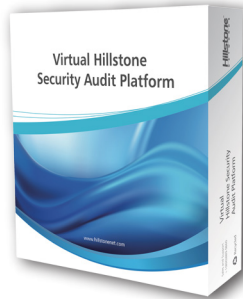


Hillstone 보안 감사 플랫폼



ISP와 대학, 대기업, 정부 기관, 대규모 데이터 센터는 매일 수백만 건의 이벤트를 생성합니다. 이처럼 오늘날의 차세대 방화벽이 생성하는 엄청난 양의 데이터를 분석하기 위해서는 고성능 로그 스토리지와 실시간 수준의 쿼리 응답이 필요합니다. Hillstone의 보안 감사 플랫폼(HSA)은 엄청나게 빠른 검색으로 순식간에 로그 데이터를 보안 인텔리전스로 전환합니다. 따라서 수십억 개의 로그 레코드와 관련 정보에 대한 즉각적인 가시성을 확보할 수 있습니다. Hillstone의 보안 감사 플랫폼은 NAT, 보안 위협, URL 및 세션 로그를 수집 및 집계하고, 세분화된 검색 기능을 통해 네트워크 트래픽에 대한 실시간 가시성을 제공합니다.

제품 주요 정보

네트워크 가시성

로그 레코드는 네트워크 동작에 대한 가시성을 제공하며 규제 준수를 이행하는 데 도움이 됩니다. 그러나 기존 로그 관리 시스템의 경우 수백만 개의 로그 데이터를 대상으로 로그 쿼리를 실행하는 데 많은 시간이 소요된다는 단점이 있습니다. 효과적인 로그 관리 없이는 기업이 자사의 환경에서 제공하는 인텔리전스를 활용하지 못하여 보안 이벤트에 무방비 상태로 노출될 수 밖에 없습니다. Hillstone의 보안 감사 플랫폼은 사용하기 쉽고 강력한 쿼리 기능을 제공하기 때문에 수많은 로그 레코드와 관련 정보에 대한 즉각적인 가시성을 확보할 수 있습니다.

고성능 로그 처리

대기업은 하루에도 100기가바이트 이상의 로그 데이터를 생성할 수 있으며, 이러한 데이터 증가 속도에 발맞출 수 있는 확장성을 갖추는 것이 로그 보관의 중요한 요구 사항입니다. Hillstone의 보안 감사 플랫폼은 표준 syslog는 물론, NAT 트래픽에서 초당 최대 100,000개의 이벤트를 수신할 수 있는 매우 우수한 성능의 바이너리 프로토콜을 지원합니다. 분산 로

드 밸런싱 기능을 활용하거나 특정 서버로 특정 로그를 전송하는 방법으로 동적으로 스토리지를 확장하여 보관/규제 준수 요구사항을 충족할 수 있습니다.

강력한 쿼리

Hillstone의 보안 감사 플랫폼을 사용하면 간편하게 쿼리를 생성 및 저장하여 필요할 때마다 또는 예약된 일정에 따라 실행할 수 있으며, 출발지 IP, 목적지 IP, URL, 공용 IP 및 시간에 대해 검색을 수행할 수 있습니다. 또한 Hillstone의 NAT 로그는 공용 IP 주소를 전용 IP 주소/포트 및 사용자 이름으로 변환할 수 있습니다. 이 기능은 NAT를 사용하며 전용 네트워크에 대한 가시성이 필요한 환경에 강력한 포렌식 세부 정보를 제공합니다.

IPv6 지원

Hillstone의 보안 감사 플랫폼은 IPv4와 IPv6 형식으로 세션 로그, NAT 로그, PBR 로그를 지원하여, IPv4에서 IPv6로의 원활한 전환을 점진적으로 지원합니다.

핵심 기능

장치 모니터링

- 장치 KPI 모니터링
- 로그 스토리지 유형의 비율 분석
- 장치 및 로그 유형의 추세 분석
- 전송 장치 모니터링
- 사용자 정의 모니터링
- 하드 디스크 상태 및 RAID 상태 모니터링

로그 관리

- NAT, 세션, URL, 메일, 온라인/오프라인 IM 및 보안 위협 방지 로그
- IPv6 NAT, 세션, PBR 로그 지원
- 윈도우 로그나 타사 장비의 Syslog를 가져와 분석 가능
- 여러 조건의 복합 검색
- 로그 애그리게이션
- SSL을 통한 로그 전송 지원
- 검색 조건 저장

- 백그라운드 검색 작업
- 여러 장치에 대한 분산 쿼리
- 확장 가능한 로그 스토리지용 NFS 서버

보고서 관리

- 여러 보고서 템플릿 내장
- 사용자 정의 가능한 보고서
- HTML, PDF 및 WORD 형식의 보고서 파일

시스템 관리

- 신뢰할 수 있는 호스트 설정
- 로그 가져오기/내보내기
- 로그 전달
- 분산 검색 설정
- 할 기반 관리: 관리자, 운영자 및 감사자
- 일광 절약 시간대 설정

제품 사양

	HSA-10P	HSA-10	HSA-4D
Performance	NAT: 100,000 EPS Syslog: 15,000 EPS	NAT: 100,000 EPS Syslog: 15,000 EPS	NAT: 50,000 EPS Syslog: 7,000 EPS
Storage	NAT log: 180 days for 10G link	NAT Log: 180 days for 5G link	NAT Log: 180 days for 2G link
HDD	16 TB	8 TB	4 TB
Fixed I/O Ports	2xGE	2xGE	2xGE
RAID Levels	RAID 5	RAID 5	RAID 0
Power Supply	Single/Dual	Single/Dual	Single
Form Factor	2U	2U	1U

vHSA-2

vCPU	Minimum 4 Core
Memory	Minimum 4G
Recommend Disk	2T (Min. disk requirement 200G)
Log Storage	NAT log: 180 Days for 2G link
Performance	NAT: 100,000 EPS, Syslog: 15,000 EPS
Hypervisor Support	VMware EXSi 5.1/5.5/6.0, VMware Workstation 12 or later version, KVM