에스지에이솔루션즈(주)
SGA Solutions Co., Ltd.

RedCastle

다양한 비즈니스 운영 환경에 최적화된
서버 보안 솔루션

패턴기반의 통제가 아닌 커널 레벨에서
정책 기반으로 통제하는 접근 통제 솔루션

서버의 보안 취약점과 운영체제의
제로데이 취약점 차단 보안 솔루션

On-Premise와 클라우드 환경에서
동일한 서버 보안 기능 제공

APT 공격과 같은 해킹과 내부자의 악의적인 위협,
그리고 Human Error로부터 시스템 및 서비스 보호

The Most Reliable Index, secured by **SGA Solutions**

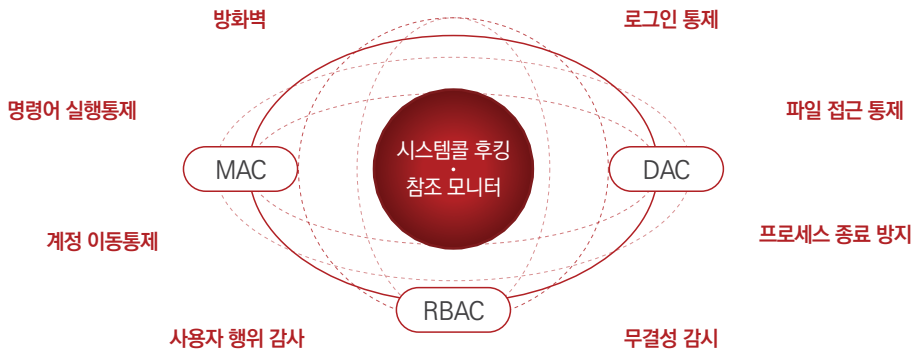
RedCastle v6.0

RedCastle v6.0은

서버보안 솔루션으로 **운영체제의 커널 레벨에서 보안 정책기반으로 사용자의 행위를 통제**하여
전통적인 패턴 기반의 보안 솔루션이 탐지 및 차단하지 못하는 공격행위를 효과적으로 탐지하고 차단하는
가장 완벽한 서버보안 솔루션입니다.

01 RedCastle의 주요기능

- **운영체제의 커널**에서 사용자의 행위를 기반으로 하는 시스템 콜(System-Call)을 Hooking하여 설정된 보안 정책과 비교한 후 접근을 통제하는 참조모니터(Reference Monitor)를 통해 **우회 접근을 사전에 차단**합니다.
- 강제적 접근제어(MAC), 임의적 접근제어(DAC)와 역할기반 접근제어(RBAC) 보안모델을 보안기능으로 구현하여 **중단없는 안정적인 서비스를 지원**하고 중요 정보를 안전하게 보호하며 **시스템에 대한 침입 차단 및 통합 보안관리를 지원**합니다.
- 전통적인 패턴기반 통제로 보안 솔루션들이 탐지 및 대응하지 못하는 보안위협들과 내부자의 실수(Human Error) 또는 악의적인 내부자를 **보안정책 기반으로 탐지하고 대응하여 시스템 보안의 마지막 보루 역할을 수행**합니다.



방화벽

- OSI 7Layer의 Layer 3(Network Layer)에서 동작하는 패킷 필터링 방식의 Light-Weight 방화벽을 통해 성능 및 안정성 보장

로그인 통제

- 시스템에 접근하는 사용자를 '접근 IP/Mac Address' - '계정' - '로그인 서비스' - '접근 시간/기간'의 조합을 통하여 통제
- AuthCastle을 연동하여 2차 인증(FIDO, OTP, ARS, PKI 등)을 통한 실사용자 기반으로 시스템에 접근하는 사용자를 통제하여 보안 강화

파일 접근 통제

- 강제적 접근제어(MAC) 기반으로 행위 주체의 보안 속성과 대상의 보안 속성을 비교하여 접근 통제
- 임의적 접근제어(DAC) 기반으로 파일ACL 기능을 통하여 대상 파일의 접근하는 주체의 권한(읽기, 쓰기, 실행 등)을 설정하여 접근 통제
- AuthCastle을 연동하여 실사용자 기반으로 파일에 대한 접근 통제

명령어 실행통제

- 사용자가 시스템에 접속하여 실행 가능한 CLI 명령어를 통제
- 운영체제의 커널에서 시스템 콜을 후킹하여 통제하기 때문에 심볼릭 링크나 스크립트 내 명령어 실행 등의 우회 명령어 실행 원천 차단

