

Executive Summary

"Security is not a Product, it's a Process."

Bruce Schneier, Counterpane Internet Security, Inc.

- Developing an effective information security programs is a long-term, evolutionary process
- CISO's need a clear understanding of the enterprise's maturity level to drive performance improvement
- To gain support for continued security investment, security must be expressed in business terms aligned to business objectives

McAfee

9/19/2008



Protect what you value.

Security Effectiveness Paradox

Issue: As security improves, management has difficulty rationalizing the business value

Effects:

- Under funding
- Uncoordinated activities
- Waning awareness
- Lack of executive support
- Fighting the last war....

“We spend millions on security and nothing bad happens. Is that because of the millions spent on security or because nothing bad was going to happen in the first place?”¹



McAfee

9/19/2008

¹ CSO Magazine : “What is Security Worth” (2006)

Protect what you value.

Statistics to Consider

“The most-efficient and secure organizations will reduce the share of security in the IT budget to 3%-4%”

“15% of chief information security officers (CISOs) will be replaced for failing to deliver business value”



“Mature information security programs will suffer 80% fewer high-impact security incidents”

“Only 37% of organizations have a strategic security plan in place”



McAfee Security Optimization Model

- Adaptation of the System Security Engineering CMM Model - International Systems Security Engineering Association (ISSEA) – SSE CMM Model
- Focused on maturity of information security practices within organizations
- Four maturity “states”:
 1. Secure
 2. Compliant
 3. Proactive
 4. Optimized
- Accompanying assessment methodology developed to benchmark performance

The McAfee logo is displayed in a bold, red, sans-serif font on a black background.

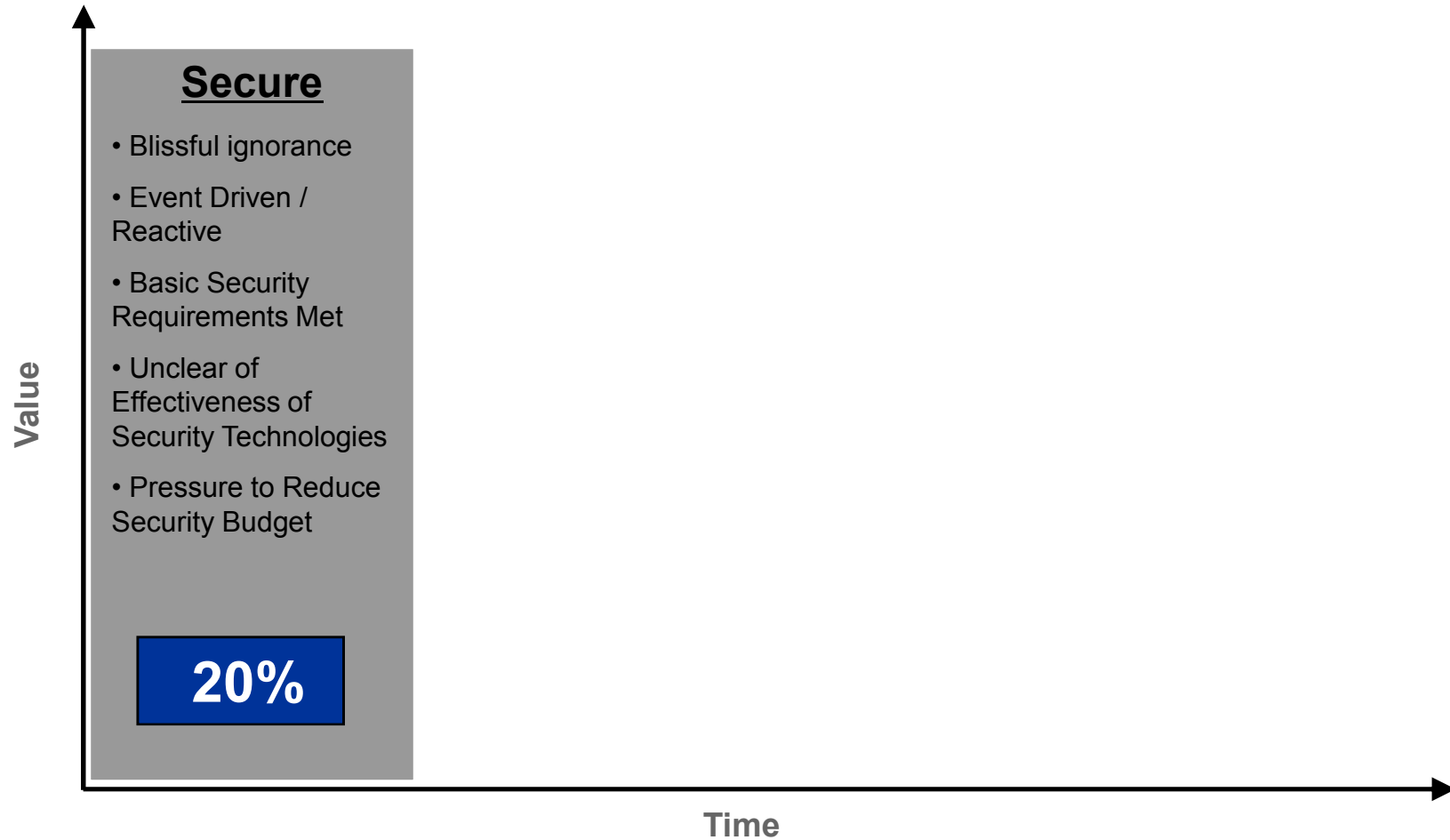
9/19/2008



Protect what you value.

