Attacks from the Inside

Eddy Willems, G Data

Righard J. Zwienenberg, Norman

Attacks from the Inside.

Agenda

- Social Networking / Engineering
- Where are the threats coming from
- Infection vectors
- The Cloud
- Q&A

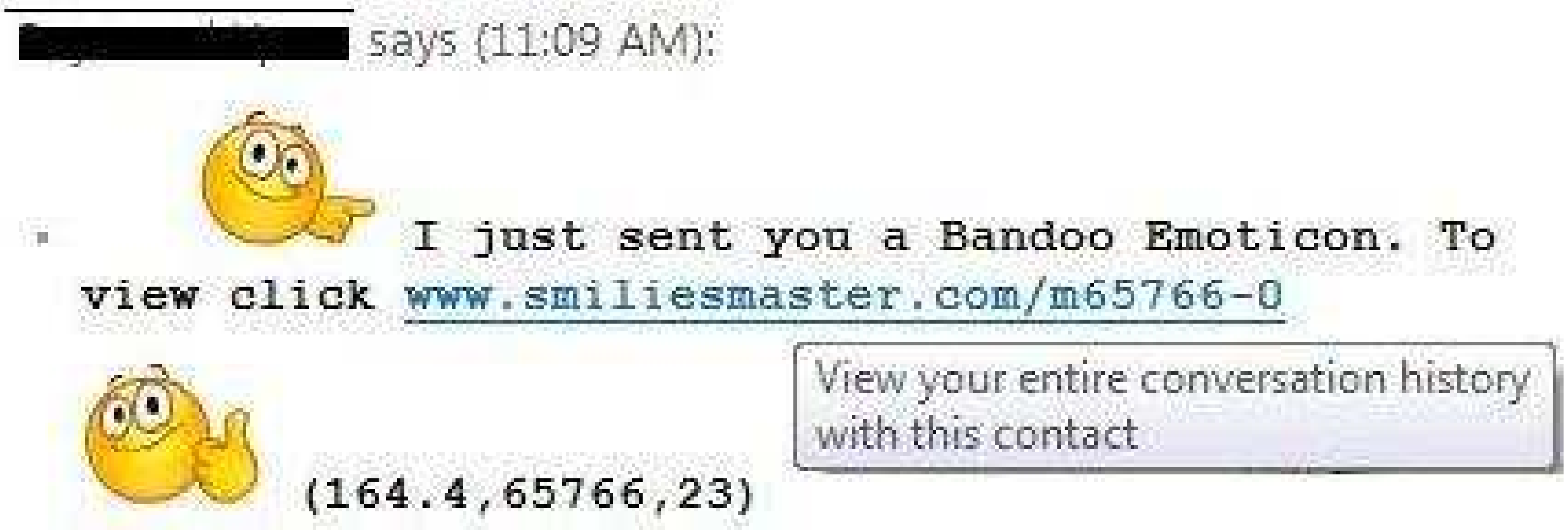
New territories: Social Networking

- Blogs, forums
- Wiki
- MySpace, YouTube
- Other online communities:

Who’s on Facebook, Twitter?

Social networking and privacy concerns.

And how it is to be fooled



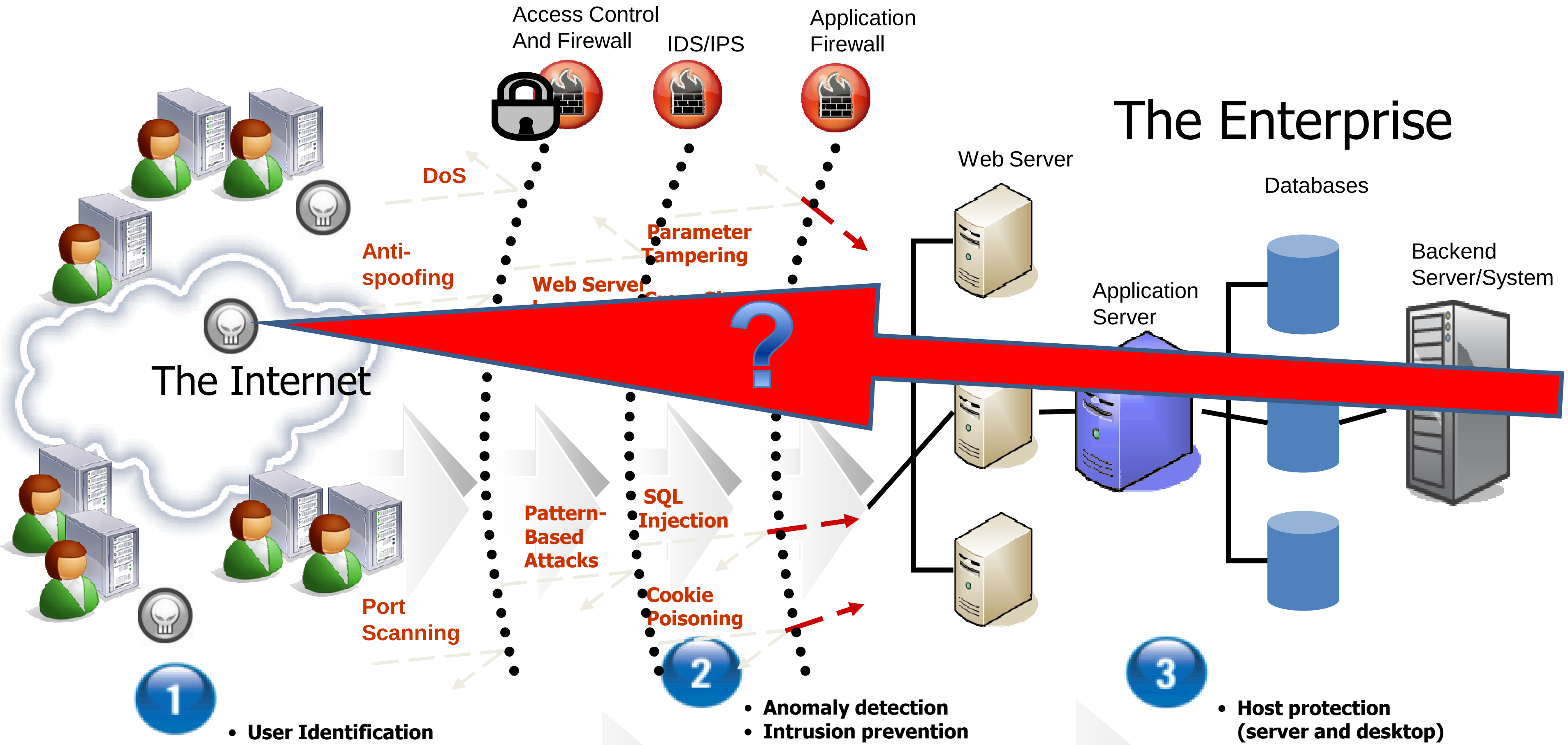
[redacted] says (11:09 AM):

I just sent you a Bandoo Emoticon. To view click www.smiliesmaster.com/m65766-0

(164.4,65766,23)

View your entire conversation history with this contact

The Threats only originated from outside?



