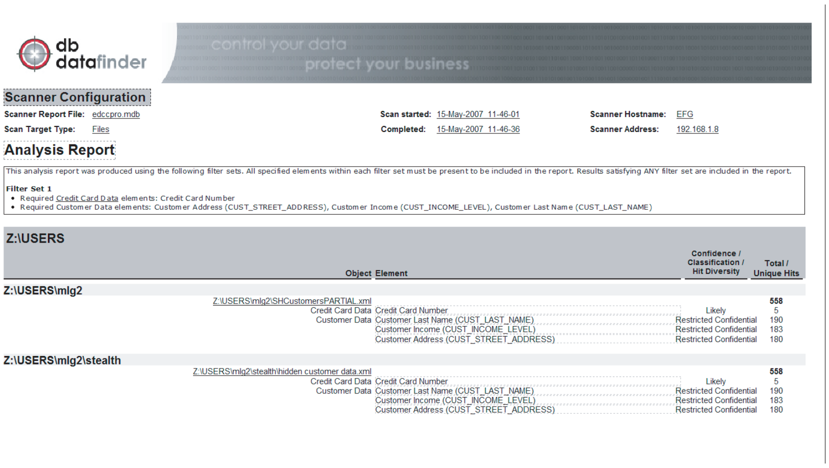
db datafinder

control your data
protect your business

YOUR MISSION:

to **control** the **proliferation and leakage** of confidential data
to **unstructured and unsecured** files and databases

dbDataFinder provides you with data oriented visibility across the various database and file servers employed within your enterprise. dbDataFinder is a secure, process oriented solution to the problem of data leakage and proliferation. dbDataFinder delivers tighter control over confidential data through its five step process.



Scanner Configuration

Scanner Report File: edccpro.mdb
Scan Target Type: Files
Scan started: 15-May-2007 11-46-01
Completed: 15-May-2007 11-46-36
Scanner Hostname: EFG
Scanner Address: 192.168.1.8

Analysis Report

This analysis report was produced using the following filter sets. All specified elements within each filter set must be present to be included in the report. Results satisfying ANY filter set are included in the report.

Filter Set 1
- Required Credit Card Data elements: Credit Card Number
- Required Customer Data elements: Customer Address (CUST_STREET_ADDRESS), Customer Income (CUST_INCOME_LEVEL), Customer Last Name (CUST_LAST_NAME)

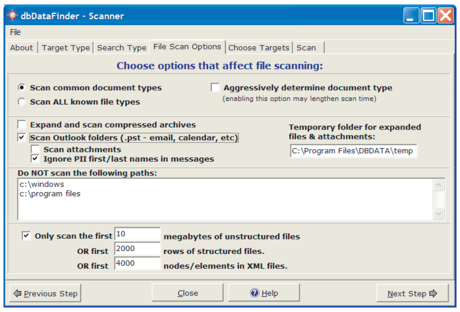
Z:\USERS

Object	Element	Confidence / Classification / Hit Diversity	Total / Unique Hits
Z:\USERS\mlg2			
Z:\USERS\mlg2\SHCustomersPARTIAL.xml			**558**
Credit Card Data	Credit Card Number	Likely	5
Customer Data	Customer Last Name (CUST_LAST_NAME)	Restricted Confidential	190
	Customer Income (CUST_INCOME_LEVEL)	Restricted Confidential	183
	Customer Address (CUST_STREET_ADDRESS)	Restricted Confidential	180
Z:\USERS\mlg2\stealth			
Z:\USERS\mlg2\stealth\hidden customer data.xml			**558**
Credit Card Data	Credit Card Number	Likely	5
Customer Data	Customer Last Name (CUST_LAST_NAME)	Restricted Confidential	190
	Customer Income (CUST_INCOME_LEVEL)	Restricted Confidential	183
	Customer Address (CUST_STREET_ADDRESS)	Restricted Confidential	180

- Identify the sources of confidential data
- Securely profile user specified data sets
- Assign data categories and classification
- Identify copies and subsets of confidential data in enterprise file and database servers
- Mitigate risk

dbDataFinder quickly scans your enterprise to pinpoint sources of confidential data as well as additional subsets, copies, and exports of that data. dbDataFinder identifies files and databases containing:

- Payment Card Information
- Customer Data
- Personally Identifying Information
- Financial data
- Corporate intellectual property



Choose options that affect file scanning:

● Scan common document types
○ Scan ALL known file types
□ Aggressively determine document type
(enabling this option may lengthen scan time)

□ Expand and scan compressed archives
☑ Scan Outlook folders (.pst - email, calendar, etc)
□ Scan attachments
☑ Ignore PII first/last names in messages

Temporary folder for expanded files & attachments: C:\Program Files\DBDATA\temp

Do NOT scan the following paths:
c:\windows
c:\program files

☑ Only scan the first 10 megabytes of unstructured files
OR first 2000 rows of structured files.
OR first 4000 nodes/elements in XML files.

