McAfee®
Proven Security™

Making IT Security Accountable Through Risk Management

Foundstone Security Evangelist

Intro

- Brian Kenyon – Foundstone Evangelist
  - Author of “Security Sage” and “Special Ops” Network Security Series
  - Foundstone 4yrs
  - Former Dir. Product Services
  - Over 10 years of computer and security experience
  - Co-Inventor of FS1000 Appliance

The Problem

Problem

- Not enough:
  - Time
  - People
  - Dollar$
- Where do we focus our efforts and prioritize what is most important
- Hard to deploy limited resources in a fashion that meaningfully reduces risk to the organization
- Are we in compliance with regulatory requirements
- Can’t fix all problems – what can we live with??
- What is the quantifiable likelihood of loss–the RISK?

ChoicePoint stock falls after data theft

February 23, 2005

BY HARRY R. WEBER
ASSOCIATED PRESS

ChoicePoint : Database Breach May Affect People Across US

DOW JONES NEWSWIRES
February 21, 2005 1:21 p.m.

ChoicePoint Stock Falls After Breach

ChoicePoint Stock Falls Amid Predictions Data Brokers Will Face More Regulation After Breach

By HARRY R. WEBER
AP Associated Press

LA lawsuit accuses ChoicePoint of compromising personal data

Associated Press

LA Lawsuit Accuses ChoicePoint of Compromising Personal Data

LOS ANGELES (AP) -- A woman in California is suing data warehouser ChoicePoint Incorporated, accusing the company of compromising her personal information following an announcement last week that bogus accounts were created to obtain information from company databases.

Eileen Goldberg sued the Alpharetta-based company in Superior Court on Friday, claiming the firm engaged in fraudulent, negligent and unfair business

Identity Theft Puts Pressure on Data Sellers

By EVAN PEREZ
Staff Reporter of THE WALL STREET JOURNAL
February 18, 2005; Page B1

Companies that compile and sell billions of private records on Americans could face new regulatory pressure in the wake of revelations by **ChoicePoint** Inc., one of the largest such information brokers, that an identity-theft ring gained access to tens of thousands of its electronic documents.

Threat Consequences - 2005

Customer Data Compromises

Wachovia	108K	May 23, 2005
Boston College	120K	March 17, 2005
ChoicePoint*	145K	Feb. 15, 2005
Polo Ralph Lauren	180K	April 14, 2005
Ameritrade	200K	April 19, 2005
LexisNexis	310K	March 9, 2005
Time Warner	600K	May 2, 2005
Bank of America	1.2M	Feb. 25, 2005
DSW Shoe Warehouse	1.4M	March 8, 2005
Citigroup	3.9M	June 6, 2005
CardSystems Solutions*	40M	June 20, 2005

“So What Can We Do?”

Manage Our Risk

Implement a Risk Management process to protect the organization and its ability to perform its mission.

What Is Risk Management?

