Cisco Stealthwatch Learning Network License

The Cisco Stealthwatch™ Learning Network License improves protection against branch threats.

The solution is part of the Cisco Stealthwatch family of products. Together they enhance visibility into advanced threats by identifying suspicious patterns of traffic within a Cisco® network.

The Learning Network License uses the Cisco Integrated Services Router (ISR) as a security sensor to monitor branch traffic through NetFlow, Network-Based Application Recognition (NBAR), intelligent sensors that use machine learning, and packet capture. It baselines traffic patterns to detect anomalies and help build effective branch security policies. You can mitigate threats directly from the branch by using the Cisco Stealthwatch manager to instruct the ISR to drop suspicious packets.

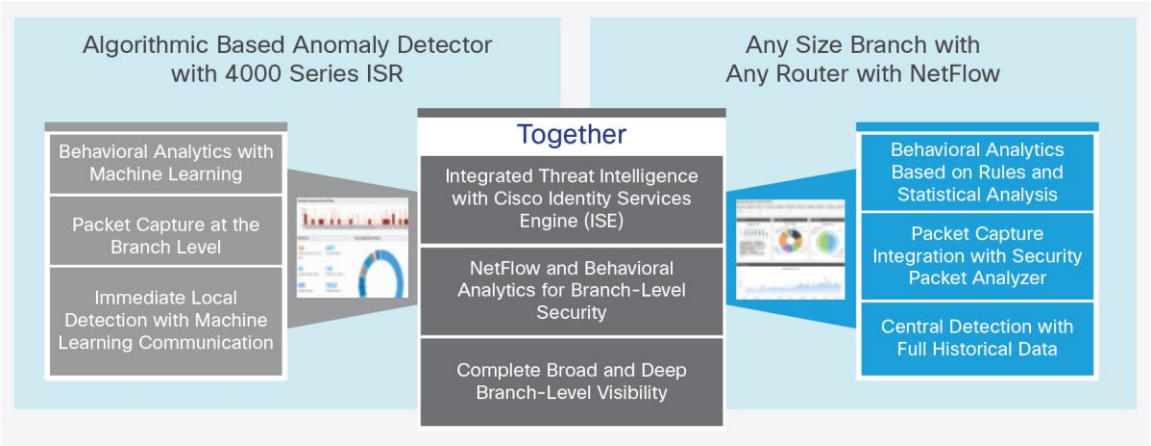
Figure 1 illustrates how we have expanded the Cisco Stealthwatch portfolio with the Learning Network License in the branch. We now offer both Cisco Stealthwatch (right) and the Learning Network License (left) to extend our "network as a sensor" and "network as an enforcer" initiatives.

With the Learning Network we add unique capabilities, including machine learning, local packet capture (PCAP) at the branch, and mitigation access control list (ACL) drop. These features are built into a Cisco IOS® container app within the Cisco 4000 Series Integrated Services Routers along with using local NetFlow and NBAR. With Cisco Stealthwatch we use NetFlow data sent to the central site, and behavioral analytics along with central detection for a full historical data. For your branch network you may want to use both solutions or only one.

Together, the two products give you:

- Exceptional anomaly detection methods
- The ability to spot zero-day attacks and to find trends 30, 60, and 90 days in the past
- Broad and deep branch-level visibility

Figure 1. Features and Capabilities of the Cisco Stealthwatch Portfolio and Learning Network License



Product Overview

The Cisco Stealthwatch Learning Network License embeds security into your network infrastructure by turning your router into a security device. It brings you deeper visibility across the branch network and between branches. It strengthens network protection and responds quickly to threats. It extends security to the branch without affecting network performance.

