

# StealthWatch

StealthWatch® System은 더 빠르고 세부적인 위협 탐지, 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. 하지만 인텔리전스 및 알림 기능은 매우 정교합니다. 이처럼 단순하면서도 세련되고 강력한 플랫폼에서는 사용성, 보안 분석, 조기 위협 탐지를 향상합니다.

## 이점

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

- 실시간 위협 탐지
- 사고 대응 및 포렌식
- 네트워크 세그먼테이션
- 네트워크 성능 및 용량 계획
- 규정 준수 요구 사항을 준수할 수 있는 역량

## StealthWatch Management Console

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

콘솔의 용량에 따라 분석하여 표시할 수 있는 Netflow 데이터의 볼륨과 구축 가능한 StealthWatch FlowCollector 수가 결정됩니다. 콘솔은 하드웨어 어플라이언스 또는 가상 머신으로 사용 가능합니다.

표 1~3에는 콘솔의 이점, 모델 및 사양이 나열되어 있습니다. StealthWatch Management Console의 주요 기능은 다음과 같습니다.

- 사용자 ID 추적
- 유연한 구축 옵션, 가상 어플라이언스 포함
- 빠른 근본 원인 분석 및 문제 해결
- 관계형 플로우 맵
- NAT 스티칭
- 맞춤형 대시보드
- 맞춤형 보고서
- 자동 차단, 교정, 속도 제한

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

표 1. StealthWatch Management Console의 주요 이점

이점	설명
실시간 최신 데이터	의심스러운 네트워크 행동을 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 작업은 단일한 컨트롤 센터에서 모두 수행합니다.
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	FlowCollector, FlowSensor 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. 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.
APT, 악성코드 및 내부자 위협 처리	진화하는 위협을 차단하는 데 필요한 심층적 가시성과 상황을 제공합니다. 여기에는 웹, 바이러스 및 기타 악성코드와 표적 공격, DDoS 시도, 내부자 위협, APT 등 모든 것이 포함됩니다. 보안 요원이 잠재적인 피해를 완화하기 위해 빠르고 결단력 있게 조치하는 데 필요한 컨텍스트 정보가 포함된 경고를 제공합니다.
네트워크 트랜잭션에 대한 감사 추적	보다 효율적인 포렌식 조사를 위해 모든 네트워크 트랜잭션에 대한 전체 감사 추적을 제공합니다.
사용자 정의 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 그룹 간에 연결을 생성하면 운영자가 이러한 그룹 간의 트래픽 이동을 빠르게 분석할 수 있습니다. 또한 해당 데이터 포인터를 선택하면 특정 시점에 발생하는 일들에 대한 심층적 통찰력을 확보할 수 있습니다.

표 2. StealthWatch Management Console 모델

모델	지원되는 최대 FlowCollectors 수	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	관리 포트 1개: 10/100/1000BASE-TX, UTP	
데이터베이스 용량	1TB(RAID 6 이중화)	2TB(RAID 6 이중화)
하드웨어 플랫폼	R630	
하드웨어 생성	13G	
랙 유닛(마운트 가능)	1RU	
전원	이중화 750W AC, 50/60Hz, 자동 범위 지정(100V~240V)	
열 소산율	시간당 최대 2,891Btus	
크기	높이: 1.68인치(4.3cm) 너비: 17.08인치(43.4cm) 깊이: 27.25인치(69.2cm)	
유닛 무게	41lb (18.6kg)	
레일	케이블 관리 암을 사용하여 ReadyRails 이동	
규정 준수	FCC(미국만 해당) Class A DOC(캐나다) Class A CE 마크(EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3, EN60950) VCCI Class A	

참고: 이러한 사양은 StealthWatch 6.7에 적용됩니다.

### StealthWatch FlowCollector

StealthWatch FlowCollector는 물리적 환경과 가상 환경 모두에 대한 네트워크 가시성과 보안 인텔리전스를 제공하여 사고 대응을 개선할 수 있도록 도와줍니다.

네트워크에서 수집되는 Netflow 텔레메트리의 볼륨은 구축된 FlowCollectors의 용량에 따라 결정됩니다. 여러 FlowCollectors를 설치할 수 있습니다. FlowCollectors는 하드웨어 어플라이언스 또는 가상 머신으로 사용 가능합니다. 표 4에서는 FlowCollector의 이점을 간략하게 설명하고 표 5에서는 해당 사양을 나열합니다.

