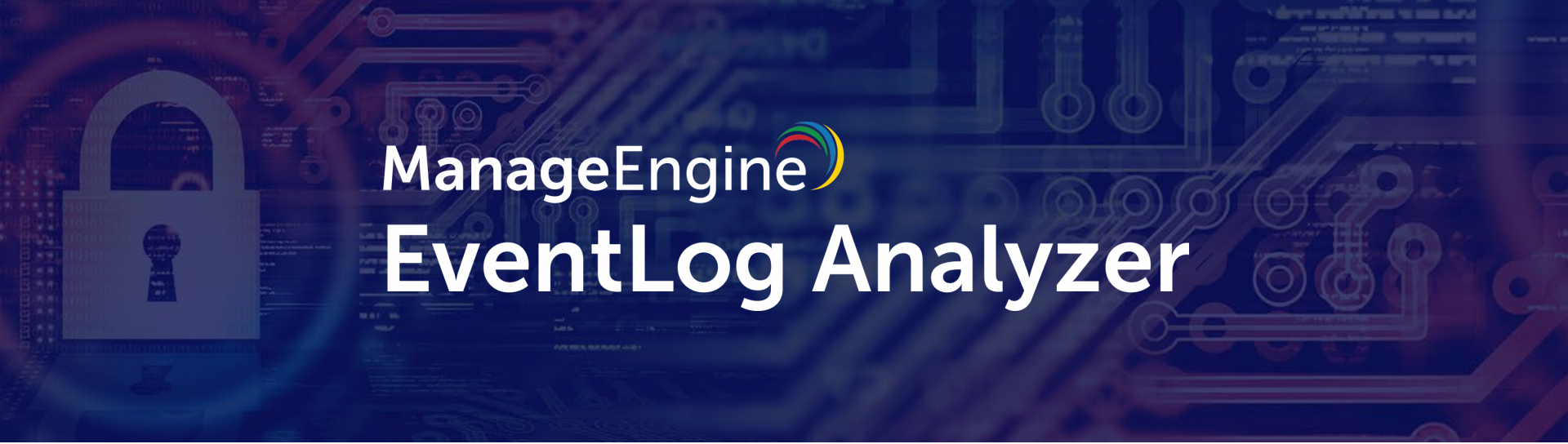
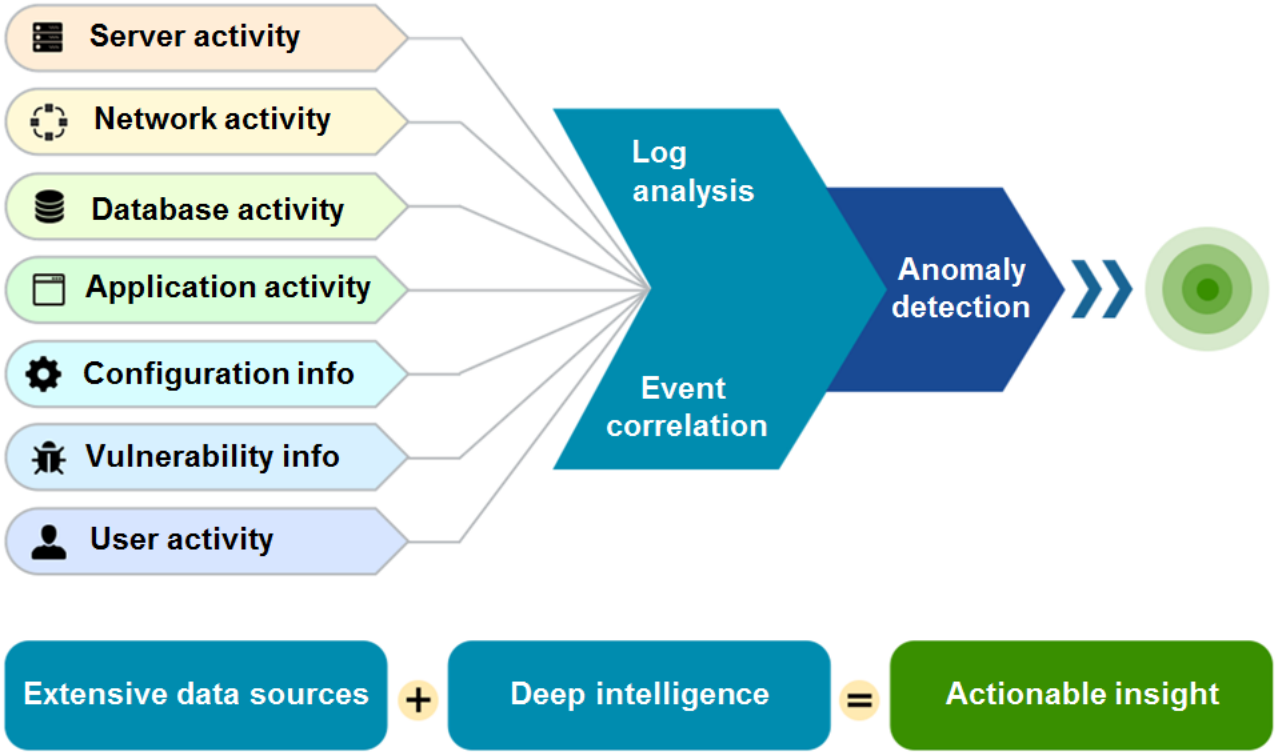


