PowerBroker

Windows/UNIX/Linux

- Application Control
- Privilege Management
- Activity Logging
- File Integrity Monitoring

Least Privilege and Application Control
for Servers and Desktops

세종정보보안 BizHuB

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Contents

I Why PowerBroker ?

II PowerBroker 중요 기능

III 접근통제 및 패스워드 관리 기능

IV PowerBroker 기능 비교

V PowerBroker 평가 및 레퍼런스

세종정보보안 BizHuB

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

I Why PowerBroker ?

PowerBroker 필요성

세종정보보안 BizHuB

최소권한(Least Privilege)의 필요성

전자금융감독규정준수와 금감원 검사 대응 및 내부 통제 강화

- 금감원 중점 검사 사항에 대하여 사전 대응하고, 작업 관련 내부 통제 방안의 수립 및 적용
- 접근권한 부여 기준, 통제절차 수립 및 준수로 주민등록번호를 포함하는 고객정보 보호
- 접근권한 부여 내역의 전산기록과, 관리책임자, 보안관리자 등의 확인 및 관리
- 작업에 대한 자동화된 책임자 승인을 통한 사전 통제로 고객정보 유출 등 보안사고 방지
- 작업 수행 내용에 대한 기록 및 수행 내역 검사를 통한 사후 통제

단말 및 서버 통제 관련 전자금융감독규정 준수

관련 규정	단말 및 서버 운영 통제 관련 전자금융감독규정 상세 내역
제13조 (전산자료 보호대책)	1. **사용자계정과 비밀번호를 개인별로 부여**하고 등록·변경·폐기를 체계적으로 관리할 것 2. 외부사용자에게 사용자계정을 부여하는 경우 **최소한의 작업권한만 할당**하고 **적절한 통제장치**를 갖출 것 4. 전산자료의 입력·출력·열람을 함에 있어 **사용자의 업무별로 접근권한을 통제**할 것
	② **제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.**
	⑤ 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용 다만, 정보처리시스템 관리자의 **주요 업무 관련 행위는 책임자가 제28조 제2항에 따라 이중확인 및 모니터링**
제14조 (정보처리시스템 보호대책)	9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것 10. 정보처리시스템 **운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제** 조치를 즉시 시행할 것
제30조 (일괄작업에 대한 통제)	1. 일괄작업은 **작업요청서에 의한 책임자의 승인**을 받은 후 수행할 것 4. 모든 일괄작업의 작업내용을 기록·관리할 것 5. 책임자는 **일괄작업 수행자의 주요업무 관련 행위를 모니터링**할 것

최소권한(Least Privilege)의 필요성

전자금융감독규정준수와 금감원 검사 대응 및 내부 통제 강화

항목	작업 통제 관련 사항	
계정 변경	정의	▪ 서버에 접속한 후 su, sudo, ssh, telnet 등을 이용하여 서버 내에서 계정을 변경
	예	① 단말에서 공용 계정(user01)로 서버에 접속한 후 su를 이용하여 root로 로그인 ② 단말에서 공용 계정(user01)로 서버에 접속한 후 su를 이용하여 DB접속 계정으로 변경 후 DB접속을 위한 Tool(sqlplus 등)을 이용하여 DB에 접속하여 작업 수행
서버 접속	정의	▪ 단말(PC) 및 콘솔 등에서 서버에 직접 접속한 후 다른 서버로 다시 접속
	예	▪ AP서버에서 ssh, rlogin, telnet 등을 이용해서 DB서버로 다시 접속
명령어 통제	중요	▪ shutdown, dd, kill, rm 등 파일을 삭제, 변경하거나 장애 등을 발생할 수 있는 명령어
	작업	▪ sqlplus 등 DB 작업이나 통제 대상 작업(전산원장 등)을 수행할 수 있는 명령어
	일반	▪ 중요, 작업 통제를 위한 명령어를 제외한 업무 운영을 위한 명령어(vi, cp, cat 등)
고려 사항	계정 적용	▪ 1인 1계정 부여, 사용자 그룹(시스템운영, 업무운영, DB운영 등) 권한 부여 등
	배치 작업	▪ 명령어 통제 정책으로 인한 정기 및 비정기 배치 작업 수행 이상 여부
	시스템 운영	▪ 명령어 통제 정책으로 인한 시스템 운영 관리 및 솔루션 운영 이상 여부

최소권한(Least Privilege)의 필요성

전자금융감독규정준수와 금감원 검사 대응 및 내부 통제 강화

항목	작업 통제 개선 방안	
계정 관리	계정 부여	▪ 사용자별 1인 1계정 부여(서버 접속 및 통제 정책 적용)
	계정 통제	▪ APP 계정 및 O/S 계정(root, admin 등) 사용 금지
접속 통제	접속 프로그램	▪ 서버 접속을 위한 단말 프로그램 통제 (putty외 설치 불가 등)
	접속 서버	▪ 사용자(계정)별 접속 가능 서버 관리 (단말 프로그램 및 서버에서 접속 통제)
	우회 차단	▪ 서버 접근통제 솔루션 우회 차단 (내부 방화벽, 서버 팜 구성, 서버 방화벽 등)
작업 통제	통제 적용	▪ 사용자 그룹(시스템운영, 업무운영, DB운영 등)에 따른 1인 1계정 부여
	명령어 통제	① 수행 가능 명령어 통제 (중요 명령어, 서버 접속, 권한 변경 등) ② 명령어 위/변조 통제(명령어를 다른 이름으로 복사하거나 Alias 적용) ③ Script 및 프로그램 내의 명령어 통제 (작업자가 직접 입력하지 않는 명령어) ④ 콘솔에서 서버에 직접 접속하여 수행하는 작업 등 우회 접속 통제 방안
	결재 기능	▪ 중요 명령어 수행 시 권한에 따른 책임자(제3자) 승인을 통한 결재 처리 프로세스
	로그 관리	▪ 서버에서 수행하는 모든 작업에 대한 로깅 및 관리를 위한 보고서 출력

최소권한(Least Privilege)의 필요성

국가정보보안 기본지침에 대한 공공기관 "정보보안 세부 지침" 준수

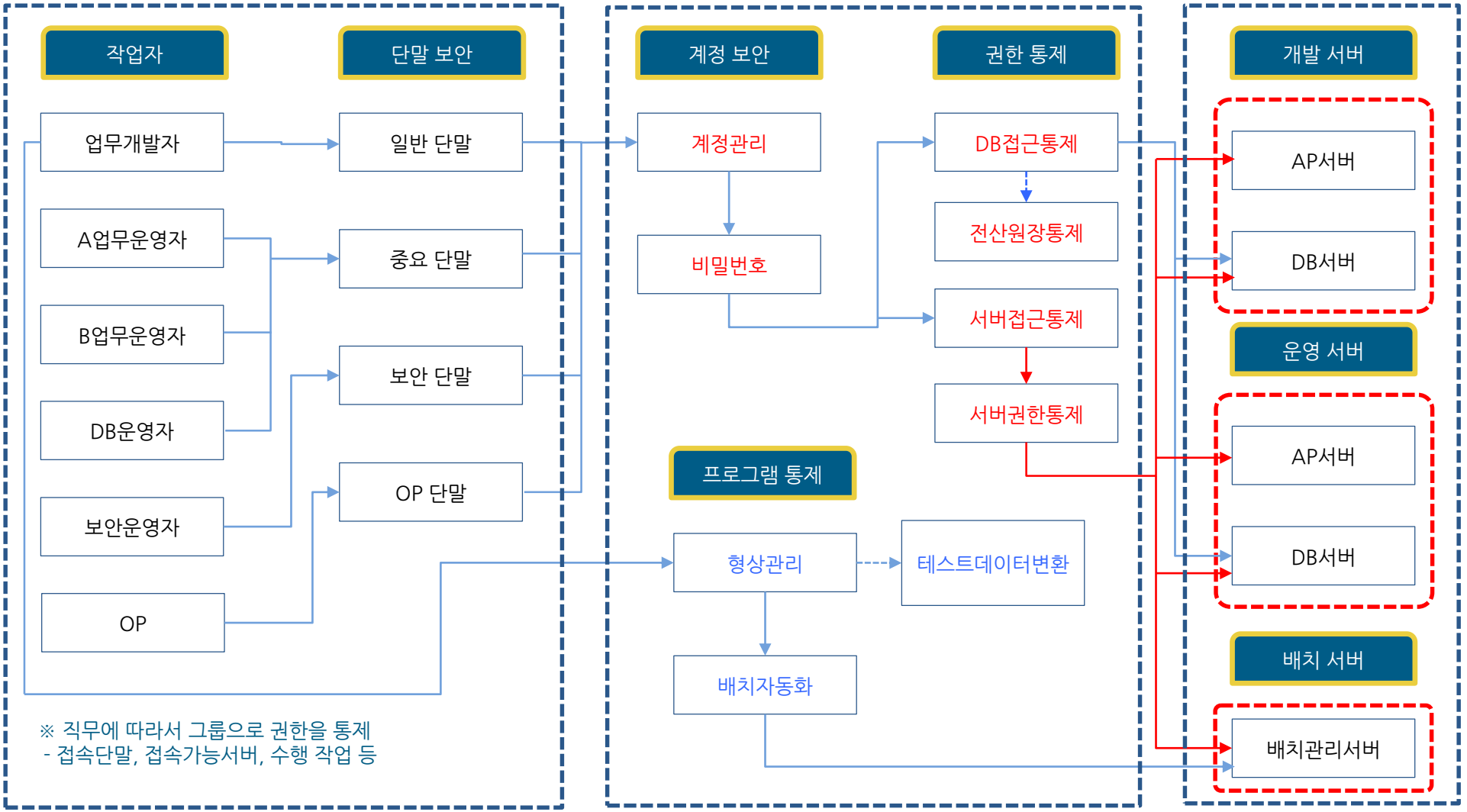
- 「국가정보보안 기본지침」에 따라 공공기관의 정보보안업무에 필요한 세부사항의 준수
- 대부분의 공공기관은 「국가정보보안 기본지침」를 기초로 각 기관의 특성에 맞도록 정보보안 세부 지침을 수립
- PC(단말)에 업무와 무관한 비인가 프로그램의 설치 및 사용을 할 수 없도록 통제 적용 필요
- 비인가 프로그램의 설치를 통제할 수 있도록 PC의 Admin 권한에 대한 통제
- 사용자의 접근권한과 범위를 업무별 · 자료별 중요도에 따라 차등 부여

공공부분 정보보안 세부 지침 내용(예시)

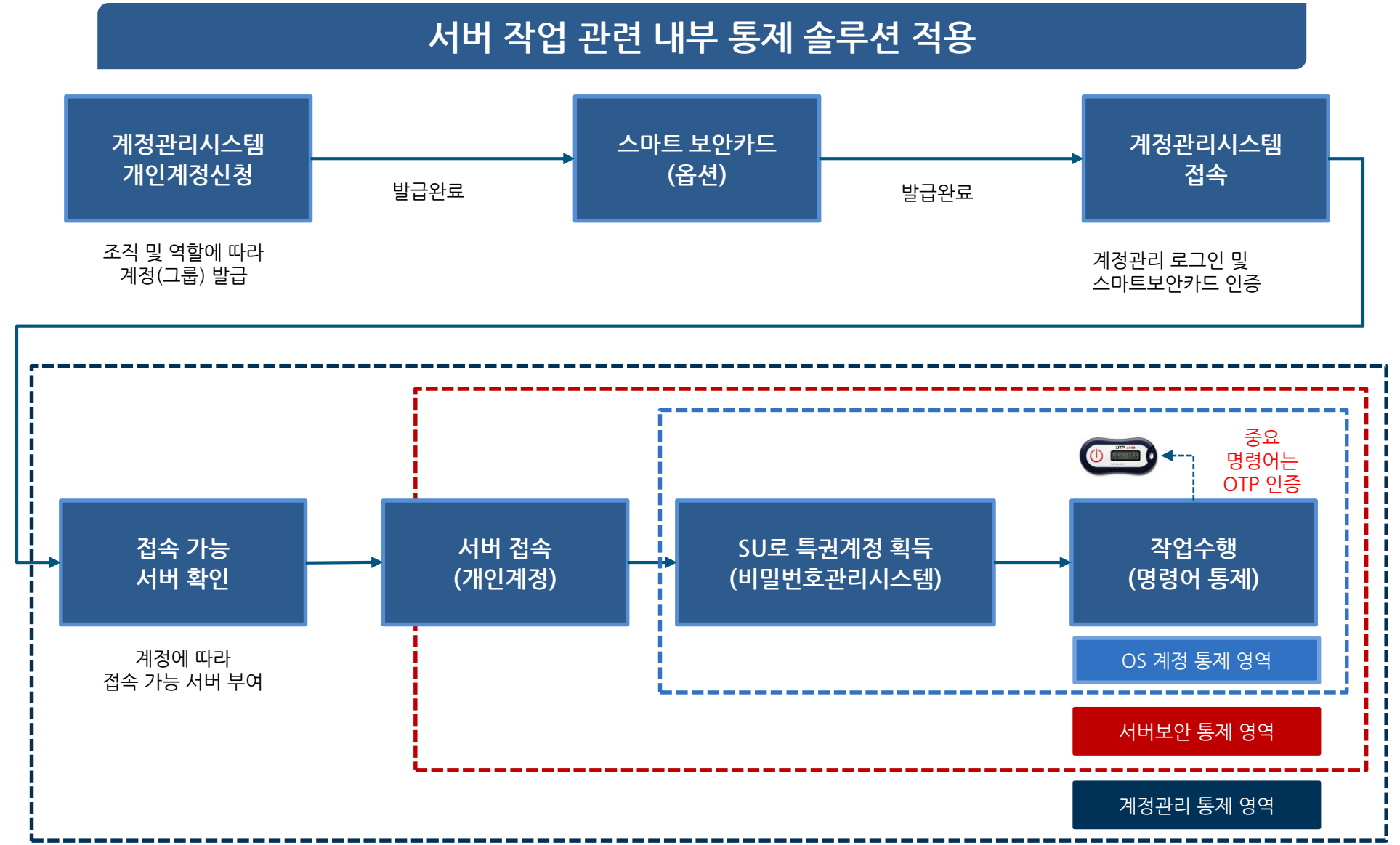
관련 규정	단말 및 서버 운영 통제 관련 정보보안 세부 지침 내역
제33조 (PC 등 단말기 보안관리)	4. **업무와 무관하거나 보안에 취약한 응용프로그램 설치 금지** 및 공유 폴더의 삭제 5. 그 밖에 국가정보원장이 안전성을 확인하여 배포 승인한 프로그램의 운용 및 보안권고문
제34조 (인터넷PC 보안관리)	정보보안담당관은 비인가자가 인터넷과 연결된 PC(이하 인터넷PC)를 무단으로 조작하여 전산자료를 절취, 위 · 변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 사용자에게 지원하며, 사용자는 이를 준수 1. 메신저 · P2P · 웹하드 등 업무에 무관하거나 Active-X 등 보안에 취약한 프로그램과 **비인가 프로그램 · 장치의 설치 금지** 2. 특별한 사유가 없는 한 문서프로그램은 읽기 전용으로 운용
제35조 (서버 보안관리)	② 서버 관리자는 서버내 저장자료에 대해 업무별 · 자료별 중요도에 따라 사용자의 접근권한을 차등 부여 ③ 서버 관리자는 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제
제44조 (악성코드 방지대책)	2. 사용자는 **출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지**하고 인터넷 등 상용망으로 자료 입수시 신뢰할 수 있는 인터넷사이트를 활용하여야 하며 최신백신으로 진단후 사용.

