IT Tools, Techniques and use of Technology as drivers for Fraud Detection and Investigation

Uphold public interest

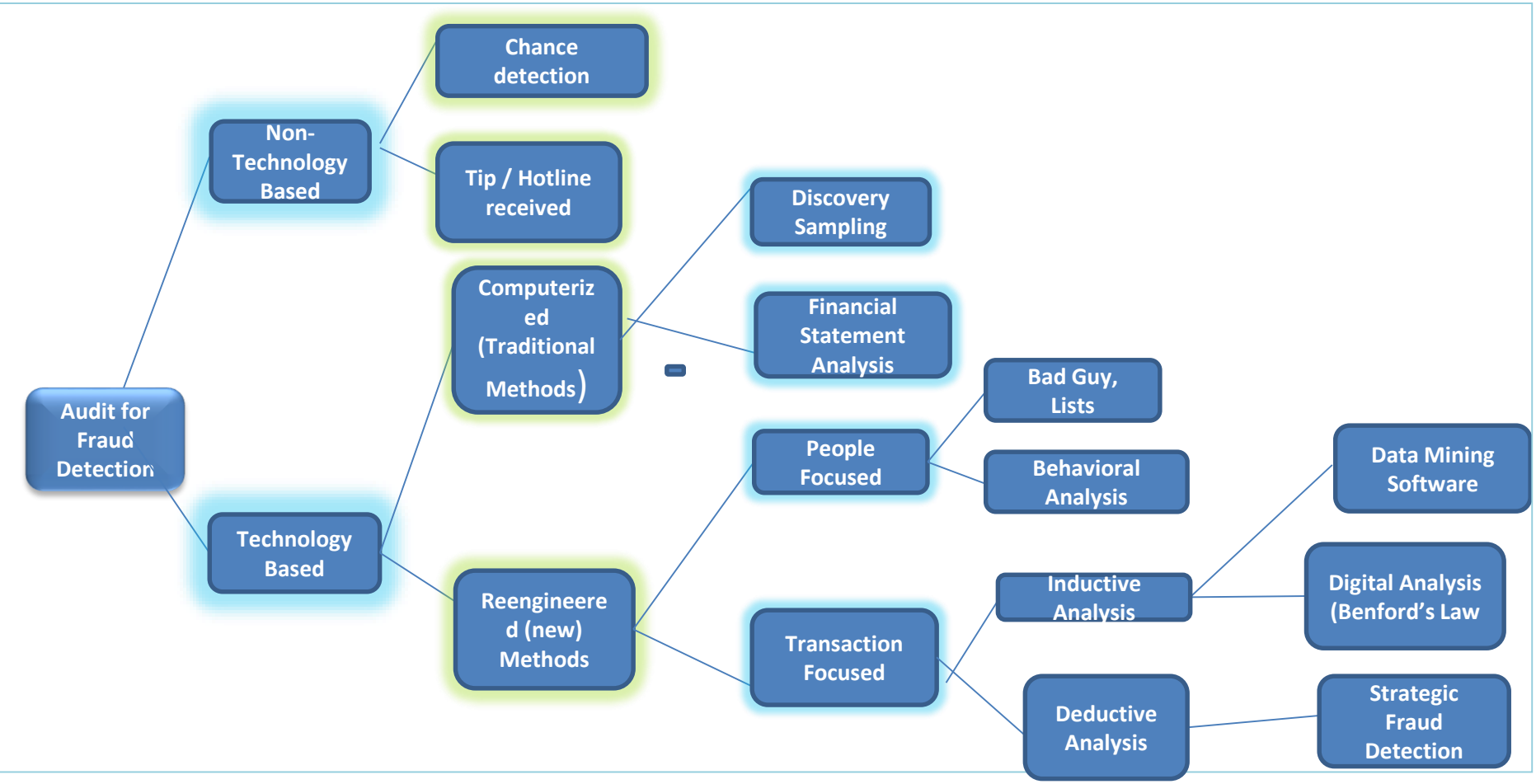
Proactive vs Reactive