Organizational Maturity

Secure State

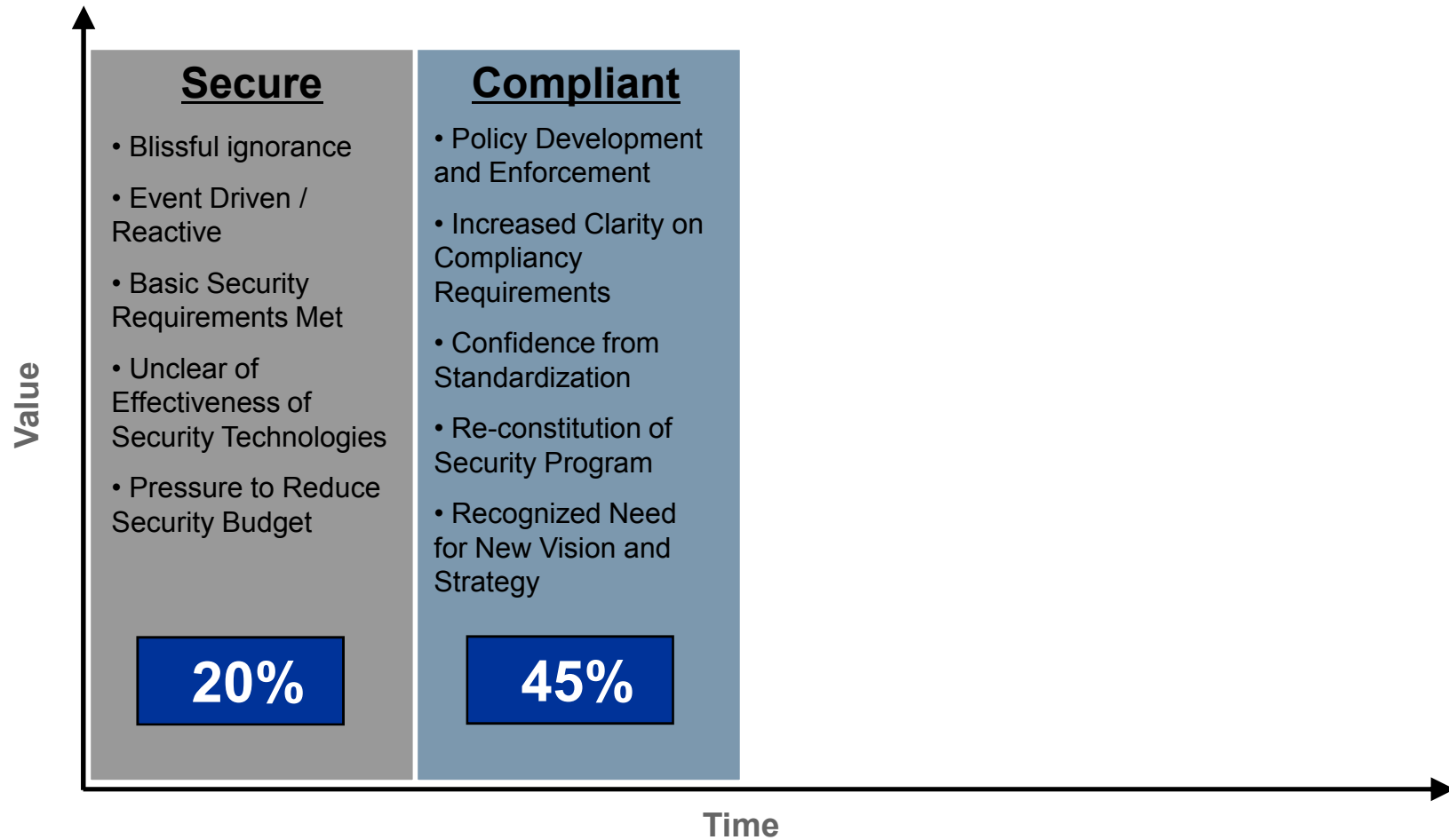


9/19/2008



Protect what you value.

