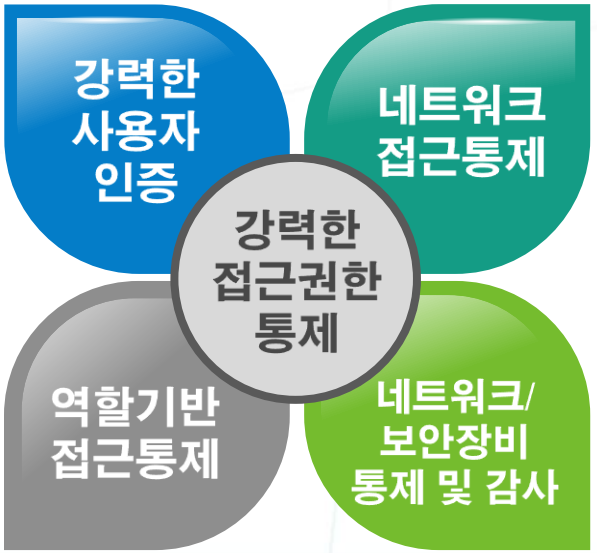
SECUVE

Secuve TOS 기능 요약 (1/6)

전자서명에 의한 강력한 사용자 인증

(PKI Based user Authentication)

- X.509 v3 국제 표준 준수
- 단순 ID/PW 인증의 취약점을 개선한 강력한 인증기능 제공
  (금융결제원 등 국내외 공인인증서 연동지원)
- PKI (공인인증서 연동)+ RBACK / MLS / MAC



네트워크 접근통제

(Server Firewall)

- 커널 레벨의 서버 방화벽 (Server Firewall) 기능제공
- IP, Service, Port 별 접근제어
- 경유지 제어
  (유·출입 패킷에 대한 IN/OUT-going 제어)
- 시스템에 유입되는 네트워크 불법침입 탐지 및 차단

역할기반의 접근통제

(Role Based Access Control)

- 사용자 역할에 근거한 강제적 접근통제
- 사용자 역할의 할당
  (X.509 v3 인증서에 사용자의 작업 권한 등록)
- 사용자 역할에 따라 23개 이상의 콜에 대한 강제적 접근통제

네트워크/보안장비 접근통제 및 행위감사

(Network/Security Equipment Access Control & User Activity Logging)

- 안전한 접속 Gateway를 제공하여 네트워크/보안장비에 대한 접근을 통제
  (CLI 터미널 방식/웹기반 UI 방식 모두 제공)
- Gateway를 통해 수행한 작업자의 모든 행위를 감사로그로 저장
- Gateway 접속 시 실사용자 확인을 위한 복합인증 수행

SECUVE

Secuve TOS 기능 요약 (2/6)

접근통제 및 침입탐지

- **전자서명 인증기반 사용자 신원확인(PKI Based User Authentication)**
  - X.509 v3국제 표준 준수
- **전자서명 인증과 다양한 접근통제정책 결합으로 강력한 접근통제 실현**
  - 복합인증을 통한 실사용자 확인 및 실사용자 기반의 접근통제 정책 지원
  - 다양한 보안정책 기반의 객체 별 접근통제
  - PKI인증 + RBAC/MLS/MAC
  - 우회 침입, 파일 위변조 및 정보 유출 방지
- 특권파일(setuid) 실행 통제 및 위변조 탐지
- 시스템 셧다운 제어
- 시스템 시간 변경 통제
- 접근통제 정책 관리 시, 파일 디렉터리 명에 와일드카드 문자 지원
- 윈도우 특화 시스템 자원 접근통제
  - 레지스트리 접근통제
  - 공유폴더 IP별 접근통제
  - 이동식 디스크 접근통제 (H/W ID 별 접근제어 가능)
  - 시스템 서비스 시작/중지 통제

제품 확장성 및 안정성

- 국내 최고의 품질과 다중 플랫폼 지원으로 안정적인 이기종 통합관리
- **Cloud Computing, 가상화 등 최신 IT 환경 지원**
- 통합계정권한관리 iGRIFFIN과의 연동 및 통합 운영 관리
- **설치, 패치, 업그레이드 시 시스템 재부팅 최소화를 통해 가용성 보장**

네트워크/보안장비 접근통제 및 행위감사

- 안전한 접속 Gateway를 제공하여 사용자별로 허용된 네트워크/보안장비에만 접근할 수 있도록 통제
  - **Command Line Interface 터미널 방식으로 관리하는 장비에 대한 접근통제** 기능 제공
  - **웹 방식의 User Interface 방식으로 관리하는 장비에 대한 접근통제** 기능 제공
- 안전한 접속 Gateway를 통해 수행한 **작업자의 모든 행위를 감사로그**로 저장
  - CLI 터미널 방식: 명령어 입/출력 감사로그
  - 웹 방식: 사용자의 행위에 따른 화면 캡쳐 감사로그
- 안전한 접속 Gateway 로그인 시 **실사용자 확인을 위한 복합인증(PKI, OTP 등)** 수행

Secuve TOS 기능 요약 (3/6)

계정 및 패스워드 관리 ***(Account & Password Management)***	• 관리콘솔을 통한 편리한 사용자 계정 / 로긴 / 패스워드 관리 - 계정 관리 : 사용자 계정 생성, 삭제, 추가 / 계정 사용기간의 지정 / 임시계정 등 - 로그인 관리 : 접근가능 IP 지정 / 사용시간 및 요일 지정/세션 제어 / 사용만료 기간 제어 등 • 다양한 패스워드 관리 정책 적용 - 조합규칙(쉬운 패스워드 불가) / 최근 암호 재사용 불가(History) / 사용 주기 / 암호 사전 등 • Profile을 통한 계정 유형별 정책 설정 • IP/시간/요일 등 다양한 조건을 통한 관리자 계정 전환(SU) 제어 (Unix/Linux 계열)
네트워크 접근통제 *(Server Firewall)*	• **자체 기술로 구현한 커널 레벨의 서버 방화벽(Server Firewall) 기능 제공** - TCP/UDP In-bound/Out-bound 접근제어 (IP/Service/Port별 접근제어 조건 지원) - 출발지 IP주소별 TCP Out-bound 제어 (경유지 제어) - 비인가 네트워크 서비스(Port) 사용 제어 (Port Bind 제어) - IPv6 지원
사용자 로그인 서비스 제어	• Telnet, FTP, SSH, rlogin, dtlogin, Winlogon, Console 등의 서비스에 대해 복합인증, IP, MAC, 호스트명, 시간, 요일, 기간 등에 따른 로그인 제어 기능 제공
권한 위임 (Unix계열)	• 특정 계정에게 허가된 기간 동안 지정한 명령어를 지정한 권한으로 실행할 수 있도록 권한위임 기능 제공
명령어 통제	• 사용자 전환(SU) 통제 (IP, 시간, 요일, 기간, 계정 및 계정 그룹 기반 통제 가능) • 위험명령어 통제 기능 제공 - 시스템 위험명령어 및 관리자가 등록한 위험명령어를 복합인증, 계정, IP, 시간, 요일, 기간 별로 제어
사용자 행위감사 (커널레벨 & 어플리케이션레벨)	• 특정 시스템 사용자의 커맨드 타이핑 실시간 모니터링 기능 제공 → 사고 및 장애 분석에 활용 • 커널레벨에서 사용자 및 프로세스 명령어 실행 행위 감사 기능 제공 • 어플리케이션 레벨에서 실사용자 식별정보 기반의 감사로그에 의한 사용자 행위 추적

Secuve TOS 기능 요약 (4/6)

자체보호	• Kernel Sealing: 불법적인 커널 백도어 설치 및 보안기능 무력화 방지 • 프로세스 보호: Secuve TOS 에이전트 프로세스의 불법 종료 방지 • 설치디렉터리 보호: Secuve TOS가 설치된 디렉터리를 보호
보안정책 시뮬레이션	• **보안정책 설정의 적합성을 사전에 시뮬레이션** • 보안정책 적용 전 영향 및 효과 분석을 통한 안정적인 서비스 운영 • 전체 및 개별 시스템 자원에 대한 보안정책의 시뮬레이션 수행
시스템콜 감시모드 설정	• **사용자 운영환경에 맞게 시스템 콜 별로 감시 모드를 보호모드/로그모드/정지모드로 선택적 운영 가능**
자동보안 설정	• 시스템 주요 파일에 대한 자동 보안설정 • 시스템 주요 프로세스에 대한 자동 보안설정 • Secuve TOS 설치 디렉터리, 실행파일 등의 자동 보안설정 기능을 통한 편의성 제공
무결성 검증	• 주요 파일에 대한 주기적 무결성 검증 • 주요 실행 파일에 대한 실시간 무결성 검증 및 위반 시 실행 차단
복합인증을 통한 실사용자 인증	• **PKI 인증서, 생체인증(지문/홍체인식 등), OTP(One Time Password), 스마트카드, ARS등 다양한 복합인증 기능제공을 통해 정확한 실사용자 식별 및 인증** • 복합인증 정책 관리, 복합인증 분석 기능 (일정기간 이상 복합인증 미사용자, 만료된 사용자 검색 등)
시스템 중앙 통합관리 *(Centralized Management)*	• **웹 기반의 중앙형 통합관리 콘솔 제공** - 전자서명 인증 및 암호화 통신을 통한 안전한 채널 제공 - 관리콘솔을 통한 이 기종 환경의 다수 서버 제어, 서버 상태 및 현황 모니터링 - 관리콘솔을 통한 편리한 보안정책의 일괄적용 - 관리대상 서버 별 정책 History, 자동 Back-up 및 Roll-Back 지원

