Cisco Stealthwatch Enterprise

Für UCS-Hardware

Stealthwatch™ Enterprise ist die branchenführende Lösung für Transparenz und Sicherheitsanalysen und nutzt Telemetriedaten des Unternehmens aus der vorhandenen Netzwerkinfrastruktur. Es bietet fortschrittliche Bedrohungserkennung, beschleunigte Reaktion auf Bedrohungen und eine einfachere Netzwerksegmentierung mithilfe von mehrschichtigem maschinellem Lernen und fortschrittlichen Verhaltensmodellen im gesamten erweiterten Netzwerk.

Mit Stealthwatch Enterprise erhalten Sie Echtzeittransparenz, mit der Sie bessere Einblicke in die Aktivitäten in Ihrem Netzwerk bekommen. Diese Transparenz können Sie in die Cloud, in das gesamte Netzwerk, in alle Zweigstellen, in das Rechenzentrum und letztendlich auf allen Endgeräten skalieren.

Das Herzstück von Stealthwatch Enterprise bilden die Flow Rate-Lizenz, der Flow Collector, die Managementkonsole und Flow Sensor. Informationen zu zusätzlichen Funktionen können Sie den nachstehenden einzelnen Datenblättern entnehmen:

- Cisco Stealthwatch Endgerät-Lizenz – verfügbar als Lizenzerweiterung zur Ausweitung der Transparenz auf Geräte von Endbenutzern.
- Cisco Stealthwatch Cloud – verfügbar als Produktangebot für Transparenz und Bedrohungserkennung in Public-Cloud-Infrastrukturen wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform.
- **Threat Intelligence License** – ein globaler Threat-Inteligence-Feed, der durch die branchenführende Threat-Intelligence-Gruppe Cisco Talos unterstützt wird, bietet zusätzlichen Schutz vor Botnets und sonstigen komplexen Angriffen. Der Feed korreliert verdächtige Aktivitäten in der lokalen Netzwerkumgebung mit den Daten zu Tausenden bekannten Command-and-Control-Servern und Kampagnen, um eine Erkennung von hoher Genauigkeit und eine schnellere Reaktion auf Bedrohungen zu ermöglichen. Cisco Talos erkennt täglich 1,5 Millionen spezifische Malware-Stichproben und blockiert 20 Milliarden Bedrohungen.

Systemvorteile

Stealthwatch Enterprise sorgt durch seine einzigartigen Möglichkeiten zur Visualisierung und Analyse des Netzwerkverkehrs für entscheidende Verbesserungen in den folgenden Bereichen:

- Echtzeit-Bedrohungserkennung
- Incident-Response und Forensik
- Netzwerksegmentierung
- Netzwerkleistung und Kapazitätsplanung
- Einhaltung gesetzlicher Bestimmungen

Erforderliche Komponenten des Systems

Flow Rate-Lizenz

Die Flow Rate-Lizenz wird für die Erfassung, Verwaltung und Analyse der Datenstromtelemetrie benötigt und aggregiert Datenströme in der Managementkonsole. Darüber hinaus definiert die Flow Rate-Lizenz das Volumen von Datenströmen, die erfasst werden können, und wird auf der Basis von Datenströmen pro Sekunde (flows per second, fps) lizenziert. Die Lizenzen können beliebig kombiniert werden, um die gewünschte Flow-Kapazität zu erzielen.

Flow Collector

Der Flow Collector nutzt Unternehmenstelemetrie, wie NetFlow, IPFIX und sonstige Typen von Datenstromdaten, aus bestehenden Infrastrukturelementen, wie Routern, Switches, Firewalls, Endgeräten und sonstigen Netzwerkinfrastrukturgeräten. Zusätzlich kann der Flow Collector Telemetriedaten aus Proxy-Datenquellen empfangen und erfassen. Diese können von Global Threat Analytics (vorher Cognitive Threat Analytics), der mehrschichtigen Engine für maschinelles lernen, für umfassende Transparenz des Web- und Netzwerkdatenverkehrs analysiert werden. Darüber hinaus kann Stealthwatch Enterprise mithilfe von Encrypted Traffic Analytics Analysen nutzen, um schädliche Muster in verschlüsseltem Datenverkehr zu erkennen und somit Bedrohungen zu identifizieren und die Reaktion darauf zu beschleunigen. Diese Funktion ist zwar ohne zusätzliche Kosten in das System integriert, muss allerdings im Rahmen der Bereitstellung aktiviert werden.

