Vergleich von Sicherheitsanalyselösungen

Erfahren Sie, wie Cisco Stealthwatch im Vergleich mit anderen Sicherheitsanalyseprodukten abschneidet. Die Lösung ist problemlos skalierbar und bietet Ihnen Transparenz im gesamten Netzwerk. Stealthwatch erkennt und reagiert auf komplexe Bedrohungen in Echtzeit mithilfe von maschinellem Lernen und Entitätsmodellierung.

Siehe Stealthwatch

	Cisco Stealthwatch	Darktrace	Plixer
Erkennung			
Malware-Analyse und -Erkennung in verschlüsseltem Datenverkehr	✓ Analyse von verschlüsseltem Datenverkehr	✗ Malware-Analyse und -Erkennung in verschlüsseltem Datenverkehr	✗ Malware-Analyse und -Erkennung in verschlüsseltem Datenverkehr
Erkennung von Data Hoarding	✓ Ereignisse werden im Data-Hoarding-Index gesammelt, der entweder ein absolutes Limit misst oder sich am gelernten Verhalten des Hosts oder der Gruppen orientiert.	Begrenzt Kann Anomalien, aber keine spezifischen Data-Hoarding-Ereignisse erkennen.	✗
Erkennung von lateralen Bewegungen	✓ Bietet Wurm-Erkennung und visuelle Verfolgung von Malware im gesamten Netzwerk.	Begrenzt Erkennt möglicherweise Anomalien, hat aber keine veröffentlichte Fähigkeit zum speziellen Aufdecken lateraler Bewegungen.	✗
Vollständiger Prüfpfad	✓ Kann jede Konversation im Netzwerk mit Flow Collectors und Flow-Sensoren protokollieren.	Begrenzt Nutzt nur Softwaresensoren, Teile des Datenverkehrs entgehen der Lösung vermutlich.	✓ Flow-Datenverkehr wird in Box gespeichert
Erkennung von Reconnaissance-Aktivitäten	✓ Kann schnelles und langsames Scannen mit einem einzigartigen Algorithmus erkennen, der auf sehr niedrige Scan-Raten sensibilisiert ist.	Begrenzt Erkennt Reconnaissance-Aktivitäten, ist aber wahrscheinlich nicht so empfindlich wie der einzigartige Scan-Algorithmus von Stealthwatch eingestellt.	✓ Mit optionaler Flow-Analyse
Maschinelles Lernen	✓ Nutzt mehrschichtiges maschinelles Lernen für Erkennung mit hoher Genauigkeit.	✓	Begrenzt Bietet begrenzte Baselining-Funktionen basierend auf umfassenden Datenverkehrserhebungen

	Cisco Stealthwatch	Darktrace	Plixer
Erkennung (Fortsetzung)			
Erkennung von Datendiebstahl	✓ Generiert einen Warnung bei vermutlichem Datenverlust für Hosts die mehr Daten (einschließlich verschlüsselten Daten) als üblich herausschleusen.	Begrenzt Verwendet nur Sensoren anstelle von Telemetriedaten aus der Netzwerk-Hardware und die Erkennung beschränkt sich auf die Sensorplatzierungen.	✗
Command-and-Control-Erkennung	✓ Erkennt mehrere Sicherheitsereignisse mithilfe von Analysen und Threat Intelligence zur Erkennung von C-&-C-Peers.	Begrenzt Verwendet nur Sensoren anstelle von Telemetriedaten aus dem Netzwerk und die Erkennung beschränkt sich auf Sensorplatzierungen.	Begrenzt Keine spezifischen Algorithmen für C & C
Anomalieerkennung	✓ Verfügt über ein ausgereiftes und bewährtes Anomalieerkennungssystem mit mehr als 150 Algorithmen.	Begrenzt Verwendet nur Sensoren anstelle von Telemetriedaten aus dem Netzwerk und die Erkennung beschränkt sich auf Sensorplatzierungen.	Begrenzt Mit optionaler Flow-Analyse
Malware-Erkennung	✓ Bietet Erkennung von Zero-Day-Angriffen.	Begrenzt Verwendet nur Sensoren anstelle von Telemetriedaten aus dem Netzwerk und die Erkennung beschränkt sich auf Sensorplatzierungen.	Begrenzt Mit optionaler Flow-Analyse
Bereitstellung			
Skalierbarkeit	✓ Kann auf 6 Millionen Flows pro Sekunde skalieren, Schnittstellenverbindungen von 100 Mbit/s bis 10 Gbit/s sowie Spitzen im Datenverkehr über Nennleistungsniveau bewältigen und Telemetriedaten von Tausenden Sensoren sammeln.	Begrenzt Nutzt nur Sensoren anstelle von Netzwerktelemetrie.	Begrenzt Zur Erstellung von konsolidierten Berichten und Flow Maps über mehrere Plixer Collectors sind erhebliche Konfigurations- und Anpassungsanstrengungen erforderlich.
Datenspeicherung	✓ Im Durchschnitt kann das System Flow-Daten von 30 bis 45 Tagen und oft noch viel mehr für tiefere forensische Untersuchungen speichern.	Begrenzt Keine Datenberichte zur Bestätigung der Storage-Funktionen	✓
Erkennung von Zero-Day-Angriffen	✓ Kann mithilfe eines verhaltensbasierten Verfahrens mit mehr als 90 Parametern neue oder einzigartige Malware erkennen, für die Signaturen noch nicht vorhanden sind.	✓ Verwendet nur Sensoren anstelle von Telemetriedaten aus dem Netzwerk und die Erkennung beschränkt sich auf Sensorplatzierungen.	Begrenzt Bietet begrenzte Baselining-Funktionen basierend auf umfassenden Datenverkehrserhebungen