Secuve TOS 기능 요약 (5/6)

정책 템플릿 관리	• **자주 사용되는 다양한 보안정책 템플릿 기본제공** - 웹 서비스 정책 등의 자주 사용되는 보안정책 템플릿을 제공하여 관리자에게 설정의 용이성 지원 • IP/MAC 주소 템플릿 지원을 통해 보안정책 설정 편의성 제공 • 세부적인 설정이 가능한 사용자 정의 보안정책 템플릿 생성 기능 제공
통합정책관리	• **보안정책 일괄적용 기능 제공** - 다수의 관리대상 서버에 보안정책을 일괄 적용하여 관리자의 업무부하 경감 및 편리성 제공
다양한 리포트	• 저장 로그 데이터에 대한 이 기종 통합 리포팅 기능 제공 - 서버 별, 로그 별, 유형 별, 날짜 별, 사용자 정의 등의 다양한 필터링 제공 - 통계자료를 이용한 보고서 제공: 그래프, 차트 등의 형식 지원
상세한 로그관리	• 보안이벤트에 대한 상세하고 다양한 로그 기능 제공 • 보안이벤트, 주체, 객체, IP, 일자/시간 등의 조건으로 검색
실시간 알람	• 발생되는 보안이벤트에 대한 실시간 모니터링 및 알람 (관리콘솔, E-mail, 휴대폰 등) • Alert Point를 통한 다중 관리자 실시간 모니터링
자원 모니터링	• 시스템 성능 (CPU, 디스크 I/O, Network I/O) 모니터링 및 한계치 관리를 통한 실시간 알람 기능 제공 • 디스크 사용량, 프로세스 상태, 네트워크 연결정보, 로그인 세션 모니터링 기능 제공
보안정책 및 로그 대조·추적	• **보안이벤트로그에서 직접적으로 관련된 보안정책 대조·추적 가능** • **'보안정책 수립 → 로그 분석 → 보안정책 개선'의 과정을 통해, 보안정책의 지속적인 강화** • 보안정책 변경 이력(신청자, 신청내용) 추적 관리를 통한 보안정책의 연속성·지속성 확보 • 보안정책 변경 이력 백업 기능을 통해 편리하게 보안정책 보관 및 복원 가능

Secuve TOS 기능 요약 (6/6)

지원환경

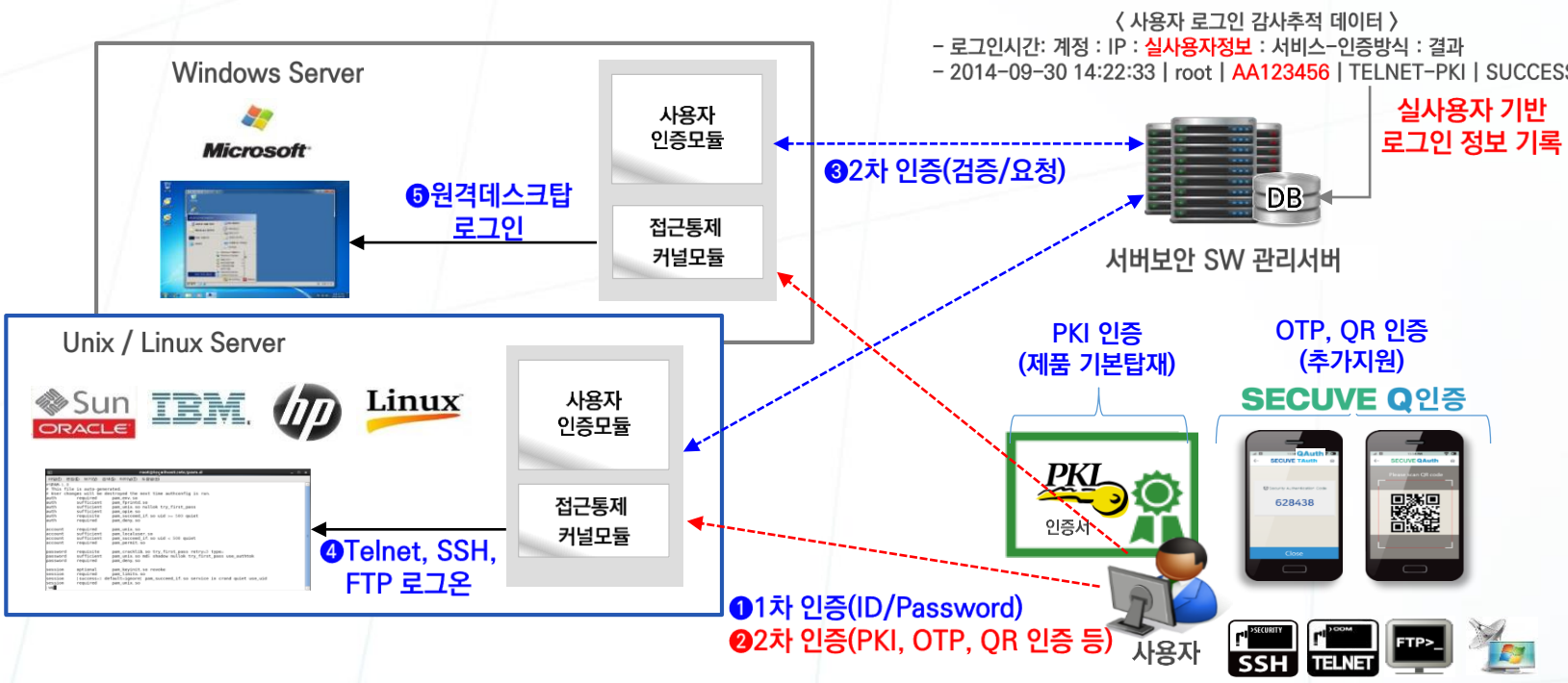
구분	세부구분	Secuve TOS 지원 플랫폼
Agent (On-premise)	SUN	• Solaris 8, 9, 10, 11 • SPARC 및 Intel x86 CPU 호환기종
	IBM	• AIX 5.3, 6.1, 7.1, 7.2 • IBM CPU 호환기종
	HP	• HP-UX 11.11, 11.23, 11.31 • PA-RISC 또는 IA64 CPU 호환기종
	Linux	• Linux kernel version 2.6.x 이상 • Intel x86 CPU 호환기종
	Windows	• Server : 2003 이상 • PC : Vista 이상 • Intel x86 CPU 호환기종
Agent (Cloud)	Linux	• Linux kernel version 2.6.x 이상 • Cloud : Amazon, IBM, KT uCloud, etc
	Windows	• Server 2003 이상 • Cloud : Amazon, IBM, KT uCloud, etc
네트워크/보안장비 (Agentless)	네트워크 장비 보안 장비	• SSH, telnet을 통해 접속 및 관리하는 장비 • 웹 기반 사용자 인터페이스를 통해 접속 및 관리하는 장비
Manager Console	Windows	• Windows 환경의 PC급 이상
관리 서버	OS	• Linux : RHEL 6.x 버전 이상 호환 Linux 배포판 • Unix : AIX 5.3, HP-UX 11.23, Solaris 10 이상 • Windows Server 2003 이상
	DBMS	• Oracle, MSSQL, Tibero, MySQL 지원
	H/W	• CPU : 2GHz * 2EA 이상 • HDD : 500GB 이상 • RAM : 16GB 이상

2 Secuve TOS 특장점 및 경쟁력

[특장점] 1. 강력한 2차인증체계 지원

PKI기반의 복합인증 기본 제공,
모바일 기기를 활용한 OTP 및 QR 방식의 편리한 복합인증도 제공 가능

특허 기술



슈퍼유저로 인증 시 모든 권한 획득	강력한 2차인증을 통한 권한 정의
키로깅 / 스푸핑 등의 인증정보 노출 취약	인증수단 기반으로 키로깅 / 스푸핑 대책 제공
인증과정에 대한 신뢰성 저하	인증과정에 대한 신뢰성 강화
실제 사용자 판단 불가	실제 사용자 판단 가능
단일 인증(ID/PWD)	복합 인증(ID/PWD + PKI, OTP, QR, BIO 인증 등)