The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

Goals

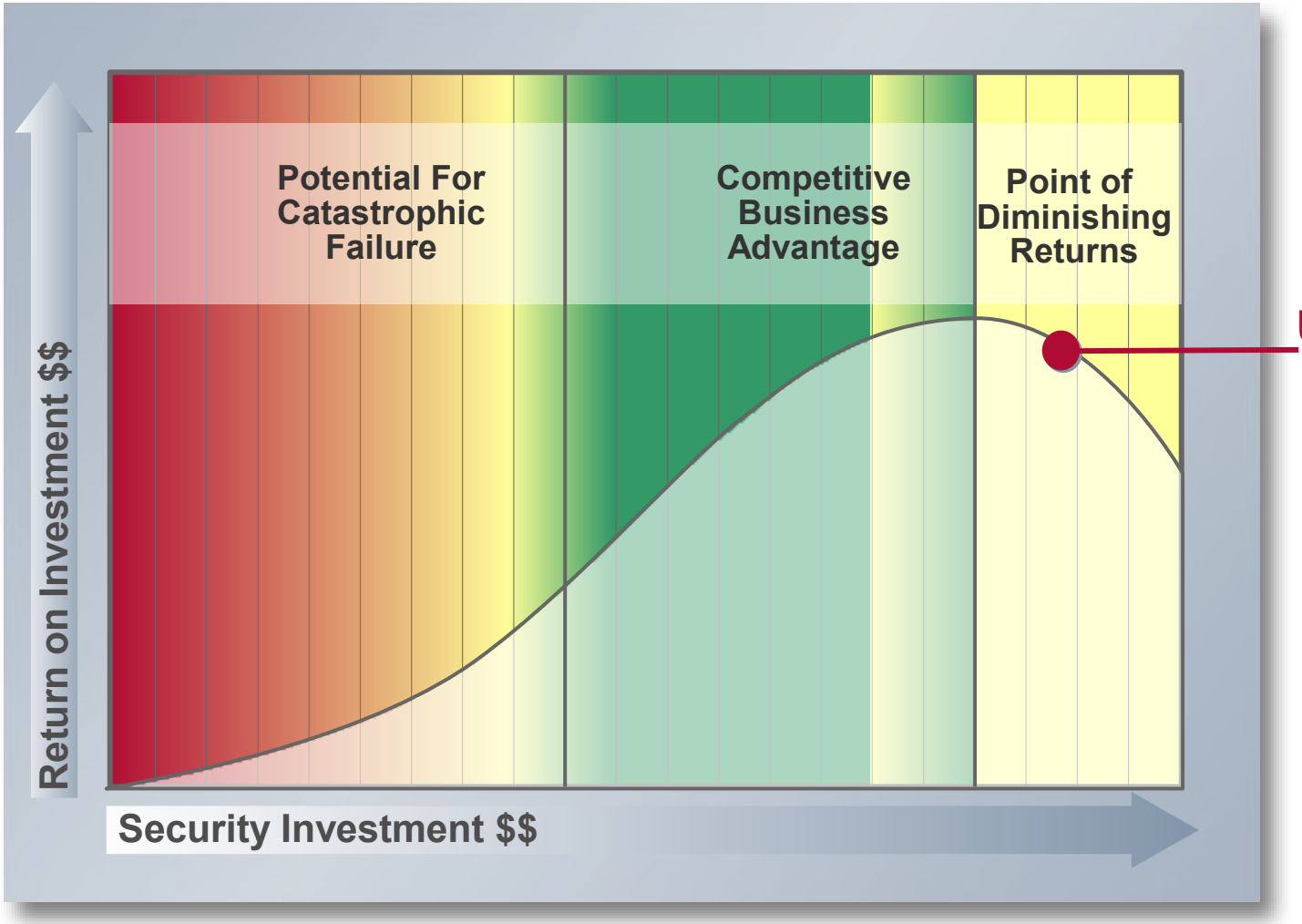
- ✓ Improve **accountability** of your security efforts
- ✓ Increase **efficiency** of risk identification and mitigation
- ✓ Improve **availability** of resources
- ✓ Improve **credibility** with audit, management, and industry regulators
- ✓ Prove your **value** to the organization
- ✓ **Save** your job!

Manage Our Risk

Risk Management Strategies include:

