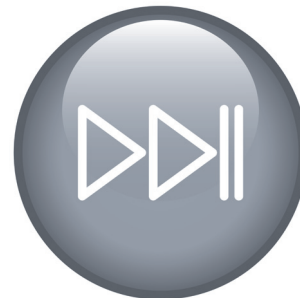


Endace Capture Replay

Capture Replay has broad application as a test tool in both the network security and trading market places. To help users with the concept, we've developed a number of use cases to illustrate how Capture Replay systems can be used to help organisations better understand their technology environments.



NETWORK SECURITY

Today's network intruders and attackers come from both outside and inside the network, so having the right defence tools in the right place is essential. But how do you know whether the network defences you're using are doing their job? There are a number of things to consider including rules and whether or not the system can cope with the levels of throughput traversing the network. Having the best rule set in the world is pointless if it only gets presented with a sample of the traffic.

One way to solve the problem is to ask the vendor what the throughput is and believe them. The right thing to do, however, is to test it yourself using your own network traffic. Endace Capture Replay Systems can be used to work out exactly how much throughput a network security system can handle before it fails. What's critical is that you're using your own traffic rather than synthetic traffic to do the test.

Step 1: Record some network traffic – say five minutes' worth of ordinary standard network traffic.

Step 2: Set up the system that you want to test with a standard rule set.

Step 3: Replay the captured traffic through your desired system at a relatively low bit rate – 0.5Mb/s and note the number of events that are triggered by the system (the assumption is that at 0.5Mb/s the detection engine will see every packet and have the opportunity to alert on it).

Step 4: Replay the traffic, increasing the speed by 100Mb/s in each pass and noting the number of events that the system alerts on each time. Compare the results to the original test. At the point in which the system shows up a smaller number of alerts than the original test, the system is deemed to have reached its point of saturation. Compare this throughput to the vendor's stated performance throughput.

Step 5: Compare the breaking point to your current traffic throughput and then factor in traffic spikes, growth in network traffic and anything else that might be important in the equation. If you're considering buying a network security system, it's vital that it can handle today's load and future loading.

endace.com | info@endace.com

Endace Limited

Level 2, Building A. 600 Great South Road
Ellerslie, Auckland 1051, New Zealand
Phone +64 9 582 0360

Endace USA Limited

14425 Penrose Place, Suite 225
Chantilly, VA 20151, USA
Phone (toll free): 800 572 0557
Phone: +1 703 378 0601

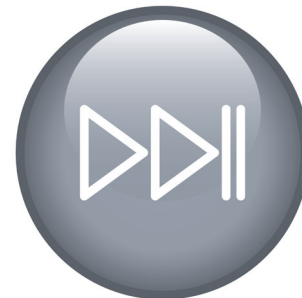
Endace Europe Limited

Davidson House, Forbury Square
Reading, Berkshire, RG1 3EU, UK
Phone +44 118 900 1425



Endace Capture Replay

Capture Replay has broad application as a test tool in both the network security and trading market places. To help users with the concept, we've developed a number of use cases to illustrate how Capture Replay systems can be used to help organisations better understand their technology environments.



ENDACE CAPTURE REPLAY FOR TRADERS

Infrastructure stress testing

If you suspect your infrastructure may have issues, Endace Capture Replay Systems are ideal for real-world stress testing of critical trading systems. Using the Endace system, you can determine the maximum throughput capability for any system based on your own unique traffic fingerprint.

Back testing

Something went wrong yesterday in your trading algorithms, but you're not really sure what. Some subtle interactions and delays occurred along the trading feed path. Because you've been monitoring and capturing your incoming market feeds with your Endace Capture Replay System, you discovered some 'very odd behaviour' in one of your feed handlers. Being confident that the exact sequence and inter-packet timing of the incoming feed was replicated accurately, you're able to implement a minor change to the feed handler's routing algorithm and, voilà — problem solved. You play the traffic back again and the old algorithm now works just fine.

Algorithm development

To see whether or not there are any anomalies in the algorithms of your trading feeds, you can put your Endace Capture Replay System into playback mode and review yesterday's market data at a faster rate. By systematically varying the playback speed, in small increments, either up or down, you can test the algorithm's ability to scale to higher traffic loads and study how the algorithm and the rest of the trading platform perform.

New marketing development

Your firm is expanding its algorithmic trading business to a new stock market. You'd like to go live as soon as possible, but the costs and timescales for deploying a full low-latency trading environment in the co-location facility adjacent to the exchange are simply too high. So, you put your Endace Capture Replay System into playback mode and select 'typical' days to replay at 100% accurate replay rate. You play the daily trading feeds back-to-back at double their normal bandwidth, accurately pushing four weeks of data through your new infrastructure in only three days' time. You can now go live at your new venue, and rest easy, knowing the new infrastructure has been thoroughly tested using live data.