- User Identification
- Access Control
- Encrypted transport of data
- Firewall
- Universal threat management

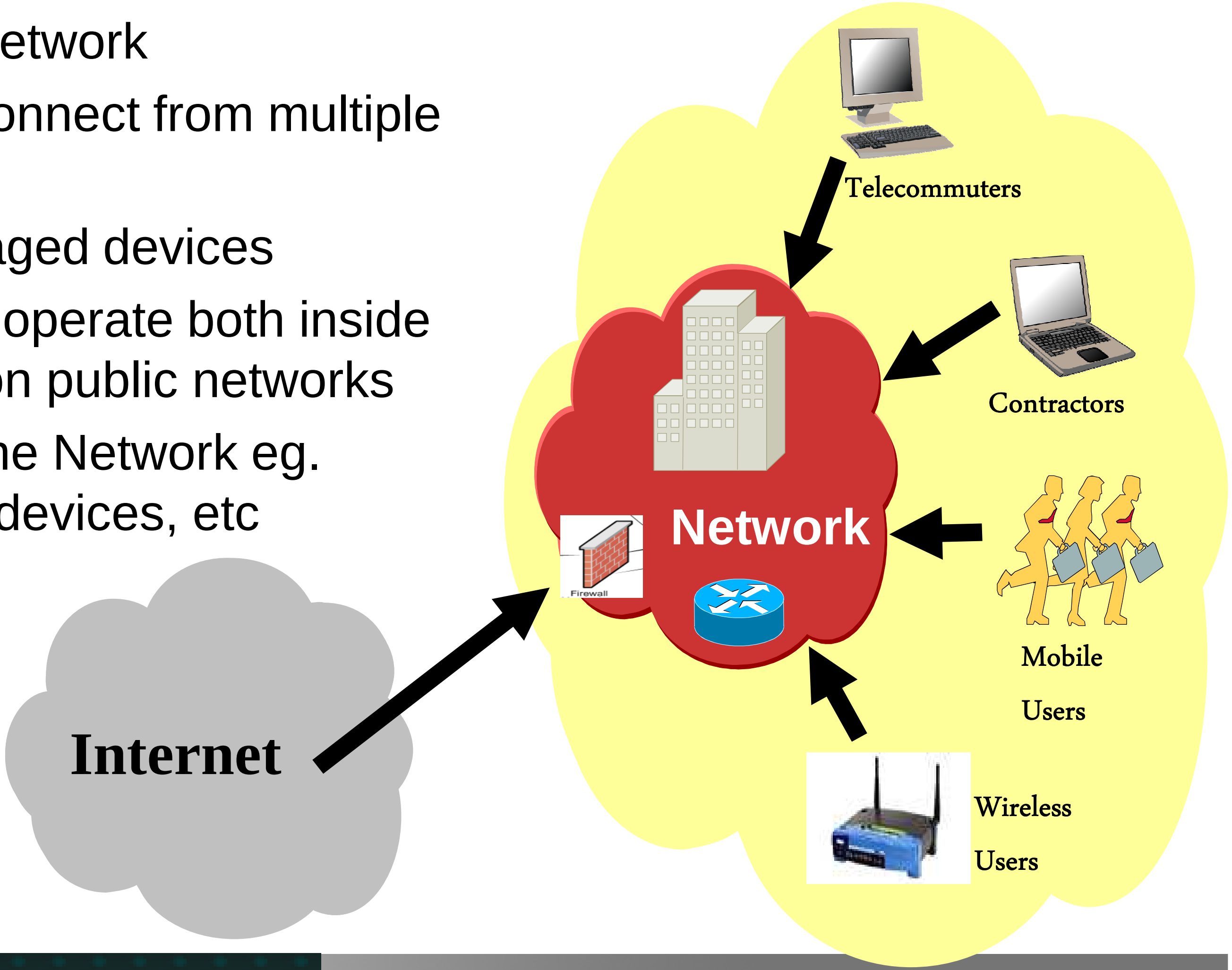
- Anomaly detection
- Intrusion prevention
- Vulnerability management
- Remediation/Patching
- Compliance and risk management

- Host protection (server and desktop)
- Layer 4 – 7 protection (content, URL, Web)
- Content Control
- Data Leakage management

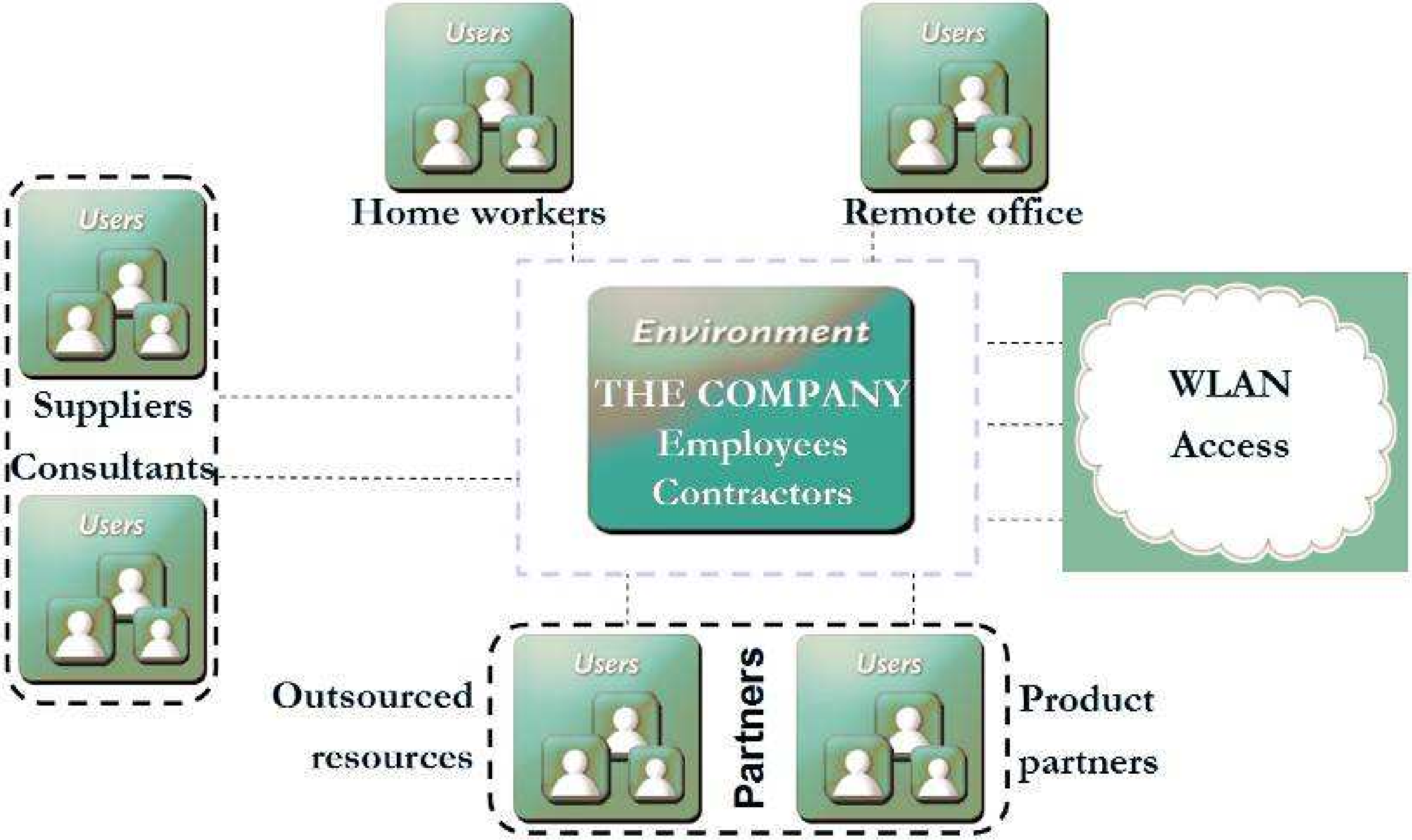
Source:IBM

Today’s Networks Lack Clear, Crisp Boundaries.