Die Telemetriedaten werden analysiert, um ein vollständiges Bild der Netzwerkaktivität zu liefern. Dank der Möglichkeit, Daten aus Monaten oder sogar Jahren zu speichern, entsteht ein Prüfpfad, der genutzt werden kann, um forensische Untersuchungen und Compliance-Initiativen zu verbessern. Das Volumen der Telemetriedaten, die aus dem Netzwerk erfasst werden, wird durch die Kapazität der eingesetzten Flow Collectors bestimmt. Es können mehrere Flow Collectors installiert werden. Flow Collectors sind als Hardware-Appliances oder als virtuelle Systeme verfügbar. In Tabelle 1 werden die Vorteile des Flow Collectors aufgeführt.

Tabelle 1. Major Benefits of the Flow Collector

Vorteil	Beschreibung
Erkennung von Bedrohungen	Verarbeitet Proxy-Datensätze und verbindet sie mit Flow-Datensätzen und liefert auf diese Weise Informationen zu Benutzeranwendung und URL für jeden Flow. Anhand dieser Kontextdaten können Bedrohungen leichter identifiziert und die mittlere Zeit bis zur Ermittlung der Ursache („Mean Time to Know“, MTTK) verkürzt werden.
Überwachung von Traffic-Flüssen	Die Traffic-Flüsse von hunderten Netzwerksegmenten werden gleichzeitig überwacht, sodass verdächtiges Verhalten schnell erkannt werden kann. Diese Funktion ist besonders für die umfangreichen Netzwerke von Großunternehmen wertvoll.
Langfristige Datenaufbewahrung	Ermöglicht die Speicherung großer Datenmengen über lange Zeiträume hinweg.
Skalierbarkeit	Bietet hohe Leistung in Hochgeschwindigkeitsumgebungen und kann unabhängig von der Größe jeden Bereich des Netzwerks schützen, der per IP erreichbar ist.
Deduplizierung und Zusammenführung	Durch Deduplizierung werden alle Flows, die mehr als einen Router passiert haben, nur einmal gezählt. Die Flow-Informationen werden dann zusammengeführt, sodass ein transparenter Überblick über alle Netzwerktransaktionen entsteht.
Zahlreiche Bereitstellungsoptionen	Die Appliance Edition bietet eine skalierbare Lösung für Unternehmen jeder Größe. Alternativ dazu steht die Virtual Edition zur Verfügung. Diese umfasst dieselben Funktionen wie die Appliance Edition, wird jedoch in einer VMware-Umgebung bereitgestellt. Diese Lösung lässt sich entsprechend den ihr zugewiesenen Ressourcen dynamisch skalieren.

* Die maximale Anzahl der Flows pro Sekunde kann je nach Netzwerkbedingungen variieren.

Flow Collector-Spezifikationen

- Stealthwatch Flow Collector 4200 – Teilenummer: ST-FC4200-K9
- Stealthwatch Flow Collector 5200 – Teilenummer: ST-FC5200-K9
- Stealthwatch Flow Collector Virtual Edition kann als FCVE-1000, FCVE-2000 oder FCVE-4000 konfiguriert werden – Teilenummer: L-ST-FC-VE-K9

Hinweis: Diese Spezifikationen gelten für Stealthwatch ab Systemversion 6.9.1

Managementkonsole

Die Stealthwatch Managementkonsole aggregiert, organisiert und präsentiert Analysen von bis zu 25 Flow Collectors, der Cisco Identity Services Engine und anderen Quellen. Die Konsole bietet eine grafische Darstellung von Netzwerkverkehr, Identitätsinformationen, benutzerdefinierte zusammenfassende Berichte und integrierte Sicherheits- und Netzwerkinformationen für umfassende Analysen.