VS

SECUVE

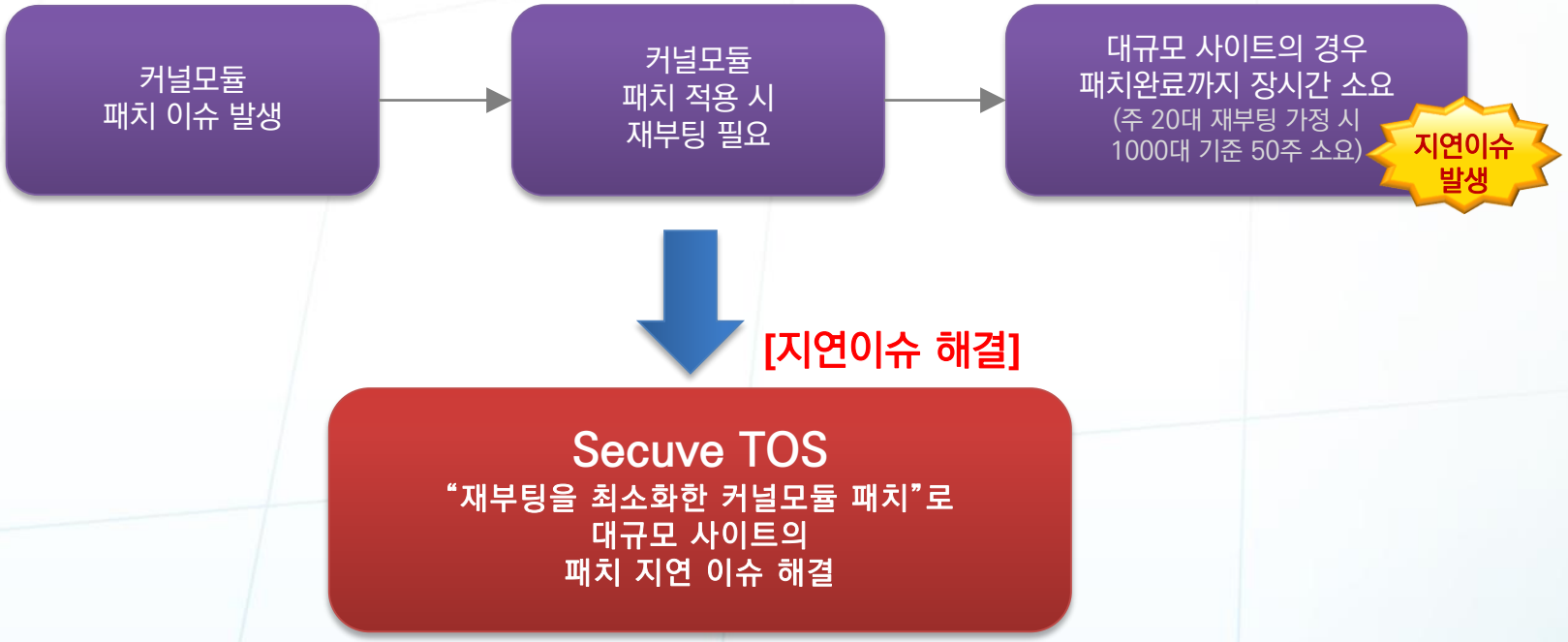
[특장점] 2. 대상서버 일괄 원격패치 제공

시스템 재부팅을 최소화한 커널모듈 원격 패치 지원

특허 기술

- 기존 서버보안 SW는 제품 특성상 커널모듈 패치를 진행할 경우 재부팅으로 인한 장시간 소요
- 대규모 사이트의 경우 다수의 시스템 커널모듈 패치 시 장기간 소요
- Secuve TOS는 재부팅 최소화한 일괄패치 기술 적용을 통해 안정적인 운영 가능

▶ 솔루션의 Agent 패치나 Upgrade 시 기존 서비스 중단(OS 다운타임) 최소화



SECUVE

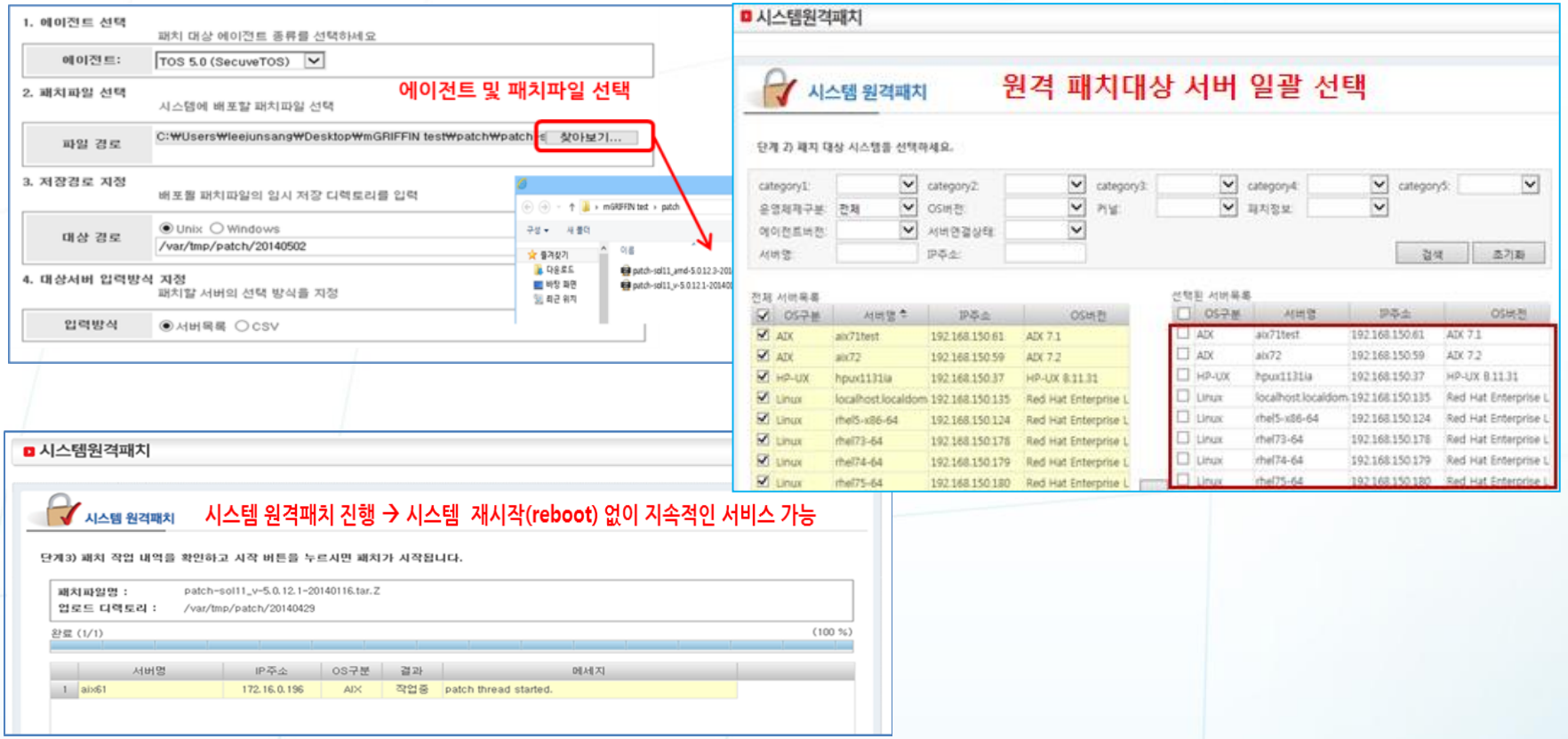
[특장점] 2. 대상서버 일괄 원격패치 제공

시스템 재부팅을 최소화한 커널모듈 원격 패치 지원

특허 기술

- Secuve TOS는 재부팅을 최소화(특허기술)하여 커널모듈 패치의 지연이슈를 해결
- 다수의 대상서버에 서버보안관리시스템을 통한 일괄원격패치 기능 제공