Organizational Maturity Compliant State



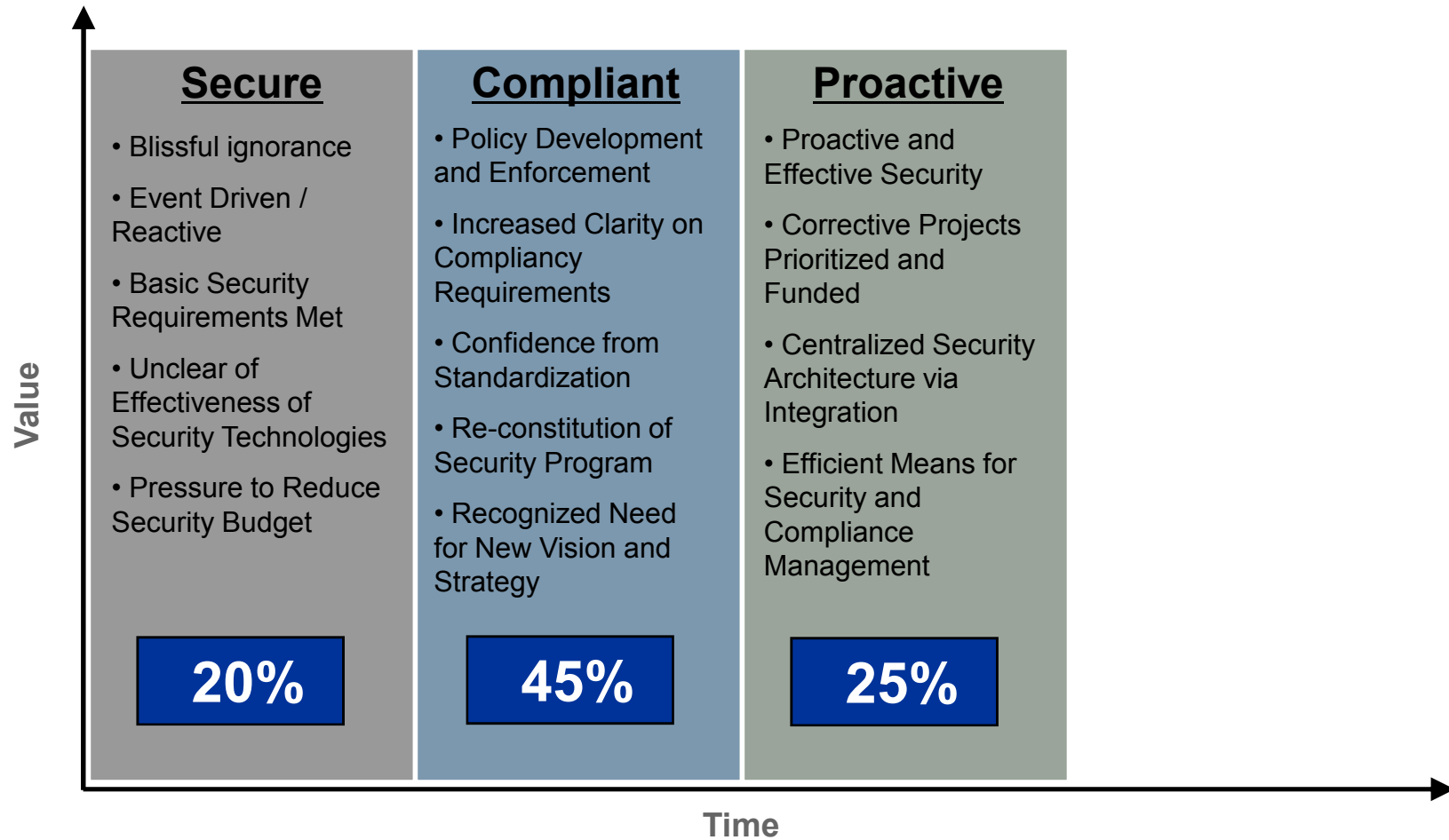
9/19/2008



Protect what you value.

