AccessData® Enterprise for Network Forensics and Incident Response

AccessData® Enterprise takes network-enabled digital investigations to the next level. Built on our industry-standard, court-validated Forensic Toolkit® technology, AD Enterprise delivers state-of-the-art incident response capabilities, deep dive analysis of both volatile and static data, as well as superior threat detection capabilities – all within an easy-to-use interface. A role-based permission system, an intuitive incident response console, secure batch remediation capabilities, unsurpassed searching and filtering, and comprehensive logging and reporting are just a few of the reasons AD Enterprise is quickly being adopted by Fortune 500 companies.

Product DETAILS >

A Secure Network Forensics Software Solution and FIPS 140-2 Certified

- To ensure that inter-component communication is secure, and that only authorized entities can communicate with the Agent, industry-standard x509 certificates and a FIPS 140-2 certified SSL encryption engine are leveraged.
- Control access by defining on a user basis which type of investigative operation can be performed and on which nodes (i.e. RAM capture, device acquisition, remediation, etc.).
- Track all administrative operations, such as user creation and modification, role creation and modification, and all network tree modifications.
- Keep detailed logs, on a user basis, of investigative operations, such as RAM acquisition, device imaging, volatile data capture, device previewing, device search and file copying.

Powerful Incident Response Software, Including Deep Analysis of All Live Processes

- The ONLY commercial enterprise investigations solution to enable the analysis of volatile memory on both 32-bit and 64-bit Windows operating systems.
- Advanced agent-side search and analysis of live memory on Windows machines across the enterprise.
- Correlate static forensic data and volatile incident response data within the same interface.
- Incident response console enables rapid review and analysis of key volatile data

elements in an easy-to-use format with "360-degree" <u>views of data across machines and across time.</u>

- Integrated analysis and forensic collection of network shares.
- Right click process kill during an IR investigation.
- GUI-integrated, secure remediation.
- <u>Batch Remediation</u> allows authorized personnel to automatically remediate threats on multiple machines at the same time, which is critical to preventing widespread damage due to fast-proliferating threats.

The Most Comprehensive and Efficient Digital Investigation of Data across the Enterprise

- <u>Distributed Processing.</u>
- Active directory and ePO integration enable quick identification and selection of nodes.
- The industry's first one-click acquisition of hard drives, RAM and volatile data.
- Automated Batch Acquisition of devices and RAM to streamline large multi-node evidence collections.
- Thorough data capture includes individual files, deleted files, unallocated space and logical volumes.
- Easy-to-use data processing wizard that automatically categorizes, indexes and exposes data.
- Search and collect from network shares.
- Market-leading <u>decryption, password recovery and cracking technology.</u>

Ease of Use, Stability and Process-oriented Workflow

- Conduct secure digital investigations on multiple machines across your network from a central location.
- Web-based management server enforces granular role-based cyber security.
- Rich, wizard-driven reporting on static and volatile data, making it easy to share information and generate meaningful reports.
- Agent Resource and Bandwidth Throttling allows you to define low, medium and high to determine how much CPU and bandwidth is used during investigative operations, where low is super stealth and high is for speed.
- Users are not confined to proprietary technology: AD Enterprise supports EnCase evidence files, AD evidence files, DD and more. In addition, there is no need to learn a proprietary scripting language. All functionality is in the GUI.
- Oracle database backend allows you to handle massive data sets, delivering case management, metadata storage and robust data manipulation capabilities.
- True Auto Save/Recovery functionality in the event of a failure.
- Forensically sound and court-validated technology.
- The AccessData Intelligent Agent is modular, meaning you do not have to uninstall and reinstall a new agent when you upgrade functionality.

Contact

Request Information

Brochures

- AD Enterprise Brochure
- What's New in Enterprise 3
- AD Enterprise Appliance
- AD Enterprise for ePO User
- AD Legal Brief

White Papers

- Enterprise System Security Overview
- AccessData Technology: Real-World Application
- LEGAL JOURNAL: The Rules of Evidence and AccessData Technology
- The Importance of Memory Search and Analysis
- The Importance of Integrating Host and Network Forensics
- Incident Response: Speed is the Difference

Product Webinars

- AccessData Enterprise: Detection, Analysis and Remediation

Easy-to-use Incident Response Console >

[Differential volatile data display >](#)

[Secure Batch Remediation functionality >](#)

[Go To Top »](#)

Products

- [Forensic Toolkit](#)
- [AD Enterprise](#)
- [AD eDiscovery](#)
- [AD Summation iBlaze](#)
- [AD Summation Enterprise](#)
- [AD Summation CaseVantage](#)
- [CIRT](#)
- [SilentRunner Sentinel](#)
- [AD Lab](#)
- [Mobile Phone Examiner Plus](#)
- [Distributed Network Attack](#)
- [Password Recovery Toolkit](#)

Support

- [AD Downloads](#)
- [Previous Releases](#)
- [Discussion Forum](#)
- [Technical Papers](#)

Resource Library

- [Brochures](#)
- [White Papers](#)
- [Webinars](#)

Training

- [AccessData Bootcamp](#)
- [AccessData Forensics](#)
- [Windows Forensics 7](#)
- [FTK 3 Transition Day](#)
- [Applied Decryption](#)
- [Internet Forensics](#)
- [Windows Forensics – XP](#)
- [Windows Forensics – Vista](#)
- [Windows Forensics – Registry](#)
- [Mobile Forensics 101](#)
- [Mobile Forensics 202](#)
- [Mobile Forensics 303](#)
- [MORE](#)

Contact Us

- [Americas/Asia Pacific](#)
- [Europe/Middle East/Africa](#)
- [Summation Software Support](#)
- [eDiscovery/Litigation Support Services](#)
- [Discovery Cracker Support](#)