# ExtraHop Dives Into the Security Analytics Fray With Reveal(x)

## Abstract

ExtraHop came out of not-so-stealthy security mode at the end of January 2018 with the introduction of its first purpose-built security analytics product, called Reveal(x). Although ExtraHop is traditionally a network and application performance management provider, they have been adding new security use cases and packages over the last year or so. The company officially planted its flag in the security analytics market with the new machine learning-based Reveal(x) offering.

## Event

The pool of security analytics providers just got one more swimmer with ExtraHop jumping into the deep end with its new Reveal(x) product. Although ExtraHop historically played in the network and application performance management markets, over the last few years, the eleven-year-old company added a purpose-built security solution created from its ability to monitor and analyze detailed network activity. Reveal(x) is the culmination of a multi-year effort to exploit the unique insights extracted from wire data to detect behavioral anomalies that potentially represent security compromises. ExtraHop's data scientists and programmers developed machine learning algorithms capable of analyzing as many as 4000 features on any given endpoint. ExtraHop then layered automated workflows to streamline the investigation of detected anomalies, creating a standalone analytics product that is not dependent on logs and event management systems. Reveal(x) automatically correlates related indicators of compromise, conducts deeper analysis on critical assets, reveals security related anomalies, and presents them along the attack chain using visualizations that enable security analysts to detect them faster. It also routinely discovers, classifies, and prioritizes any device, client, or application traversing the network. Discovery and classification extend to encrypted traffic, thanks to ExtraHop's passive SSL and TLS decryption, which includes perfect forward secrecy.

**Reveal(x) automatically correlates related indicators of compromise and presents them using visualizations that enable security analysts to detect them faster.**

With Reveal(x), ExtraHop turned its focus to East/West network traffic, allowing it to detect activities along the multiple stages of an attack. In fact, the anomaly's view in the Reveal(x) user interface cleanly displays the number of anomalies classified as command and control, reconnaissance, lateral movement, and data exfiltration activities, and it provides plain English descriptions of those detected activities. Reveal(x) displays transactions that are logged in a tabular way and allows security analysts to click on individual transactions to replay a packet capture for root cause analysis. The aim is to greatly reduce the length of time it takes to detect low and slow attacks—in other words, dwell time. For most organizations, attacker dwell time before detection is measured in months.

Unlike earlier network behavior anomaly detection vendors who straddled network performance and security use cases, ExtraHop analyzes full data streams and transaction-level protocols, rather than less granular network flow data, to find anomalies. ExtraHop officials maintain that its focus on live data stream processing makes it harder for attackers to evade detection by employing tricks like turning off auditing or disabling logs because "you can't evade the wire."

To appeal to a range of security organizations that span different sizes, skillsets, and maturity levels, ExtraHop created three different Reveal(x) options. For more modest security programs, the standard edition provides network analytics, anomaly detection, global index, and search. For organizations with a formal security operations center, the premium edition adds full traffic decryption with open data integration to SIEMs or automation platforms. For the most mature security operations, the ultra-edition provides full analytics and packet capture, which require a greater amount of storage capacity.

## Context

A lot of security vendors use machine learning to detect unseen or unknown threats, and there are a variety of firms that take different approaches to gather the data and intelligence needed to analyze traffic and activity for anomalies. Security analytics providers typically come from one of three different market segments or perspectives: SIEM, anomaly detection, or predictive analytics. Reveal(x)'s underpinnings are in anomaly detection, but it draws on ExtraHop's ability to gather highly granular data from the network itself, with wire data in network industry parlance. ExtraHop does not see itself competing with SIEM vendors (or incident response vendors, for that matter), and it actually provides integration with SIEM systems. While ExtraHop does not focus on logs as a SIEM does, those vendors are moving into the security analytics market through acquisition or organic development. Given its heritage in the network monitoring and performance management arena, it competes more closely with Darktrace and Vectra Networks.

The security analytics market today is highly fragmented and ill-defined. However, at least one forecast calls for a compounded annual growth rate of 27.6 percent between 2015 and 2020, reaching $7.1 billion. How cloudy that particular crystal ball is remains to be seen. One potential factor is the level of skill required to make security analytics tools useful. ExtraHop sought to bridge that divide through the automation and visualization it built into Reveal(x).

## EMA Perspective

It's true that most security practitioners are unsatisfied with many of the legacy tools in their defense in-depth security toolbox and are looking for better approaches to detection that come with less noise. The challenge for ExtraHop is to be heard above the din of security analytics providers. What might help them is their ability to analyze wire data in real time, which they claim provides much richer insights than just session and flow-level data used in the past. For enterprises deploying encryption more broadly across their networks and more sophisticated security operations conducting advanced monitoring, Reveal(x)'s wire speed decryption and high capacity are very attractive. If they can get their foot in the door to security-initiated deals and conduct proof of concept trials, ExtraHop has a good shot at winning in competitive situations. The easier they make that exercise for prospects, the greater the opportunity to win.

**Reveal(x) represents ExtraHop's first serious foray into the security analytics market.**

Prior to the launch of Reveal(x), ExtraHop had already engaged security practitioners with free add-on packages or applications to its existing network performance management technology that address specific security use cases, such as ransomware detection. In fact, a healthy percentage of its customers have already applied its monitoring technology to detect security threats. Still, Reveal(x) represents ExtraHop's first serious foray into the security analytics market. Given the level of investment in Reveal(x) and its growing appeal as a threat detection tool, it probably won't be their last.

### About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn. 3668.020818