▶ 다수의 대상서버에 일괄원격패치 적용

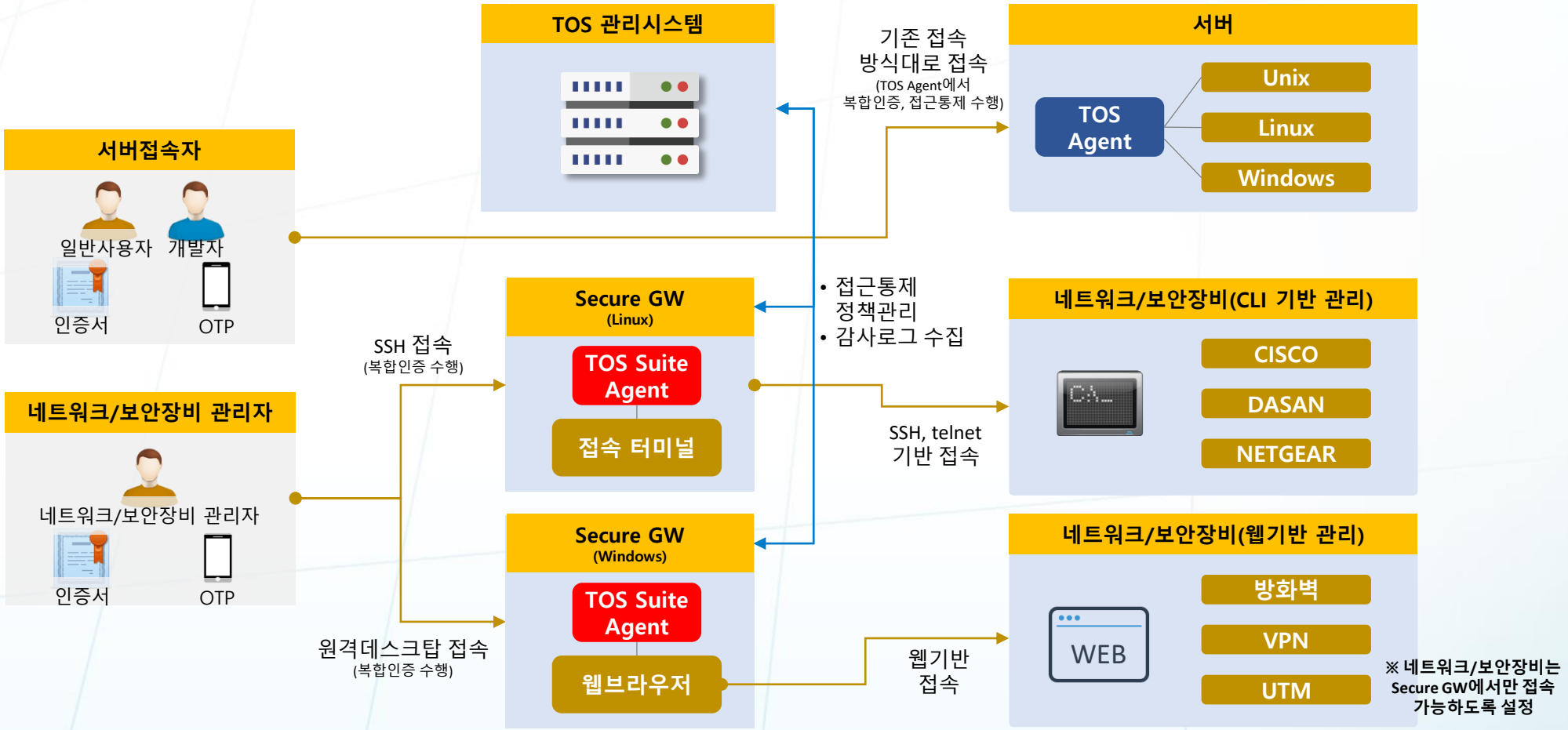


SECUVE

[특장점] 3. 네트워크/보안장비 접근통제 및 행위감사

네트워크/보안장비에 대한 접근통제, 행위감사, 복합인증 기능 제공

- Secure GW는 보안정책에 의해 허용된 네트워크/보안장비에만 접근 가능하도록 접근통제
- CLI 방식, 웹방식의 접속을 통한 사용자 행위에 대해 모두 행위감사로그 기록

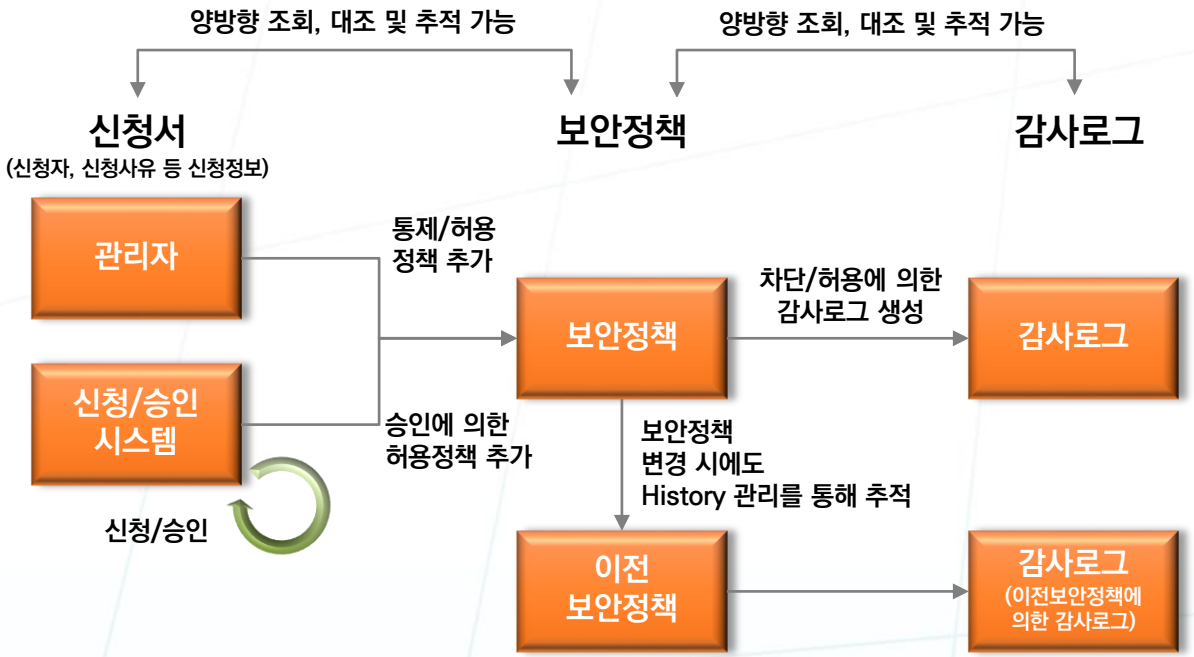


SECUVE

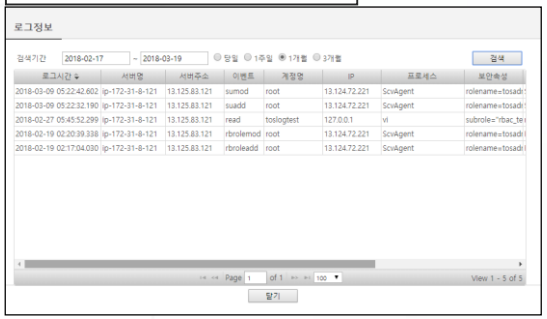
[특장점] 4. 보안정책 및 감사로그 양방향 대조 및 추적 기술

특허 기술

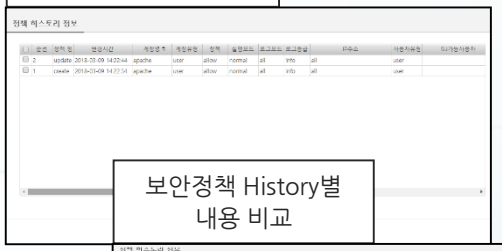
과거부터 현재까지의 보안정책과 로그정보를 양방향으로 실시간 조회, 대조 및 추적이 가능하여 해킹 및 보안침해사고 발생 시 원인분석과 대응을 신속하게 수행 가능



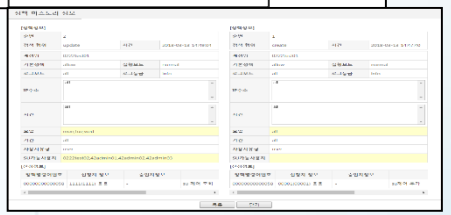
보안정책에 따른 로그정보 조회



보안정책 History 조회



보안정책 History별 내용 비교



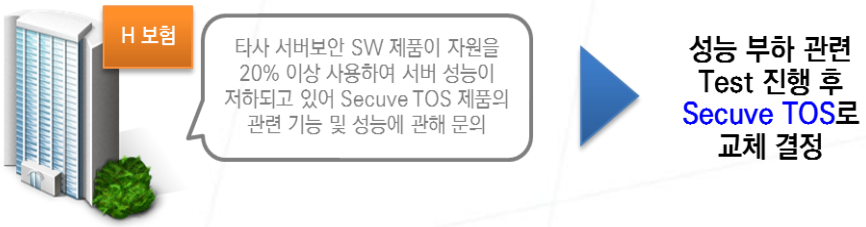
SECUVE

[특장점] 5. 자체 기술로 개발한 네트워크 접근통제 기능

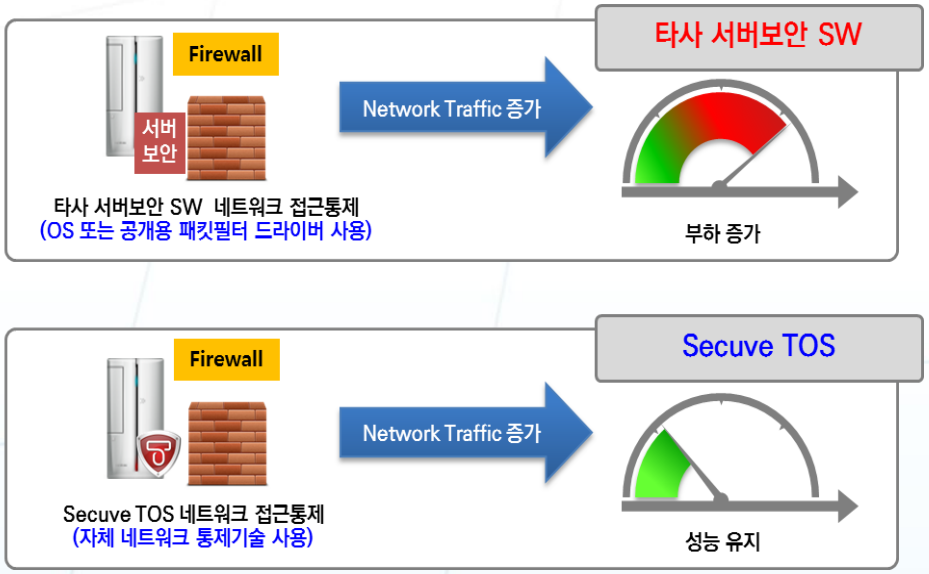
성능 저하 요인 최소화 및 시뮬레이션 기능이 포함된 네트워크 접근통제 적용

