Cisco Stealthwatch Learning Network License Safeguards Branch Networks

Gaining network visibility across a branch network, particularly a distributed branch with multiple locations, can be complex as well as costly. The Cisco® Stealthwatch Learning Network License is a cost-effective solution for extending network security to branch and remote networks.

Today's enterprise network is more complex than ever before, and new distributed networks mean new security challenges. The increase in enterprise mobility, the wide availability of commodity Internet access, the growth of the Internet of Things, and other trends have expanded the network attack surface. Securing this complex environment requires visibility into the branch. You need to see traffic flows, applications, users, and devices that are known as well as unknown to determine whether there is anomalous behavior.

A new solution is needed for the branch network that easily enables visibility without affecting network bandwidth. It should require interaction and data movement only when an action needs to be taken. It should deliver packet capture at the network device level for fast incident response and device-level mitigation. And it should make use of Cisco network infrastructure.

Overview

The Cisco Stealthwatch Learning Network License is an extension of Cisco's network as a sensor and network as an enforcer initiatives. You can take advantage of your existing Cisco networking investment by using NetFlow data generated by Cisco devices to improve visibility and security on your network.

Cisco Stealthwatch Learning Network License is an additional network sensor that improves visibility, security, and response across the network branch. It enables and IOS XE Intelligent Application Agent within the Cisco Integrated Security Router (ISR), ISRv, CSRv or Enteperise Network Compute 5400 Series to act as a security sensor. It embeds security anomaly detection into the network element itself, using packet capture along with intelligent detectors to identify, mitigate, and remediate threats. The solution provides visibility without affecting bandwidth and can require interaction and data movement only when an action needs to be taken.

The Learning Network License identifies traffic at the network device level using network behavior, NetFlow, and network-based application recognition to make decisions about, and drop, suspicious packets. Incident response and device-level mitigation are faster.

It extends visibility and security into the branch network without affecting network performance. A web-based tool gives you visibility, control, and the ability to take action across multiple routers on the network from a single interface.

Additional information about traffic flows such as user contextual data, identity, and telemetry can be obtained by using the Cisco Identity Services Engine with Learning Network License. Integration with the Talos threat feed allows the solution to gain real time threat intelligence to make improved decisions about traffic reputation and indicators of compromise.

Benefits

- Improved threat detection with intelligent sensors that monitor branch traffic and that learn to understand specific patterns and policies allowable for traffic at the device level.
- Deeper visibility across the branch and between branches. Granular insight into branch traffic.
- Ability to modify policies based on traffic and packet behavior without affecting network performance.
- Faster incident response with automated threat detection and mitigation. Web-based management console and dashboard that provide a central view across all agents.

Visibility and Automated Threat Detection at the Branch Network

Today's users are demanding to onboard more devices and work from everywhere, and organizations lack the visibility into all this additional traffic. It is also challenging for organizations to detect the anomalous behavior of these devices. Companies continue to merge and acquire others, which means merged IT systems, departments, networks, access, and security policies and tools, which means greater complexity for network traffic flows. This complexity around visibility across the network is compounded by the growth in the Internet of Things (IoT), which will bring billions more devices that will generate even more traffic flows in the near future.

You cannot protect against threats that you cannot see. Visibility into the network is critical to securing the enterprise. Threats continue to become more sophisticated. They are also getting harder to detect while signature- and intelligence-based detections have difficulty keeping pace. A new approach is needed that incorporates threat detection into the network itself and extends this model beyond the network perimeter, to the branch, the public and private cloud, and proxy servers.

Network visibility is even more difficult across a branch network with multiple remote locations. Bandwidth is greatly affected when telemetry is gathered across all network devices. Visibility into the network is also critical at the branch. However, the cost of bandwidth on branch networks as well as the impact to the network when capturing network telemetry makes the challenge of visibility even more complex.