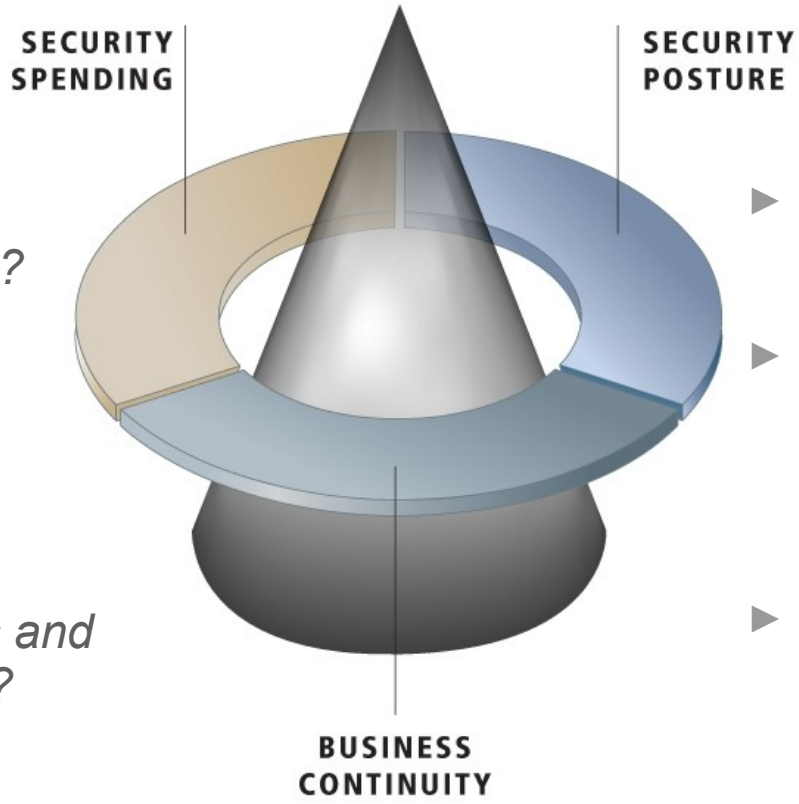
Risk Transfer	► Contractual transfer to 3rd party ► Insurance provider
Risk Avoidance	► Eliminate existing exposures/capabilities
Risk Acceptance	► Security spending has a point of diminishing returns, some risk is easier to accept
Risk Mitigation	► Security countermeasures (people/process/technology)

Why is Risk Assessment/Management Important?



Managing Risk Is A Balancing Act…

- *What are my mission-critical assets?*
- *What are my critical priorities?*
- *Can you help find the exceptions to organizational policies and technology standards?*

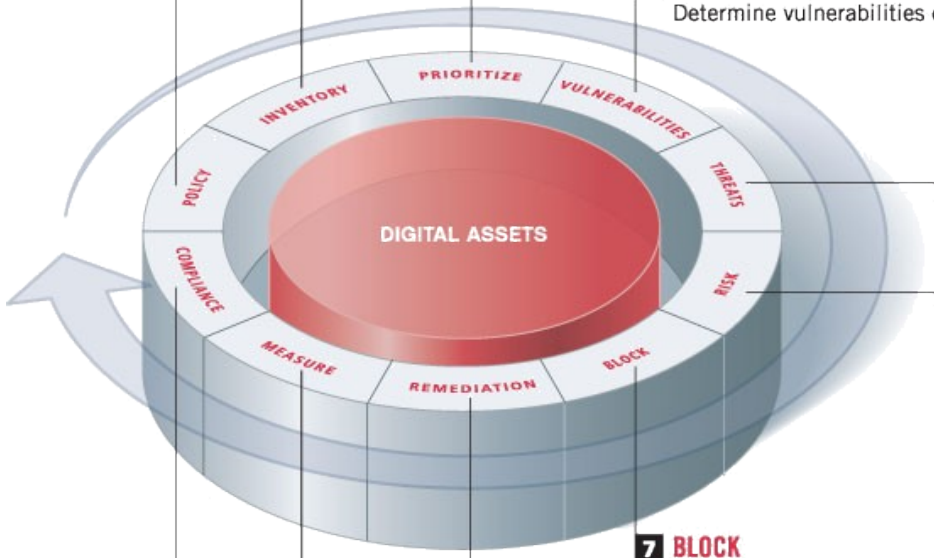


- *Can I better manage security investments?*
- *How can I better deploy resources against core business priorities?*
- *Are we compliant?*

