Different fields of digital forensics require various tools, but these tools assist in completing a focused task as optimally as possible, says Nicholas Logan.

Digital forensics is just one of many fields that have posed the question, "Is there a tool that provides universal functionality?" There are multipurpose tools, but there will be situations that cannot be handled by a single tool.

The analysis of petabytes of data in real time, and the use of mobile devices, are just two examples of unforeseen situations to which digital forensics has had to adapt. Though the use of one tool that applies itself to any situation would no doubt seem convenient, it could not possibly account for these types of unforeseen advancements. Furthermore, multipurpose products could burden users with many tools they may never have cause to use, as different fields of digital forensics place a vast range of requirements on the tools being used.

Approach each of these product purchases with a clear understanding of needs and the functionality that the product offers.

Mandiant Intelligent Response v1.4.5

Vendor	Mandiant
Price	$86,000
Contact	www.mandiant.com

Mandiant Intelligent Response (MIR) is a powerful incident response investigation and evidence collection tool. It is designed by and for incident responders to collect evidence from possibly compromised machines anywhere in a company's network. Even though it is not an end-to-end forensic investigation tool, it offers investigators exceptional information to help in their searches.

The installation of the MIR box is fairly easy. It consists of three parts: the agents (sensors on specified devices for monitoring), the controller (the information gathering center), and the consoles (user interfaces).

The MIR worked well in our simulated company environment. All from one location, it is capable of gathering everything an investigator would need should a system become compromised. It has a generous amount of storage space, but its memory is limited to that of the workstation on which it is being used. Most importantly, it encrypts the information both in transit and in storage and collects it in a forensically sound manner capable of withstanding courtroom scrutiny.

Documentation is supplied on a CD along with the agent installation. The administrator's guide is flawless, and the same can be said for the user's guide.

Mandiant offers 24/7/365 phone, email and web support, and there also is a user forum.

There is no doubt that the Mandiant Intelligent Response appliance is expensive, but for large companies, its performance is well worth the price. The value of quickly and thoroughly investigating an incident before it becomes overwhelming certainly outweighs the cost of this device. We find that the product is a good value given its purpose and the competent way it addresses it.

SC MAGAZINE RATING

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★☆
OVERALL RATING	★★★★★

Strengths Collects everything an investigator needs for solid incident response.
Weaknesses RAM is limited to what the console workstation possesses.
Verdict Exceptional incident response platform with solid forensic applications. Recommended.

MANDIANT®

Mandiant
1 (800) 647-7020
info@mandiant.com
www.mandiant.com

SC MAGAZINE Reprints

Exceptional incident response platform with solid forensic applications. Recommended.

Nicholas Logan