

MANDIANT INTELLIGENT RESPONSE FEATURES & BENEFITS

	FEATURE	FUNCTION/BENEFIT
DATA ACQUISITION	DELETED & UNDELETED FILES	Deleted or undeleted file contents and file listings, in addition to relevant metadata — including file length, device ID, file mode, time stamps, reference count, disk block pointers, file naming criteria, username, groupname, security identifier (SID), SID type, last login date/time, “disabled” status, “locked out” status, user password age, PEChecksum, BaseAddress, PTimeStamp, PESubsystem, Exports (ExportsTimeStamp, NumberOfFunctions, NumberOfNames & ExportedFunctions — ArrayOfString), ExtraneousBytes and EpJumpCodes (Depth & Opcodes) can be acquired via raw disk access and file table structure parsing on NTFS and FAT32 filesystems.
	EVENT LOG ENTRY/FILE	Event log entries — including description, date, time, user, computer, event ID, source, type and category — can be acquired via raw disk access and Windows API.
	HOST CONFIGURATION DATA	Host configuration data — including host name, network interface configurations, amount of memory, processor type(s), and BIOS data — can be acquired via Windows API.
	IN-MEMORY DRIVERS	Drivers in memory can be identified via context free searches through memory blocks representing driver objects, and/or a linked list of drivers to potentially identify hidden drivers.
	LOGICAL/PHYSICAL DISK IMAGE	DD-compatible logical or physical disk image(s) can be acquired and stored in Advanced Forensics Format (AFF) containers — an extensible, open format for disk image storage.
	NETWORK PORT STATUS	The network ports list — including port number, port state, protocol, IP connection information, associated process(es), and associated executable(s) — can be acquired via Windows API.
	REGISTRY DATA	Registry entries (and specific sub-keys) — including registry class, registry name, type, value data and binary value data — can be acquired for currently logged-in users.
	RUNNING PROCESSES	Running process list, in addition to its relevant metadata, including start time, run time, elapsed time, path to executable, command line executed with parameters, process ID (PID), username, groupname, security identifier (SID), SID type, last login date/time, “disabled” status, “locked out” status, and user password age can be acquired via Windows API and/or memory process listing from both live memory and memory files by specifying either the process name(s) and/or PID(s). (Note: items 7-14 are solely acquired via Windows API, not memory process listing.)
	RUNNING SERVICES	The running service list — including mode, process ID, status, name, description, type, path to executable, start-up parameters, and service originator — can be acquired via Windows API and/or direct memory access.
	SCHEDULED DATA ACQUISITION	Users can edit recurring schedules and custom event queues, particularly valuable when data must be acquired from a large number of hosts.
	SCHEDULED TASKS	Scheduled task listings — including job name, path to executable, job comments, command line options, and job privilege level — can be acquired via raw disk access, and is helpful in identifying batch files or Windows scripts installed to regularly conduct malicious activities.
	USER DATA	User information related to accounts within the Guest, Administrator, User, and Power User account groups can be acquired via Windows API.
VOLATILE MEMORY	A system memory image, along with relevant metadata — including running processes, executable pages (i.e. “code” for a running process), open process handles, open network ports, and loaded DLL files — can be acquired and parsed.	

MANDIANT INTELLIGENT RESPONSE FEATURES & BENEFITS (CONTINUED)

