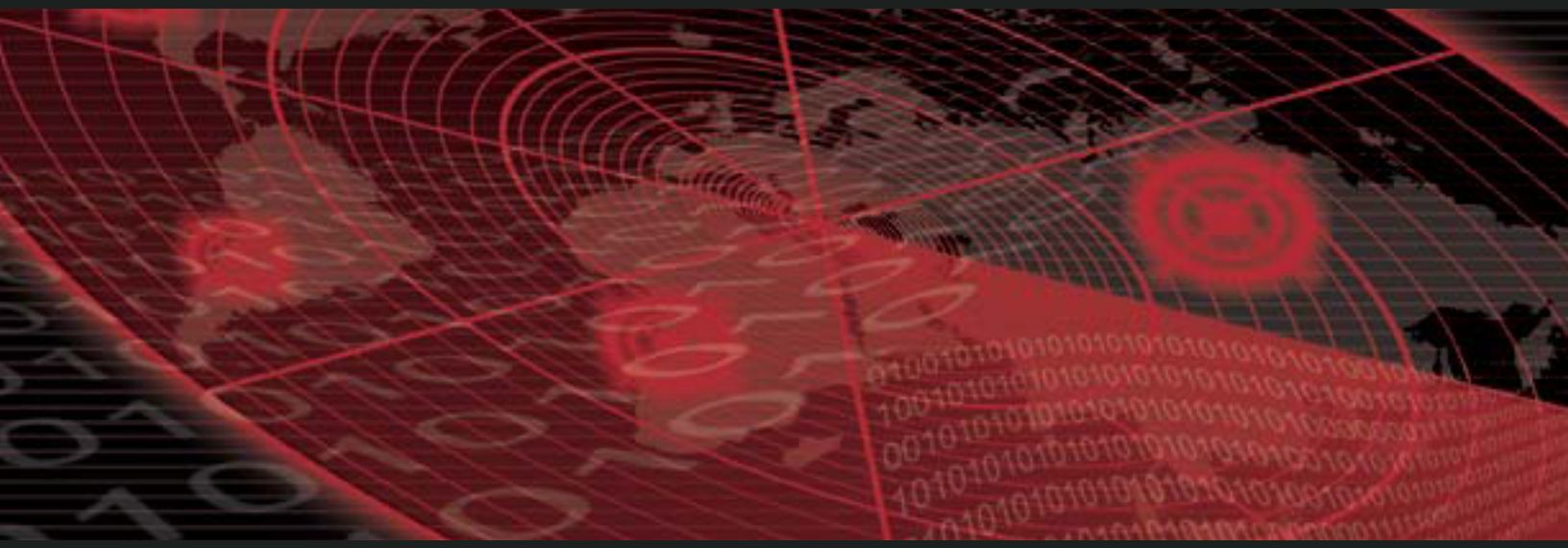
CIRT



THE ONLY SOLUTION TO INTEGRATE NETWORK ANALYSIS, HOST ANALYSIS and DATA AUDITING

AccessData®
A Pioneer in Digital Investigations Since 1987

When all else fails…
THIS IS YOUR LAST LINE OF DEFENSE

Situational awareness cannot be achieved if an organization has a reactionary mindset. It is very much a proactive proposition, yet most investigative tools available to government agencies and corporations are, by nature, reactionary. To make matters worse, organizations are limited in their ability to react to critical threats, because they are relying on a broad range of disparate security products, most of which are signature-based and prevention-oriented.

However, the fact is, when an entity has compromised your system and is operating in stealth on the network, no signature-based technology is going to help. The only way to detect, understand and remediate these threats is to employ a solution that provides visibility from multiple vantage points, such as what is happening on the host — both static and volatile — as well as what is happening on the network.

THE FIRST CYBER SECURITY SOLUTION TO INTEGRATE NETWORK FORENSICS, HOST FORENSICS AND LARGE-SCALE DATA AUDITING WITHIN A SINGLE INTERFACE

This automated, integrated security framework allows you to address threats, data spillage and compliance obligations more quickly and more effectively. Using CIRT, you can proactively and reactively identify, analyze and remediate security incidents of any kind, including zero day events, hacking, data spillage and advanced persistent threats. For example, you can scan thousands of computers across the enterprise to identify rogue executables existing on your network. Perform root cause analysis efficiently by correlating network and host data within a single interface. During analysis, you can replay incidents in real time to fully understand how the exploit proliferated. Drill down into affected machines to analyze behavior at the host level. Scan the enterprise to identify all affected nodes and, most importantly, remediate the threat. Finally, using the intelligence gathered with CIRT during incident analysis, you can build threat profiles to mitigate the recurrence of threats in the future.

