Competitive brief

VECTRA®

Stealthwatch and the risk of equating networking with security

We get it. You already have Cisco in your network. Why not use them for security too? But just like eating fast food for every meal isn't very good for you, spending all your budget with Cisco doesn't do your security posture any favors either.

That is especially apparent when it comes to network detection and response (NDR) solutions. At Vectra®, we often see Cisco Stealthwatch show up for proof-of-concept (POC) evaluations alongside our Cognito® platform, and we love it.

For one, friendly competition keeps us honest and on our toes. But the real reason is because we win. Especially if the customer is using a red team to simulate real-world attacks.

That's because our AI models are developed by security researchers and data scientists working together to create supervised and unsupervised machine learning algorithms.

You can't see anything if you don't know what to look for

Stealthwatch uses NetFlow to capture and analyze traffic. The problem? NetFlow is fundamentally a network performance monitoring tool that Cisco has remarketed for security. NetFlow does not provide the level of detail needed for security teams to accurately triage an incident.

For example, NetFlow can show that a connection was made but cannot tell you what the connection was used for. Think of it like a cell phone bill – it can tell you a call was made and how long it lasted but not what was discussed. This level of visibility is helpful for network performance monitoring, but it's not enough for security.

Security teams need to know, for example, whether an SMB connection was used to authenticate a user, mount a share or execute code. NetFlow can't tell you that, making Stealthwatch ineffective for visibility and detection. A long line of other examples would include whether an attacker is using encrypted tunnels to exfiltrate data.

Prepare to be overloaded by anomaly events

When pitted against real humans rather than canned attacks, Cognito algorithmic models from Vectra outshine the simple anomaly-based detections of Stealthwatch. In fact, the Cognito platform supports over 85% of the MITRE ATT&CK framework. This comprehensive capability quickly becomes apparent during the POC.

As an anomaly detection system, Stealthwatch can't identify the highest-risk threats and will overwhelm your security team with a deluge of events that you have to manually investigate.

In stark contrast, the Cognito platform from Vectra reduces the security operations workload by 34X. It automatically triages alerts into incidents, prioritize host devices that pose the highest risk, and extracts security-enriched metadata from network traffic for investigations and forensics.

Conversely, Stealthwatch alerts must be manually and individually triaged, which increases your security operations workload.

Get ready to spend time on maintenance

For accurate network visibility, Stealthwatch requires you to spend an inordinate amount of time configuring network equipment and maintaining asset groups. Switches, firewalls and other networking equipment must send NetFlow data to Stealthwatch FlowCollectors. This can be cumbersome to implement because large enterprises have thousands of networking devices.

Further, a Stealthwatch deployment requires the configuration and constant maintenance of Stealthwatch HostGroups. In order to tune noise and alerts, all network assets must be classified into groups. This usually involves grouping assets based on their functional role on a network, such as DNS servers, AD servers and DHCP servers.

Most large corporate environments have trouble sourcing this information quickly, and it changes rapidly. Communication, ownership and change management policies can quickly become insurmountable because network and security teams are often in different departments. Without these continuously maintained HostGroups, Stealthwatch security policies become meaningless.

Of course, consistent with Cisco's business model, they can help you with this – for an ongoing fee.

On the flip side, the Cognito platform from Vectra delivers high-fidelity network metadata instead of NetFlow. This lets you know what's happening in every conversation.

Additionally, the Cognito platform enriches the metadata with context specific to security applications, including the names of hosts, existence of beacons and the privilege levels of accounts. Cognito reduces attacker dwell time and improves triage times by 34X. All without any need for ongoing tuning.

Cognito from Vectra: NDR that works

The Cognito platform delivers complete visibility – from enterprise to cloud – using the broadest set of machine learning algorithms. Cognito gives you the following advantages over Cisco Stealthwatch:

- Detects real-world attacks based on the supervised and unsupervised machine learning algorithms, from cloud workloads to user and IoT devices.
- Identifies threats from day one without requiring a baseline learning period.
- Reduces your SOC workload by 34X. Cognito triages security alerts into prioritized incidents for the fastest, conclusive response.
- True platform performance integrates with other solutions in your security stack.

Vectra empowers organizations to embrace hybrid cloud architectures with purpose-built detection models for securing workloads in the cloud and on-premises.

