# Stealthwatch

## StealthWatch® System은 더 빠르고 정밀한 위협 탐지, 보안 사고 대응 및 포렌식을 위해 업계 최고의 네트워크 가시성과 보안 인텔리전스를 제공합니다.

NetFlow 및 기존 인프라의 기타 텔레메트리 데이터를 사용하여 비용 효율적으로 전체 네트워크를 센서 그리드로 전환하고, 제로 데이 악성코드, DDoS(Distributed Denial-of-Service) 공격, 내부 위협, APT(Avanced Persistent Threat)를 비롯한 비정상적인 트래픽 및 행동을 탐지합니다. StealthWatch의 웹 인터페이스는 직관적입니다. 또한 네트워크에서 트래픽의 측면 이동에 대한 단일 보기를 제공합니다. 그러면서도 인텔리전스 및 알림 기능은 매우 정교합니다. 이처럼 단순하면서도 세련되고 강력한 플랫폼에서 사용성, 보안 분석, 조기 위협 탐지를 향상합니다.

### 장점

StealthWatch는 네트워크 트래픽에 대한 고유한 보기 및 분석을 통해 다음을 획기적으로 개선합니다.

- 실시간 위협 탐지
- 보안 사고 대응 및 포렌식
- 네트워크 세그먼테이션
- 네트워크 성능 및 용량 계획
- 규제 요건을 준수할 수 있는 역량

### Stealthwatch Management Console

StealthWatch Management Console은 네트워크 전반에서 이루어지는 모든 활동에 대한 상황 정보를 볼 수 있도록 서로 다른 IT 그룹에 대해 단일 관점을 제공합니다. 운영자는 한 눈에 볼 수 있는 간단한 인터페이스를 통해 문제를 신속하게 파악하고 적절히 대응할 수 있습니다.

콘솔의 수용력에 의해 분석되고 표시 가능한 NetFlow 데이터의 용량이 결정될 뿐만 아니라 구축 가능한 StealthWatch Flow Collector 수도 결정됩니다. 콘솔은 하드웨어 어플라이언스 또는 가상 머신으로 제공됩니다.

표 1~3에는 콘솔의 장점, 모델 및 사양이 나열되어 있습니다.

StealthWatch Management Console의 주요 기능은 다음과 같습니다.

- 사용자 신원 추적
- 유연한 구축 옵션, 가상 어플라이언스 포함
- 빠른 침입 경로 분석 및 트러블슈팅
- 관계형 플로우 맵
- NAT 스티칭

- 맞춤형 대시보드
- 맞춤형 보고서
- 자동 차단, 치료, 속도 제한
- 애플리케이션, 서비스, 포트, 프로토콜, 호스트, 피어 및 상호작용에 대한 "Top n" 보고서
- 트래픽 구성 분석
- Point-of-View™ 기술을 기반으로 맞춤화가 가능한 사용자 인터페이스
- 멀티 기가비트 및 대규모 MPLS(Multiprotocol Label Switching) 네트워크 환경 지원
- 고급 플로우 시각화
- 거대용량 확장 기능
- 내부 및 외부 모니터링 결합
- 용량 계획 및 트래픽 트렌드 기록
- WAN 최적화 보고
- DSCP(Differentiated Services Code Point) 대역폭 사용
- 웜 전파 시각화
- 고속 네트워크에 대한 내부 보안

**표 1.** StealthWatch Management Console 의 주요 혜택

| 장점 | 설명 |
|---|---|
| **실시간 최신 데이터** | 의심스러운 네트워크 동작을 파악할 수 있도록 수백 개 네트워크 세그먼트에서 트래픽을 동시에 모니터링하기 위한 데이터 흐름을 제공합니다. 이 기능은 엔터프라이즈 레벨에 특히 유용합니다. |
| **보안 위협 탐지 및 우선순위 지정 기능** | 보안 위협을 신속하게 탐지하여 우선순위 지정, 네트워크 오용 및 최적화되지 않은 성능 파악, 엔터프라이즈 전반의 이벤트 대응 관리 등과 같은 작업이 하나의 컨트롤 센터에서 모두 이루어집니다. |
| **네트워크 그룹** | 조직의 트래픽 상태를 쉽게 확인할 수 있도록 네트워크 그룹 및 관계 맵을 생성합니다. 운영 및 보안 팀에서 주의해야 할 위치를 몇 초 이내에 정확하게 파악할 수 있습니다. |
| **그래픽 표현** | 네트워크의 상태를 명확하고 이해하기 쉬운 형식으로 표현합니다. |
| **보안 상태를 빠르게 평가** | 운영자가 조직의 보안 상태를 빠르게 평가할 수 있도록 홈 대시보드에 다양한 경보 카테고리를 표시합니다. |
| **StealthWatch 어플라이언스 관리** | Flow Collector, Flow Sensor 및 IDentity 어플라이언스를 비롯한 StealthWatch 어플라이언스를 구성, 조정 및 관리합니다. |
| **다양한 유형의 플로우 데이터 사용** | Netflow, IPFIX(Internet Protocol Flow Information Export), sFlow를 비롯한 다양한 유형의 플로우 데이터를 사용합니다. 결과: 비용 효율적인 행동 기반 네트워크 보호를 실현합니다. |
| **확장성** | 아무리 큰 네트워크 수요도 지원합니다. 초고속 환경에서도 잘 작동하며 크기에 상관없이 IP 연결이 가능한 네트워크의 모든 부분을 보호할 수 있습니다. |
| **전달 방법 선택** | 모든 규모의 조직에 적합한 확장형 디바이스인 Appliance Edition을 주문할 수 있습니다.<br>또는 Appliance Edition과 동일한 기능을 수행하지만 VMware 환경에서 사용하도록 설계된 Virtual Edition을 주문할 수 있습니다. |
| **향상된 네트워크 관리** | 트렌드 분석, 방화벽 및 용량 계획, 성능 모니터링을 통해 네트워크 관리 기능을 개선합니다. |