서버보안 SW의 네트워크 접근통제 성능 이슈

▶ 타사 서버보안 SW의 성능 저하 사례 : 성능 저하를 유발하는 OS 패킷 필터 사용으로 인함



▶ 서버보안 SW 의 네트워크 접근통제 성능 이슈



방화벽 구현방식에 따른 기능 비교

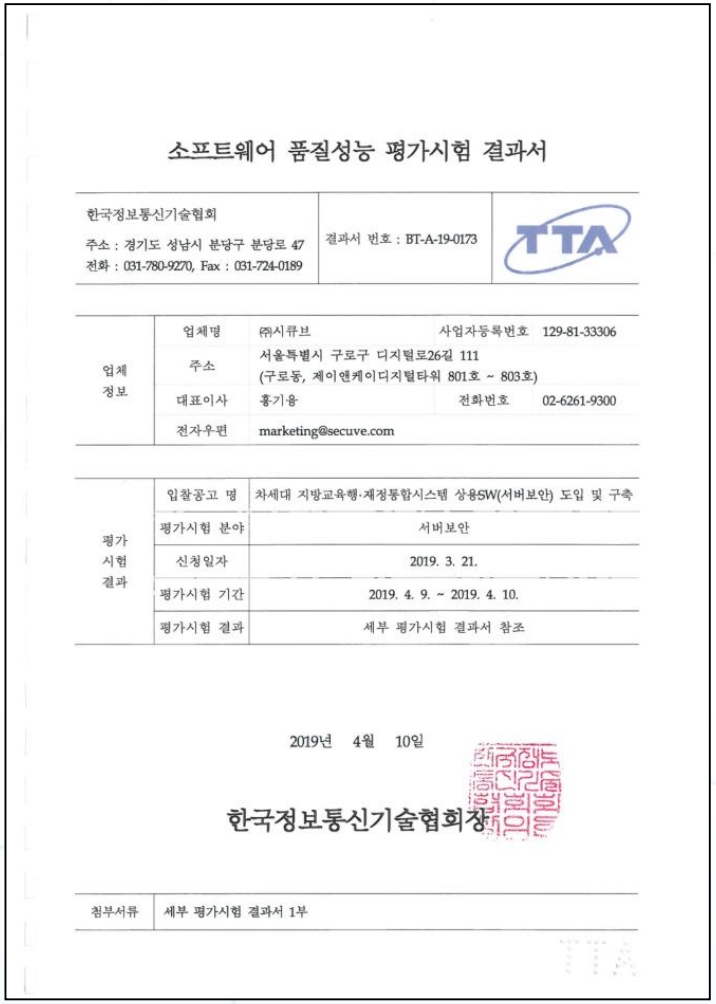
구 분	Secuve TOS 방식	기존 패킷 필터 이용 방식
구현 방식	▪ 자체 개발	▪ OS 에서 제공하는 패킷 필터 또는 오픈소스 패킷 필터 이용
보안정책 시뮬레이션	▪ 다양한 시뮬레이션 기능 제공 – 시스템 콜(System Call)별, 기능/정책별 다양한 시뮬레이션 기능 제공 ▪ 신규 보안정책을 적용하기 전에, 시뮬레이션을 통한 사전 검증 및 적용 효과 확인 가능 ☞ 타 서버보안 SW에서는 불가능	▪ 시뮬레이션 기능 제공 불가 (OS 제공 또는 오픈소스 패킷 필터 특성 상 별도 시뮬레이션 기능을 제공하지 않음)
기술지원 및 유지보수	▪ 자체 지원 – 제안사 독자적으로 기술지원 및 유지보수 가능	▪ 자체 지원 불가 – OS 벤더 또는 오픈 커뮤니티의 지원을 받아야 함

SECUVE

[특장점] 6. BMT 평가항목 All Pass 제품

TTA 주관 '소프트웨어 품질성능 평가시험(BMT)' 평가항목 All Pass 제품

- 차세대 지방교육행 · 재정통합시스템 사업, 2019.04 -



소프트웨어 품질성능 평가시험 결과서

한국정보통신기술협회 주소 : 경기도 성남시 분당구 분당로 47 전화 : 031-780-9270, Fax : 031-724-0189	결과서 번호 : BT-A-19-0173	TTA	

업체 정보	업체명	㈜시큐브	사업자등록번호	129-81-33306
	주소	서울특별시 구로구 디지털로26길 111 (구로동, 제이앤케이디지털타워 801호 ~ 803호)		
	대표이사	홍기용	전화번호	02-6261-9300
	전자우편	marketing@secuve.com		

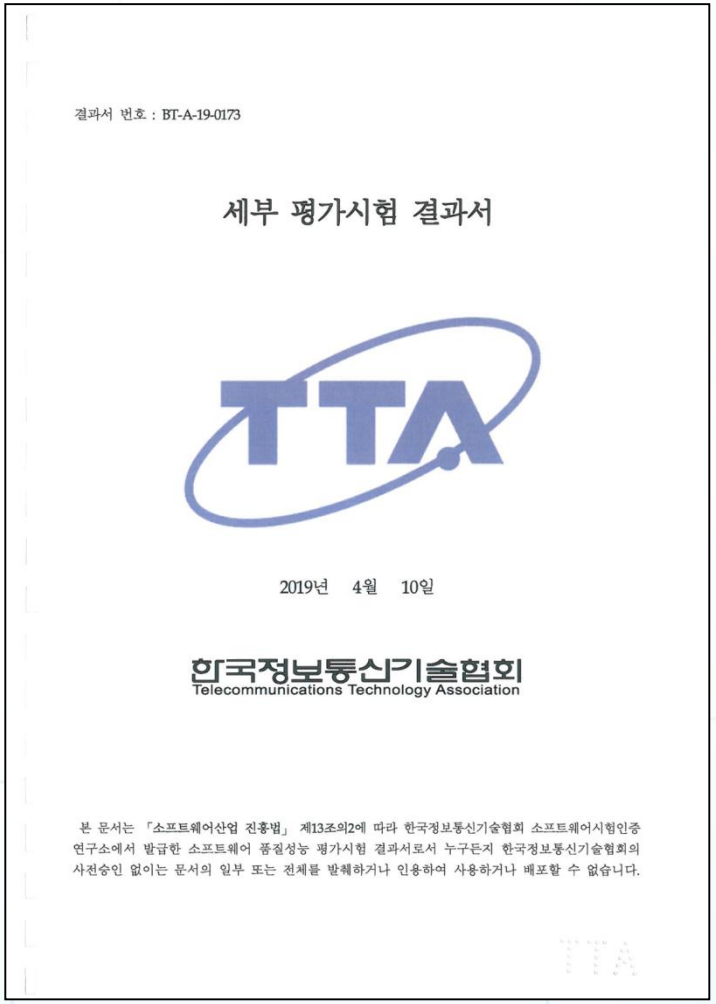
평가 시험 결과	입찰공고 명	차세대 지방교육행·재정통합시스템 상용SW(서버보안) 도입 및 구축
	평가시험 분야	서버보안
	신청일자	2019. 3. 21.
	평가시험 기간	2019. 4. 9. ~ 2019. 4. 10.
	평가시험 결과	세부 평가시험 결과서 참조

2019년 4월 10일

한국정보통신기술협회장

첨부서류	세부 평가시험 결과서 1부

TTA



결과서 번호 : BT-A-19-0173

세부 평가시험 결과서

TTA

2019년 4월 10일

한국정보통신기술협회
Telecommunications Technology Association

본 문서는 「소프트웨어산업 진흥법」 제13조의2에 따라 한국정보통신기술협회 소프트웨어시험인증연구소에서 발급한 소프트웨어 품질성능 평가시험 결과서로서 누구든지 한국정보통신기술협회의 사전승인 없이는 문서의 일부 또는 전체를 발췌하거나 인용하여 사용하거나 배포할 수 없습니다.

TTA

[특장점] 6. BMT 평가항목 All Pass 제품

TTA 주관 '소프트웨어 품질성능 평가시험(BMT)' 평가항목 All Pass 제품

- 차세대 지방교육행 · 재정통합시스템 사업, 2019.04 -

3. 소프트웨어 품질성능 평가시험 결과

구분	항목	ID	평가항목	평가결과	비고
기능 확인	계정 관리 및 식별	F01	관리자 계정 관리 기능 - 계정 생성/수정/삭제 - 계정 잠금 및 해제	P	-
		F02	관리자 계정 세션 유효기간 설정 기능	P	-
		F03	사용자 계정 관리 기능 - 계정 생성/수정/삭제 - 그룹 계정 추가/수정/삭제 - 계정 잠금 및 해제	P	-
		F04	인가된 관리자 및 사용자 식별 기능	P	-
	인증	F05	인증 기능 - ID/PW 방식 - PKI 방식	P	-
		F06	관리자 및 사용자의 인증서 관리 기능 - 인증서 발급 - 인증서 폐기	P	-
	관리	F07	중앙통합관리 기능 - 관리 대상 서버 추가/변경/삭제 - 관리 대상 서버보안 상태 확인	P	-
		F08	정책 관리 기능 - 그룹으로 정책 설정 - 보안정책 설정 - 보안정책 배포 기능	P	-
	무결성	F09	보안정책 무결성 유지 기능	P	-
		F10	무결성 검증 기능 - 로그 데이터 - 실행 코드(파일)	P	-

