

A red banner with a dotted pattern on the left side. It contains several technical icons: a gear, a network diagram with nodes and arrows, a document with a checkmark, and a circular icon with a lightning bolt and a shield.

Securing Your Web World



Data Leak Prevention Trend Micro LeakProof™

Michał Antoniak

2008-06-01

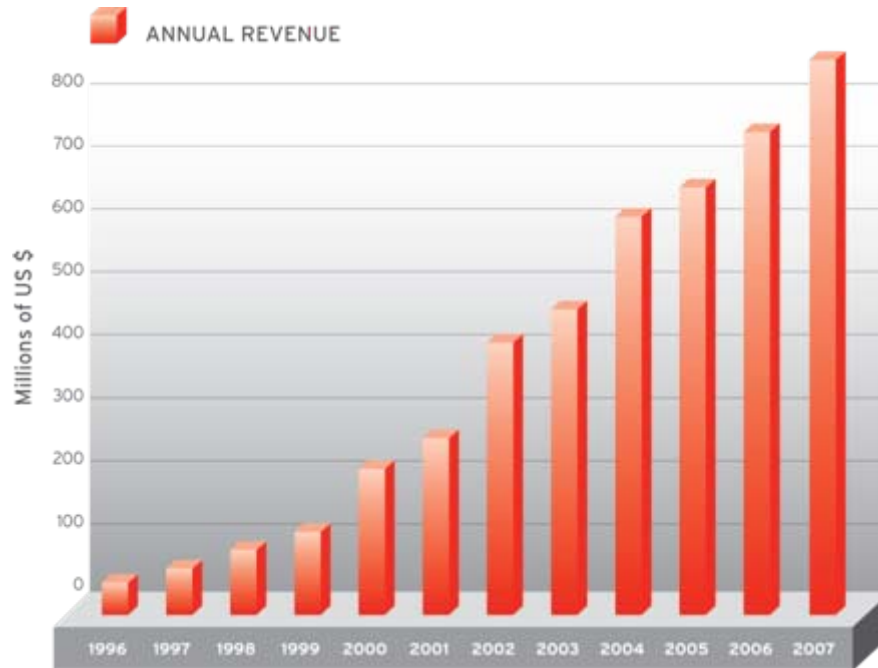
Company Overview



CEO | Eva Chen

Founded United States in **1988**
Headquarters Tokyo, Japan
Employees 3,800+
Market Internet Content Security
2007 Revenue **US \$848 Million**

- Operations in more than 50 countries; 10 global R&D centers
- Tokyo Stock Exchange (4704)



TrendLabs Expertise



TrendLabs helps provide a worldwide platform for delivering timely threat intelligence, service, and support anytime, anywhere.



- More than 1,000 threat research, service, and support experts at 10 locations
- 24/7 operations
- Real-time alerts for new threats

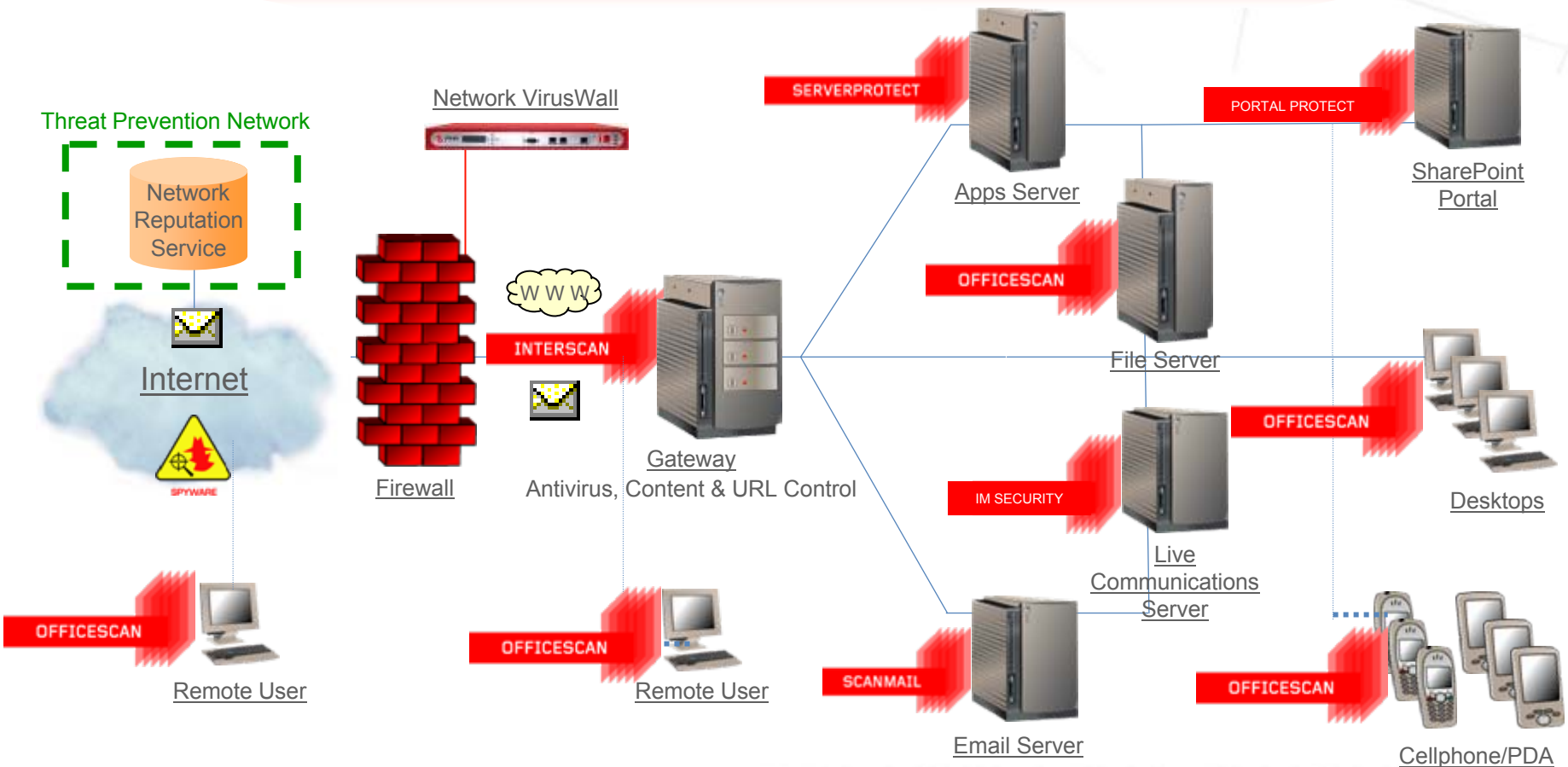
- ▶ Protection requires more than a product...
- ▶ It requires service—timely and expert service.

Trend Micro - The Complete Solution



Trend Micro: Protecting All Layers of the Network

Trend Micro Control Manager - Centralised Outbreak Management



Data Leaks = Executive Visibility



A 24-year-old software engineer at America Online Inc. was arrested yesterday on federal charges that he hacked into the sold and company's computers to steal **92 million** e-mail addresses that were later used to bombard AOL members with spam.

Smathers

Credit card
card accou
considered
holders ar
closely ex
have to wc



aid.

child
HMRC).

Personal d
from the residence of a D...
improperly took the material home. The data...
Security numbers and dates of birth for the veterans, Nicholson...
but "there is no indication at this time" that the data had been used for
identify theft.









The records contain the **names, addresses, dates of birth and National Insurance** numbers of the entire HMRC child benefit database, which also includes the **bank account details of more than seven million.**

Two Primary Concerns:

1. Protect privacy (customer/employee)
 2. Protect intellectual property
- Creates a tremendous need for action*

DLP: Many Reasons to Care



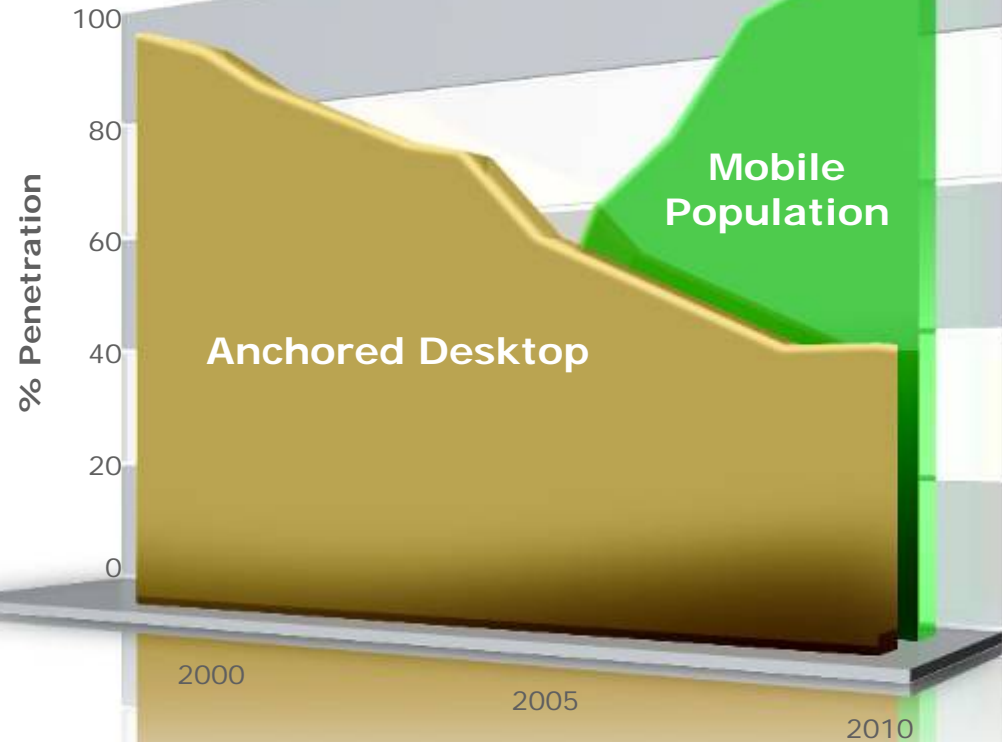
Segment	Privacy	Intellectual Property	Data Leak Threat
Financial Services, Retail			Credit card, accounts, PII, transactions, compliance regulations/fines
Government			Citizen and employee records, legal cases/disclosures
Technology, Manufacturing			Source code, schematics, designs
Pharmaceutical			Formula's, test results/reports, project data
Healthcare, Higher Education			Patient privacy data, diagnoses, credit card and payment info, student data
Public Companies			Pre-disclosure of financials, M&A activity, compliance regulations/fines
Large Employers			Employee records, customer accounts

Mobile Insecurity

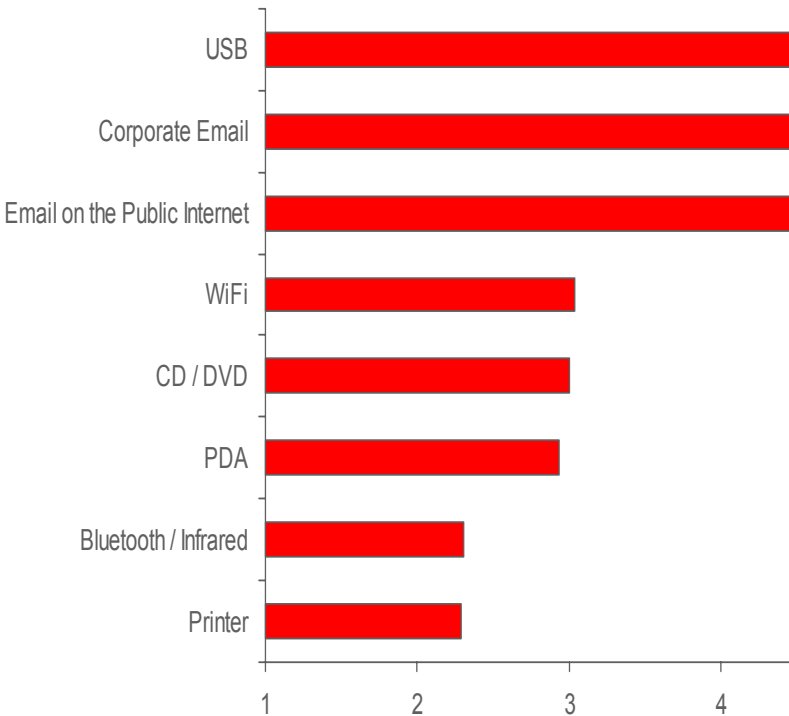


Desktop and Mobile Leakage

Enterprise Mobile Device Market Penetration Over Time



Top Leakage Concerns



Source: Market Research International

Source: The 451 Group and Infolock

The 'Insider Threat'



- 78% of data breaches come from Authorized Insiders

- Ponemon Institute Study – 2006

Authorized Insiders

Threat

- ▶ Accidental or malicious breach

Goals

- ▶ Monitor, log, prevent breaches
- ▶ Assess risk - continuously
- ▶ Educate employees