	FEATURE	FUNCTION/BENEFIT
AGENT ARCHITECTURE	AGENT AUTHENTICATED REGISTRATION SERVICE	“Call-in” registration with a centralized discovery service using strong certificate authentication enables users to conduct trusted searches for any and all agents, regardless of IP lease. Searches can also be conducted on an individual IP or range of IPs for agent identification.
	FLEXIBLE LOADING MECHANISMS	Can be loaded from a network share, removable read/write media, or removable read-only media.
	LOADED DLL AUTHENTICATION	DLL code validation before execution prevents injection of malicious/untrusted code.
	MODULAR AGENT PLATFORM DESIGN	Modular design enables parallel module execution to invoke data gathering/writing/processing jobs on multiple agents.
	SELF-SIGNED SSL CERTIFICATES	SSL-encrypted XML over HTTP connections are validated against pre-installed trust chains and certificate revocation lists to ensure data integrity and confidentiality.
	TAMPER-RESISTANT AGENT	Industry-standard code de-compilation techniques inhibit low-level agent analysis.
	TRUSTED AGENT INSTALL	Authenticode-signed installer enables immediate agent execution/availability.
	VARIED SOFTWARE DEPLOYMENT SUPPORT	Installation in headless mode via Windows Installer 3.1, Microsoft Systems Management Server (SMS), Microsoft Active Directory or local control panel/command line.
	VARYING RUNTIME MODES	Agents can be run interactively from the command line, as an invoked daemon or as a persistent installed service.
	WINDOWS PLATFORM SUPPORT	Can be installed on Windows 2000 SP4, Windows Server 2003 SP2 and Windows XP SP2.
DATA ANALYSIS	ADVANCED DATA COLLECTION CAPABILITIES	Data collection capabilities enable customizable job creation via client initialization scripts, audit scripts and analysis scripts.
	BOOKMARK FUNCTIONALITY	User search queries/terms can be saved as persistent system objects, creating a familiar bookmarked search or “search folder” experience.
	CASE-ORIENTED GUI & WORKFLOW	A flexible GUI expedites identification, collection and analysis of data by joining a myriad of data objects — for example, hosts, acquisitions, jobs, job results, analysis and saved searches — with individual or multiple cases.
	COMMON CONTENT-TYPE HEX VIEWER	Common graphics formats, such as gif, jpg, and tiff, and plain-text files can be viewed via an embedded hex viewer, enabling search for embedded malicious code within otherwise harmless files.
	DATA OBJECT EXPORTING	Multiple data objects can be exported to local data stores in a variety of XML formats. Acquired disk images can be exported from AFF containers.
	DATA OBJECT LABELING	Data objects and data object views can be multi-labeled to provide context for subsequent analysis/evaluation.
	ENVIRONMENTAL VARIABLE SUPPORT	File auditors can now expand Environment Variables allowing the user to, for instance, replace the potentially inaccurate “C:\Windows” with “%SYSTEMROOT%”, making audits more generic.
	FILE VARIANCE ANALYTICS	Ability to compare two “same-type” acquisitions acquired in different ways — for example, API acquisitions vs. raw disk acquisitions — delivers visibility into variance, which is critical when searching for potentially compromised hosts.
	TIMELINE NORMALIZATION	Acquired datasets can be overlaid and time-normalized, reducing time spent determining varying date/time stamps from disparate datasets to understand how multi-faceted events transpired.

MANDIANT INTELLIGENT RESPONSE FEATURES & BENEFITS (CONTINUED)

	FEATURE	FUNCTION/BENEFIT	
COLLABORATION	COLLABORATIVE WORKSPACE	Multi-user consolidated HTML-enabled workspaces enable dispersed investigators to simultaneously develop and share case notes on individual data objects and data object views, accelerating analysis.	
	URI-BASED OBJECT REFERENCING	Data objects and data object views can be referenced via URI, facilitating sharing of relevant data within case notes and via external mechanisms such as e-mail, instant messaging and word processing applications.	
	ASCII & UTF-8 SUPPORT	ASCII or UTF-8-encoded data can be extracted and indexed from audit results or bin-image — for example, acquired files from a target system — content.	
CONTROLLER ARCHITECTURE	CONTROLLER FIELD UPGRADE	Controllers can be field upgraded via read-only media — such as a DVD — inserted directly into a Controller, and/or network-based services.	
	FASTER INDEXING & SEARCHING	Enhancements to indexing and search capabilities expedite a user's ability to search acquired data across a large number of hosts.	
	INDEXING RECOVERY MECHANISM	Data indexing automatically restarts if a controller's indexer shuts down or crashes. Acquired data previously scheduled for indexing remains prioritized for indexing.	
	INTUITIVE BACK-UP/RESTORE FUNCTIONALITY	All user-created data, including audits, audit results, jobs, acquired content and user-defined scripts can be backed up using rsync to a target NFS-mounted share, or to a separate network-accessible data store via SSH.	
	MODULAR ANALYSIS ENGINE	Enables rapid development of analysis modules designed to solve new customer problems without having to re-build the entire platform; third parties or customers may potentially also develop extension modules.	
	NETWORK BANDWIDTH THROTTLING	Administrative users can throttle MIR network bandwidth. Connections can be prioritized by class, where class is port, content, etc.	
	USER ACTIVITY LOG	All user activity — such as identity, date/time of event, user location, specific operation(s), target(s), and results — are maintained in a “live” container, which records and outputs log information as it happens, and within exportable plain-text logs.	
	SECURITY	ADMINISTRATIVE USER DESIGNATION	Multiple users can be assigned with the privilege of performing system maintenance, archiving/deleting data, administering users and resetting passwords.
		USER AUTHORIZATION	Authenticated user functionality limited by role-based access control (RBAC) authorization mechanisms (administrator vs. non-administrator), including read/write access to data objects, and ability to collect data from designated host(s).
USER INTERFACE	“OUTLOOK”-LIKE USER INTERFACE	Windows-based console delivers familiar “look and feel” application access.	
	UI “DRAG AND DROP” FUNCTIONALITY	A flexible user interface enables custom screen layouts to be created per desired workflow.	