Encryption is important in security. But although you may use encryption to protect data and privacy, attackers useit to conceal malware and evade detection by network security products. Stealthwatch Learning Network License has enhanced analytics capabilities, so you can better understand whether encrypted traffic on the network is malicious., It applies machine learning and statistical modeling for encrypted traffic and pinpoints malicious patterns in encrypted traffic to identify threats and accelerate the appropriate response.

Major Capabilities of the Stealthwatch Learning Network License

The Learning Network License embeds security anomaly detection into the network element, using packet capture and intelligent detectors at the device level for incident response.

Improved Protection Against Branch Network Threats

You can turn your Cisco Integrated Service Router (ISR), ISRv, CSRv or Enteperise Network Compute 5400 Series into a security device, stop the lateral movement of threats between branches, and extend security, all without affecting performance. Intelligent sensors are embedded into the ISR, ISRv, CSRv or Enterprise Network Compute 5400 Series called a Distribute Learning Agent that enable the ability identify potential threat vectors within encrypted traffic flows. This encrypted traffic analytics functionality can give customers cryptographic compliance as well as malware detection within encrypted traffic. This enhanced functionality allows for the inspection of encrypted traffic flows. By inspecting the first packet of traffic, the sequence and length of packet times and the distribution of the packets, suspicious traffic can be flagged. They build policies from traffic patterns, learning and making adjustments over time. This information is reported to a single web-based management console where users can either override or change the intelligent agents, or enable the automated decision making to continue. These intelligent sensors capture and inspect packets by using application recognition and flag potential threats as anomalies. They can then develop policies to prevent suspicious packets or traffic from being shared across the branch network and stop the lateral movement of threats between branches. This localized device protection reduces unnecessary communications across the branch network and thus reduces bandwidth requirements and implementation costs.

Deeper Visibility Across the Branch Network

The Learning Network License enables deeper visibility across the branch network because it allows for the development of branch-specific traffic patterns at the device level. The intelligent agent algorithmically builds policies based on packet behavior. It can drop packets, flag and report anomalies, and modify patterns based on user feedback. The central web-management console gives you deep visibility across all your intelligent agents, across all branches. You gain visibility into the agents, nodes, traffic, and policies at each branch, with metrics like anomalies per day, by severity, the number of applications used, and the number of edges, hosts, and clusters.

Faster Threat Detection and Response

You also reduce your time to detect and mitigate suspicious events at the branch level with Learning Network License. The intelligent sensors use machine learning, Network-Based Application Recognition and NetFlow to process and analyze traffic at the ISR, which can flag or drop suspicious packets at the device and report incidents. Because this analysis happens at the device level, it shortens the time to view and respond to the incident. The web-based management console also speeds time to detection and mitigation. You can see the threat probability of flagged anomalies, review traffic information gathered by each agent, provide feedback with a simple click, and highlight only the events that need attention.

The Cisco Stealthwatch Learning Network License is designed to work on the Cisco ISR 4000 Series. For more information about router configurations and components, visit: http://www.cisco.com/go/stealthwatch.

The Cisco Stealthwatch Learning Network License consists of agents and controllers.

A distributed learning agent is part of the network device operating system. It can also be installed on a module in a device. This agent uses telemetry from the network device to learn about its environment and to determine when conditions require action to protect the device and the network.

Use Cases

Retail	▪ Supports thousands of stores with Internet access ▪ Can deliver security posture assessments per store ▪ Supports the collection of store-level network baseline behavior and identifies non-business-related activities ▪ Identifies individual security anomalies at the store branch level
Financial	▪ Identifies targeted attacks and data exfiltration at the branch level ▪ Enables broad NetFlow analysis across branches ▪ Eases deployment across thousands of branches ▪ Can enable programmed mitigation and quarantine at the branch level
Oil and Gas	▪ Can identify and deny billions of unauthorized access attempts annually ▪ Identifies targeted data exfiltration to protect proprietary data
Any	▪ Uses ISR networking investments by turning the router into a security sensor that can make decisions about traffic directly on the router ▪ Enables a cost-effective solution for extending the network as a sensor or enforcer to branch and remote networks ▪ Extends visibility and security into the branch network without affecting network performance ▪ Provides visibility, control, and the ability to take action across multiple routers on the network from a single management console

