Ochsner Health System has grown to over 40 remote clinics and 9 hospitals, comprising close to 20 thousand end-points. With an enterprise this size, scalability was a big factor in a forensic/incident response tool. With ProDiscover Incident Response (IR), Ochsner cybersecurity has the ability to push a remote agent from a central forensic server and conduct live analysis on remote systems, which includes memory (including the acquisition of a complete memory image), processes, ports/connections, registry keys, and other important artifacts, quickly and efficiently. Once malicious processes and executables are discovered and identified, they can be searched for and prevented from further entering our end-points and enterprise, providing us a cyber "kill chain." Finally, Ochsner Health System is under various regulatory requirements, such as HIPAA and PCI, so remote acquisition of hard drives is an important part of Ochsner's eDiscovery and litigation support program. I highly recommend ProDiscover Incident Response, as ProDiscover products have been an important part of our forensic/incident response toolkit for over 10 years.

Mark Maher
Information Security Officer
Ochsner Health System