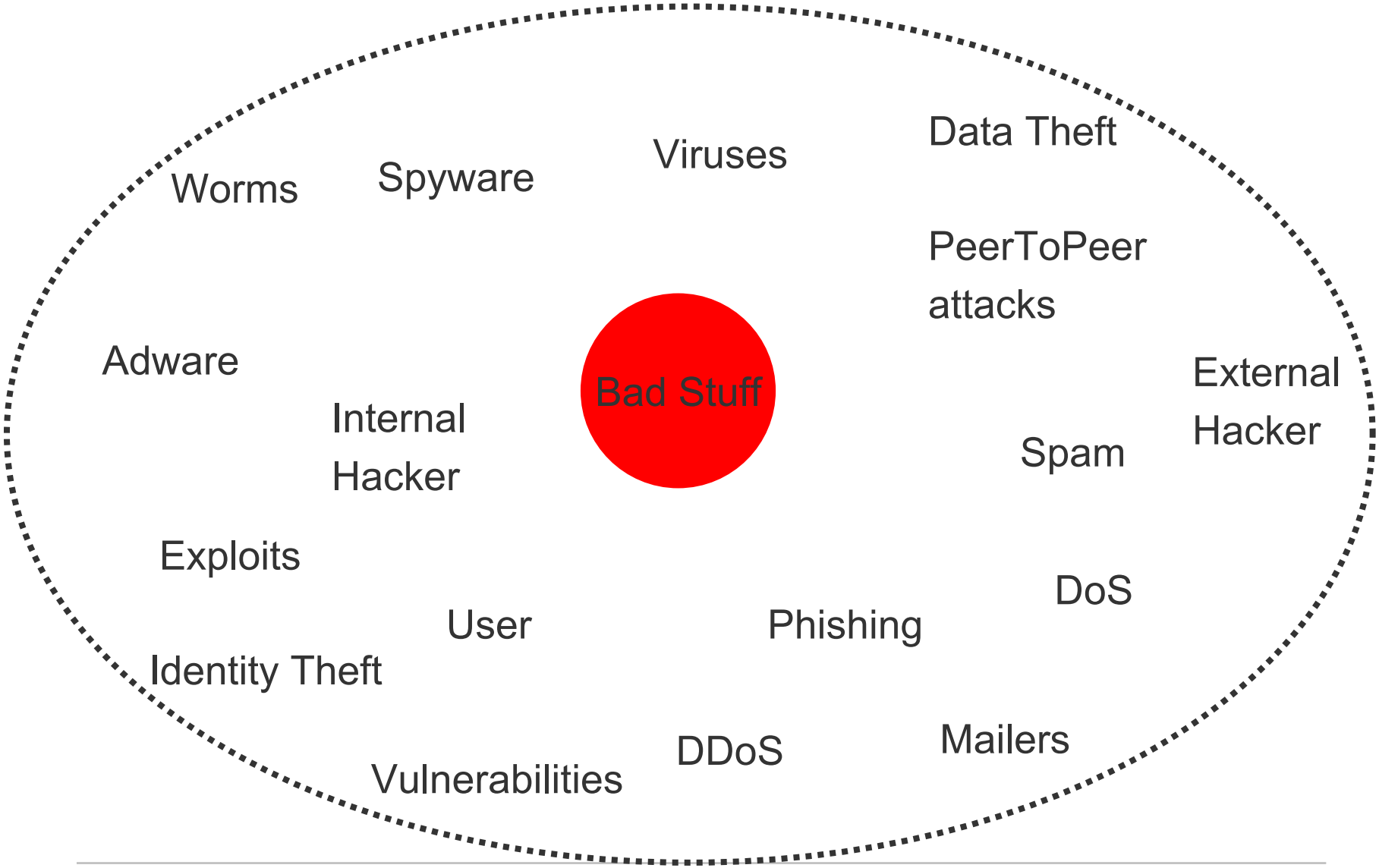
McAfee
Proven Security™

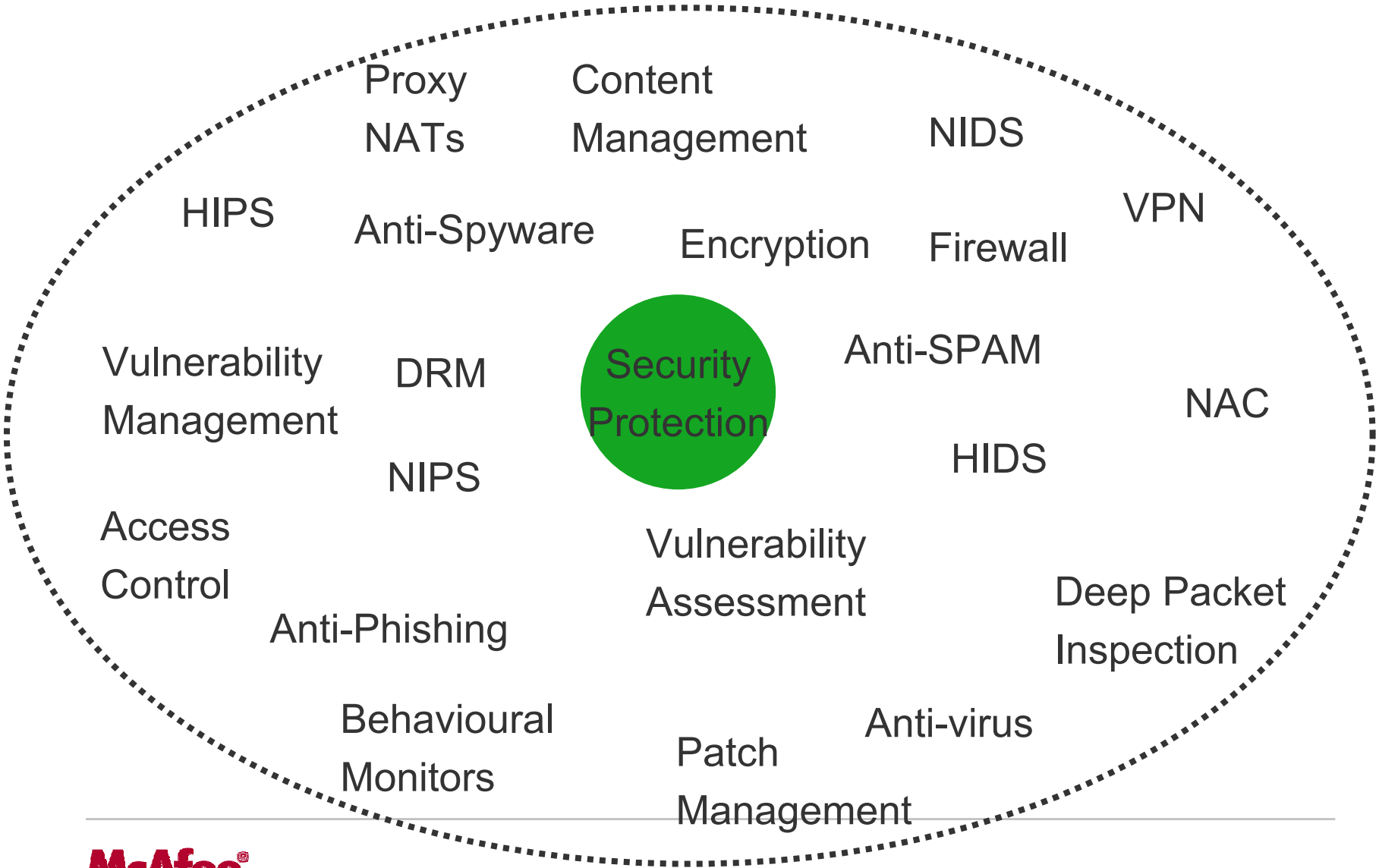
A Practical Understanding of Malware Security

Greg Day
McAfee Security Analyst

Where to start with the Security threats?