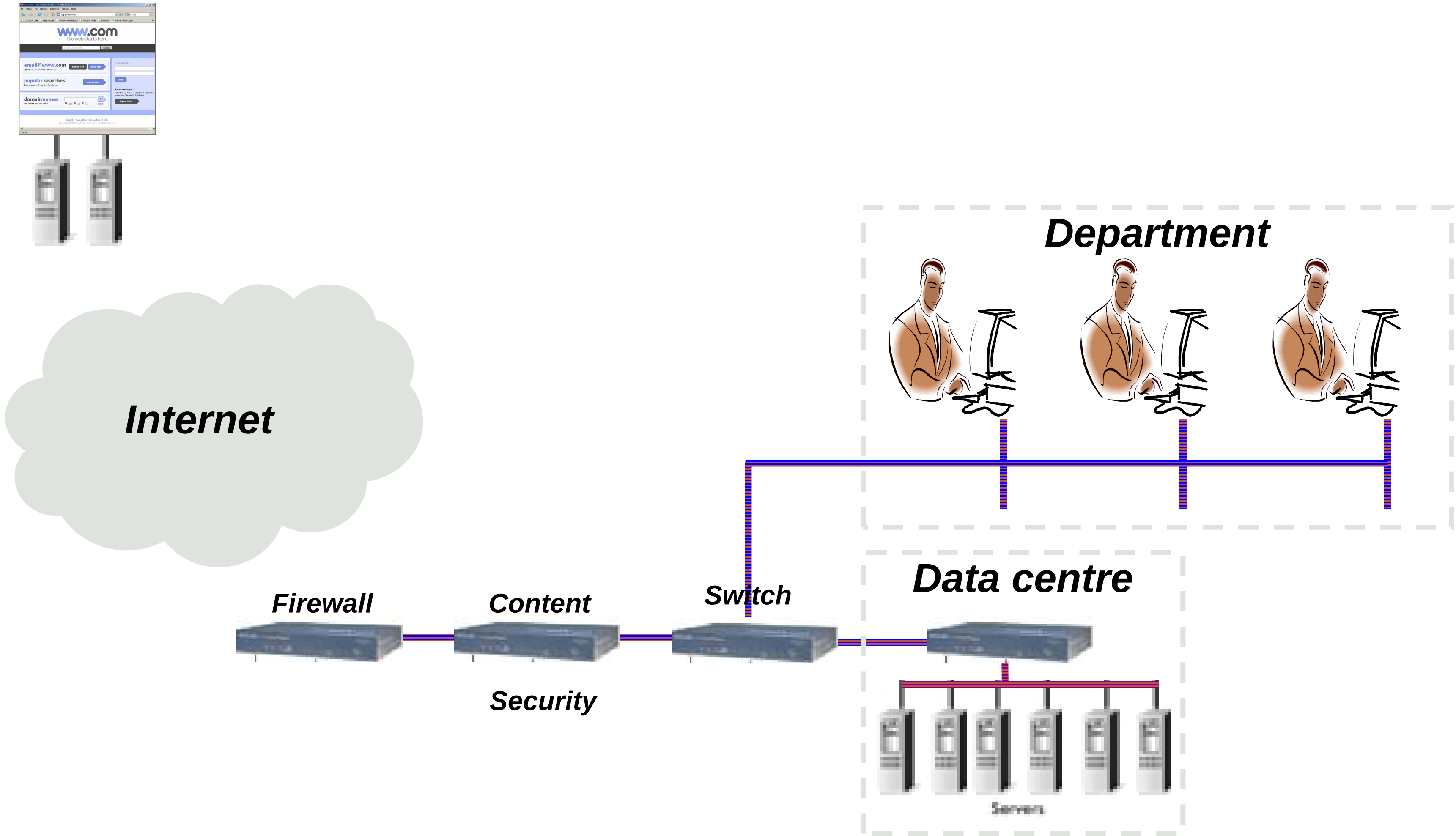
- Internal/External network
- Individual Users connect from multiple locations
- Managed/Unmanaged devices
- Individual devices operate both inside the network, and on public networks
- New Devices on the Network eg. Netbooks, Mobile devices, etc



Today's networks



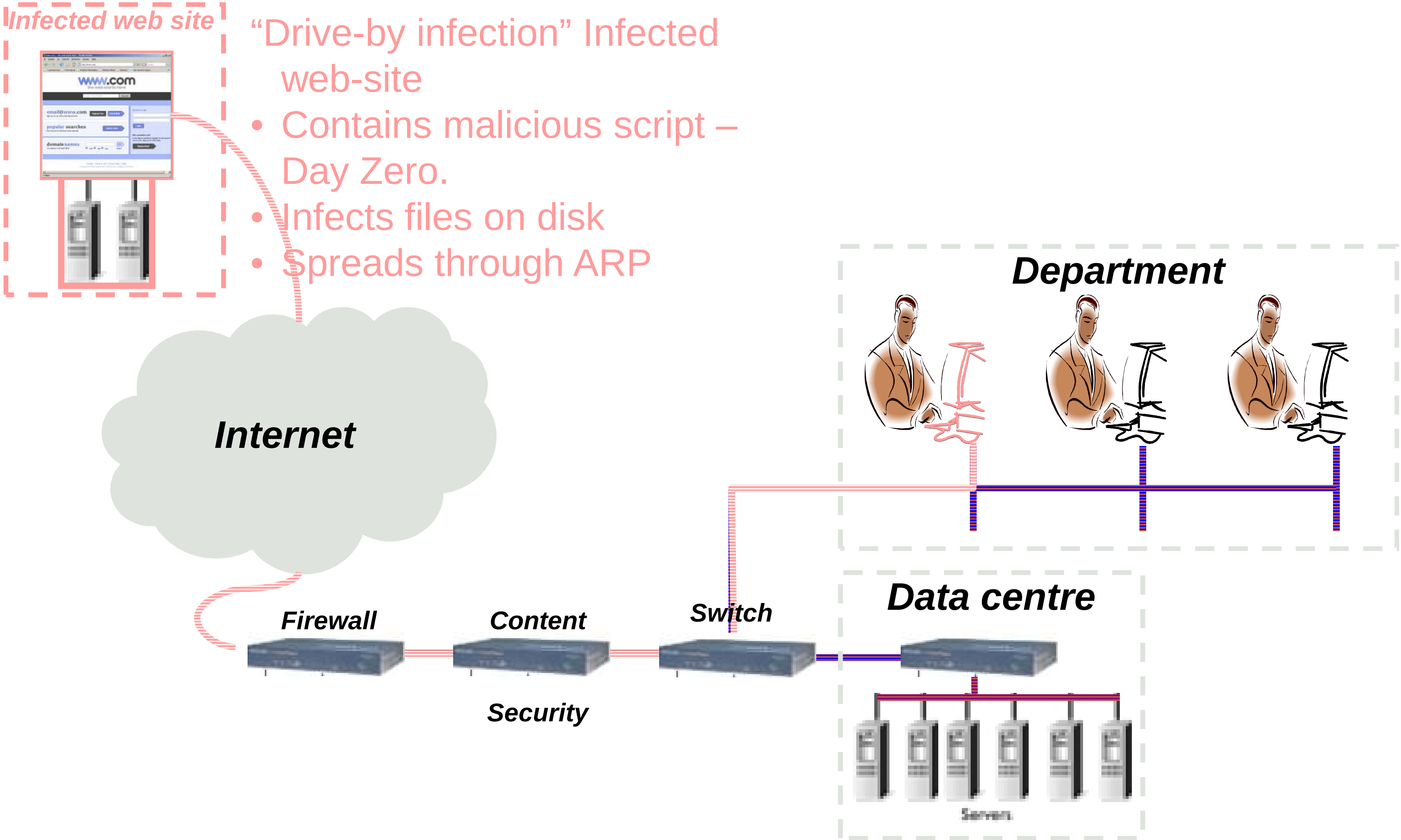
Infection scenario – Start



Infection scenario – “drive by infection”