No other cyber security solution delivers a single interface, within which, you can analyze and correlate static host data, volatile data and network traffic. Furthermore, no other incident response product offers the secure, remote “batch remediation” capabilities of AccessData’s CIRT. The CIRT security framework delivers the critical capabilities that are currently missing from the traditional cyber security infrastructure: *VISIBILITY, AUTOMATION, INTEGRATION and COLLABORATION*

THE BENEFITS OF A FULLY INTEGRATED SECURITY FRAMEWORK…

INCIDENT RESPONSE & CYBER INTELLIGENCE

- CIRT facilitates continuous monitoring, allowing you to schedule automated, ongoing operations with real-time information feeds.
- Correlate event logs.
- Proactively detect security threats.
- Faster identification, root cause analysis and remediation.
- Integrated analytics enable you to more effectively chase down advanced persistent threats.
- Efficiently gather cyber intelligence and build profiles to defend your network.

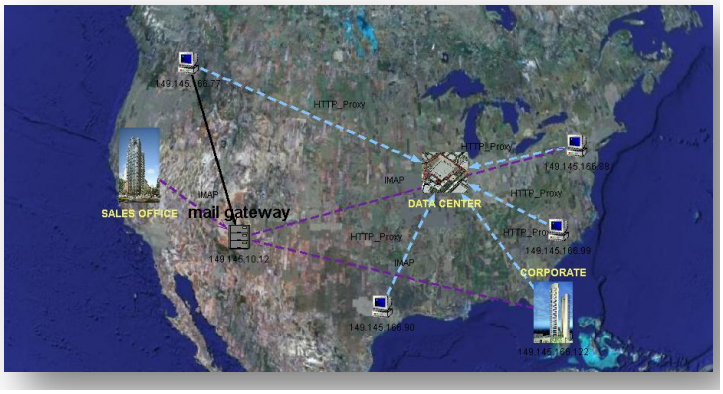
INFORMATION ASSURANCE & COMPLIANCE AUDITING

- Automated, large-scale data auditing allows you to identify data spillage across the enterprise.
- Easily locate responsive documents for FOIA requests.
- Perform regular PCI audits more efficiently and cost effectively.
- Natively connect to structured data repositories for targeted searching without creating an index.
- DOD-certified wiping when circumstances and policies allow.

WHAT CAN YOU DO WITH THE CIRT SECURITY FRAMEWORK?

Ease of Use, Process-oriented Workflow & Real-time Communication Up and Down the Chain of Command

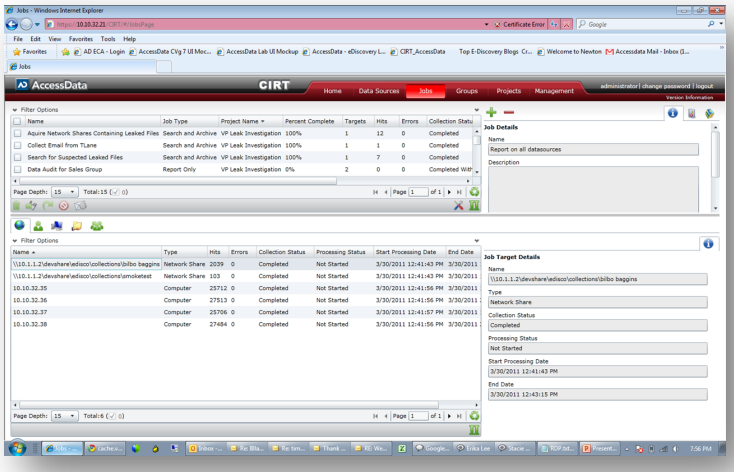
- Easy-to-use web-based interface enables **real-time communication**.
- Strict, **granular role-based permissions**.
- Assign tasks and track progress.
- Real-time status on security operations.
- **Active Directory and ePO** integration for easy deployment.



Map proliferation of exploits and data leakage then analyze target machines—all within same solution.

Powerful Incident Response, Including Analysis of All Live Processes

- Advanced, **agent-side** search and analysis of live memory on 32- and 64-bit Windows machines.
- Automatically **scan thousands of machines** for anomalies.
- Correlate static and volatile data with network traffic.
- Integrated analysis and forensic collection of network shares.
- The industry's first **one-click acquisition** of hard drives, RAM and volatile data.
- Automated **batch acquisition**.
- Easy-to-use data processing wizard.
- Market-leading **decryption and cracking technology**.



Schedule and manage spillage and compliance audits.

Real-Time Network Capture

- Real-time network data capture at **Gig speeds**.
- Monitors **more than 1,500 protocols and services** out of the box.
- Network data is stored in a central database that can be queried.
- Capture and analyze wireless Ethernet 802.11b and 802.11g.
- Log correlation and analysis.

Pattern and Content Analysis with On-demand Incident Playback

- Advanced visualization tools aid in more effective **root cause analysis**.
- **Interactive graphical representations** illustrate propagation.
- Distinguish between diversionary and malicious incidents.
- **Map proliferation** of viruses, worms and confidential data leakage.
- Watch the exact sequence of events with **on-demand incident playback**.