구분	항목	ID	평가항목	평가결과	비고
기능 확인	접근통제	F11	사용자 접근통제 기능	P	-
		F12	관리자 다중등급 접근통제 기능	P	-
		F13	사용자 계정별 동시 로그인 통제 기능	P	-
		F14	경유 통제 기능	P	-
		F15	원격 프로토콜의 접근통제 기능 - Telnet - SSH - FTP - SFTP	P	-
		F16	계정별 다양한 조건(IP, 시간, 날짜)의 조합에 따른 접근통제 기능	P	-
	파일 보호	F17	지정된 파일에 대해 다양한 조건(IP, 계정, 경유 프로그램, 접근권한) 조합에 따른 접근통제 기능	P	-
		F18	지정된 파일에 대해 다양한 조건(사용자별, 그룹별, 프로세스별, 권한별) 접근통제 기능	P	-
	시스템 보호	F19	지정된 프로세스 및 데몬에 대한 강제종료 방지 기능	P	-
		F20	비인가된 사용자에 의한 시스템 종료 방지 기능	P	-
		F21	관리 서버에 대한 보안 기능	P	-

구분	항목	ID	평가항목	평가결과	비고
기능 확인	로그 생성	F22	사용자 로그인/로그아웃에 대한 감사 로그 수집 기능	P	-
		F23	서버 사용 내역 기록 기능	P	-
		F24	보안이벤트 관련 감사로그 생성/저장 기능	P	-
		F25	프로세스 명령어 실행에 대한 커널 레벨의 이력 기록 기능	P	-
	로그 조회	F26	조건별 감사로그 조회 기능 - 사용자 ID - IP - 시간 - 위반대상 - 위반내용 - AND/OR 연산자 - 검색어	P	-
		F27	보고서 출력 기능	P	-
	경고 알림	F28	보안 경고에 대한 알람 기능	P	-

SECUVE

[특장점] 7. Windows 공유 폴더에 대한 접근통제 (IP정보에 기반한 추가적인 통제 가능)

로컬 파일/폴더와 동일한 Windows 공유 폴더에 대한 접근통제

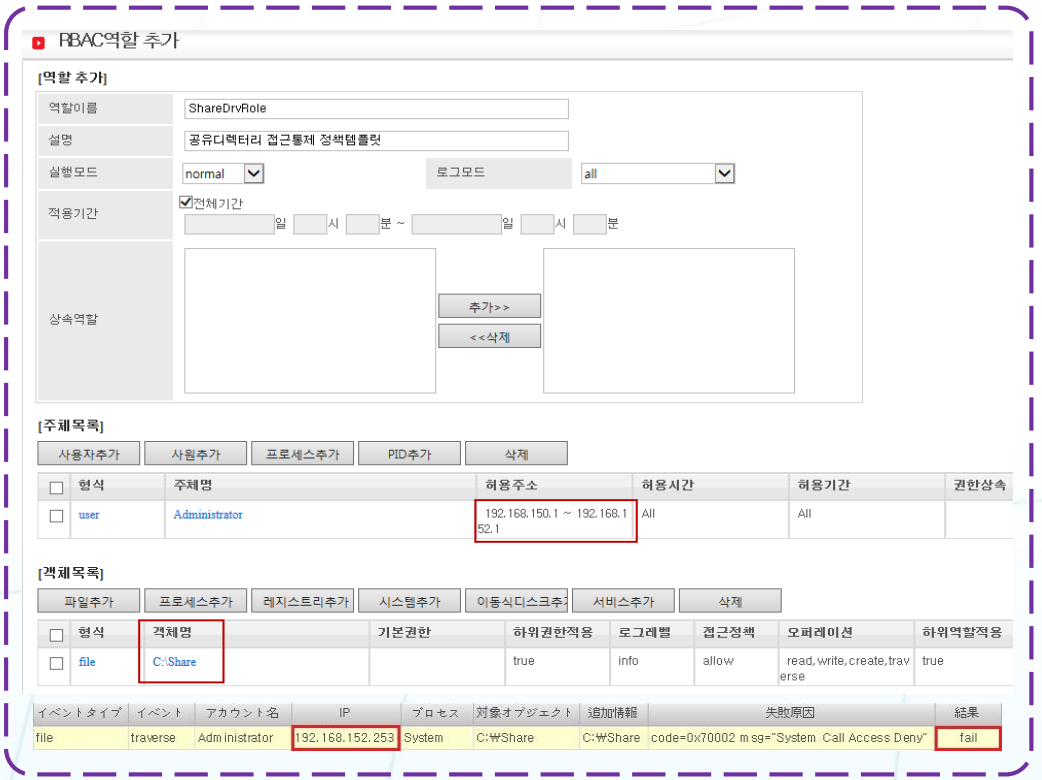
특허 기술

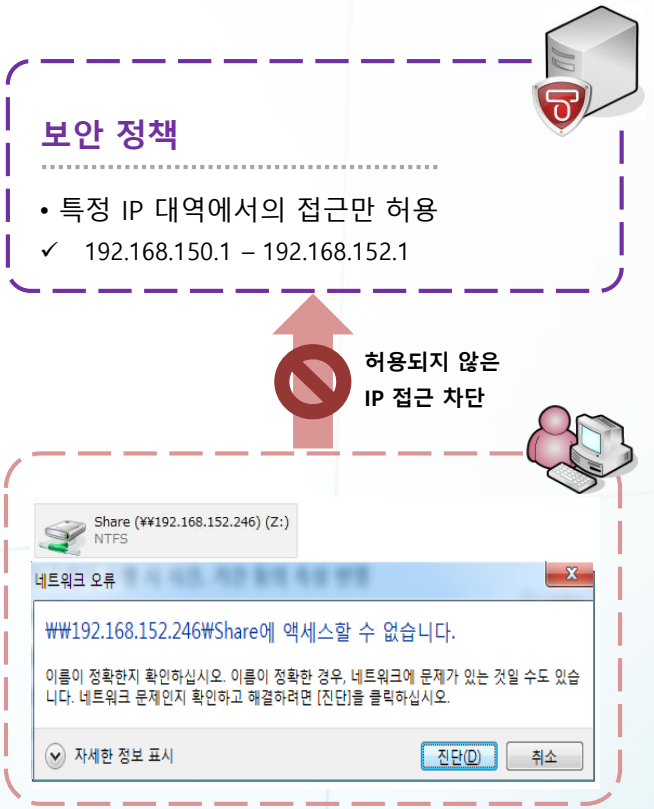
로컬 파일/폴더와 동일한 접근제어 기능 제공

- 시스템 계정/그룹, 자연인, 프로세스 등 다양한 주체 별 접근 정책 설정 가능
- 접근제어 수행 시 시간, 기간 등의 속성 반영

원격 시스템에서 공유 폴더 접근 시 IP별로 추가 제어 가능

- NetBIOS를 통한 공유 폴더 접근 시 원격 시스템의 IP 파악
- IP 기반으로 공유 폴더 내 자원에 대한 오퍼레이션 (read, write 등) 제어



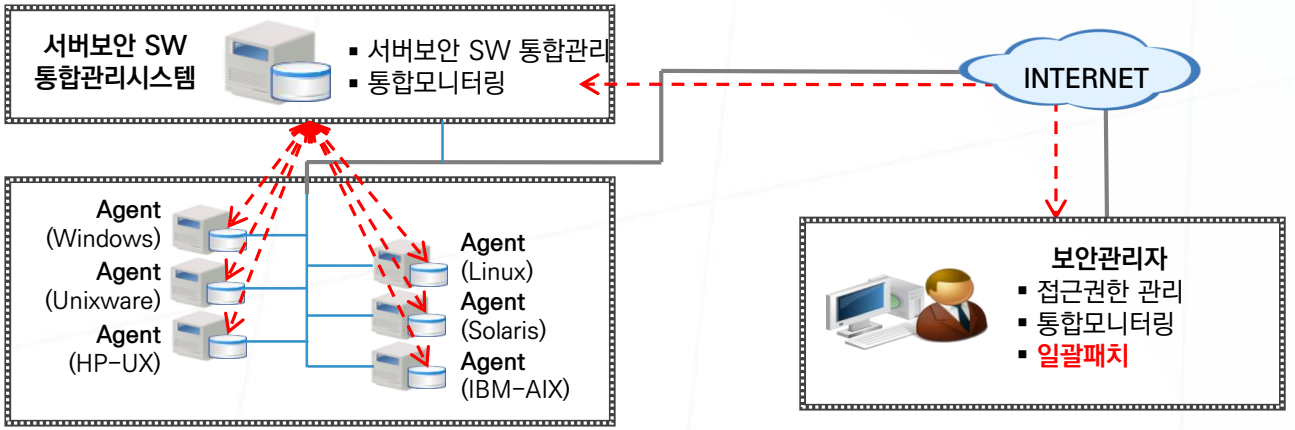


SECUVE

[특장점] 8. 통합관리시스템을 통한 관리 편의성 확보

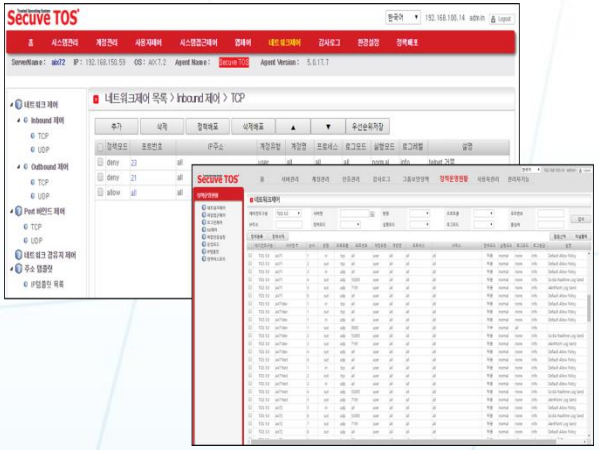
이기종 OS 및 관리대상 서버에 대해 일관되고 통합된 웹 기반 GUI를 기반으로 통합 관리의 편의성을 제공

