기술정보

차세대 Endpoint 통합보안관제 솔루션 'Tanium'

효성ITX㈜

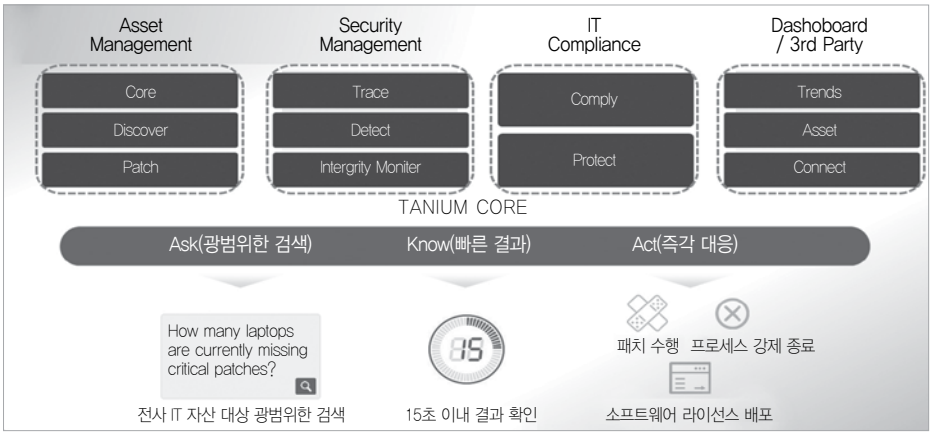
개요

효성의 정보통신(IT) 전문 계열사 '효성ITX'는 End point 통합보안관제시스템인 'Tanium(태니엄)'을 국내 기업/포털/금융/공공기관에 공급 및 운영을 개시했다.

Tanium(태니엄)은 15초 이내에 전사 네트워크에 연결된 Endpoint 시스템의 보안정책/이벤트/자원 상태를 확인 및 제어할 수 있는 차세대 통합보안관제 솔루션이다. Endpoint는 대체로 PMS(패치관리시스템), NAC(네트워크 제어시스템), SMS(시스템관리), EDR(Endpoint 탐지/대응시스템) 등 단위 보안 솔루션을 통하여 개별적으로 운영하고 있다.

그리고 통합보안관제시스템(SIEM/ESM)은 FW, IPS, WAF 등 탐지 이벤트를 통합적으로 수집하여 정책 생성을 통한 실시간 경보 및 분석 업무를 행한다. 대응 업무 시 FW, IPS 등 네트워크 보안시스템 위주의 한계성이 발생하며, 특히 최근 대부분의 보안 사고가 발생하는 End point에 대한 대응은 근본적인 한계가 발생한다.

Tanium(태니엄)은 Detect, Trace, Patch, Asset 등의 다양한 Module을 활용하고, 운영 중인 Endpoint 솔루션과 통합하여 Endpoint 통합보안관제 업무를 수행한다. Endpoint 통합보안관제시스템인 Tanium을 통해 Windows, Mac OS, Linux, Unix 등의 Endpoint를 15초 이내에 상황 인지 및 즉각 대응 관리를 통한 End point 통합보안관제 업무를 수행한다.



Endpoint 통합보안관제 솔루션 Tanium

개발 배경

기존 Endpoint 통합관리시스템은 매니저 서버 1대로 수천 대 수준의 관리의 한계를 보였으며, 특히 국내에서는 망분리 및 가상화 등으로 점점 증가하는 Endpoint를 통합적으로 보안관제하기 위한 획기적인 솔루션이 필요하게 되었으며, Tanium(태니엄)은 기존 수천 대 대비 100배 이상 증가된 수십만 대에서 백만 대 이상의 대규모 Endpoint를 15초 이내에 통합보안관제가 가능하도록 구축 및 운영할 수 있다.

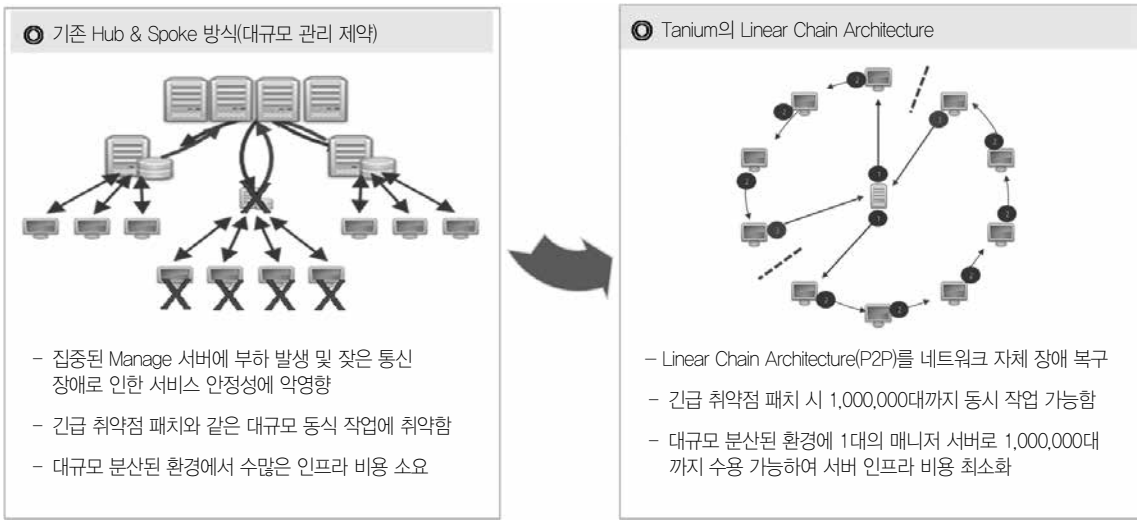
특히 시스템에서 일어나는 모든 정보를 실시간으로 파악할 수 있기 때문에 보안 리스크를 크게 감소시킬 수 있다. 피해가 발생했을 때 보안 담당자는 피해를 인지한 즉시 네트워크를 분리하고 포렌식 과정을 거쳐 패치를 배포해야 하지만, 대규모 Endpoint를 보유한 기업의 경우 기존의 보안 솔루션으로 전사의 추가 감염 여부 및 패치 배포를 하기는 어렵다. 효성ITX의 Tanium은 이러한 문제에 즉시 대응 가능하다.