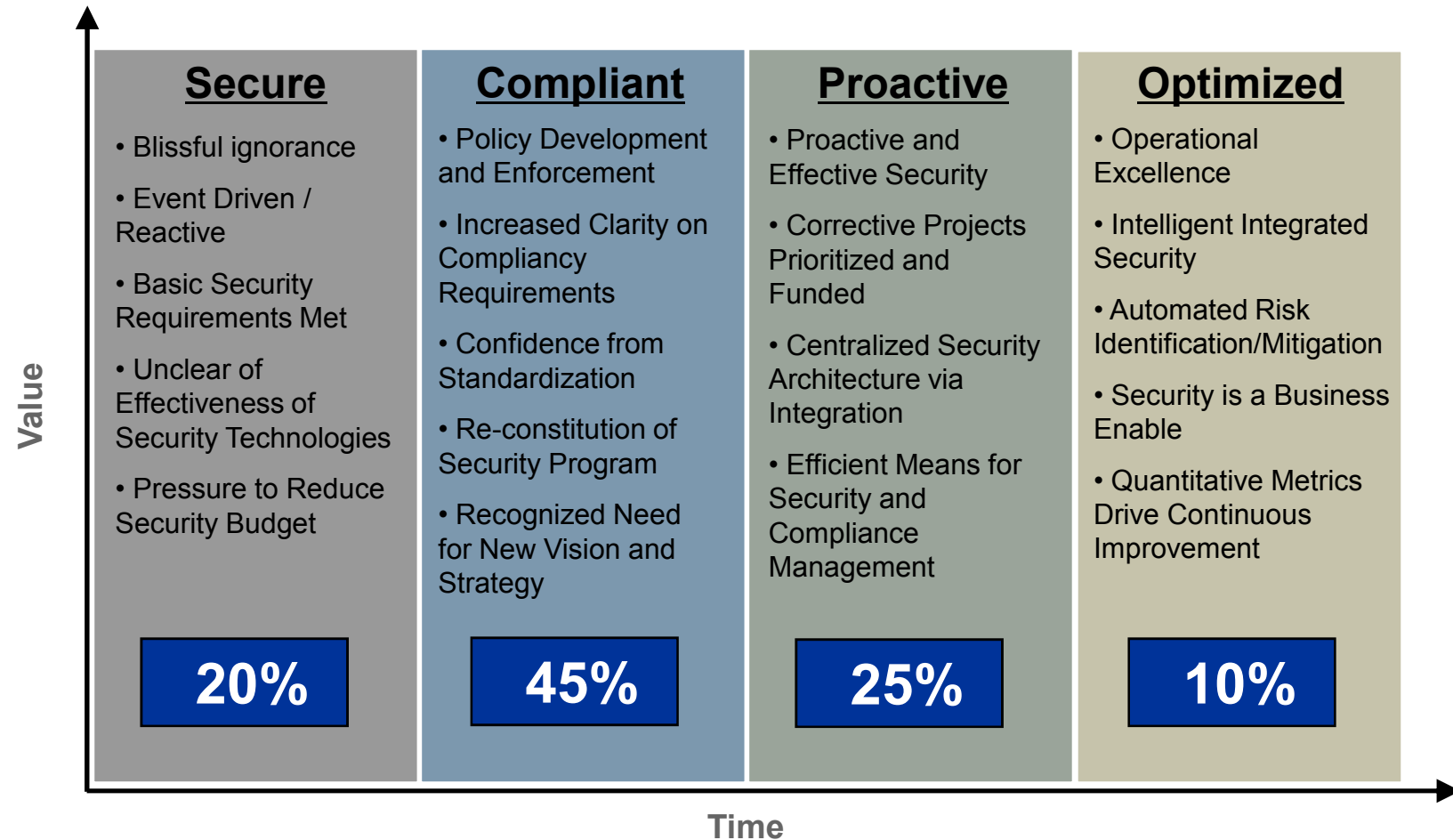
Organizational Maturity

Proactive State



Organizational Maturity

Optimized State



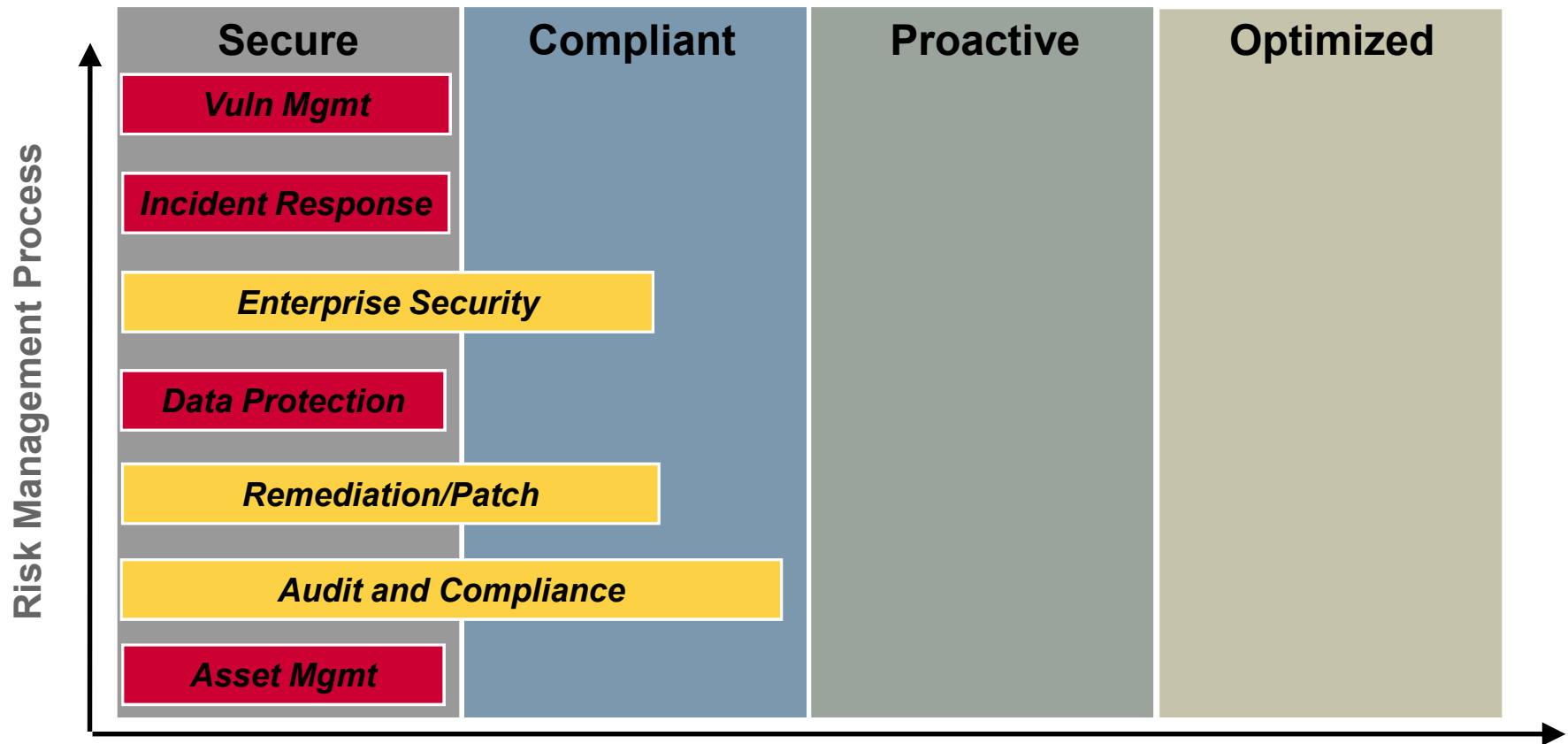
McAfee

9/19/2008



Protect what you value.

Risk Processes Maturity Assessment



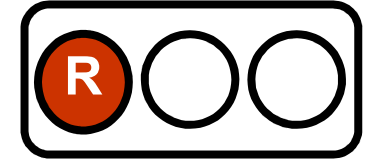
SAMPLE

McAfee

9/19/2008

Protect what you value.

Vulnerability Management

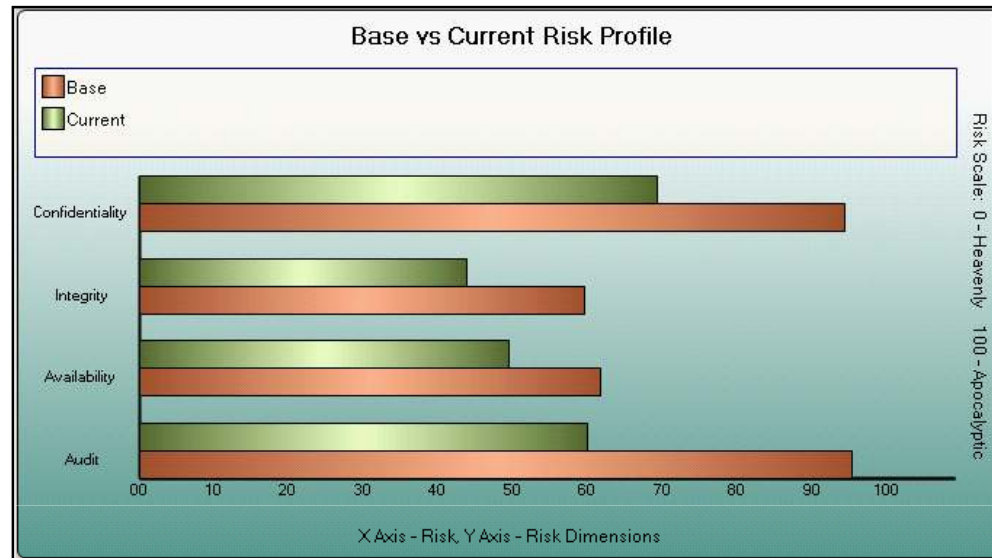


- Description
 - Determines how an organization identifies and reports on vulnerabilities and threats that exist on servers, workstations and network devices
- Observations
 - Recognized need to develop Threat and Vulnerability Management (TVM) processes
 - Comprehensive inventory and classification of assets is not maintained
 - TVM not integrated with incident response process
- Business Impact
 - Current TVM processes create a porous security environment for business systems -- exposing them to unmitigated risks
 - Lack of business domain knowledge (asset valuation) limits business involvement/accountability in risk decision making



Baseline Risk Profile

Consolidated Site Data



Risk Index	Base (Systemic) Risk	Current (Residual) Risk	Risk Ranking	Key Observation
Confidentiality	94%	69%	High	Data protection controls require attention
Integrity	59%	44%	Medium	Sec/Bus alignment needs improvement
Availability	62%	49%	High	BCP/DR efforts in progress
Audit	95%	60%	High	Reactive IR and monitoring

SAMPLE

McAfee

9/19/2008

Protect what you value.

Risk Management Process Maturity

ISO 17799:2005 Compliance

Optimized Processes

Proactive Processes

Compliant Processes

- Compliance : 76%
- Security Policy: 71%
- Physical/Environmental: 79%

Secure Processes

- Incident Management: 38%
- Business Continuity: 27%
- Communications/Operations: 42%
- Access Control: 44%
- Organizational Security: 44%
- Asset Classification/Control: 0%
- Development/Maintenance: 11%
- Personnel Security: 46%



SAMPLE

McAfee

9/19/2008

Protect what you value.

Recommendation #1 – Data Protection

- Process Recommendations

- Conduct a self-assessment to analyze business goals, company culture and organizations needs related to protecting data
- Identify key data stakeholders and map data collections within the business
- Baseline current data security practices against security policies
- Define future state for protecting data and obtain organizational commitment

- Technology Recommendations

- Deploy DLP technology that provides flexibility in automating data protection
- Implement full drive encryption for your mobile and at-risk assets
- Utilize technology to control appropriate locations for storing sensitive data
- Ensure Encryption can be exported outside of US to high risk geos, such as China
(Compliant with US Dept Commerce – CCL 5D002.c.1 & Bureau of Industry & Security License Exception ENC)

The McAfee logo is displayed in a bold, red, sans-serif font on a black background.

9/19/2008

A large, red, rectangular box with the word "SAMPLE" in white, bold, sans-serif capital letters is positioned in the bottom right corner of the slide.The slogan "Protect what you value." is written in a small, white, sans-serif font at the bottom right of the slide, below a row of small, colorful images.

Recommendation #1 – Data Protection (Cont.)