종합
로그 관리 솔루션

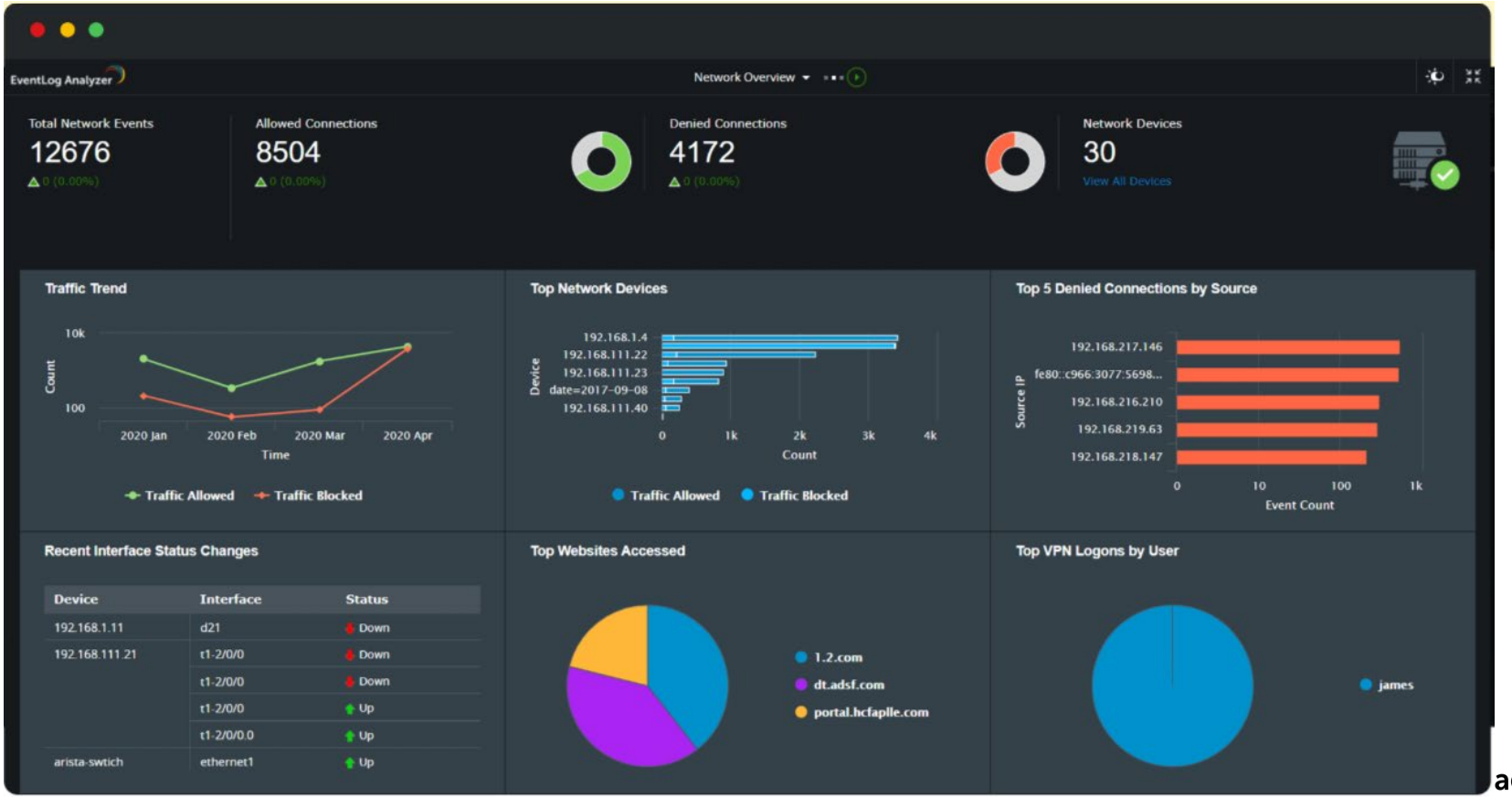
www.eventloganalyzer.com

EventLog Analyzer의 기능



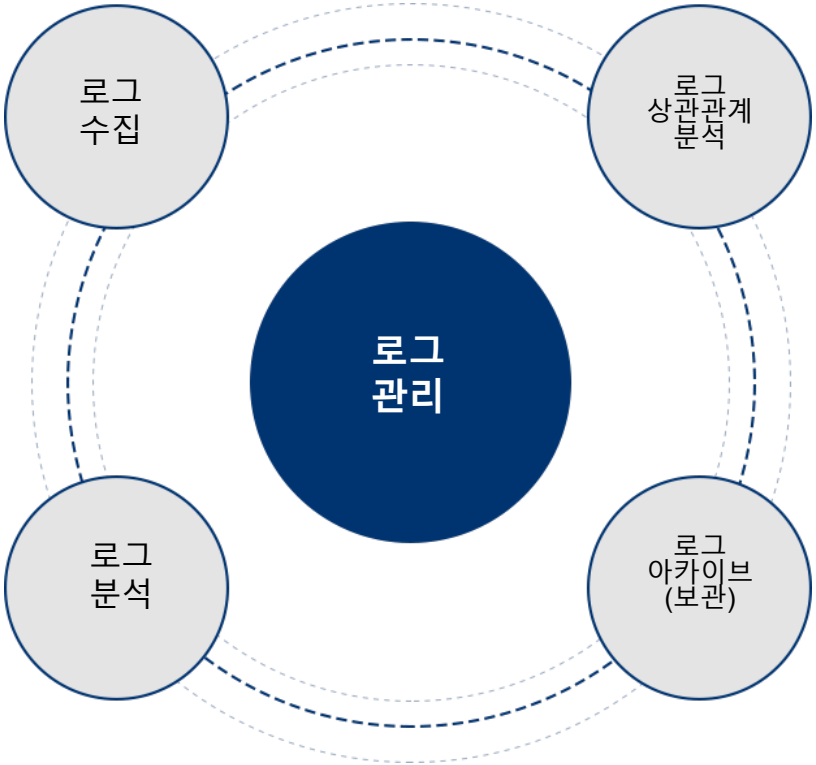
Dashboard (1)

Dashboard (2)



목 차

로그 관리



로그 수집

- 에이전트 기반 및 에이전트 없는 로그 수집 방법을 모두 지원.
- 600개 이상의 로그 소스를 지원.
  - 네트워크 장치: 라우터, 스위치, IDS/IPS 및 방화벽
  - Windows 및 Linux/Unix 서버, IBM AS400
  - Oracle 및 Microsoft SQL Server
  - Apache 및 IIS 서버
  - 취약점 스캐너, 위협 인텔리전스 솔루션 등
- 사용자 지정 장치, 사내 응용 프로그램 등이 발생하는 사람이 읽을 수 있는 모든 로그 형식을 구문 분석 가능.

지원되는 Log Source (1)

Database Platforms

- Microsoft SQL Servers
- Oracle On-premises Databases

Web Servers

- Apache HTTP Server
- Microsoft IIS

Routers and Switches

- Cisco
- Hewlett-Packard

Hypervisors

- Microsoft Hyper-V
- VMware

Vulnerability Scanners

- Nessus
- Nmap
- Nexpose
- OpenVAS
- Qualys

Linux and Unix Systems

- Linux
- IBM AIX
- HP UX
- Solaris

지원되는 Log Source (2)

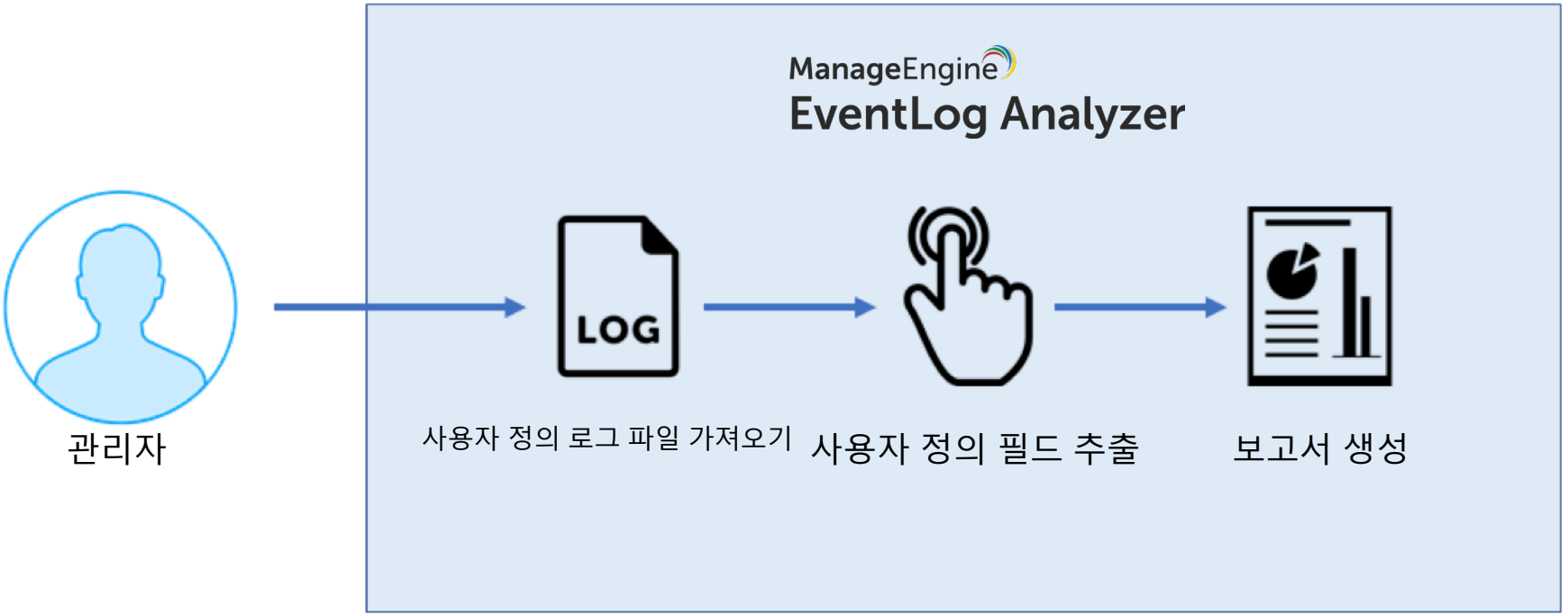
Firewalls, NGFWs, IDS, and IPS

- Barracuda
- Check Point
- Cisco
- Cisco Meraki
- Cyberoam
- Fortinet
- Huawei
- Juniper
- Juniper NetScreen
- Palo Alto
- pfSense
- SonicWall
- Sophos
- Watchguard
- F5 firewall

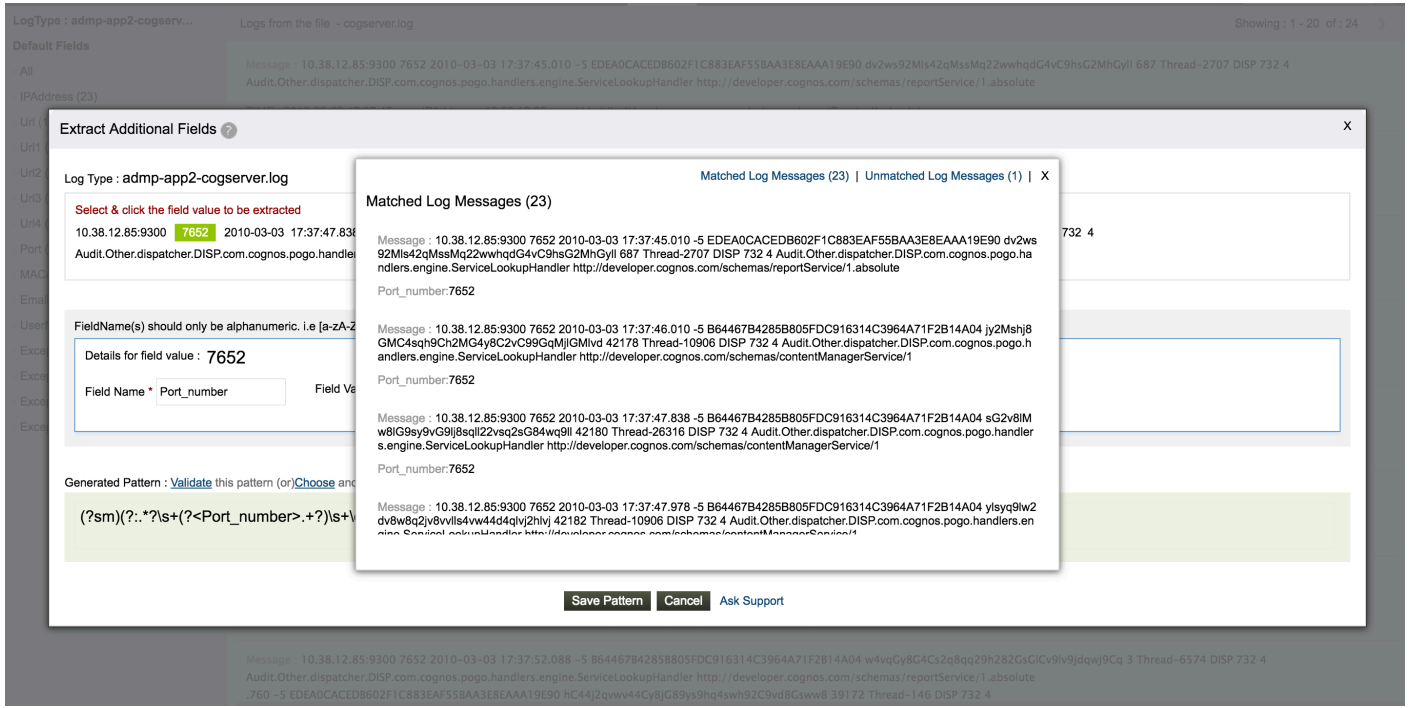
Endpoint Security Solutions

- ESET Antivirus
- Kaspersky Antivirus
- Microsoft Antimalware
- Norton Antivirus
- Sophos Antivirus
- FireEye
- Malwarebytes
- McAfee
- Symantec Endpoint Protection