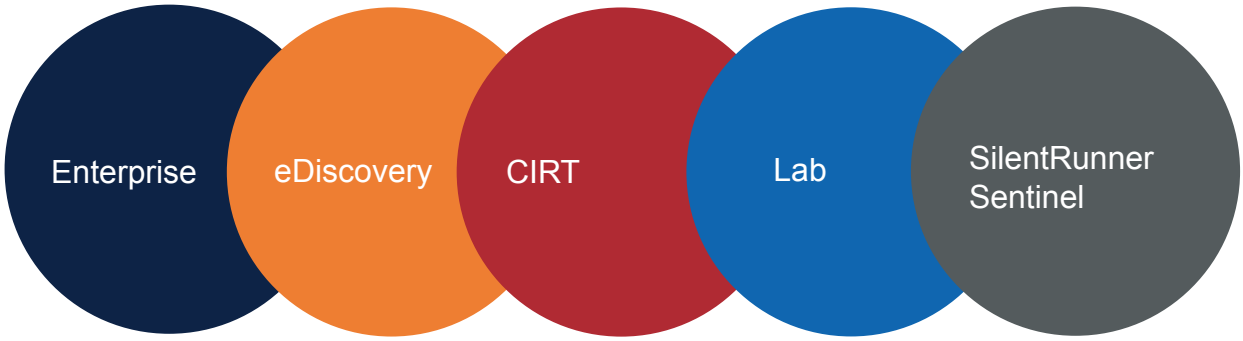
Superior Smart-Target, Large-scale Auditing

- An automated, efficient way to **detect data leakage and enforce PCI compliance**.
- Extensive dash-boarding and reporting capabilities.
- Extensive logging of all discovery activity for **chain of custody and auditing** purposes.
- Determine **where classified or personal data lives** and categorize it.
- Conduct automated audits using virtually any search criteria.

The Power to Act Immediately, Effectively and Securely

- Respond quickly to **FOIA requests**.
- Respond quickly and effectively to alerts, **correlating user activity and network traffic**.
- Flag non-compliant files and log their locations for manual remediation operations.
- Wipe rogue files from a central location, and replace them with stub documents.
- **Right click process kill** and **batch remediation** for authorized users.
- DOD-certified wiping.
- AccessData's "Secure Network Communications Module" is **FIPS 140-2 certified** and leverages SSL 128-bit encryption

THE ACCESSDATA® PLATFORM FAMILY OF PRODUCTS



Build an investigative solution to meet your organization's specific needs. This enterprise-class collection of products is designed to allow you to expand your investigative capabilities as your needs grow and evolve. The following enterprise building blocks work together to deliver visibility into all data, unmatched investigative reach and the utmost efficiency.

AccessData Enterprise

- ✓ No scripts — all functionality is in the GUI.
- ✓ True Auto Save/Recovery functionality.
- ✓ Forensically acquire RAM and devices.
- ✓ Schedule bulk acquisitions of RAM and devices.
- ✓ Integrated Incident Response Console — correlate processes, sockets and ports in a single view across nodes.
- ✓ Live memory search and analysis.
- ✓ Right click process kill functionality.
- ✓ Wizard-driven processing, filtering and reporting.
- ✓ Computers "Check In" automatically, enabling capture and analysis of data from machines, no matter where they are.

SilentRunner™ Sentinel™

Visibility into network traffic to complete the investigative picture and properly remediate security breaches, data theft and policy violations.

- ✓ Capture network traffic at full gigabit network line speeds.
- ✓ Works with AD Enterprise to deliver 360-degree view into all data — host-based static data, RAM and network traffic data.
- ✓ Advanced visualization graphically illustrates nodal communications and data propagation.
- ✓ On-demand incident playback allows you to replay events exactly as they occurred.
- ✓ Forensically record and analyze massive amounts of network data.
- ✓ Monitors more than 1,500 services and protocols out of the box.
- ✓ Dramatically improve your ability to identify perpetrators and determine root cause.

AccessData eDiscovery

A complete turnkey solution for internal litigation preparedness.

- ✓ Web-based review platform delivers cutting-edge analytics and collaborative review of ESI.
- ✓ Advanced early case assessment capabilities.
- ✓ Enables sophisticated searching methodologies.
- ✓ Forensically collect data from workstations, laptops, network shares, email servers, databases and more than 30 structured data repositories.
- ✓ Rich reporting with strong chain of custody support.
- ✓ Automated processing and deduplication.
- ✓ Load file creation.
- ✓ Rich workflow with integrated matter and custodian management.

Cyber Intelligence & Response Technology (CIRT)

The first solution to integrate network forensics, host forensics and large-scale data auditing into a single interface.

- ✓ Facilitates continuous monitoring and counter cyber intelligence.
- ✓ Log correlation and analysis.
- ✓ Correlate data gathered from network and host analysis with auditing results:
  - Chase down advanced exploits.
  - Proactively identify security threats and remediate.
  - Identify data leakage, determine how it propagated and remediate.