WIRE DATA ANALYSIS PROVES A SURE THING FOR BET365

WITH HELP FROM EXTRAHOP, BET365 IS USING INNOVATIVE WIRE DATA ANALYSIS TO IMPROVE APPLICATION DELIVERY, NETWORK PERFORMANCE AND STRENGTHEN ANTI-FRAUD DEFENCES.

Established in 2001 from a portakabin in Stoke-on-Trent, bet365 has grown into a global operation employing over 2,000 people. Operating in 17 languages it delivers its experience to over 11 million customers worldwide.

Customer numbers have consistently increased. At any one time up to two million people are connected generating thousands of updates per second. Behind the scenes the company operates critical IT systems across multiple locations using both off the shelf and custom applications, processing billions of transactions annually.

Developers and operations teams work to ensure the service is delivered while a security team continually examines systems to prevent and detect irregular activities. The IT department uses a range of management tools, tending to be an early adopter of IT innovation so as to gain a competitive edge and enhance the customer experience.

In 2012 ExtraHop were approached with a requirement to increase visibility of IT operations and to resolve some niggling challenges. Central to this was the avoidance of technology requiring additional clients, probes or that created a performance burden to the carefully tuned servers.

The requirements for a new monitoring system included spanned performance optimisation, development analysis and pervasive infrastructure monitoring and anomaly and security event detection in real time, as well as guidance for the IT team concerning anomalous behaviour.

Many monitoring tools rely on either historical logs or agents to collect performance statistics. ExtraHop's Wire Data Analytics platform monitors all L2-L7 communications, including the bi-directional payload. This network and application traffic, wire data, is the most complete source of information concerning performance, availability and security of an IT environment, whether on premise, in the cloud, virtualised or hybrid.

The Wire Data Analytics platform goes beyond passive monitoring, delivering real-time reassembly of packets into per-client transactions, flows, and sessions across a range of protocols including HTTP/S, MQ, SOAP, SQL, CIFS, LDAP and others commonly used by client server and web applications at up to 20Gbps.

By analysing Wire Data, ExtraHop provides the IT team with actionable insights into performance, availability and security of the IT estate. Starting with performance optimisation, bet365 wanted to quantify improvements or degradations in application performance attributable to patches, upgrades and development changes. Using ExtraHop they could evaluate the impact of changes across multiple parts of the application delivery chain, through linked applications, infrastructure elements and even sites.

The identification of suspicious behaviour with a record of the entire event for inspection by the security team was essential. With multiple data centres, virtualised servers and distributed architecture it was only through wire data analytics that bet365 were able to gain the high resolution view of complex trends that were previously obscured by a huge volume of disparate transaction data.

"ExtraHop is playing an important role in helping us to reduce the complexity of maintaining our network," said Neil Selby, Head of Networks and Security. Real time visibility of the transactions within our traffic, such as changes to code, failure of code or appliances and the detection of malicious traffic, can be identified without the need for time consuming, intensive manual packet capture and analysis."

A future evolution includes the ability to feed data into a complex event processing platform that helps the gambling industry manage risk and avoid fraudulent activity. Previously, funnelling data from multiple applications, locations, services and applications into this system was incredibly complex.

bet365 is now experimenting with ExtraHop to examine, rebuild and generate real-time snapshots of the entire transaction landscape that can be quickly fed into the platform. If successful, ExtraHop would replace a legacy solution that requires multiple physical servers that has struggled to keep pace with the growing workload. NC