로그 수집: 사용자 정의 로그 구문 분석



로그 수집: 사용자 정의 로그 구문 분석

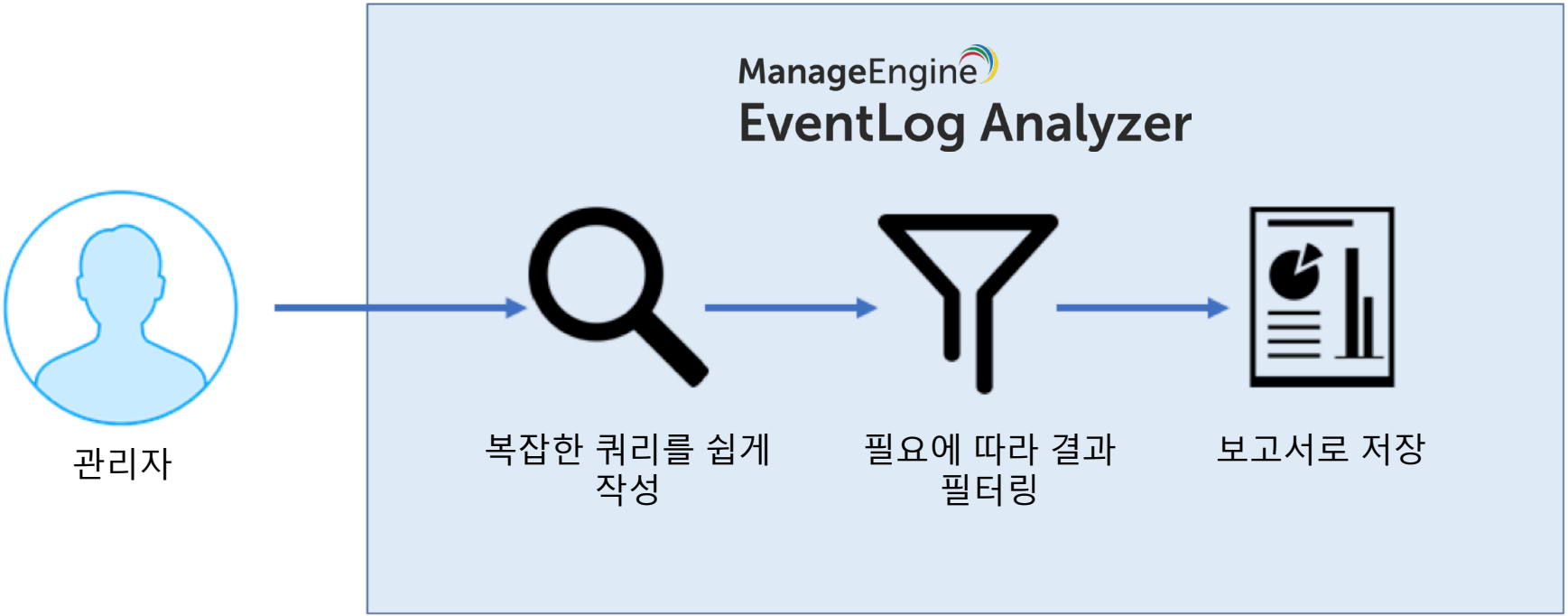


ManageEngine

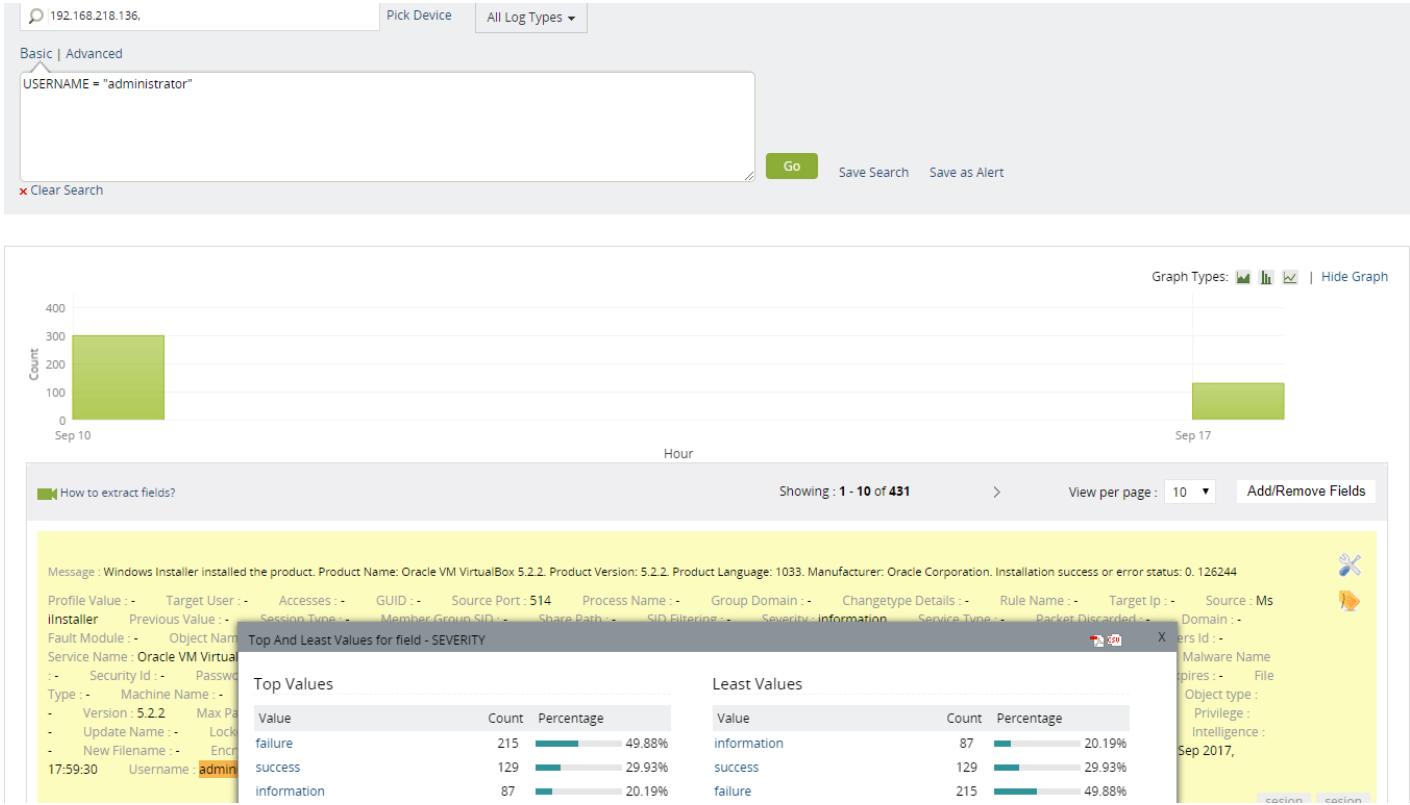
로그 분석

- 보안, 감사 및 규정 준수 요구 사항을 충족하는 1000개 이상의 즉시 사용 가능한 보고서 및 경고 프로필 제공
- 특정 요구 사항을 충족하는 사용자 지정 보고서 및 경고 프로필 제작 도구 제공.
- 빠르고 사용하기 쉬운 검색 엔진으로 심층 로그 포렌식을 수행하고 수백만 개의 로그를 검색.
  - **20,000 syslog / 초**
  - 2,000 Windows 이벤트 로그 / 초

