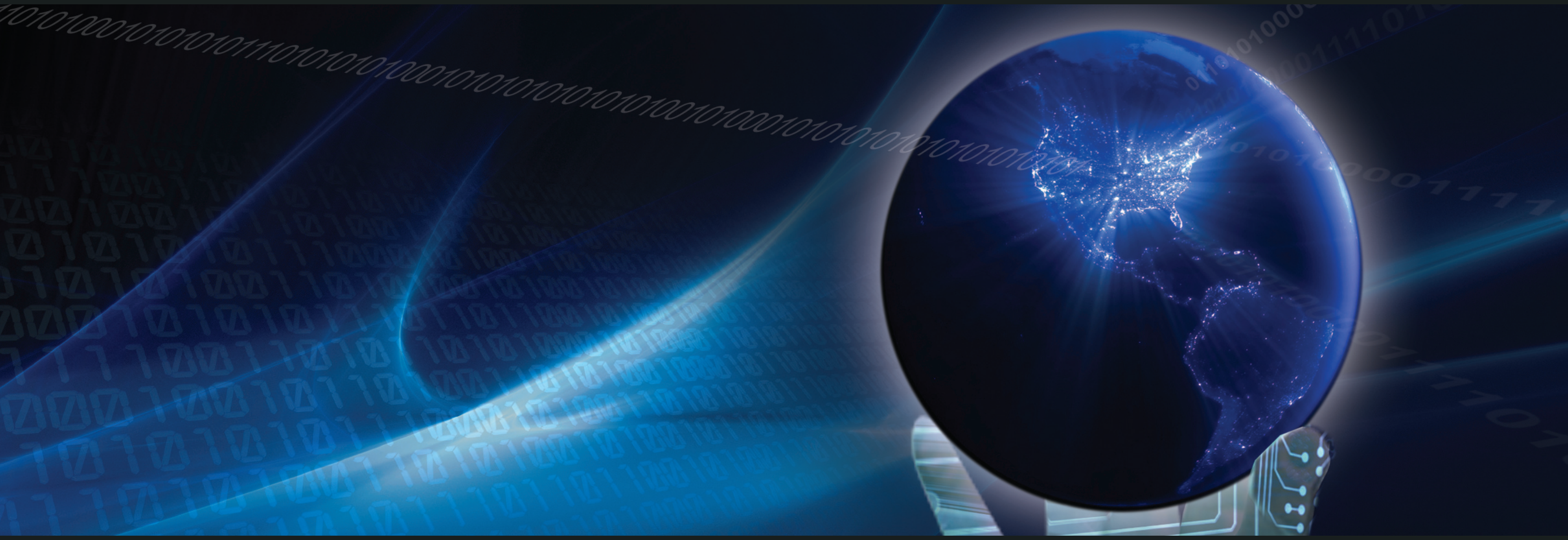
AccessData Enterprise



INVESTIGATION and INCIDENT RESPONSE with ENTERPRISE-WIDE REACH

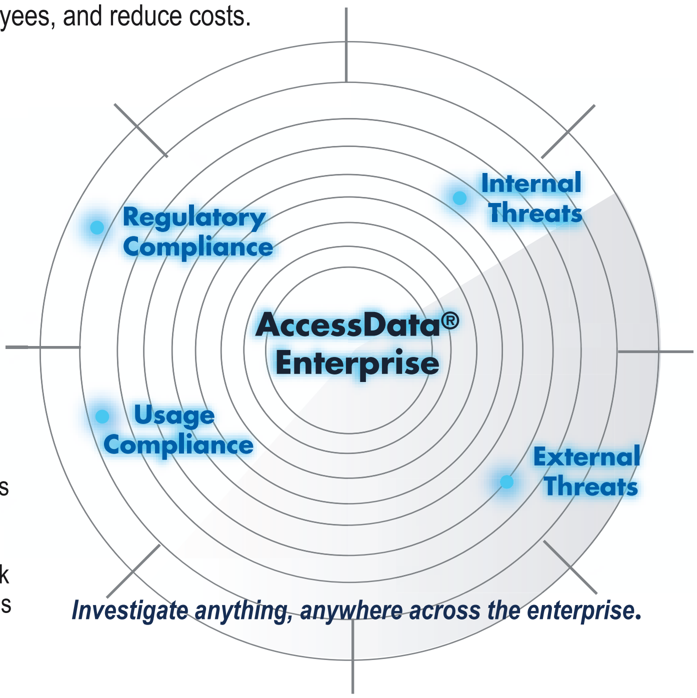
AccessData®

A Pioneer in Digital Investigations Since 1987

Defend Your Information Assets by Achieving Visibility across Your Enterprise...

Despite all the money spent on preventative technologies, bad things still happen. The method of detection is often just accidental discovery. While perimeter defense and alerting technologies serve a critical role in the protection of information assets, an enterprise-wide investigative capability is of equal importance. How do you identify security breaches that have circumvented your defenses? How do you detect intellectual property theft when the offender is a technologically sophisticated employee? How do you verify fraudulent activity without alerting those you are investigating? How do you ensure that you've properly indentified malware and isolated every machine on which it lives?

AccessData® Enterprise allows you to achieve visibility into all data across the enterprise, enabling you to detect, identify, analyze, report on and forensically preserve data, as well as remediate security issues. It is a new breed of investigative product built for scale, speed and broad functionality. This easy-to-use enterprise solution delivers network-wide investigative reach, allowing you to enforce policies, protect your data and employees, and reduce costs.



Investigate anything, anywhere across the enterprise.

Regulatory and Policy Compliance:

AccessData Enterprise facilitates regulatory compliance allowing organizations to respond quickly to investigate accusations or suspicions of employee malfeasance, such as fraud, PII theft, or the theft of credit card information. Having visibility into data on desktops, laptops, peripheral devices and network shares allows an organization to maintain compliance with regulations, such as Sarbanes-Oxley, PCI requirements, HIPAA, FISMA, and internal policies.

Usage Compliance:

Scan thousands of machines for unapproved processes, and if policies allow, IT personnel with the proper credentials can simply right-click to kill a specific process. Or if, for example, several unapproved processes are found to be running on multiple machines across the enterprise, IT personnel can initiate a batch remediation operation.

Internal Threats:

AccessData Enterprise allows you to see all data wherever it lives across your enterprise. You can proactively investigate users' machines across your network to identify artifacts that might indicate wrongdoing, such as intellectual property theft. In addition, you can react immediately and stealthily to validate whether an employee is guilty of IP theft, harassment or other wrongdoing. Once an internal threat has been validated, you can forensically preserve all evidence from a central location, even if there are multiple suspects spread throughout the world. For example, if one of your employees is suspected of sending confidential information to a competitor, and that person is traveling on the other side of the globe, his laptop (if an agent is installed) will check in with AD Enterprise whenever he goes online. He doesn't have to log into your network; he just needs to be online. (i.e. checking his web mail at a Starbucks).

External Threats:

Perimeter defense and monitoring technologies can only prevent or alert on threats that have been defined. Furthermore, savvy hackers have a multitude of sophisticated methods by which to circumvent these products. Therefore, your information security solution is not complete without enterprise-wide visibility and investigative reach, INCLUDING the ability to remediate immediately from a remote location. Proactive and reactive scanning with AD Enterprise will allow you to indentify rogue processes and malicious attributes, even those hidden by rootkits. It enables you detect external threats—even Advanced Persistent Threats, analyze the compromise to understand how it operates, conduct a network-wide assessment to identify all other affected nodes AND remediate all affected nodes from a central location. For far too many organizations, this capability is the missing piece in their information security puzzle. Without this response capability organizations are not able to effectively prevent widespread damage in the event of a security incident and they are not able to ensure thorough remediation.

Detect, Investigate and Remediate...

ACCESSDATA® ENTERPRISE

EXTERNAL THREATS

Hacking
Thoroughly and rapidly scan thousands of machines to determine scope of a breach and perform root cause analysis.

Malware
Scan thousands of machines quickly for unknown and known malicious processes and dlls.

Advanced Persistent Threats
Identify malicious artifacts running in memory.

IDS Alerts
View current activity on a given machine to resolve IDS alerts.

Compromise Assessment
Create a threat profile and audit to identify all contaminated machines.

INTERNAL INVESTIGATIONS

Content Monitoring Alerts
Quickly correlate user activity with a content monitoring alert and forensically preserve relevant data.

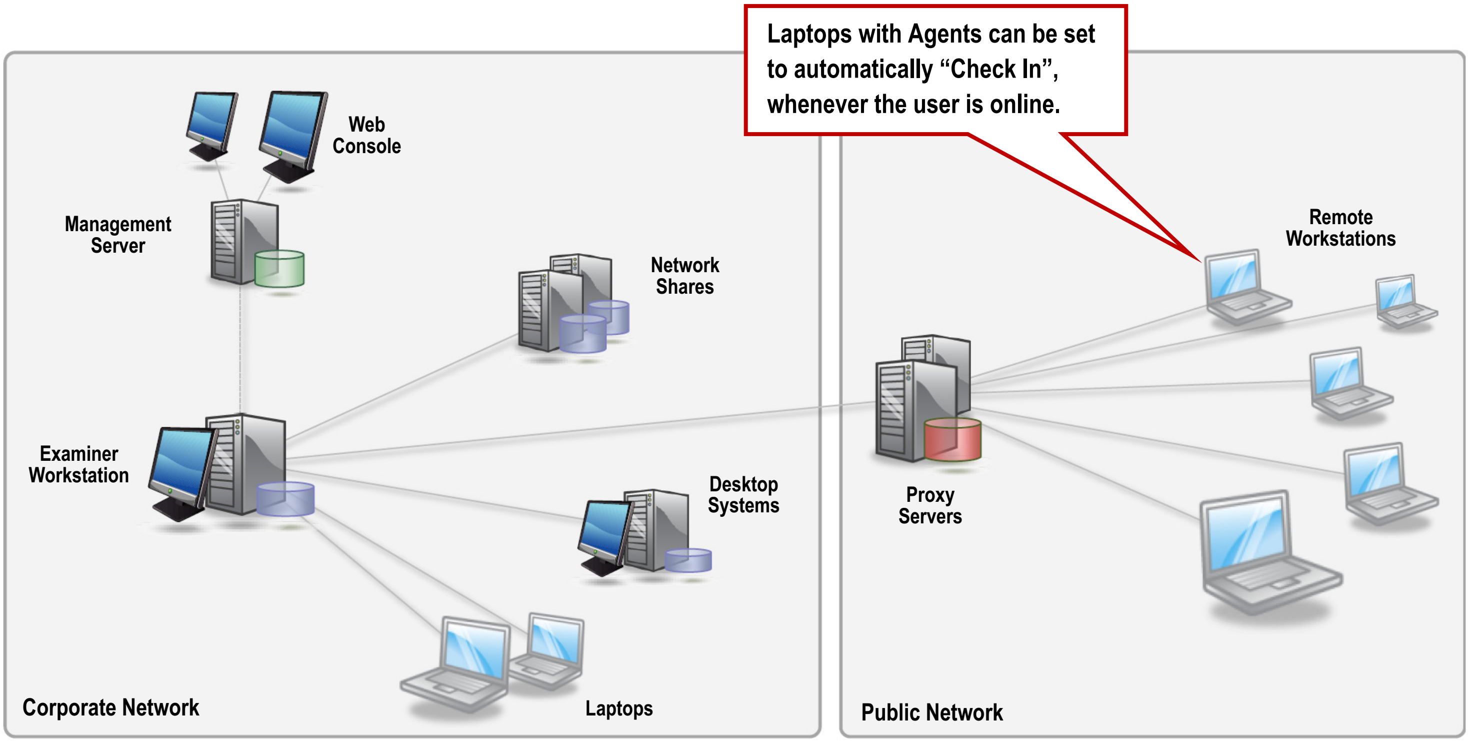
Employee Malfeasance
Conduct complete forensic investigations over the wire in stealth to verify whether malicious activity has occurred.

IP Theft
Conduct quick and thorough investigations of multiple individuals with a focus on user files and email.

Computer Usage Violations
Quickly scan the network for unapproved processes and preview drives to determine if computer usage violations have occurred.

Legal Matters
Conduct complete forensic investigations over the wire to identify, analyze and collect sensitive data relevant to any given matter.

How It Works…


Laptops with Agents can be set to automatically "Check In", whenever the user is online.

1. Examiner authenticates against the Management Service, is authorized for certain investigative operations, and creates a case.
2. If performing a remote investigation, the Examiner queries the Management Server or Active Directory for a list of nodes and selects target computers.
3. If the Examiner is authorized for the target nodes, investigation options become available, and requests are sent to the Agents.
4. Agents verify authorization of the request, accept commands and send back device status, OS information and drive information.
5. Examiner chooses to preview devices, acquire hard drives or RAM, or to gather volatile data.
6. Agents respond with a preview of attached drives and volatile data.
7. FTK accepts data from the Agents and displays requested information in the GUI.
8. Examiner remotely previews devices, processes data, and analyzes information relevant to the case.

Solution Highlights:

Powerful incident response without the use of scripts…

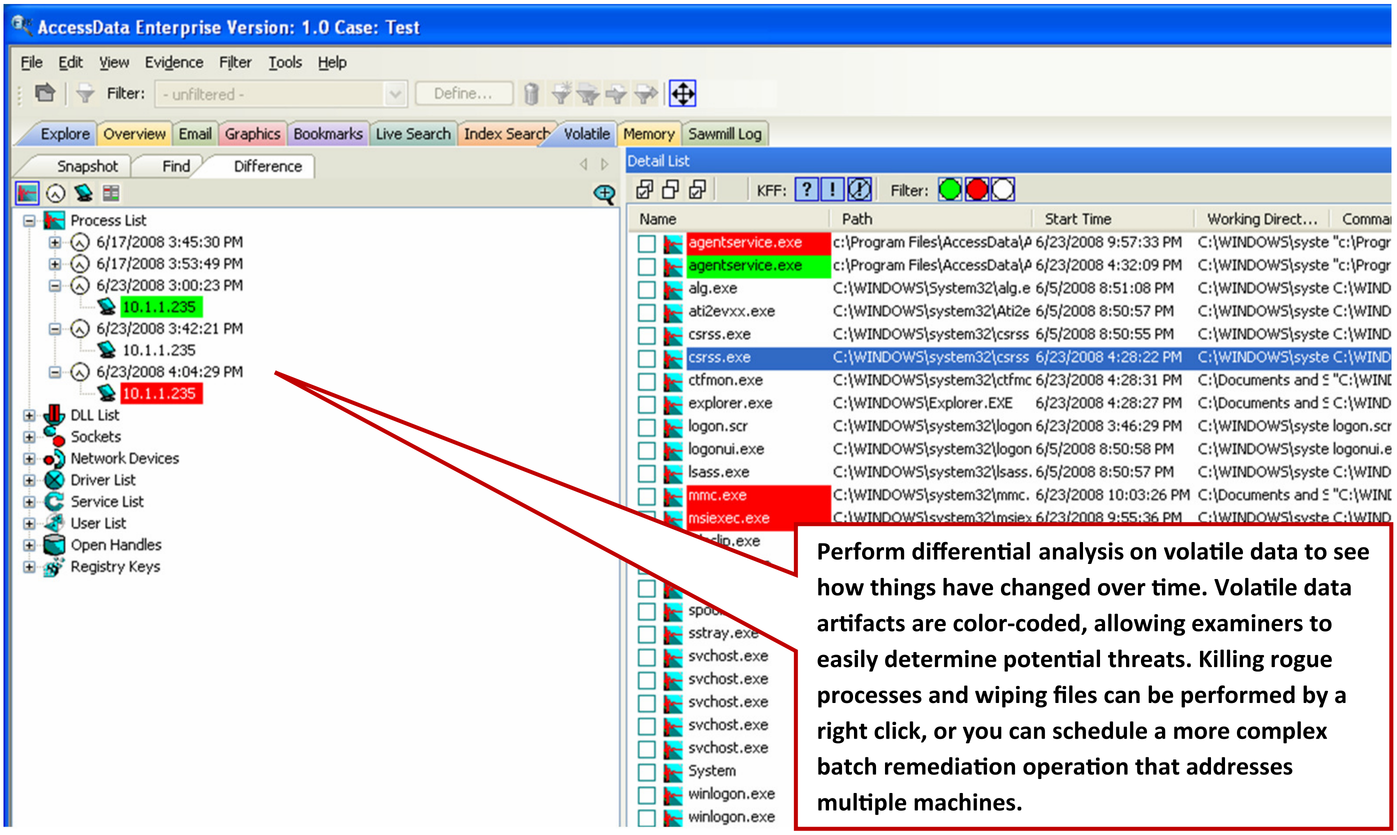
- The industry's first and only commercial enterprise investigations platform to enable the remote search and analysis of live memory on both 32-bit and 64-bit computers.
- Live memory searching: scan thousands of nodes for a string/keyword in memory, review results in context and export responsive exe/dlls.
- Integrated Incident Response Console: rapid review, analysis and correlation of processes, sockets, drivers, users, ports, dlls, handles and more, in a single view across nodes both, from RAM and Windows API.
- GUI-integrated right click process kill and wipe.
- View static and volatile data within the same interface.
- Batch Remediation Wizard: Define automated, secure remediation operations to be performed on multiple nodes.
- Analyze thousands of machines rapidly, either proactively or reactively.

Securely access, analyze and forensically preserve a wide variety of data over the wire…

- Multi-machine, forensic analysis with wizard-driven processing, filtering and reporting.
- Active Directory integration facilitates the selection of target nodes and authentication.
- ePO integration greatly facilitates agent deployment and the identification of target nodes.
- The industry's first single-click acquisition of hard drives, RAM and volatile data.
- Bulk acquisition supports the largest jobs.
- Market-leading decryption, password recovery and cracking.
- Computers "Check In" Automatically: Capture and analyze data from machines, wherever they might be—whether the machine is at Starbucks or a home office, you don't have to wait for the node to be active on the organization's network.

The only investigative solution with automated analysis & advanced processing power…

- Data Processing Wizard automatically processes email, zip files and unallocated space, removes known binaries, verifies file identity, and automatically categorizes and indexes all data.
- Oracle backend handles massive data sets, delivers case management, metadata storage and robust data manipulation.
- Distributed processing allows you to process massive amounts of data with ease.
- True Auto Save/Recovery functionality.


AccessData Enterprise Version: 1.0 Case: Test
File Edit View Evidence Filter Tools Help
Filter: - unfiltered -
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile Memory Sawmill Log
Snapshot Find Difference
Detail List
KFF: ? !
Filter:

- Process List
  - 6/17/2008 3:45:30 PM
  - 6/17/2008 3:53:49 PM
  - 6/23/2008 3:00:23 PM
    - 10.1.1.235
  - 6/23/2008 3:42:21 PM
    - 10.1.1.235
  - 6/23/2008 4:04:29 PM
    - 10.1.1.235
- DLL List
- Sockets
- Network Devices
- Driver List
- Service List
- User List
- Open Handles
- Registry Keys

	Name	Path	Start Time	Working Direct…	Comma
□	agentservice.exe	c:\Program Files\AccessData\A	6/23/2008 9:57:33 PM	C:\WINDOWS\syste	"c:\Progr
□	agentservice.exe	c:\Program Files\AccessData\A	6/23/2008 4:32:09 PM	C:\WINDOWS\syste	"c:\Progr
□	alg.exe	C:\WINDOWS\System32\alg.e	6/5/2008 8:51:08 PM	C:\WINDOWS\syste	C:\WIND
□	ati2evxx.exe	C:\WINDOWS\system32\Ati2e	6/5/2008 8:50:57 PM	C:\WINDOWS\syste	C:\WIND
□	csrss.exe	C:\WINDOWS\system32\csrss	6/5/2008 8:50:55 PM	C:\WINDOWS\syste	C:\WIND
□	csrss.exe	C:\WINDOWS\system32\csrss	6/23/2008 4:28:22 PM	C:\WINDOWS\syste	C:\WIND
□	ctfmon.exe	C:\WINDOWS\system32\ctfmc	6/23/2008 4:28:31 PM	C:\Documents and S	"C:\WINI
□	explorer.exe	C:\WINDOWS\Explorer.EXE	6/23/2008 4:28:27 PM	C:\Documents and S	C:\WIND
□	logon.scr	C:\WINDOWS\system32\logon	6/23/2008 3:46:29 PM	C:\WINDOWS\syste	logon.scr
□	logonui.exe	C:\WINDOWS\system32\logon	6/5/2008 8:50:58 PM	C:\WINDOWS\syste	logonui.e
□	lsass.exe	C:\WINDOWS\system32\lsass.	6/5/2008 8:50:57 PM	C:\WINDOWS\syste	C:\WIND
□	mmc.exe	C:\WINDOWS\system32\mmc.	6/23/2008 10:03:26 PM	C:\Documents and S	"C:\WINI
□	msiexec.exe	C:\WINDOWS\system32\msiex	6/23/2008 9:55:36 PM	C:\WINDOWS\syste	C:\WIND
□	clip.exe				
□	[illegible]				
□	[illegible]				
□	spoo				
□	sstray.exe				
□	svchost.exe				
□	svchost.exe				
□	svchost.exe				
□	svchost.exe				
□	svchost.exe				
□	System				
□	winlogon.exe				
□	winlogon.exe				

Perform differential analysis on volatile data to see how things have changed over time. Volatile data artifacts are color-coded, allowing examiners to easily determine potential threats. Killing rogue processes and wiping files can be performed by a right click, or you can schedule a more complex batch remediation operation that addresses multiple machines.