최소권한(Least Privilege)의 필요성

서버 작업 관련 내부 통제 솔루션 적용



최소권한(Least Privilege)의 필요성



최소권한(Least Privilege)의 필요성

공유 계정 금지	파일 접근 제어	유저 권한 분리	명령어 제어	패스워드 관리
• 자신만의 Identity 구분 • 작업 수행자에 대한 식별 • 사용자(계정)별 권한 부여	• 접근 및 사용 가능한 파일에 대한 정의 • 사용 가능한 권한(수행)에 대한 정의	• 유저의 권한에 따른 가능 작업 분류 • Blacklisting 방식	• 유저의 시스템 및 명령어 접근 및 제어 • O/S 계정이 아닌 사용자(계정) 권한 통제	• 특권유저의 패스워드 Rotation • Application 공유 계정의 일반 접속 사용 금지

- root, administrator 나 특권 유저(시스템운영자, DBA, 보안관리자 등) 로그인 작업 : 특권 권한을 모두 부여 받음
- su, sudo, runas 를 이용 : su, sudo, runas(windows 관리자 권한 실행)는 통제 대상이 아니고 제거 대상임

PowerBroker : 최소권한 부여

- 작업자에게 일반 유저 할당 후 필요 권한 부여 및 상승(ELEVATION)
- APT 공역 등에 의한 MALWARE 방지
- 내부 사용자 권한에 따른 작업 내용에 대한 상세 통제 적용
- 장애 방지 (고의적 OR 실수)
- 불법 소프트웨어 설치 및 실행 방지

금감원 망분리 대체 정보보호통제 대응

전자금융감독규정시행세칙 제2조의2 (망분리 적용 예외)

전자금융감독규정 망분리 관련 조항

관련 규정	서버 운영 통제 관련 전자금융감독규정 상세 내역
전자금융감독규정 제15조(해킹 등 방지대책)	3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지 **(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)**
전자금융감독규정시행세칙 제2조의2 (망분리 적용 예외)	① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 내부 업무용시스템을(규정 제12조의 중요단말기는 제외한다) 업무상 필수적으로 특정 외부기관과 연결해야 하는 경우를 말한다 (다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).
	③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 <별표 7>에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

<별표 7> 망분리 대체 정보보호통제

대책	세부사항
내부망 보안 강화	▪ 업무망에 반입되는 전산자료 대상으로 악성코드 감염여부 진단·치료 대책 수립
외부망 보안 강화	▪ **지능형 해킹(APT)차단 대책 수립** ▪ 외부망을 통해 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
단말기 보안 강화	▪ **PC 사용자의 관리자 권한 제거** ▪ **승인된 프로그램만 설치·실행토록 대책 수립** ▪ 단말기 전산 자료 암호화 저장

금감원 망분리 대체 정보보호통제 대응

PC 사용자 관리자 권한 제거

구분	PowerBroker 기능
Application	▪ 설치나 실행 시 프로세스 단위 Admin 권한의 임시 부여
시스템 작업	▪ 시스템 작업 시 자유로운 Admin 권한 부여 : IP변경, Time 설정, 프린터 설정 등
CUI 작업	▪ 시스템관리자나 유저의 명령어 작업에 대한 Admin 권한 부여의 용이성

PC(단말)에 임의 프로그램 설치 방지를 위한 권한 통제 필요

PowerBroker

- 유저의 변경 없이 일반 유저에서 필요한 프로세스 및 TASK 단위로 관리자 권한을 부여

금감원 망분리 대체 정보보호통제 대응

승인된 프로그램만 설치·실행토록 대책 수립

• 승인된 프로그램은 Installation Program & Portable Program & Device Driver 등 모든 프로그램을 포함

통제 요구 사항

- 단말에 어떤 소프트웨어도 임의적 설치 불가
- 승인된 프로그램만 설치 및 실행 가능

승인되지 않은 프로그램의 설치 방지로 라이선스 및 자산 관리 필요

PowerBroker : Least Privilege + WhiteListing

- WHITELISTING과 LEAST PRIVILEGE를 구현하는 솔루션
- 세계적 REFERENCE
- LEAST PRIVILEGE + WHITELISTING = RANSOMWARE 방지

화이트리스팅(Application Control)의 필요성 - Windows 서버/단말

Windows 서버 및 단말(Windows/Mac) 상의 Application Control

- 어떤 명령어의 수행을 금지하고 허락 할 것인가
- 수행 명령어의 keystroke 및 Mouse Click 로깅

통제 요구 사항

- 단말 및 서버에 임의의 프로그램 설치 (포터블 프로그램 포함)
- 랜섬웨어의 위험성 (윈도우 서버에 랜섬웨어의 지속적 대두)
- Malware를 어떻게 효과적으로 막을 수 있는가?
- 파일이나 스크립트 등의 수정이나 실행을 어떻게 통제 할 것인가?
- 명령어나 Powershell 이나 Update가 어떤 권한으로 수행 될 것이고 어떤 권한으로 수행되고 있는가?
- Session 로깅이 동영상이 아닌 스냅샷 형태로 유저별 어플리케이션별로 선별 가능한가?

스냅샷을 이용한 동영상 저장 모니터링을 이상 행위 감지를 위해서는 수작업으로 검토가 필요

PowerBroker 대응

- 완벽한 APPLICATION CONTROL
- PRIVILEGE ACTIVITY 모니터링 및 KEYSTROKE & MOUSE CLICK 로깅
- 권한 위임 : 최소 권한의 할당

랜섬웨어에 대한 대비 필요

APT(Advanced Persistent Threat)는 ?

01 지능적 (ADVANCED)

▪ 공격자는 코딩 기술, 이전에 알려지지 않은 OS, APP의 취약점을 찾아내 이용하는 능력 등 공격 대상의 보안 약점을 악용하는 데 필요한 상당한 기술적 능력을 갖추고 있습니다.

02 지속적 (PERSISTENT)

▪ 일시적인 기회에 한 번 공격하고 마는 단기 해킹과 달리 APT는 수년에 걸쳐 진행되기도 하며 좀더 중요한 여러 정보에 액세스하기 위해 다양한 수단을 활용하여 시간을 두고 여러 가지 보안 위협을 가합니다.

03 위협 (THREAT)

▪ APT 공격을 가하는 개인, 집단 및 조직은 동기(랜섬웨어 감염을 통한 금전적 이익, 사이버 테러 등)를 갖고 있으며, 공격을 성공시키는 데 필요한 능력과 리소스를 보유하고 있습니다.

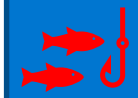
믿을 만한 지인이나 회사 등으로 가장해 '사회공학적(social engineering)기법'의 공격을 감행

※주1 : drive-by download는 사용자가 위험 노출 되었던 적법한 웹사이트를 방문 시 발생하며, 공격자들이 악의적 소프트웨어를 사용자의 허가나 인지 없이 설치

랜섬웨어에 대한 대비 필요

이메일을 이용한 APT 공격의 대표적인 방법

해커의 낚시질 "피싱"



- '피싱'(phishing)은 일명 낚시질입니다. 이메일이나 메신저로 믿을 수 있는 사람인 것처럼 속여 아이디나 비밀번호 등 중요한 정보를 빼돌리려는 해킹 수법이죠. 악성코드를 숨긴 이메일을 무작위로 보냈죠? 이걸 피싱이라고 합니다.
- 피싱을 이메일 대신 문자메시지(SMS)로 하면 '스미싱'(Smishing)이라
- 피싱과 스미싱은 스팸메일과 다릅니다. 스팸메일은 불특정 다수에게 보
인터넷으로 뿌리는 광고전단지랄까요. 스팸메일은 보낸 사람은 정보를 빼가려는 의도는 없습니다. 반면 피싱과 스미싱에는 정보를 빼돌리려는 흑심이 숨어 있습니다. 이메일이나 문자메시지는 겉보기일 뿐, 그 뒤에는 더 거대한 음모가 숨어 있는 거죠.
- 스미싱 방지 원칙, '링크 안 누르기'

"링크인지 모르고 누르는 경우도 많음"

해킹계 정밀유도탄 "스피어피싱"

- 스피어피싱(spear-phishing). 해킹계의 정밀유도탄이라고 보시면 되겠
노리는 피싱 공격을 스피어피싱이라고 합니다. 날카로운 창 끝으로 타깃을
이름이 붙었죠.
- 해킹해 얻은 정보로 특정인을 공격한 수법이 스피어피싱입니다. 지난해 말 사회를 들었다 놨던 한국수력원자력(한수원) 해킹도 스피어피싱 기법을 썼다고 설명했습니다.

"메일 주소나 내용은 아는 사람이 보낸 것인데 일단 확인해봐야"

사회공학 공격 (Social Engineering)

- 담을 넘으면 마치 그 회사 직원처럼 위장합니다. 직원 행세하며 녹아 들
정보를 주로 다루는지, 그 사람이 무슨 시스템을 쓰는지 파악합니다. 그리
보냅니다.
- 이런 식으로 공격 대상의 사회적 맥락을 파악하고 맞춤으로 공격하는 방식을 사회공학 공격이라 부릅니다. 다른 말로는 지능형지속위협(APT)이라고도 합니다. 국가 정보기관도 중요한 정보를 빼돌릴 때 사회공학 기법을 쓴 사실이 드러났습니다.

"회사 직원(특히 상사나 고객)이 보낸 것인데 일단 확인해봐야"

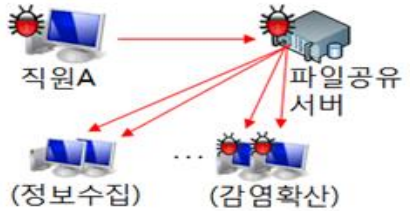
랜섬웨어에 대한 대비 필요

I사 메일을 이용한 APT 공격 공격(스피어 피싱)

① 메일을 통한 내부망 최초 감염 (침투)

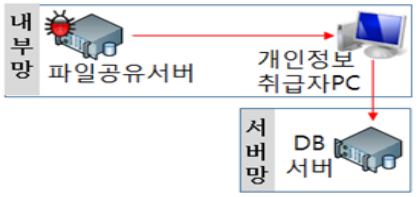
① 해커가 지인을 사칭해 악성코드가 첨부된 이메일을 발송(5.3, 16:38)
② 직원A가 해당 메일을 열람하고 악성코드에 감염(5.3, 17:15)

② 내부망 감염확산 및 정보수집 (검색)



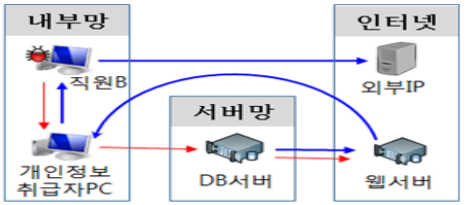
③ 직원A PC를 경유, 파일공유서버 접속 및 악성코드 설치(5.3, 17:41)
④ 파일공유서버를 통해 패스워드 대입공격 수행(감염확산 및 정보수집)

③ 개인정보취급자PC. DB서버 점거 (수집)



⑤ 파일공유서버를 경유, 개인정보취급자PC로 접속(5.4, 23:04)
⑥ 기존 연결 상태를 이용하여 DB서버로 접속(5.5, 02:10)

④ 개인정보 탈취 및 유출 (유출)



⑦ 직원B를 경유, 개인정보취급자PC 및 DB서버에 재접속(5.5, 11:39)
⑧ DB서버의 개인정보를 탈취, 웹서버→취급자PC→직원B PC를 거쳐 외부 유출(5.5 12:08~5.6 02:05)

"② 직원A가 해당 메일을 열람하고 악성코드에 감염" 되는 단계에서 악성코드 감염(설치) 방어 필요

랜섬웨어에 대한 대비 필요

APT 공격에 대응하는 대표적인 방어 기술의 문제점을 해커는 이미 알고 있음

정적 분석 시그니처 기반

이미 수집된 악성코드의 특징을 분석해 해당 악성코드를 탐지 하는 시그니처를 생성하여 비교 분석

새로운 형태의 공격(Zero-Day, Unknown) 에는 대응 불가

동적 분석 가상 행위 기반

가상 환경에서 악성코드를 실행하여 어떤 악의적인 행위를 수행하는지 판단하는 행위 기반으로 악성코드를 탐지

SandBox를 인지하여 우회하는 기술에는 대응 불가

해커들은 샌드박스 특유의 코드를 파악해 샌드박스를 감지해 실행을 하지 않거나 일정 시간동안 실행을 중지하는 등의 지능형 악성코드를 개발. 일정 기간 별다른 악성 행위가 없으면 본 시스템으로 이전시키는 샌드박스 기능의 특성을 이용하여 공략

동적 분석 평판 기반 탐지

악성코드의 실행 형태와 얼마나 유사한 행위를 하는지 측정하여 파일의 악성코드를 탐지

알려지지 않은 악성코드의 실행은 대응 불가

랜섬웨어에 대한 대비 필요

APT 솔루션을 운영하고 있어도 새로운 APT 공격 방어에는 취약

01 Zero-Day 공격	제로 데이 공격(또는 제로 데이 위협, Zero-Day Attack)은 컴퓨터 소프트웨어의 취약점을 공격하는 기술적 위협으로, 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격 출처 : https://ko.wikipedia.org/wiki
02 Unknown 공격	기존 APT 방어 솔루션들은 '알려진 위협'(Known threat)을 차단하고 있어서 '알려지지 않은 위협'(Unknown threat)은 방어가 불가능
03 내부 우회 공격	기존 APT 방어 솔루션은 Perimeter(외부 방벽) 모델로 해커가 우회하여 내부로 진입할 수만 있다면(**메일 수신 이후 등**) 그 이후부터는 정상 유저와 해커의 구분이 어려워 탐지와 조치가 매우 어려움

기존의 APT 솔루션으로는 다양한 형태의 메일 APT 공격에 대한 방어가 취약

Ransomware를 비롯한 모든 Malware 방지를 위한 기본 준수 사항은 최소권한의 실행으로 root 및 특권유저실행을 금지하는 것임

랜섬웨어에 대한 대비 필요

Best Practice for Unix/Linux/Windows Ransomware

Best Practice	설명
최소권한(Least Privilege) 실행	▪ 최소권한의 실행은 root 및 특권유저실행을 금지하는 것이며, Ransomware를 비롯한 모든 Malware 방지를 위한 기본 준수 사항 ▪ 최소권한은 프로그램 및 파일 등 네트워크 리소스 변경을 제한함으로써 랜섬웨어 감염을 최소화 하며, 많은 랜섬웨어들이 보조 도구로 Admin권한의 명령어들을 사용하므로 이를 방지해야 함
File Integrity Monitoring의 실현	▪ 특정 파일 및 Binary의 변동 방지 및 변경내역 트래킹은 위의 최소권한과 통합하는 경우 강력한 리눅스 서버의 랜섬웨어를 비롯한 멜웨어의 감염을 최소화 가능
시스템이나 서버의 최신 상태 유지	▪ 설치된 하드웨어 및 소프트웨어 Checking 및 최신 Patch 유지 ▪ 지속적인 취약점 분석 및 조치 ▪ 구성 상태의 분석 및 조치 (share/Port 등)
회사가 규정해 놓은 소프트웨어외에 설치 금지 (Whitelisting의 실현)	▪ 회사가 정의한 소프트웨어외에는 설치가 가능한 환경을 만들어서는 안됨
네트워크 트래픽에 대한 적극적인 모니터링	▪ 네트워크 트래픽의 Identify, Filter & Block
백업 방안 강구	▪ 최소한의 강구 방안
망분리	▪ Subnet 등

화이트리스팅(Application Control)의 필요성 - UNIX/Linux

Unix/Linux상의 Application Control

- 어떤 명령어의 수행을 금지하고 허락 할 것인가?
- 수행 명령어의 Input & Output Logging

통제 요구 사항

- 어떤 서버나 Switch에 어떤 명령어, 파라미터를 실행 가능하게 할 것인가?
- 금지된 명령어가 스크립트내에 있을 경우 이 스크립트를 어떻게 관리 할 것인가?
- 파일이나 스크립트 등의 수정이나 실행을 어떻게 통제 할 것인가?
- 명령어나 스크립트에 대한 변경이 어떤 권한으로 수행 될 것이고 어떤 권한으로 수행되고 있는가?
- 사용자(계정) 별로 상세한 통제를 위하여 어떤 조합이라도 가능한 룰을 만들 수 있는가?
- 로깅이 단순 명령어 레벨이 아닌 스크립트내에서 수행 또는 외부 명령어 또는 다른 위치에서 수행되는 것에 대한 모든 로깅이 가능한가?
- 단순 명령어 Elevation이 아닌 어플리케이션, 스크립트 Elevation을 어떻게 수행할 것인가?