- Business Value

- Compliance to regulatory requirements related to protecting data
- Protection of intellectual property to maintain competitive advantages (e.g. patents, trade secrets)
- Safeguard company brand by reducing risk of losing company, customer or partner data

- Measures of Success

- # mobile systems with disk encryption – measure value of mobile data protection
- # detected/contained data policy violations per period – measure data protection enforcement
- % data infractions related to restricted/classified data sets – toxicity rate of sensitive data infractions
- # HR escalations for data infractions – organizational commitment to data protection

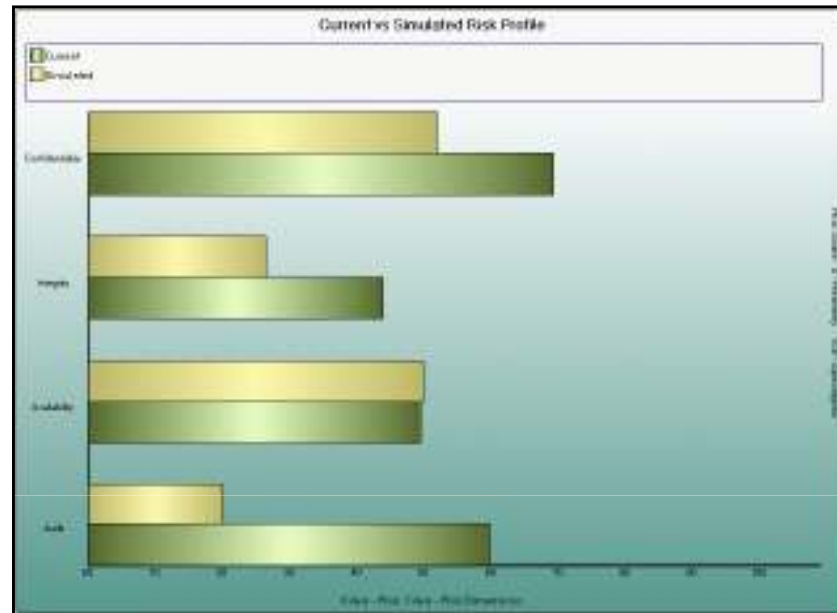
The McAfee logo is displayed in a bold, red, sans-serif font on a black background.

9/19/2008

SAMPLE

The slogan "Protect what you value." is written in a small, white, sans-serif font at the bottom right of the slide. Above it is a collage of various small images, including a person, a globe, and other abstract scenes.

Risk Simulation Modeling



Risk Index	"As-Is" Risk	"To Be" Risk	Recommendations
Confidentiality	69%	52%	Encryption; Data Leakage Protection
Integrity	44%	26%	System Hardening; Standardization
Availability	49%	49%	
Audit	60%	20%	Endpoint Security; Data Leakage Protection