Risk Management Lifecycle

McAfee®

Taking Control of the RM Lifecycle



1 POLICY
Establish process, standards and guidelines

2 INVENTORY
Discover all assets across the network

3 PRIORITIZE
Assign business value to assets

4 VULNERABILITIES
Determine vulnerabilities on assets

5 THREATS
View potential threats

6 RISK
Determine risk level

$$R = \frac{A}{C} \times \frac{V}{C} \times \frac{T}{C}$$

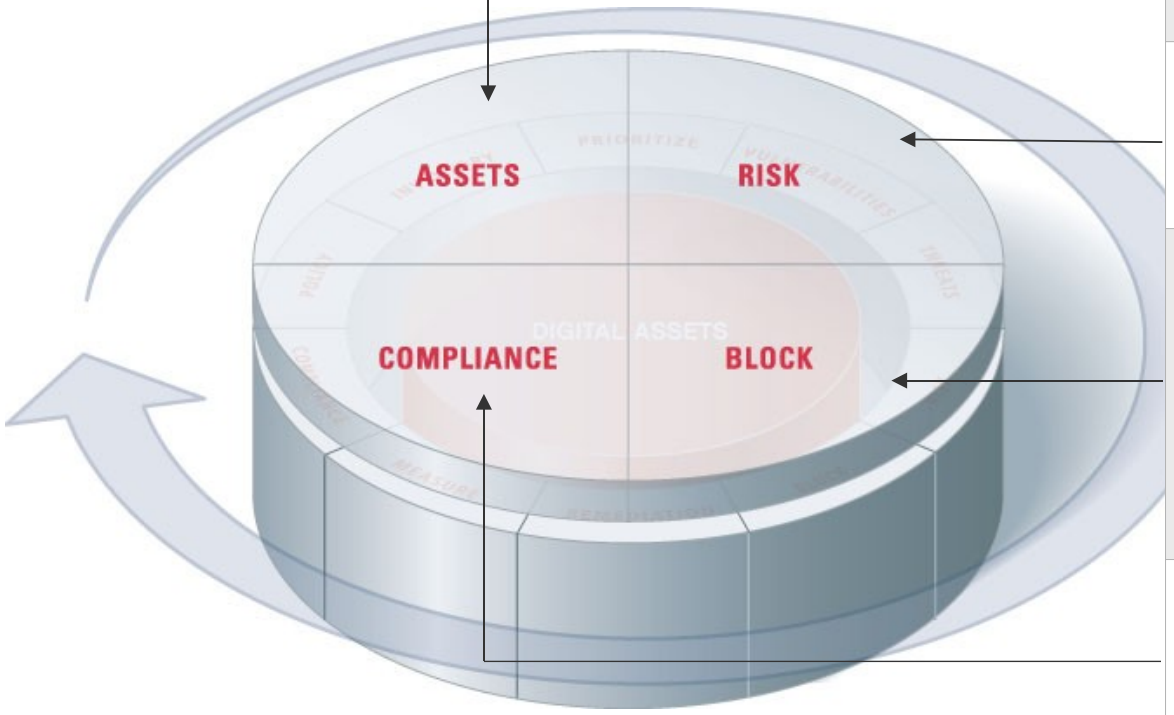
7 BLOCK
Stop intrusions in real-time

8 REMEDIATION
Proactively fix vulnerabilities

9 MEASURE
Measure impact of security decisions and actions

10 COMPLIANCE
Review for policy compliance

Applying Business Discipline to Security



Focus finite resources on mission-critical assets