Sudo로 해결 : 공식적 지원 주체 부재 / sudo 자체의 취약성 존재 / 통합성부재(모든것을 로컬처리) / Policy 관리의 어려움 / 대규모 사이트 적용 부재

PowerBroker 대응

- 모든 APPLICATION CONTROL
- PRIVILEGE ACTIVITY 모니터링 및 KEYSTROKE 로깅
- 권한 위임 : 최소 권한의 할당

Logging의 필요성

Unix/Linux/Windows상의 Logging

- 명령어 Input & Output Logging
- Mouse Click Logging

통제 요구 사항

- 스크린상 또는 키보드 입력 모든 것에 대한 로깅 필요 (Stderr 의 Logging 및 Keyword Search 포함)
- 스크립트내나 Powershell내의 Imbed된 명령어에 대한 로깅 필요
- 콘솔작업의 로깅 필요
- 모든 로그에 대한 중앙화 및 Indexing & Searching 필요
- 윈도우에서도 Keyword Search 필요성

스냅샷을 이용한 동영상 저장 모니터링을 이상 행위 감지를 위해서는 수작업으로 검토가 필요

PowerBroker 대응

최고의 KEYSTROKE LOGGING 솔루션

File Integrity Monitoring의 필요성

Unix/Linux/Windows 상의 파일 관리

- 단순 유저의 파일 접근 관리
- 파일 변화 사항에 대하여 Keystroke Monitoring에 의한 변경 파악
- 파일 변경 내역 파악 및 파일에 대하여 Hash 값 정도의 참조

통제 요구 사항

- 중요 파일의 변동 방지를 단지 Hash 값만 비교 할 것인가?
- 파일의 변경 내역에 대한 일목 요연한 관리의 필요성
- 변조된 파일이나 명령어의 실행이 금지 가능한가
- 스크립트 내에도 Auditing 가능한가?
- 필요시 특정 시점으로 roll back이 가능한가?

중요 파일에 대한 위변조 방지를 위한 파일 접근 통제 필요

PowerBroker : 완벽한 File Integrity Monitoring

- 파일이나 폴더에 대한 LOCATION, OWNERSHIP, PERMISSIONS, SIZE, DATE/TIME, FILE HASH등을 보관 및 변조 방지 및 실행 금지
- 중요 파일들에 대한 변경내역 트래킹(변경/추가/삭제/POLICY 위반)
- 특정시점의 ROLL-BACK (WINDOWS 적용)

네트워크 장비 통합 관리의 필요성

네트워크 장비 관리

- Configuration 중앙관리
- 단순 패스워드 관리

통제 요구 사항

- 유저가 Login한 후 통제 불가능
- 수행되는 명령어 통제 불가능
- Session Logging 불가능
- Active Session에 대한 통제 불가능
- 모든 네트워크 장비에 대한 Audit data의 중앙화 불가능

네트워크 장비에 대한 통합적인 접근 통제 및 모니터링 필요

PowerBroker : 완벽한 네트워크 Monitoring

- 네트워크 장비에 대한 명령어 제어 및 SESSION MONITORING

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

II PowerBroker 중요 기능

UNIX/Linux/Windows OS 특권유저관리 및 Session 관리

세종정보보안 BizHuB

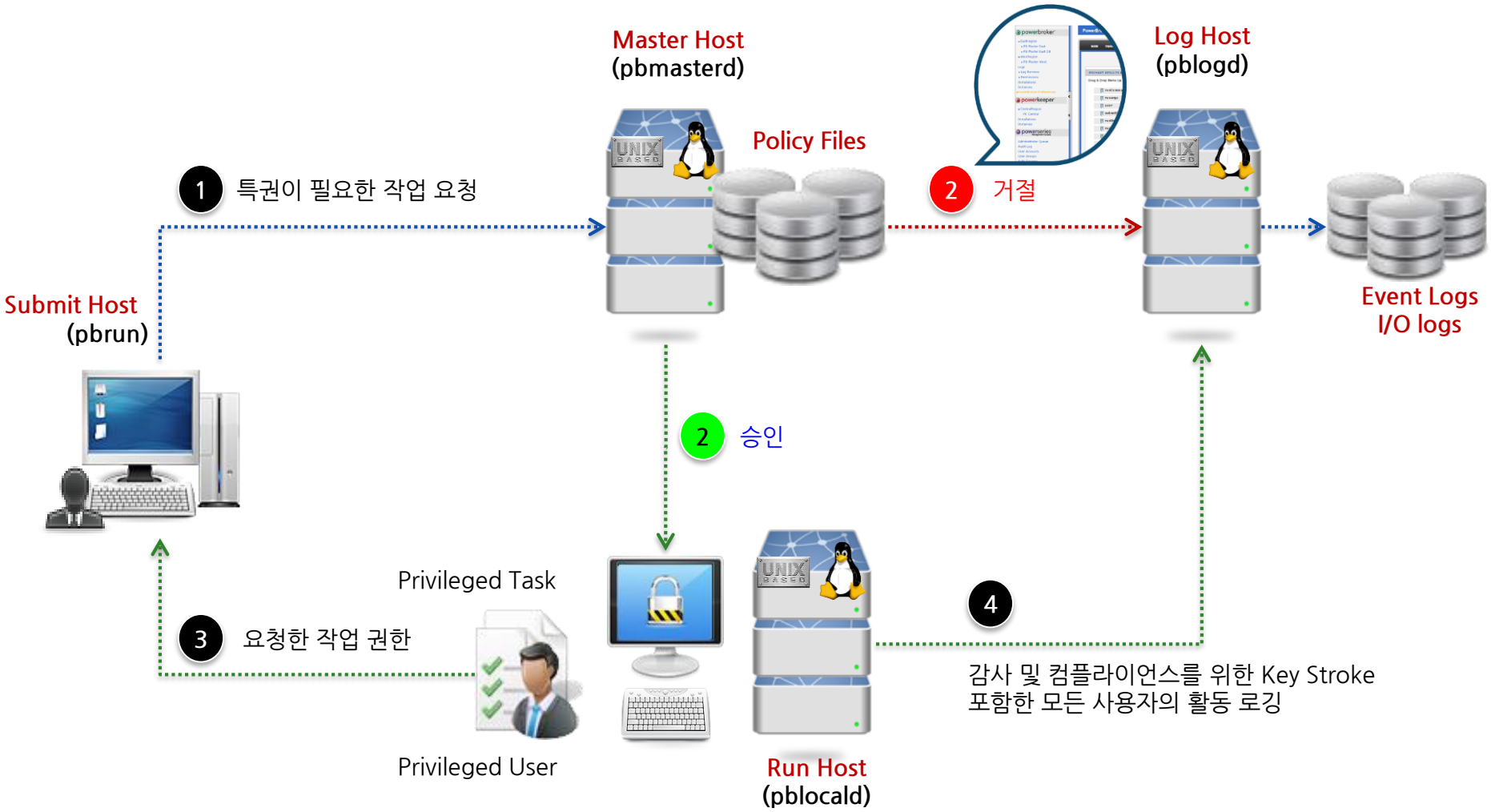
완벽한 특권 권한 관리를 위한 7단계 통합 프로세스

PowerBroker의 7단계 통합 프로세스

1단계	▫ 권한 있는 패스워드에 대한 책임 소재 및 통제 강화
2단계	▫ Windows 및 Mac의 최소 권한 및 어플리케이션 제어 구현
3단계	▫ 어플리케이션 수준의 위험을 권한 결정을 위한 기준으로 활용
4단계	▫ Unix 및 Linux 환경에서 최소 권한 구현
5단계	▫ 중앙 집중의 관리 정책, 보고 및 위험 분석
6단계	▫ Windows 및 Mac, Unix 및 Linux 를 통합하여 권한 통제
7단계	▫ Windows 환경의 변경 사항을 실시간으로 감사 및 복구

PowerBroker for UNIX/Linux/Windows > 솔루션 서비스 개요

PowerBroker 권한 통제 적용



PowerBroker for UNIX/Linux/Windows > 솔루션 서비스 개요

PowerBroker 권한 통제 적용

sudo

- #ls -al /usr/bin/sudo
  -rwsr-xr-x 1 **root** root 159852 7월 4 2017 /usr/bin/sudo
- **setuid**는 명령어 실행 시 임시적으로 사용자의 권한을 파일 소유자 권한(root) 부여
- sudo를 이용하면 root 권한(setuid)으로 명령어를 실행 가능
- 사용자가 아닌 서버 계정(id)로 권한을 임시로 부여하여 통합 관리 및 상세 보안 적용 불가

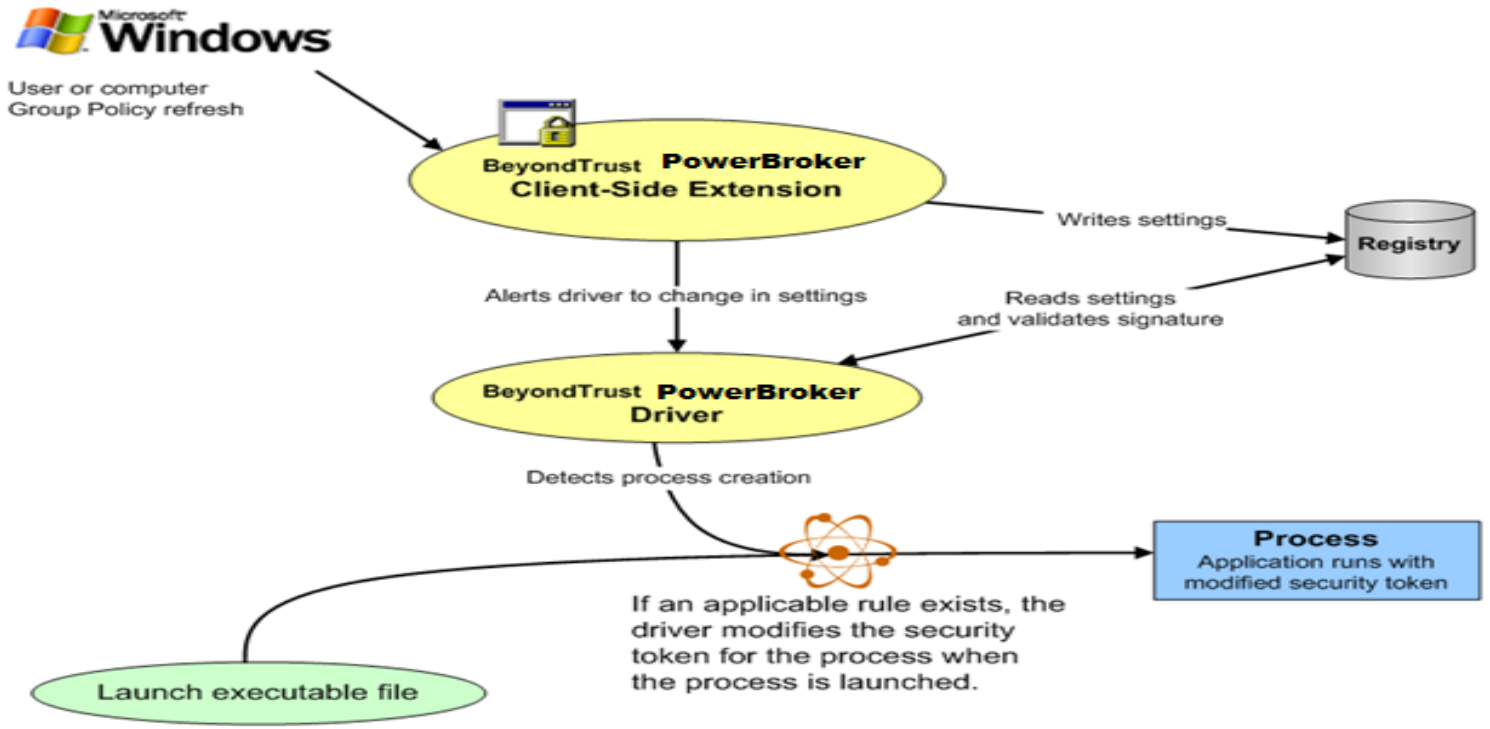
서버의 O/S 계정이 아닌 전체 시스템의 사용자 단위 권한 통제 필요

pbrun

- ls -l /usr/local/bin/pbrun
  -r-**s**--x--x 1 **root** root 1953576 Oct 18 15:28 /usr/local/bin/pbrun
  # ls -l /usr/sbin/pblocald
  -r-x--x--x 1 root root 1925920 Oct 18 15:28 /usr/sbin/pblocald
- **pbrun**은 명령어 실행 시 임시적으로 사용자의 권한을 파일 소유자 권한(root) 부여
- **서버 단위가 아닌 전체 시스템에 대한 사용자 관점의 통합 관리 및 상세 보안 적용**

특허 받은 Elevation 기법

- Elevation시 유저가 속하는 그룹을 변경함으로써 Elevation 하여서는 안됨
- 어느 한 순간이라도 유저가 admin속성을 지니는 그룹에 속해서는 안되며, 유저가 아닌 Process만 elevation 되어야 함
- Windows XP 부터 Windows 2012까지 하나의 Agent에서 처리 가능