| 장점 | 설명 |
| --- | --- |
| **APT, 악성코드 및 내부자 위협 처리** | 진화하는 위협을 차단하는 데 필요한 심층적 가시성과 상황을 제공합니다. 여기에는 웜, 바이러스 및 기타 악성코드와 표적 공격, DDoS 공격, 내부자 위협, APT 등 모든 것이 포함됩니다. 보안 담당자가 잠재적인 피해를 완화하기 위해 빠르고 결단력 있게 조치하는 데 필요한 상황 정보가 포함된 경고를 제공합니다. |
| **네트워크 트랜잭션에 대한 감사 추적** | 보다 효율적인 포렌식 조사를 위해 모든 네트워크 트랜잭션에 대한 전체적인 감사 추적을 제공합니다. |
| **맞춤화가 가능한 실시간 관계형 플로우 맵** | 조직 트래픽의 현재 상태에 대한 그래픽 보기를 제공합니다. 관리자는 위치, 기능, 가상 환경 등과 같은 기준에 따라 네트워크의 맵을 쉽게 구성할 수 있습니다. 2개의 호스트 그룹을 연결하면 운영자가 이러한 그룹 간의 트래픽 이동을 빠르게 분석할 수 있습니다. 그리고 문제의 데이터 포인트를 선택하면 어떠한 시점에서나 발생하는 일들에 대한 심층적인 통찰력을 확보할 수 있습니다. |

**표 2.** StealthWatch Management Console 모델

| 모델 | Flow Collector 최대 지원 개수 | 플로우 스토리지 용량 |
| --- | --- | --- |
| **StealthWatch Management Console VE** | 최대 5 | 1TB |
| **StealthWatch Management Console 1000** | 5 | 1TB |
| **Stealthwatch Management Console 2000** | 25 | TB |

**표 3.** StealthWatch Management Console 사양, 모델별

| | SMC 500 및 1010 | SMC 2010 |
| --- | --- | --- |
| **네트워크** | 1 management port: 10/100/1000BASE-TX, copper | |
| **데이터베이스 용량** | 1TB (RAID 6 redundant) | 2TB (RAID 6 redundant) |
| **하드웨어 플랫폼** | R630 | |
| **하드웨어 생성** | 13G | |
| **랙 유닛(마운트 가능)** | 1RU | |
| **전원** | Redundant 750W AC, 50/60 Hz, auto-ranging (100V to 240V) | |
| **열방출량** | 시간당 최대 2,891Btus | |
| **규격** | 높이: 1.68인치(4.3cm)<br>너비: 17.08인치(43.4cm)<br>깊이: 27.25인치(69.2cm) | |
| **유닛 무게** | 41lb(18.6kg) | |
| **레일** | Sliding ReadyRails with cable management arm | |

| | |
|---|---|
| **규제 준수** | FCC(미국만 해당) Class A<br>DOC(캐나다) Class A<br>CE Mark (EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3, EN60950)<br>VCCI Class A<br>UL 1950<br>CSA 950 |

**참고:** 이러한 사양은 StealthWatch 6.7 에 적용됩니다.

## Stealthwatch Flow Collector

StealthWatch Flow Collector는 물리적 환경과 가상 환경 모두에 대한 네트워크 가시성과 보안 인텔리전스를 제공하여 보안 사고 대응을 개선할 수 있도록 돕습니다.

네트워크에서 수집되는 Netflow 텔레메트리의 용량은 구축된 Flow Collector의 용량에 따라 결정됩니다. Flow Collector를 여러 대 설치할 수 있습니다. Flow Collector는 하드웨어 어플라이언스 또는 가상 머신으로 제공됩니다. 표 4는 Flow Collector의 장점을 간략하게 설명하고 표 5에는 해당 사양이 나와 있습니다.