Un-Authorized Outsiders

Threat

- ▶ Lost or stolen data

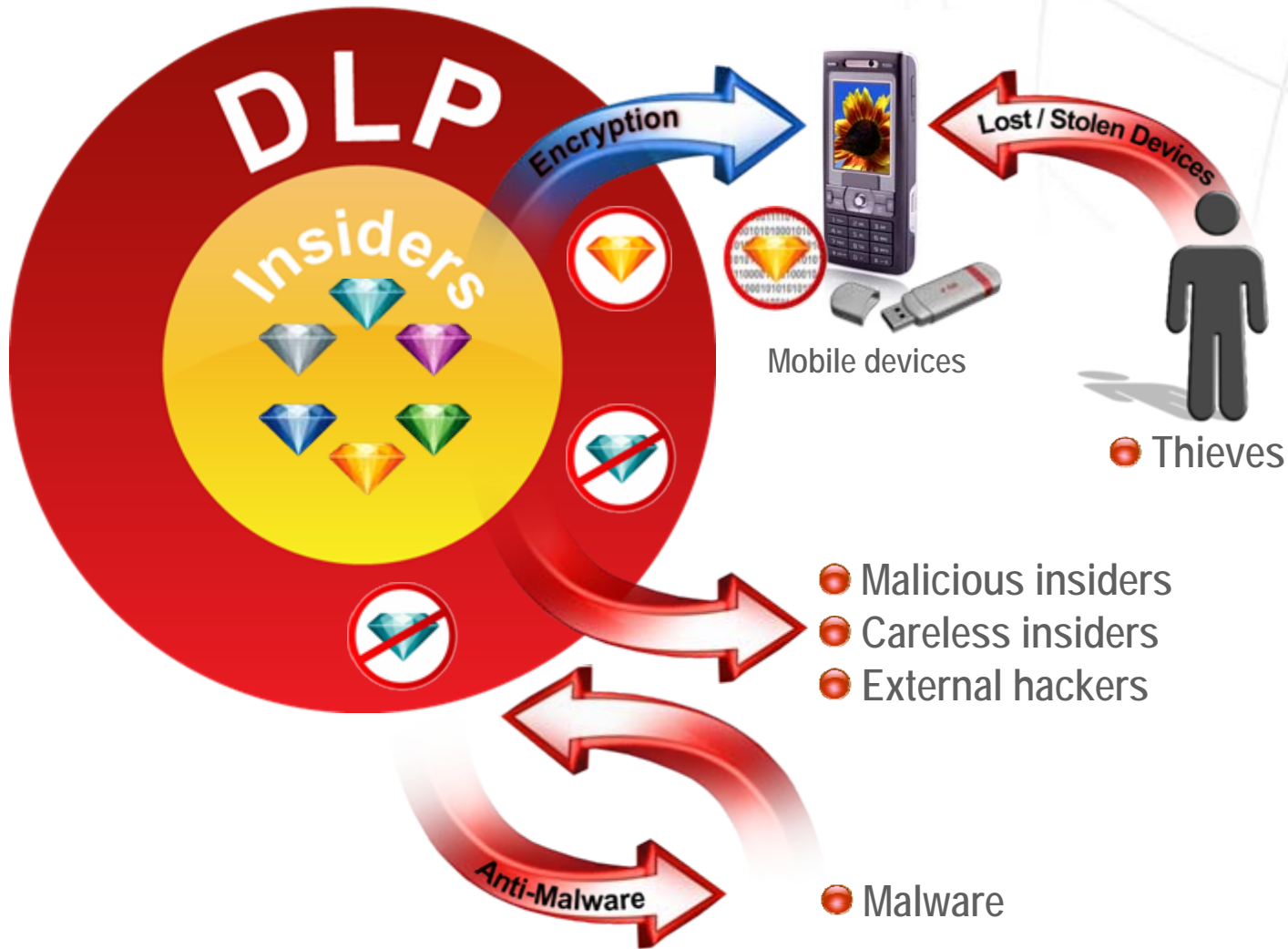
Goals

- ▶ Prevent use of data by unauthorized people

Data Leak Prevention



Layered protection that complements Web Threat Protection





LeakProof enables companies to
reduce the risk
of data breaches and
ensure privacy and compliance

LeakProof understands the content of
data at rest, in use, and in motion
on every enterprise endpoint,
providing protection of sensitive data

Scenes of Mobile Data Leakage

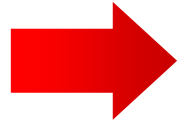


Scene 1



Kristina, at Starbucks™ ...

How do you know?



...edits a confidential document...

How can you tell it wasn't a love letter?



...and emails it

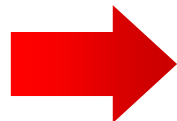
Could you have stopped it?

Scene 2



Gary, at a branch office...

How do you know?



...encrypts customer data...

Is he authorized?



...and copies it

Can you centrally monitor & log?