PowerBroker for UNIX/Linux/Windows > 솔루션 서비스 개요

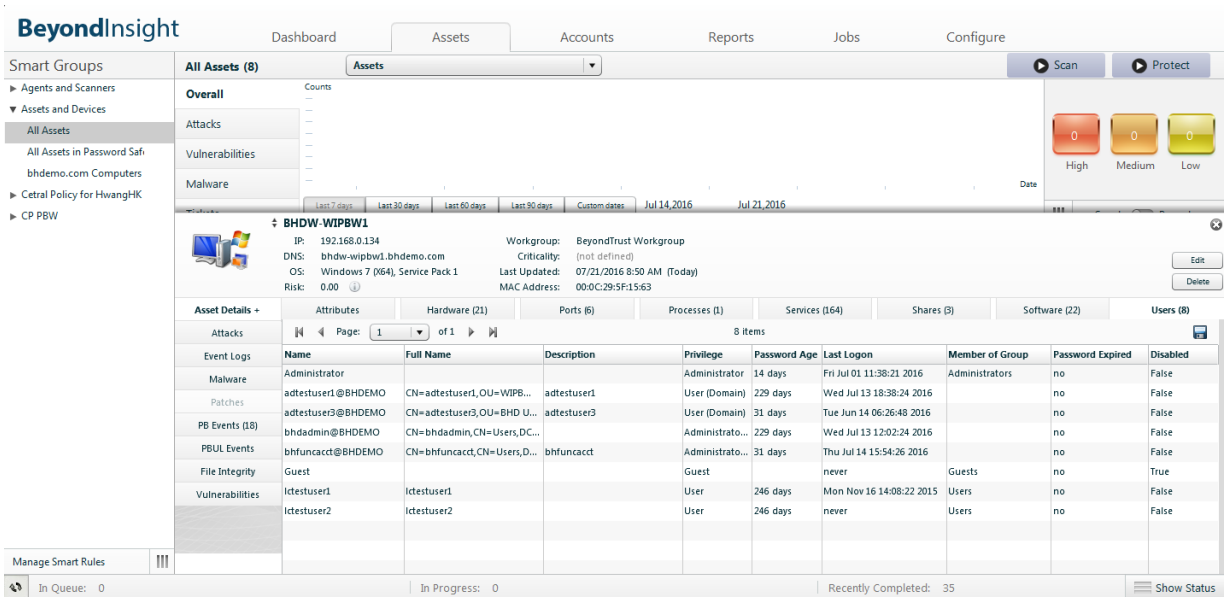
PowerBroker 주요 기능 요약

서버보안강화(최소 권한)	▫ 유저권한분리/공유ID제거 ▫ 최소권한 부여(root/administrator/유/sap등 관리자 권한 제거) ▫ 슈퍼유저의 남용방지
Session 관리	▫ 작업자가 특정 Session 동안 Key-in/Mouse Click한 모든 내역의 Display (Key Stroke Logging) ▫ 키워드 Search 기능
자산 Scanning	▫ H/W, S/W User 등의 사내 모든 자산(UNIX/LINUX/WINDOW/NETWORK등)에 대하여 H/W, S/W User 등의 자산 Scanning & Reporting
Event Logging	▫ 언제 작업을 수행 했는가? , 어떤 유저가 프로그램을 요구 했나 ? ▫ 어떤 시스템에서 작업했는가?, 어떤 프로그램을 시도 했는가 ? ▫ 어떤 시스템에서 Execution 실행하게 했나?, 누가 root 유저로 수행 하였나 ?
File Integrity Monitoring	▫ 중요 파일의 변동 방지 ▫ 파일이나 폴더에 대한 Location, Ownership, Permissions, Size, Date/Time, File hash등을 보관 ▫ 중요 System Binary, Product Binary 나 구성파일들의 위 변조 방지 ▫ 중요 파일들에 대한 변경 내역 트래킹(변경/추가/삭제/Policy 위반) ▫ 변조된 파일이나 명령어 실행금지 및 스크립트내의 Auditing 가능
Application Control	▫ Whitelisting 방식의 Application Control ▫ Ransomware 방지 ▫ 서버나 단말의 설치 소프트웨어 통제

상세 기능 > 자산 Scanning

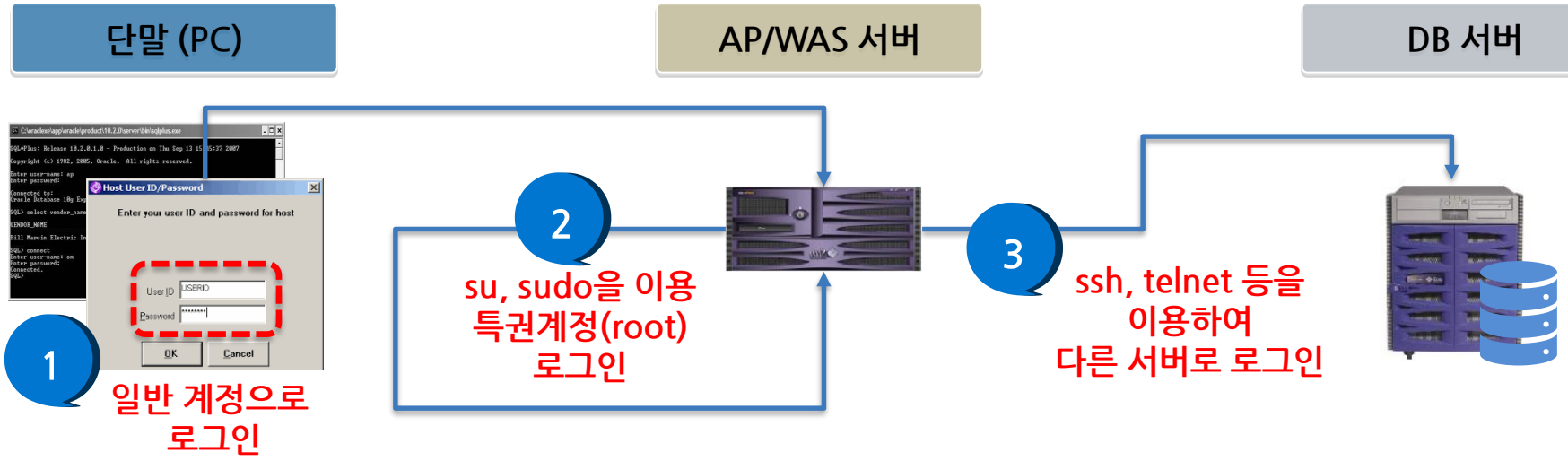
H/W, S/W, User, Process 등의 자산 Scanning

- 접근가능(accessible), 불가능(inaccessible) 그리고 접근여부(no access) 등으로 자산을 관리
- 스캔된 자산을 csv 포맷으로 리포팅하며, 자산 정보는 자산이름, IP address, DNS, domain 과 operating system 정보 등을 포함
- 발견된 자산의 Summary
- 하드웨어 및 모든 발견된 자산의 Delta 값(Port/Port Delta/Service/Service Delta/Software/Software Delta/User/User Delta/Asset Delta 등)



상세 기능 > 권한 상승

권한 상승 통제



단말 접속 프로그램 (putty 등)

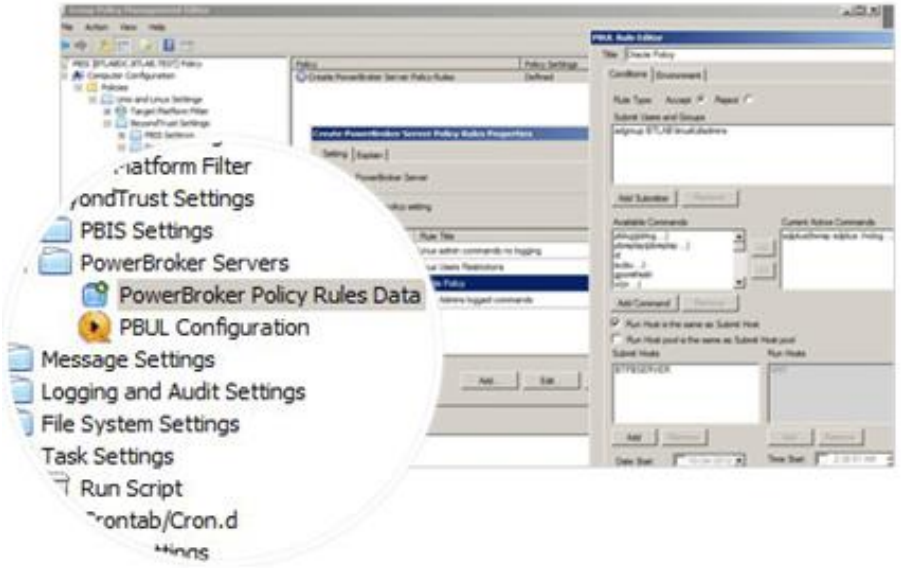
- putty 등을 이용하여 계정 및 패스워드 관리솔루션에서 부여 받은 일반 계정으로 로그인
- 서버에 로그인 후 su, sudo 등을 이용하여 특권 계정(root)으로 로그인
- 서버에 로그인 후 ssh, telnet 등을 이용하여 다른 서버로 로그인

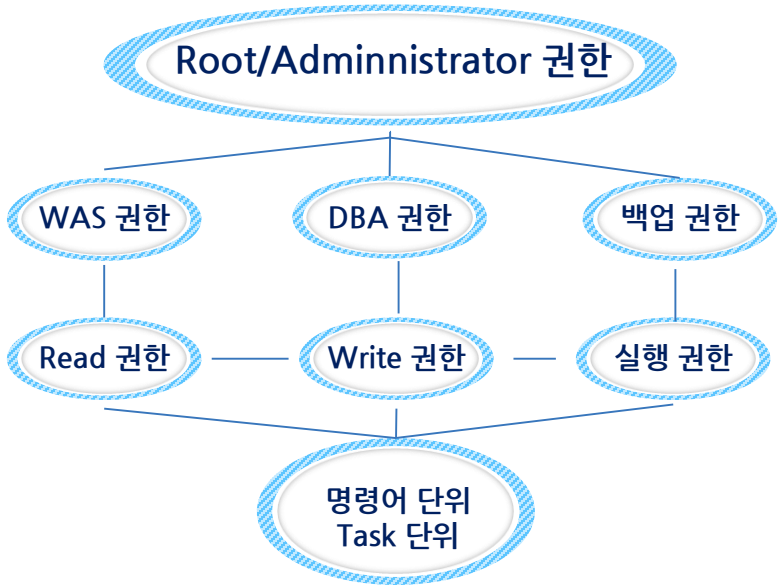
서버 로그인 이후 권한 변경 작업에 대한 통제 적용 필요

상세 기능 > 권한 상승

권한 상승 통제

- root 유저나 기타 특권권한 계정의 패스워드 노출 없이 Unix나 Linux의 특권 권한(Privilege)의 효과적 위임
- 서버(root/administrator) 및 어플리케이션 특권계정(WAS,DBA) 사용 금지
- 외부 작업자/Contractor/Outsourcing 작업자 등의 사용 가능한 작업 권한 분리
- Standard User : Standard User에게 필요한 super user권한을 부여하는 방식은 진정한 SoD를 구현 한다
- root 및 기타 superuser (Oracle/SAP/WAS admin 유저) 유저로 로그인은 Malware 측면 뿐만 아니라 작업자 실수 유발 가능성 상존
- **커널에 영향을 주지 않음(Rebooting 없음)**
- Policy Language 사용으로 무한정 및 유연한의 rule을 만들 수 있어야 함





상세 기능 > Advanced Control & Audit

명령어 레벨이 아닌 시스템 레벨에서 파일의 접근을 관리

입력 String으로 통제 하는 경우 같은 패턴의 정상적인 Script, 명령어 수행도 차단

예: delete, delete_sh_proc, # 주석 :: 특정 데이터를 delete 합니다.

사용자 입력이 아닌 실제로 수행되는 명령어 통제 적용 필요

상세 기능 > Advanced Control & Audit

명령어 레벨이 아닌 시스템 레벨에서 파일의 접근을 관리

- 스크립트 내부의 Activity 까지 명령어 통제 및 Auditing
- 파일이나 폴더에 접근 관리
- 변조되거나 위협이 있는 Binary의 블로킹
- 접속 대상 서버 통제(단말에서 서버 접속, 서버에서 타 서버 접속 등)
- 주요 명령어(shutdown, init, reboot, su, sudo, rlogin, telnet, dd, rm 등) 통제
- Rename 되거나 link된 명령어 통제**(기존 서버 접근통제 솔루션은 통제 불가)**
- 기타 모든 파일 통제

예 제	Powerbroker	타 솔루션
▪ root로 로그인하는 하더라도 shutdown 명령어 사용 못함 ▪ Oracle DBA 유저로 로그인하더라도 sqlplus 사용 못함	▪ root/oracle 특권 유저 사용을 못하므로 룰을 만들 필요 없음 ▪ Root/oracle 특권유저로 로그인 하는 경우라도 Shutdown 명령어를 사용 못하게 룰 설정 가능 ▪ shutdown/sqlplus 명령어가 rename되거나 link되더라도 통제 가능 ▪ shutdown/sqlplus 명령어가 shell script 내에 있어도 통제 가능	▪ root/oracle로 로그인 기본이므로 룰을 만들어야 함 ▪ root/oracle로 로그인 기본이므로 root와 oracle 특권유저는 all mighty 기능이므로 통제룰을 모두 만들어야 함(실제적으로 불가능) ▪ root/oracle 특권유저로 로그인 하므로 로그인 유저가 룰을 마음대로 조작 가능
▪ 정기/비정기적인 작업	▪ 할당된 사용자(일반권한) 에게 본인이 작업할수 있는 비정기 작업 할당	▪ 할당된 사용자(일반 권한)에게 작업 할당하려면 su 로 특권유저로 로그인 한 후 작업 수행 후 로그 아웃

상세 기능> File Integrity Monitoring

File Integrity Monitoring에 의한 권한관리의 통제

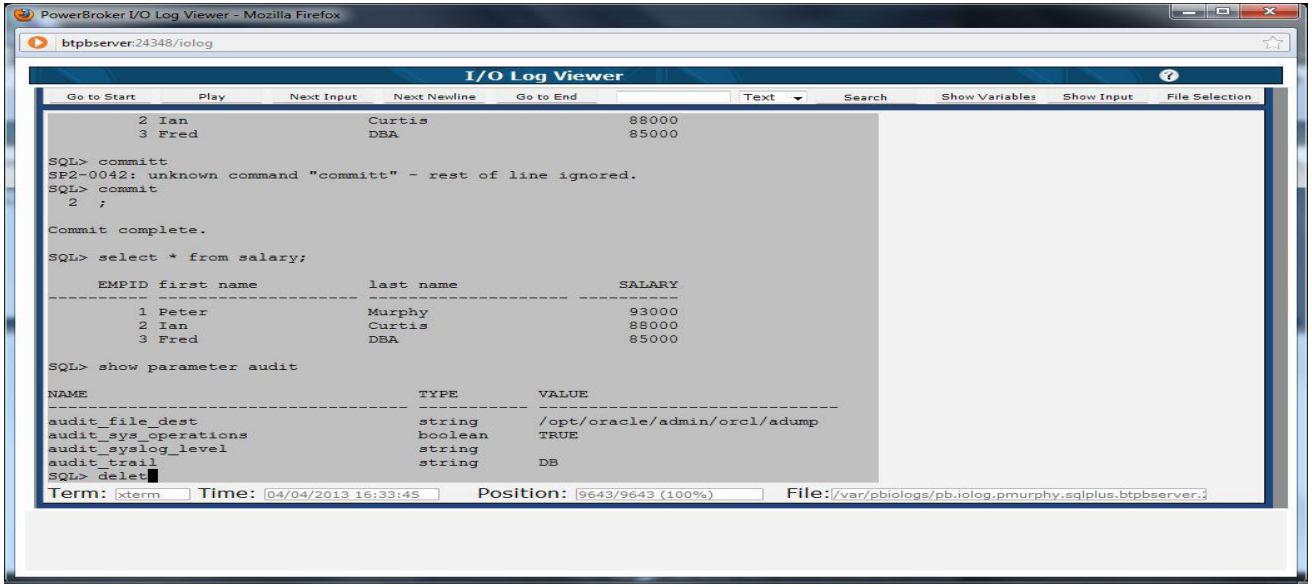
- 모든 서버의 중요 파일에 대한 중앙 집중 관리
- 지정된 중요 파일이 권한상승을 가지고 수행될 경우 심각한 위협 초래
- 선택된 파일이나 폴더에 대한 Location, Ownership, Permissions, Size, Date/Time, File hash등을 보관
- 실행이나 작업시 중요 System Binary, Product Binary 나 구성파일들의 위변조 방지
- 중요 파일들에 대한 변경내역 트래킹 (변경/추가/삭제/Policy 위반)