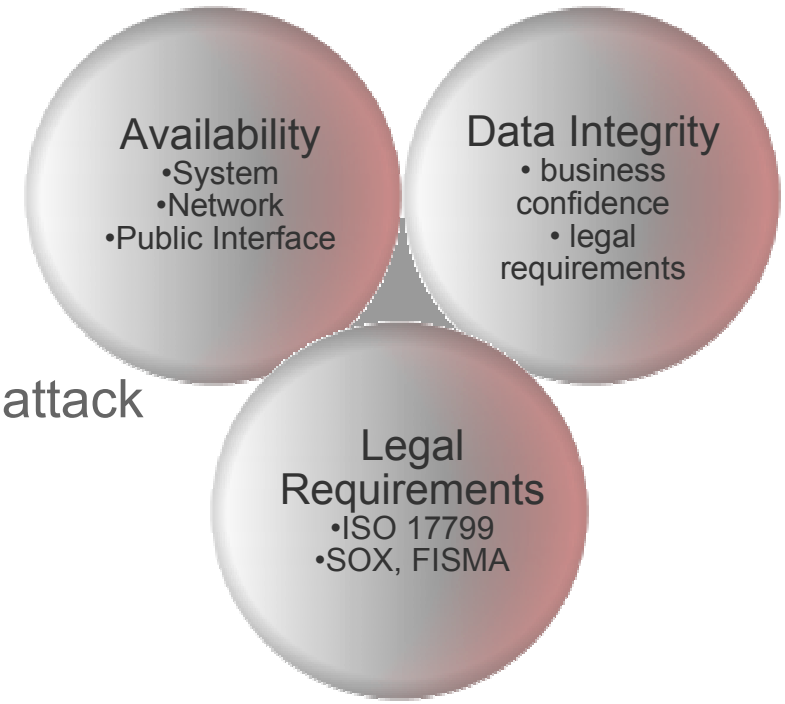


Which Security solution best solved the problem?



Security investment drivers

- A business perspective
  - With traditional security approaches there is still a cost to the business
- Why?
  - Speed of attack vs. time to react
  - Indirect impacts associates with the attack
    - System stability/availability
    - Network stability/availability



Time challenges

- Patching is not an instant process
  - Test, Deploy, Validate
- AV - updates may be released after attack start
  - Time to deploy
- Policy changes
  - Need to understand the attack to define changes (e.g. Block ports)
  - Understand the impact these will have on the business

The more critical the system = the slower changes implemented

What are the indirect impacts on your business?

- System stability
  - Which systems are critical
  - When does the masses outweigh the few?
- Bandwidth availability
  - Which resources require 24x7 access?
  - How much resilience does you're network have?
- Potential external access to your systems?
  - Data theft
- External 3rd parties utilising your systems
  - Liability for attacking others, SPAM, DdOS

P'n'P - A recent example

"Worm strikes down Windows 2000 systems"

CNN INTERNATIONAL .com

August 17, 2005

- "Among those hit were offices on Capitol Hill, which is in the midst of August recess, and media organizations, including CNN, ABC and The New York Times. Caterpillar Inc., in Peoria, Illinois, reportedly also had problems."

"Plug and Play pandemonium"

The Register

August 17, 2005

- "Computer systems at CNN, ABC, The *Financial Times*, and the *New York Times* have all been disrupted. General Electric, United Parcel Service and Caterpillar were also affected by the attack."

"Corporate computer networks suffer rash of viruses"

FT.com FINANCIAL TIMES

August 17, 2005

- "Companies affected included CNN, ABC News, the New York Times and the Financial Times. Computers at DaimlerChrysler, Kraft and UPS were also reported to have been infected by the worms."