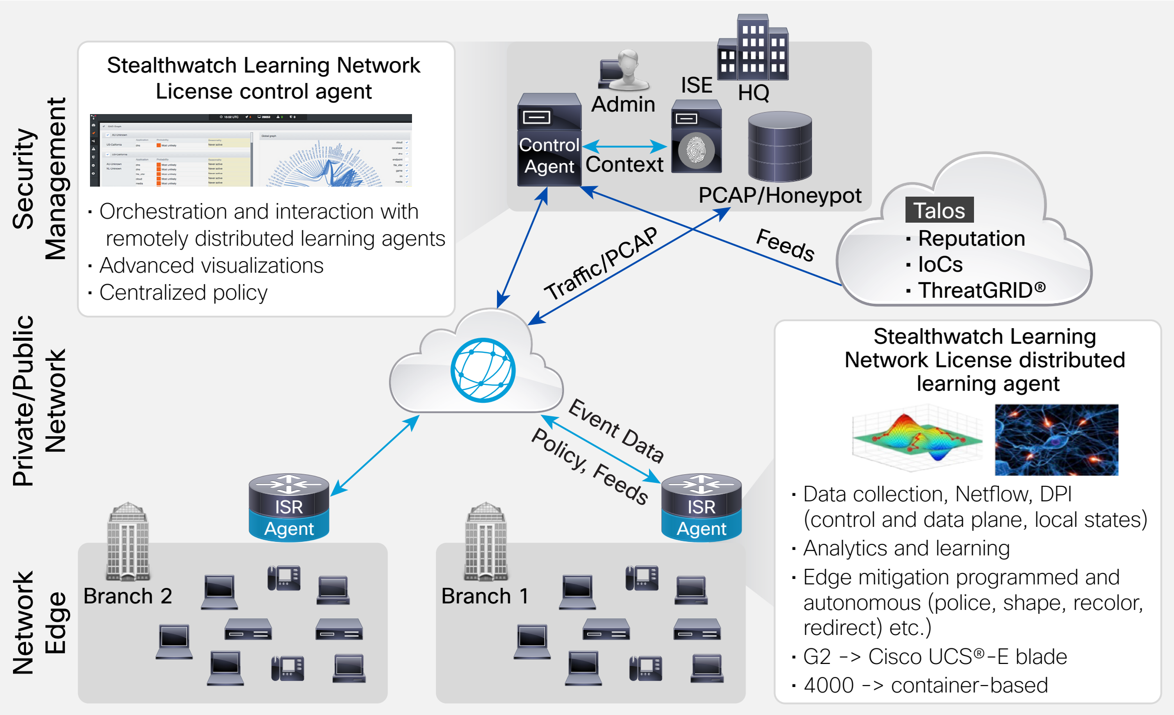
Why Cisco?

Cisco delivers intelligent cybersecurity for the real world, extending security everywhere employees are and data is. Cisco provides one of the industry's most comprehensive advanced threat protection portfolios of solutions that is pervasive, integrated, continuous, and open. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing unmatched visibility, consistent control, and advanced threat protection across the entire attack continuum—before, during, and after an attack.

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.



Stealthwatch Learning Network License control agent

- Orchestration and interaction with remotely distributed learning agents
- Advanced visualizations
- Centralized policy

Talos

- Reputation
- IoCs
- ThreatGRID®

Stealthwatch Learning Network License distributed learning agent

- Data collection, Netflow, DPI (control and data plane, local states)
- Analytics and learning
- Edge mitigation programmed and autonomous (police, shape, recolor, redirect) etc.)
- G2 -> Cisco UCS®-E blade
- 4000 -> container-based

Next Steps

To learn more about the Cisco Stealthwatch Learning Network License, visit http://www.cisco.com/go/stealthwatch or contact your local Cisco account representative.