Name	Location
File Size	Date and Time
Ownership	Hash
Permissions	Policy Violations

상세 기능> IO Logging

Searchable I/O, Log Indexing, Enhanced Reporting

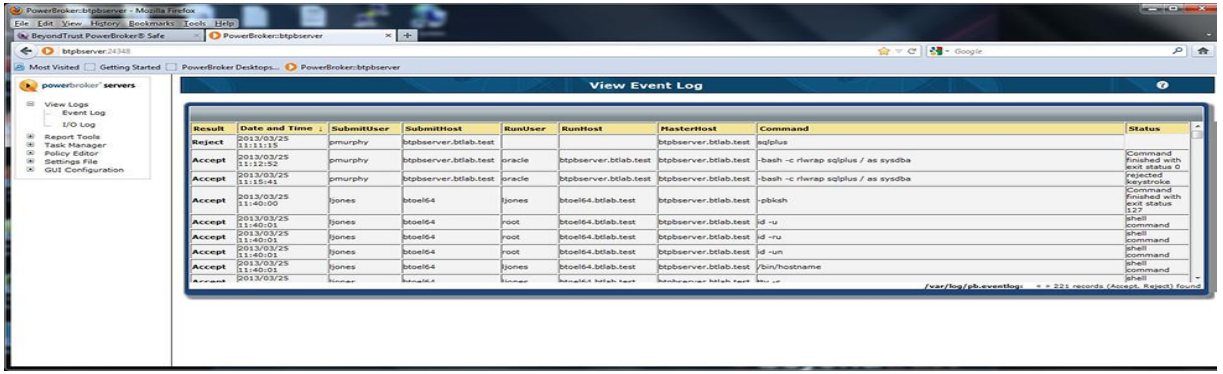
- 작업자가 특정 Session동안 Key-in한 모든 내역의 Display 이는 언제 어디서 Session이 시작되었으며 그에 따른 Output이나 Error 상태의 reply 가능(pbreplay기능) 또한 작업자의 Keystorke 내역을 시스템 관리자가 동시에 볼 수 있으므로 위험스런 작업을 즉시에 정지 가능
- Shell Script내의 작업내역 로깅 가능



상세 기능> Event Logging

모든 작업 수행에 대한 상세한 로깅

- 누가 root유저로 로그인을 시도했는가?
- 언제 request/어떤 유저가 프로그램을 요구했나?
- 어떤 시스템에서 작업했나?
- 어떤 프로그램을 실행했나?
- 어떤 시스템에서 Execution 실행했나?



Who(누가)	when (언제)	where(어디서)	what(무엇을)	Why(왜)	how(어떻게)
업무운영자 A (계정ID: 1234567)	2017년 4월 17일 10시 15분 17초	PC(중요 단말) A에서 DB 서버 S에 접속	/etc/passwd 파일을 편집	신규 사용자 등록 (user01)	vi /etc/passwd

상세 기능 > 네트워크 장비 통제

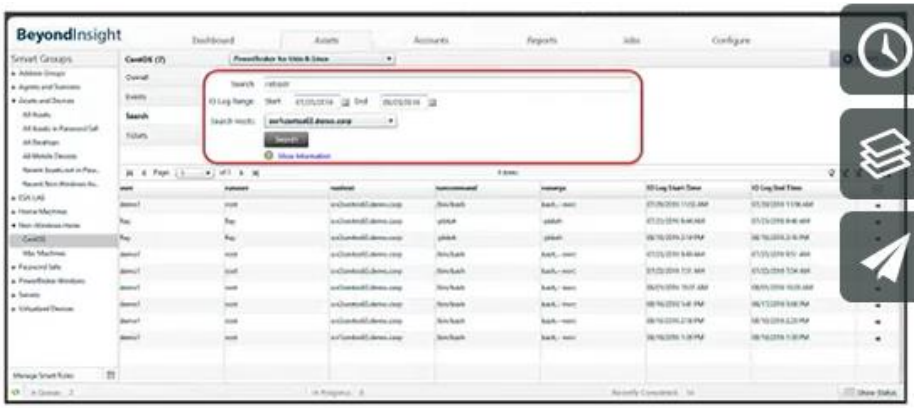
모든 네트워크 장비에 대한 상세한 로깅

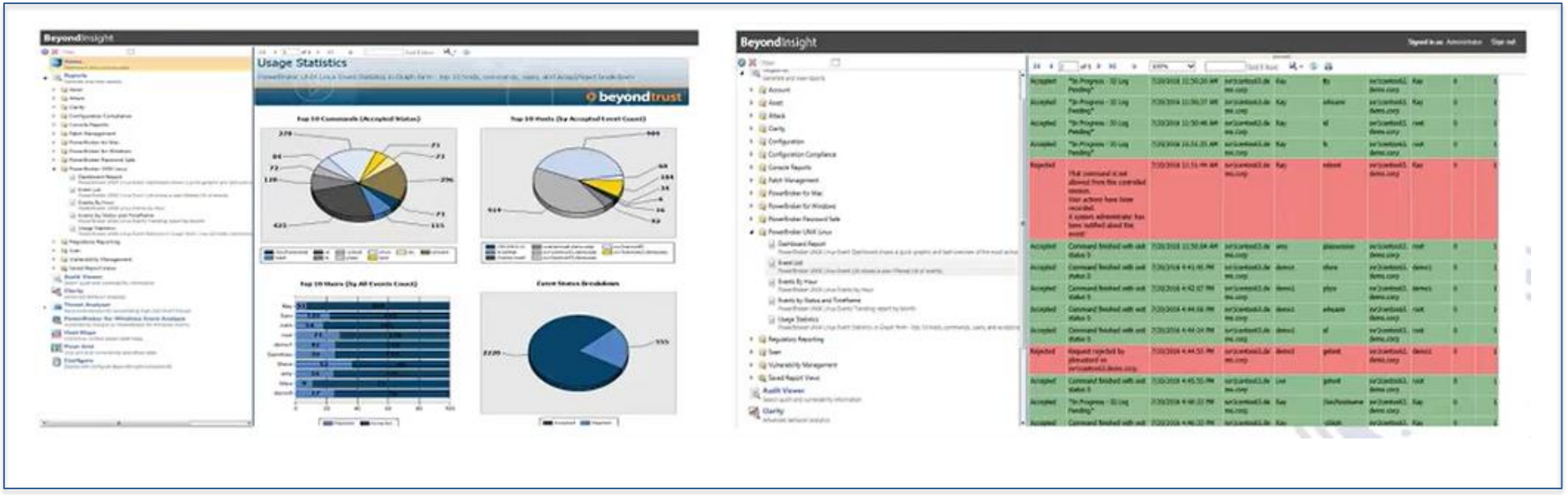
- 완벽한 명령어 제어 (Full Command Control) : 네트워크 디바이스에서 수행되는 모든 명령어 제어
- 감사 및 세션 관리(Audit and Session Recording) : 네트워크 장비에 수행된 모든 명령어 및 세션의 Audit
- 유연한 정책 부여 (Flexible Policy Language) : 정책을 Policy Language로 유연하게 부여 함으로써 단순 Blacklisting이 아닌 가능한 모든 정책의 부여
- Data Driven Policy : Policy의 외부 소스 이용 가능(예, 데이타베이스,LDAP query)
- 세션 실행 제어 (Session Termination) : 유저가 사용하는 세션을 실시간 관리자에 의한 통제
- 명령어의 Whitelisting/Blacklisting 통제 : 명령어의 Accepting(Blacklisting) or Denying(Whitelisting) 기능 가능
- SSO (Single Sign-on) 제공 : PBPS(PowerBroker PasswordSafe)나 타 패스워드 관리 솔루션 연동 시 proxy 연결을 통한 SSO 기능 제공
- Syslog 지원 : 모든 또는 일부 action에 대하여 syslog를 통한 SIEM등에 전달
- User Message 변경 지원 : Prompt user, message of the day, Warning, One-time Message등의 부여 가능
- Rest Interface : Policy 관리를 위한 API 제공

상세 기능 > 상세 포렌직 & 리포팅

모든 작업 수행에 대한 상세한 로깅

- Searchable Index
- Scheduled Reporting
- Custom Reporting





BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

III 접근통제 및 패스워드 관리 기능

전사적 패스워드 관리 및 세션 모니터링(시스템 접근제어)

세종정보보안 BizHuB

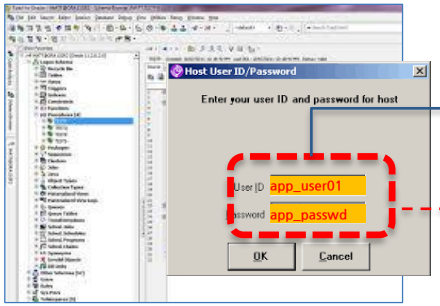
접근통제 및 패스워드 관리 기능

계정관리 및 패스워드 관리 솔루션을 적용한 경우에도 Application Source내에 하드코딩 된 계정 정보를 이용하여 서버 및 DB에 접속하는 경우에 대한 통제 방안 필요

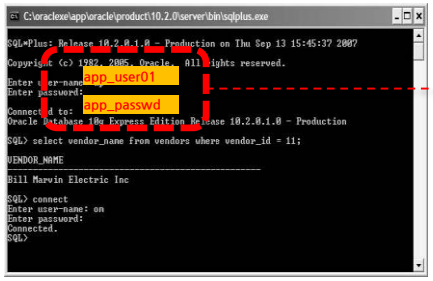
단말 (PC)

계정 및 패스워드 관리 솔루션

서버(O/S)



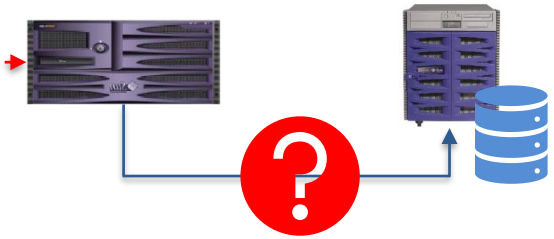
DB 접속 프로그램 (Toad 등)



단말 접속 프로그램 (putty 등)

AP/WAS 서버 등

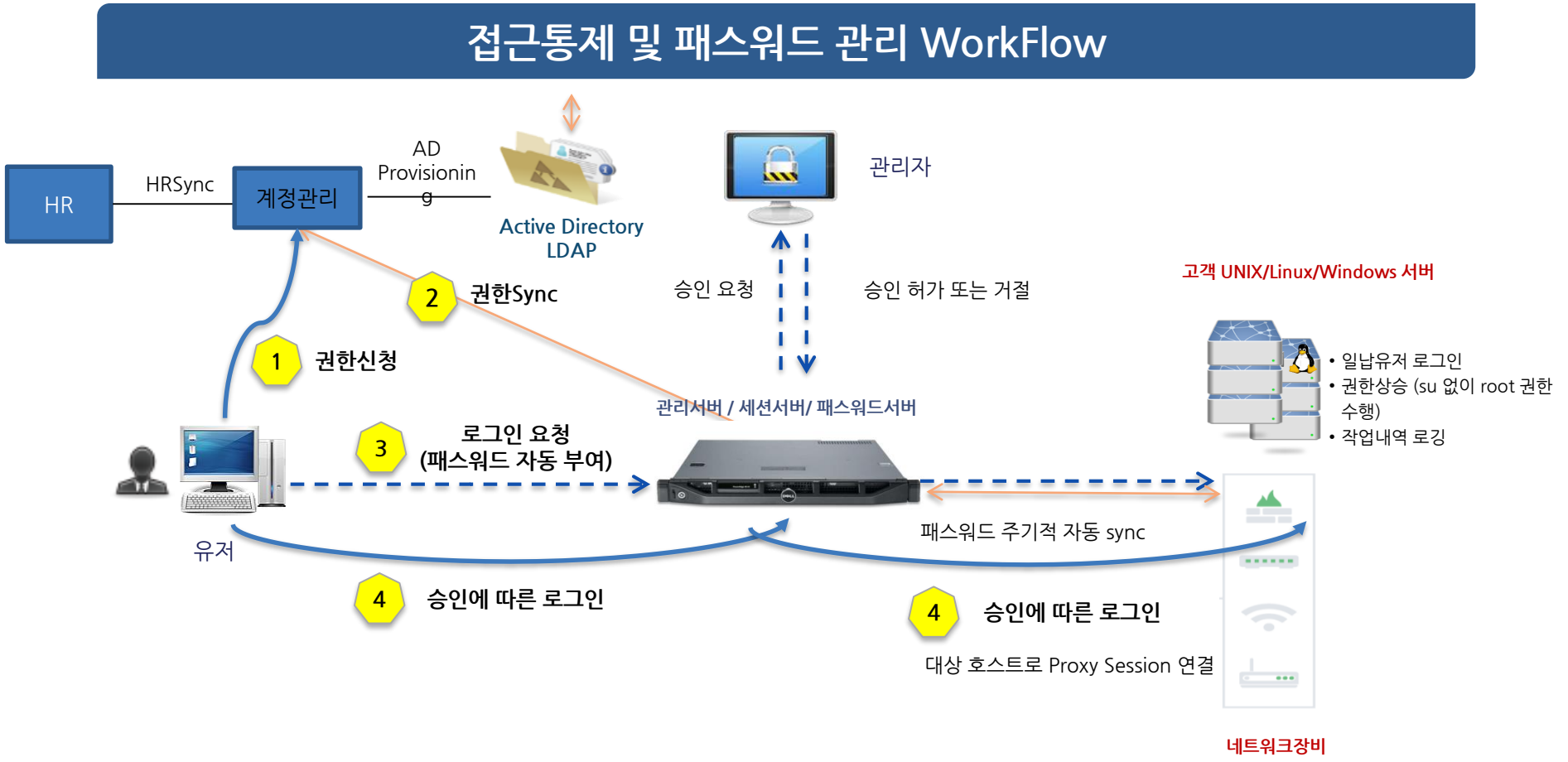
DB 서버 등



```
char *username = "app_user01";
char *password = "app_passwd";

EXEC SQL CONNECT :username IDENTIFIED BY :password;
```

- 일반 계정은 계정관리 및 패스워드 관리 솔루션에서 통제하므로 사용 불가
- Application 운영을 위한 계정을 이용하여 작업을 수행하는 경우 통제 불가
- 특히 서버에 접속하여 Application 계정을 이용하여 작업을 수행하면 통제 불가

접근통제 및 패스워드 관리 기능



- 사용자는 패스워드를 입력하지 않음 : 패스워드 입력 방식은 Pass-the-Hash에 의한 패스워드 절취 가능성
- 패스워드 자동 관리와 세션 로깅이 동시에 수행
- 세션에 로그인 하자 마자 패스워드 변경 가능 (절취된 패스워드 사용 못함)

접근통제 및 패스워드 관리 기능

PowerBroker 접근통제 및 패스워드

자산 Scanning

- H/W, S/W, User 등의 사내 모든 자산 Scanning 및 Reporting

Session 관리(접근통제)