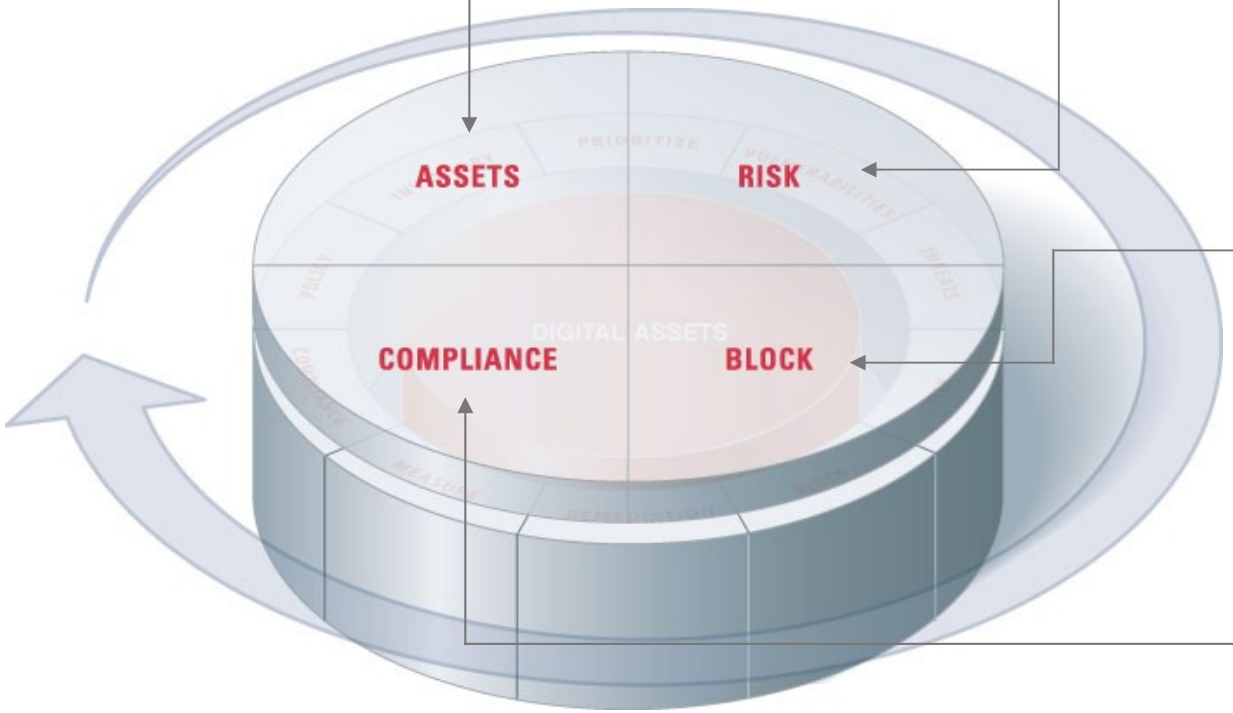
Calculate ***acceptable risk*** threshold

$$R = \frac{A}{C} \times \frac{V}{C} \times \frac{T}{C}$$

Proactively and automatically stop attacks while planning and implementing remediation strategies

View ***proven metrics*** and benchmarks for compliance and enforce technical and procedural standards

Broad Based Solutions Portfolio



McAfee ePolicy Orchestrator®
McAfee Foundstone®

McAfee Foundstone

<u>Network Protection</u>
McAfee IntruShield®
McAfee SecureWebGateway
McAfee Secure Messaging Gateway
<u>System Protection</u>
McAfee Entercept®
McAfee VirusScan® Solutions
McAfee AntiSpyware
McAfee Desktop Firewall™
McAfee GroupShield for Mail Servers