The Learning Network is made up of two components:

1. Distributed learning agents are placed at the edges of your network in your ISR branch routers. An agent can be implemented as a software agent with Cisco IOS XE Software and the Container feature. Optionally it can also be installed with the Cisco UCS® blade on the ISR.
2. The agent is managed by a central monitoring agent. The manager is installed on any virtual machine server. Each agent becomes uniquely customized to its environment, using machine-learning algorithms and techniques to learn what is normal (baseline) and to consequently detect anomalies. Each agent autonomously models traffic characteristics thanks to various data feeds such as NetFlow records, deep packet inspection of raw packets (for example, DNS packets), and even the local state available on the branch router or switch.

The agent builds its own models and avoids forwarding heavy traffic over the WAN for centralized analysis. It is designed to be lightweight in terms of memory and CPU consumption.

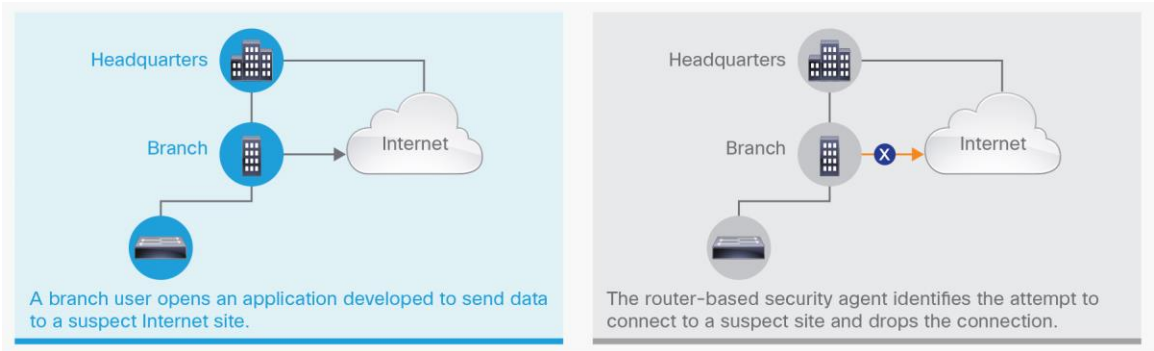
The manager is the user's point of entry to the Learning Network License solution. It is a highly scalable application running in the data center. It "orchestrates" the agents. It aggregates and stores the information they provide and amplifies their context with information from different sources. (These can include threat intelligence from Cisco pxGrid and the Cisco Identity Services Engine, intelligence from Talos, DNS transaction details, and so on.) The manager provides a way to retrieve all information for analysis and gives the user the ability to control and provide feedback to the system.

Features and Benefits

Feature	Benefit
Anomaly detection	"Anomaly detection" refers to the capability of a system such as the Learning Network to build a complex representation (model) of normal traffic. It potentially captures many dimensions (time of day, nature of traffic, number of packets per flow, flow duration, unseen traffic, etc.) with high granularity. Such models are used to detect "outliers," or anomalies, that can indicate security attacks and vulnerabilities. Such systems make extensive use of machine-learning algorithms that are usually (but not exclusively) unsupervised.
Relevance learning	Relevance learning is a crucial concept of self-learning networks. A "false positive" usually refers to an event that has been incorrectly determined as anomalous by anomaly detection. For example, if a system is trained to recognize a car and misclassifies a bike as a car, that classification is said to be a false positive. User relevancy is dynamically learned by the system thanks to labels provided by the user (for example, "like" or "dislike"). Upon receiving an anomaly, the user can provide like/dislike feedback. The h Learning Network License uses this feedback to constantly improve the relevancy of the anomalies raised by the system.
Mitigation actions	Distributed learning agents may be used not only for anomaly detection but also for anomaly mitigation. Anomalies are reported in detail by each agent to the manager. When the anomalous activity is understood, the user may prevent the anomalous traffic from being forwarded through the network, where it may do harm. For example, the user may drop the anomalous traffic on the local router adjacent to the detecting agent Alternatively, the user may drop all traffic to or from an anomalous host wherever it is seen in the network. The manger can also send access control lists back to the ISR.
Integration with an external system's ISE	The Learning Network License takes advantage of threat intelligence information available in the network to provide additional insights into anomalous activity in your network. If you have deployed the Cisco Identity Services Engine (ISE), the agent communicates with the ISE through the pxGrid API to ingest a rich set of personalized information regarding network users, their locations, and other attributes. When anomalous activity is detected in your network, the manager can provide finer detail regarding the offending hosts. It can possibly even identify the name of the user, his current location (the switch and switch port to which he is connected), and so on.
Integration with an external system's Talos database	The manager also takes advantage of a Talos database containing IP addresses known to have been involved in anomalous activity in the past, including the nature of that activity. The Talos database is another source of threat intelligence information applied to each anomaly.
Packet capture	In anomaly detection it is also critical to be able to capture the event details. Using the capabilities of the Integrated Services Router, the manager can instruct the router to packet-capture any event. Incident response and device-level mitigation can be done more quickly. The packet capture is limited by the hard-drive storage capabilities of the ISRs.