공개 정보

Tanium이 특허 받은 Linear Chain Architecture는 Peer to Peer(P2P) 기반 프로토콜을 통해 수초 안에 모든 Endpoint의 상태를 조회하고 관리하여 수십만 대의 Endpoint를 보호, 통제 및 관리를 15초 이내에 수행할 수 있다.

Tanium에서 배포한 Client S/W는 Desktop, Server, POS 등 Endpoint에 설치되어 현황(HW, Application, 파일명, 레지스트리, OS 정보, Network, 관리/미관리 SW 자산 목록 등)을 단 15초 만에 가시화하여 즉각적인 대응이 가능하다.

또한 특허 받은 P2P 기반 프로토콜이 탑재된 Tanium Client는 전사 네트워크 전체를 Scan해 허가되지 않은 기기 및 어플리케이션 및 MAC Address 확인하여 미인지 자산을 관리할 수 있도록 한다.



Tanium Linear Chain Architecture 비교

Tanium(태니엄)의 주요 특장점

- Automated Threat Detection – 악의적인 이상 행위와 IOC 패턴을 적용하여 빠르게 탐지/대응
- Incident Response – Endpoint의 과거 발생한 사건을 포렌식 데이터를 이용해 면밀히 조사하고 공격을 막아내는데 소모되는 시간과 노력을 단축
- Asset Management – 이용 빈도가 낮은 하드웨어, 라이선스가 종료된 소프트웨어와 같이 관리가 미흡한 자산을 식별하고 정리하는 과정을 통해 비용 절감
- Patch Management – 기존 솔루션 대비 약 10,000배 빠른 패치 속도 제공
- Compliance – Endpoint 보안 상태를 항상 투명하게 유지하고, 침해사고 발생 시 Endpoint 단에서 적합한 IT 정책을 유지

통합보안관제시스템(SIEM/ESM)을 통한 통합보안관제 프로세스는 '탐지 → 분석(정/오탐 분석) → 대응(네트워크 차단) → 보고'의 4단계로 이루어지고, Tanium(태니엄)을 통한 "Endpoint 통합보안관제 프로세스"는 '예방 → 정보 수집 → 탐지 → 분석 → 1차대응 → 2차대응 → 보고'의 7단계로 이루어진다.

실시간 경보 기반(통합보안관제)의 한계를 해결하기 위해 3단계를 추가했다.

1) OS 및 Application의 취약점 패치를 통한 사전 Risk 예방
2) 지속적으로 발생하는 알려지지 않은 Threat(위협)을 능동적으로 찾음은 물론, Threat Hunting을 통한 사전(Threate) 위협 분석
3) Endpoint의 포렌직 수준의 분석을 통한 Threat 접점(유입 지점) 차단 및 확산 경로 차단

또한 Endpoint에 대한 Vulnerability(취약점)+Asset(자산)+Threat(위협)을 통한 위험도 평가를 통한 사전 예방 및 사고 발생 시 포렌직 수준의 분석 및 OS 기반의 제어를 통하여 Endpoint 통합보안관제 업무 프로세스를 수행한다.

〈용어 설명〉

1) Endpoint : 엔터프라이즈 네트워크에 연결되고 네트워크 기반 응용프로그램을 실행하는 모든 네트워크 장치. 네트워크 장치에는 랩톱, 데스크톱 시스템 및 서버가 포함된다.
2) EDR : EDR(Endpoint Detection and Response)은 Endpoint 레벨에서 지속적인 모니터링과 대응을 제공하는 보안 솔루션을 의미
3) NAC : NAC(Network Access Control) 시스템은 과거 IP 관리 시스템에서 발전한 솔루션으로, 기본적인 개념은 IP 관리 시스템과 거의 같고, IP 관리 시스템에 네트워크에 대한 통제를 강화한 것이다.
4) FW : FW(Firewall)은 기업이나 조직의 모든 정보가 컴퓨터에 저장되면서, 컴퓨터의 정보 보안을 위해 외부에서 내부, 내부에서 외부의 정보통신망에 불법으로 접근하는 것을 차단하는 시스템이다.
5) IPS : IPS(Intrusion Prevention Sytem)은 인터넷 웜 등의 악성코드 및 해킹 등을 통한 침입이 일어나기 전에 실시간으로 침입을 막고 알려지지 않은 방식의 침입으로부터 네트워크와 호스트 컴퓨터를 보호하는 솔루션이다.

차세대 Endpoint 통합보안관제솔루션(Tanium)을 통한 통합보안관제 프로세스