로그 분석: 로그 포렌식


ManageEngine
EventLog Analyzer
관리자
복잡한 쿼리를 쉽게 작성
필요에 따라 결과 필터링
보고서로 저장

로그 분석: 로그 포렌식

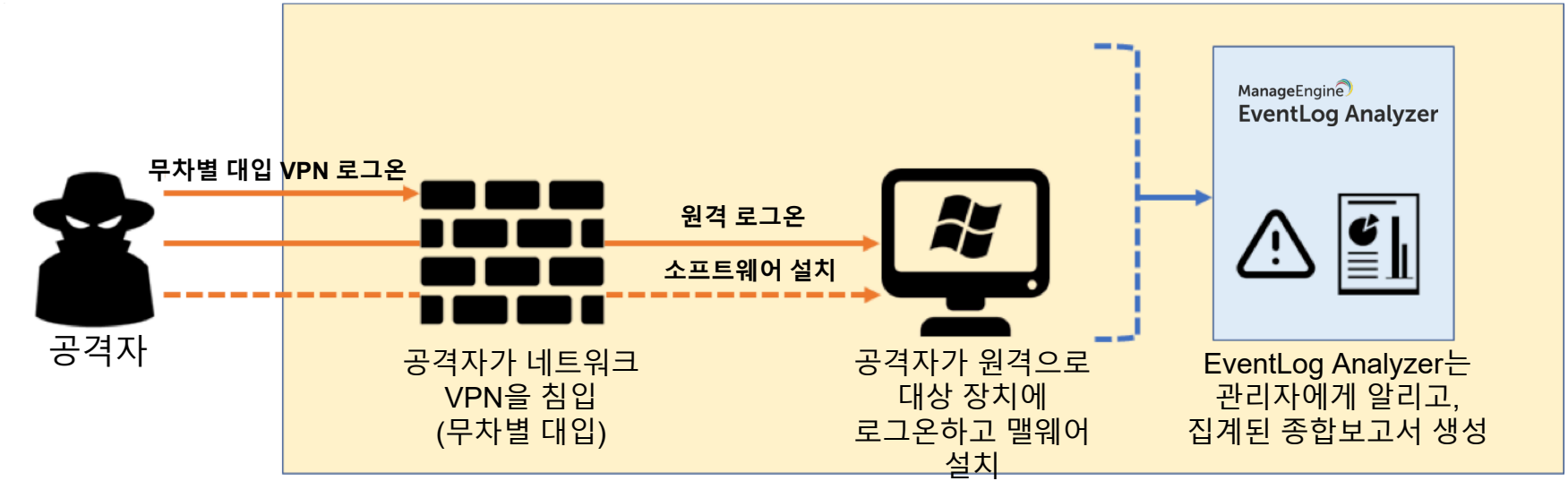


ManageEngine

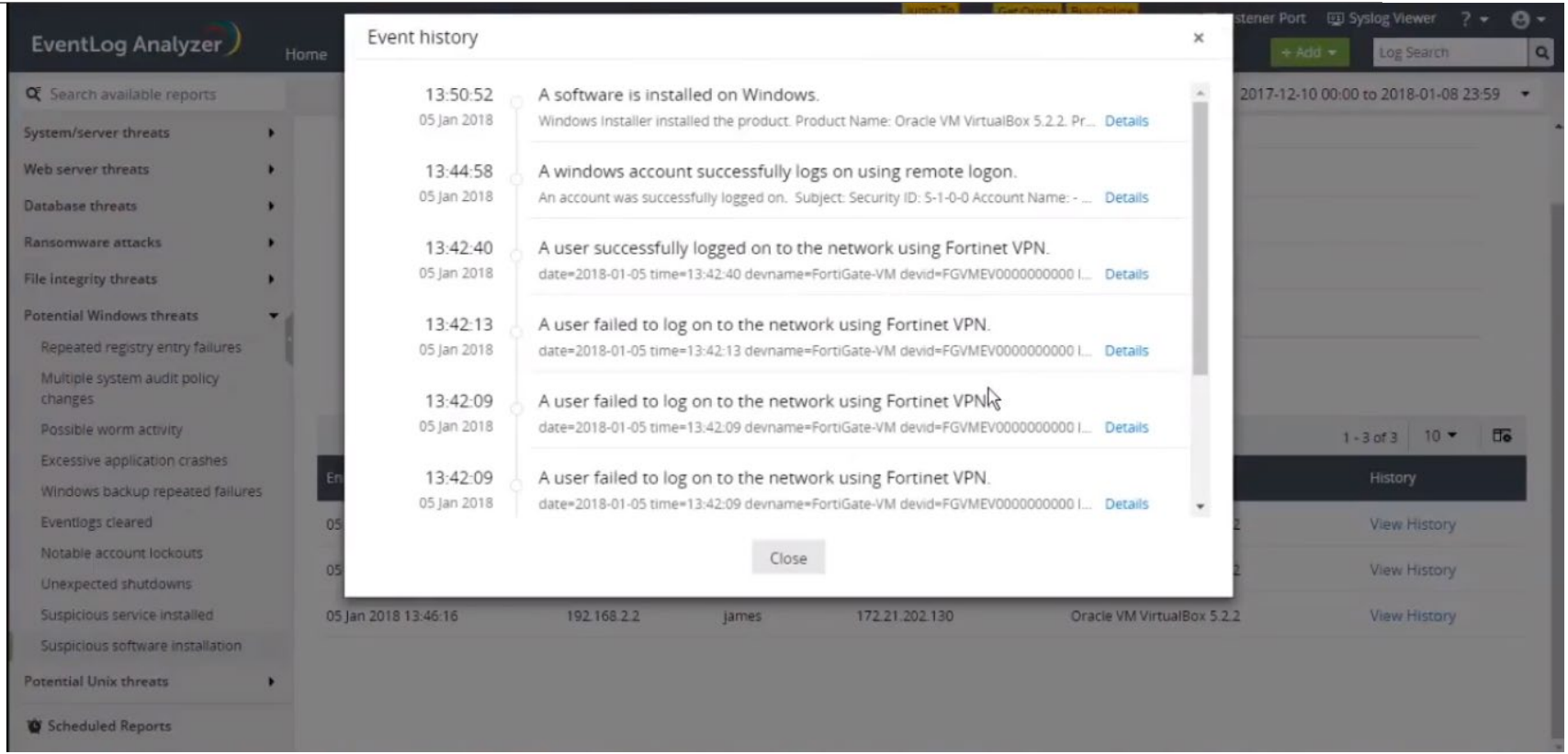
로그 상관 관계 분석

- 30개 이상의 사전 정의된 상관 관계 규칙을 통해 장치 전반의 공격 패턴을 탐지.
- 의심스러운 소프트웨어 설치, 웜 활동과 같은 공격 등의 이상 징후를 탐지.
- 타임라인 형식으로 로그 추적을 표시하는 집계 보고서 제공.
- 비즈니스 환경에 특정한 공격 패턴을 생성하고 탐지하는 맞춤형 상관 관계 규칙 제작 도구 지원

로그 상관 관계 분석: 예


무차별 대입 VPN 로그온
원격 로그온
소프트웨어 설치
ManageEngine
EventLog Analyzer
공격자
공격자가 네트워크 VPN을 침입 (무차별 대입)
공격자가 원격으로 대상 장치에 로그온하고 맬웨어 설치
EventLog Analyzer는 관리자에게 알리고, 집계된 종합보고서 생성

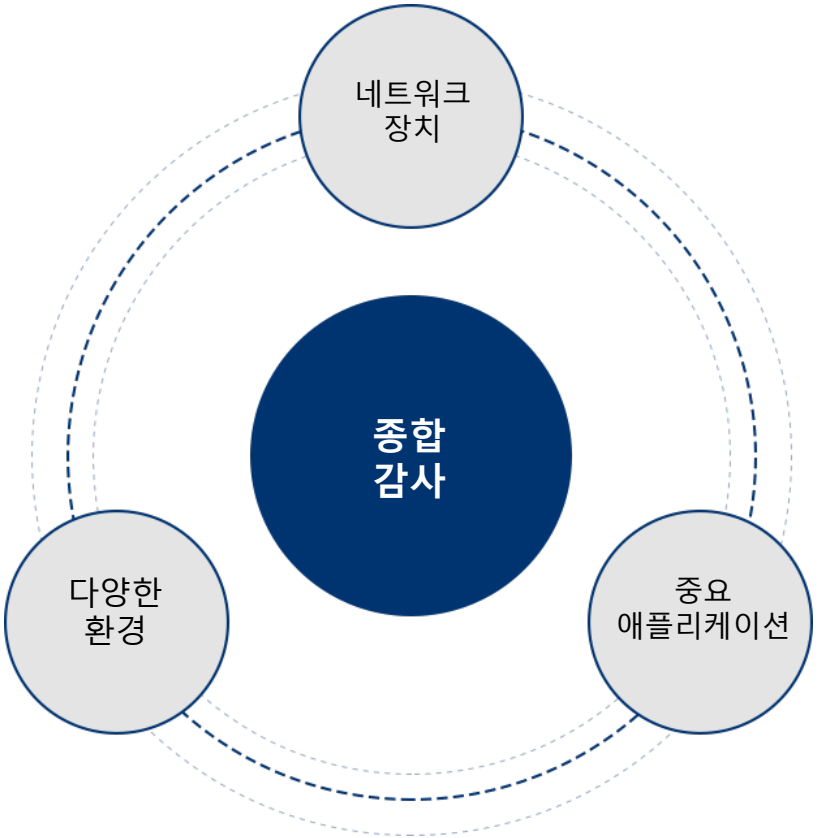
로그 상관 관계 분석: 상관 이벤트



로그 장기 보관

- 로그 파일은 향후 포렌식 분석, 규정 준수 및 내부 감사를 위해 로그 데이터가 보호되도록 암호화 지원
- 기본적으로 수신된 모든 원시 로그가 포함된 로그 아카이브 파일은 24시간마다 생성됨. 그런 다음 이러한 파일은 하드 디스크 공간을 절약하기 위해 7일마다 압축됨.
- 언제든지, 원하는 파일을 EventLog Analyzer 데이터베이스에 로드할 수 있으며, 보관된 이벤트 데이터에 대한 보고서를 생성 가능