- Keystroke, Mouse Click 등 사용자 작업 기록
- 키워드 Search 기능

Password 관리

- 서버, 네트워크, 데이터베이스, Application 등 전사적 패스워드 관리
- 시스템 접근 시 작업자의 Single Sign-on 제공
- ssh key 관리/서비스계정관리

명령어 관리

- 실시간 행위 Alert
- Command Blacklisting
- Hostname or IP Address Monitoring

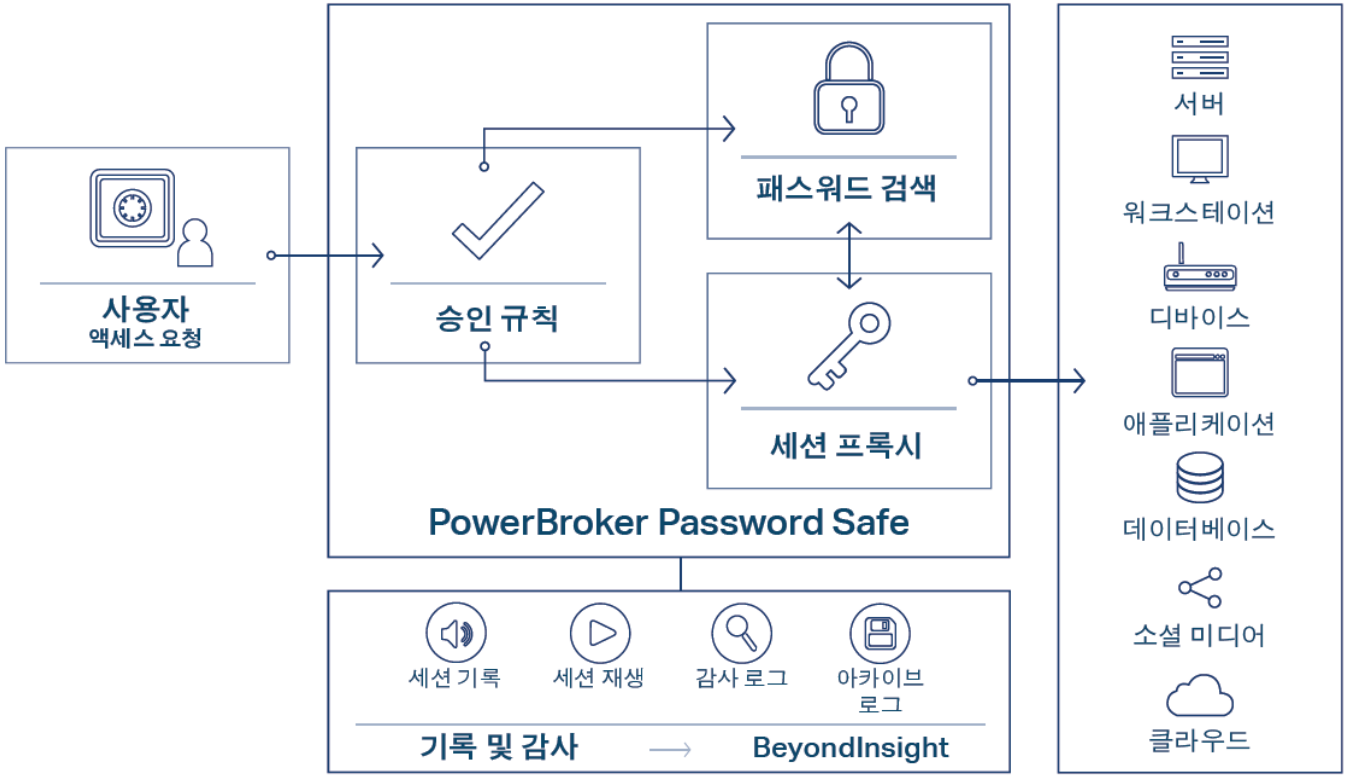
통합관리 Appliance : PBPS

- PASSWORD관리/SESSION관리/자산 SCANNING/명령어제어 등을 동시에 수행
- 단독 APPLIANCE 또는 가상머신
- 하드디스크와 저장 패스워드의 이중 AES256 ENCRYPTION
- AD/LDAP INTEGRATION
- 풍부한 REPORTING
- 4가지 기능을 하나로 통합

접근통제 및 패스워드 관리 기능

사용자 패스워드 발급 · 회수하는 제어 기능 제공

PowerBroker Password Safe는 모든 infrastructure를 대상으로 사용자 패스워드 요청에 대하여 안전한 방법으로 패스워드 발급 · 회수하는 제어 기능을 제공



접근통제 및 패스워드 관리 기능

패스워드의 자동 발급, 접근제어(세션), 어플리케이션 Access를 One-Click에 실행

- 사용자에게 로그인 SSO 제공
- 사용자는 패스워드를 Key-in 하지 않고 시스템에 접근
- PBPS와 시스템 사이의 패스워드 자동 Sync
- 패스워드는 주기적 변경,로그온시 바로 변경,이벤트 발생에 따른 변경
- 세션 모니터링 및 로깅, 그리고 명령어 제어가 동시 수행

접근통제 및 패스워드 관리 기능

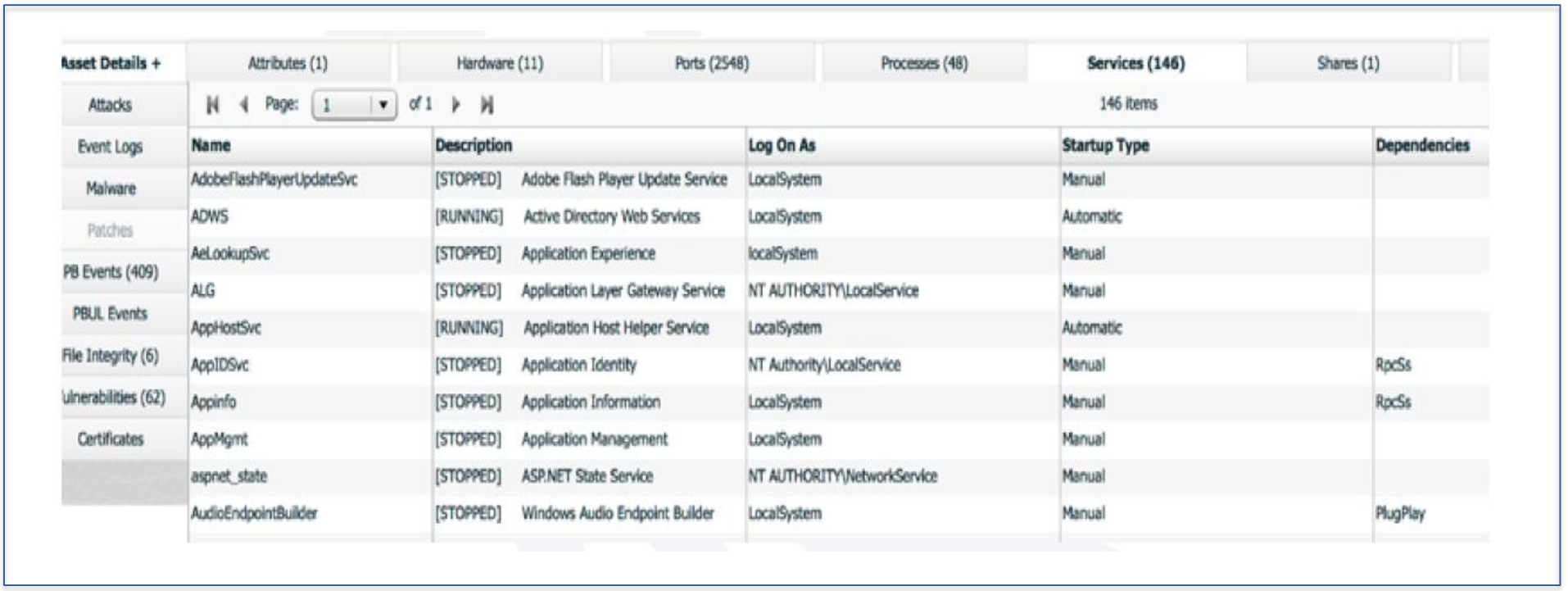
서비스 어카운트의 패스워드 자동 파악

01 발견 (Discovery) & 저장 (Inventory)

PBPS에 포함된 DART Scan 엔진은 서비스 계정을 포함한 모든 Privileged Account를 검색하여 보고

02 개선(Remediate) & 자동화(Automation)

패스워드 변경의 스케줄링 및 자동화



접근통제 및 패스워드 관리 기능

SSH 키 관리

- 사용자가 SSH Key 세션에 접근을 즉시 또는 워크플로우를 통하여 수행
- SSH key는 절대 노출되지 않는다
- 완전 자동화된 SSH Key 변경
- SSH Key Release 시 실시간 통보
- SSH Key Session의 완벽 녹화 & Replay
- 패스워드 Authentication으로 자동 Fail-Over

접근통제 및 패스워드 관리 기능

하드코딩 패스워드 관리

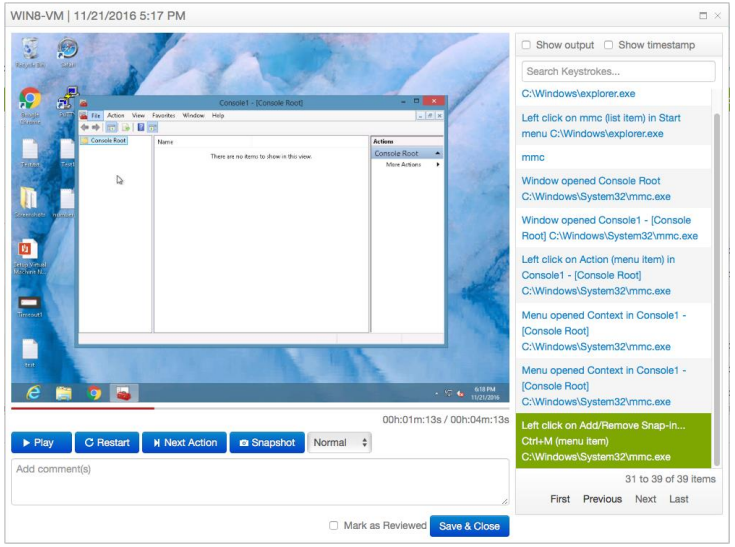
- 어플리케이션이나 스크립트에서 하드코드 패스워드 제거
- C/C++, Perl, Net, Java등 다양한 언어를 지원하는 Rest API
- 사용시 패스워드의 자동 변경가능

```
            Console.WriteLine("\t" + passwordRetrievalResponse.StatusCode);
            Console.WriteLine("\t" + passwordRetrievalResponse.Content.ReadAsStringAsync().Result);
            return;
        }

        string responseString = passwordRetrievalResponse.Content.ReadAsStringAsync().Result;
        Console.WriteLine("-- Retrieved Password (Encrypted) --");
        Console.WriteLine(responseString);
    }

    private static void ReleasePassword()
    {
        /*****************************************************
         *
         * Release a password
         *
         *****************************************************/
        Console.WriteLine("\n-- Release a Password --");
        Console.Write(">> Request ID: ");
        string requestIdInput = Console.ReadLine();
        Console.Write(">> Comment (optional): ");
        string releaseComment = Console.ReadLine();

        PasswordReleaseModel passwordReleaseModel = new PasswordReleaseModel();
        passwordReleaseModel.requestId = Convert.ToInt32(requestIdInput);
        passwordReleaseModel.reason = releaseComment;

        StringContent passwordReleaseContent = new StringContent(JsonConvert.SerializeObject(passwordReleaseModel));
        passwordReleaseContent.Headers.ContentType = new MediaTypeHeaderValue("application/json");

        Uri passwordReleaseUri = new Uri(BASE_API_URL + "/ReleasePassword");
        HttpResponseMessage passwordReleaseResponse = client.PostAsync(passwordReleaseUri, passwordReleaseContent).Result;

        if (!passwordReleaseResponse.IsSuccessStatusCode)
        {
            Console.WriteLine("\n\n\tError: ReleasePassword");
            Console.WriteLine("\t" + passwordReleaseResponse.StatusCode);
            Console.WriteLine("\t" + passwordReleaseResponse.Content.ReadAsStringAsync().Result);
            return;
        }
        else if (passwordReleaseResponse.StatusCode == HttpStatusCode.NoContent)
        {
            Console.WriteLine("\n\t[Password Released]\n");
        }
    }
}
```

접근통제 및 패스워드 관리 기능

Session Recording

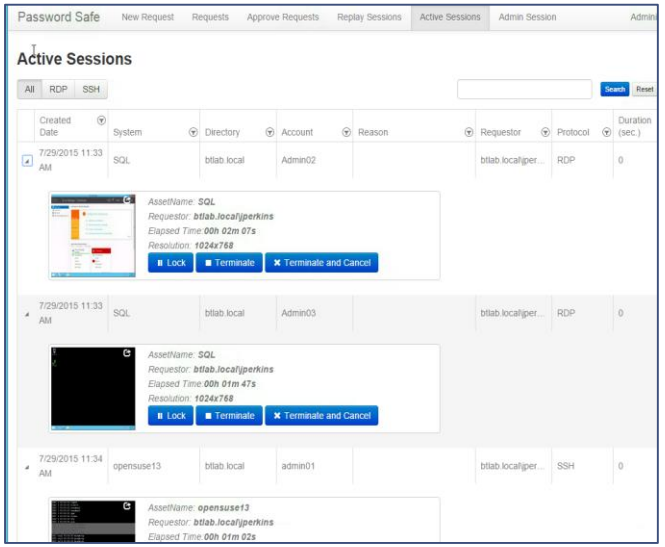
- 모든 행위로 인한 Keystroke는 저장되고 Indexed & Searchable하다
- 행위에 Click 만으로 화면으로 Jump
- 동영상 방식 저장이 아닌 snapshot을 유저나 시스템에 따라 선별적 관리
- Timestamp 제공
- Windows 장비의 Keystroke에 대하여 Keyword search 가능
- Input 뿐만 아니라 Output도 Keyword Search



접근통제 및 패스워드 관리 기능

Live Session 관리

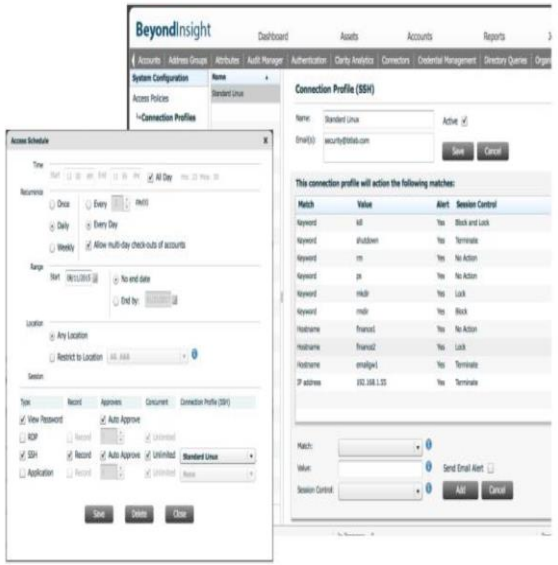
- Dual Control 가능
- 관리자가 세션을 스톱 시킬수 있는 “Lock” 옵션 제공
- 유저를 세션에서 Disconnect 항수 있는 “Terminate” 옵션 제공
- 유저를 세션에서 Disconnect하고, 재 연결 할 수 없도록 하는 “Terminate & Cancel” 옵션
- 어플리케이션을 killing 하지 않고 보안팀에서 이상행위를 체크 가능케 함



접근통제 및 패스워드 관리 기능

명령어 관리

- Real-time Activity Alerts : Keyword, Hostname, IP-address를 근간으로 한 email alert
- Command Blacklisting : Block command, Lock session, Terminate Session
- Hostname or IP address Monitoring : 특정 호스트나 Address에서 작업시 Lock or Termination
- 세션이 연결된 후 UNIX/Linux/Jump호스트를 활용하여 명령 또는 스크립트 실행



BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

IV PowerBroker 기능 비교

PowerBroker와 기존 보안 솔루션 기능 비교

세종정보보안 BizHub

접근제어솔루션 vs PowerBroker

▪ 시스템 접근통제, DB 접근통제, 통합 계정관리, Secure O/S 등 다양한 보안 솔루션을 운영하고 있는데 PowerBroker가 왜 필요한가?