“Drive-by infection” Infected web-site

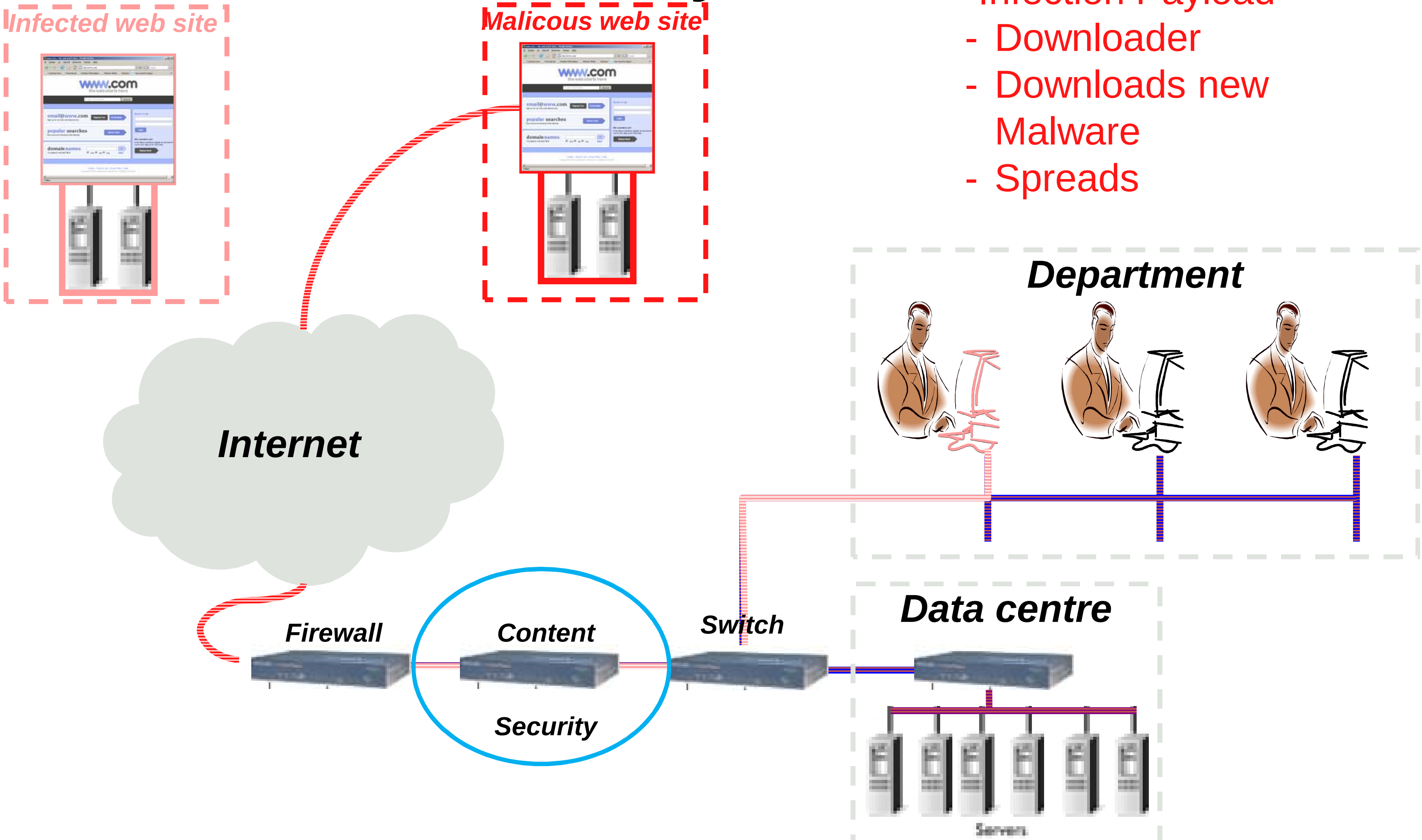
- Contains malicious script – Day Zero.
- Infects files on disk
- Spreads through ARP



Infection scenario II – "Payload"

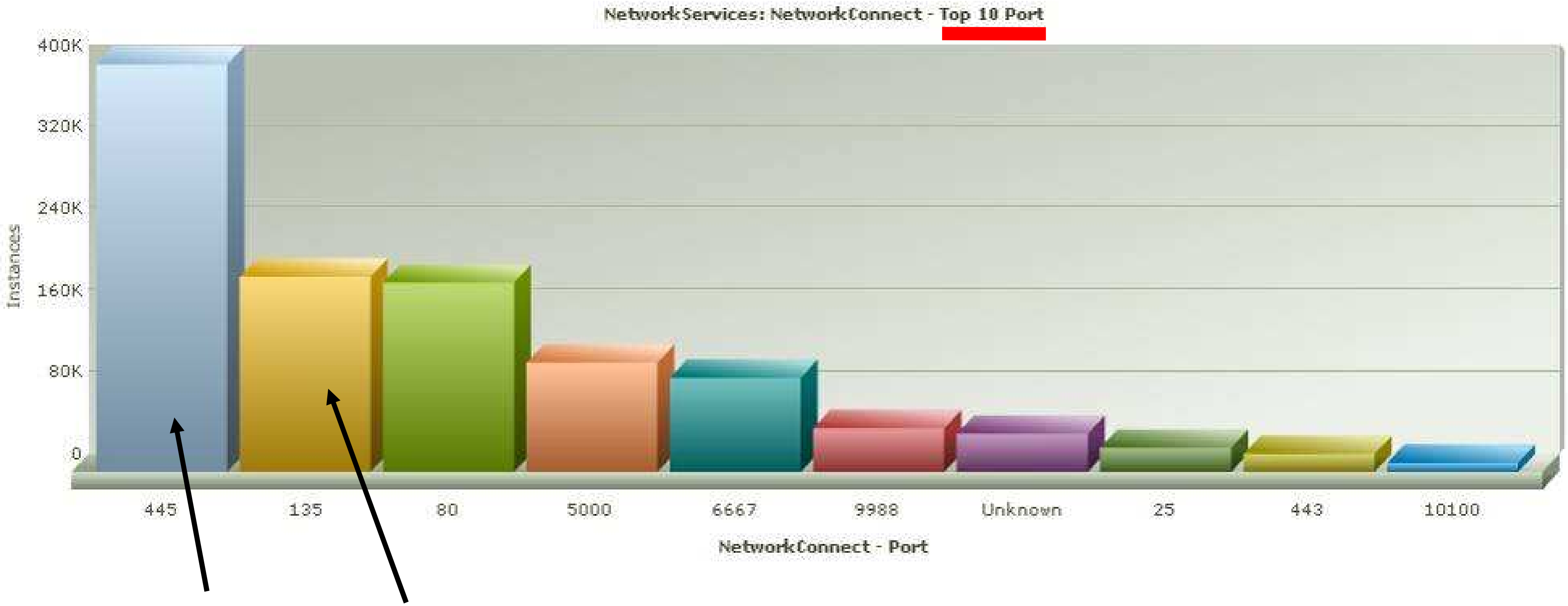
"Infection Payload"