LeakProof™ Secures From the Endpoint



Client software

- Intelligent
 - Fingerprint, Regex, Keyword, Meta-data
- Interactive
- Invisible
- Independent
- Robust



Anti-leak client



Protect



Educate



Justify



Discover



DataDNA server

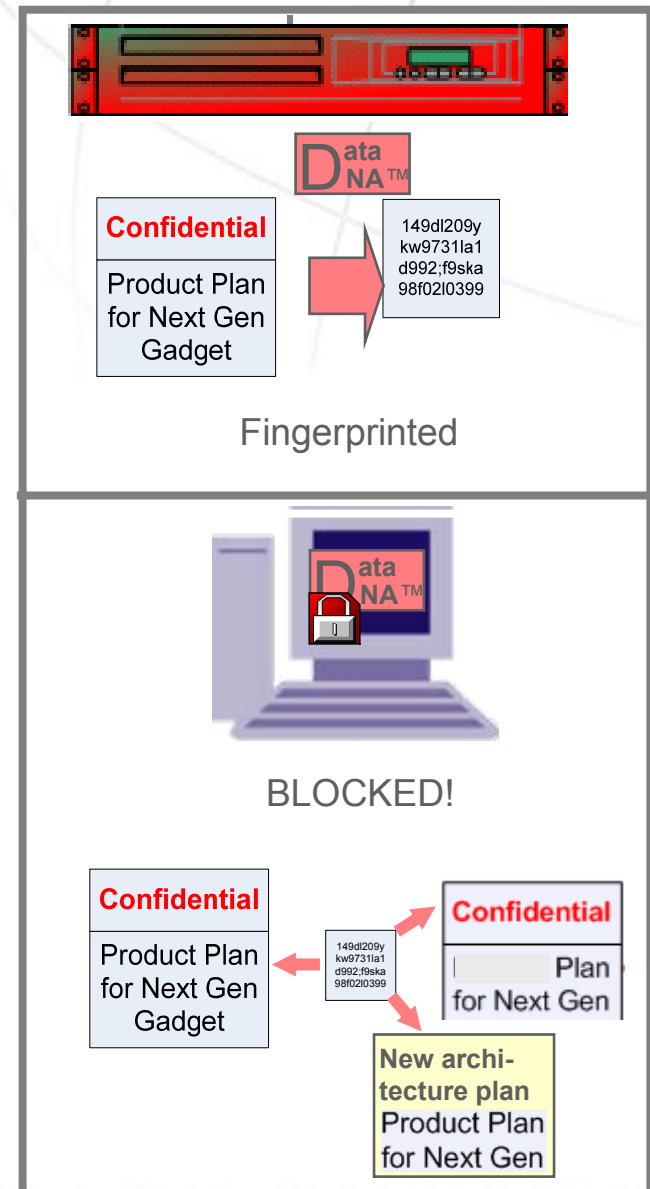


Enterprise management

- Policy
- Visibility
- Workflow

Core Filtering Technology

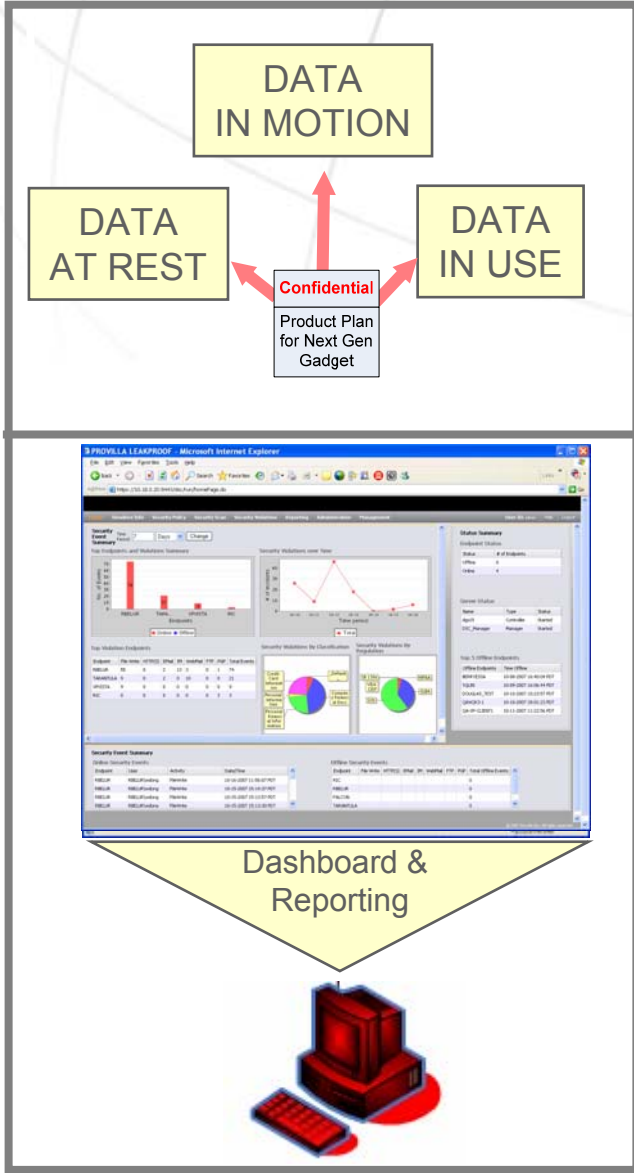
- DataDNA™ Matching Engine
 - High confidence, low false positives
 - Language independent
 - Multiple matching methods
 - Signature/fingerprint
 - Entity / Regex
 - Keyword
 - File meta-data
- Robust Anti-Leak A/L Agent
 - DataDNA matching engine protects
 - Online OR offline
 - On edited, re-saved, cut/pasted content
 - Broadest coverage
 - Devices, channels, applications, email clients, network protocols
 - Authorizes encryption