- 시스템 접근통제 등 기존 솔루션은 사용자가 입력한 내용(String)으로 통제
- 명령어를 변경(rename, alias 등)한 경우 통제 불가 : rm != rr
- Script 등을 이용하여 명령어를 숨기는 경우 통제 불가 : rm != r.sh
- 콘솔 등 시스템 접근통제 장비를 경유하지 않는 명령어 수행 통제 불가
- Secure O/S는 O/S Kernel 변경이 필요하고 사용자별 통합 관리가 불가

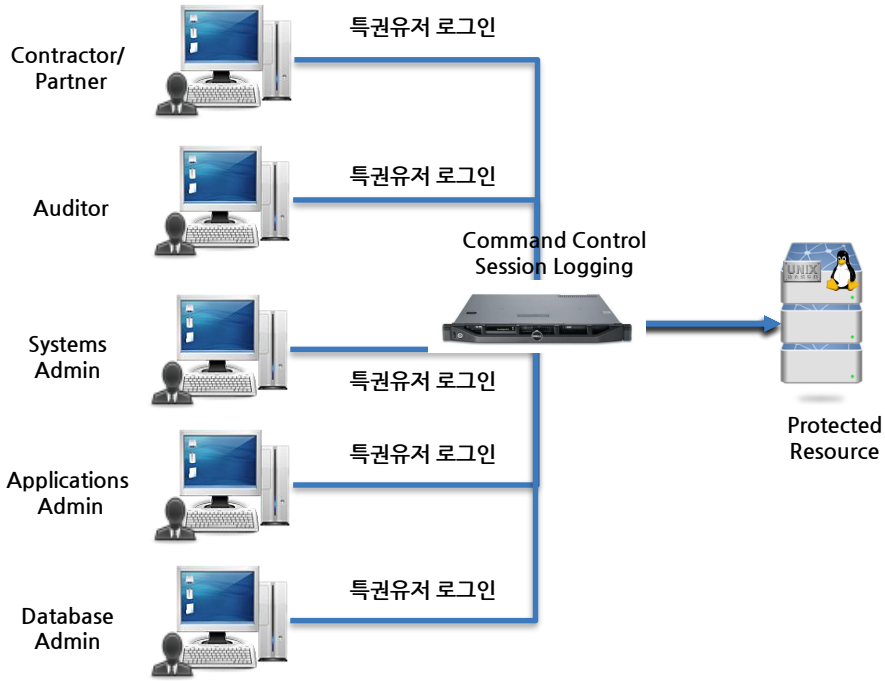
PowerBroker : 전사적 서버 작업 통제

항목	상세내용	
계정 통제	계정 부여	작업자 별 1인 계정 부여
	계정 통제	서버 접속을 위한 특권 계정 사용 및 접속 금지 (root,asministrator,oracle,was,sap)
접속 통제	접속 프로그램	서버 접속을 위한 단말 프로그램 통제 (putty 외 설치 금지등)
	접속 서버	서버 접속을 위한 특권 계정 사용 및 접속 금지 (root,asministrator,oracle,was,sap)
	우회 차단	특정 IP대, 특정 시간대 접속 기능
	계정 변경	su, ssh , telent, rlogin 등 계정 변경 명령어 통제
작업 명령어 통제	통제 적용	1인 1계정에 각 계정 마다 필요한 권한 부여 (각 계정에 각 명령어 단위 할당 가능)
	명령어 통제	Whitelisting/Blacklisting 방식의 명령어 통제
		명령어 위 변조 통제, 위 변조톤 명령어 통제 (Alias or rename)
		Script 및 프로그램내의 명령어 통제
		콘솔 작업 통제
	결재 기능	주요 명령어 수행 시 OTP 연동 또는 승인
	로그 관리	언제/누가/어떤 시스템에서/어떤 프로그램을 시도/어떤 시스템에서 실행/수행 여부/누가 root유저로 시도
		Link, rename된 명령어 로깅, Script 내의 명령어 실행 내역 로깅
		Searchable Indexing, Windows도 Keyword search
패스워드 관리	서비스계정관리	서비스 계정 Password 관리
	ssh key 관리	ssh key search & 관리
	어플리케이션 하드코드	어플리케이션 내의 하드코드된 유저 패스워드 관리

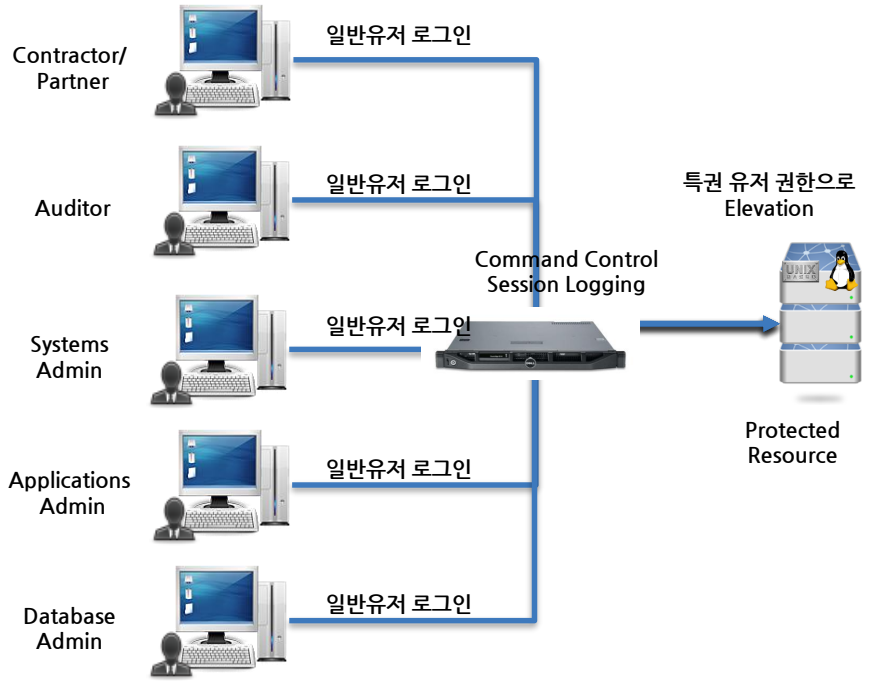
접근제어솔루션 vs PowerBroker

- 접근제어 솔루션은 주로 Appliance를 Proxy로 하여, 서버에 접근을 통제하는 솔루션으로 부수적으로 명령어 제어 기능을 가지고 있으나, 유저의 권한 제어를 하지는 못함
- PowerBroker는 Proxy 방식에 의하여 접근을 통제 가능하며, 명령어 제어는 Proxy방식 또는 Agent 방식으로 가능하고, 유저 권한 통제 기능 제공

접근통제 솔루션



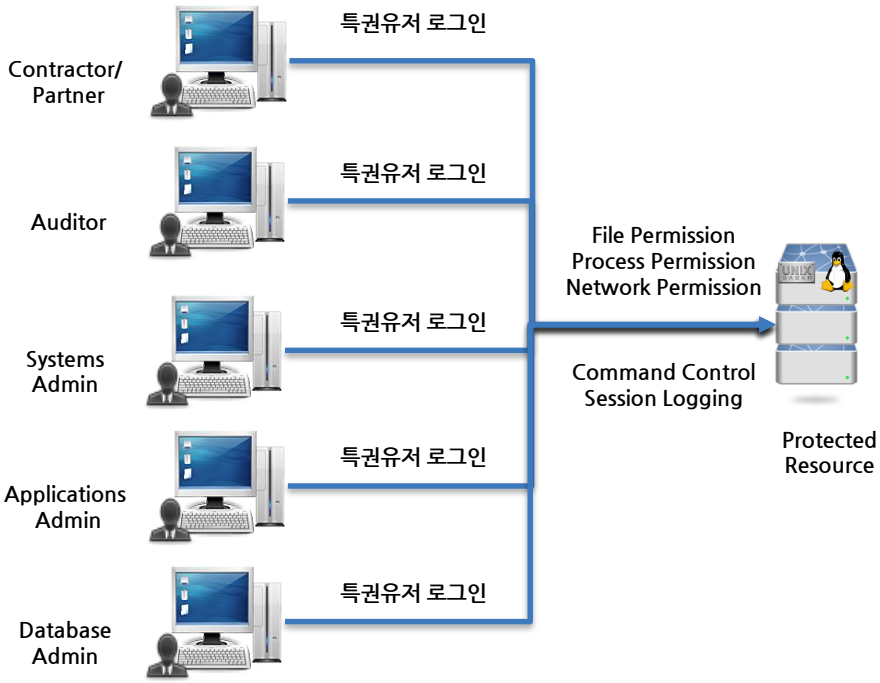
PowerBroker



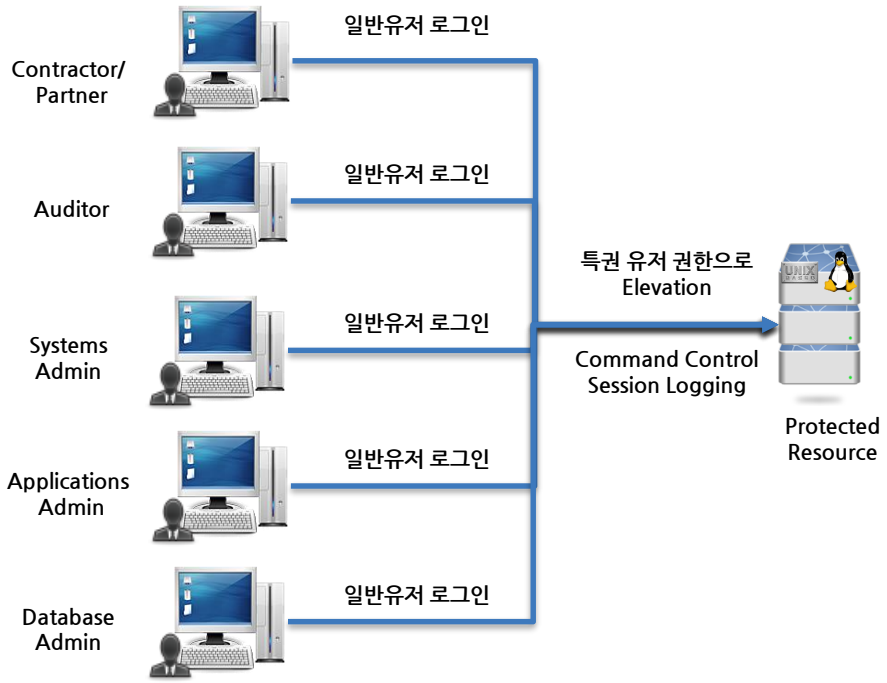
SecureOS vs PowerBroker

- PowerBroker는 Privilege(Access Control 포함) 솔루션이고, SecureOS는 Access Control 제품
- PowerBroker는 권한의 위임 및 상승, 그리고 특권 유저 관리에 중점을 두고 있는 반면, SecureOS는 Permission control에 주안점을 두고 전반적 접근 관리 치중

Secure OS 솔루션



PowerBroker



SecureOS vs PowerBroker

배치작업 통제 비교

단계	검토내용	담당부서
개발	본사 IT 본부 산하 개발자	은행 개발 부서
등록	본사 IT 본부 산하 개발자들이 등록	은행 개발 부서
수행	협력사 소속 OP들이 24시간 모니터링 및 이상현상 발생시 본사 IT 인력에 보고	협력사 OP
장애 대응	개발자들이 로그 확인 할 수 있는 계정으로 로그인하여 로그 확인후 조치	은행 개발 부서
서버 작업	별도 작업공간에서 책임자 승인 하에 서버 접속 작업	은행 시스템 부서

Secure OS 솔루션

- ✓ 은행소속과 협력사 소속을 개념적으로는 분리 가능
- ✓ 각 작업자의 Identity 분리 가능
- ✓ 각 작업자에 업무에 따라 그룹을 부여(업무개발/업무운영/시스템운영/모니터링 등)
- ✓ 그룹에 따른 명령어 통제
- ✓ 배치 작업의 권한이 주어진 특권 유저(그룹 할당)로 로그인하여 시스템부서/협력업체/개발부서가 각자의 일을 정확히 할당 곤란 등
- ✓ 서버 작업을 위하여서는 su로 root의 full 권한 획득 가능
- ✓ 그룹에 정해진 룰 이외에 다른 권한 획득의 어려움
- ✓ 서버 작업자나 개발자가 본인 작업 이외에 의도적/비의도적 변경 가능 (su사용 또는 각 권한의 특권 유저로 로그인)
- ✓ 배치 Shell 내 또는 Crontab내의 각각의 작업에 대한 로깅 불가능
- ✓ SU의 사용이나 각자 기능의 특권 유저로 로그인 하기 때문에 명령어 잘못 사용 가능

PowerBroker

- **은행소속과 협력사 소속을 개념적으로는 분리 가능**
- **각 작업자의 Identity 분리 가능**
- **각 작업자에 업무에 따라 그룹이 아닌 특정 Task 부여(그룹 부여도 가능) 따라서 다양한 룰 작성 후 할당의 편리성**
- **유저에(또는 그룹)따른 명령어 통제**
- **각 작업자가 일반유저로 로그인하여 각자에 주어진 일만 수행 가능 특권 유저로 su 가 아닌 일반 유저에서 root나 특권유저 권한 부여**
- **여러가지 룰을 그때에 따라 작업 대상에 부여 가능**
- **배치 Shell 또는 Crontab내의 모든 명령어에 대한 로깅 가능**
- **금칙어등은 룰로 부여된 경우를 제외하고는 사용하기 어려움 또한 룰로 부여 되어도 OTP등의 2차 검증 가능**