Network Traffic Analysis Capability	Vectra	Cisco	Assessment
Data source	Security-enriched network metadata	NetFlow	NetFlow is a network performance monitoring tool re-marketed for security. NetFlow shows that a connection was made, but says nothing about what the connection was used for. It's like a cell phone bill: it can tell you that a call was made and how long it lasted, but nothing about what was discussed. While this level of visibility can be very helpful for network performance monitoring, it's not enough for security. For security, you need to know, for example, whether an SMB connection was used to authenticate a user, mount a share, or execute code. NetFlow can't tell you that, and it makes it ineffective both for visibility and detection. Cognito delivers high-fidelity network metadata – knowledge of what's happening in every conversation – enriched with context specific to security applications, e.g. the names of hosts, existence of beacons, and the privilege level of accounts.
Metadata streaming to data lake/SIEM	✓	✗	Vetra Cognito streams searchable metadata in Zeek format to the data store of your choice with Kafka, syslog and Elastic support. Because of its inherent data source, Cisco Stealthwatch only exports Netflow
AI-derived metadata enrichments	✓	✗	Inherent and embedded into the platform, ML-enrichments derived by an award-winning team of Ph.D. data scientists and security researchers provide security teams with the insights for effective threat hunt. Example use cases and enrichments can be found in the following blog.
Deep learning	✓	✗	The Cognito platform from Vectra applies optimized AI techniques – supervised, unsupervised machine learning and deep learning – to precisely identify attacker behaviors with greater efficacy and fewer false positives. Vectra delivers a higher fidelity signal and much lower noise than Stealthwatch, which uses a low-resolution data source, NetFlow. Vectra applies the optimal machine learning models to security-enriched metadata. NetFlow data is only optimized for network performance monitoring and diagnosis (NPMD) and lacks the requisite resolution and the details needed for threat detection.
Supervised machine learning	✓	✓	
Unsupervised machine learning	✓	✓	
Imports IoCs for detection	✓	✓	The Cognito platform and Stealthwatch both combine the detection of hidden threats using AI with the detection of known threats using high-quality IoCs. However, Stealthwatch machine-learning detections are lower quality because the data source is NetFlow and not network metadata. Stealthwatch generates a high volume of false positives compared to the specific attacker-behavior detections of the Cognito platform.
Aggregates individual alerts into incidents with full PCAP on-demand for forensic investigation	✓	✗	Vectra delivers a greater reduction in the security operations workload by triaging and correlating security alerts into incidents, prioritizing hosts with incidents, and providing PCAPs for incident investigations and forensics. Stealthwatch alerts must be individually triaged, which increases the security operations workload.
Tracks cyberattacks across the enterprise and automatically shows all compromised workloads and devices	✓	✗	Vectra empowers security operations teams to address all workloads and devices that may be impacted by a cyberattack, which speeds-up response time and reduces the overall security operations workload. With Stealthwatch, security analysts must manually correlate hosts with similar alerts to understand the scope of an attack, which delays response and increases risk to an organization.
Includes detection models specific to data center and cloud use-cases	✓	✗	Vectra delivers complete enterprise coverage from cloud and data center workloads to user and IoT devices using the broadest set of machine learning algorithm, leaving attackers with nowhere to hide. Vectra empowers organizations to embrace hybrid cloud architectures with purpose-built detection models for securing workloads on-premises and in the cloud. Stealthwatch simply applies the same generic detection models it uses for IoT and user devices to NetFlow information from the data center and flow-based data from cloud service providers.
Integrates with firewall, NAC, endpoint, SIEM and SOAR products to streamline incident response	✓	✓	Vectra delivers the agility to respond appropriately based on the threat detected. Vectra can immediately integrate into an enterprise's security architecture, enabling existing endpoint, NAC and firewall security to block new classes of threats and provide the best starting point for an investigation in a SIEM or their data lake. Stealthwatch integrations with the Cisco Identity Services Engine (ISE) to quarantine hosts, but they do not integrate with security solutions from other vendors, locking customers into a Cisco-only solution.
Delivers a complete solution for network detection and response	✓	✗	Vectra delivers a platform for both network detection and response (NDR) with Cognito Detect, Cognito Recall and Cognito Stream. Vectra has the longest tenure and greatest investment in the development of AI for detecting attacker behaviors as well as collecting and enriching metadata for threat hunting and incident investigations. Stealthwatch only saves on-demand PCAPs (full PCAP is not supported), which significantly limits threat hunting and incident investigations. Stealthwatch cannot send PCAPs to a data lake, use your existing Zeek tooling or build custom queries with tools like Elasticsearch.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai