

AD Enterprise 3



What's New in AD Enterprise?

Additional Encryption Support:

- Supports popular encryption technologies, such as Credant, SafeBoot, Utimaco, EFS, PGP, Guardian Edge, Sophos Enterprise and S/MIME.

Live Memory Search:

This is the industry's first enterprise investigative platform to enable advanced agent-side search of memory on nodes across the network. In addition, it is the first and only commercial product of its kind to enable the remote search and analysis of live memory on both 32-bit and 64-bit Windows machines. You can scan thousands of nodes looking for strings/keywords in memory, review the results in context, such as the associated processes, dlls or unallocated, along with locations containing the hit(s), and export the responsive exe/dlls/unallocated for further analysis.

- Memory search and analysis of live Windows machines
- Process- and DLL-specific live memory searching
- Right-click memory search hit view and dumping from the Volatile tab
- Memory analysis is performed by the agent itself
- The agent holds strings/keywords provided by the examiner, which are identified in memory, and the results — the associated processes/dlls/unallocated and locations — are sent back to the examiner for further action.
- The examiner can investigate the results, and if the event is found to be real, the investigator can acquire the entire memory or carve out the individual files for further analysis on the examiner's workstation.
 - o acquire just the process
 - o acquire just the dll
 - o acquire the process and all the supporting dlls
 - o acquire a chunk of unallocated containing the hit
- All live memory analysis is available via the "Check In" feature. (See below.)

Check In:

Securely investigate (capture and analyze) data from machines, wherever they might be, from a network perspective. Whether the machine is at a coffee shop or a home office, Check In gives you the ability to securely capture data without waiting for the node to be active on the organization's network.

- Designed to support organizations with strict security policies, utilizing a drone proxy intermediary.
- Agent has a lot of flexibility in how Check In operates (frequency, time between check ins, where the check in happens, how long it tries to check in, on/off).
- Management server keeps track of machines that have checked in.
- Examiners define policies/rules for a given node, which are then consumed by the drone proxy. When an agent checks in, the operation is performed by the drone proxy and then automatically brought back to the examiner for analysis.
- Check In supports:
 - o Physical and Logical disk acquisition with resumption
 - o Memory acquisition
 - o Memory analysis
 - o Volatile data capture (processes, dlls, network sockets, logged on users, network shares, open files, services, drivers)
 - o Live memory search