**표 4.** StealthWatch Flow Collector의 주요 장점

| 장점 | 설명 |
|---|---|
| **플로우 상황 정보 증가** | 프록시 서버에서 URL 및 프록시 사용자 데이터를 수집하여 해당 네트워크 플로우 데이터와 연결합니다. |
| **트래픽 가시성 향상** | 웹 프록시를 통과하는 네트워크 상호작용을 고려하면 Stealthwatch System에 대한 가시성이 향상됩니다. |
| **SLIC 위협 피드 모니터링** | 프록시 기록의 URL 데이터를 SLIC(StealthWatch Labs Intelligence Center) 위협 피드와 자동으로 비교합니다. |
| **조사 지원** | 콘솔 내의 데이터를 수동으로 조사합니다. |
| **정확도 향상** | Stealthwatch System에 상황 데이터를 제공하여 보안 이벤트의 정확성을 높입니다. |
| **프록시와 플로우 데이터의 상관관계** | 프록시 서버에서 URL 및 프록시 사용자 데이터를 수집하여 해당 네트워크 플로우 데이터와 연결합니다. 이 정보는 SLIC 위협 피드와 자동으로 비교됩니다. 또한 콘솔 내에서 수동 조사를 지원하는 데 사용됩니다. |
| **가시성** | 조직에서 프록시 상호작용의 상대 측에 연결된 번역된 주소를 확인하도록 허용하여 네트워크에서 사각 지대를 제거합니다. |
| **위협 탐지** | 프록시 기록을 수집한 후 플로우 기록과 연결하여 각 플로우에 대한 사용자 애플리케이션 및 URL 정보를 제공함으로써 상황 인식을 높입니다. 이 프로세스에서는 조직에서 위협을 파악하고 MTTK(Mean Time to Know)를 단축할 수 있도록 역량을 강화합니다. |
| **보안 사고 대응** | 더 정확한 트러블슈팅, 사고 대응 및 포렌식을 위해 프록시 서버를 통해 이동하는 웹 트래픽에 대한 추가 상황을 제공합니다. |
| **실시간 트래픽 분석** | 청구, 대역폭 어카운트, 네트워크 성능 문제 해결을 위해 실시간 트래픽 분석을 제공합니다. |
| **플로우 트래픽 모니터링** | 의심스러운 네트워크 행동을 파악할 수 있도록 수백 개 네트워크 세그먼트를 통해 플로우 트래픽을 동시에 모니터링합니다. 이 기능은 엔터프라이즈 레벨에 특히 유용합니다. |
| **보안 침입 경로 식별** | 더 빠른 보안 사고 대응을 위해 몇 초 이내에 침입 경로를 격리합니다. |
| **실행 가능한 인사이트** | 많은 비용이 드는 프로브를 사용하지 않고 성능에 대한 실행 가능한 인사이트를 제공합니다. |
| **확장된 데이터 보존** | 조직과 기관에서 많은 양의 데이터를 장기적으로 보관할 수 있습니다. |
| **다양한 유형의 플로우 데이터** | 비용 효율적인 행동 기반 네트워크 보호를 제공하도록 다양한 유형의 플로우 데이터(Netflow, IPFIX, sFlow)를 사용합니다. |
| **확장성** | 초고속 환경에서도 잘 작동하며 크기에 상관없이 IP 연결이 가능한 네트워크의 모든 부분을 보호할 수 있습니다. |
| **중복 제거 및 스티칭** | 둘 이상의 라우터를 통과하는 플로우를 한 번만 계산하도록 중복을 제거합니다. 그런 다음 플로우 정보를 결합하여 |

| 장점 | 설명 |
|---|---|
| | 네트워크 트랜잭션에 대한 전체 가시성을 제공합니다. |
| **지리적으로 분산된 네트워크를 통한 엔드 투 엔드 가시성** | 엔드 투 엔드 보호를 제공하고 지리적으로 분산된 네트워크의 성능을 향상할 수 있도록 여러 네트워크 또는 네트워크 세그먼트에서 고속 네트워크 행동 데이터를 집계합니다. |
| **전달 방법 선택** | 모든 규모의 조직에 적합한 확장형 디바이스인 Appliance Edition을 주문할 수 있습니다.<br>또는 Appliance Edition과 동일한 기능을 수행하지만 VMware 환경에서 사용하도록 설계된 Virtual Edition을 주문할 수 있습니다. 이 솔루션은 할당된 리소스에 따라 동적으로 확장됩니다. |