- Downloader
- Downloads new Malware
- Spreads



Most used spreading protocols

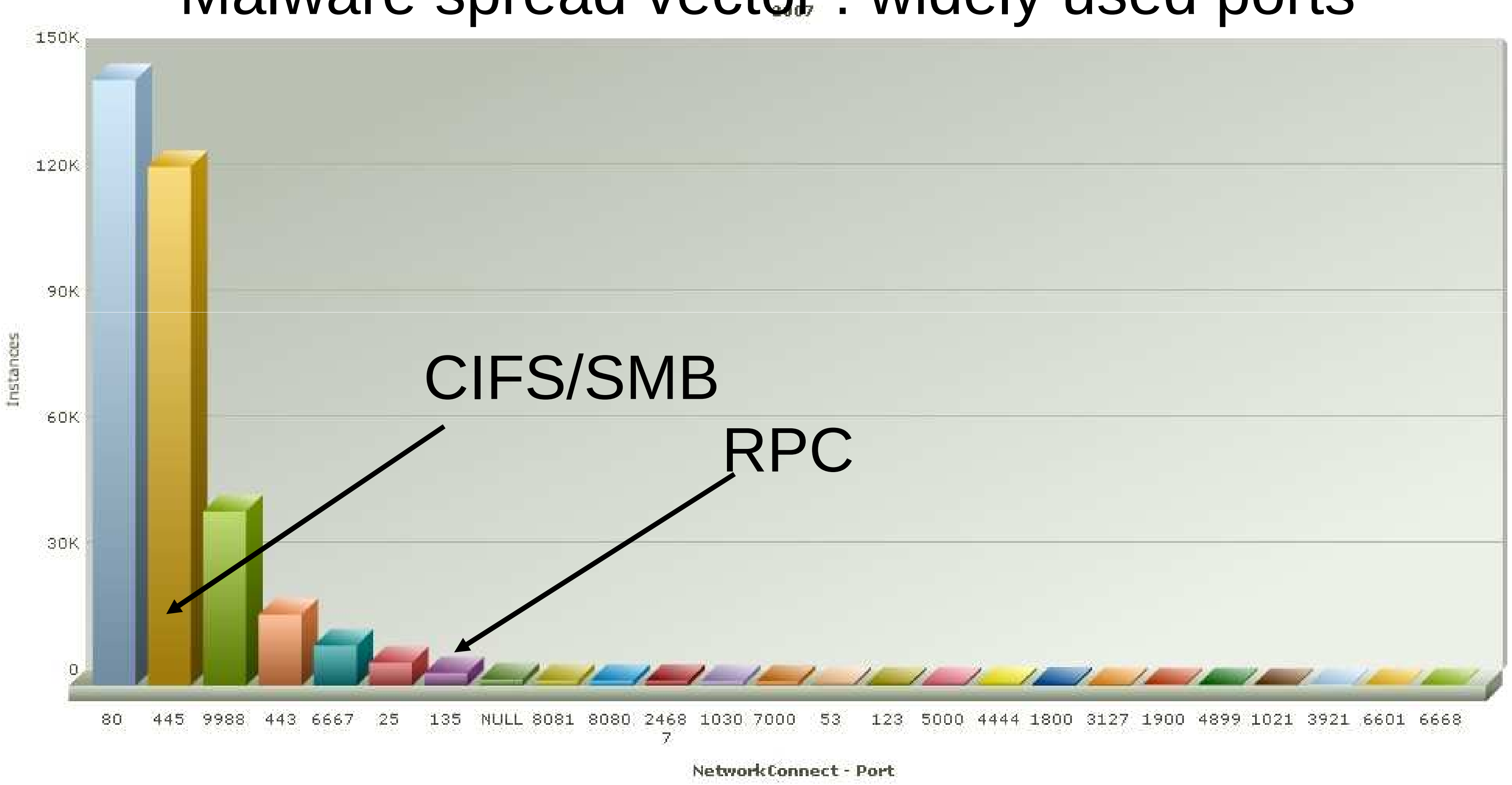
Malware spread vector: widely used ports



CIFS/SMB RPC

Why are CIFS and SMB important?

Malware spread vector : widely used ports



CIFS/SMB

RPC

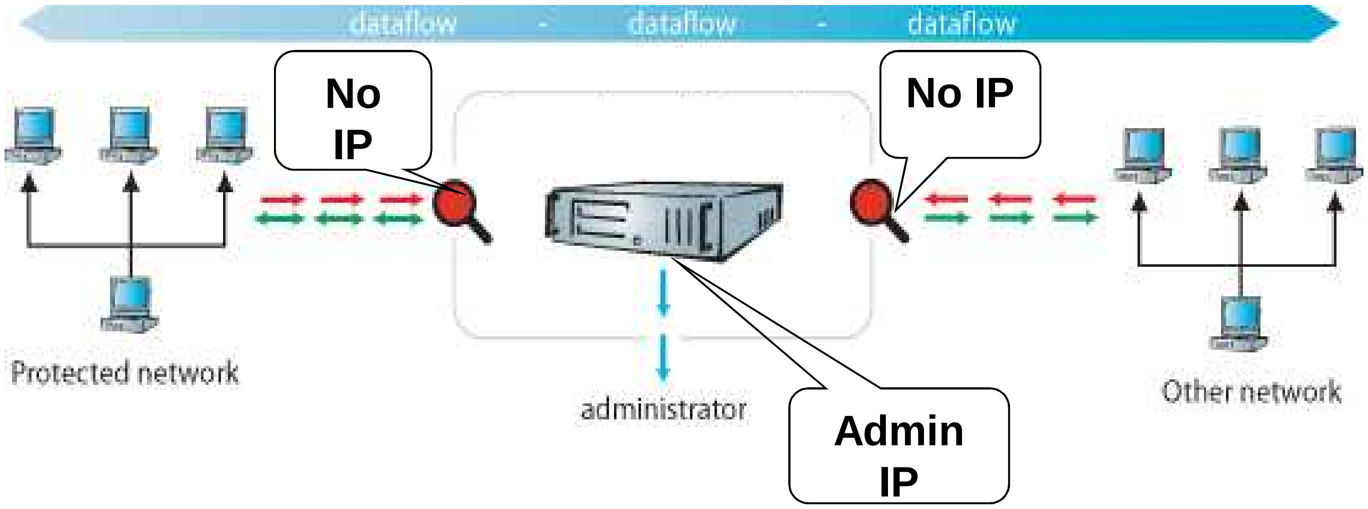
Avoid infections

- User training (MSN, unknown pop-up’s, e-mail, etc.)
- Patch management
- (Hardware) Remediation
- Anti-virus management
  - Activated, according to policies
  - Up-to-date definition files
  - Discovery of unknown nodes in the network
  - Alerts
- In-line Network traffic content scanning

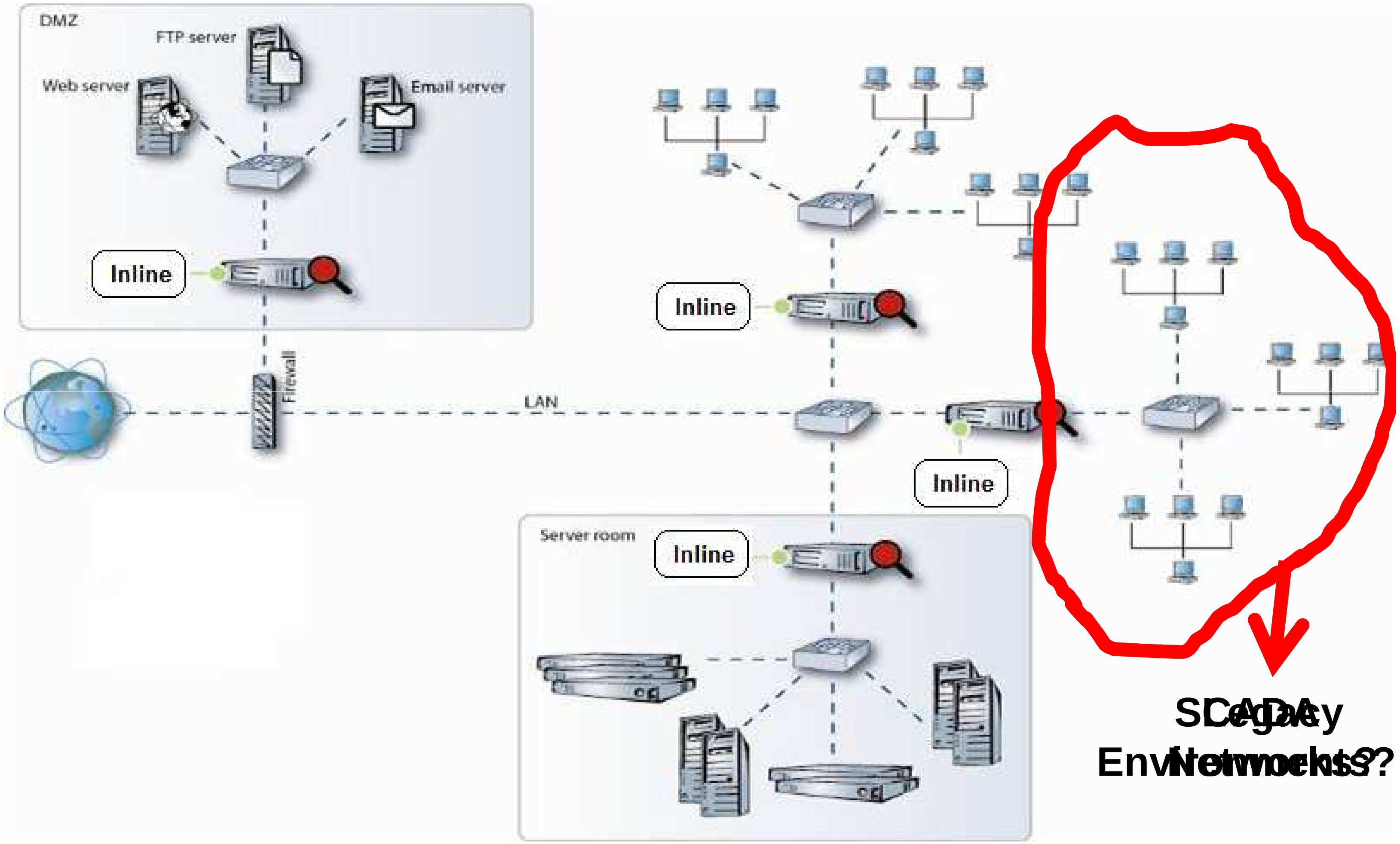
In-Line Network Content Scanner

Network transparent real-time malware-scanner

Scans HTTP, FTP, SMTP, TFTP, RPC, POP3, IRC, SMB/CIFS



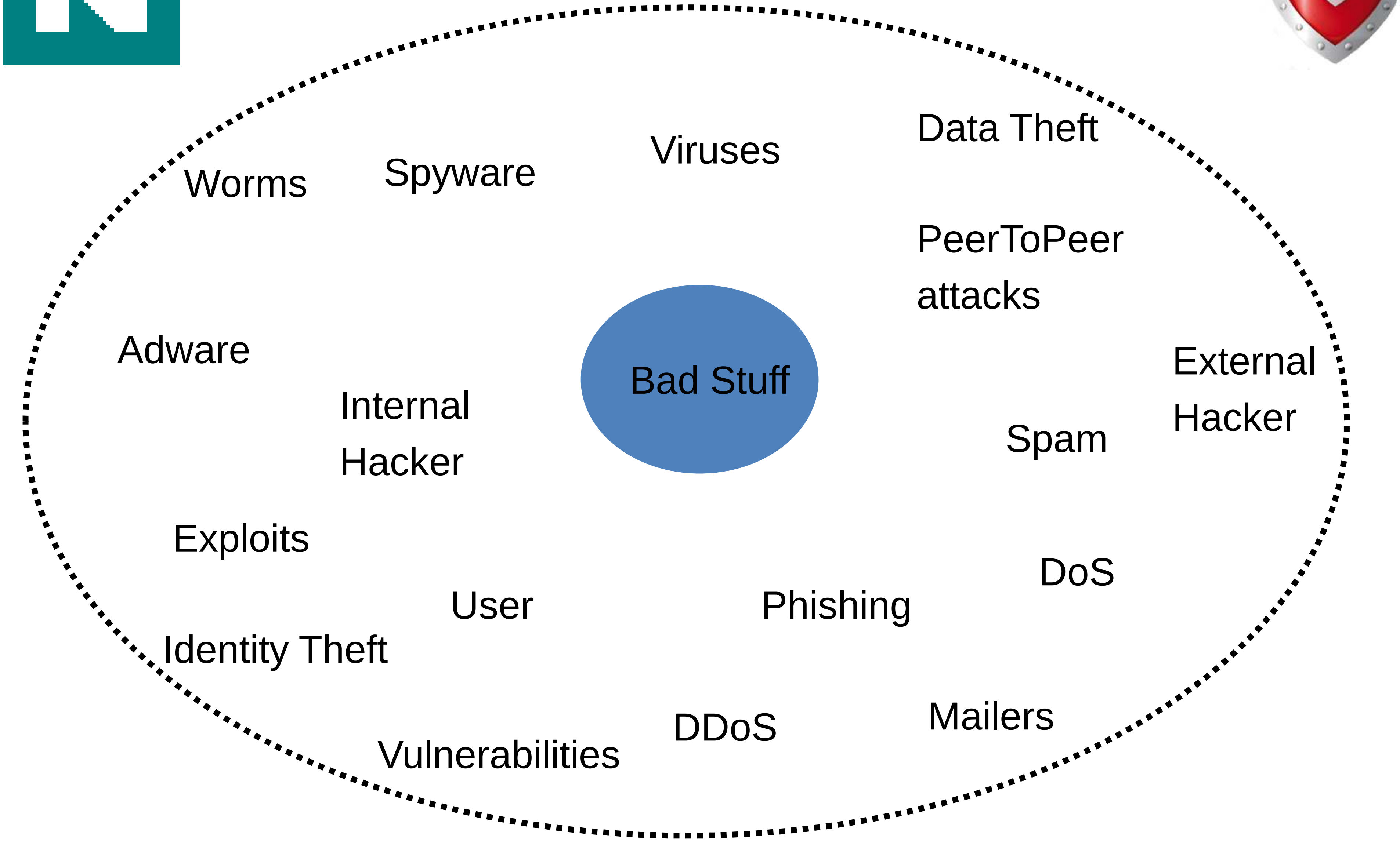
Content scanning: where to install?



SCADA Environments?

Legacy Networks?

Changing Solutions ?



Worms

Spyware

Viruses

Data Theft

PeerToPeer attacks

Adware

Internal Hacker

Bad Stuff

External Hacker

Spam

Exploits

User

Phishing

DoS

Identity Theft

Vulnerabilities

DDoS

Mailers

In the Cloud

Difficult to “lay down” a definition as it depends on the use

“Cloud Computing is an on-demand service model of IT provision often based on virtualization and distributed computing technologies. It’s divided up in several categories.”