Die Kapazität der Konsole bestimmt die Menge der Telemetriedaten, die analysiert und dargestellt werden können, sowie die Anzahl der bereitgestellten Flow Collectors. Die Konsole ist als Hardware-Appliance oder als virtuelles System verfügbar. In Tabelle 2 werden die Vorteile der Konsolen aufgezählt.

Tabelle 2. Major Benefits of the Management Console

Vorteil	Beschreibung
Minutengenaue Echtzeitdaten	Liefert Flow-Daten, mit deren Hilfe der Datenverkehr in Hunderten von Netzwerksegmenten gleichzeitig überwacht und verdächtiges Verhalten somit schneller erkannt werden kann. Diese Funktion ist besonders für die umfangreichen Netzwerke von Großunternehmen wertvoll.
Erkennung und Priorisierung von Bedrohungen	Bedrohungen können schnell erkannt und priorisiert, Netzwerkmissbrauch und Leistungsprobleme identifiziert und die Reaktion auf Ereignisse unternehmensweit verwaltet werden – all das über ein zentrales Kontrollzentrum.
Verwaltung von Appliances	Übernimmt die Konfiguration, Koordination und Verwaltung von Cisco Stealthwatch Appliances wie Flow Collector, Flow Sensor und UDP Director.
Nutzung verschiedener Typen von Flow-Daten	Das System nutzt verschiedene Typen von Flow-Daten, darunter NetFlow, Internet Protocol Flow Information Export (IPFIX) und sFlow und ermöglicht so einen kosteneffizienten, verhaltensbasierten Netzwerkschutz.
Skalierbarkeit	Erfüllt die Anforderungen selbst umfangreichster Netzwerkumgebungen. Bietet hohe Leistung in Hochgeschwindigkeitsumgebungen und kann unabhängig von der Größe jeden Bereich des Netzwerks schützen, der per IP erreichbar ist.
Prüfpfade für Netzwerktransaktionen	Ein umfassender Prüfpfad für alle Netzwerktransaktionen ermöglicht effektivere forensische Untersuchungen.
Individuelle Erstellung von Echtzeit-Flow-Maps	Grafische Ansichten bieten einen Überblick über den aktuellen Status des Datenverkehrs des Unternehmens. Administratoren können nach beliebigen Kriterien, z. B. Standort, Funktionsbereich oder virtuelle Umgebung, Karten des Netzwerks erstellen und durch Verbinden von zwei Hostgruppen darauf den Datenverkehr zwischen diesen schnell analysieren. Durch Auswahl eines entsprechenden Datenpunkts sind dann noch tiefergehende Einblicke in die aktuellen Vorgänge möglich.
Flexible Implementierungsoptionen	Sie können die physische Appliance bestellen, ein skalierbares Gerät, das sich für Organisationen aller Größenordnungen eignet. Alternativ dazu steht die Virtual Edition zur Verfügung. Diese umfasst die gleichen Funktionen wie die Appliance Edition, wird jedoch in einer VMware-Umgebung bereitgestellt.

Spezifikationen der Managementkonsole

- Stealthwatch Managementkonsole 2200 – Teilenummer: ST-SMC2200-K9
- Die Virtual Edition der Stealthwatch Managementkonsole kann als SMC VE oder SMC VE 2000 konfiguriert werden – Teilenummer: L-ST-SMC-VE-K9

Hinweis: Diese Spezifikationen gelten für Stealthwatch ab Systemversion 6.9.1

Optionale Komponenten des Systems

Flow Sensor

Der Flow Sensor ist eine optionale Komponente von Stealthwatch Enterprise und erzeugt Telemetriedaten für Segmente der Switching- und Routing-Infrastruktur, die keine nativen NetFlow-Daten erzeugen können. Darüber hinaus bietet er Einblicke in Daten der Anwendungsschicht. Neben allen Telemetriedaten, die von Stealthwatch erfasst werden, liefert der Flow Sensor einen zusätzlichen Sicherheitskontext zur Verbesserung der Sicherheitsanalysen von Stealthwatch. Umfassende Verhaltensmodelle und Cloud-basiertes mehrschichtiges maschinelles Lernen werden auf diesen Datensatz angewendet, um fortschrittliche Bedrohungen zu erkennen und schnellere Untersuchungen durchzuführen.

