



Compare Security Analytics Solutions

Learn how Cisco Stealthwatch compares with other security analytics products. This solution scales easily, giving you visibility across the entire network. Stealthwatch can detect and respond to advanced threats in real time using machine learning and entity modeling.





[See Stealthwatch](#)

	Cisco Stealthwatch	Darktrace	Plixer
Detection			
Malware analysis and detection in encrypted traffic	 Uses Encrypted Traffic Analytics	 Malware analysis and detection in encrypted traffic	 Malware analysis and detection in encrypted traffic
Data hoarding detection	 Events accumulate in the Data Hoarding Index, which is metered either by an absolute limit or by learned behavior of the host or groups.	 Can detect an anomaly but not a specific data hoarding event	
Lateral movement detection	 Provides worm detection and visual tracking of malware across the network	 May detect an anomaly but has no published ability to specifically call out lateral movement	
Complete network audit trail	 Can log every conversation on the network using Flow Collectors and Flow Sensors	 Uses sensors only, so is likely to miss some traffic	 Flow traffic stored on box
Reconnaissance detection	 Can detect fast and slow scanning using a unique algorithm that is highly sensitive to very low scan-rate events	 Can detect reconnaissance, but not likely to be as sensitive as Stealthwatch's unique scan algorithm	 With optional Flow Analytics
Machine learning	 Uses multilayer machine learning to provide high-fidelity detection		 Has limited baselining capabilities based on broad traffic counts

	Cisco Stealthwatch	Darktrace	Plixer
Detection (continued)			
Exfiltration detection	<p>✓</p> <p>Generates a “suspect data loss” alarm for hosts exfiltrating more data (including encrypted data) than normal</p>	<p>Limited</p> <p>Uses only sensors rather than telemetry from network hardware, and detection is limited to sensor-placement locations</p>	<p>✗</p>
Command-and-control detection	<p>✓</p> <p>Can detect multiple security events using analytics and threat intelligence to detect C&C peers</p>	<p>Limited</p> <p>Uses only sensors rather than telemetry from the network, and detection is limited to sensor-placement locations</p>	<p>Limited</p> <p>No specific algorithms for C&C</p>
Anomaly detection	<p>✓</p> <p>Has a mature and proven anomaly detection system with more than 150 algorithms</p>	<p>Limited</p> <p>Uses only sensors rather than telemetry from the network, and detection is limited to sensor-placement locations</p>	<p>Limited</p> <p>With optional Flow Analytics</p>
Malware detection	<p>✓</p> <p>Can provide zero-day exploit detection</p>	<p>Limited</p> <p>Uses only sensors rather than telemetry from the network, and detection is limited to sensor-placement locations</p>	<p>Limited</p> <p>With optional Flow Analytics</p>
Deployment			
Scalability	<p>✓</p> <p>Can scale to 6 million flows per second, handle 100 Mbps to 10 Gbps interface connections, spikes in traffic above rated levels, and can collect telemetry from thousands of sensors</p>	<p>Limited</p> <p>Uses only sensors rather than telemetry from network</p>	<p>Limited</p> <p>Significant configuration and customization is required to support consolidated reporting and flow maps across multiple Plixer collectors.</p>
Data storage	<p>✓</p> <p>On average, the system can store 30-45 days' worth of flow data, and often much more, for deeper forensic investigation.</p>	<p>Limited</p> <p>No reported data to confirm storage capabilities</p>	<p>✓</p>
Zero-day exploit detection	<p>✓</p> <p>Can detect new or unique malware for which signatures do not yet exist using a behavioral method with more than 90 parameters</p>	<p>✓</p> <p>Uses only sensors rather than telemetry from the network, and detection is limited to sensor-placement locations</p>	<p>Limited</p> <p>Has limited baselining capabilities based on broad traffic counts</p>