프로세스 종료 방지

- 특정 프로세스의 인가되지 않은 종료 차단
- 운영체제의 커널에서 동작중인 프로세스에 전달되는 인가되지 않은 '종료 시그널'을 차단하는 기능 제공

사용자 행위 감사

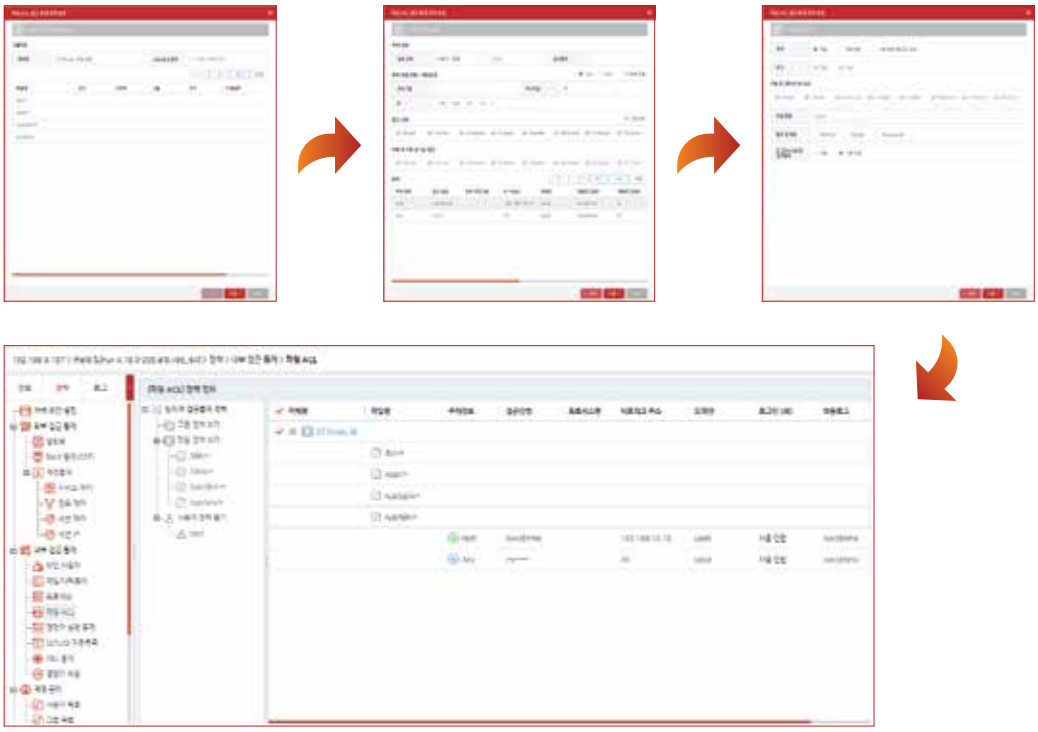
- 시스템에 접근한 사용자의 로그인부터 로그아웃까지의 모든 행위를 감사
- TTY 모니터링은 vi와 같은 편집기, sqlplus와 같은 대화형 어플리케이션에서의 입·출력을 모두 모니터링하여 동영상으로 재현
- 사용자 추적 기능은 커널에서 스크립트 혹은 화면 입·출력 없이 실행되는 명령어도 모두 로깅하여 우회 및 감사의 무력화 행위 차단

02

RedCastle의 특장점

정책 마법사와 와일드 카드(*)

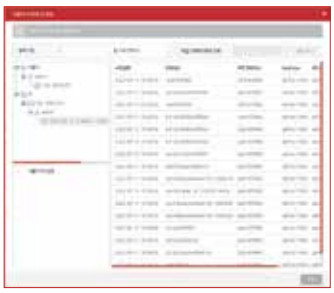
- 파일 접근통제에 사용되는 파일ACL 기능에서 정책 마법사 기능을 제공하여 '대상 설정' → '주체 설정' → '권한 설정' 차례로 지정하여 하나의 보안 정책을 손쉽게 설정 가능
- 대상 설정 시에 와일드 카드(*) 기능을 제공하여 다수의 파일에 일관된 보안정책을 설정할 수 있고, 새롭게 추가되는 신규 파일이라도 설정된 보안정책이 자동으로 적용되어 보안의 지속성 제공