Use Case: Split Tunnel VPN Branch (IWAN)

Figure 2 shows a typical branch use with a split tunnel, direct Internet access, and a VPN link to headquarters. In this case the user is attempting to load a new application at the branch, and the application is attempting to send data to a suspected Internet site. The machine learning agent at the router identifies the suspicious traffic. The Learning Network Centralized Agent Manager (SCA) mitigates the event by applying an access control list to drop the connection.



Platform Support

The Stealthwatch Learning Network License is specifically designed to take advantage of the new Cisco 4000 Series Integrated Services Routers and their Cisco IOS XE module architecture. It allows the agent to be installed as a software agent in Cisco IOS XE containers. The agent can also be installed on a Cisco UCS E-Series blade. (For more information, go to: http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-e-series-servers/index.html).

You can add the Stealthwatch Learning Network License to any 4451, 4431, 4351, or 4331 ISR. (The 4321 and 4221 ISRs are being qualified now. Please contact Cisco for the latest support.) We recommend that you order the 4000 Series AX, AXV, or Cisco ONE 4000 Series ISR bundle. These come with the AppX license that the Stealthwatch Learning Network License requires and that all our security features, including Intelligent WAN, support. Please see the bundle ordering guide (Cisco 4000 Series Integrated Services Router Family Ordering Guide). In addition, please see the Cisco ONE WAN bundles C1-CISCO4431/K9, C1-CISCO4451/K9, C1-CISCO 4351, and C1-CISCO 4321. These also support SLN and include an 8 GB memory upgrade that the SLN requires. For information, visit: http://www.cisco.com/c/en/us/products/software/one-wan/wan-part-numbers.html.

Product Family	Platforms Supported	Cisco IOS Images (Feature Sets) Supported
Cisco 4000 Series ISRs	4431, 4451, 4351, 4331 ISRs; The *4321 and 4221 to be supported when testing is complete* The agent is supported as a software-only installation agent and optionally on the Cisco UCS E-Series blade. * Other ISR models are planned to be supported at later date.	Cisco IOS XE 3.16.0S or later with Universal and Application Experience (AppX) licenses or an AX or AXV bundle that includes AppX licenses.
Cisco UCS E-Series Server	Cisco UCS E140S M2 Software and later (for example, E160).	ESXi 5.5
Cisco 2900 and 3900 Series ISRs	2921, 2951, and 3945 ISRs. Supported only with the Cisco UCS E-Series blade.	Cisco IOS Release 15.5(3)M1 or later and the NBAR(2) Protocol Pack

Licensing

The Cisco Stealthwatch Learning Network License is a Smart Software licensing enabled product. The agent is sold under 1-year and 3-year term licenses. The manager has a perpetual license. If you do not already have a Smart License account, please see your Cisco representative to set one up. For information about Smart Software licensing go to: http://www.cisco.com/web/ordering/smart-software-licensing/index.html.

