NORTH|STAR™

UTILITIES SOLUTIONS

Covalence Frequently Asked Questions

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

What's a Cyber Threat?

Before we can understand the scope of a threat surface, let's begin by defining what a cyber threat is:
Attackers implement cyber threats using various techniques, technology, and tradecraft to achieve their objectives. Regardless of individual circumstances, attackers are typically trying to:

- Obtain sensitive information,
- Use a privileged digital identity for fraudulent purposes (such as a business email compromise and financial redirection, and/or
- Deny or disrupt the ability to use the network (as in cases of ransomware).

NORTH|STAR™
UTILITIES SOLUTIONS

What's a Threat Surface?

There is some bad news: threat actors use various tools and techniques to compromise, or otherwise affect (attack), a victim's network. The sum of all these vulnerabilities and attack points across a network is known as its Threat Surface.

But there's good news! These tools and techniques are only effective against the points on a network that are both accessible and vulnerable to attack. The goal is to make your threat surface as small and inaccessible as possible by addressing every known vulnerability.

What Makes a Vulnerability?

When threat actors can use points in a network to achieve their goals, they are vulnerable to threat actors gathering or removing data, encrypting data to use as ransomware, and/or disrupting the network's service. Vulnerabilities exist in a variety of forms, but here are a few examples:

- Weak passwords
- Misconfigured endpoints
- Lack of user awareness/education
- Phishing emails

In terms of defending a network, you should focus your defense efforts on these vulnerable points.

The Kill Chain

Let's shift focus to the attacker's perspective and imagine having personal data on your network that a group of threat actors intends on exfiltrating.

Like a thief picking a lock, the threat actors need to perform several steps to accomplish their mission. We know this process as the Kill Chain. If any, one step is unsuccessful, the threat actor cannot complete his process, and that step could stop him altogether.

As a network operator, you want adequate protection across every link in the kill chain. Having a protection method for every link in the kill chain can maximize the chances that the threat actor has a bad day. And like a good lock, a layered approach to your defenses may stop them from even making an attempt to get into your network.

Phone: 1-884-888-9904 **www.northstarutilities.com** **email: info@northstarutilities.com**

Reducing the Threat Surface

Threat actors spend days, or even their "careers," focused on defeating network security. So, you also need to be hyper-vigilant when managing your threat surface.

Some immediate considerations surrounding your threat surface should include:

- The hardware running on your network,
- The services and applications in use, and
- The humans using the network.

Once you assess the risk of the considerations above, reducing a network's threat surface can mean many things, including:

- Implementing technical measures that restrict certain system activities,
- Limiting the number of users with elevated administrative privileges, and
- Turning off non-essential services.

All these elements, and many more, must be measured, managed, and reduced. While it sounds daunting, with Covalence in your arsenal, you're well on your way.

At the end of the day, it's simple: the smaller your Threat Surface (the fewer attackable targets), the harder it will be for attackers to achieve their objective - and the easier it will be to defend.

How does Covalence work?

Covalence offers the same high-end sensor and monitoring capabilities typically reserved for enterprise environments by measuring activity on the network, on endpoint systems, and from cloud system APIs.

Covalence can gather essential data, such as telemetry information, security events from desktop and server systems, use machine learning and other algorithms to identify suspicious network communications with deep packet inspection, and implements sophisticated analytics to identify compromised accounts other security threats in cloud systems.

Covalence detects threats and vulnerabilities using data from the sensors combined with automated analytics aided by expert Covalence analysts to reduce false positives and periodic threat hunting across all sensor domains.

How are security threats detected in Covalence?

Threat detection is specific to the “domain” (network, endpoint, cloud) of detection. Network monitoring provides high-resolution network capture, analysis, and storage for networks. The network monitoring component uses physical network monitoring appliances, offering the ability to directly identify threats and vulnerabilities affecting all devices within a network.

Endpoint monitoring capabilities offer detailed insight into the configuration, behavior, vulnerabilities, and threats facing individual endpoints across workstations and servers alike. We distribute and install endpoint agents on devices across your network, and we can deploy them on Windows, macOS, and Linux systems.

Cloud monitoring protects a domain and cloud-based programs, including Office 365, G Suite, AWS, Dropbox, Box.com, and Okta, by identifying suspicious login activity and other security-related events to your domain and cloud data.

Covalence uses threat intelligence and traditional indicators of compromise (e.g. blacklists), machine learning, anomaly detection (e.g. identify machines behaving in ways that they haven't previously, such as RDP'ing within a network where before it only had web and email traffic), manual threat analysis and hunting, protocol anomaly identification (e.g. finding DNS traffic over port 1234), and much more. When it comes to cloud analytics, UEBA (User and Entity Behavioural Analysis) is used as the primary baseline.

What type of threat intelligence does Covalence use?

Covalence uses several open-source commercial and government threat intelligence feeds. This continuously updated set of threat intelligence is derived from:

- Open-source feeds (e.g., abuse.ch),
- Government feeds (e.g., FBI, Canada's Cyber Center),
- Commercial feeds (e.g., Snort Rule Subscriptions), and
- Proprietary information (information from Covalence operations, such as scanners, phishers, and malware indicators we discover).

At any given time, there are between 30K and 300K indicators applied to a client's monitoring profile. The number of indicators varies as the threat intelligence is updated, aged off, and adjusted according to high priority emerging threats.

How does the Mini-SIEM functionality work?

Covalence approaches security through direct measurement and detection of threats to a network. At the same time, external data sources are also valuable for security analysis or regulatory requirement purposes. Covalence can ingest log data from any source capable of generating "Syslog" formatted data. Covalence also supports RFC31564 or Common Event Format (CEF) messages. Typical data sources include switches and routers, desktop and servers, IoT devices, 3rd party security tools, firewalls, and Other SIEMs.

A customer's firewall is experiencing critical alerts and sending these logs to a Syslog server. Can Covalence ingest these critical alerts and generate AROs for the customer?

Receiving Syslog data is a built-in function of Covalence, and AROs can be generated based upon this data. However, this requires a custom integration to be configured by the Covalence Security Operations team. If it is something as simple as generating an ARO for any record with the text "CRITICAL," it would be relatively easy to implement. If the requirement is to parse the data and enrich it based on observations from the network sensor, it would require more work. A determination of the amount of work involved can be made once the data and specific requirements have been defined. Depending on the complexity, there may be an additional cost associated with doing the integration.

This type of request comes up frequently with potential clients. Once clients realize that Covalence directly monitors network traffic, they tend to drop interest in ingesting log data.

What is Domain Monitoring? How is it different from the DNS Firewall service?

Once a client begins Covalence network monitoring, their domains are added to a Domain Monitoring service that interrogates domain name authorities - known as registrars - to identify whether any domain names similar to their own have been recently registered. If they are, Covalence will notify them through an ARO.

For example, if acme.net is registered and acme.com is the client, they would be notified. Covalence does not block these domains by default because threat actors deliberately choose domains that the victim could reasonably use – the client could have registered a .net domain. If the domain is, in fact, deemed malicious, it can be added to the DNS Firewall service, which will actively block requests to the domain in the future.

What is the profile of a typical Covalence client?

Clients can range in size from 5-2500 employees, but a typical client 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 unique than not. Covalence does include the ability to be a 'micro SIEM' and receive and store Syslog-formatted data.

Still Have Questions?

Give us a call: 844-888-9904

Email us: info@northstarutilities.com

Log a Support Ticket

https://www.northstarutilities.com/support