- Proactive-Detection
- Reactive-Investigation

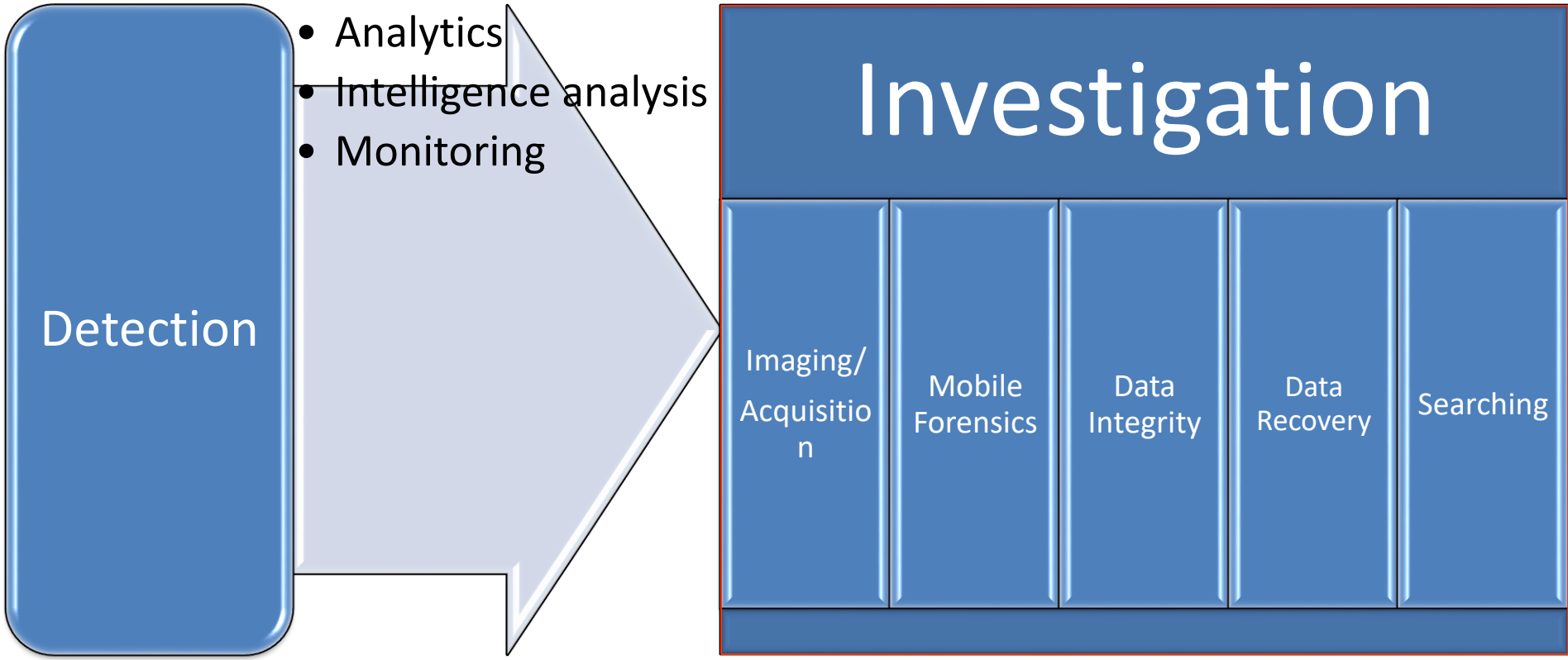
Over one third of frauds were discovered by accident, making "chance" the most common fraud detection tool.

- PriceWaterhouseCoopers, Global Economic Crime Survey 2005

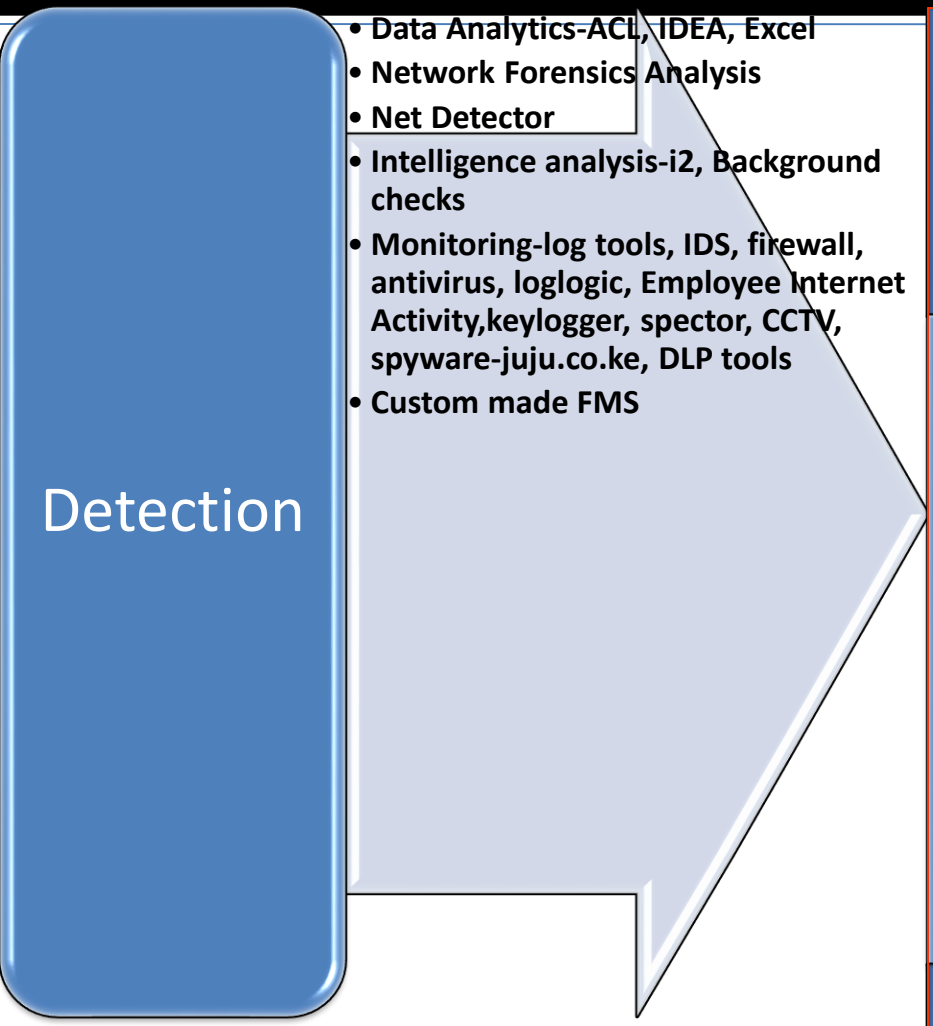
Fraud Detection Methods



IT Techniques



IT Tools


Detection
• Data Analytics-ACL, IDEA, Excel
• Network Forensics Analysis
• Net Detector
• Intelligence analysis-i2, Background checks
• Monitoring-log tools, IDS, firewall, antivirus, loglogic, Employee Internet Activity,keylogger, spector, CCTV, spyware-juju.co.ke, DLP tools
• Custom made FMS


Investigation
Imaging/ Acquisition
Encase
FTK
DD
Mobile Forensics
Cellebrite
MPE
Data Integrity
MD5
Easy Crypto
Private Disk
Data Recovery
PC inspector recuva,
Searching
dtSearch
Email analysis

Importance of IT Forensic Techniques

- Majority of fraud is uncovered by chance
- Auditors often do not look for fraud
- Prosecution requires evidence
- Value of IT assets growing

Using Data Analytics for Fraud Auditing

Effective data analysis requires:

- Translating knowledge of organization and common fraud indicators into analytics tests
- Effectively using technological tools
- Resolving errors in data output due to incorrect logic or scripts
- Applying fraud investigation skills to the data analysis results to detect potential instances of fraud
- Data analysis techniques alone are unlikely to detect fraud; human judgment is needed to decipher results.

Data Analytics- Types of Data That Can Be Analyzed

Relevant data comes from numerous sources and takes numerous forms:

- Accounting and financial data
- Human resources data
- Customer data
- Vendor data
- Internal communications and documents
- External benchmarking data

Data analytics

- Population Analytics-Although testing a sample of data is a valid audit approach, it is not as effective for fraud detection purposes.
- To detect fraud, data analysis techniques must be performed on the full data population.
- Define population boundaries, including amount of historical data to include.

Benefits of Data Analytics

- Identify fraud before it becomes material.
- Focus detection efforts on suspicious transactions.
- Gain insight into how well internal controls are operating.
- Compare data from diverse sources to identify instances of fraud or noncompliance.

Audit Command Language(ACL)

ACL is the market leader in computer-assisted audit technology and is an established forensics tool.

Clientele includes …

70 percent of the Fortune 500 companies

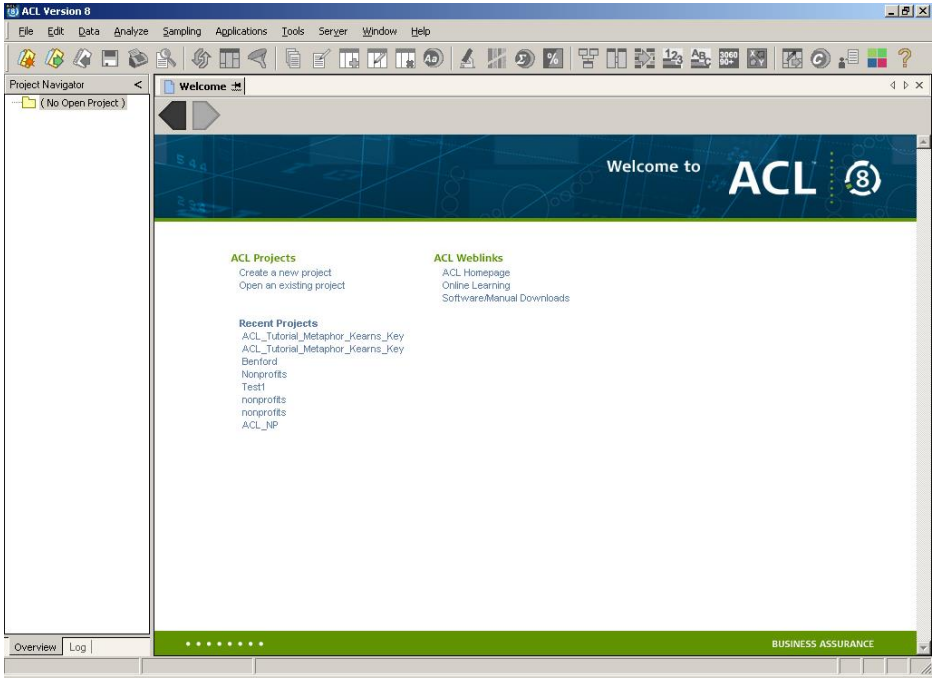
over two-thirds of the Global 500

the Big Four public accounting firms

Audit Command Language

ACL is a computer data extraction and analytical audit tool with audit capabilities …

- Statistics
- Duplicates and Gaps
- Stratify and Classify
- Sampling
- Benford Analysis



Data Analytics –Specifics

Accounts payable

- Vendor / Employee collusion

Purchasing

- Purchase splitting
- Purchases without Requisitions

Purchase cards

- Inappropriate, unauthorized purchases

Travel & Entertainment Expenses

- Duplicate claims, inappropriate activity

Payroll

- Phantom employees
- Unauthorized overtime

Data Analytics –Accounts Payable

Questionable invoices

- Invoices without a valid P.O.
- Sequential invoices

Over-billing

- Quantity shipped less than quantity ordered
- Pricing outside norm for product category
- Item shipped of lower value than item ordered

Duplicate invoices

- Multiple invoices for same item description
- Invoices for same amount on the same date
- Multiple invoices for same P.O. and date

Data Analytics – Purchasing

Questionable purchases

- P.O./invoices with amount paid > amount received
- Purchases of consumer items

Split purchases

- Similar transactions for same vendor within specific timeframe

Inflated prices

- Compare prices to standard price lists or to historical prices

Phantom vendors

- Vendor/employee comparison
- Vendor has mail drop as sole address

Data Analytics –Time and Expense

Duplicate claims

- Submitting claims twice

Tracking “no receipt” claims

- Isolate expenses without receipts and identify underlying trends through profiling techniques

Threshold reviews

- Track personnel exceeding thresholds

Inappropriate activity

- Compare expenses to travel records to ensure expenses claimed for valid trips

Trends by employee compared to peers

Benford Analysis

States that the leading digit in some numerical series is follows an exponential rather than normal distribution

Applies to a wide variety of figures: financial results, electricity bills, street addresses, stock prices, population numbers, death rates, lengths of rivers

Leading Digit	Probability
1	30.1 %
2	17.6 %
3	12.5 %
4	9.7 %
5	7.9 %
6	6.7 %
7	5.8 %
8	5.1 %
9	4.6 %

Auditor's Knowledge, Skills, Abilities

- Accounting
- Auditing
- IT (weak)

Needed …

- Increased IT knowledge
- Fraud and forensic accounting knowledge
- Forensic investigative and analytical skills and abilities

Digital Crime Scene Investigation

A process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred.

IT Forensic Techniques are used to capture and analyze electronic data and develop theories.