**표 5.** StealthWatch Flow Collector 사양, 모델별

| | FC 1010 | FC 2010 | FC 4010 | FC 5020 |
|---|---|---|---|---|
| **설명** | 여러 인터페이스에서 플로우를 수집하도록 예비 전원, 스토리지 및 추가 인터페이스 제공 중간 규모 이상의 네트워크를 위한 마력 | 매우 큰 Netflow, sFlow 또는 IPFIX 환경을 위한 전체 하드웨어 이중화 및 플로우 처리 마력 | 대규모 확장성, 확장 가능한 스토리지 기능, 대용량 플로우 데이터 처리 가능 | Cisco UCS 플랫폼에 탁월한 성능을 요구하는 엔터프라이즈 고객을 위해 생성된 대용량 플로우 수집 솔루션 |
| **초당 최대 플로우 수*** | 최대 30,000 | 최대 60,000 | 최대 120,000 | 최대 240,000 |
| **최대 내보내기 또는 라우터** | 500 | 1000 | 2000 | 4096 |
| **하드웨어 플랫폼** | R630 | R630 | R630 | • **엔진:** UCSC-C220-M4S<br>• **데이터베이스 노드:** UCSC-C240-M4S2 |
| **네트워크** | 관리 포트 1개:<br>10/100/1000BASE-TX, copper<br>3 monitor or listening ports | | | • 1x 1Gbps dedicated management port<br>• 1x Port 10000SFP+ Uplink to Engine/Database Node<br>• 2x Intel i350 GbE Ethernet controller ports (LAN1, LAN2) |
| **플로우 스토리지** | 1TB<br>(RAID 6 redundant) | 2TB<br>(RAID 6 redundant) | 4TB<br>(RAID 6 redundant) | 8TB<br>(RAID 10 redundant) |
| **하드웨어 생성** | 13G | | | |
| **랙 유닛(마운트 가능)** | 1RU | | 2RU | • **엔진:** 1RU<br>• **데이터베이스 노드:** 2RU |
| **전원** | Redundant 750W AC, 50/60 Hz, auto-ranging (100V to 240V) | | | • **엔진:** Redundant 770W Power Supplies (1+1)<br>• **데이터베이스 노드:** Redundant 1200W Power Supplies (1+1) |
| **열방출량** | 2891 Btus per hour, maximum | | | **엔진:** 2891 Btus per hour maximum<br>**데이터베이스 노드:** 4100 Btus per hour maximum |
| **규격** | • **높이**: 1.68인치(4.3cm)<br>• **너비**: 17.08인치(43.4cm) | • **높이**: 1.68인치(4.3cm)<br>• **너비**: 17.08인치(43.4cm) | • **높이**: 3.4인치(8.7cm)<br>• **너비**: 17.5인치(44.4cm) | **엔진**<br>• **높이:** 1.7인치(4.32cm)<br>• **너비:** 16.89인치(43.0cm)<br>• **깊이:** 29.8인치(75.6cm) |

| | FC 1010 | FC 2010 | FC 4010 | FC 5020 |
|---|---|---|---|---|
| | • **깊이**: 27.25인치(69.2cm) | • **깊이**: 27.25인치(69.2cm) | • **깊이**: 27.25인치(69.2cm) | **데이터베이스 노드**<br>• **높이:** 3.43인치(8.7cm)<br>• **너비:** 17.65인치(44.8cm)<br>• **깊이:** 29.0인치(73.8cm) |
| **무게** | 41lb(18.6kg) | | 65 lb(29.5 kg) | • **엔진:** 38파운드(17.24kg)<br>• **데이터베이스 노드:** 65파운드(29.48kg) |
| **레일** | Sliding ReadyRails with cable management arm | | | Sliding Rack Rails (UCSC-RAILB-M4) |
| **규제 준수** | • FCC(미국만 해당) Class A<br>• DOC & ICES(캐나다) Class A<br>• CE Mark (EN55022 Class A, EN55024, EN61000-3-2, EN 61000-3-3, EN60950)<br>• VCCI Class A UL 1950<br>• CSA 950<br>• 목록 전체가 필요하면 이메일(sales@lancope.com)에 문의하십시오. | | | • 제품은 규제 지침 2004/108/EC 및 2006/95/EC에 따라 CE 마크 표시를 준수해야 합니다.<br>• UL 60950-1 Second Edition<br>• CAN/CSA-C22.2 No. 60950-1 Second Edition<br>• EN 60950-1 Second Edition<br>• IEC 60950-1 Second Edition<br>• AS/NZS 60950-1<br>• GB4943 2001<br>• 목록 전체가 필요하면 이메일(sales@lancope.com)에 문의하십시오. |

| **Virtual Flow Collector** | | | | | |
|---|---|---|---|---|---|
| **L-LC-FC-NF-VE-K9** | Flow Collector for NetFlow Virtual Edition | 30,000* | 1,000* | 1.0TB | 가상 |
| **L-LC-FC-SF-VE-K9** | Flow Collector for sFlow Virtual Edition | 30,000* | 1,000* | 1.0TB | 가상 |
| **L-LC-SW-VE-CONV-K9** | 물리적 어플라이언스에서 Virtual Edition으로 전환 | | | | |

**참고:** 이 사양은 StealthWatch 6.7에 적용됩니다.

* 초당 최대 플로우 수는 네트워크 상태에 따라 변할 수 있습니다.

## StealthWatch Flow Sensor

Flow Sensor는 Netflow를 지원하지 않는 스위치 및 라우팅 인프라의 세그먼트에 Netflow 데이터를 생성하는 구성요소입니다. 또한 오버레이 모니터링 솔루션이 IT 조직의 운영 모델에 더 적합한 환경에서 작동합니다. Flow Sensor에서 Cisco® NBAR(Network-Based Application Recognition)이 지원되지 않는 환경에 대한 레이어 7 애플리케이션 정보를 제공할 수 있습니다.