Working definition from Enisa

In the Cloud: SaaS

Software as a Service:

- SaaS is software offered by a third-party provider, available on demand, usually via the Internet and remotely configurable.
- Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (*Google Docs, etc.).*

In the Cloud: PaaS

- Platform as a Service

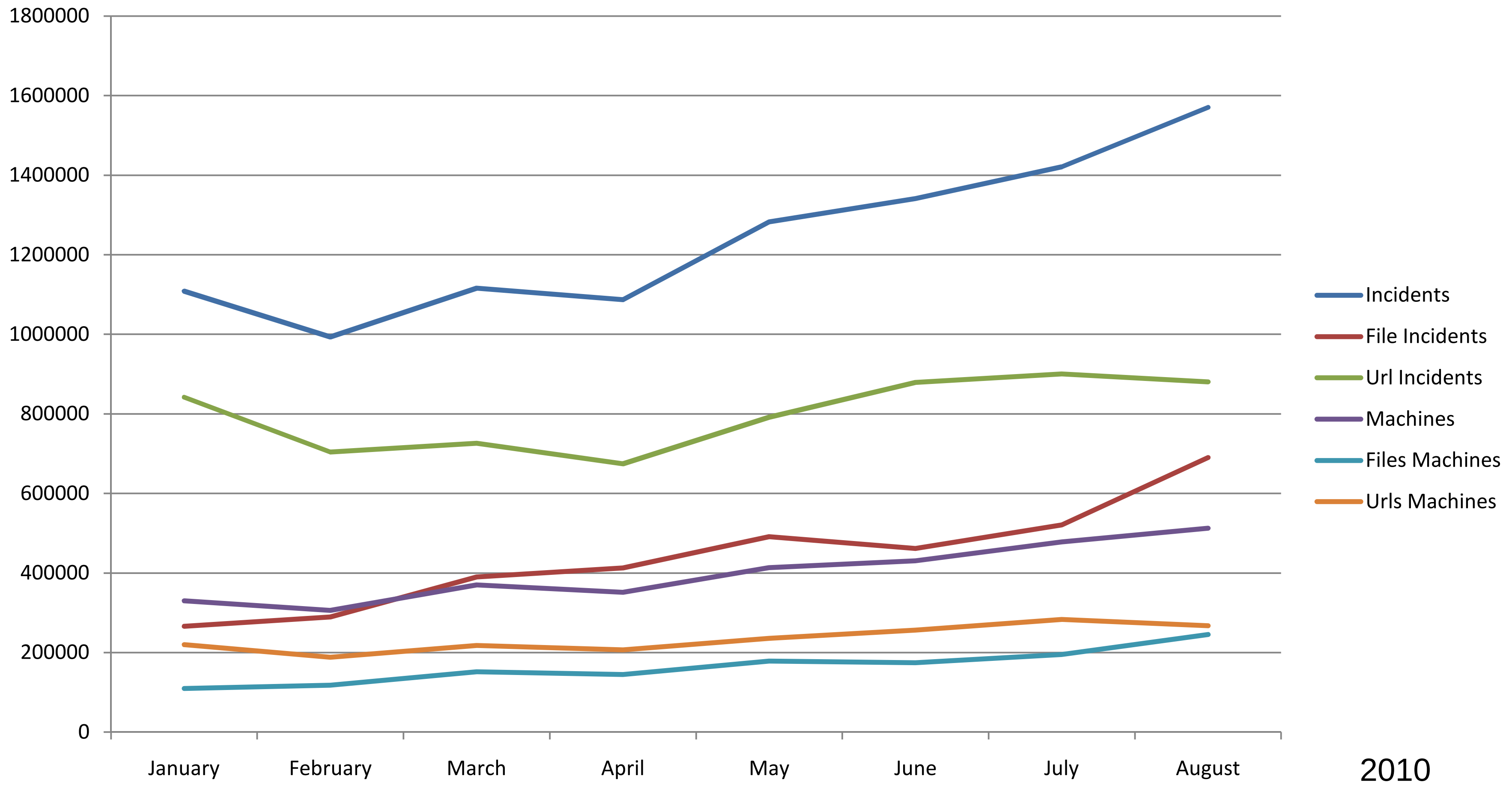
- PaaS allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management and deployment platforms.
- Examples are *Microsoft Azure or the Google App* engine

In the Cloud: IaaS

- Infrastructure as a Service

- IaaS provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API.
- Examples are *Terremark Enterprise Cloud, Windows Live Skydrive, etc …*

Malware Information Initiative (Mii)
In the Cloud technology



NORMAN® Proactive IT security
Go safe. Go safer. G Data.

The security benefits of cloud computing:

- The benefits of scale and rapid smart scaling of resources
- Standardized interfaces for managed security services
- Audit and evidence gathering
- More timely, effective and efficient updates and defaults.

We love cloud computing

Questions:

What about the in-the-cloud infrastucture ? DDOS?

Could it be circumvented?

How will the user react?

How will the vendor react?

Top 9 “In-The-Cloud” Problems

#9 Identity management

Top 9 “In-The-Cloud” Problems

#8 Nefarious use of Service

Top 9 “In-The-Cloud” Problems

#7 Account/Service Hijacking

Top 9 “In-The-Cloud” Problems

#6 Financial DDOS

Top 9 “In-The-Cloud” Problems

#5 Data Loss/Data Leakage

Top 9 “In-The-Cloud” Problems

#4 Unknown Risk Profile

Top 9 “In-The-Cloud” Problems

#3 Hidden Logs/Intrusion Attempts

Top 9 “In-The-Cloud” Problems

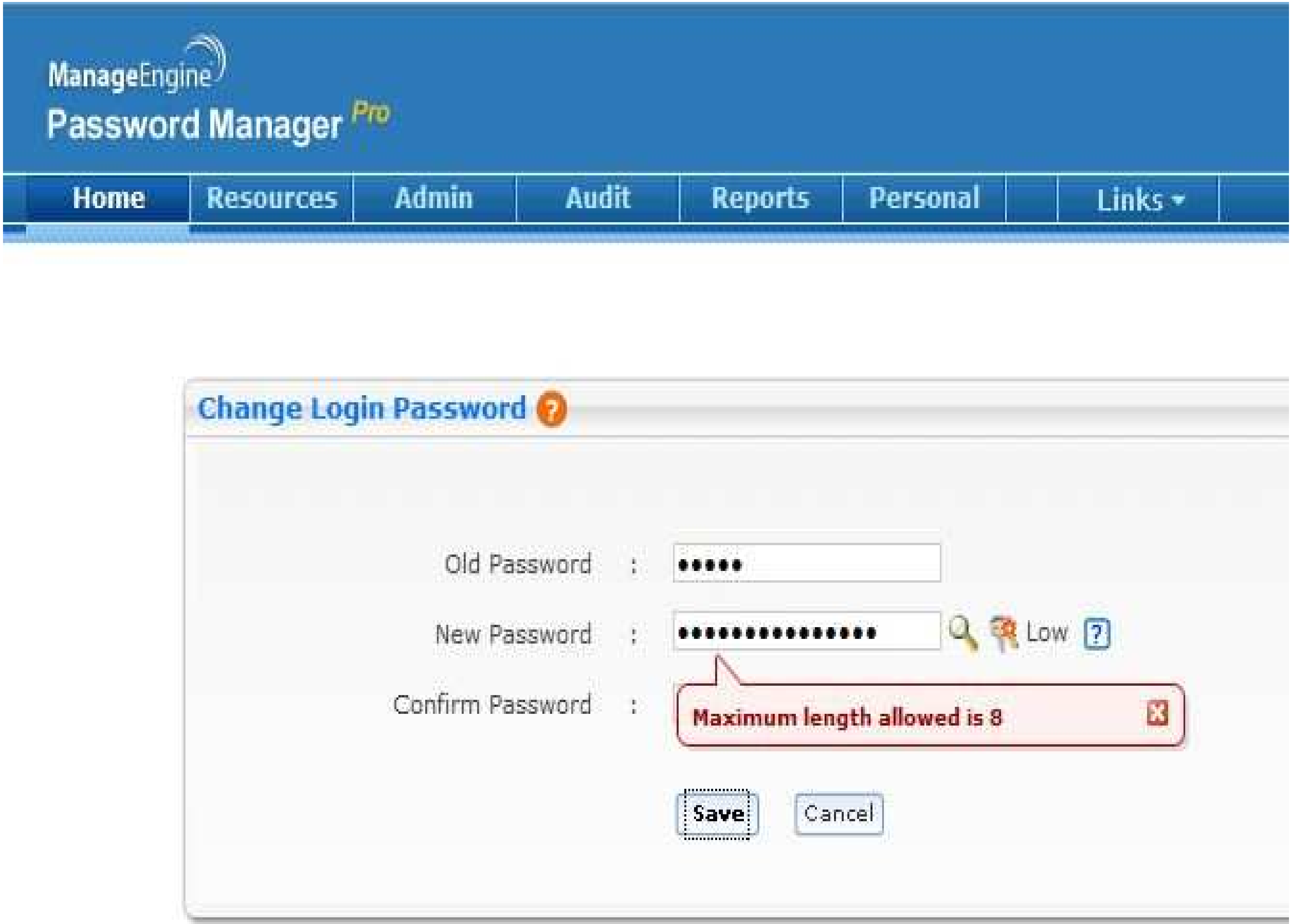
#2 Insider abuse

Top 9 “In-The-Cloud” Problems

#1 Centralized AAA Abuse/Trust (Authentication,Authorization en Accounting)

Now you see why we love the cloud ...