표 4. StealthWatch FlowCollector의 주요 이점

이점	설명
플로우 컨텍스트 증가	프록시 서버에서 URL 및 프록시 사용자 데이터를 수집하여 해당 네트워크 플로우 데이터와 연결합니다.
트래픽 가시성 향상	웹 프록시를 통과하는 네트워크 상호작용을 고려하면 StealthWatch 시스템에 대한 가시성이 향상됩니다.
SLIC 위험 피드 모니터링	프록시 기록의 URL 데이터를 SLIC(StealthWatch Labs Intelligence Center) 위험 피드와 자동으로 비교합니다.
조사 지원	콘솔 내의 데이터를 수동으로 조사합니다.
정확도 향상	StealthWatch 시스템에 상황 인식 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 위험 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.
위험 탐지	프록시 기록을 수집한 후 플로우 기록과 연결하여 각 플로우에 대한 사용자 애플리케이션 및 URL 정보를 제공함으로써 상황 인식을 높입니다. 이 프로세스에서는 조직에서 위험을 파악하고 MTTK(Mean Time to Know)를 단축할 수 있도록 역량을 강화합니다.
사고 대응	더 정확한 문제 해결, 사고 대응 및 포렌식을 위해 프록시 서버를 통해 이동하는 웹 트래픽에 대한 추가 컨텍스트를 제공합니다.
실시간 트래픽 분석	청구, 대역폭 계정 및 네트워크 계정 관리 및 네트워크 성능 문제 해결을 위해 실시간 트래픽 분석을 제공합니다.

이점	설명
플로우 트래픽 모니터링	의심스러운 네트워크 동작을 파악할 수 있도록 수백 개 네트워크 세그먼트를 통해 플로우 트래픽을 동시에 모니터링합니다. 이 기능은 엔터프라이즈 레벨에 특히 유용합니다.
보안 근본 원인 식별	더 빠른 보안 사고 대응을 위해 몇 초 이내에 근본 원인을 격리합니다.
실행 가능한 통찰력	많은 비용이 드는 프로브를 사용하지 않고 성능에 대한 실행 가능한 통찰력을 제공합니다.
확장된 데이터 보존	조직과 기관에서 많은 양의 데이터를 장기적으로 보관할 수 있습니다.
다양한 유형의 플로우 데이터	다양한 유형의 플로우 데이터(Netflow, IPFIX, sFlow)를 사용하여 비용 효율적인 행동 기반 네트워크 보호를 제공합니다.
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 중복 제거를 수행합니다. 그런 다음 플로우 정보를 결합하여 네트워크 트랜잭션에 대한 전체 가시성을 제공합니다.
지리적으로 분산된 네트워크를 통한 엔드 투 엔드 가시성	여러 네트워크 또는 네트워크 세그먼트에서 고속 네트워크 행동 데이터를 집계하여 엔드 투 엔드 보호를 제공하고 지리적으로 분산된 네트워크를 통해 성능을 향상합니다.
전달 방법 선택	모든 규모의 조직에 적합한 확장형 디바이스인 Appliance Edition을 주문할 수 있습니다. 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 FlowCollector 사양, 모델별

	FC 1010	FC 2010	FC 4010	FC 5000
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	탁월한 성능을 요구하는 엔터프라이즈 고객을 위해 작성된 대용량 플로우 수집 솔루션
초당 최대 플로우 수*	최대 30,000	최대 60,000	최대 120,000	최대 240,000
최대 내보내기 또는 라우터 네트워크	500	1000	2000	4096
관리 포트 1개: 10/100/1000BASE-TX, UTP 모니터 또는 수신 포트 3개				<ul style="list-style-type: none"> <li>관리, 모니터링 또는 수신 포트 1개: 10/100/1000BASE-TX</li> <li>향후 사용을 위해 예약된 포트 1개: 10/100/1000BASE-TX</li> <li>데이터베이스 노드 연결 포트 1개: 10Gbps</li> <li>향후 사용을 위해 예약된 포트 1개: 10Gbps</li> </ul>
플로우 스토리지	1TB (RAID 6 이중화)	2TB (RAID 6 이중화)	4TB (RAID 6 이중화)	6TB (RAID 10 이중화)
하드웨어 플랫폼	R630	R630	R630	<ul style="list-style-type: none"> <li>엔진: R620</li> <li>데이터베이스 노드: R820</li> </ul>
하드웨어 생성 랙 유닛(마운트 가능)	13G 1RU		2RU	<ul style="list-style-type: none"> <li>엔진: 1RU</li> <li>데이터베이스 노드: 2RU</li> </ul>
전원	이중화 750W AC, 50/60Hz, 자동 범위 지정(100V~240V)			<ul style="list-style-type: none"> <li>R620: 이중, 핫 플러그, 예비 전원 공급 장치(1+1), 750W</li> <li>R820: 이중, 핫 플러그, 비이중화 전원 공급 장치(2+0), 1100W</li> </ul>
열 소산율	시간당 최대 2,891Btus			<ul style="list-style-type: none"> <li>R620: 시간당 최대 2,891Btus</li> <li>R820: 시간당 최대 4,100Btus</li> </ul>