"'War of the Worms' Spurs Latest Cyber-Attack"

abcNEWS

August 17, 2005

- "Companies including ABC, CNN, The Associated Press, The New York Times and Caterpillar all found their networks slowed to a virtual standstill on Tuesday."

Microsoft Plug'n'Play exploit

- P'n'P first launched in Microsoft Windows 95 OS
- 9/8/05 – MS05-039 (Critical - Win2000, Important WinXP, Win2003)
  - Plug and Play Could Allow Remote Code Execution
- 9/8/05 – Cert advisory (CAN-2005-1983)
- 10/8/05 – Exploit code POC shell code to port 7777
- 14/8/05 – Zotob, SDBot!MS05-039
- 16/8/05 – IRCBot!MS05-039, Mydoom.bv@MM, SDbot!51326
- 17/8/05 – Bozori.b

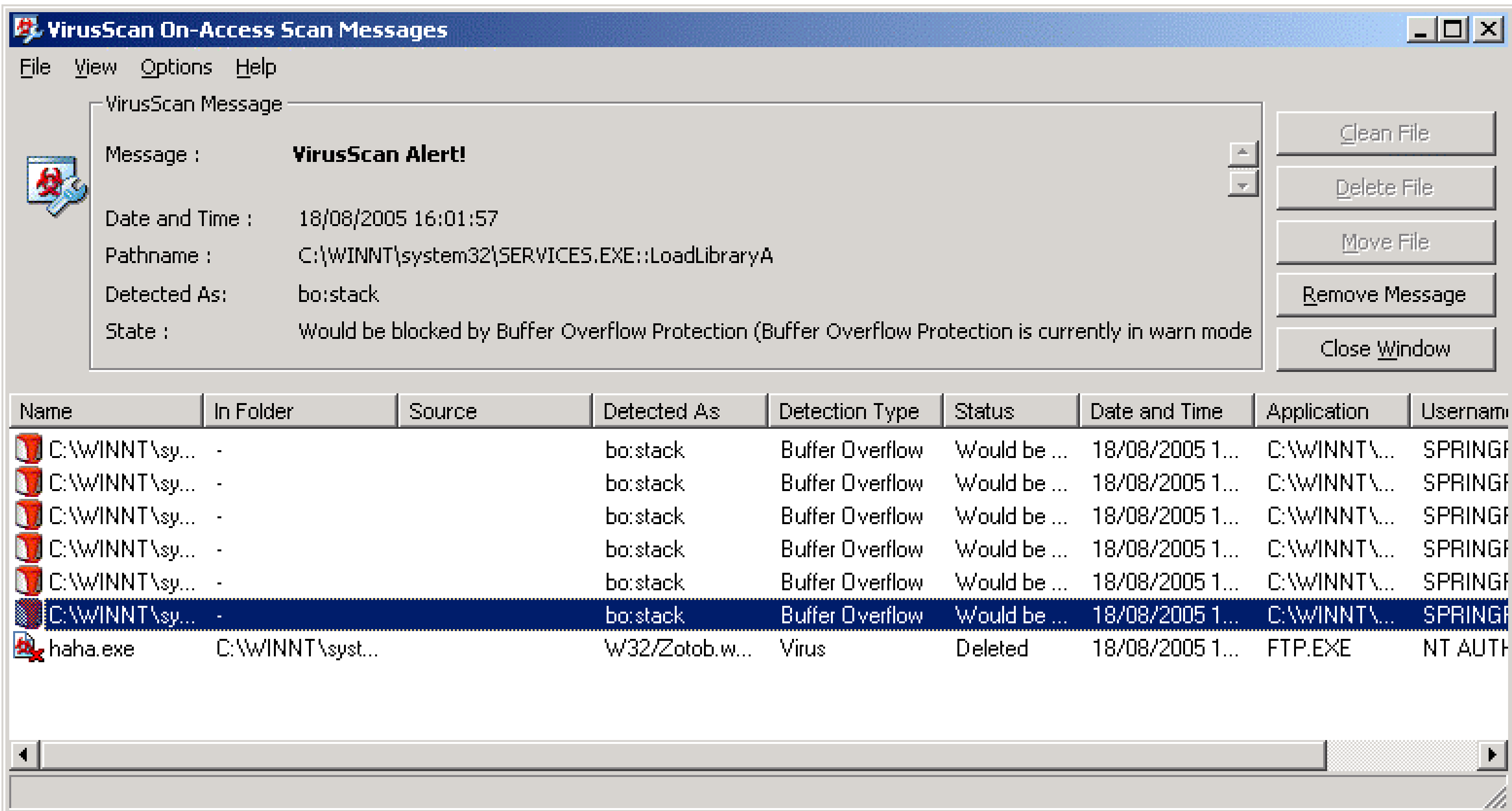
…

Understanding the Network Worm methodology

- Understanding the method will help you:
  - Assess the impact the attack has on your business
- Understand how each security technology can play a part in preventing the attack
  - How much does it reduce the business impact?

Demo – W32/Zotob

Testing results – inconsistent!



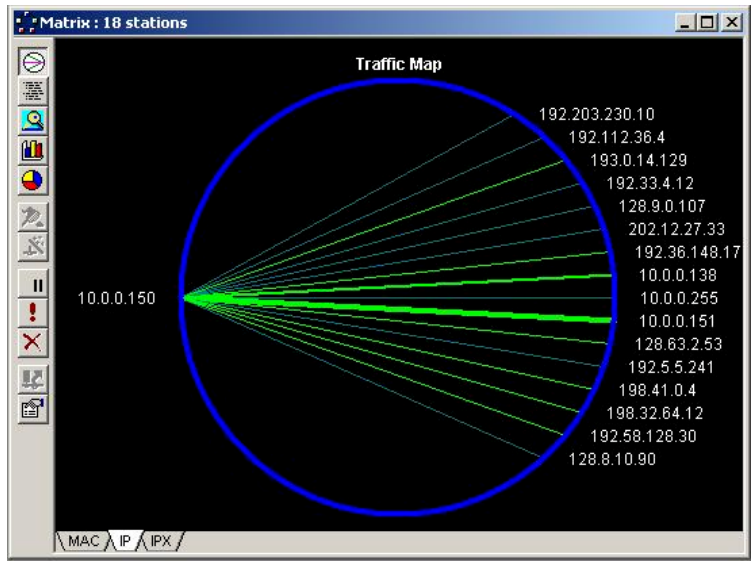
Summary of Zotob infection methodology

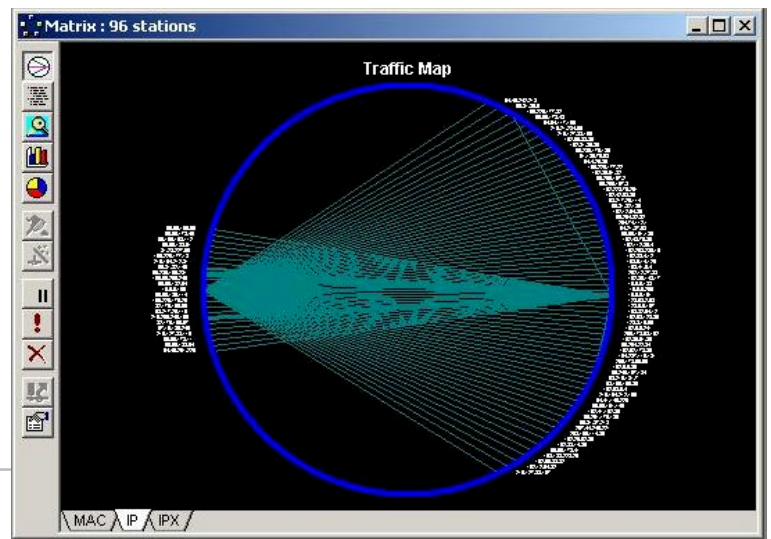
- Random Class B ARP requests – find systems
- TCP SYN/ACK handshake on port 445
- SMB Null session connection
  - RPC Buffer overflow to P'n'P
- Opens up remote Shell through port 8888
  - Downloads FTP script "2PAC.TXT"
  - Executes script
- Victim connects to FTP server on attacker (port 33333)
  - downloads worm

What could these attacks do to your business ?