Flow Sensor에서는 네트워크와 서버 성능 메트릭에 대한 포괄적인 가시성을 제공합니다. 또한, 애플리케이션 및 프로토콜을 식별하기 위해 DPI(Deep Packet Inspection)와 행동 분석을 결합합니다. 따라서 보안, 네트워크 운영 및 애플리케이션 성능이 최적화됩니다.

네트워크에서 생성되는 Netflow 데이터의 양은 구축된 Flow Sensor의 용량에 의해 결정됩니다. Flow Sensor를 여러 대 설치할 수 있습니다. Flow Sensor는 가상 머신 환경을 모니터링하는 데 사용되며 하드웨어 어플라이언스 또는 소프트웨어로 제공됩니다. 표 6과 7에는 Flow Sensor의 주요 장점과 사양이 나열되어 있습니다.

StealthWatch Flow Sensor의 주요 기능은 다음과 같습니다.

- 레이어 7 애플리케이션 상황 정보
- 플로우 가시성
- Netflow 생성
- 가상 환경 가시성
- 최신 위협에 대한 실시간 업데이트
- TCP 연결을 위한 RTT(Round-Trip Time) 및 SRT(Server Response Time) 계산

**표 6.** StealthWatch Flow Sensor의 주요 장점

| 장점 | 설명 |
|---|---|
| **레이어 7 애플리케이션 가시성** | 애플리케이션 정보를 패킷 레벨 성능 통계와 함께 수집하여 실질적인 레이어 7 애플리케이션 가시성을 제공합니다. |
| **패킷 레벨 성능 및 분석** | 애플리케이션 정보를 패킷 레벨 성능 통계와 함께 수집하여 실질적인 레이어 7 애플리케이션 가시성을 제공합니다. |
| **네트워크 이상 징후에 대한 경고** | 비정상적인 네트워크 행동을 파악하고 즉시 상황과 관련된 인텔리전스와 함께 알람을 전송하여 보안 담당자가 빠르게 조치하여 피해를 줄일 수 있도록 합니다. |
| **비용 절감** | 몇 초 이내에 문제 또는 사고의 근본 원인을 식별하여 격리함으로써 운영 효율성을 높이고 비용을 절감합니다. |
| **전달 방법 선택** | 모든 규모의 조직에 적합한 확장형 디바이스인 Appliance Edition을 주문할 수 있습니다.<br>또는 Appliance Edition과 동일한 기능을 수행하지만 VMware 환경에서 사용하도록 설계된 Virtual Edition을 주문할 수 있습니다. |

**표 7.** StealthWatch Flow Sensor 사양

| | FS 1010 | FS 2010 | FS 3010 | FS 4010 |
|---|---|---|---|---|
| **커뮤니케이션** | | | | |
| **처리량** | 1.0Gbps<br>(512바이트 패킷)<br>400Mbps<br>(64바이트 패킷) | 2.5Gbps<br>(512바이트 패킷)<br>800Mbps<br>(64바이트 패킷) | 5.0Gbps<br>(512바이트 패킷)<br>1.2Gbps<br>(64바이트 패킷) | 20.0Gbps<br>(512바이트 패킷)<br>4Gbps<br>(64바이트 패킷) |
| **인터페이스** | | | | |
| **관리 포트** | 1 port: 10/100/1000BASE-TX, copper | | | |
| **모니터 포트** | 3 ports: 10/100/1000BASE-TX, copper | 5 ports: 1GB<br>(5 copper or 3 copper and 2 fiber optic);<br>rated to monitor 2.5Gbps | 2 ports: 10GB, fiber optic; rated to monitor 5Gbps total | 4 ports: 10GB, fiber optic; rated to monitor 20Gbps total |
| **콘솔 포트** | Serial, Kernel-based Virtual Machine (KVM) | | | |
| **물리적** | | | | |
| **하드웨어 플랫폼** | R220 | R630 | | |
| **하드웨어 생성** | 12G | 13G | | |
| **폼 팩터** | | 스택 가능 | | |
| **크기** | **높이**: 1.67인치(4.24cm)<br>**너비**: 17.09인치(43.4cm)<br>**깊이**: 15.5인치(39.37cm) | **높이**: 1.68인치(4.3cm)<br>**너비:** 18.99인치(48.24cm) 랙 래치 포함, 17.08인치(43.4cm) 랙 래치 제외<br>**깊이:** 29.25인치(74.3cm) | | |
| **무게** | 35 lb(15.4 kg) | 41파운드(18.6kg) maximum configuration | | |
| **스토리지** | 500GB nonredundant | 300GB (RAID 1 redundant) | | |
| **환경** | | | | |
| **전원** | Single; 250W (nonredundant) | Redundant 750W AC, 50/60 Hz, auto-ranging (100V to 240V) | | |
| **열방출량** | 1040 Btus per hour | 2891 Btus per hour maximum | | |
| **온도** | 작동: 10°C~35°C<br>(50°F~95°F)<br>스토리지: -40°C~65°C<br>(-40°F~149°F) | 작동: 10° to 35°C (50° to 95°F) with a maximum gradation of 10°C (50°F) per hour. 참고: For altitudes above 2950 feet, the maximum operating temperature is derated –17°C (1°F) per 550 feet<br>스토리지: -40° to 65°C (–40° to 149°F) with a maximum gradation of 20°C (68°F) per hour | | |
| **상대습도** | 작동: 10% to 80% (noncondensing) with maximum gradation of 10% per hour. 스토리지: 5% to 95% (noncondensing) | | | |
| **규제 준수** | CE Emissions/FCC Class A/RoHS | FCC(미국만 해당) Class A<br>DOC(캐나다) Class A<br>VCCI Class A/UL 1950/CSA 950<br>CE Mark (EN 55022 Class A, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 60950) | | |