	Cisco Stealthwatch	Darktrace	Plixer
Bereitstellung (Fortsetzung)			
Datenkomprimierung	✓ Nach Empfang der Flows auf dem Collector werden sie in bidirektionale, speicherresidente Flows synthetisiert. Dadurch reduziert sich die Zahl falsch-positiver Meldungen und es werden eine effiziente Datenspeicherung sowie präzise Berichte zur Host-Ebene ermöglicht.	**Nicht zutreffend** Nutzt nur Sensoren anstelle von Telemetriedaten aus dem Netzwerk.	**Begrenzt** Einige Informationen werden nicht berücksichtigt.
Bereitstellungsmodell	**Siehe Hinweis** Die Bereitstellung von Sensoren oder teuren Sonden ist nicht erforderlich. Die Telemetriedaten können zur Analyse des Netzwerkverkehrs einfach über Netzwerkgeräte aktiviert werden.	**Siehe Hinweis** Kunden müssen Sensoren erwerben und Links zur Überwachung bestimmen, anstatt einfach die Telemetriedaten über Netzwerkgeräte zu aktivieren, um alle Konversationen zu erhalten. Das Model ist kostspielig und schwer zu skalieren.	**Siehe Hinweis** Kann die meisten Flow-basierten Telemetriequellen nutzen.
Transparenz an Endpunkten	✓ Mit Cisco AnyConnect 4.2 oder höher erfasst die Endpunkt-Datenlizenz Endpunkt-Telemetriedaten über das Cisco Network Visibility Flow (NvzFlow)-Protokoll.	✗	✗ Es fehlen Funktionen wie Passworteinrichtung, Konfigurationsvoreinstellungen für NAD-Typen und TACACS+-Proxy.
Cloud-Transparenz	✓ Kann die Public-Cloud über die SaaS-basierte Stealthwatch Cloud-Lösung überwachen.	**Begrenzt** Nutzt Sensoren zur Überwachung des Private-Cloud-Netzwerks und einen Cloud Connector für bestimmte Anwendungen.	**Begrenzt** Das System nutzt Amazon AWS-Protokolle, die Flows ähneln und Aktionen genehmigen und verweigern.
Datenexport	**Siehe Hinweis** Verfügt über Integrationen mit Sicherheitsinformationssystemen und bietet APIs für individuelle Integration. Unterstützt auch SOAP und REST-APIs.	**Siehe Hinweis** Hat einen Splunk-Anschluss, der JSON-Syslog-Input von einer Darktrace-Appliance zieht und Sicherheitsvorfälle auf Splunk anzeigt; verknüpft diese mit den Berichten im Darktrace Threat Visualizer.	**Siehe Hinweis** Unterstützt die REST-API und Protokollausgabe.
Warnmeldungen	**Siehe Hinweis** Bietet E-Mail- oder Syslog-Export ins SIEM-System, ins Netcool- und Remedy-Ticketsystem usw. mit E-Mail-, SNMP- und Syslog-Benachrichtigungen.	**Siehe Hinweis** Bietet formatierte Syslog-Ausgabe.	**Siehe Hinweis** Bietet ausgehende Protokollierung und Warnmeldungen.