- Cause systems instabilities
- Infect you with worms, mass mailers, BOTs
- Open your network up to external attackers (IRC Bots)
- Reduce your Internet Explorer settings (Increase Spyware)
- Flood the network with attack traffic

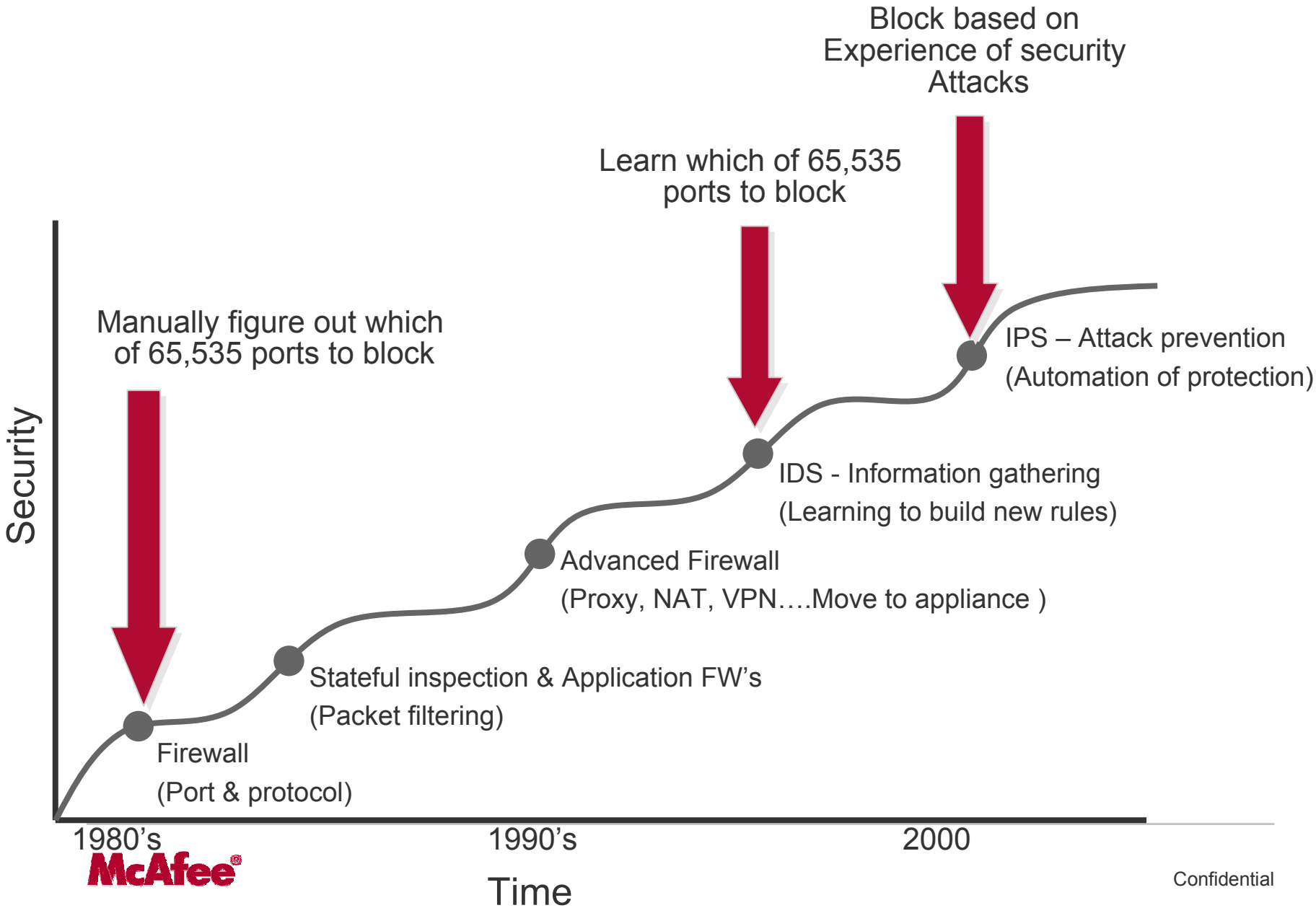
*** Demo Traffic ***



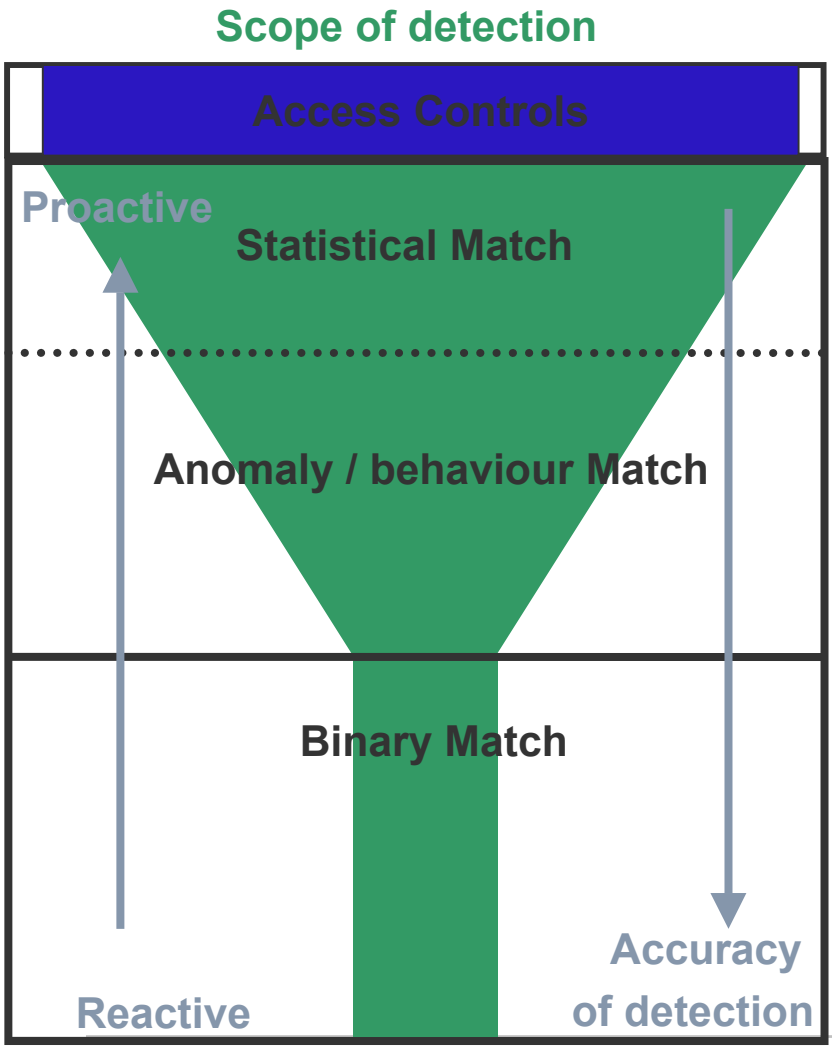


Understanding the changes in Security Protection Strategies

IPS – An example of the Security strategy evolution



IPS fundamentals – how does it work?
Binary signature & Behaviour Rules



	Signature	Rules
	Near Zero false positives	
	Known attacks	
	Before attack occurs	