- Leak Protection Policies
 - Logging, alerting, blocking
 - Education, Encryption, Justification
 - By endpoint, user, or group
 - By data classification
 - HIPAA, Customer, SOX, SS#
 - Separate online and offline policies

- Inventory & Forensics
 - Discovery
 - By endpoint, group, policy
 - Investigate events, see actual sensitive content

- Scalability, Availability
 - Server clustering
 - Agent monitoring





Fast

Performance Evaluation of Anomaly-Based Intrusion Detection

Small

Kymie M.C. Tan and Roy A. Maxion

Accurate

Language Independent

Abstract

Despite the fact that anomaly-based intrusion detection is that one size fits all: a single anomaly detector should detect all anomalies. Cooperation of any performance shortcomings is sometimes offset by relying to correlation techniques, which could be seen as making use of detector diversity. Such diversity is intimately based on the language of the anomalies. Over the years, despite the increasing number of diverse anomaly detectors that have appeared in the intrusion detection literature, there has, unfortunately, not been a concomitant improvement in intrusion detection effectiveness.

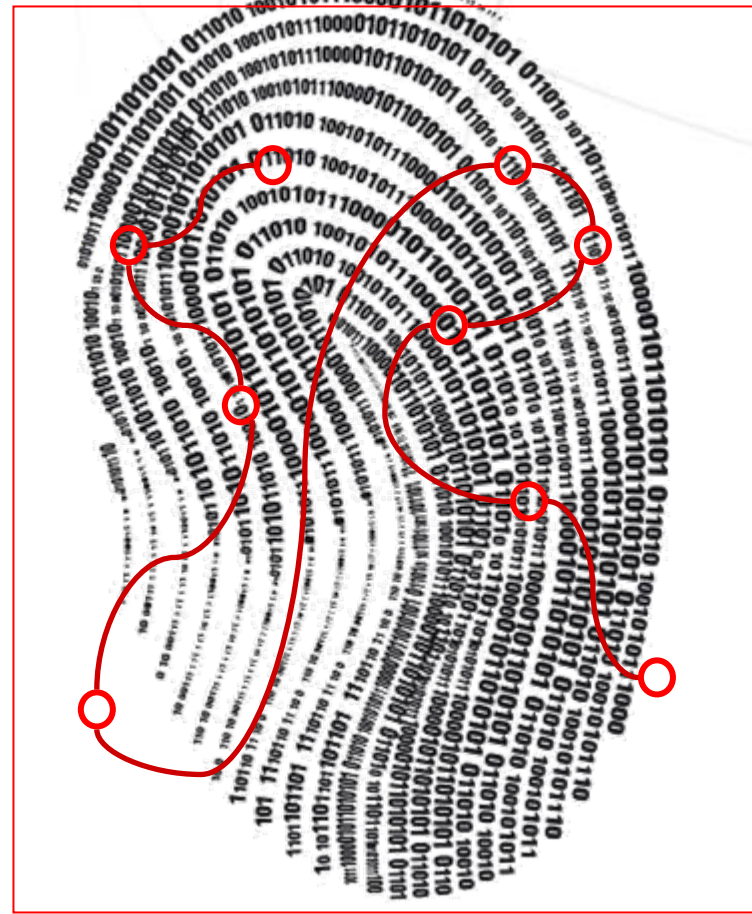
Despite these problems that make an effective anomaly detector an elusive quantity, anomaly detection continues to play a significant role in the intrusion detection arsenal. This is because anomaly detection remains, arguably, the most promising technology for detecting more insidious, and potentially more disruptive, intrusions such as zero-day attacks and insider threats—such incidents are difficult to detect because they typically do not constitute a clear signature of a well-understood attack. Over the years, despite the increasing number of diverse anomaly detectors that have appeared in the intrusion detection literature, there has, unfortunately, not been a concomitant improvement in intrusion detection effectiveness.

