McAfee Total Protection

Endpoint Security Overview for MEEC

July 12, 2011

Sumeet Gohri, CISSP

Sr. Sales Engineer GovED + Healthcare

McAfee, Inc.

Agenda

○ Endpoint Protection Challenges

○ McAfee Endpoint Protection Products

○ McAfee ePO walkthrough

○ McAfee EMM Overview & walkthrough

Threats Are Targeting You

Spam volume down ~50%, but mobile threats up 46%

(Q4 2010, McAfee Labs)

An average of 4 million new zombies created per month[1]

New attacks on Adobe vulnerabilities outnumber those on Microsoft products 100:1

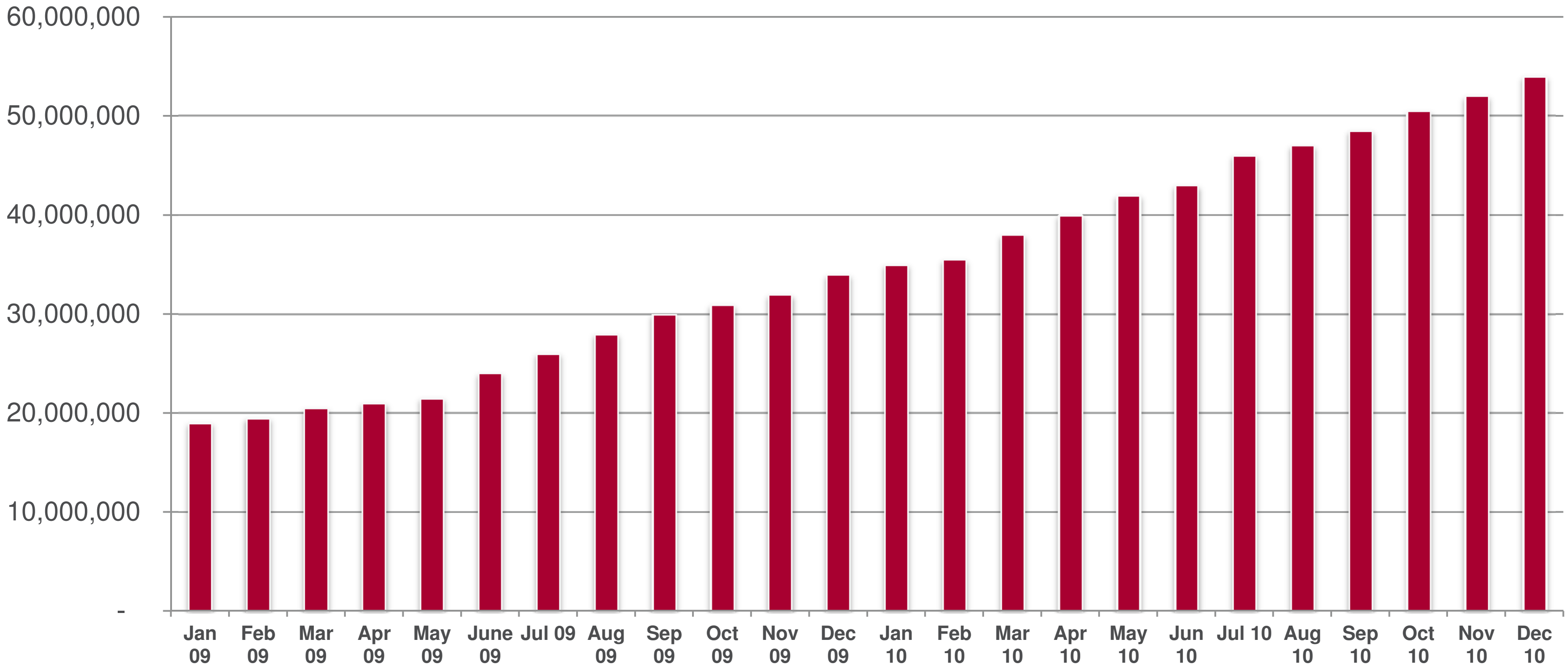
(Q4 2010, McAfee Labs)

Email is the main carrier of malware and phishing scams[1]

Source: [1]McAfee, [2]Javelin Strategy & Research

Key Trend: Malware Growth Continues

○ McAfee Labs identifies approximately 55,000 pieces of new malware each day



Total Malware Samples in the McAfee Labs Database

The growth in the number of new malware samples found continued in Q4 growing 15% over Q3.