PowerBroker vs 타 솔루션

기능	Powerbroker	SecureOS	접근제어 솔루션
총평	▪ 권한(Privilege) 제어 솔루션 ▪ 권한의 위임 상승 가능 (완벽한 RBAC) ▪ 특권유저 제거 가능 ▪ 시스템레벨 명령어 콘트롤 가능 ▪ 접근제어 가능 ▪ 유닉스/리눅스/윈도우스(서버/단말)/맥 모두 가능 및 동일 기능	▪ Permission 제어 솔루션 ▪ 권한 위임 상승 일부 가능 (일부 RBAC) ▪ 특권유저 일부 제거 가능 ▪ 시스템레벨 명령어 콘트롤 일부 가능 ▪ 접근제어 불가능 ▪ 유닉스/리눅스/윈도우스서버 모두 가능 하나 주로 유닉스 서버 기능 ▪ 단말 통제 기능 없음	▪ 접근(Access) 제어 솔루션 ▪ 권한 위임 상승 일부 가능 (일부 RBAC) ▪ 특권유저 제거 불가능 ▪ 시스템레벨 명령어 콘트롤 불가능 ▪ 유닉스/리눅스/윈도우스서버 모두 가능 하나 주로 유닉스/리눅스 서버 기능 ▪ 단말 통제 기능 없음
동작 방식	▪ Agent Based (접근제어는 Proxy 방식)	▪ Agent Based	▪ Proxy 방식
커널모드작동	▪ 비 커널 모드로 작동 ▪ 인스톨시부터 Rebooting 필요 없음	▪ 커널 모드에서 작동 ▪ 커널 모드 작동 솔루션은 커널 모드로 작동함으로써 많은 충돌이 발생함 ▪ 커널 모드는 운영체제 또는 자체 또는 주변 어플리케이션이 Upgrade되면 어떤 충돌 문제를 야기할지 모르는 단점을 가지고 있습니다	▪ 비 커널 모드 작동
Least Privilege	▪ - 가능 ▪ (서버를 셧다운하거나 리부팅하는 명령어(shutdown, reboot)는 1921921921 IP 에서 honggildong 계정으로 접속한 뒤, 이 명령어를 지속적으로 일반 유저 계정인 honggildong 의 user context 상에서 실행을 허용하고, 나머지 모두 실행을 거부하며 허용과 위반 감사로그를 모두 기록한다 또한 이 명령어가 언제나 1921921921 IP상에서만 또는 다른 서버 상에서만 실행되도록 통제한다)	▪ 일부 가능 ▪ (서버를 셧다운하거나 리부팅하는 명령어(shutdown, reboot)는 1921921921 IP 에서 honggildong 계정으로 접속한 뒤 root 로 su하였을 때만 실행을 허용하고 나머지 모든 접근은 거부하며 허용과 위반 감사로그를 모두 기록한다) ▪ 일부 가능하지만 주로 SU 이용 ▪ su는 통제 대상이 아닌 제거 대상	▪ 불가능 ▪ (서버를 셧다운하거나 리부팅하는 명령어(shutdown, reboot)는 1921921921 IP 에서 honggildong 계정으로 접속한 뒤 root 로 su하였을 때만 실행을 허용하고 나머지 모든 접근은 거부하며 허용과 위반 감사로그를 모두 기록한다) ▪ 권한의 분리는 가능하나 최소권한 부여는 하지 못한다 ▪ su를 이용하거나 반드시 특권유저 로그인을 기본으로 한다

PowerBroker vs 타 솔루션

기능	Powerbroker	SecureOS	접근제어 솔루션
root 유저 관리	▪ 특수 상황 제외하고는 root 유저로 login을 불가능 하게하여, 일반 유저에 root 유저 권한을 부여하는 Whitelisting 방식 ▪ root 유저의 해킹을 원천 봉쇄 ▪ 특권 유저 권한 관리에 중점	▪ root 유저 login을 기본으로 하여 root 유저의 권한을 제한하는 방식 ▪ root 유저가 해킹이 되었다는 전제하에 특권 유저의 행위 제한	▪ root 유저 로그인을 기본으로 하여 root 유저가 사용하는 명령어 제한하는 방식
기타 특권 유저 관리	▪ 기타 특권 유저로 login을 불가능 하게하여 일반 유저에 특권 유저 권한을 부여하는 Whitelisting 방식	▪ 기타 특권 유저로 로그인하여 특권 유저의 권한 제어	▪ 기타 특권 유저로 로그인 하여 특권 유저의 명령어 제어
RBAC(Role-Based Access Control)	▪ 가능	▪ 일부 가능	▪ 일부가능
Whitelisting	▪ 가능 (일반유저로 로그인하여 어드민권한이 필요한 신규 인스톨 소프트웨어만 권한 상승)	▪ 불가능 (OS 내의 Installp등 인스톨을 위한 OS 명령어를 통제하므로 특정 소프트웨어만 신규 인스톨 설치 통제 불가능)	▪ 불가능 (OS 내의 Installp등 인스톨을 위한 OS 명령어를 통제하므로 특정 소프트웨어만 신규 인스톨 설치 통제 불가능)
File Integrity Monitoring	▪ 가능	▪ 일부 가능 ▪ 파일의 Hash 값 정도 참조 기능 ▪ 중요 파일의 변경 내역 트래킹	▪ 불가능
랜섬웨어 대응	▪ 가능	▪ 일부 가능	▪ 불가능
Unix/Linux Keystroke	▪ Shell Script 내에도 가능 ▪ Link 및 rename 로깅 가능 ▪ 현재 접속하여 수행중인 사항의 모니터링,Pause,Termination ▪ Keyword Indexing ▪ Stdout keyword search ▪ Xwindow 및 GUI 기반 터미널에서 수행된 명령 로깅 가능 ▪ vi editor등 편집내역 로깅가능 ▪ 모든 작업내역에 대한 로깅 ▪ 콘솔 로깅 가능	▪ 단순 Input & Output 위주 ▪ 동영상 형태의 기록 및 동영상 replay ▪ Xwindow 및 GUI 기반 터미널에서 수행된 명령은 감사 기록 불가능 ▪ Keyword Indexing 기능 없음 ▪ Vi editor등 편집 내역 로깅 못함 ▪ 모든 작업에 대해서 로깅을 하지는 못함 ▪ Link 및 rename 로깅 불가능 ▪ 콘솔 로깅 가능	▪ 단순 Input & Output 위주 ▪ 동영상 형태의 기록 및 동영상 replay ▪ Xwindow 및 GUI 기반 터미널에서 수행된 명령은 감사 기록 불가능 ▪ Keyword Indexing 기능 없음 ▪ Vi editor등 편집 내역 로깅 못함 ▪ 모든 작업에 대해서 로깅을 하지는 못함 ▪ 콘솔 작업 로깅 불가능 ▪ Shell Script 내 로깅 불가능 ▪ Link 및 rename 로깅 불가능

PowerBroker vs 타 솔루션

기능	Powerbroker	SecureOS	접근제어 솔루션
Windows keystroke	▪ - Windows Keystroke 로그를 Keyword Search 가능 ▪ Action이 발생시(keystroke, Mouse Click시)에만 저장 ▪ Application/대상서버/유저별로 로깅	▪ Windows keyword Search 불가 ▪ 기간내 모든 저장 (동영상 방식)	▪ Windows keyword Search 불가 ▪ 기간내 모든 저장 (동영상 방식)
스크립트내의 명령어 로깅	▪ 가능	▪ 가능	▪ 불가능
원격 접속 명령어 실행 통제	▪ 가능 (명령어로 통제)	▪ 일부 가능	▪ 불가능
명령어 실행 2차 인증	▪ 가능	▪ 불가능	▪ 불가능
네트워크통제	▪ 가능 ▪ 유저가 로그인한 후 명령어 통제 (Whitelisting & Blacklisting) ▪ Session Logging (Keystroke Logging) ▪ Active Session 통제 ▪ Audit 중앙화	▪ 불가능	▪ 불가능
Rename,link등 변경된 명령어 실행 허가 금지	▪ 가능	▪ 일부 가능	▪ 불가능
리포팅	▪ 풍부	▪ 일부	▪ 일부
자산 Scanning	▪ 가능	▪ 불가능	▪ 하드웨어 및 소프트웨어 및 기타 자산 스캐닝
패스워드 관리	▪ PBPS라는 모듈 이용 시 고도화된 패스워드 관리 기능	▪ 기본적 단순 기능 부여(전용 패스워드 관리 툴을 따로 사용해야함)	▪ - 다른 툴 사용 하여 가능
Windows keystroke	▪ - Windows Keystroke 로그를 Keyword Search 가능 ▪ Action이 발생시(keystroke, Mouse Click시)에만 저장 ▪ Application/대상서버/유저별로 로깅	▪ Windows keyword Search 불가 ▪ 기간내 모든 저장 (동영상 방식)	▪ Windows keyword Search 불가 ▪ 기간내 모든 저장 (동영상 방식)

PowerBroker(PBW) vs 타 솔루션

기능	Powerbroker	SecureOS
권한상승방식	• 어플리케이션 Token 변경 방식	• Run As 방식
개요	• 동일 유저의 Credential을 이용하여 어플리케이션이 필요한 Security Token을 변경하여 Elevation	• Secondary Logon Service를 이용하여 다른 유저의 Credential과 그룹 멤버십을 이용하여 실행
장단점	• 사용자계정과 실행 계정의 일치 (User Context Switching 일어나지 않음) • 프로파일 불일치 없음	• 사용자 계정과 실행 계정의 불일치 (User Context Switching 일어남) • 어플리케이션이 인스톨 시 유저의 프로파일에 변경을 가하는 어플리케이션일경우, 로그인 유저 프로파일에 변경을 가해야 하는데 권한이 있는 다른 유저의 프로파일에 변경을 가함. 다시 로그인 유저로 돌아와서 어플리케이션을 기동하려고 하면,프로파일 차이로 기동이 안되거나 기동 되더라도 사용 중 문제를 일으키는 경우가 발생 • Registry에 있는 정확한 HKEY-CURRENT-USER Hive를 Access 일치하지 않음 • 네트워크 share는 언제나 current 유저의 context를 기반으로 하기 때문에 네트워크 share에 읽거나 쓰기를 실패 할 수 있음. • Windows update 할 수 없음. SCCM에 의존. • 네트워크 IP 변경 등을 위하여 Network Configuration Operators라는 그룹에 유저를 넣어서 권한 상승을 시킴 • 사용자 계정과 실행 계정의 Printer나 Drive Mapping이 다를 경우 발생. Universal Naming Convention (UNC) paths 사용 할 수 없음. • Credential 이 해킹 될수 있음 (Pass the hash 로 부터 안전하지 않아서 마이크로소프트사가 사용을 제한하는 방법) • Launcher(바로가기아이콘 수정/등록)또는 Toolbar 등록
Whitelisting 방식	• PBW내의 Whitelisting 기능 이용	• 윈도우 기본 기능인 Applocker 이용 • No Central Management Interface • 로그가 로컬에 저장됨 (중앙집중화는 파워셀을 사용해야함) • Admin 유저에서 Application Identity Service Disable 가능 • LOCAL 컴퓨터의 어드민이 Local GPO내의 Applocker Policy 변경가능 • Shell Script 같은 Interpret Code처리 불가 • APPLOCKER 통과하는 많은 방법이 이미 시중에 존재

PowerBroker(PBW) vs 타 솔루션

기능	PBW	타 솔루션	비 고
Agent	단일 Agent (win7/Win10/Win2012/Win2016)	OS에 따른 에이전트의 변화	OS Upgrade시 난이도 발생 가능성
적용 환경	도메인 환경, 워크그룹 환경	도메인 환경	환경이 공존 시 문제 발생 가능성
멀티 OS 지원	Win7,Win10,Win2012,Win2106,Mac OSX, Linux, UNIX	Win7, Win10	PBW는 Win7에서 Win10으로 Upgrade시 Migration Tool 제공
제공 정책	Hash / Publisher / Path MSI / ActiveX / Shell File Integrity (중요 폴더 접근 제한)	Hash/Publisher/Path 방식	타사는 정책 룰이 많지 않아서 룰 작업 시 권한상승이 안되는 경우 발생
Admin 권한상승	SECURITY Token 변경 (개발 된지 20년 이상과 글로벌 5,000개 레퍼런스)	권한상승용 별도 계정 이용 방식 (run-as 방식)	사용자 계정/세션 불일치 사용자 세션 불일치 바로가기 이용
	GUI/CLI/시스템 작업이 동일 방식	명령어 Elevation 기능이 없음	타 솔루션은 시스템 작업 시 어드민 유저 필요
정책 적용 단위	AD OU 또는 자체 그룹 단위 으로 적용하고 OU간의 동일 속성끼리 상세 적용 대상을 지정 가능	AD OU 또는 자체 OU 만들어서 OU단위 지속적인 OU를 만들어야함	정책 적용이 유연함
Whitelisting	가능	Whitelisting 기능 없음	AD 사용시에만 Applocker에 의존
룰 분배	변경분 적용가능	룰 분배시 모든 룰을 재전송	단말수가 많고 룰수가 많으면 분배시 성능문제 발생
멀웨어 및 랜섬웨어 실행 방지	All Deny 규칙을 통해 신뢰되지 않은 프로그램에 대한 실행 차단	미 지원 (Applocker에 의존하나 기능 미미)	
자산정보수집	가능	미 지원	
파일 변경 검출	지원	미 지원	
레퍼런스	전세계 5,000여 개 Reference	국내 일부 (극히 소수)	
관리서버 유저 Interface	모든 Agent OS 버전 동일	OS 버전마다 다름, 자체 소프트웨어 버전마다 다름	
리포팅	풍부 (여러 조합에 따라 많은 리포팅 생성)	Text Based 일부 리포팅	

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

PowerBroker 평가 및 레퍼런스

세계 최대 은행 8/10이 사용하는 PowerBroker

세종정보보안 BizHub

PowerBroker에 대한 평가

- 모든 제품군을 구비한 대표적 벤더("… 'Representative vendor' for all five key feature solution categories")
- PAM 분야의 통합 제품 제공("…Integrated, one-stop approach to PAM…")
- 많은 고객 보유("…Pure-player in the…market; significant position in the market")
- Frost & Sullivan의 "PowerBroker Password Safe" 에 대한 찬사
- PBW - 어드민 유저를 쉽게 제거 솔루션("Leverage a solution like BeyondTrust's PowerBroker for Windows to transparently remove administrator privileges")
- PAM 분야 메이저벤더 : Major Player' in Privileged Access Management"
- 권장할수 있는 벤더("BeyondTrust is a vendor you can rely on… impressive set of flexible and tightly integrated auditing tools")
- 윈도우 뿐만 아닌 유닉스/리눅스/맥 OS에도 적용 가능한 제품

PowerBroker Reference - 국외

세계 최대 은행 8/10이 사용하며, 미국 내 최대 은행 7/10이 사용

Energy

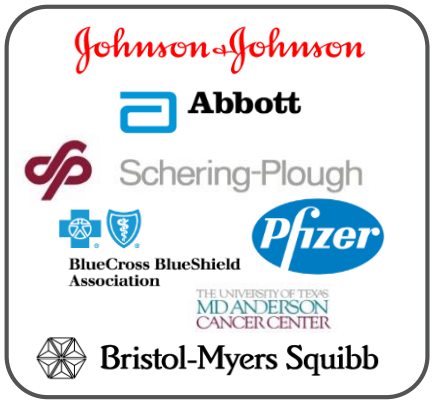
Financial Services

Government

Manufacturing & Technology

Media / Telecom

Health Care & Pharmaceuticals



- 세계 최대 은행 8/10이 사용하며, 미국 내 최대 은행 7/10이 사용 중
- 세계 최대 항공우주산업 및 방위산업 회사 중 7/10이 사용 중
- 미국 내 최대 제약사 7/10이 사용 중
- 다우존스 등록된 회사의 절반 이상이 사용 중

PowerBroker Reference - Media

FOX, NBC, HBO 등 유수의 방송사에서 사용

PowerBroker Reference - 국내

KB국민은행, 삼성생명 등 대형 금융기관에서 사용

감사합니다
Thank you

세종정보보안㈜
강 윤 채 / 부대표
T : 010-2047-5543
E : yckang@sejonginfo.co.kr

BizHuB BeyondTrust