ResponSight

Corvum Suite Overview

Corvum Collector
Gathers the metrics and telemetry

Corvum Aggregator
Bundles and manages data delivery to third party solutions

Corvum Analytics Engine
Does the heavy lifting, performing analytics for enterprise risk profiling

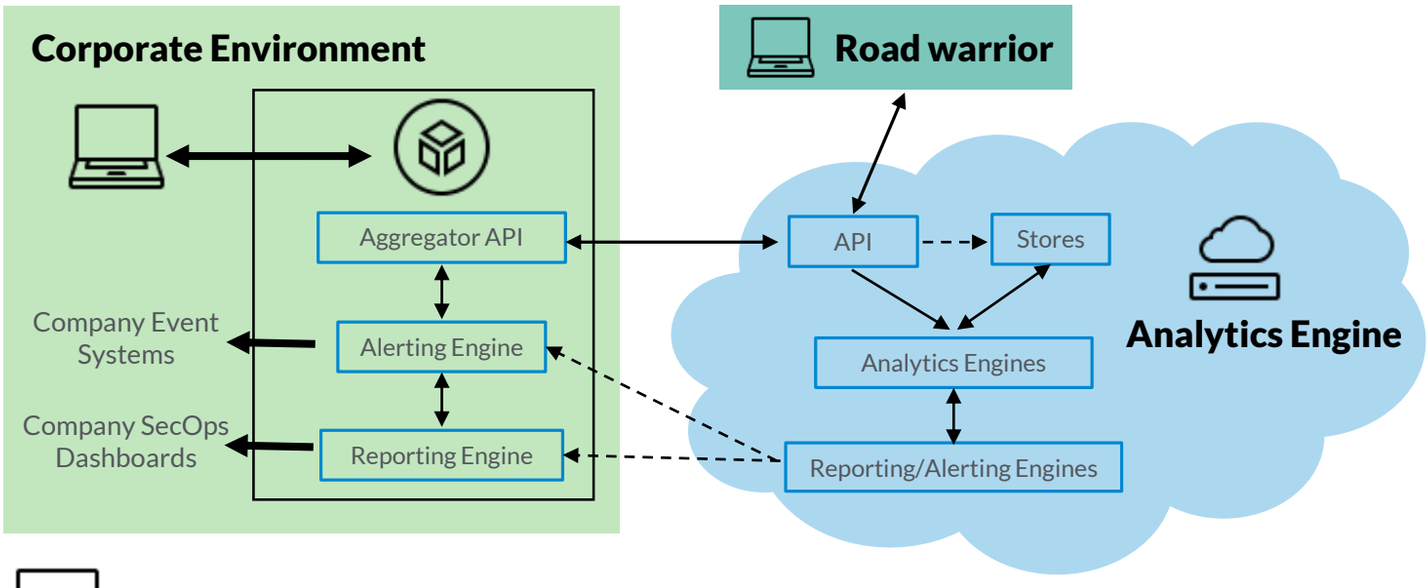
ResponSight provides enterprise risk profiling technology by ingesting user telemetry to analyse risk across the entire organisation in a scalable and cost effective way.

ResponSight's Corvum Suite collects and analyses data from laptops, desktops and servers across an organisation to create a profile of "normal" behaviour over time. Incident responders are then alerted to behaviour that differs from that machine's usual usage pattern.

Unlike endpoint detection and response (EDR) or user and endpoint behavioural analytics (UEBA) software, ResponSight does not rely on private or sensitive information that might be divulged by the user or "heavy" endpoint technologies to assess risk.

Corvum Suite is **lightweight** and **goes unnoticed** by the user – there's no dock icon or application interface, and no support headaches for your team. It is designed to **work with your existing cyber security solutions**, playing the "detective" role, while existing "blocking" technology can be better leveraged to set priorities.

Architecture



Corvum Collector

The **Corvum Collector** runs as-a-service, integrating directly into a user's hardware to gather metrics and activity telemetry, including numerical, mathematical and statistical data about how the laptop, desktop or server is used to determine the behavioural fingerprint of each user.

Unlike other solutions, the Collector is cautious of the operating system in which it plugs into and the data that is collected. When the Collector plugs into a user's system, it does not leave the operating system, nor does it rely on logs produced by Windows to confirm the authenticity of a data source. Instead, data is collected from various points inside the operating system, before it is correlated with other data points to validate what is collected is reliable and can be trusted, which no other solution does.

By not trusting the platform, it also means the collected data produces a mix of results that are not typically revealed.

When large volumes of raw numerical telemetry and selected metrics are combined, it's possible to build activity and behaviour profiles about users, without ever knowing who that user is.

For example:

- Our software can detect when a browser is opened, but does not capture specific details of the user's activity inside the browser;
- ResponSight has visibility of process names and paths, but this data is hashed or encrypted before delivery to our Corvum Analytics Engine Service, so even non-sensitive information is protected to ensure sensitive information is not inadvertently disclosed.

The key to identifying changes in risk is based on being able to tell when someone else (an attacker, or a piece of malware) is controlling the laptop, desktop or server. It is not easy for an attacker to replicate days, weeks or months of security profile analysis to mimic the real user in a short period of time, and that's the trigger for changes in risk and how potential security breaches can be initially identified.

Corvum Aggregator

The Corvum Aggregator is a lightweight standalone virtual machine (less than 1GB) that can be installed in a user's virtual environment. Aimed to help users ensure consistent network design compliance in existing and new implementations, the Aggregator bundles and manages data delivery through gateways so organisations can monitor, filter, and maintain control over their corporate network.

It also connects and updates integrations to third-party solutions, such as your security information and event management (SIEM) software. The Aggregator acts as a "traffic cop" connection/traffic proxy and communications manager.

The Aggregator can be used with any or all of the following requirements:

- Laptops, desktops and servers are not generally permitted to connect directly to the Internet (i.e. they already communicate through gateways and proxies);
- The enterprise wishes to take advantage of opportunities to integrate with existing security investments such as SIEM and ticketing/alerting systems;
- The enterprise has a requirement to link the endpoint with other identification systems, where the username/machine name must be known (as ResponSight does not collect these).

Corvum Analytics Engine

The Corvum Analytics Engine has been designed to do all the heavy lifting and performs the analytics for enterprise risk profiling, removing load from the user's networks and reduces overall overhead.

All of the information that is collected is placed in secure repositories. Separate data repositories are created for each client and are keyed, encrypted, isolated, and independently managed. Client maps are also securely stored off from any of ResponSight's Analytics Engine.

All the information is delivered via a single dashboard that can provide access to:

- Executive summary – overall summary at board level
- Monthly risk scores – trends over time and within months
- Risk summary – risk exceptions as a percentage of total
- Risk scores of all users
- Activity risk by endpoints
- Time series for more details and technical view
- Exceptions – for example, process counts

"With a truly tiny footprint, Corvum Collector goes unnoticed by the user"

Corvum Suite Collector currently supports Windows 7, 8 and 10, and MacOS Sierra and High Sierra. Nothing is visible to the user, so there is no help desk overhead

Optimum Privacy

All metrics are primarily numerical or system generated

No uniquely identifiable information linking to the actual identity of the user

No metadata is collected

ResponSight supports all major cloud providers, including Azure and Amazon Web Services. Cloud storage locations are dictated by the location of the client. However, clients can choose a preferred location.

Contact us for further information

W: responsight.com **E:** info@responsight.com responsight