	FC 1010	FC 2010	FC 4010	FC 5000
크기	높이: 1.68인치(4.3cm) 너비: 17.08인치(43.4cm) 깊이: 27.25인치(69.2cm)	높이: 1.68인치(4.3cm) 너비: 17.08인치(43.4cm) 깊이: 27.25인치(69.2cm)	높이: 3.4인치(8.7cm) 너비: 17.5인치(44.4cm) 깊이: 27.25인치(69.2cm)	<b>R620</b> 높이: 1.68인치(4.3cm) 너비: 17.08인치(43.4cm) 깊이: 27.25인치(69.2cm) <b>R820</b> 높이: 3.4인치(8.7cm) 너비: 17.5인치(44.4cm) 깊이: 29.2인치(74.1cm)
무게	41lb(18.6kg)		65 lb(29.5kg)	<b>R620:</b> 64lb(29.03kg) <b>R820:</b> 85lb(38.5kg)
레일 규정 준수	케이블 관리 암을 사용하여 ReadyRails 이동 FCC(미국만 해당) Class A DOC & ICES(캐나다) Class A CE 마크(EN55022 Class A, EN55024, EN61000-3-2, EN 61000-3-3, EN60950) VCCI Class A UL 1950 CSA 950			

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

\* 초당 최대 플로우 수는 네트워크 상태에 따라 변경될 수 있습니다.

### StealthWatch FlowSensor

FlowSensor는 Netflow를 지원하지 않는 스위치 및 라우팅 인프라의 세그먼트에 대한 Netflow 데이터를 생성하는 구성 요소입니다. 또한 오버레이 모니터링 솔루션이 IT 조직의 운영 모델에 더 적합한 환경에서 작동합니다.

FlowSensor에서는 Cisco® NBAR(Network-Based Application Recognition)이 지원되지 않는 환경에 대한 레이어 7 애플리케이션 정보를 제공할 수 있습니다.

FlowSensor에서는 네트워크 및 서버 성능 메트릭에 대한 포괄적인 가시성을 제공합니다. 또한 DPI(Deep Packet Inspection)와 행동 분석을 결합하여 애플리케이션 및 프로토콜을 식별합니다. 따라서 보안, 네트워크 운영 및 애플리케이션 성능이 최적화됩니다.

네트워크에서 생성되는 Netflow 데이터의 볼륨은 구축된 FlowSensors의 용량에 따라 결정됩니다. 여러 FlowSensors를 설치할 수 있습니다. FlowSensors를 하드웨어 어플라이언스 또는 소프트웨어로 사용하여 가상 머신 환경을 모니터링할 수 있습니다. 표 6과 7에는 FlowSensors의 주요 이점과 사양이 나열되어 있습니다.

StealthWatch FlowSensor의 주요 기능은 다음과 같습니다.

- 레이어 7 애플리케이션 컨텍스트
- 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 FlowSensor의 주요 이점

이점	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	보안 요원이 빠르게 조치하여 피해를 줄일 수 있도록 비정상적인 네트워크 행동을 파악하고 즉시 컨텍스트 인텔리전스와 함께 알람을 전송합니다.
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. 또는 Appliance Edition과 동일한 기능을 수행하지만 VMware 환경에서 사용하도록 설계된 Virtual Edition을 주문할 수 있습니다.