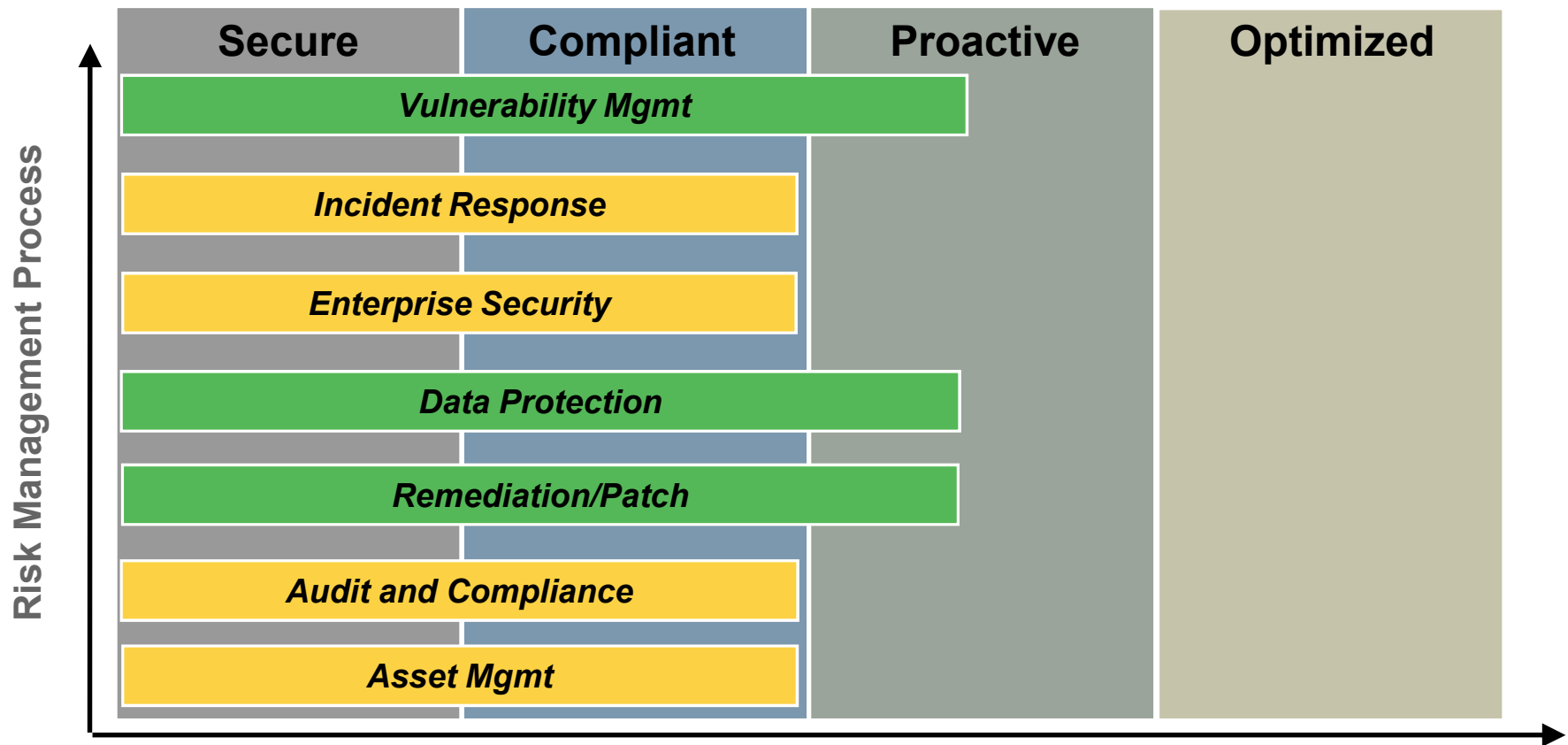
SAMPLE

McAfee

9/19/2008

Protect what you value.

Risk Process Maturity “To-Be” Environment



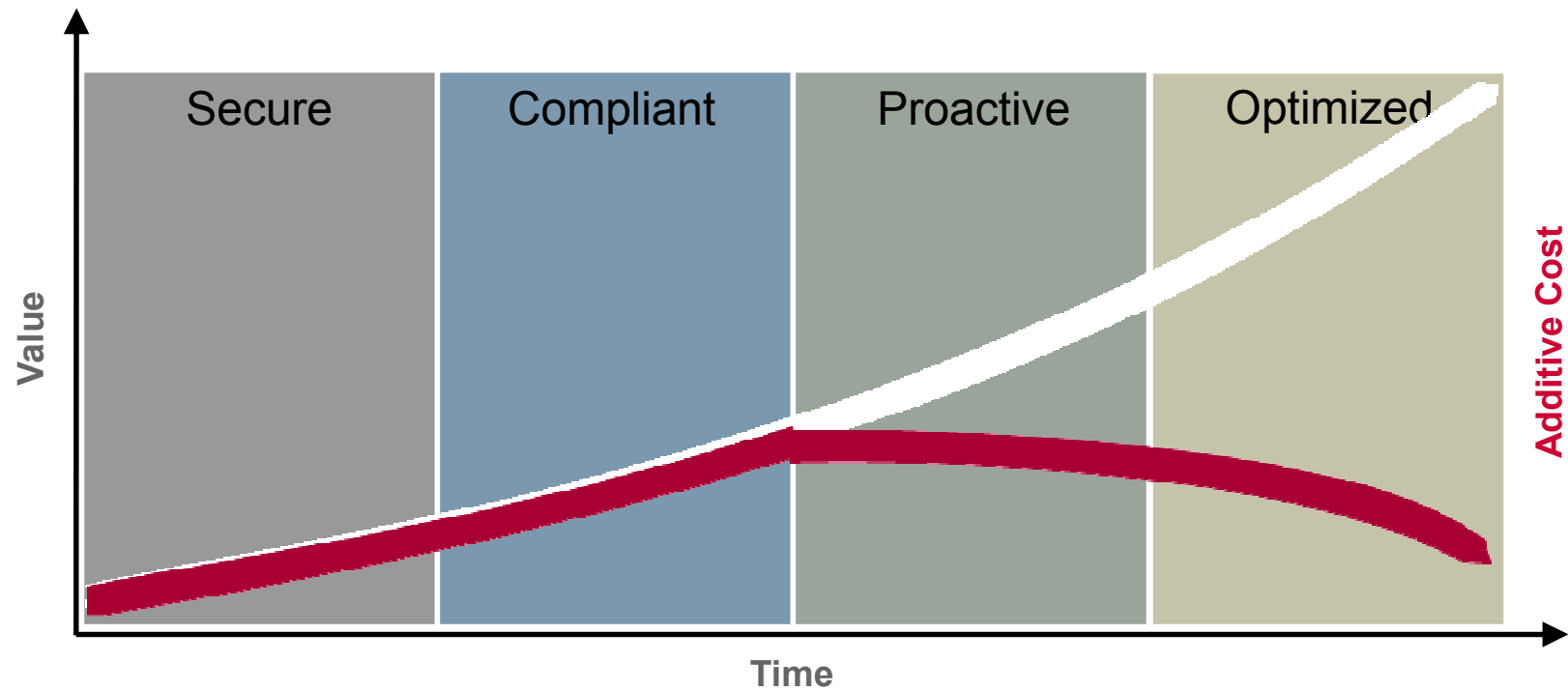
SAMPLE

McAfee

9/19/2008

Protect what you value.

Cost to Value Relationship



The relationship to cost and security diverge during progression to the Proactive and Optimized states.

McAfee

9/19/2008



Protect what you value.