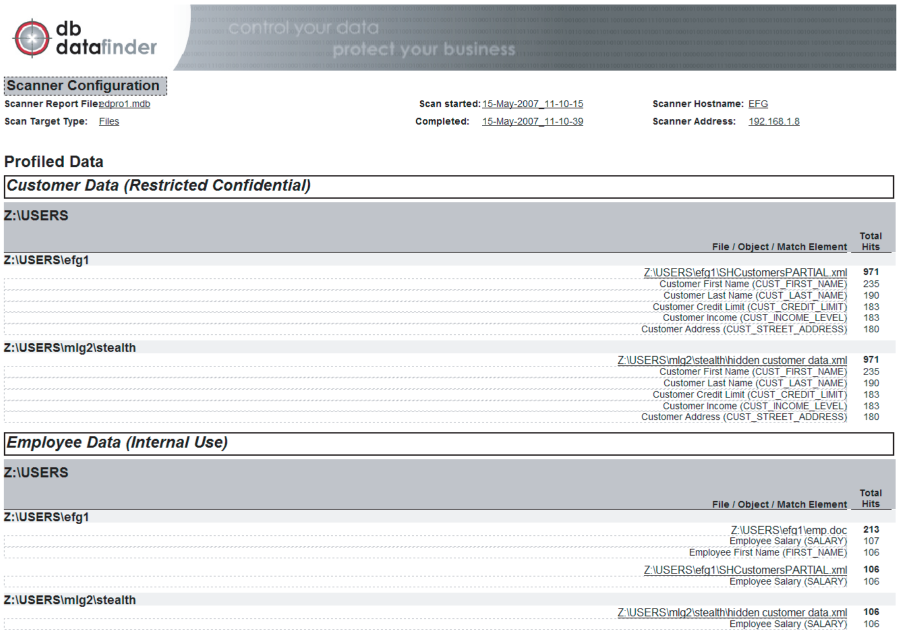
dbDataFinder uses its combination of data signatures, custom specified search terms, and a secure profile of your organization's valued data to eliminate false positives and identify exports of your sensitive data to:

- Spreadsheets
- Enterprise and Personal Databases
- Mail
- Archives
- Over 200 different document types.

dbDataFinder features multiple scanners each tuned to identify the individual data elements that comprise particular type of data. Scanners include:

- PII Scanner (Privacy related data)
- PCI Scanner (Customer and payment card data)
- Profiled Data Scanner (User specified data sets)
- Custom Search Term Scanner
- Application Data Scanner (Oracle, PeopleSoft, Seibel)

control your data **protect your business** www.**dbdatafinder**.com



Scanner Configuration

Scanner Report File:	edpro1.mdb	Scan started:	15-May-2007_11-10-15	Scanner Hostname:	EFG
Scan Target Type:	Files	Completed:	15-May-2007_11-10-39	Scanner Address:	192.168.1.8

Profiled Data

Customer Data (Restricted Confidential)

Z:\USERS

	File / Object / Match Element	Total Hits
Z:\USERS\efg1		
	Z:\USERS\efg1\SHCustomersPARTIAL.xml	**971**
	Customer First Name (CUST_FIRST_NAME)	235
	Customer Last Name (CUST_LAST_NAME)	190
	Customer Credit Limit (CUST_CREDIT_LIMIT)	183
	Customer Income (CUST_INCOME_LEVEL)	183
	Customer Address (CUST_STREET_ADDRESS)	180
Z:\USERS\mlg2\stealth		
	Z:\USERS\mlg2\stealth\hidden customer data.xml	**971**
	Customer First Name (CUST_FIRST_NAME)	235
	Customer Last Name (CUST_LAST_NAME)	190
	Customer Credit Limit (CUST_CREDIT_LIMIT)	183
	Customer Income (CUST_INCOME_LEVEL)	183
	Customer Address (CUST_STREET_ADDRESS)	180

Employee Data (Internal Use)

Z:\USERS

	File / Object / Match Element	Total Hits
Z:\USERS\efg1		
	Z:\USERS\efg1\emp.doc	**213**
	Employee Salary (SALARY)	107
	Employee First Name (FIRST_NAME)	106
	Z:\USERS\efg1\SHCustomersPARTIAL.xml	**106**
	Employee Salary (SALARY)	106
Z:\USERS\mlg2\stealth		
	Z:\USERS\mlg2\stealth\hidden customer data.xml	**106**
	Employee Salary (SALARY)	106

download it >> *www.dbdatafinder.com/download_landing.html*

dbDataFinder's ability to securely profile application data enables organizations to pinpoint internal confidential data leak and proliferation. Profile based scanning eliminates false positives resulting from the existence of files or databases containing relevant data types, i.e. PII, but irrelevant data values. Profiling enables a differentiation between files containing leaks of corporate HR data and the file or database containing masked or dummy data used for development purposes.

dbDataFinder enables the creation and enforcement of your own data protection policies. dbDatafinder filter sets are used to group individual data elements that, when combined within a file or database, would represent high risk information. Instances where a First and Last Name may not in itself constitute high risk. When accompanied within a file with a Social Security number, address or other personally identifying data, the combination of data elements represents exponentially greater risk.

dbDataFinder enables you to manage your organization's specific risks by focusing on your data. dbDataFinder eliminates false positives and finds copies and subsets of the specific data that is important to you with pinpoint accuracy. dbDataFinder identifies instances where your confidential data has moved or leaked from your structured database environment to other databases or to file systems in any of over 200 different unstructured file formats.

dbDataFinder speeds the mitigation of risk with concise reports that detail the location and the nature of the data related risks to your business that exist today. dbDataFinder is an integral part of any data security, classification or compliance program.

ABOUT US

Founded by information security and data management experts, BrainTree Technology, LLC was founded to provide solutions to companies that need to manage security for confidential data regardless of its form or wherever it goes over the course of it useful lifecycle.

BrainTree Technology, LLC
164-I Summer Street #428
Kingston, MA 02364

Phone	800-806-1571
Email	*info@dbdatafinder.com*
Website	*www.dbdatafinder.com*