	Cisco Stealthwatch	Darktrace	Plixer
Nachforschungen			
Vollständige investigative Workflows	✓ Kann langanhaltende Sicherheitsereignisse untersuchen. Generiert kontextbasierte und benutzerdefinierte Warnungen, verbindet Benutzername mit IP-Adresse, überwacht Schnittstellennutzung, führt Deep Packet Inspection durch und protokolliert jede Art der Netzwerkkommunikation.	**Begrenzt** Klassifiziert die erkannte Bedrohung und visualisiert sie im Threat Visualizer.	**Begrenzt** Es fehlen anpassbare Schnittstellen, schnelle Trendanzeige historischer Daten, automatisierte Beseitigung von Malware und Ursachenanalysetools.
Effektivität für Geschäftskunden	✓ Vereinfacht die Segmentierung durch logische Erstellung von Host-Gruppen zum Ordnen von Benutzern nach Standort, IP-Adresse, Funktion usw. Bietet benutzerdefinierte Benachrichtigungsdetails und Formate mit Alarmquittierung.	**Begrenzt** Verwendet nur Sensoren anstelle von Telemetriedaten aus dem Netzwerk, sodass die Skalierung für Unternehmen schwierig ist.	**Begrenzt** Zur Erstellung von konsolidierten Berichten und Flow Maps über mehrere Plixer Collectors sind erhebliche Konfigurations- und Anpassungsanstrengungen erforderlich.
Flexibles Abfrage- und Filtersystem	✓ Alle erfassten Felder können abgefragt werden. Erweiterte Suche ist für verschlüsselten Datenverkehr für verschlüsselten Schlüsselaustausch, Verschlüsselungsalgorithmus, Schlüssellänge, TLS/SSL-Version usw. verfügbar.	**Nicht zutreffend** Keine Vergleichsinformationen in veröffentlichten Materialien verfügbar	**Begrenzt** Es fehlen anpassbare Schnittstellen, schnelle Trendanzeige historischer Daten, automatisierte Beseitigung von Malware und Ursachenanalysetools.
Cyberthreat-Dashboard	**Siehe Hinweis** Bietet relevante Informationen für SecOps-Mitarbeiter, z. B. in welche Indizes Warnungen eingepflegt werden, welche Warnungen aktiviert sind, für welche Hosts die meisten Warnmeldungen generiert werden usw. Darüber hinaus besteht die Möglichkeit, weitere Details und zugehörige Telemetriedaten zu erhalten.	**Siehe Hinweis** In erster Linie ein Sicherheitstool mit auf die SecOps konzentriertem Arbeitsbereich	**Siehe Hinweis** Dashboard-basiert für Sicherheit und Netzwerküberwachung
Visualisierung und Zuordnung	**Siehe Hinweis** Generiert automatische Karten wie Wurmausbreitungspfade und benutzerdefinierte Beziehungskarten zur Visualisierung jeder beliebigen Host-Gruppe und deren Kommunikation mit anderen Gruppen.	**Siehe Hinweis** Stark grafikorientiert	**Siehe Hinweis** Einfache Grafiken und Diagramme
Aufklärung von Vorfällen	**Siehe Hinweis** Die Benutzeroberfläche ist nach rollenbasierten Workflows gestaltet, damit die Administratoren sofort zu den Ursachen und entsprechenden Informationen gelangen.	**Siehe Hinweis** Verfügt über einen Threat Visualizer für Transparenz und den Umgang mit Bedrohungen.	**Siehe Hinweis** Investigative Workflows stehen zur Verfügung.

	Cisco Stealthwatch	Darktrace	Plixer
Kontext			
Umfassende kontextbezogene Datenfunktionen	✓ Integriert in Cisco Identity Services Engine (ISE). Ermöglicht das Aufrufen von Host-Informationen wie Benutzer-ID, MAC-Adresse, Gerätetyp und Switch-Port. Erfordert keine separate Abfrage für den zugeordneten Benutzer, da die Benutzer-ID geschrieben werden kann.	Begrenzt Integration von Active Directory für Benutzerdaten	Begrenzt Bietet Sensoren mit Fokus auf einer Vielzahl von Daten, einschließlich der Anwendungsleistung und tiefen DNS-Einblicken.
Identitätsdaten	✓ Integration mit Cisco ISE, Cisco ASA-Produkten (NSEL), DHCP-/ RADIUS-Servern und Active Directory-Authentifizierungs-Servern für die Korrelation der Identität zu Telemetrie.	Begrenzt Integration von Active Directory für Benutzerdaten	Begrenzt Integration mit Active Directory
Anbieterintegration für Routing und Switching	✓ Router, Switches, Firewalls und Wireless-Controller sind die primären Datenquellen. Kann viele Versionen von Telemetrie- und NetFlow-Daten von mehreren Anbietern nativ analysieren, z. B. IPFIX und sFlow sowie andere Layer-7-Protokolle.	✗ Nutzt nur Sensoren anstelle von Telemetriedaten aus dem Netzwerk. Erfordert SPAN oder TAP für jeden überwachten Link und ist beschränkt auf den jeweiligen Link.	
URL-Datenerfassung	Siehe Hinweis Flow-Sensoren können URL-Daten extrahieren, die von den Flow-Collectors und dem Management Center verwendet werden. URL-Daten können auf Basis von Operatoren abgefragt werden. Cisco Security Packet Analyzer zum Herunterladen präziser Datagramme, die den Datenfluss im PCAP-Format darstellen, ist ebenfalls integriert.	Siehe Hinweis Vollständig sensorbasiert und Einblick in Paketdaten	Siehe Hinweis Kann URL-Daten mit Sensoren erfassen.

