FIELD EFFECT
COVALENCE

Understanding Your Threat Surface

Covalence - Leading Edge Cyber Security Monitoring and Analysis

ABOUT FIELD EFFECT SOFTWARE

Field Effect Software is headquartered at Lansdowne Park in Ottawa, Canada. Our mission is to strengthen the IT security operations of large enterprises and small to medium sized businesses alike. We are leaders in the development of network application solutions, low level systems development, and cyber security analytics. Our solutions are trusted by major organizations worldwide and our team is a unique mix of deeply skilled security professionals, software developers and analysts with a passion for improving security.

WHAT IS COVALENCE?

Covalence is a network and endpoint monitoring and analysis system that identifies malicious and anomalous activity while providing a powerful view into your network. It features advanced monitoring and analytics to measure, manage and reduce the threat surface of your network and associated infrastructure.

- **Incident Detection and Remediation**. Strengthen the resilience of your IT network. Covalence identifies suspicious/malicious threat actor behavior and allows your team to quickly obtain data for remedial action.
- **Threat Surface Measurement**. Access and review network, endpoint and application data points, identify attacker-accessible assets. IT Asset enumeration: Identify and track systems on your network.
- **Threat Surface Minimization**. Easily compare enterprise network configuration and security posture reporting against key mitigation measures like the Australian Signals Directorate's Essential 8, Communications Security Establishment's Top 10 IT Security Actions, the SANS 20 Critical Security Controls, etc.

What is a Threat Surface?

Your network's Threat Surface is the totality of all hardware and software vulnerabilities that are accessible to unauthorized users. For example, servers offering web services to the Internet, BYOD users accessing the corporate network, even your office network-enabled thermostat.

Many cyber security products seek to identify malicious and other unwanted behavior on your network. Covalence not only targets these activities but gives you the power to identify, understand, reduce and defend your organization's threat surface.

" If you really want to protect your network, you really have to know your network."

Rob Joyce

National Security Agency

HOW COVALENCE WORKS

Covalence is comprised of three easily deployed components: sensors, an analytic engine, and user interface. Covalence may be deployed in as little as a single virtual machine, receiving NetFlow feeds from your network devices, or deployed in a distributed manner with both full take (PCAP) sensors at key network points and endpoint agents installed on your hosts.

Covalence gathers data on your network and runs continuous analytics to identify known-bad as well as anomalous system and network activity while measuring the shape, size and behavior of your network – all presented to your team in a rich, intuitive view. Covalence also includes data-enrichment capabilities built-in, reducing false-positives while helping to provide the context needed to understand what is happening on your network – deep insight without the noise.

We recognize that speed, scale, and effectiveness are key to modern cyber security solutions. For this reason, Covalence implements both discrete as well as machine learning-based analytics, including:

- IP, protocol, domain and URL blacklisting
- Beacon and Hostile Scan detection
- Darkspace analysis and alerting
- Typosquatting detection
- Abnormal system behavior (e.g. out of hours activity)

WHY COVALENCE?

- **Integrate with your enterprise IT operations**. Work with, annotate, and assign incidents for remediation via integration with helpdesk and trouble ticket solutions. Leverage your existing security infrastructure (e.g. SIEMs). Easily import data to Field Effect's Cyber Range for training and simulation – strengthen your security and your teams using simulations based on real events and infrastructure.
- **Simplicity**. Easy, package-based deployment (.deb, .rpm). Integrate with existing corporate tools (Active Directory, Jira, etc.). An analyst friendly interface, with the ability to quickly search and query datasets, respond and take action.
- **Scalability**. Support for NetFlow, as well as full high-speed data capture (10Gb+). Works with *Field Effect endpoint solution*.
- **Extensibility**. APIs and SDKs available. Add and load custom analytic modules. Integrates with 3rd party tools and technology. Directly access and leverage sensor operation and data.

Covalence in action

Designed for analysts but with the views to give executives peace of mind that their network is in good hands

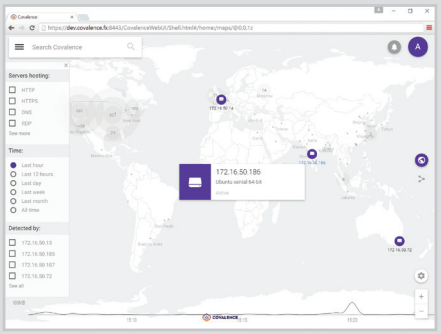

***Figure 1:** Global view - see your network entirely, know and manage your threat surface from the top*

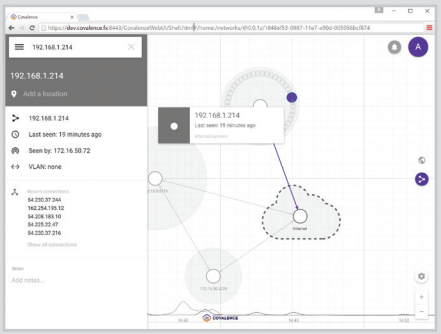

***Figure 2:** Internals - highly refined view and controls give you and your team detailed insight and power*

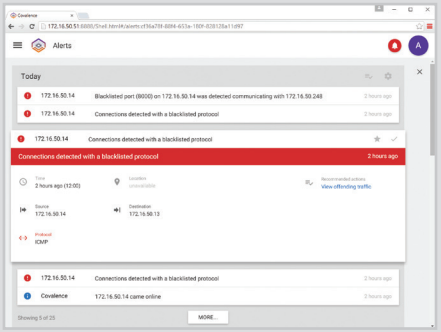

***Figure 3:** Alerting - real-time monitoring & analysis provide event context for response & reporting*

Want to learn more about Covalence?

Contact us at **hello@fieldeffect.com** or **+1.613.686.6342**

207-825 Exhibition Way
Ottawa, ON K1S 5J3
Canada

+1.613.686.6342
hello@fieldeffect.com
http://covalence.fieldeffect.com

FIELD EFFECT SOFTWARE