Today's Security strategy

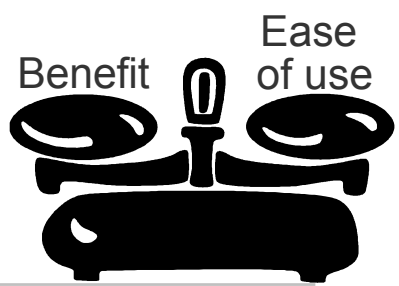
- Attack prevention

  The attack methods stay the same

  - Most common attack
    - Mass mailer – installs hidden mail client
  - Mass Mailers & Worms
    - add file(s) to Windows (system) folder & modify StartUp process
  - Mosts common security breach
    - Buffer Overflow exploits
      - Same method, different app
  - Most common BOTs
    - Use IRC but over non standard ports

Adding in the layers of protection - Zotob & Nachi

- Some behavioural controls (what's the business gain)
- System
  - Buffer overflow protection (system)
    - Network monitoring
    - System monitoring
  - System security (file)
    - Block .EXE writes
    - Block registry changes
  - System security (network)
    - Block (T)FTP sessions, block FTP scripts
    - Block ICMP pings
    - Block ports used? (33333, 8888, 445)
- Network protection
  - Packet Analysis
    - Packet anomaly
    - BO signature detection



Some examples of adding in the layers of protection

- W32/Nachi.worm
  - Same attack methodology
  - More consistent behaviour

- W32/Nachi Demo – some examples

  - Buffer Overflow

  - ICMP ping

Adding in the layers of protection (Zotob & Nachi)

- AV signatures — Detection of method – (FTP txt script)
- System
  - Buffer overflow protection (system)
    - Network monitoring — Zero impact to system
    - System monitoring — Stops infection, not system instabilities
  - System security (file)
    - Block .EXE writes — Stops infection, not system instabilities
    - Block registry changes — Stops attack being re-launched at Start-up
  - System security (network)
    - Block (T)FTP sessions, block FTP scripts — Zotob uses non standard FTP port
    - Block ICMP pings — Stops infection
    - Block ports used — Stops infection, not system instabilities
- Network protection
  - Packet Analysis
    - Packet anomaly — Prevents traffic – likelihood of use?
    - BO signature detection — Prevents traffic

2004 Medium+ risk attacks affected (Total for year - 46)

Network IPS	
(Signature detection) SMTP: Worm Detected in Attachment Looks for attachments with an EXE, PIF or SCR extension. *some instances this would not completely contain the infection, as the mailer may use additional attachment types*.	87%
(Signature detection) P2P: KaZaA, Gntella, Gnucleus, Morpheus, BearShare, LimeWire, Grokster, Phex, Xolox, eDonkey, WinMX & Swapper File Transferring.	52%
(Signature Detection) DCERPC: Microsoft Windows LSASS Buffer Overflow	7%
Host IPS and Security products	
(Shield Signature) New Startup folder program creation - detects registry write	98%
(Network Access control - Port Rule) Block mass mailing worms from sending mail	89%
(Shield Signature) System Executable Creation or deletion - detects New EXE's to Windows system folder.	76%
(System Access control - File/folder protection) - Prevent the creation of new files the System32 folder (.EXE)	74%
(Custom Rule) Block new EXE writes to folders with "Shar" or "Sharing". Use block sting "**shar**.exe" & "**sharing**.exe"	39%
(Custom Rule) Block new EXE's being created in the Windows folder	26%
(Signature): Generic Buffer Overflow detection	11%

Summary

- Security protection must focus on business enablement
  - System availability/stability
  - Network availability/stability
- Security solutions focusing on proactive security enforcement
  - Consider
    - Ease and likelihood of use
    - Time and ease of implementation (proactive/reactive)
- Your business requirement will drive your investment
  - Understand how attacks can impact against them
  - You have the requirement for your security investment
  - Understand which technologies meet your requirements

McAfee® Mission

Delivering Business Availability

Through Proactive Risk Mitigation

With Optimized Cost of Ownership