Clouds



Change Login Password

Old Password : •••••

New Password : ••••••••••••••• Low ?

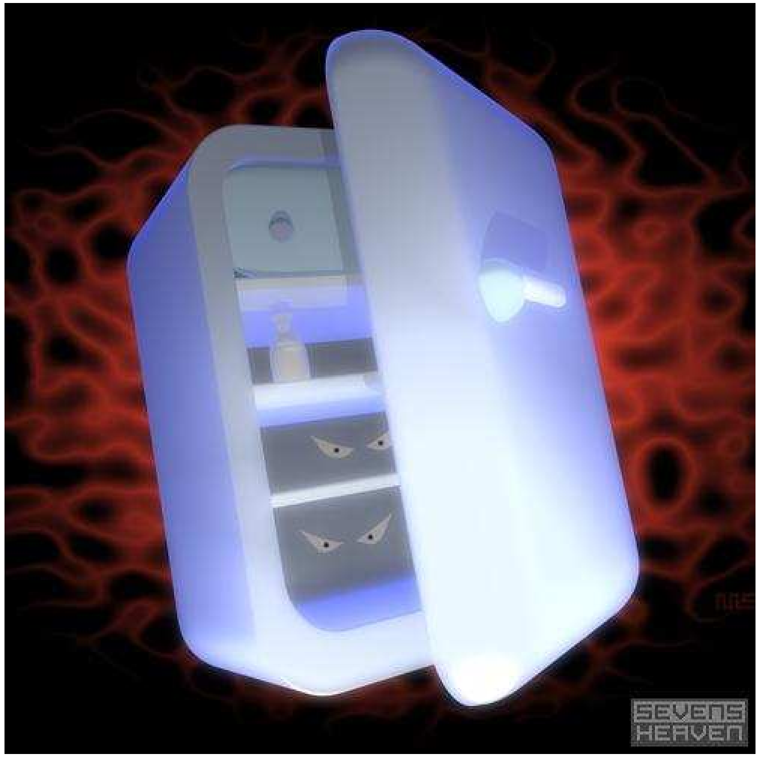
Confirm Password :

Maximum length allowed is 8

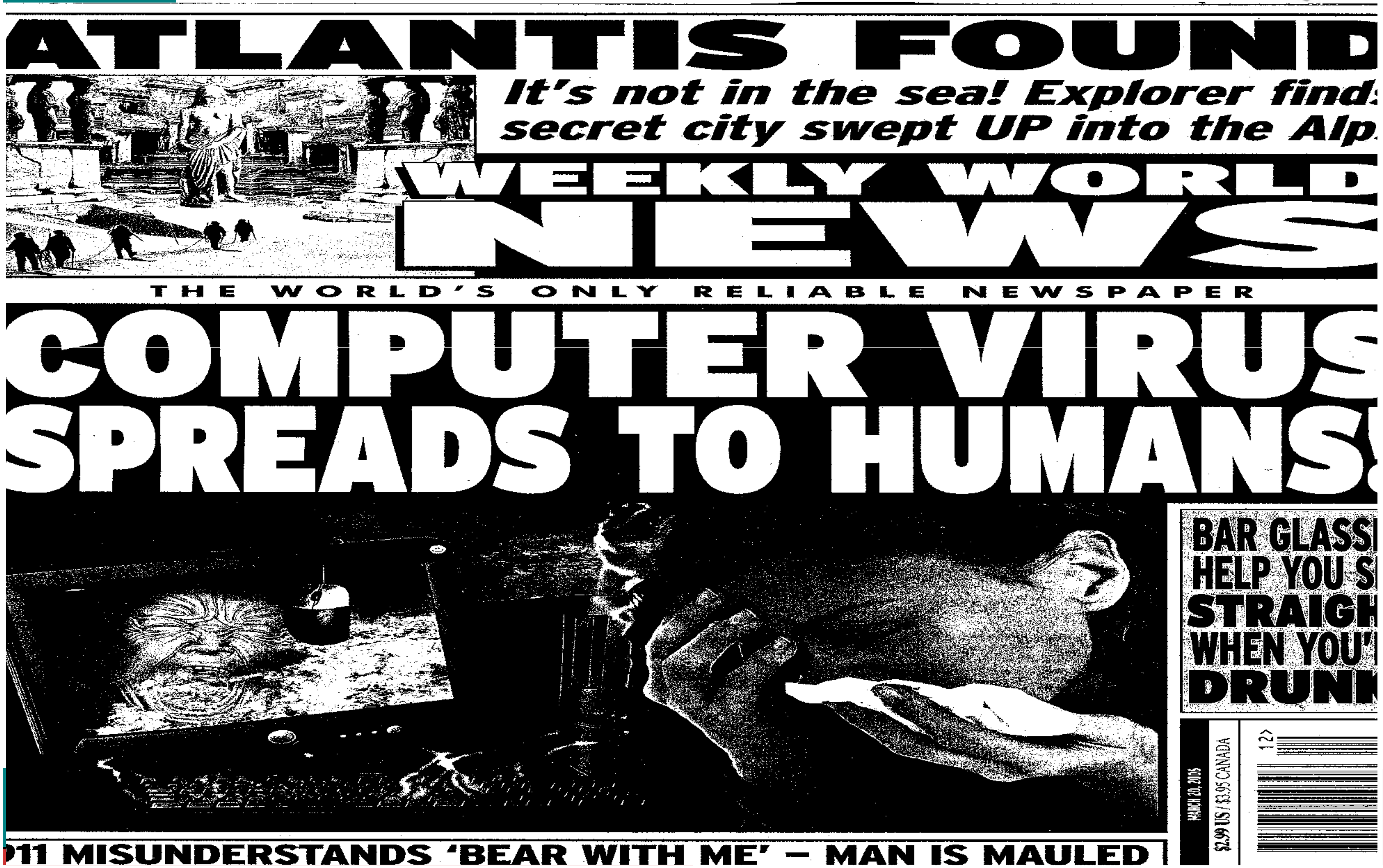
The Future?

Viruses on your RADIO?

Viruses on your refrigerator?



Oh no … Crossover viruses!



ATLANTIS FOUND

It's not in the sea! Explorer find secret city swept UP into the Alp

WEEKLY WORLD NEWS

THE WORLD'S ONLY RELIABLE NEWSPAPER

COMPUTER VIRUS SPREADS TO HUMANS

BAR GLASS HELP YOU S STRAIGH WHEN YOU' DRUNK

MARCH 20, 2006

$2.99 US / $3.95 CANADA

12>

911 MISUNDERSTANDS 'BEAR WITH ME' – MAN IS MAULED

Science Fiction ideas that came true (sort of)

Nanobots

In his story “A Menace in Miniature” (1937), Raymond Z. Gallun imagined sinister “ultra-microbots”.

Eddy Willems

Security Evangelist

Eddy.Willems@gdata.de

Righard J. Zwienenberg

Chief Research Officer

Righard.Zwienenberg@norman.com