



## INTELLIGENT RESPONSE

HOW THE ENTERPRISE SOLVES COMPUTER SECURITY INCIDENTS

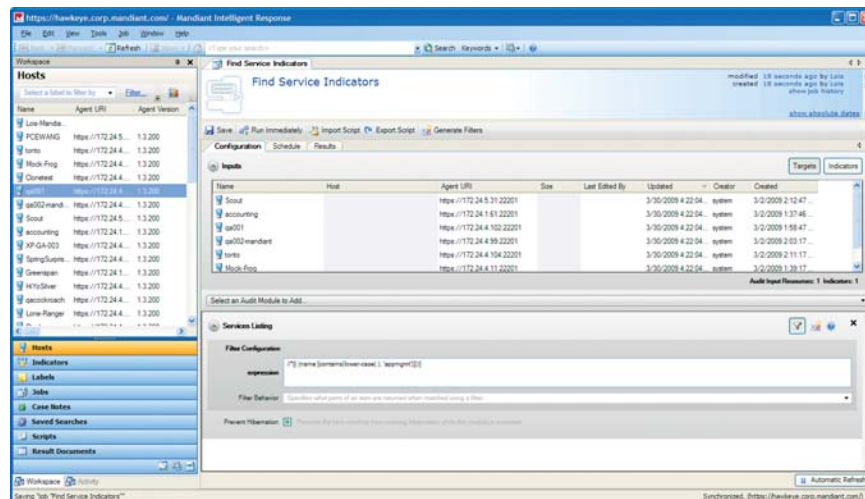
**MANDIANT Intelligent Response™ (MIR)** is the industry's first enterprise-grade incident response solution. MIR can perform complex inspection of each system in an enterprise, looking for hundreds of specific indicators of compromise with the simple push of a button, eliminating the need for expensive manual review. MIR's data collection options range from collecting a single registry key to performing full forensic images of hard drives and live memory, all across the network. You can search your enterprise and only collect data when specific conditions are met.



### WHY MIR?

MIR saves organizations time and money by making incident response faster and more cost-effective. A single responder using MIR can do in hours what used to take an entire team several days.

- Save time and money
- Lower risk when preventative security measures fail
- Follow a forensically-sound methodology
- Collect data in a precision-strike manner
- Detect compromises that anti-malware and anti-virus programs cannot
- Collaborate among multiple users
- Respond to the incident at the enterprise level
- Enjoy a simple licensing structure
  - Unlimited agents
  - Unlimited user seats
  - Simultaneous agent connections



# ARCHITECTURE

## IDENTIFY

- Search across all of your systems
- Locate indicators of compromise quickly
- Find information responsive to legal inquiry
- Perform precision-strike data collection

## COLLECT

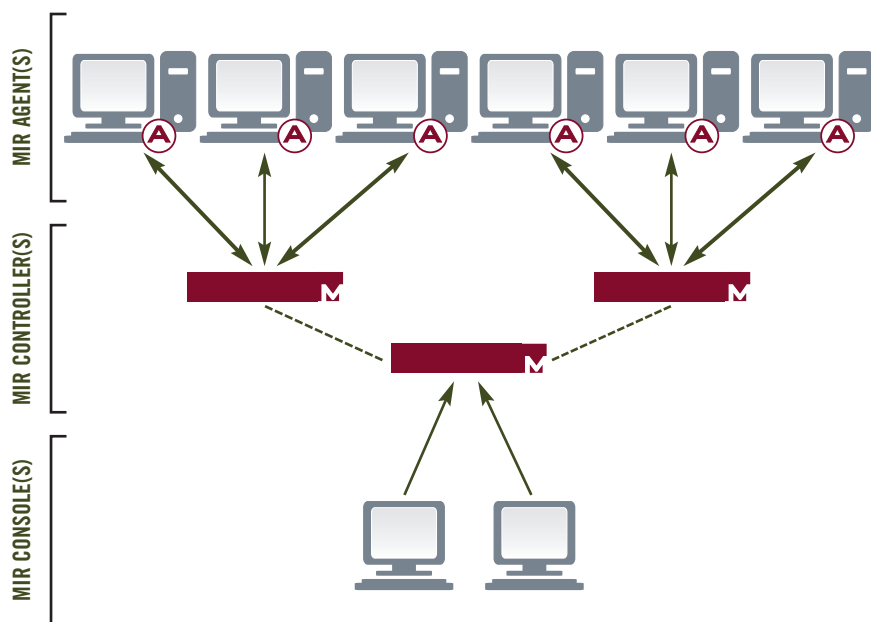
- Live system state
- Live memory forensics
- Active and deleted files
- Drive images
- Process and port listings
- Registry entries
- System and process memory

## ANALYZE

- Conduct indexed search of collected data
- Sort, filter and annotate data on the fly
- Perform relational analysis on acquired data
- Compare files against known hashes and checksums

## REPORT

- Create reports in a shared workspace
- Link directly to acquired data, analyses and annotations
- Export all data and reports in a common industry formats



# PRODUCT SPECIFICATIONS

## AGENT

### Supported Operating Systems

- Microsoft Windows XP Professional SP3 (32-bit)
- Microsoft Windows Server 2003 SP2 (32-bit)
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows 2000 Server SP4

### Coming Soon

- Microsoft Windows Server 2003 SP2 (64-bit)
- Microsoft Windows Vista SP1 (32-bit)

### Footprint

- 4.0 MB Installer
- 11.7 MB on disk

### Security

- Silent installation, no reboot required
- SSL encrypted network communications
- Configurable port numbers
- Service can be renamed to obscure it

## CONTROLLER

### Power Requirements

- AC: 100/240V, 8.5A (50-60 Hz)
- Dual power supplies

### Dimensions

- Chassis: 2U rack height
- Weight: 60 lbs (27 kg)
- Height: 3.375 in (8.59 cm)
- Width: 19.00 in (48.26 cm)
- Depth: 21.00 in (53.34 cm)
- Standard 19" rack-mountable
- Extending rack rails included

### Storage

- High performance hardware RAID 5 array
- About 2 TB usable storage

### Network Interfaces

- Two 10/100/1000 Ethernet interfaces

### Other Interfaces

- Three IEEE 1394a interfaces
- Two USB 2.0 interfaces
- Front-panel LCD & controls
- Dual, redundant, hot swappable power supplies

### Environmental

- Operating temperature 32°F to 122°F (0°C to 50°C)

### Security

- Encrypted network communications
- Internal public-key infrastructure
- 2048-bit or greater keys
- 3DES, RC4, AES128/256 encryption

## CONSOLE

### Supported Operating Systems

- Microsoft Windows XP Professional SP2 or higher (32-bit)
- Microsoft Windows Vista

### Security

- SSL encrypted network communications to Controller

To learn more about MANDIANT or to schedule a demonstration of MANDIANT Intelligent Response, contact us at +1 703 683 3141 or [info@mandiant.com](mailto:info@mandiant.com).