In order to address the sluggish progress in the area of anomaly-based intrusion detection requires a slight shift in focus from the creation of ever-nicer, ever-better, anomaly detection algorithms. Strategies are needed that attempt to evaluate, understand and harness the strengths of the detectors that are already present in the literature [29, 26, 30]. These efforts have served to highlight the paucity of evaluation methods for establishing the operational effectiveness of anomaly detectors in a manner that is consistent and repeatable. The lack of such evaluation strategies makes it extremely difficult to assess the effectiveness of anomaly detectors, compare their relative strengths and weaknesses, make measurable improvements to—perhaps more interestingly—understand how to select and combine anomaly detectors effectively to improve detection performance, taking advantage of their inherent algorithmic diversity.

It is interesting to observe that despite the variety of anomaly detectors currently present in the intrusion detection literature, there appears to be an implicit assumption that a single anomaly detection algorithm is all that is required to detect intrusions or attacks on a system. This assertion is supported by a further observation. First, intrusion detection systems claiming to perform anomaly detection typically employ only one kind of anomaly detection algorithm (e.g. [3, 10, 9, 23]). There is, however, no evidence to suggest that a single anomaly detector will be sufficient for a given intrusion detection task. This is mainly because there is currently no study showing that the kinds of anomalies arising as manifestations of at-

1 Introduction

There are many problems that plague anomaly-based intrusion detection systems today; e.g. high false-alarm rates [5], inconsistency of detector performance [10, 30], training issues, e.g. how often should an anomaly detection system be retrained to ensure acceptable performance [2], inadvertent incorporation of normal behavior into a detector's concept of normal behavior possibly causing the intrusion to be missed by the detector [13], and so forth.



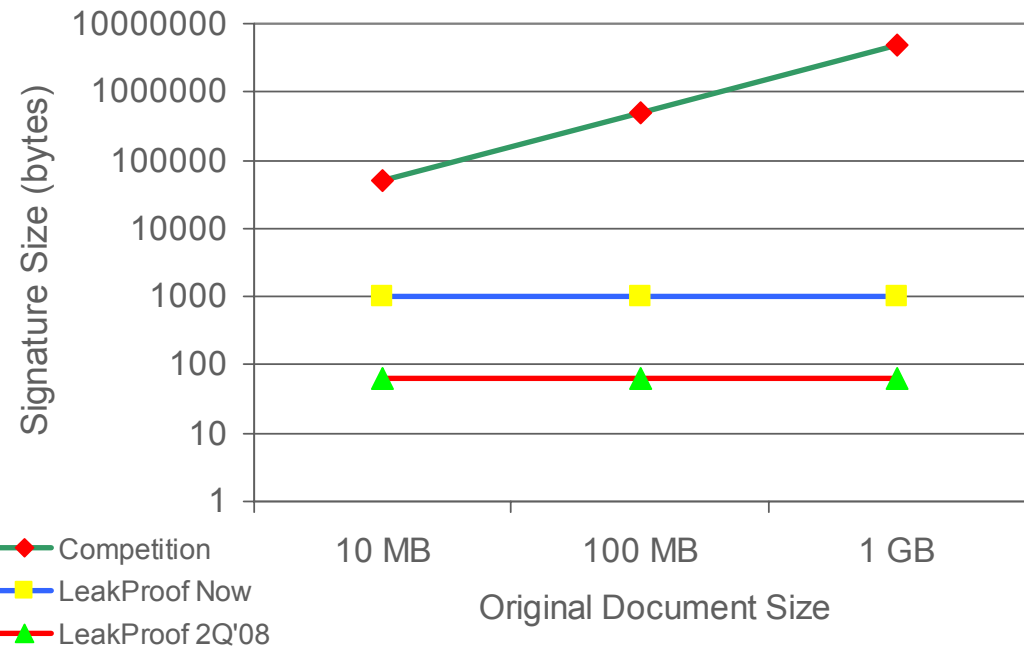
Leading Agent Performance and Technology



- Fast and light
- Fastest matching engine
- Smallest signatures
- Unobtrusive, invisible
 - Not in task manager
 - Not in service list
 - Hidden files/directory

CPU cycles		2.54% (1/2)
Run-time Memory		8,280K (1/5)
Search	Provilla A/L Agent	Competition
Keywords: 1000	12.0 MB/s (10x)	1.3 MB/s
Entity –SSN, Phone, Date	190 MB/s (40x)	4.75 MB/s

Fixed Signature Size



New Dashboard and Workflow



PROVILLA LEAKPROOF - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address: https://10.18.0.20:8443/dsc/run/homePage.do

