GATEONE

시스템 접근제어 및 보안감사

GATEONE은 서버관리자, DBA, 개발자 등 인가된 시스템 작업자가 서버(윈도우, UNIX, LINUX)나 네트워크 장비에 대한 접근제어 및 보안감사 솔루션입니다 시스템의 접근제어, 명령어 실행 제어, 접속 세션 관리, 실시간 모니터링, 접속 이력 저장, 작업 로그의 저장 및 녹화 기능을 제공합니다.

GATEONE 필요성

COMMON

접근통제
- 사용자의 접속 가능한 시스템 리스트 통제 필요

작업관리
- 사용자의 작업에 대한 사전 검토와 승인체계 필요

세션 통제
- 접속중인 세션에 대한 실시간 모니터링 및 통제 필요

암호화 통신
- 사용자의 원격접속 환경의 안정성 확보를 위해 통신 구간의 암호화 필요 (암호화 통신)

강력한 통계자료
- 중요한 시스템 관리를 위한 작업 명령어 및 접속 기록의 강력한 통제 자료 필요

UNIX,LINUX,NETWORK

휴먼 에러 방지
- 작업자의 명령어 사용 통제하여 휴먼에러로 발생할 수 있는 시스템 장애 요소 제거

작업로그 저장
- 신뢰성 있는 감사를 위해 사용자의 입력과 시스템 응답 데이터를 모두 로그 저장

WINDOWS

원격 터미널 서비스(RDP) 보안감사
- 그래픽 기반 작업 환경을 위한 동영상 로그 저장 필요

웹 브라우저 감사
- 웹 브라우저를 통해 관리되는 네트워크 장비 및 다양한 보안장비의 관리 이력을 동영상 로그로 저장

SPECIAL

Agentless
- PC와 서버 환경에서 세션통제와 로그저장을 위한 Agent 미설치

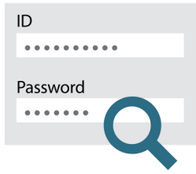
빠른 장애 복구
- 신속하고 정확한 장애 원인 분석 및 복구를 위해 빠른 로그검색과 사용자 작업화면의 재생 필요

GATEONE 기대효과와 주요기능

기대효과

▪ **휴먼에러 방지**	작업관리, 명령어 통제, 실시간 모니터링 등의 기능을 이용하여 사용자의 휴먼에러를 방지
▪ **정보유출 방지**	시스템 접근 권한 및 작업 관리, 세션 통제를 통해 중요 정보에 대한 사용자의 접근을 통제하고 정보유출 사고 시 유출 경로 추적과 증거자료를 제공하여 피해를 최소화하고 재발 방지 효과를 제공
▪ **시스템 안정성 확보**	시스템 장애 및 정보보안 사고의 예방을 통해 시스템 안정성을 확보
▪ **비용절감 효과**	시스템 안정성이 확보되어 가용성이 높아지고 이에 따른 유지 비용이 절감, 또한 시스템 장애로 발생하는 기업의 비용 리스크 제거
▪ **기업 경쟁력 향상**	보안 강화를 통해 내부의 정보 자산을 안전하게 관리하여 기업의 신뢰도와 경쟁력 향상
▪ **ROI 증대**	도입 비용 대비 효과 증대

주요기능



▪ 감사 및 로그
- 사용자의 모든 작업 로그 저장 (실행 명령어, 서버 응답 데이터)
- 윈도우 원격터미널 접속 및 HTTP(S) 접속 동영상 로그 저장
- 접속 이력 조회 및 저장된 작업 로그의 열람 또는 재생

▪ 모바일 OTP앱
- 계정 소유자의 본인 확인 및 인증 강화를 위한 모바일 OTP 인증 기능
- 안드로이드, iOS 지원

▪ 사용자 계정 통제
- 유효기간 설정 및 기간 만료계정 자동 중지
- 로그인 시 사용자 네트워크 접근 제어
- ID / Password + OTP의 Two Factor 사용자 인증
- 장기 미접속 상태의 휴면계정 관리
- Idle 상태의 웹 로그인 UI 잠금 및 로그오프
- 보안성 강화를 위한 패스워드 생성 규칙

▪ 시스템 접근 제어
- 명령어 제어 (금지명령어 및 허용 명령어 통제)
- TELNET, FTP, SSH, SFTP, RDP, VNC,HTTP(S) 프로토콜 제어
- 작업제어를 위한 워크플로우 (신청 및 승인)
- 세션 제어 *(Idle Time-Out, 접속중인 세션 강제 종료, 접속시간 제어)
- 접근제어 (접속 리스트 관리 및 비인가 시스템에 대한 우회접속 금지)
- Rule 기반의 정책 관리

GATEONE 구축사례

▪ **공공기관**	안정적인 대 국민 서비스를 위해 시스템의 안정성 확보가 필요하며 그 방안으로 시스템 작업에 대한 적절한 접근통제의 필요성 대두. 또한, 정부의 정보시스템 접근 권한 관리 규정에서 요구하는 주요 시스템 접근에 대한 사용자 인증 및 권한 관리 기능과 시스템 접속 이력, 작업 내용의 저장 기능 요구
▪ **금융기관**	안전한 전자금융 시스템을 위한 사용자의 시스템접근 통제와 작업통제, 명령어 통제 등 기능 요구
▪ **일반기업**	많은 기업에서 정보유출 및 사용자에 의한 장애를 방지하기 위해 내부 전산 인력과 외부 아웃소싱 개발자, 그리고 유지보수 업체의 기술지원 인력에 대한 작업의 통제 및 감사 기능을 제공하여 장애 예방 및 원인 분석을 통한 빠른 복구기능 요구