McAfee ePolicy Orchestrator
McAfee Foundstone
McAfee Policy Enforcer

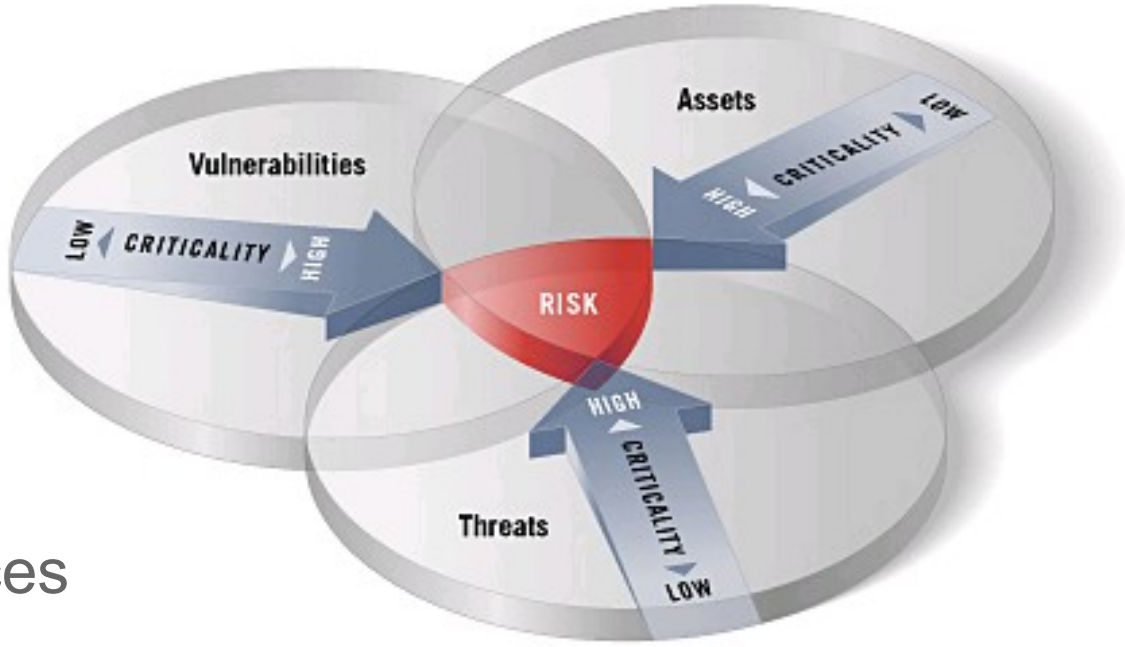
Risk – In the Context of Security

Risk

*Is a function of the **likelihood** of a given **threat** exercising a particular **vulnerability**, and the resulting **impact** of that adverse event on the organization*

Calculate Risk

- The Union of:
  - Vulnerabilities
  - Assets
  - Threats
- Based on the criticality of VAT
- Focus your resources on the TRUE risk



SRM Metrics Formula

Risk = V/C * A/C * T/C

Vulnerability Criticality	*	Asset Criticality	*	Threat Criticality
Countermeasures • Patch management • IPS • Anti-virus		**Countermeasures** • Insurance • Redundancy • 3rd party transfer		**Countermeasures** • Firewalls/filtering • Policy enforcement • Defense in depth

Measure

"When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind …"

– Lord Kelvin (circa 1870)

Measure

Why Security Metrics?

- Identification of risks
  - Successes and failures of past decisions
- Understand effectiveness of controls
  - Demonstrate the value of Information Security
- Influence decision makers
  - Influence IT and security strategy
  - Garner support for security initiatives
- Measure performance against set goals
  - Improve accountability to stakeholders
- Demonstrate Compliance
  - OSFI, SEC, Basel II, US legislation (FISMA), SarBox, etc.
  - Internal and external auditors

Paradox

The more successful your security investment—the less visible and measurable the results

So How Does It Work In Practice?