	Cisco Stealthwatch	Darktrace	Plixer
Deployment (continued)			
Data compression	<p style="text-align: center;">✓</p> <p>As flows are received by the collector, they are synthesized into bidirectional, memory-resident flows. This reduces false positives and allows efficient data storage and accurate host-level reporting.</p>	<p style="text-align: center;">Not applicable</p> <p>Uses only sensors rather than telemetry from network.</p>	<p style="text-align: center;">Limited</p> <p>Some information is discarded</p>
Deployment model	<p style="text-align: center;">See note</p> <p>Does not require deployment of sensors or expensive probes. Telemetry can simply be turned on from network devices to analyze the network traffic.</p>	<p style="text-align: center;">See note</p> <p>Customers must purchase sensors and choose links to monitor rather than simply enabling telemetry from network devices and getting all conversations; model is expensive and difficult to scale.</p>	<p style="text-align: center;">See note</p> <p>Can consume most flow-based telemetry sources</p>
Endpoint visibility	<p style="text-align: center;">✓</p> <p>With Cisco AnyConnect 4.2 and later, the Endpoint Data License collects endpoint telemetry using the Cisco Network Visibility Flow (nvzFlow) protocol.</p>	<p>✗</p>	<p style="text-align: center;">✗</p> <p>Lacks features such as enable password, configuration presets for NAD types, and TACACS+ proxy</p>
Cloud visibility	<p style="text-align: center;">✓</p> <p>Can monitor the public cloud through the SaaS-based Stealthwatch Cloud solution</p>	<p style="text-align: center;">Limited</p> <p>Uses sensors to monitor the private cloud network and a Cloud Connector for particular apps</p>	<p style="text-align: center;">Limited</p> <p>Consumes Amazon AWS logs, which are similar to flows and include permit and deny actions</p>
Data export	<p style="text-align: center;">See note</p> <p>Has integrations with security information systems and offers APIs for custom integration; also supports SOAP and REST APIs</p>	<p style="text-align: center;">See note</p> <p>Has a Splunk connector that takes JSON syslog input from a Darktrace appliance and displays security incidents on Splunk; also links them to reports on the Darktrace Threat Visualizer</p>	<p style="text-align: center;">See note</p> <p>Supports REST API and log outputs</p>
Alarm notifications	<p style="text-align: center;">See note</p> <p>Provides email or syslog export to the SIEM system, Netcool, Remedy ticketing system, etc., with email, SNMP, and syslog notifications</p>	<p style="text-align: center;">See note</p> <p>Provides formatted syslog output</p>	<p style="text-align: center;">See note</p> <p>Provides outbound logging and alerting</p>

	Cisco Stealthwatch	Darktrace	Plixer
Investigation			
Full-scope investigative workflows	<p style="text-align: center;"></p> <p>Can investigate long-running security events. Generates context-based and custom alarms, ties username to IP address, monitors interface use, performs deep packet inspection, and logs every network conversation.</p>	<p style="text-align: center;">Limited</p> <p>Classifies the threat it detects and visualizes it on the Threat Visualizer interface</p>	<p style="text-align: center;">Limited</p> <p>Lacks customizable interfaces, rapid historical trending, automated remediation capabilities, and root cause analysis tools</p>
Effectiveness for enterprise customers	<p style="text-align: center;"></p> <p>Simplifies segmentation by logical host-group modeling to organize users by location, IP address, function, etc.; provides customized notification details and formats with alarm acknowledgment</p>	<p style="text-align: center;">Limited</p> <p>Uses only sensors rather than telemetry from the network, so scaling to enterprises is difficult</p>	<p style="text-align: center;">Limited</p> <p>Significant configuration and customization is required to support consolidated reporting and flow maps across multiple Plixer collectors.</p>
Flexible query and filtering system	<p style="text-align: center;"></p> <p>Can query on all captured fields. Advanced search is available for encrypted traffic for encryption key exchange, encryption algorithm, key length, TLS/SSL version, etc.</p>	<p style="text-align: center;">Not applicable</p> <p>No comparison information available in published materials</p>	<p style="text-align: center;">Limited</p> <p>Lacks customizable interfaces, rapid historical trending, automated remediation capabilities, and root cause analysis tools.</p>
Cyberthreats dashboard	<p style="text-align: center;">See note</p> <p>Provides pertinent information for SecOps personnel, such as which indexes are populated with alerts, which alarms are active, which hosts have the most alarms associated with them, etc. Also provides the ability to obtain more details and associated telemetry.</p>	<p style="text-align: center;">See note</p> <p>Primarily a security tool and the workspace is focused on SecOps</p>	<p style="text-align: center;">See note</p> <p>Dashboard-based for security and network monitoring</p>
Visualization and mapping	<p style="text-align: center;">See note</p> <p>Generates automatic maps such as worm propagation paths and custom relationship maps, allowing the visualization of any set of hosts and how they communicate to any other set</p>	<p style="text-align: center;">See note</p> <p>Heavily graphics oriented</p>	<p style="text-align: center;">See note</p> <p>Simple graphs and charts</p>
Incident investigation	<p style="text-align: center;">See note</p> <p>The UI is organized around persona-based workflows, leading administrators immediately to the root causes and supporting information.</p>	<p style="text-align: center;">See note</p> <p>Has a Threat Visualizer that enables visibility and the handling of threats</p>	<p style="text-align: center;">See note</p> <p>Investigative workflows are provided.</p>