	Cisco Stealthwatch	Darktrace	Plixer
Kontext (Fortsetzung)			
NetFlow-Generierung für VMware-Umgebungen	✓ Verwendet die NetFlow-Exportfunktion virtueller Switches oder virtueller Flow-Sensoren.	**Nicht zutreffend** Nicht zutreffend, da zur Protokollierung von Datenverkehr Sensoren verwendet werden.	✓ Kann die NetFlow-Telemetriedaten von VMware nutzen.
Sammlung von Anwendungs- und L7-Flow-Daten	✓ Hält den Flow-Zustand aufrecht (aktiv, inaktiv oder laufend), generiert NetFlow-Informationen basierend auf SPAN-Port-Überwachung oder TAPs, verfügt über Proxy-Integration und bietet Anwendungsidentität für mehrere Anbieter wie Palo Alto Networks und L7 Defense und nutzt NBAR sowie NBAR2 mit dem Flow-Sensor.	✓ Nutzt Sonden, die diese Daten direkt von Rohpaketen analysieren.	**Begrenzt** Kann Firewall-Daten, Flow-Daten aus einem SPAN mit Sensor und App-IDs von einem Sensor oder einer Firewall empfangen. Keine NBAR-Unterstützung oder Proxy-Integration.
Vollständige Paketerfassung	✓ Integration mit dem Cisco Security Packet Analyzer, einem auf einem SPAN oder TAP installierten Tool, das einen Ringpuffer an Datagrammen auf einem Segment verwaltet und die Möglichkeit bietet, genaue Datagramme herunterzuladen, die die Telemetrie im PCAP-Format und sogar die im PCAP enthaltenen Dateien darstellt. Mit dem Tool lässt sich auch die Paketentschlüsselung starten, sodass keine andere App heruntergeladen werden muss.	**Unbekannt** Keine Vergleichsinformationen in veröffentlichten Materialien verfügbar	✗ Keine Möglichkeit für vollständige Paketerfassung
Analyse verschlüsselter Daten	✓ Nutzt Encrypted Traffic Analytics oder erweiterte Telemetrie aus dem Cisco-Netzwerk zur Erkennung von Malware und zur Gewährleistung von Crypto Compliance. Stealthwatch analysiert verschlüsselten Datenverkehr mithilfe von erweitertem maschinellem Lernen und Global Threat Intelligence.	**Begrenzt** Könnte einige ungewöhnliche Verhaltensweisen in verschlüsseltem Datenverkehr erkennen.	✗ Keine Möglichkeit zur Analyse von verschlüsseltem Datenverkehr
Unternehmensweite Rufbewertung	✓ Erstellt indexbasierte Bewertungen für jeden Host, bei dem ungewöhnliche Aktivitäten von einem Host stattfinden.	**Unbekannt** Das Anomalieerkennungsmodell könnte einen globalen Bewertungsmechanismus nutzen.	✗ Kein Ansatz zur Sicherheitsindizierung, löst nur reine Warnmeldungen aus.

	Cisco Stealthwatch	Darktrace	Plixer
Threat Intelligence			
Threat-Intelligence-Feed	✓ Stealthwatch Threat Intelligence License und Global Risk Map unterstützt durch Talos ist ein Threat-Feed aus verschiedenen Quellen, der mindestens einmal pro Stunde aktualisiert wird. Ziel ist es, keine einzige falsch-positive Information zu liefern.	✓ Ein Threat Feed mit einer Liste bekannter schädlicher Websites ist verfügbar.	✗ Gewisse Angriffe sollen erkannt werden, es ist aber unklar in welchem Umfang.
Erkennung von Datendiebstahl	✓ Kann interne Bedrohungen wie Datendiebstahl und Command-and-Control-Kommunikation sowie lange und langsame Angriffe erkennen. Sicherheitsereignisse werden an die Indizes geleitet, um durch verhaltensbasierte Algorithmen und absoluten Grenzen, die durch den Betreiber festgelegt werden können, Warnungen auszulösen.	✓ Nicht vorhanden, obwohl Plixer über eine DNS-ausgelegte Appliance zur Erkennung von DNS-Probleme verfügt.	✗
Freigabe von Threat Intelligence.	✓ Daten von Stealthwatch Threat Intelligence werden durch Cisco Talos und umgekehrt verwendet. Cisco tauscht Daten mit Hunderten von Partnern, Kunden und Anbietern über die Aegis-, Crete- und Aspis-Programme aus und ist Mitglied der Cyber Threat Alliance.	✗	✗