Protecting an Enterprise Customer

People & Geography

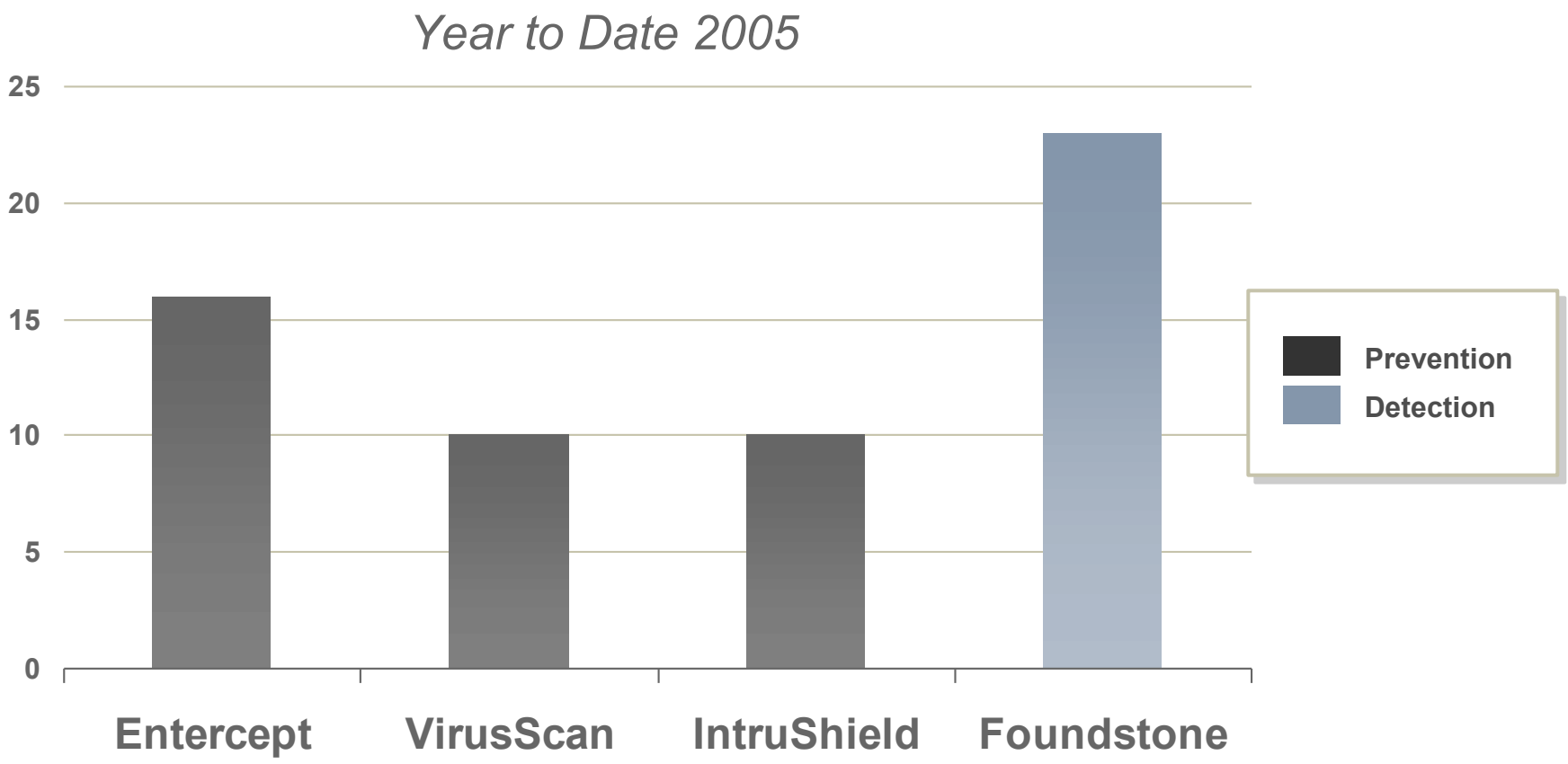
- 3000+ Employees and Contractors
- 31 Countries
- 70+ Global Offices

Technology

- 1200+ Laptops, 4K Desktops
- 600+ Wintel Servers
- 70+ Firewalls
- 8.5 Gbps Internet Bandwidth
- 50+ Routers and 80+ Switches

