Brewin Dolphin Improves Security Visibility and Control with ExtraHop

Rich, contextualized data accessible by entire IT organisation

Enhanced team effectiveness and accelerated troubleshooting

Easy integration with other applications enables validation and augmentation of alerts

BREWIN DOLPHIN PLC

Founded in 1762, Brewin Dolphin PLC is one of the United Kingdom's leading wealth managers, helping clients achieve their ambitions through expert personalised financial planning and investment management advice. Listed on the London FTSE 250, the company incorporates environmental, social, and governance factors in each investment decision.

TECHNOLOGY REFRESH AND CLOUD ADOPTION HIGHLIGHT VISIBILITY NEEDS

In late 2018, Brewin Dolphin embarked on a major transformation of its network services. Over the next 3 years it replaced legacy network equipment and services across more than 40 locations.

As part of this transformation, the firm's Digital Security & Resilience team, led by Neil Beattie, launched an initiative to identify a network monitoring solution that would provide the Network and Security teams with comprehensive insight on activity across the evolving technology environment.

"

The wide range of capabilities and functionality of the ExtraHop platform are driving value across our entire technology organization.

NEIL BEATTIE
HEAD OF DIGITAL SECURITY AND RESILIENCE, BREWIN DOLPHIN PLC.

DIGGING DEEPER THAN EVER BEFORE

Following two rounds of RFP evaluations to assess available options, Neil and his team determined that ExtraHop offered the best set of solutions to meet Brewin Dolphin's network and security requirements. He recalled, "ExtraHop goes much deeper than the typical transactional reporting of traffic by analysing actual behaviours occurring across the network and on endpoints."

ExtraHop can collect data and strip out all of what Neil calls the "rubbish" information. Using full stream analysis, traffic decryption, and machine learning, ExtraHop surfaces only meaningful detections with low false positives and correlated metrics and forensic details that can then be monitored and reviewed through the unified interface.

As soon as ExtraHop was deployed, Neil knew he made a good choice when the platform detected activities resulting from a penetration test that was being conducted at the same time. "We were immediately able to see events occurring that we previously had limited visibility into," recounted Neil.

SHARING THE VALUE

Neil did not want a solution that was restricted to being used solely by the firm's Network and Security teams. He commented, "The way that ExtraHop is architected means that we've been able to make the platform accessible to colleagues across other operational teams. The wide range of capabilities and functionality of the ExtraHop platform is driving value across our entire technology function."

One of the initial objectives of the ExtraHop deployment was to establish a baseline of core network activity and create an understanding of the applications used across the company's distributed infrastructure. Building on ExtraHop's commitment to creating strong, open technical integrations, the Security team has integrated detection-related data into its SIEM platform.

The elevated visibility provided by ExtraHop also is proving to be beneficial in rectifying obscure and hard-to-detect issues. "We were having some problems with domain controllers disconnecting and our legacy infrastructure monitoring solution just wasn't picking anything up," described Neil. "However, analyzing the ExtraHop data revealed a metric that directly correlated to the drops. We set up an alert in ExtraHop, cross-referenced the information to identify the root cause, and subsequently resolved the situation."

He summarized, "We use the detailed metrics from ExtraHop to cross-check events generated by other controls across the environment. The rich, contextualized data we receive from ExtraHop enables us to be better informed and operate more effectively."

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats––before they can compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101