**참고:** 이 사양은 StealthWatch 6.7에 적용됩니다.

## Virtual Flow Sensor

| 제품 부품 번호 | 설명 | 최대 네트워크 트래픽 | 네트워크 모니터링 포트 | 폼 팩터 |
|---|---|---|---|---|
| **Virtual Flow Sensor** | | | | |
| **L-LC-FSVE-VMW-K9** | Flow Sensor virtual appliance for VMware | * | - | 가상 |
| **L-LC-SW-VE-CONV-K9** | 물리적 어플라이언스에서 Virtual Edition으로 전환 | | | |

* 가상 머신 리소스에 따라 달라질 수 있습니다.

**참고:** Flow Sensor 어플라이언스 또는 Flow Sensor VE에 의해 생성된 플로우는 전체 Flow Collection 라이선스 제한에서 제외됩니다.

## StealthWatch UDP Director

UDP Director®는 엔터프라이즈 전반에서 네트워크 및 보안 데이터의 수집과 배포를 간소화합니다. 또한 여러 위치에서 필수 네트워크 및 보안 정보를 수신한 다음, 이러한 정보를 단일 데이터 스트림 형식으로 하나 이상의 대상에 전달하여 네트워크 라우터 및 스위치의 처리 전원을 줄일 수 있도록 도와줍니다.

표 8과 9는 Director의 주요 장점과 사양을 간략히 보여 줍니다.

**표 8.** StealthWatch UDP Director의 주요 장점

| 장점 | 설명 |
|---|---|
| **계획되지 않은 다운타임 및 서비스 중단 감소** | UDP Director High Availability는 UDP Director 2000 어플라이언스에서만 사용 가능하며, 1000 어플라이언스에서는 지원되지 않습니다. |
| **네트워크 보안 및 모니터링 간소화** | UDP Director에서는 Netflow, sFlow, syslog 및 SNMP(Simple Network Management Protocol) 정보에 대한 단일 표준화된 대상을 통합 및 제공함으로써 대규모 엔터프라이즈 내에서 다양한 유형의 네트워크와 보안 데이터 통합을 대폭 간소화합니다. UDP Director 어플라이언스는 연결되지 않은 모든 UDP애플리케이션에서 데이터를 수신할 수 있으며, 필요한 경우 데이터를 복제하여, 이를 여러 대상에 다시 전송할 수 있습니다. |
| **연결되지 않은 UDP 애플리케이션 지원** | 여러 라우터에서 보낸 tFlow 기록을 여러 Netflow 컬렉터에 복제할 수 있습니다. 이러한 유연성으로 인해 Netflow 내보내기 컨피그레이션의 많은 Netflow 대상 사양이 필요하지 않습니다. 여러 라우터와 스위치에서 보낸 sFlow 샘플을 여러 sFlow 컬렉터에 복제할 수 있습니다. Netflow 예에서와 마찬가지로 sFlow 엑스포터 컨피그레이션에 여러 sFlow 대상 사양이 필요하지 않습니다. Syslog 메시지를 여러 syslog 컬렉터에 자동으로 복제할 수 있습니다. 라우터, 스위치 및 기타 네트워크 디바이스의 SNMP 트랩을 여러 SNMP 관리 스테이션에 자동으로 수집하고 배포할 수 있습니다. |
| **모든 소스의 UDP 데이터를 모든 대상에 전달 가능** | 연결되지 않은 모든 UDP 애플리케이션에서 데이터를 수신할 수 있으며, 필요한 경우 데이터를 복제하여, 이를 여러 목적지로 다시 전송할 수 있습니다. |
| **인프라를 재구성할 필요 없음** | 새로운 툴을 추가하거나 제거할 때 인프라를 재구성할 필요 없이 포인트 로그 데이터(Netflow, sFlow, syslog, SNMP)를 단일 대상으로 연결합니다. |
| **상세한 플로우 통계 제공** | 조직에서는 상세한 Flow Statistics(플로우 통계) 기능을 사용하여 해당 환경의 초당 플로우(fps) 수를 예측하고 모니터링 요건을 확인할 수 있습니다. |
| **네트워크 인프라에 대한 컨피그레이션 시간 감소** | 네트워크 보안 및 모니터링 간소화 |
| **대역폭 감소** | 중복된 네트워크 로그 데이터를 줄여서 WAN 대역폭 사용을 줄입니다. |
| **서비스 중단 감소** | 계획되지 않은 다운타임 및 서비스 중단 감소 |