Der Flow-Sensor wird auf einem gespiegelten Port oder Netzwerk-Tap installiert und erzeugt Telemetriedaten basierend auf dem beobachteten Datenverkehr. Das Volumen der Telemetriedaten, die aus dem Netzwerk generiert werden, wird durch die Kapazität der eingesetzten Flow Sensors bestimmt. Es können mehrere Flow Sensors installiert werden. Flow Sensors dienen zur Überwachung von Umgebungen mit virtuellen Systemen und sind als Hardware-Appliances oder als virtuelle Appliances verfügbar. Die Komponente kann auch in Umgebungen eingesetzt werden, in denen eine Overlay-Monitoring-Lösung, die einen zusätzlichen Sicherheitskontext benötigt, besser zum Betriebsmodell der IT-Abteilung passt.

In Tabelle 3 werden die wichtigsten Vorteile des Flow Sensors aufgezählt.

Tabelle 3. Wichtigste Vorteile des Flow Sensors

Vorteil	Beschreibung
Layer-7-Anwendungstransparenz	Bietet echte Layer-7-Anwendungstransparenz durch die Erfassung von Anwendungsinformationen und Ad-hoc-Paketerfassung (PCAP) auf Anforderung. Dies umfasst datenorientierte Funktionen wie RTT (Round Trip Time), SRT (Reaktionszeit des Servers), erneute Übertragungen.
Leistung und Analyse auf Paketebene	Bietet echte Layer-7-Anwendungstransparenz durch die Erfassung von Anwendungsinformationen und Ad-hoc-Paketerfassung (PCAP) auf Anforderung. Dies umfasst datenorientierte Funktionen wie RTT (Round Trip Time), SRT (Reaktionszeit des Servers), erneute Übertragungen.
Warnungen bei Netzwerkanomalien	Zusätzliche Telemetriedaten des Flow Sensors, z. B. URL-Informationen für Web-Datenverkehr und Details zu TCP-Flags, helfen mit kontextbezogenen Informationen bei der Erzeugung von Alarmen, damit das Sicherheitspersonal schnell Maßnahmen ergreifen und die Schäden eingrenzen kann.
Niedrigere Kosten	Durch die Identifikation und Isolierung der Ursache eines Problems oder Vorfalls innerhalb von Sekunden werden die Betriebseffizienz gesteigert und Kosten gesenkt.
Zahlreiche Bereitstellungsoptionen	Die Appliance Edition bietet eine skalierbare Lösung für Unternehmen jeder Größe. Alternativ dazu steht die Virtual Edition zur Verfügung. Diese umfasst die gleichen Funktionen wie die Appliance Edition, wird jedoch in einer VMware- oder KVM Hypervisor-Umgebung bereitgestellt.

* Diese Zahlen werden in unseren Testumgebungen anhand durchschnittlicher Kundendaten erzeugt.

Flow Sensor-Spezifikationen

- Stealthwatch Flow Sensor 1200 – Teilenummer: ST-FS1200-K9
- Stealthwatch Flow Sensor 2200 – Teilenummer: ST-FS2200-K9
- Stealthwatch Flow Sensor 3200 – Teilenummer: ST-FS3200-K9
- Stealthwatch Flow Sensor 4200 – Teilenummer: ST-FS4200-K9
- Stealthwatch Flow Sensor Virtual Edition – Teilenummer: L-ST-FS-VE-K9

Hinweis: Diese Spezifikationen gelten für Cisco Stealthwatch ab Version 6.9.1

UDP Director

UDP Director vereinfacht die unternehmensweite Erfassung und Verteilung von Netzwerk- und Sicherheitsdaten und entlastet zudem die Verarbeitungskapazitäten von Netzwerkroutern und -switches. Möglich wird dies, indem die erfassten Netzwerk- und Sicherheitsinformationen in einem einzigen Datenstrom zusammengefasst und dann an ein oder mehrere Ziele weitergeleitet werden. In Tabelle 4 werden die wichtigsten Vorteile von UDP Director aufgezählt.