Well-known Financial Corporation

Optimization through integration & consolidation

Secure and Optimized



Web Content Filtering



Email Content Filtering – Gateway AV



McAfee ePO



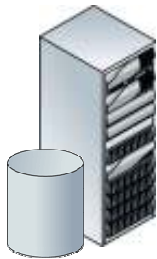
Network IDS



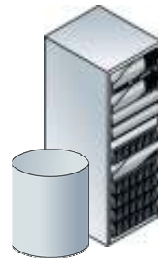
Qualys



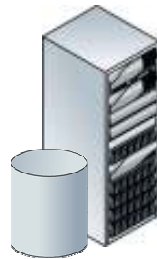
Host IPS



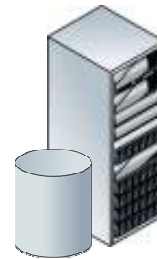
Web Content Filtering



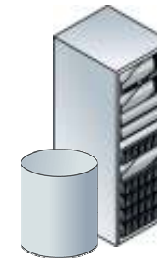
Email Content Filtering – Gateway AV



McAfee ePO



Network & Host IPS



Desktop IPS



Value of Optimized Security and Compliance in Action

		McAfee on McAfee		
		2005	2006	2007
NonOptimized Environment				
	Exposure: 9 Days			
McAfee Optimized Environment				
	Exposure: 0 Days			
	Number of Patch Cycles	19	9	4
	Number of People Assigned to Patch Operations	41	19	4
	Average Hours per Patch Cycle	73	68	24
	Total FTE	27	5.6	1.5

Approximately 5,000 Desktops and Laptops, 700 Servers; in 31 countries,

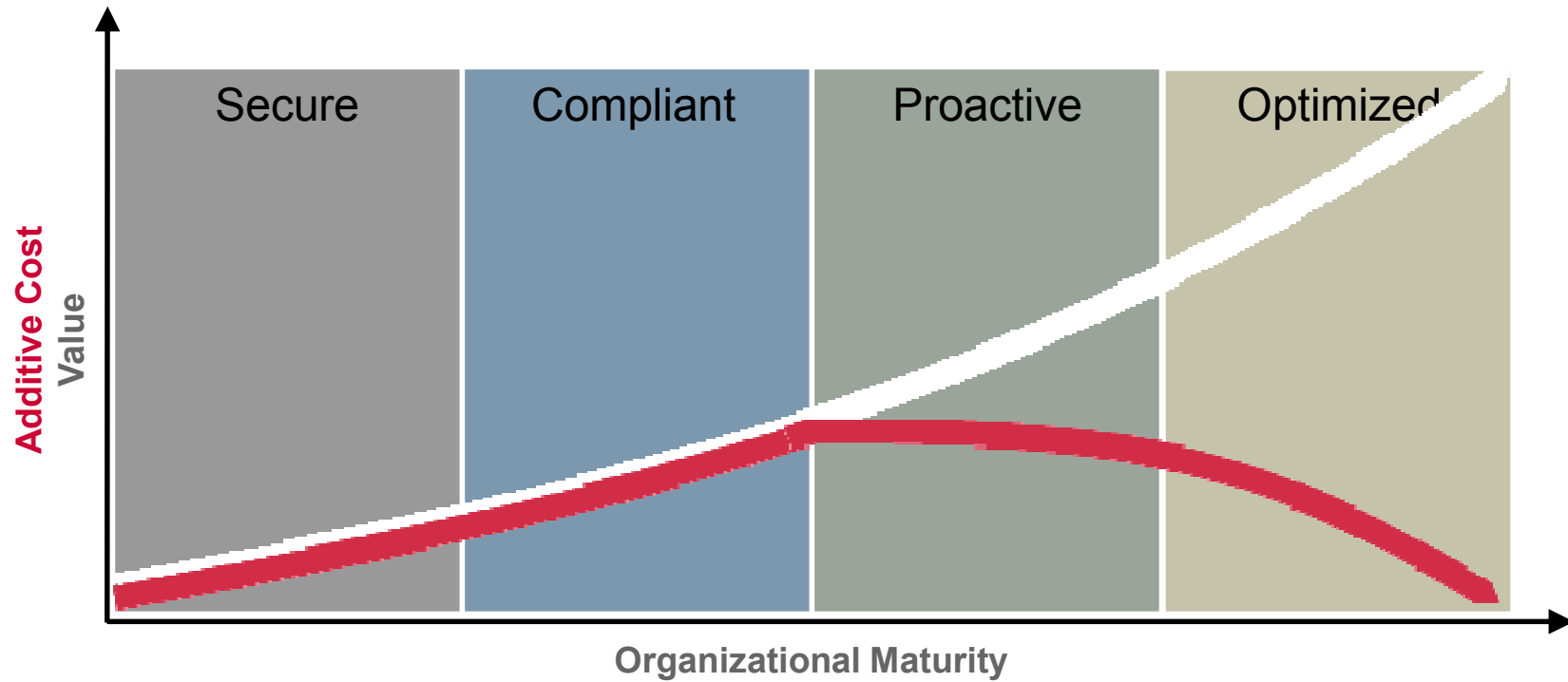


9/19/2008



Protect what you value.

Where Is My Organization?



McAfee

9/19/2008



Protect what you value.

Thank You

972-963-79710

510-914-0177

Charles_Ross@mcafee.com

www.mcafee.com

| Direct

| Mobile

| E-mail

| Web

McAfee

9/19/2008



Protect what you value.