ACCESSDATA

CASE STUDY

Fortune 500® Utilities Company: Processing over a Terabyte of Complex Data in 12 Hours

A major utilities company has 150 locations throughout its region of service. In previous years, the organization was using FTK® and EnCase® Forensic, relying on these stand-alone tools to address internal investigations and e-discovery. With caseload growing year over year, the company saw the need to explore options to improve its computer forensics and e-discovery capabilities.

Typically, the company sees one new computer forensics case a week, with data sets ranging in size from 80GB to 500GB.

E-discovery matters typically involve 12GB of email and a total of 5TB of data. Knowing these volumes will only trend upward, the organization's information security operations team launched an initiative to dramatically increase the speed with which they are able to process and index data.

In particular, the goal was to get a better handle on computer forensics caseload, which requires a much deeper level of processing than an e-discovery matter would require.

The Solution

Given the sheer processing speed, ease of use and innovative capabilities of AccessData® technology, the decision was made to adopt AD Enterprise and AD eDiscovery®. These solutions are built on Forensic Toolkit® technology and allow processing to be distributed among four "workers," enabling investigators to move into the analysis phase faster. However, processing performance is also dependent on hardware capabilities, such as disk I/O. As there are virtually innumerable ways in which to configure distributed processing with AccessData technology, the AccessData Technical Account Manager team was asked to assist the utilities company in tailoring the architecture to fit its needs.

Testing was rigorous to ensure the most reliable results. One test data set when compressed filled a terabyte drive and had close to 13 million items.

Full forensic-level processing refers to the processing actions selected in the Additional Analysis processing refinement pane within AD Enterprise. In this case, all actions were selected except Optical Character Recognition and Cerberus malware analysis.

AD Enterprise Additional Analysis selection screen showing the full depth of processing options available in nearly all AccessData technology.

> "With our current setup, we're able to keep up with caseloads very well. We can get eyes on the case faster than ever before ..."
>
> —Member of the Information Security Operations Team

Results

Before implementing AD Enterprise and the new architecture, it typically took six days to forensically process a terabyte of complex data. Now, this Fortune 500 utilities company is able to perform full forensic-level processing on data sets of that size and complexity, including carving and indexing, in just 12 hours. "The only reason we were able to do this is because of the AccessData Technical Account Manager experts who came out to assist us," claimed a member of the Information Security Operations team. In addition, he explained that this would not be possible with other computer forensics solutions. "AccessData technology absolutely helped. With our current setup we're able to keep up with caseload very well. We can get eyes on the case faster than ever before ... much more time doing and lot less time waiting."

Hardware Infrastructure

The infrastructure employed to support the improvements in the company's processing and investigative capabilities includes four servers and a network attached storage (NAS) device. AD Enterprise provides for the use of four distributed processing engines working in unison to handle nearly any volume of data. The inclusion of a NAS device, while not required, can improve the rate at which evidence can be accessed and sent to the processing engine(s).

AD Enterprise Processing Summary

Items Enumerated (Identified):
12,678,306

Total Processing Job time:
8:46:13A.M. – 8:23:02P.M. = 11:36:49 (hh:mm:ss)

ACCESSDATA®

Whether it's for investigation, litigation or compliance, AccessData® offers industry-leading solutions that put the power of forensics in your hands. For 30 years, AccessData has worked with more than 130,000 clients in law enforcement, government agencies, corporations and law firms around the world to understand and focus on their unique collection-to-analysis needs. The result? Products that empower faster results, better insights, and more connectivity. For more information, visit www.accessdata.com

Visit us online:
www.accessdata.com

Global Headquarters
+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales
+44 20 7010 7800
internationalsales@accessdata.com