**표 9.** UDP Director 사양

| | UDP Director 1010 | UDP Director 2010 |
|---|---|---|
| **패킷 복제 속도(입력)**** | 25,000pps | 37,500pps |
| **패킷 복제 속도(출력)**** | 50,000pps | 75,000pps |
| **네트워크** | • 1 management port: 10/100/1000BASE-TX, copper<br>• 1 monitor or listening port<br>• Integrated HTTPS web UI; serial and KVM access to command-line interface (CLI) | • 1 management port: 10/100/1000BASE-TX, copper<br>• 3 monitor or listening ports<br>• 선택 사항: 2 add-on Gbps optical fiber single-port NICs |
| **스토리지** | 160GB, nonredundant | 300GB, RAID 6, redundant |
| **하드웨어 플랫폼** | R220 | R630 |
| **하드웨어 생성** | 12G | 13G |
| **랙 유닛(마운트 가능)** | 1RU | |
| **전원** | Single power supply (250W) | • Redundant 750W AC, 50/60 Hz<br>• Auto-ranging (100V to 240V) |
| **열방출량** | 1039 Btus per hour maximum | 2891 Btus per hour maximum |
| **운영 체제** | Hardened Linux | |
| **크기** | **높이**: 1.67인치(4.24cm)<br>**너비**: 17.09인치(43.4cm)<br>**깊이**: 15.5인치(39.37cm) | **높이:** 1.68인치(4.3cm)<br>**너비:** 18.99인치(48.24cm) 랙 래치 포함, 17.08인치(43.4cm) 랙 래치 제외<br>**깊이:** 29.25인치(74.3cm) 전원 공급 장치 및 베젤 포함, 27.25인치(69.2cm) 전원 공급 장치 및 베젤 제외 |
| **유닛 무게** | 34 lb(15 kg) | 65 lb(29.5 kg) |
| **레일** | Rack chassis with Versa Rail, round holes for third-party racks | Sliding ReadyRails with cable management arm |
| **규제 준수** | FCC(미국만 해당) Class A<br>DOC(캐나다) Class A<br>CE Mark (EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3, EN60950)<br>VCCI Class A UL 1950 | |

## Virtual Edition UDP Director

| 제품 부품 번호 | 설명 | 최대 입력(pps) | 최대 출력(pps) | 모니터링 포트 | 폼 팩터 |
|---|---|---|---|---|---|
| L-LC-UDP-VE-K9 | UDP Director VE 라이선스 | | | | |

* 가상 머신 리소스에 따라 달라질 수 있습니다.

## Proxy License

Lancope의 Proxy License 구성요소는 네트워크 보안 애널리스트에게 더 많은 네트워크 가시성과 위협 탐지 기능을 제공합니다. 또한 프록시의 상대 측에서 상호작용에 대한 추가 상황 정보를 수집하여, 보안 위협을 처리할 시기를 효율적으로 결정할 수 있도록 해줍니다.

Proxy License 기능에서 지원하는 웹 프록시는 다음과 같습니다.

- Blue Coat
- McAfee
- Squid
- Cisco

표 10에 Proxy License에 대한 주문 정보가 설명되어 있습니다.

**표 10.** Proxy License 주문 정보

| 부품 번호 | 설명 |
|---|---|
| **PX-100-U** | 최대 100명의 사용자에 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스 |
| **PX-1000-U** | 최대 1000명의 사용자에 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스 |
| **PX-10000-U** | 최대 10,000명의 사용자에 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스 |
| **PX-25K-U** | 최대 25,000명의 사용자에 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스 |
| **PX-50K-U** | 최대 50,000명의 사용자에 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스 |
| **PX-100K-U** | 최대 100,000명의 사용자에 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스 |

## Stealthwatch Cloud License

워크로드를 오프프레미스와 클라우드 환경으로 이동하는 추세가 두드러지고 있습니다. 이를 통해 조직에는 유연성이 확대되지만, 이러한 가상 인스턴스 내에서 트래픽 플로우를 보는 기능이 저해되기도 합니다. 그러나 Stealthwatch Cloud License가 있으면 퍼블릭, 프라이빗 및 하이브리드 클라우드 환경에서 Cisco Stealthwatch의 모든 네트워크 가시성, 위협 탐지 및 분석 기능을 이용할 수 있습니다. Stealthwatch Cloud License는 Cisco Stealthwatch의 가상 라이선스 애드온(add-on)으로서 NaaS(Network as a Sensor)를 클라우드로 확장하여 사용자가 실시간 상황 인식을 확보하고 전체 인프라에 대한 보안을 강화할 수 있습니다.