표 7. StealthWatch FlowSensor 사양

	FS 1010	FS 2010	FS 3010	FS 4010
<b>커뮤니케이션</b>				
처리량	1.0Gbps (512바이트 패킷) 400Mbps (64바이트 패킷)	2.5Gbps (512바이트 패킷) 800Mbps (64바이트 패킷)	5.0Gbps (512바이트 패킷) 1.2Gbps (64바이트 패킷)	20.0Gbps (512바이트 패킷) 4Gbps (64바이트 패킷)
<b>인터페이스</b>				
관리 포트	포트 1개: 10/100/1000BASE-TX, UTP			
모니터 포트	포트 3개: 10/100/1000BASE-TX, UTP	포트 5개: 1GB (UTP 5개 또는 3개 및 광섬유 2개), 2.5Gbps 모니터링 가능 정격	포트 2개: 10GB, 광섬유, 총 5Gbps 모니터링 가능 정격	포트 4개: 10GB, 광섬유, 총 20Gbps 모니터링 가능 정격
콘솔 포트	시리얼, KVM(Kernel-based Virtual Machine)			
<b>물리적</b>				
하드웨어 플랫폼	R220	R630		
하드웨어 생성	12G	13G		
폼 팩터		스택 가능		
크기	높이: 1.67인치(4.24cm) 너비: 17.09인치(43.4cm) 깊이: 15.5인치(39.37cm)	높이: 1.68인치(4.3cm) 너비: 18.99인치(48.24cm) 랙 래치 포함, 17.08인치(43.4cm) 랙 래치 제외 깊이: 29.25인치(74.3cm)		
무게	35lb(15.4kg)	41lb(18.6kg) 최대 컨피그레이션		
저장	500GB 비이중화	300GB(RAID 1 이중화)		
<b>환경</b>				
전원	단일, 250W(비이중화)	이중화 750W AC, 50/60Hz, 자동 범위 지정(100V~240V)		
열 소산율	시간당 1,040Btus	시간당 최대 2,891Btus		
온도	작동: 10°C~35°C(50°F~95°F) 보관: -40°C~65°C(-40°F~149°F)	운영: 10°C~35°C(50°F~95°F) 시간당 10°C(50°F)의 최대 차이 참고: 고도가 2,950피트를 초과할 경우 최대 작동 온도는 550피트당 -17°C(1°F)씩 감소됩니다. 보관: -40°C~65°C(-40°F~149°F) 시간당 20°C(68°F)의 최대 차이		
상대습도	운영: 10%~80%(비응축) 시간당 10%의 최대 차이 보관: 5%~95%(비응축)			
규제 준수	CE Emissions/FCC Class A/RoHS	FCC(미국만 해당) Class A DOC(캐나다) Class A VCCI Class A/UL 1950/CSA 950 CE 마크(EN 55022 Class A, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 60950)		

참고: 이러한 사양은 StealthWatch 6.7에 적용됩니다.

## 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 단일한 데이터 스트림 형식으로 하나 이상의 대상에 전달하여 네트워크 라우터 및 스위치의 처리 전원을 줄일 수 있도록 도와줍니다.

표 8과 9에서는 Director의 주요 이점과 사양을 간략히 보여 줍니다.