System Requirements

Agent in Cisco IOS XE Software	When the agent is run in Cisco IOS XE containers, it requires at least 8 MB RAM. When packet capture is to be used, it is limited to 500 MB with flash. If you intend to use packet capture for higher usage, you need to add storage to your ISR with the NIM carrier card for solid-state drives.
Agent on Cisco UCS E-Series Server	The Cisco UCS E-Series Open Virtualization Archive (OVA) is configured to use a 155-GB disk, 5 GB of memory, 4 vCPUs, and ESXi 5.5.
Manager	The manager requires ESXi 5.5 or later with 4 vCPUs, 24 GB RAM, and 200 GB storage. The manager can support up to 1000 agents. For installation of more than 50 agents the recommendation is 64 GB of memory, 16 vCPUs, and 4 TB of storage.

Ordering Information

Part Number	Product Description
L-SW-LN-44-1Y-K9	Cisco Stealthwatch Learning Network License for 4400 Series 1 Yr Term
L-SW-LN-44-3Y-K9	Cisco Stealthwatch Learning Network License for 4400 Series 3 Yr Term
L-SW-LN-43-1Y-K9	Cisco Stealthwatch Learning Network License for 4300 Series 1 Yr Term
L-SW-LN-43-3Y-K9	Cisco Stealthwatch Learning Network License for 4300 Series 3 Yr Term

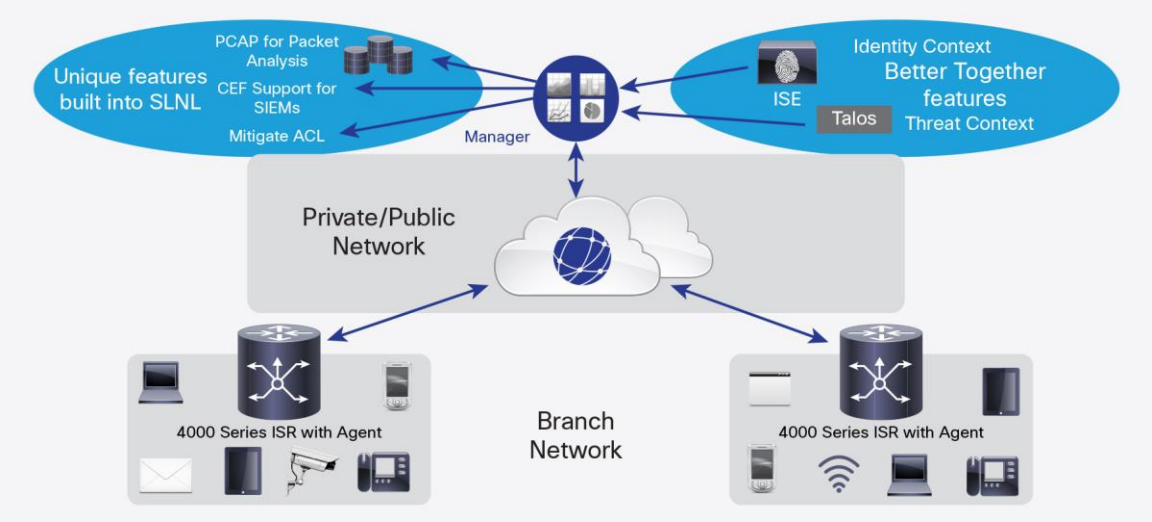
Part Number	Product Description
L-SW-LN-UCS-1Y-K9	Cisco Stealthwatch Learning Network License for UCS Series 1 Yr Term
L-SW-LN-UCS-3Y-K9	Cisco Stealthwatch Learning Network License for UCS Series 1 Yr Term
L-SW-SCA-K9	Cisco Stealthwatch Learning Network Centralized Agent Manager

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Summary: Learning Networks Deployment



For More Information

To learn more about Cisco Stealthwatch Learning Network License, go to http://www.cisco.com/go/stealthwatch.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-737494-02 11/16