서버보안 SW 통합관리시스템 제공

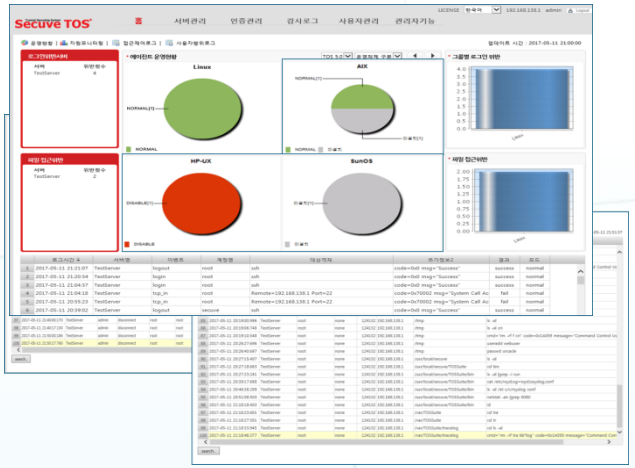


통합된 인터페이스 제공

▶ 정책그룹 적용 및 정책 운영 현황 확인



▶ 운영 현황 및 실시간 로그 확인

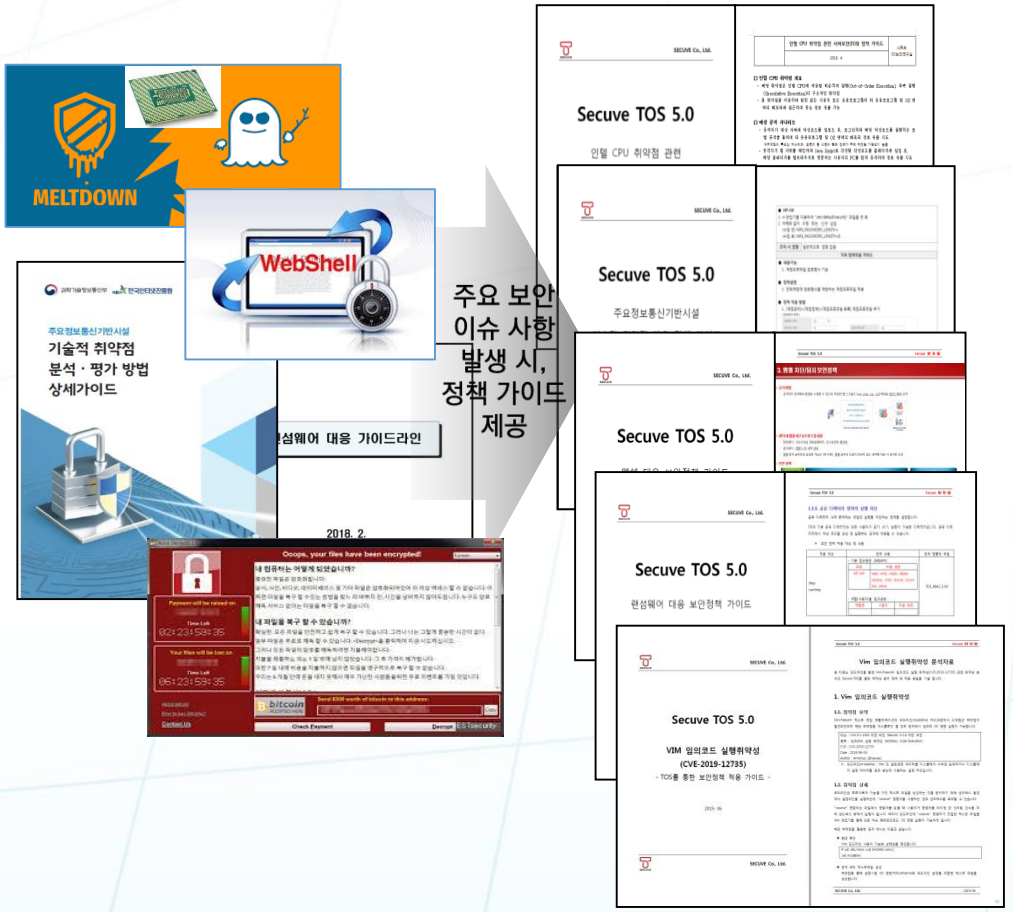


▶ 반응형 웹 UI를 통한 다양한 관리환경 지원

[특장점] 9. 사이버위협 대응 및 예방 운영지원 노하우 보유

주요 사이버위협 이슈 사항에 대응할 수 있는 보안정책 가이드를 선제적으로 제공하는 노하우를 보유

주요 보안 이슈사항 대응 보안정책 가이드



주요 사이버위협 이슈 사항 대응 보안정책 가이드 제공

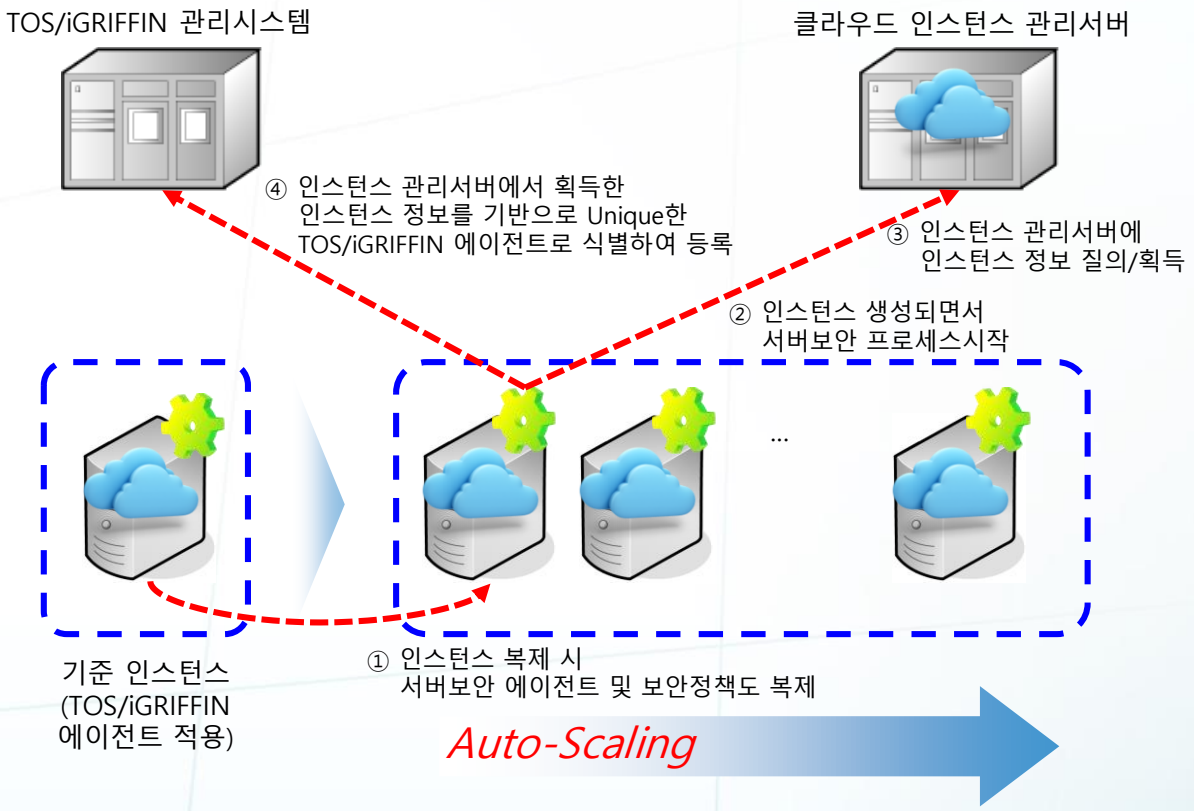
인텔 CPU 취약점 대응 서버보안 SW 보안정책	• 주요 내용 – OS의 데이터영역, 실행영역, 공유영역 등 영역별 보안정책 가이드 • 기대 효과 – 공격자의 공격 난이도를 증가시켜 인텔 CPU 취약점 공격 시도 무력화 – 웹 서버가 공격자의 악성코드 배포지로 이용될 수 있는 가능성을 최소화
주요정보통신기반시설 기술적취약점대응보안정책	• 주요 내용 – 취약점 평가 항목(Unix/Linux 73개, Windows 82개) 대응 보안정책 가이드 • 기대 효과 – Unix/Linux, Windows 서버의 기술적 취약점 제거 및 완화 – 관련 법령•규제 대응 및 서버 보안성 증대
웹쉘 대응 보안정책	• 주요 내용 – 웹 서비스 프로그램의 비인가 쉘 명령어 실행 통제 및 웹 페이지 위•변조 방지 정책 가이드 • 기대 효과 – 웹 서비스 데몬의 쉘 명령어 실행 권한을 통제하여 웹쉘 공격 차단 및 웹 서비스 보호
랜섬웨어 대응 보안정책	• 주요 내용 – 비인가 프로그램 실행 차단 및 주요 데이터영역의 위•변조 방지 보안정책 및 적용 가이드 • 기대 효과 – 랜섬웨어 등으로 인한 중요 데이터 파일의 위•변조 가능성 최소화
Vim 임의코드 실행 취약성 대응 보안정책	• 주요 내용 – Vim 텍스트 편집기의 취약성으로 인한 원격 OS 명령어 실행 공격 방지 보안정책 및 적용 가이드 • 기대 효과 – Vim 임의코드 실행 취약점을 통한 OS 명령어 및 백도어•리버스 쉘 실행의 원천적인 방어