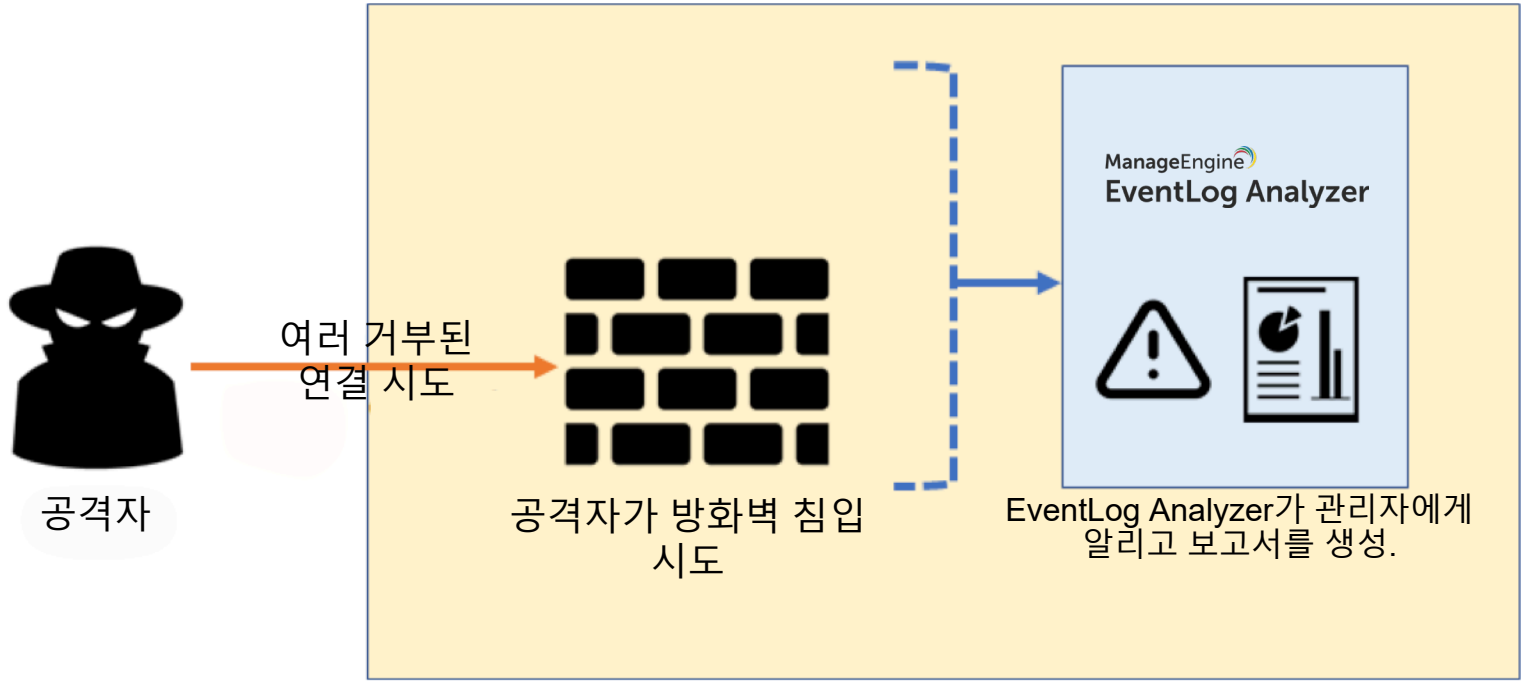
종합 감사



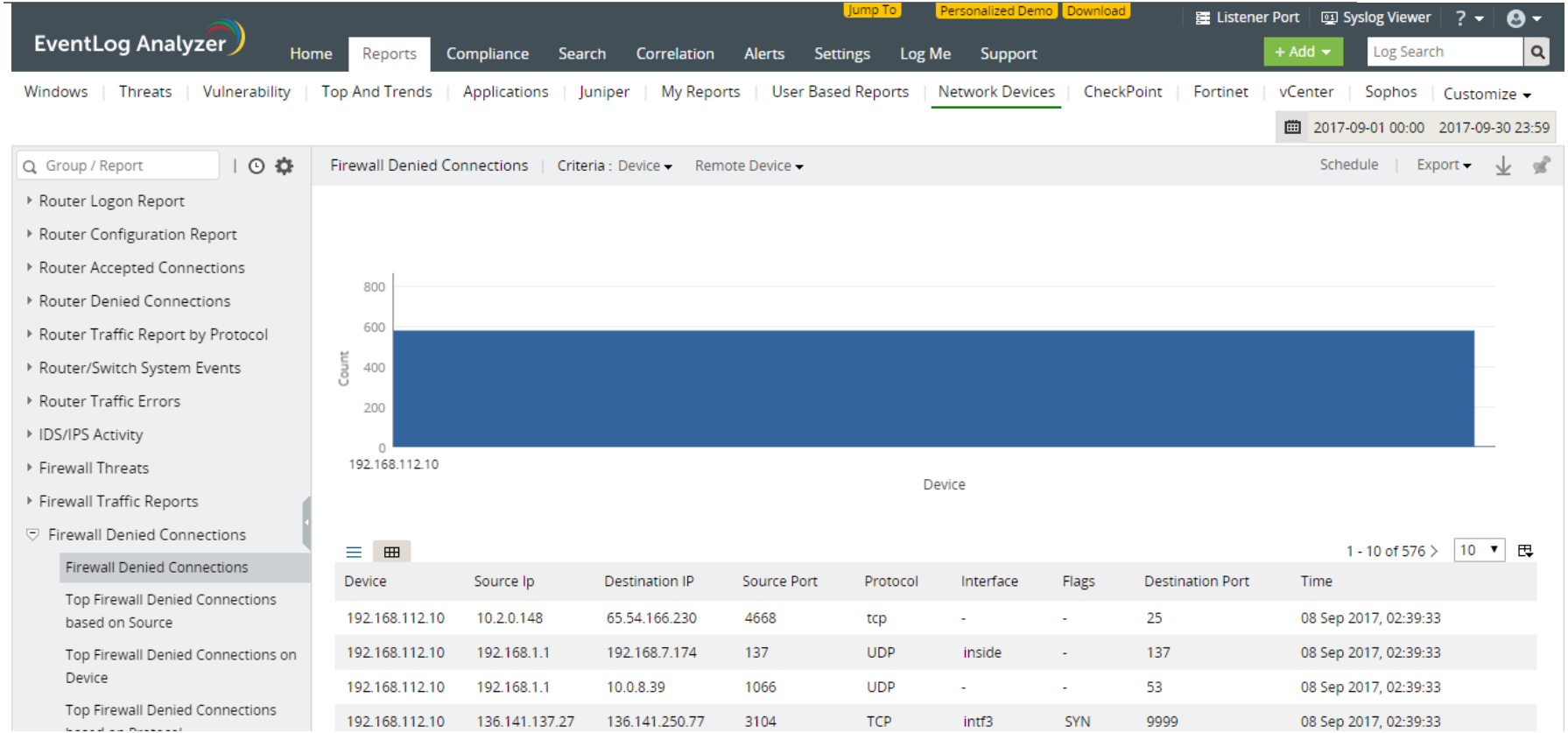
네트워크 장치 감사

- 방화벽 구성 및 규칙 변경을 모니터링.
- 경계 장치에 대한 무단 액세스 시도 및 권한 상승을 식별.
- 라우터, 스위치, 방화벽 및 IDS/IPS 장치에서 거부된 연결, 위협 및 기타 비정상적인 사건을 감지.