〈RedCastle 파일ACL 설정 화면〉

커널에서 감사 로깅하는 사용자 행위 추적과 TTY 모니터링

- 커널에서 실제로 사용되는 명령어를 추적하여 스크립트 혹은 화면 입·출력 없이 실행되는 명령어도 모두 로깅
- 사용자의 작업 내용을 동영상으로 재현하여 감사 추적에서의 직관성 극대화



〈사용자 행위 추적 화면〉

〈TTY 모니터링 화면〉

IPv6 지원

- IPv4 프로토콜 주소의 한계에 따른 IPv6 프로토콜 완벽 지원
- 외부 접근 통제(방화벽, 로그인 통제 등)와 내부 접근 통제(파일 ACL, 명령어 실행 통제 등)에서 IPv6기반으로 보안 정책 설정이 가능하며, 이에 따른 감사 로그 지원

〈RedCastle Manager의 IPv4/IPv6 지원 화면〉

클라우드 및 가상화 환경 지원

- AWS, Azure, 네이버 클라우드 등 Public Cloud 및 다양한 가상화 기반의 운영체제 지원
- 클라우드의 가용성을 지원하는 Auto Scaling 환경 완벽 지원

구분		S/W	Host OS	Guest OS
Private Cloud	Host 가상화	· VMware Server · MS Virtual Server · Oracle(SUN) VirtualBox	●	●
	Native / Bare-Matal or Hypervisor	· VMware vSphere, Linux KVM · MS Hyper-V, Citrix Xen Sever · Oracle(SUN) xVM Server	×	●
	HCI (Hyper Converged Infrastructure)	Nutanix	●	
Public Cloud	Amazon	AWS(EC2)	●	
	Microsoft	Azure	●	
	Google	Google Cloud	●	
	Oracle	Oracle Cloud(OCI)	●	

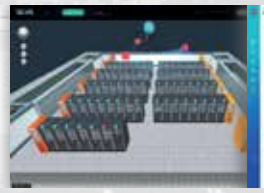
* 공공기관의 경우 지원 환경 관련하여 별도 협의

확장성을 통한 보안성 극대화

- 2차 인증(FIDO, OTP, ARS, PKI 등)을 지원하는 **AuthCastle**을 통하여 실사용자 기반으로 통제 정책 설정이 가능하며, 실사용자 기반 감사 추적 가능
- 3-tier 구성을 통하여 대단위 시스템 환경을 지원하는 **EnterpriseCastle**을 연동하여 대단위 시스템의 보안 관리 지원
- 보안 이벤트와 시스템 로그를 텍스트 기반이 아닌 3D로 구현하는 시각화 솔루션 **VisualCastle**을 통하여 보안의 직관성 극대화
- 하이브리드 클라우드 환경에서의 기본 보안 솔루션인 CWPP(Cloud Workload Protection Platform)제품 **vAegis**와 동시 운용 지원
- **보안성 강화 및 보안 사각지대 해소**


〈AuthCastle 화면〉


〈EnterpriseCastle 화면〉


〈VisualCastle 화면〉


〈vAegis 화면〉

03 도입효과

정부기관 및 공공기관 서버 보안 강화

- 내부자 및 외주 업체 엔지니어의 행위 감시 및 작업 내역 기록
- 백도어 및 공격 도구의 생성/실행 감시 및 차단
- 서버에 대한 IP, 계정, 시간에 의한 접속 제어
- 보안 정책 위반 명령어에 대한 실행 통제

금융기관 계정 및 인터넷 뱅킹 서버 보안 강화

- 주요 서버의 내부통제 및 감사 기능 강화
- 패스워드 유출 없이 특정 권한 위임 수행
- 인터넷 뱅킹 서버의 웹 해킹 차단
- 금융 계좌 정보 유출 차단 (FTP, SSH, DB 접근 통제)
- 배치 작업 솔루션 통제 (APT 공격방어)

클라우드 시스템의 보안 강화

- On-Premise 환경의 서버보안 기능을 클라우드 환경에서도 동일하게 구현
- Auto Scaling에 완벽하게 대응하여 클라우드 환경에서 동일한 보안 환경을 실시간으로 구축/운영
- 데이터 유출, 내부자 위협, 제로데이 취약점 등의 클라우드 보안 취약점 대응

SGA Solutions Co., Ltd.
에스지에이솔루션즈(주)

주소 : 16108 경기도 의왕시 광진말로 54 의왕스마트시티 B동 5층
제품구입문의 : sales@sgacorp.kr **URL :** www.sgasol.kr

KOSDAQ 코스닥상장법인 | GOOD Software | 특허청