Home Sensitive Info Security Policy Security Scan Security Violations Reporting Administration Management User ID: admin Help Logout

Security Event Summary

Time Period: 7 Days Change

Top Endpoints and Violations Summary

Endpoint	Online	Offline
RBELUR	74	0
TARA...	21	0
XPVISTA	9	0
RIC	3	0

Security Violations over Time

Time period	Total
10-10	25
10-11	10
10-12	45
10-13	18
10-14	0
10-15	2
10-16	5

Top Violation Endpoints

Endpoint	File Write	HTTP(S)	Email	IM	WebMail	FTP	PGP	Total Events
RBELUR	55	0	2	13	3	0	1	74
TARANTULA	9	0	2	0	10	0	0	21
XPVISTA	9	0	0	0	0	0	0	9
RIC	0	0	0	0	0	0	3	3

Security Violations By Classification

Security Violations By Regulation

Status Summary

Status	# of Endpoints
Offline	0
Online	4

Server Status

Name	Type	Status
dgs15	Controller	Started
DSC_Manager	Manager	Started

Top 5 Offline Endpoints

Offline Endpoints	Time Offline
BERRYESSA	10-08-2007 16:40:04 PDT
YQLIN	10-09-2007 16:06:44 PDT
DOUGLAS_TEST	10-10-2007 10:23:57 PDT
QAW2K3-1	10-10-2007 18:01:23 PDT
QA-XP-CLIENT1	10-11-2007 11:22:56 PDT

Security Event Summary

Online Security Events

Endpoint	User	Activity	Date/Time
RBELUR	RBELUR\wdong	FileWrite	10-16-2007 11:56:07 PDT
RBELUR	RBELUR\wdong	FileWrite	10-15-2007 15:14:37 PDT
RBELUR	RBELUR\wdong	FileWrite	10-15-2007 15:13:57 PDT
RBELUR	RBELUR\wdona	FileWrite	10-15-2007 15:13:30 PDT

Offline Security Events


Endpoint	File Write	HTTP(S)	Email	IM	WebMail	FTP	PGP	Total Offline Events
RIC								0
RBELUR								0
FALCON								0
TARANTULA								0

Employee Education





Brandable
Logo and custom
messages

Security alert!



**TREND
MICRO™**

The data you are sending or copying contains sensitive information.
You have 2 message(s).

	Time	Message	Link
	12:26.22	Hello, this is security alert!	www.trendmicro.com
	12:26.22	File transfer: E:\CreditCardNumber10.tx...	

Powered by Trend Micro, Inc. All rights reserved.

Dismiss

ACME Laboratories - Microsoft Internet Explorer

Address <http://www.acme.com/>

ACME Customer Privacy Protection

Employees of ACME are expected to protect sensitive information containing customer information such as names, account numbers, social security numbers etc. Please report any ... Call the helpdesk or email.

ACME Laboratories - Microsoft Internet Explorer

Address <http://www.acme.com/>

Protection of Intellectual Property

The IP of ACME is very valuable to us, and we expect all employees to help protect this data. Files containing IP secrets should not be emailed, copied to USB, ... If you have any questions about this, please contact HR at ...

Custom Links
Company Policies

Severity
Blocked, warn & log,
info only

Custom Alert Messages
File {name} contains {class} data and should
not be sent via {channel}

How to deploy Effective DLP



Recent Leaks



Compliance

1. Identify the pain



2. Identify the data



3. Understand the threat

People



Process

Technology

4. Evaluate & Deploy

The LeakProof Difference



- Most COMPREHENSIVE coverage of leakage vectors, channels, and languages with best performance, security, matching engine, signature technology
 - **Alternatives have weak, immature endpoint coverage**
- Endpoint is MOST SCALABLE for enterprise
 - **Network solutions don't scale well, require third parties to enforce**
- INTELLIGENT about sensitive content
 - Non-intrusive, not 'tagging' based, not limited to device controls
 - **Alternatives don't have true content awareness at endpoint**

LeakProof 3.0 Extends Endpoint Leadership



● Broadest DLP Threat Protection at the endpoint

- USB, email, webmail, IM, network

NEW

- Windows Vista / Office 2007, Yahoo IM filtering, PrintScreen blocking

● Interactive employee education & workflow

- Log, block, client alert

NEW

- Education: custom messages and URL links

NEW

- Encryption for USB copying

NEW

- Justification

● Discovery of sensitive data

BETTER

- Stand-alone discovery/scan module

● Administrative workflow

BETTER

- Dashboard, policies, and monitoring

Thank You

Trend Micro

Securing Your Web World