Digital Crime Scene Investigation

Goal: Determine what fraud events occurred by using digital evidence

Three Phases:

- Preserve & Document Scene
- Analyze/Search & Document Data
- Reconstruct & Document Fraud Event

Extract, process, interpret

- Work on the imaged data or “safe copy”
- Data extracted may be in binary form
- Process data to convert it to understandable form
  - Reverse-engineer to extract disk partition information, file systems, directories, files, etc
  - Software available for this purpose
- Interpret the data – search for key words, phrases, etc.

Data Integrity
MD5

Message Digest – a hashing algorithm used to generate a checksum

- Available online as freeware
- Any changes to file will change the checksum

Use:

- Generate MD5 of system or critical files regularly
- Keep checksums in a secure place to compare against later if integrity is questioned

Free Log Tools

Name	Type	URL
fwlogwatch	Log analyzer	http://fwlogwatch.inside-security.de/
Log Parser	Log parser	http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en
Log Tool	Log parser	http://xjack.org/logtool/
LogSentry (formerly known as Logcheck)	Log analyzer	http://logcheck.org/, http://sourceforge.net/projects/logcheck/
Logsurfer	Log analyzer	http://www.cert.dfn.de/eng/logsurf/
Logwatch	Log analyzer	http://www.logwatch.org/
Project Lasso	Windows event log management	http://sourceforge.net/projects/lassolog
Swatch	Log analyzer	http://swatch.sourceforge.net/

Employee Internet Activity

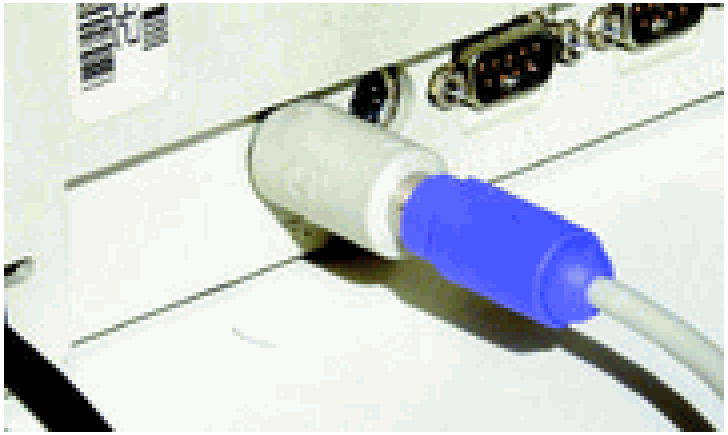
Spector captures employee web activity including keystrokes, email, and snapshots to answer questions like:

- Which employees are spending the most time surfing web sites?
- Which employees chat the most?
- Who is sending the most emails with attachments?
- Who is arriving to work late and leaving early?
- What are my employees searching for on the Internet?

Data Capture : Key Log Hardware

KeyKatcher

- Records chat, e-mail, internet & more
- Is easier to use than parental control software
- Identifies internet addresses
- Uses no system resources
- Works on all PC operating systems
- Undetectable by software



Background Checks

- Public Databases
- Government Websites
- Corporate Records
- Internet
- Social Media
- News Sources/Newspapers
- IP address tracking

Conclusion

IT Forensic Investigative Skills Can …

- Decrease occurrence of fraud
- Increase the difficulty of committing fraud
- Improve fraud detection methods
- Reduce total fraud losses

Questions or Comments?

Michael Karanja

mike.wanguru@gmail.com

+254702898434

Resources

ACL
http://www.acl.com/Default.aspx?bhcp=1

Eraser
http://www.heidi.ie/eraser/

Private Disk
http://www.private-disk.net/

HashCalc
http://www.slavasoft.com/hashcalc/index.htm

PC Inspector
http://www.download.com/3000-2242-10066144.html

VeriSign
http://www.verisign.com

HandyBits Encryption
http://www.handybits.com/

EnCase
http://www.handybits.com/

IP tracking
http://www.whatismyipaddress.com

Resources

Spector
http://www.spectorsoft.com/
Stolen ID Search
https://www.stolenidsearch.com/
Abika Background Check
http://www.abika.com/
Guide to Log Management
http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
NetWitness
http://www.netwitness.com/
GASP Std V 7.0 Free Software
http://www.bsa.org/usa/antipiracy/Free-Software-Audit-Tools.cfm
Federal Guidelines for Searches
http://www.cybercrime.gov/searchmanual.htm
Recuva
www.piriform.com/recuva
DLP-Data loss prevention
www.websense.com