Tabelle 4. Wichtigste Vorteile von UDP Director

Vorteil	Beschreibung
Weniger ungeplante Ausfallzeiten und Serviceunterbrechungen	Hochverfügbarkeit von UDP Director ist auf der UDP Director 2200-Appliance verfügbar.
Vereinfachte Absicherung und Überwachung des Netzwerks	UDP Director bildet das Standardziel, in dem alle Syslog-, NetFlow- und SNMP-Informationen (Simple Network Management Protocol) aggregiert werden. Die UDP Director-Appliances empfangen Daten von jeder beliebigen verbindungslosen UDP-Anwendung und übertragen diese dann an verschiedene Ziele, wobei die Daten bei Bedarf dupliziert werden.
Weiterleitung von UDP-Daten von jeder Quelle an beliebige Ziele	Von jeder beliebigen verbindungslosen UDP-Anwendung werden die Daten erfasst und an verschiedene Ziele weitergeleitet, wobei die Daten bei Bedarf dupliziert werden.
Keine Neukonfiguration der Infrastruktur erforderlich	Punkt-Protokolldaten (NetFlow, sFlow, SNMP, Syslog) werden an ein einzelnes Ziel geleitet, ohne dass die Infrastruktur neu konfiguriert werden muss, wenn neue Tools hinzugefügt oder bestehende entfernt werden.

Spezifikationen von UDP Director

- Stealthwatch UDP Director 2200 – Teilenummer: ST-UDP2200-K9
- Cisco Stealthwatch UDP Director Virtual Edition – Teilenummer: L-ST-UDP-VE-K9

Bestellinformationen

In der Bestellanleitung für das Cisco Stealthwatch-System werden die verfügbaren Modelle, Komponenten und Lizenztypen näher beschrieben. Wenden Sie sich an Ihren Ansprechpartner, wenn Sie eine Bestellung aufgeben möchten.

Service und Support

Für das Cisco Stealthwatch-System sind zahlreiche Serviceprogramme verfügbar. Mit diesen Services sorgen Sie für umfassenden Schutz für Ihre Netzwerkinvestitionen, optimieren den Netzwerkbetrieb und bereiten Ihr Netzwerk auf die Integration neuer Anwendungen vor. Gleichzeitig erweitern Sie die Intelligenz Ihres Netzwerks und rüsten Ihr Unternehmen für zukünftige Herausforderungen. Weitere Informationen zu den Professional Services finden Sie auf der Seite des technischen Supports.

Cisco Capital

Mit der Cisco Capital®-Finanzierung können Sie die Technologien erwerben, die Sie benötigen, um Ihre geschäftlichen Ziele umzusetzen und wettbewerbsfähig zu bleiben. Mit unserer Unterstützung senken Sie Ihre Kapitalausgaben, Beschleunigen Sie Ihr Unternehmenswachstum. und optimieren Ihre Investitionen und Ihren ROI. Mit der Cisco Capital-Finanzierung sind Sie flexibel beim Erwerb von Hardware, Software, Services und zusätzlichen Drittanbietergeräten – und dies alles mit nur einer einzigen planbaren Zahlung. Cisco Capital ist in mehr als 100 Ländern verfügbar. Mehr dazu hier.

Weitere Informationen

Weitere Informationen über Cisco Stealthwatch finden Sie unter https://www.cisco.com/go/stealthwatch. Wenden Sie sich alternativ an Ihren Cisco Security-Kundenbetreuer, wenn Sie erfahren möchten, wie Ihre Organisation Transparenz im gesamten erweiterten Netzwerk erhalten kann, indem Sie an einer kostenlosen Stealthwatch-Transparenzbewertung teilnehmen.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Gedruckt in den USA C78-739398-03 04/18