[특장점] 10. Cloud 환경 Auto-Scaling 지원

Cloud 환경에 특화된
TOS/iGRIFFIN 인스턴스 식별 및 관리 기능 제공

TOS/iGRIFFIN 클라우드 버전 특화 기능

- Scaling 에 따른 인스턴스 자동 인식
- Auto-scaling에 따른 그룹별 보안정책 자동적용
- NAT 환경 지원
- 중계서버 상태 모니터링
- 클라우드 서비스 사업자 연동 인터페이스
  (AWS, Joyent, Azure(예정), Google Cloud(예정))



SECUVE

3 Summary

Summary

Secuve TOS만의 특장점 및 경쟁력

01 강력한 2차인증체계 지원

02 재부팅을 최소화한 대상서버 일괄 원격패치 제공

03 네트워크/보안장비 접근통제 및행위감사 기능 제공

04 보안정책 및 감사로그 양방향 대조 및 추적 기술

05 자체 기술로 개발한 네트워크 접근통제 기능

06 TTA 주관 BMT 평가항목 All Pass 제품

07 Windows 공유 폴더에 대한 접근통제 (IP주소기반)

08 웹 GUI 기반 통합관리시스템을 통한 관리 편의성 확보

09 사이버위협 대응 및 예방 운영지원 노하우 보유

10 Cloud 환경 Auto-Scaling 지원

4 주요 고객사

주요 고객사

금융

농협중앙회 | NH농협은행 | KB국민은행 | IBK기업은행 | KDB산업은행 | 부산은행 | 대구은행
신협 | K bank | NH농협금융지주 | KB금융그룹 | NH농협카드 | KB국민카드 | 비씨카드
NH농협생명 | 신한생명 | 하나생명 | lifeplanet | KDB생명 | DGB생명 | MetLife
삼성생명서비스 | NH농협손해보험 | The-K손해보험 | 현대해상 | SGI서울보증 | NH투자증권 | SK증권
MERITZ 메리츠종금증권 | 하나대투증권 | 유진투자증권 | 키움증권 | 한국증권금융 | DGB캐피탈 | KDB캐피탈
MERITZ 메리츠캐피탈 | Finnq | 하나금융티아이

기업

SAMSUNG | HYUNDAI MOTOR GROUP | DOOSAN | HYUNDAI MOBIS | posco | emart mall | 신세계몰
금호아시아나 | THE E-LAND GROUP | 중앙미디어네트워크 | LOTTE Homeshopping | CJ 엘로비전 | samyang 삼양사 | HOME & SHOPPING
THE SHILLA | MBC PLUS | LOTTE WORLD TOWER | SK | SK가스

대학교

서울대학교 | 연세대학교 YONSEI UNIVERSITY | 이화여자대학교 EWHA WOMANS UNIVERSITY | 국립 한국해양대학교 KOREA MARITIME UNIVERSITY | 고려대학교 KOREA UNIVERSITY | 경희대학교 | 성균관대학교
경인교육대학교 | INU 인천대학교 | 용인대학교 | 인하대학교 | 대진대학교 | 가천대학교 | 대림대학교

SECUVE

주요 고객사

금융 / 기업 / 의료

● 금융

KB금융지주, KB국민은행, KB국민카드, KB생명, 농협(중앙회,은행,지주), NH농협카드, NH투자증권, NH농협손해보험, NH농협생명보험, 신한생명, 신한저축은행, 신한아이타스, 신한신용정보, 신한BNP파리바자산운용, KDB산업은행, KDB생명, KDB캐피탈, IBK기업은행, IBK신용정보, IBK자산운용, K뱅크, 대구은행, DGB생명, 부산은행, 한국은행, 신협중앙회, 핀크, 삼성생명서비스, SK증권, 하나대투증권, 하나HSBC생명보험, 하나금융티아이, 웰컴크레디라인대부, 현대해상, 비씨카드, 더케이손해보험, 메트라이프생명, 한국증권금융, 교보디지털생명, 유진투자증권, 아이앰투자증권, 새마을금고중앙회, 나이스평가정보, 나이스디앤비, 나이스정보통신, 한국전자금융, 키움증권, 교통은행, 메리츠증권, 메리츠캐피탈

● 기업

현대모비스, 현대글로비스, 현대비앤지스틸, 지아이티(현대자동차그룹), HL그린파워(현대자동차그룹), 삼성전자, 삼성그룹, 삼성엔지니어링, 삼성중공업, 삼성물산(상사), 삼성물산(패션), 호텔신라, 삼성경제연구소인력개발원, LG유플러스, 서브원, 두산중공업, K뱅크, KT, SK홀딩스, SK주식회사 C&C, SK네트웍스, SK가스, SK어드밴스드, SK해운, 워커힐, 신세계(SSG.COM), 이마트(SSG.COM), 신세계페이먼츠, 롯데백화점 ,롯데홈쇼핑, 롯데월드타워, 삼양그룹, 이랜드그룹, 홈앤쇼핑, MBC플러스미디어, 한국전자인증, 한국정보인증, 영원무역, 스포츠토토 ,CJ헬로비전 ,중앙일보 ,중앙미디어네트워크 ,코나아이, 금성출판사

● 의료

국립암센터(복지부), 원자력병원, 경찰병원, 중앙보훈병원, 전국국립정신병원, 전국산재의료원, 한일병원(산자부), 이대목동병원, 한양대학교병원, 전북대학교병원, 제주대학교병원, 을지대학교병원, 순천향의료원, 고려대학교의료원, 강북삼성병원, 삼성서울병원, 보라매병원, 국립마산병원, 국립중앙의료원

주요 고객사

공공 / 국방 / 교육

● 공공

우정사업정보센터, 한국방송통신전파진흥원, 건강보험심사평가원, 보건복지부, 국토교통부, 기획재정부, 외교부, 법무부, 서울출입국관리사무소, 인천공항출입국관리사무소, 서울지방교정청, 행정자치부, 정부통합전산센터, 산업통상자원부, 근로복지공단, 한국지역난방공사, 한국전력공사, 한국남동발전, 한국동서발전, 한국중부발전, 한전KPS, 국민안전처, 국세청, 경찰청, 관세청, 고용노동부, 한국방송공사, 통계청, 대법원, 한국지역정보개발원, 한국산업기술평가관리원, 한국산림복지진흥원, 한국인터넷진흥원, 국토지리정보원, 중소기업기술정보진흥원, 한국건강증진개발원, 한국정책방송원, 한국공정거래조정원, 국립농산물품질관리원, 서울산업진흥원, 한국생명공학연구원, 국토지리정보원, 한국과학기술정보연구원, 한국산업안전보건공단, 한국보훈복지의료공단, 광해관리공단, 인천국제공항공사, 한국농어촌공사, 한국가스안전공사, 한국공항공사, 한국광물자원공사, 한국철도시설공단, 코레일네트웍스, 질병관리본부, 농림축산검역본부, 농촌진흥청, 산림청, 화성시청, 연천구청, 관세청, 한국국제협력단, 한국원자력의학원, 중앙전파관리소, 서울종합방재센터, 한국저작권위원회

● 국방

국방부, 방위사업청, 국방통합정보관리소(DIDC), 국군지휘통신사령부, 육군, 해군, 공군, 기무사령부, 국군정보사령부, 해병대사령부, 해군군수사령부, 해군작전사령부, 한미연합사령부, 한국국방연구원, 공군중앙관리단, 육군교육사령부, 국방시설본부, 국군의무사령부, 국방과학연구소, 국방기술품질원, 국방대학교, 국방전산정보원, 국방홍보원, 육군사관학교, 해군사관학교, 전쟁기념관, 국방지형정보단, 국군인쇄창, 합동군사대학교, 군인공제회C&C

● 교육

한국교육학술정보원, 한국교육개발원, 교육부, 강원도교육청, 인천광역시교육청, 한국장학재단, 한국교육과정평가원, 한국대학교육협의회, 여주교육지원청, 경기도동두천양주교육지원청, 수원교육지원청, 경상북도교육청, 서울특별시교육청, 경기도교육정보기록원, 안산교육지원청, 강원교육과학정보원, 서울시교육연구정보원

SECUVE

감사합니다 !