네트워크 장치 감사: 방화벽 침해 시도



네트워크 장치 감사: 방화벽 침해 시도

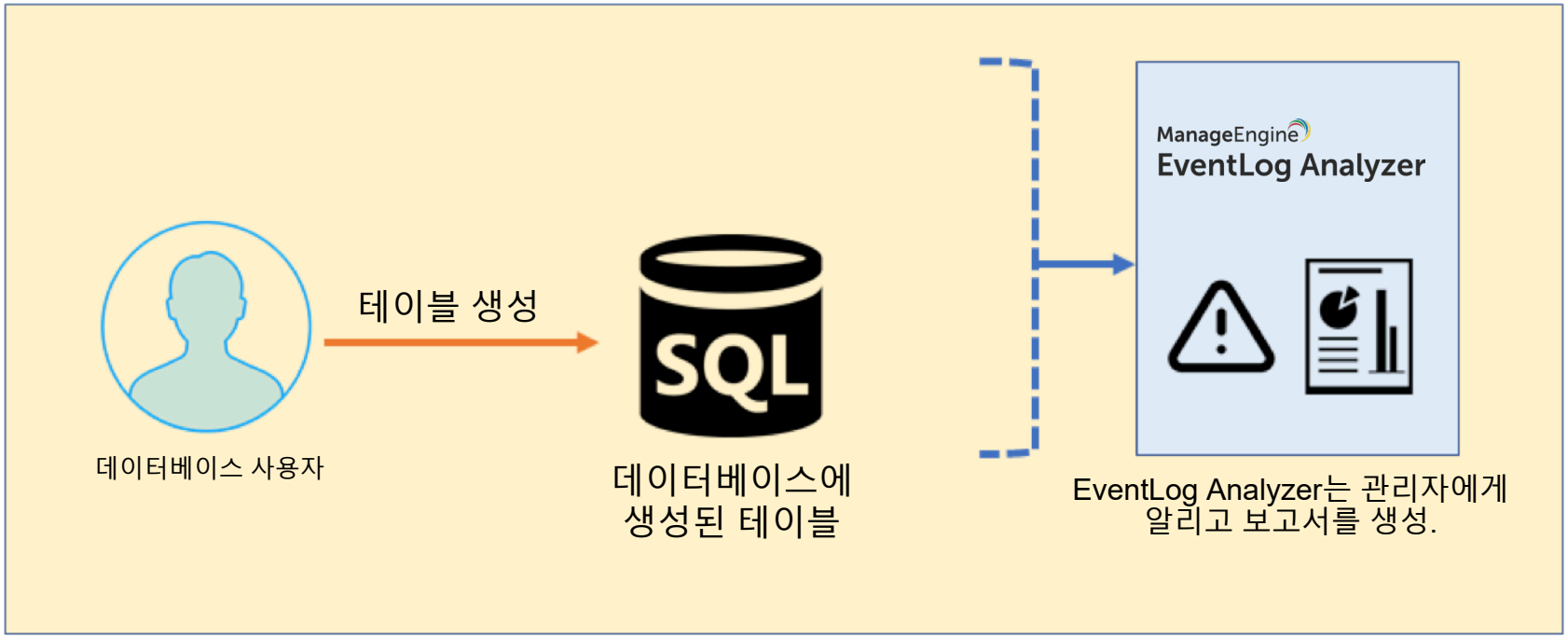


ManageEngine

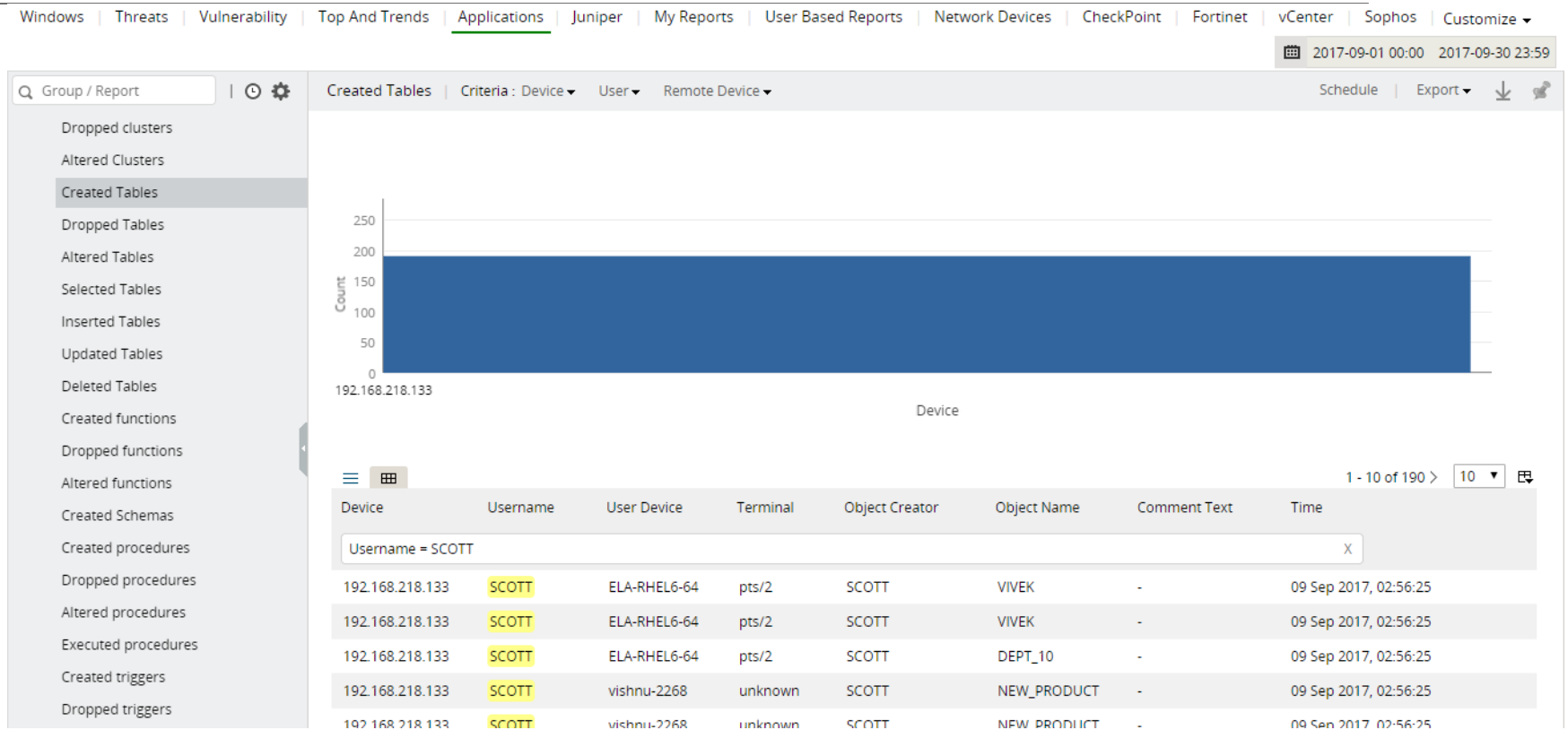
애플리케이션 감사

- 애플리케이션 로그 데이터 가져오기 자동화: 가져온 로그에서 보안 보고서를 추출하고, 사용자 지정 로그 파서를 사용하여 사내의 애플리케이션 로그를 분석.
- IIS 및 Apache 웹 서버 보안: 오류 이벤트, 로그온 시도 실패, 서버 공격과 같은 비정상적인 활동을 실시간으로 식별.
- Microsoft SQL Server 및 Oracle 데이터베이스 감사: 사용자 작업, DML 및 DDL 쿼리, 데이터베이스 변경 사항, 서버 계정 변경 사항을 추적.
- 취약점 스캐너 및 위협 인텔리전스 솔루션 감사: 가장 취약한 포트, 호스트, 감염, 데이터 도난, 잠재적 보안 위험 등에 대한 자세한 자료 제공.

애플리케이션 감사: 특정 사용자가 생성한 테이블

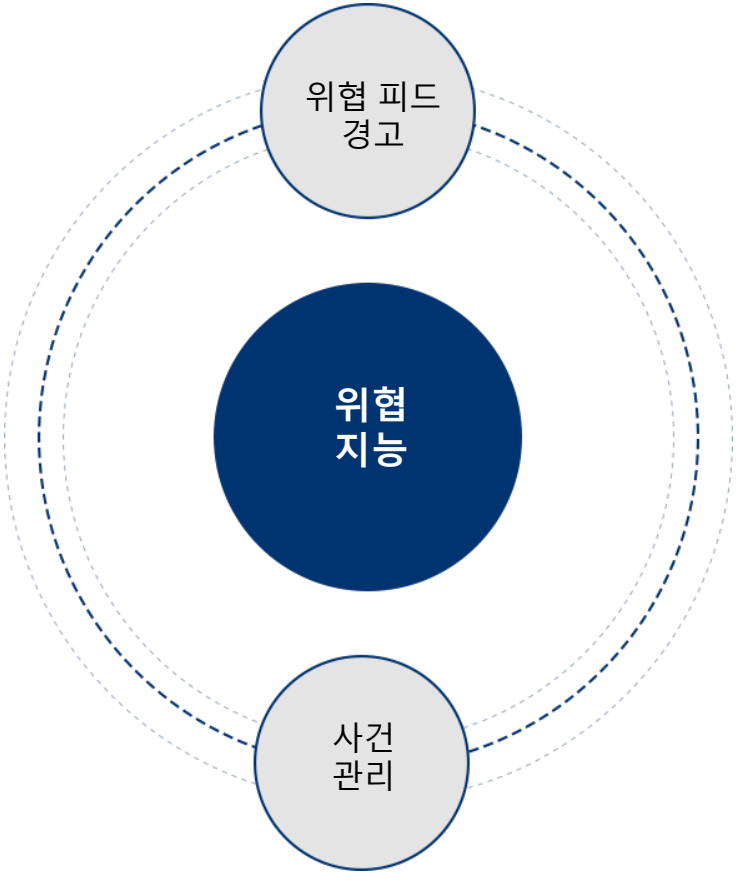


애플리케이션 감사: 특정 사용자가 생성한 테이블



ManageEngine

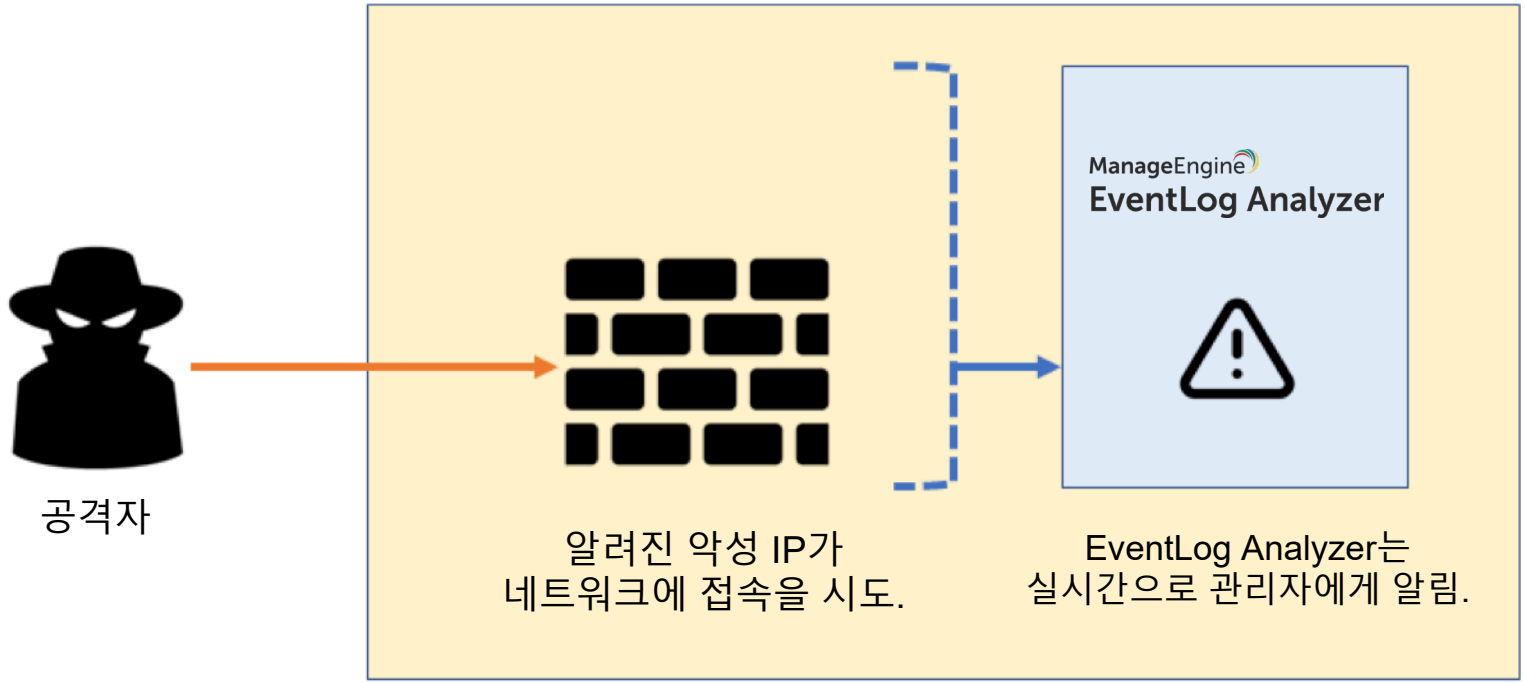
위협 인텔리전스 (Threat intelligence)