	Cisco Stealthwatch	Darktrace	Plixer
Context			
Contextual data richness	<p style="text-align: center;"></p> <p>Integrated with Cisco Identity Services Engine (ISE). Enables host information look-up such as user ID, MAC address, device type, and switch port information; does not require a separate query to look up the associated user because user ID can be written</p>	<p style="text-align: center;">Limited</p> <p>Integrated with Active Directory for user data</p>	<p style="text-align: center;">Limited</p> <p>Offers sensors focused on a variety of data, including app performance and DNS deep dives</p>
Identity data	<p style="text-align: center;"></p> <p>Integrated with Cisco ISE, Cisco ASA products (NSEL), DHCP/RADIUS servers, and Active Directory authentication servers for identity-to-telemetry correlation</p>	<p style="text-align: center;">Limited</p> <p>Integrated with Active Directory for user data</p>	<p style="text-align: center;">Limited</p> <p>Integrated with Active Directory</p>
Routing and switching vendor integration	<p style="text-align: center;"></p> <p>Routers, switches, firewalls, and wireless controllers are the primary data source. Can parse many versions of telemetry and NetFlow from multiple vendors natively, such as IPFIX and sFlow, plus other Layer 7 protocols.</p>	<p style="text-align: center;"></p> <p>Uses only sensors rather than telemetry from the network. Requires SPAN or TAP for each monitored link and is limited to what's on the link.</p>	
URL data capture	<p style="text-align: center;">See note</p> <p>Flow Sensors can extract URL data used by the Flow Collectors and Management Center. URL data can be queried based on operators. Also integrated with Cisco Security Packet Analyzer, which can download exact datagrams that the flow represents in PCAP format.</p>	<p style="text-align: center;">See note</p> <p>Completely sensor-based and has visibility into packet data</p>	<p style="text-align: center;">See note</p> <p>Can capture URL data using sensors</p>

	Cisco Stealthwatch	Darktrace	Plixer
Context (continued)			
NetFlow generation for VMware environments	<p style="text-align: center;">✓</p> <p>Uses the virtual switch NetFlow export feature or virtual flow sensor</p>	<p style="text-align: center;">Not applicable</p> <p>Not applicable because it uses sensors to log traffic</p>	<p style="text-align: center;">✓</p> <p>Can consume NetFlow telemetry from VMware</p>
Collection of application and L7 flow data	<p style="text-align: center;">✓</p> <p>Maintains flow state (active, inactive, or ongoing); generates NetFlow based on SPAN port monitoring or TAPs; has proxy integration; and provides application identity for multiple vendors such as Palo Alto Networks and L7 Defense; and uses NBAR and NBAR2 with the Flow Sensor</p>	<p style="text-align: center;">✓</p> <p>Uses probes that parse this data directly from raw packets</p>	<p style="text-align: center;">Limited</p> <p>Can receive firewall data, flow from a SPAN with sensor, and app ID from a sensor or firewall. No NBAR support or proxy integration.</p>
Full packet capture	<p style="text-align: center;">✓</p> <p>Integrated with the Cisco Security Packet Analyzer, a tool installed on a SPAN or TAP that maintains a rolling buffer of datagrams on a segment and provides the ability of downloading exact datagrams that the telemetry represents in PCAP format and even the files contained within PCAP. It can also launch the packet decoding instead of downloading another app.</p>	<p style="text-align: center;">Unknown</p> <p>No comparison information available in published materials</p>	<p style="text-align: center;">✗</p> <p>No ability for full packet capture</p>
Encrypted traffic analysis	<p style="text-align: center;">✓</p> <p>Uses Encrypted Traffic Analytics or enhanced telemetry from the Cisco network to detect malware and to help ensure crypto compliance. Stealthwatch analyses encrypted traffic using advanced machine learning and global threat intelligence.</p>	<p style="text-align: center;">Limited</p> <p>Might be able to detect some anomalous behavior in encrypted traffic</p>	<p style="text-align: center;">✗</p> <p>No ability to analyze encrypted traffic</p>
Enterprisewide reputation scoring	<p style="text-align: center;">✓</p> <p>Creates index-based scoring for every host that tallies unusual activity by a host</p>	<p style="text-align: center;">Unknown</p> <p>Anomaly detection model might be using a global scoring mechanism</p>	<p style="text-align: center;">✗</p> <p>No concept of security indexes; triggers only raw alerts and alarms</p>

	Cisco Stealthwatch	Darktrace	Plixer
Threat Intelligence			
Threat intelligence feed	<p style="text-align: center;">✓</p> <p>Stealthwatch Threat Intelligence License and Global Risk Map, powered by Talos, is a threat feed from a number of sources, updated at least once an hour. It aims to provide a zero false-positive information set.</p>	<p style="text-align: center;">✓</p> <p>A threat feed that has a list of known malicious sites is available.</p>	<p style="text-align: center;">✗</p> <p>None, although Plixer has a DNS-focused appliance for detecting DNS issues</p>
Exploitation detection	<p style="text-align: center;">✓</p> <p>Can detect insider threats like data exfiltration and command-and-control communications, plus long and slow attacks. Security events feed the indexes to trigger alarms by means of behavioral algorithms and absolute limits that can be set by the operator.</p>	<p style="text-align: center;">✓</p> <p>Detection of a number of exploits is called out but the scope is unknown.</p>	<p style="text-align: center;">✗</p>
Threat intelligence sharing	<p style="text-align: center;">✓</p> <p>Stealthwatch Threat Intelligence data is used by Cisco Talos, and vice versa. Cisco shares data with hundreds of partners, customers, and providers through the Aegis, Crete, and Aspis programs, and is a founding member of the Cyber Threat Alliance.</p>	<p style="text-align: center;">✗</p>	<p style="text-align: center;">✗</p>