Millions of Attacks in 2005

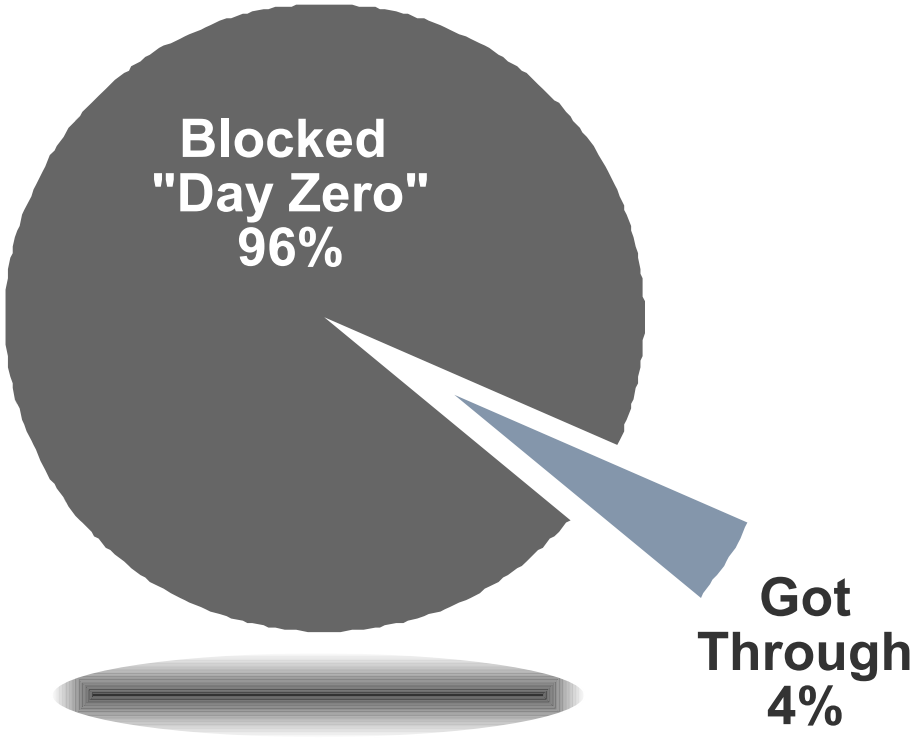
23 Microsoft Vulnerabilities



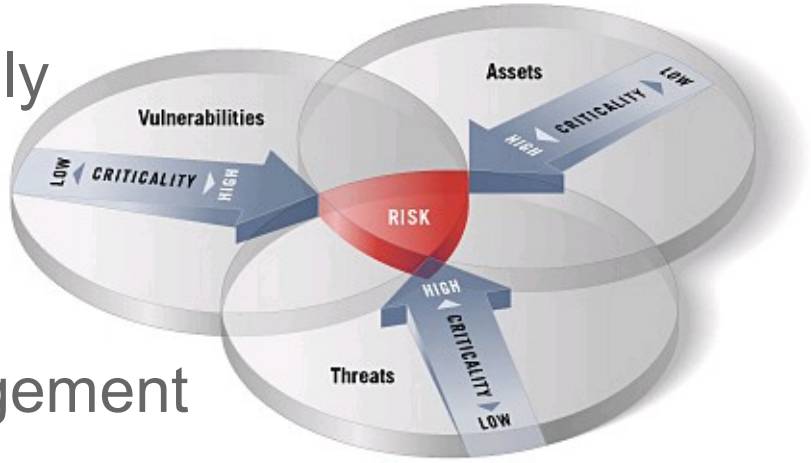
McAfee's Intrusion Prevention & Risk Management Strategy Works

Beyond Anti-Virus

- 96% Blocked "Day Zero"
- Reactive Patching Virtually Eliminated
- No Damage



Conclusions



- All assets are not created equally
- You cannot respond to or even protect against all threats
- An effective vulnerability management program focuses on Risk
  - Vulnerabilities + Assets + Threats
- RM is truly preventative and proactive, not reactive
- Finds and fixes the core problems, not the symptoms
- No other form of security is as effective in reducing risk

For McAfee information:

www.mcafee.com or www.foundstone.com
1-877-91.FOUND
info@foundstone.com

Brian Kenyon
bk@foundstone.com
949-297-5600

- Thank You!
- Informal Q&A