Boost Your Security Analytics Performance

The new Dell R640 SA server cuts search times by up to half.

April 2022

Incident response and threat hunting searches through terabytes of stored packet and metadata require significant CPU resources. That's why previous SA servers have included 40 (s500) and 48 (Dell R730) cores. Even so, CPU resources have continued to be the limiting factor for end-user response times during analysis tasks.

The new Dell R640 SA server's two Intel Xeon Gold CPUs provide more than double the CPU horsepower with 104 cores allowing it to complete analytics requests in as little as half the time taken by older servers.

How We Tested

Platforms

1. Our legacy SA Sensor was a **Dell R730** with **48 cores** and 40 TB of internal storage running SA v8.2.5.

2. The new SA Sensor was a **Dell R640** with **104 cores**. It was attached to one 144TB storage array and two 144TB JBODs for a total of 432 TB external storage and was also running SA v8.2.5.

Capture Traffic and Load

Both servers were capturing the same PCAP tcpreplay traffic during the tests on 3 interfaces with steady rates of 500Mbps, 100Mbps, and 1Mbps. Each server's storage was populated with the same traffic over more than one week.

The Test

The test was an automated request for all data related to 13 metadata elements: application_group, application_group_time, filename, file_type, mime_type, web_query, file_extension, user_agent, http_method, ipv4_initiator, ipv4_responder, ipv4_conversation, and vlan_id.

Query time ranges included 15 minutes, 1 hour, 5 hours, 24 hours, and 7 days.

Each test was sent to both SA servers simultaneously so the servers are responding under the same capture and indexing load.

We ran each test up to 25 times per time range to achieve reliable averages.

Results

The benefits of the additional Dell R640 CPU resources range from 8-56%, increasing as your search size increases. They suggest all incident response and threat hunting task response times will improve, with some cut by more than half.

Query Time Range	Search Size	Duration (seconds) Dell R730	Duration (seconds) Dell R640	Improvement
15 minutes	57 GB	27.7	25.5	8.1%
1 hour	228 GB	43.4	35.1	19.2%
5 hours	1.11 TB	122.1	75.2	38.4%
24 hours	5.32 TB	529.5	262.2	50.5%
7 days	37.26 TB	2754.9	1218.9	55.8%

These results are based on our realistic test workloads. We recommend you perform your own measurements to better understand the application of these results to your environment.

In other words, your mileage may vary.