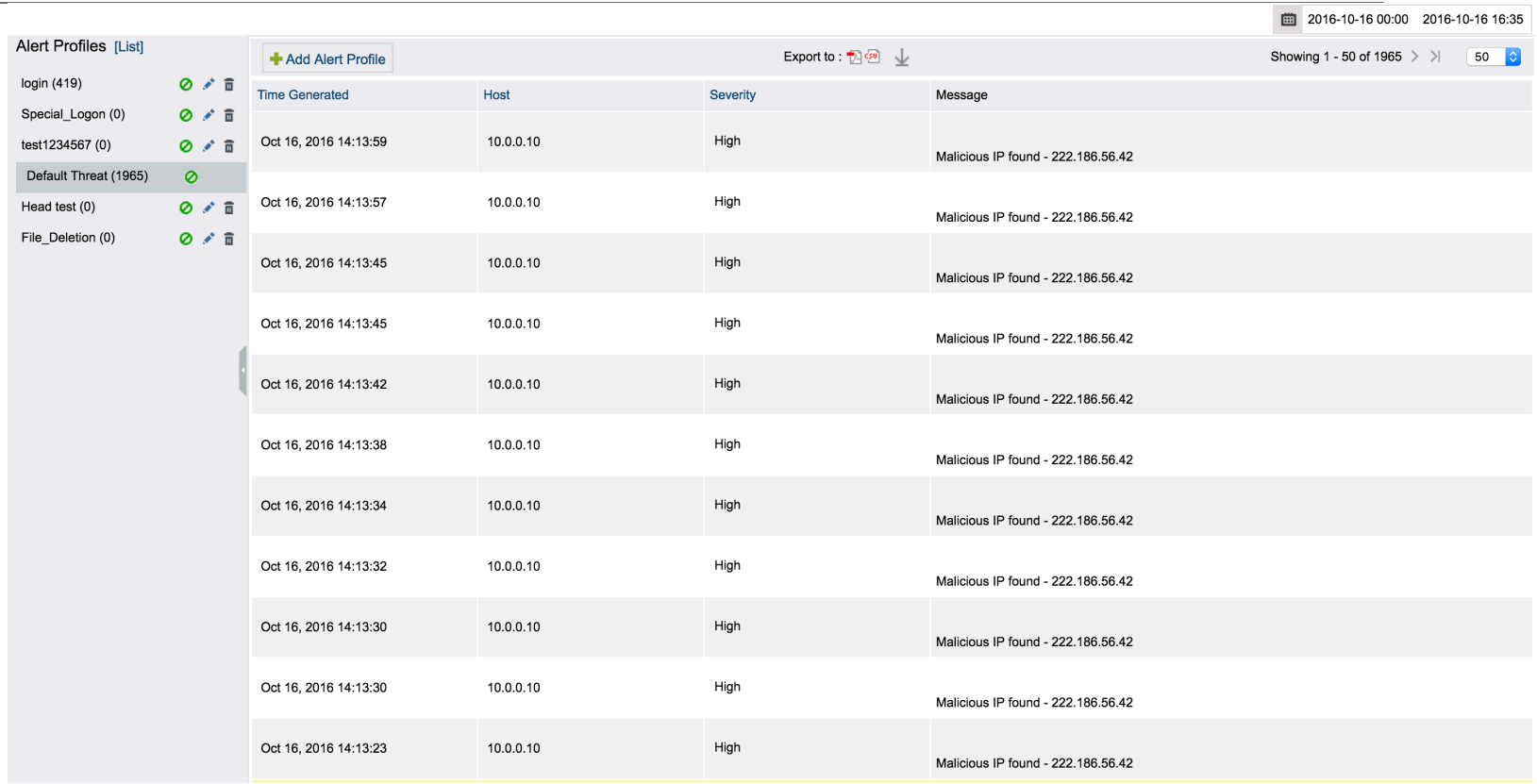
위협 피드 경고

- EventLog Analyzer는 여러 오픈 소스 및 STIX/TAXII 기반 위협 피드를 처리.
- 동적으로 업데이트되는 6억 개 이상의 악성 IP, URL 및 도메인 데이터베이스.
- 의심스러운 IP, URL 및 도메인에서 트래픽이 감지되면 실시간 알림을 제공.
- 이 기능을 설정하는 데 사전 구성이 필요 없음.

위협 피드 경고: 예


ManageEngine
EventLog Analyzer
공격자
알려진 악성 IP가
네트워크에 접속을 시도.
EventLog Analyzer는
실시간으로 관리자에게 알림.

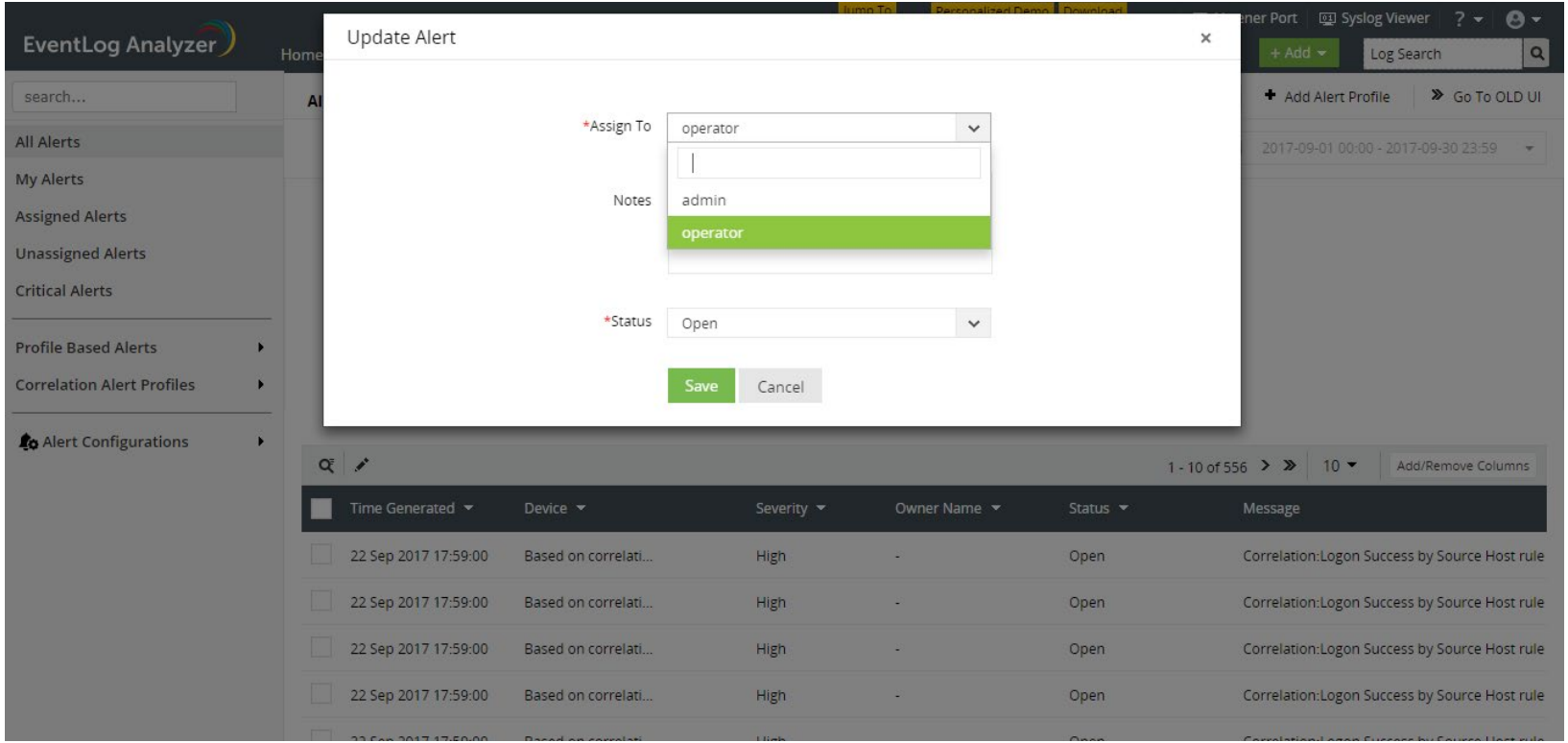
위협 피드 경고: 예


2016-10-16 00:00
2016-10-16 16:35
Alert Profiles [List]
login (419)
Special_Logon (0)
test1234567 (0)
Default Threat (1965)
Head test (0)
File_Deletion (0)
Add Alert Profile
Export to :
Showing 1 - 50 of 1965
50
Time Generated
Host
Severity
Message
Oct 16, 2016 14:13:59
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:57
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:45
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:45
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:42
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:38
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:34
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:32
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:30
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:30
10.0.0.10
High
Malicious IP found - 222.186.56.42
Oct 16, 2016 14:13:23
10.0.0.10
High
Malicious IP found - 222.186.56.42

사건 관리

- 내장된 사건 관리 콘솔을 사용하여 보안 사건을 관리.
- 운영자에게 사고 티켓을 자동으로 할당.
- 사건 티켓을 추적하고 여러 보기를 사용하여 티켓을 필터링하는 등의 작업을 수행.
- 또는 사건 티켓을 ServiceDesk Plus 등의 ITSM 또는 헬프데스크로 전달.