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

이점	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 단일하고 표준화된 대상을 통합 및 제공함으로써 대규모 엔터프라이즈 내에서 다양한 유형의 네트워크와 보안 데이터 통합을 대폭 간소화합니다. UDP Director 어플라이언스에서는 연결되지 않은 UDP 애플리케이션에서 데이터를 수신한 다음, 이를 여러 대상에 다시 전송할 수 있으며, 필요한 경우 데이터를 복제합니다.
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 내보내기 컨피그레이션의 여러 sFlow 대상 사양이 필요하지 않습니다. Syslog 메시지를 여러 syslog 컬렉터에 자동으로 복제할 수 있습니다. 라우터, 스위치 및 기타 네트워크 디바이스의 SNMP 트랩을 자동으로 수집하여 여러 SNMP 관리 스테이션에 배포할 수 있습니다.
모든 소스의 UDP 데이터를 모든 대상에 전달 가능	연결되지 않은 UDP 애플리케이션에서 데이터를 수신한 다음, 이를 여러 대상에 다시 전송하고, 필요한 경우 데이터를 복제합니다.
인프라를 재구성할 필요 없음	새로운 톨을 추가하거나 제거할 때 인프라를 재구성할 필요 없이 포인트 로그 데이터(Netflow, sFlow, syslog, SNMP)를 단일 대상에 전달합니다.
세부 플로우 통계 제공	조직에서는 Detailed Flow Statistics(세부 플로우 통계) 기능을 사용하여 해당 환경의 초당 플로우(fps) 수를 예측하고 모니터링 요구 사항을 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	<ul style="list-style-type: none"> <li>• 관리 포트 1개: 10/100/1000BASE-TX, UTP</li> <li>• 모니터 또는 수신 포트 1개</li> <li>• 통합 HTTPS 웹 UI, CLI(Command Line Interface)에 대한 시리얼 및 KVM 액세스</li> </ul>	<ul style="list-style-type: none"> <li>• 관리 포트 1개: 10/100/1000BASE-TX, UTP</li> <li>• 모니터 또는 수신 포트 3개</li> <li>• 선택 사항: 애드온 Gbps 광섬유 단일 포트 NIC 2개</li> </ul>
저장	160GB, 비이중화	300GB, RAID 6, 이중화
하드웨어 플랫폼	R220	R630
하드웨어 생성	12G	13G
랙 유닛(마운트 가능)	1RU	
전원	단일 전원 공급 장치(250W)	<ul style="list-style-type: none"> <li>• 이중화 750W AC, 50/60Hz</li> <li>• 자동 범위 지정(100V~240V)</li> </ul>
열 소산율	시간당 최대 1,039Btus	시간당 최대 2,891Btus
운영 체제	Hardened Linux	
크기	<p><b>높이:</b> 1.67인치(4.24cm)</p> <p><b>너비:</b> 17.09인치(43.4cm)</p> <p><b>깊이:</b> 15.5인치(39.37cm)</p>	<p><b>높이:</b> 1.68인치(4.3cm)</p> <p><b>너비:</b> 18.99인치(48.24cm) 랙 래치 포함, 17.08인치(43.4cm) 랙 래치 제외</p> <p><b>깊이:</b> 29.25인치(74.3cm) 전원 공급 장치 및 베젤 포함, 27.25인치(69.2cm) 전원 공급 장치 및 베젤 제외</p>
유닛 무게	34lb(15kg)	65lb(29.5kg)
레일	Versa 레일이 장착된 랙 새시, 서드파티 랙을 위한 둥근 구멍	케이블 관리 암을 사용하여 ReadyRails 이동
규정 준수	FCC(미국만 해당) Class A DOC(캐나다) Class A CE 마크(EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3, EN60950) VCCI Class A UL 1950	

## ProxyWatch

Lancop의 ProxyWatch 구성 요소는 네트워크 보안 분석가에게 추가적인 네트워크 가시성 및 위협 탐지 기능을 제공합니다. 또한 프록시의 상대 측에서 상호작용에 대한 추가 컨텍스트를 수집하여, 보안 위협을 처리할 시기를 효율적으로 결정할 수 있도록 해줍니다.

ProxyWatch 기능에서 지원하는 웹 프록시는 다음과 같습니다.

- Blue Coat
- McAfee
- Squid
- Cisco



표 10에는 ProxyWatch 모델이 나열되어 있습니다.

표 10. ProxyWatch 주문 정보

부품 번호	설명
PX-100-U	최대 100명의 사용자에게 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스
PX-1000-U	최대 1,000명의 사용자에게 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스
PX-10000-U	최대 10,000명의 사용자에게 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스
PX-25K-U	최대 25,000명의 사용자에게 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스
PX-50K-U	최대 50,000명의 사용자에게 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스
PX-100K-U	최대 100,000명의 사용자에게 대한 프록시 기록의 수집, 상관관계 및 분석을 위한 라이선스

### StealthWatch 플로우 라이선스

플로우 라이선스는 StealthWatch Management Console에서 플로우를 집계하는 데 필요합니다. 또한 플로우 라이선스는 수집할 수 있는 플로우의 볼륨을 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 시스템 주문 가이드를 통해 시스템의 모델, 구성 요소 및 라이선스 유형을 이해할 수 있습니다.

주문하려면 어카운트 담당자에게 문의하십시오.

### 서비스 및 지원

StealthWatch를 위한 다양한 서비스 프로그램을 제공합니다. 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](#) 홈페이지를 참조하십시오.

### Cisco Capital

#### 목표 달성을 지원하는 파이낸싱

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 결제가 단 한 번뿐입니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. [자세히 알아보십시오.](#)

---

추가 정보

[Lancope.com](http://lancope.com)을 방문하거나 [info@lancope.com](mailto:info@lancope.com)에서 세일즈 담당자에게 문의하십시오.

StealthWatch 시스템에 대한 자세한 내용은 <http://lancope.com>을 참조하십시오.




---

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](http://www.cisco.com/go/offices)에서 확인하십시오.

 Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks)로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)