NORTH|STAR™

UTILITIES SOLUTIONS

Covalence Competitor Comparison FAQ

844-888-9904
info@northstarutilities.com
www.northstarutilities.com

How Does Covalence's Threat Minimization Process Compare to a Vulnerability Scan?

Threat Surface Minimization is the process of identifying a network's attackable points then removing them. An example would be to identify vulnerable software and then patch it. Although an overlap with vulnerability scanning exists, it's not quite the same. Vulnerability scanning is typically point-in-time data, while Covalence continuously gathers and processes data through network, cloud, and endpoint sensors. Vulnerability scanning will identify vulnerable versions of specific equipment. Covalence can do the same thing.

Customers can request vulnerability scanning directed at specific assets. Covalence uses analytics and machine learning to identify systems with vulnerabilities and tells the customer there's an issue with systems A, B, and C.

Vulnerability scanning typically involves automated network scanning only. Other platforms identify software versions through interaction with the service over the network. Covalence can identify software versions directly from the system using endpoints and, depending on the service, from network-based observations.

Does Covalence Remove the Requirement for a Vulnerability Assessment Scanning Tool?

Covalence does not apply ‘active scanning’ against a network. However, identifying and discovering high-risk and vulnerable applications, configurations, protocols, and services are fundamental to the service. Covalence aims to reduce or remove vulnerabilities from a network before they can transform into a problem.

For example, with endpoint agents, Convalence continuously monitors to identify the installation or existence of vulnerable software (based on a CVE? metric of 8 or above, typically signifying remotely exploitable vulnerabilities). The service will also identify high-risk network applications and patterns, such as the use of SMBv1, which is fully patchable, recommended for removal by vendors, and commonly used by ransomware actors to move laterally within a network. We recommend the use of a firewall + antivirus in addition to Covalence. A fully up-to-date Windows 10 with Windows Defender is sufficient for ‘antivirus.’

The Covalence service includes a team of analysts who monitor and maintain the sensors and systems deployed, update threat intelligence, monitor alerts from the tools and sensors, and perform threat hunting. The customer’s experience is to receive low-volume AROs which direct specific and contextualized notifications/alerts/advisories.

What is the profile of a typical Covalence client?

Clients can range in size from 5-2500 employees, but a typical client size is 100-1000 employees.

Can Covalence be sold to a client that has an existing SIEM?

Yes, Covalence can exist alongside other technical solutions, including SIEMs.

Does Covalence negate the requirement for a SIEM?

Some customers may have specific regulatory or other business requirements to trap and store logs, in which case a SIEM would provide additional value beyond the Covalence service. Still, these scenarios tend to be more an exception than the rule. Covalence does include the ability to be a ‘micro SIEM’ and receive and store Syslog-formatted data.

Does Covalence compete directly with Endpoint Only Solutions?

EndPoint solutions focus on endpoints ONLY, taking a cloud-centric approach that uploads observed data to the cloud for analysis. Covalence keeps client data within the client network and takes a holistic approach by covering your entire threat surface, including endpoint, network, and cloud monitoring.

Does Covalence compete directly with AI-only Platforms?

AI-Platforms is a machine-learning platform that is fundamentally different from the Covalence service. Some of the key differences are:

- AI Platforms are a SIEM-enablement technology; Covalence is a turnkey monitoring and threat hunting service.
- AI Platforms are reactive and identify when systems are behaving abnormally, suggesting that something is wrong. Covalence does this too but further identifies threats and vulnerabilities BEFORE they become a problem and is therefore preventative.
- To maximize the benefit of AI Platforms, clients must perform expert configuration and tuning, which requires clients to be heavily involved in the process. Our support team of world-class analysts and engineers do all the heavy lifting for the client and manage the Covalence service.
- AI Platforms are an enterprise-class product, which is being scaled down and price-modified to support smaller markets. Covalence is purpose-built for small to mid-sized businesses. Covalence supports organizations with less IT and security resources (or none at all), understands the threats most likely to affect these organizations, and provides technology (and pricing) that supports the types of technology that SMEs use.

Covalence supports all aspects of cloud deployments, ranging from integrating with a cloud provider's native security APIs to deploying endpoint agents within the application space of the client (e.g., within VMs).

Companies are prone to be attacked in specific ways, and it is not clear that AI Platforms provide the detection and support that a company may require. We designed Covalence to protect a company's core business by identifying and stopping problems that are likely to lead to ransomware, data loss, financial redirection attacks, and much more.

Like AI Platforms, Covalence uses Machine Learning (ML) to help understand and characterize a client's network, including beacon detection (fixed interval communication), dark space identification (systems that are trying to communicate with unused IP-space), and User and Entity Behaviour Analysis (UEBA). The critical difference is that Covalence uses both ML and human expertise to identify anomalies that AI alone may miss.

Covalence also includes a module called "Connection Monitor," which allows Covalence to characterize the expected behavior for specific systems and signal alerts for deviations. With just this one module, Covalence accomplishes the same overall objective of an AI Platform.

How does the DNS Firewall service align with other DNS Security strategies (e.g., Cisco Umbrella)?

The Covalence DNS Firewall service is a competitor to Cisco Umbrella and other DNS security solutions. We include it as part of the Covalence service (at no additional cost), and clients who do not have a DNS firewall on their network can use this service.

Since a DNS firewall is a critical part of network security and health, Field Effect has partnered with CIRA – a leader in DNS operations, with a commitment to security, uptime, and operational efficiency. CIRA's DNS firewall technology directly integrates with Covalence. Because they work together, it is easy to enable Covalence's ARO alerting process, which provides a single, simplified set of security alerts for all dimensions of security monitoring, including DNS firewall events.

In addition, because cybersecurity experts and engineers managed the DNS firewall service, Covalence also offers custom threat intelligence beyond what you would typically find in other products and services such as Cisco Umbrella.

Still Have Questions?

Give us a call: 844-888-9904

Email us: info@northstarutilities.com

Log a Support Ticket https://www.northstarutilities.com/support