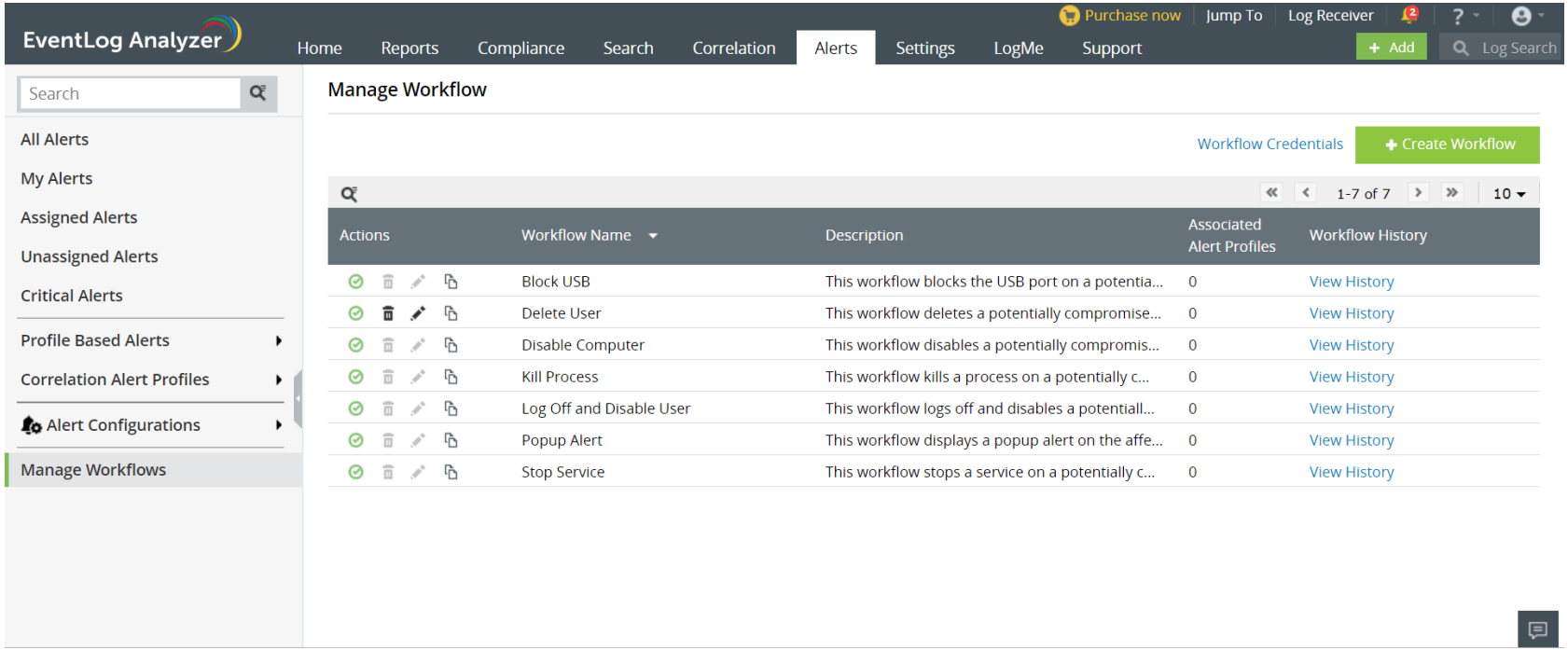
사건 관리 – 담당자 배정


EventLog Analyzer
Home
search...
All Alerts
My Alerts
Assigned Alerts
Unassigned Alerts
Critical Alerts
Profile Based Alerts
Correlation Alert Profiles
Alert Configurations
Update Alert
*Assign To
operator
Notes
admin
operator
*Status
Open
Save
Cancel
Syslog Viewer
+ Add
Log Search
Add Alert Profile
Go To OLD UI
2017-09-01 00:00 - 2017-09-30 23:59
1 - 10 of 556
10
Add/Remove Columns
Time Generated
Device
Severity
Owner Name
Status
Message
22 Sep 2017 17:59:00
Based on correlati...
High
-
Open
Correlation:Logon Success by Source Host rule

자동화된 워크플로

- 사건 대응 관리를 자동화하여 공격을 억제하거나 영향을 최소화.
- 사전 정의된 워크플로를 경고 프로필과 연결하여 감지된 보안 사고를 자동으로 수정.
- 보안 경고가 트리거될 때 자동으로 실행되는 사건 워크플로를 만들고 관리.
- EventLog Analyzer의 기본 제공 워크플로를 사용하거나 유연한 워크플로 빌더를 사용하여 요구 사항에 따라 워크플로 규칙을 사용자 지정.

자동화된 워크플로



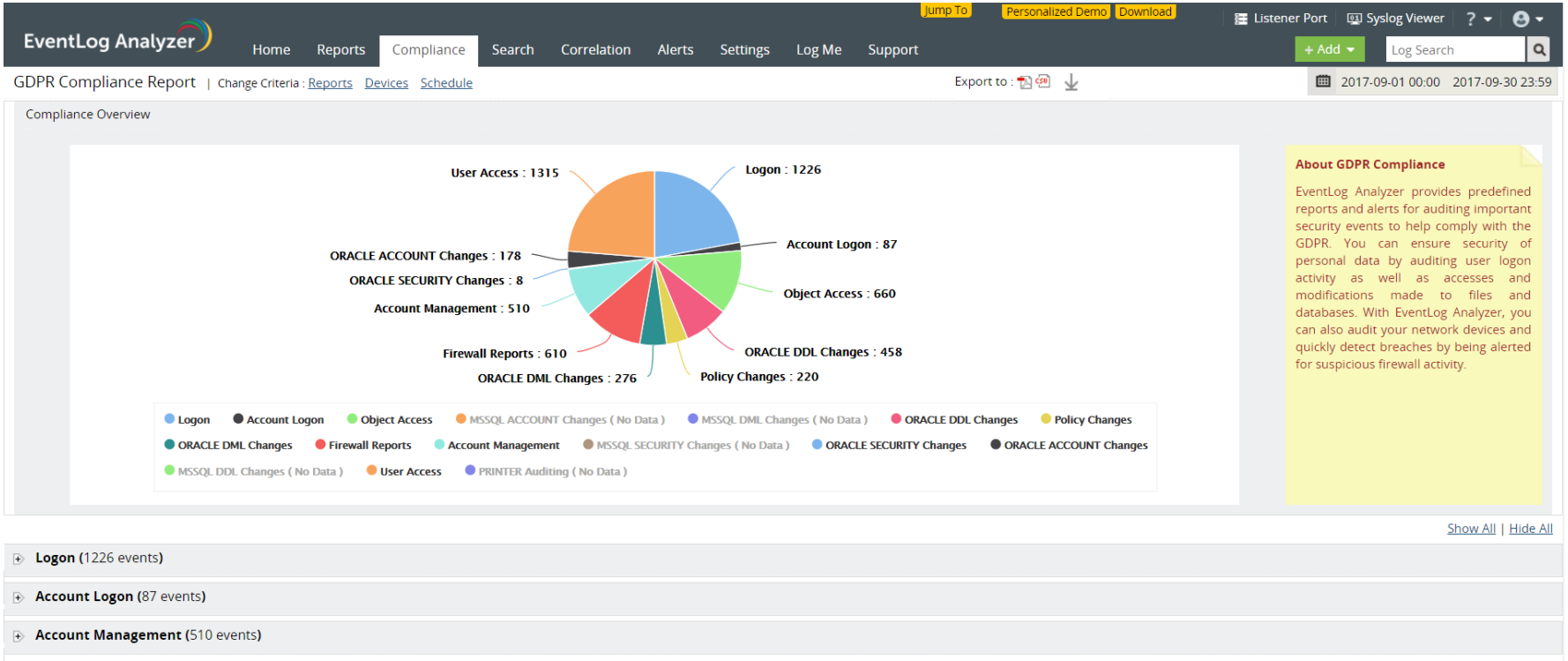
ManageEngine

통합 규정 준수 관리 시스템

통합 규정 준수 관리 시스템

- 즉시 사용 가능한 규정 준수 보고서 (국제 산업계 표준):
  - PCI DSS
  - GDPR
  - FISMA
  - HIPAA
  - GLBA
  - SOX
  - ISO 27001
- 내부 보안 정책을 충족하기 위해 기존 보고서를 수정하거나 새 규정 준수 보고서 작성 가능.
- 강력한 검색 기능과 보안 로그 보관 기능으로 대부분의 규정 준수 정책에 대한 포렌식 분석 및 로그 보관 요구 사항을 충족

통합 규정 준수 관리 시스템



ManageEngine

EventLog Analyzer: 제품 차별화 요소

- 배포 및 사용이 간편합니다.
- 다양한 로그 소스를 지원합니다.
- 추가 기능이 필요 없습니다!
- SIEM 솔루션과 쉽게 통합할 수 있습니다.
- 간단한 라이선스 모델 - 대상 장비 수량 기준

Edition 비교

Features	Premium Edition	Distributed Edition
Log collection and archival	✓	✓
Universal Log Parsing and indexing	✓	✓
File Integrity Monitoring	✓	✓
Real-time event correlation and alerts	✓	✓
Compliance reporting	✓	✓
Log forensics	✓	✓
Scalable architecture	✗	✓
Multi-geographical location monitoring	✗	✓
Server specific reports	✗	✓
Rebranding and client specific views	✗	✓

전세계 10,000 이상의 고객이 사용 중

ManageEngine

감사합니다

텔리맨트 주식회사
https://www.tmn.co.kr
02) 588-7350

기술 질문: inforeq@tmn.co.kr
견적 요청: sales-info@tmn.co.kr