Cisco StealthWatch Cloud License의 기능은 클라우드 컴퓨팅 서비스인 AWS(Amazon Web Services)에도 설치가 가능합니다.

현재 다음과 같은 호스트 운영 체제를 지원합니다.

- Linux

  CentOS 5, 6, 7(x64 전용)

  RedHat Enterprise Linux 5, 6, 7(x64 전용)

표 11에는 주요 기능 및 혜택이 나열되어 있습니다. 표 12에는 크기 정보가 요약되어 있습니다.

**표 11.** Cloud License의 기능 및 장점

| 장점 | 설명 |
|---|---|
| **가시성 향상** | 퍼블릭, 프라이빗 및 하이브리드 클라우드 인프라 내의 사각지대를 없애 NaaS(Network as a Sensor)를 클라우드로 확장합니다. |
| **보안 강화** | 의심스러운 활동과 잠재적 공격에 대한 실시간 위협 탐지로 강화된 보안을 제공합니다. |
| **대응 가속화** | 정교한 보안 분석으로 탁월한 포렌식 조사 기능을 제공합니다. |
| **규제 준수 강화** | 네트워크 전체에서 규정을 준수할 수 있도록 실시간 상황 인식 및 네트워크 가시성을 제공합니다. |

**표 12.** Cloud License Concentrator 크기 정보

| 에이전트 | Rec AWS 인스턴스 유형 | 가상 어플라이언스 등가 사양 | | | |
|---|---|---|---|---|---|
| | | CPU 코어 | 메모리(GB) | 디스크(GB) | 네트워크 대역폭 |
| **1000** | c4.large | 2 | 4 | 8 | 250Mbps |
| **2000** | c4.xlarge | 4 | 8 | 16 | 500Mbps |
| **4000** | c4.2xlarge | 8 | 16 | 32 | 1Gbps |
| **10000** | c4.4xlarge | 16 | 32 | 64 | 2Gbps |
| **20000** | c4.8xlarge | 32 | 64 | 64 | 4Gbps |

## Cloud License Agent 리소스 사용량

리소스 사용량은 에이전트가 구축된 호스트 VM에서 발생하는 활동량에 따라 달라집니다.

- 1% CPU 일반, 5% 최대
- 128-200MB RAM, 1% - 2% 일반, ~1% 최악의 케이스
- <1G 디스크 공간

참조용 상위 최종 사용량:

- CPU: 8 개 코어, 모두 100% 사용률
- RAM: 연결 수 20,000 개 이하, 활성/비활성 혼합

## Cloud License 주문 정보

**표 13.** Cloud License 주문 정보

| Base PID | Tiering |
|---|---|
| **L-SW-CL-LIC=** | 1~400개의 호스트 |
| | 401~800개의 호스트 |
| | 801~1,200개의 호스트 |
| | 1,201~2,000개의 호스트 |
| | 2,001~6,000개의 호스트 |
| | 6,001~20,000개의 호스트 |

| | |
|---|---|
| | 20,001~80,000개의 호스트 |
| | 80,001~200,000개의 호스트 |
| | 200,001~400,000개의 호스트 |
| | 400,001~2,000,000개의 호스트 |

### Stealthwatch Flow License

플로우 라이선스는 StealthWatch Management Console에서 플로우를 집계하는 데 필요합니다. 또한 플로우 라이선스는 수집할 수 있는 플로우의 용량을 정의합니다. 라이선스를 임의의 순열로 결합하여 원하는 레벨의 플로우 용량을 달성할 수 있습니다. 사용 가능한 라이선스 용량은 다음과 같습니다.

- 1,000개의 플로우
- 10,000개의 플로우
- 25,000개의 플로우
- 50,000개의 플로우
- 100,000개의 플로우

## 주문 정보

Stealthwatch System 주문 가이드가 시스템의 모델, 구성요소 및 라이선스 유형을 이해을 이해하는 데 도움이 될 것입니다.

주문하려면 어카운트 담당자에게 문의하십시오.

### 서비스 및 지원

다양한 서비스 프로그램이 StealthWatch용으로 제공되고 있습니다. Cisco의 혁신적인 프로그램은 높은 수준의 고객 만족을 실현하기 위해 인력, 프로세스, 툴, 파트너의 조합을 통해 제공됩니다. 이러한 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다. 전문 서비스에 대한 자세한 내용은 기술 지원 홈 페이지를 참조하십시오.

## Cisco Capital

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용 가능합니다. 자세한 내용은 관련 웹 사이트에서 알아보십시오.

## 추가 정보

Cisco Stealthwatch에 관한 자세한 내용은 www.cisco.com/go/stealthwatch를 참조하십시오.

자세히 알아보려면 Stealthwatch-interest@cisco.com으로 이메일을 보내십시오.


미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.





Printed in USA C78-736512-03 07/16