

Metascan® Customer Snapshot

Computer Crime Investigation Team

About the Customer

Computer crime is an unfortunate artifact of today's wired and global society, as individuals involved in criminal behavior have embraced technology as a method for improving or extending their criminal tradecraft. One Metascan customer is a prominent but secretive research team that tackles the issue of computer crime by focusing on critical gaps in the field of information security that are not addressed by commercial tools or standard computer forensic techniques. Commonly supporting law enforcement, the organization performs important work in computer triage and examinations, handling a daunting backlog of computers used by criminals for every aspect of criminal activity. Detecting, identifying and understanding malware discovered on criminal machines is a critical function for this customer.



Customer Challenges

One major challenge for the customer's research staff is the inevitable booking-up of schedules, demanding deadlines and time commitments that continue months and years into the future for the growing and seemingly unending volume of triage work. On average, the organization requires from one to three days for its researchers to manually analyze one individual computer for malware. Considering the enormous backlog of computers awaiting triage, malicious code detection represents a very time consuming, expensive, and necessary part of the forensic process. A key initiative for this customer was to find a technical solution able to replace the slow, human-error-prone manual malware detection process with a device able to scan computers faster, more efficiently, more reliably and in an automated fashion not possible with the "one-computer-at-a-time" manual process.

OPSWAT's Solution

OPSWAT's Metascan Ultra was selected by the organization because it offers 8 powerful antivirus engines as a standard feature, and can support as many as 30 **built-in antivirus engines**. The customer chose to add additional antivirus engines, including U.S. Government DoD and NIST certified solutions, to improve the likelihood that any malware threat missed by one engine would be detected by the other engines in the Metascan Ultra deployment.

Results

The customer's triage of one individual computer previously required from one to three days of scanning time and demanded countless man-hours for handling, managing and controlling the manual process. This scanning can now be effortlessly accomplished by Metascan Ultra in minutes or hours in a reliable, consistent, and fully-automated fashion that requires no human intervention.

For more information please contact sales@opswat.com.