Are These Impacting You?

Technology explosion bringing unknown threats

Win 7 OS Refresh

Reduced IT Budget

Virtualization Projects

Security Audit brings new requirements

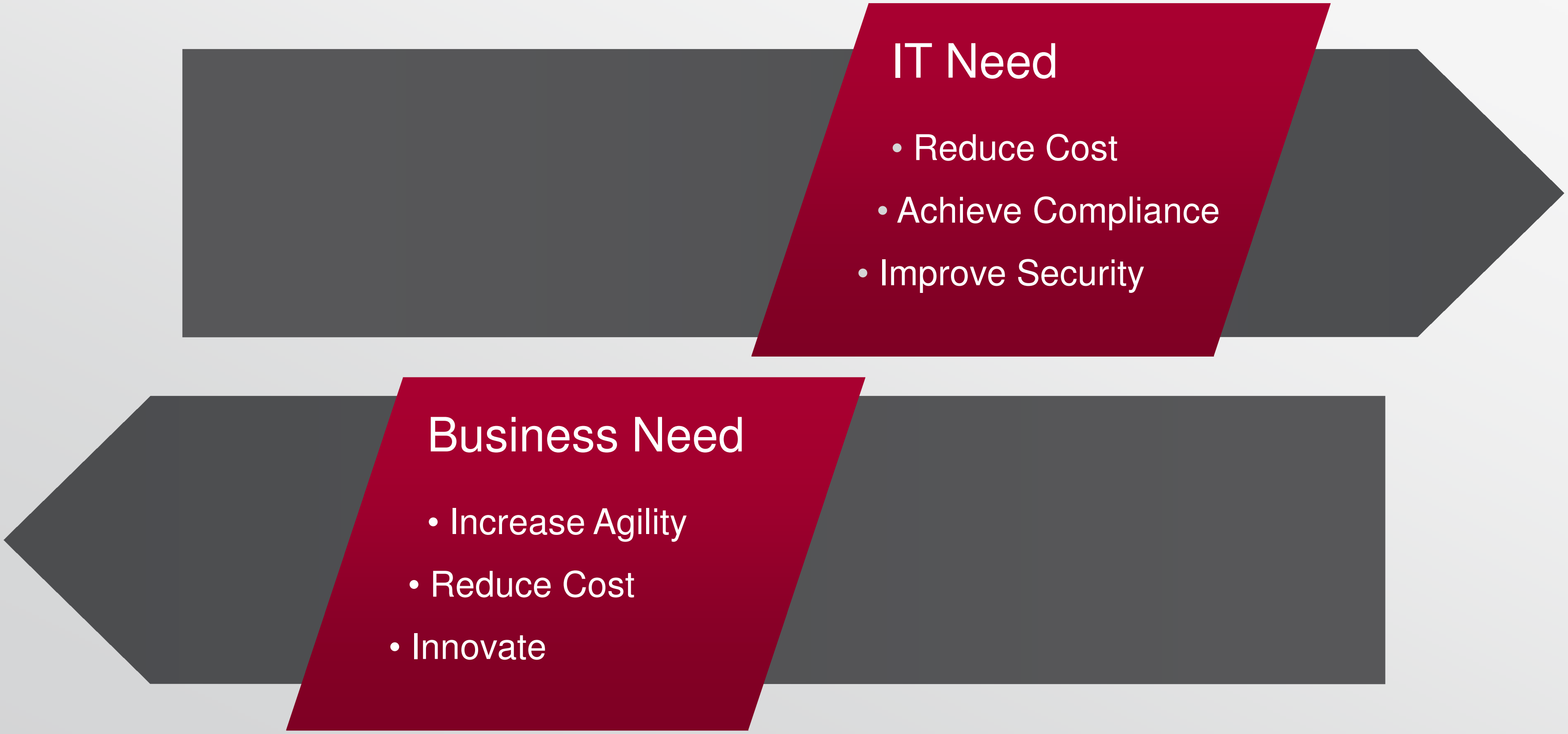
Company Acquisition or Divestiture

New management
New IT strategy

New Regulatory Compliance Needs

Today's Dilemma

McAfee



IT Need

- Reduce Cost
- Achieve Compliance
- Improve Security

Business Need

- Increase Agility
- Reduce Cost
- Innovate

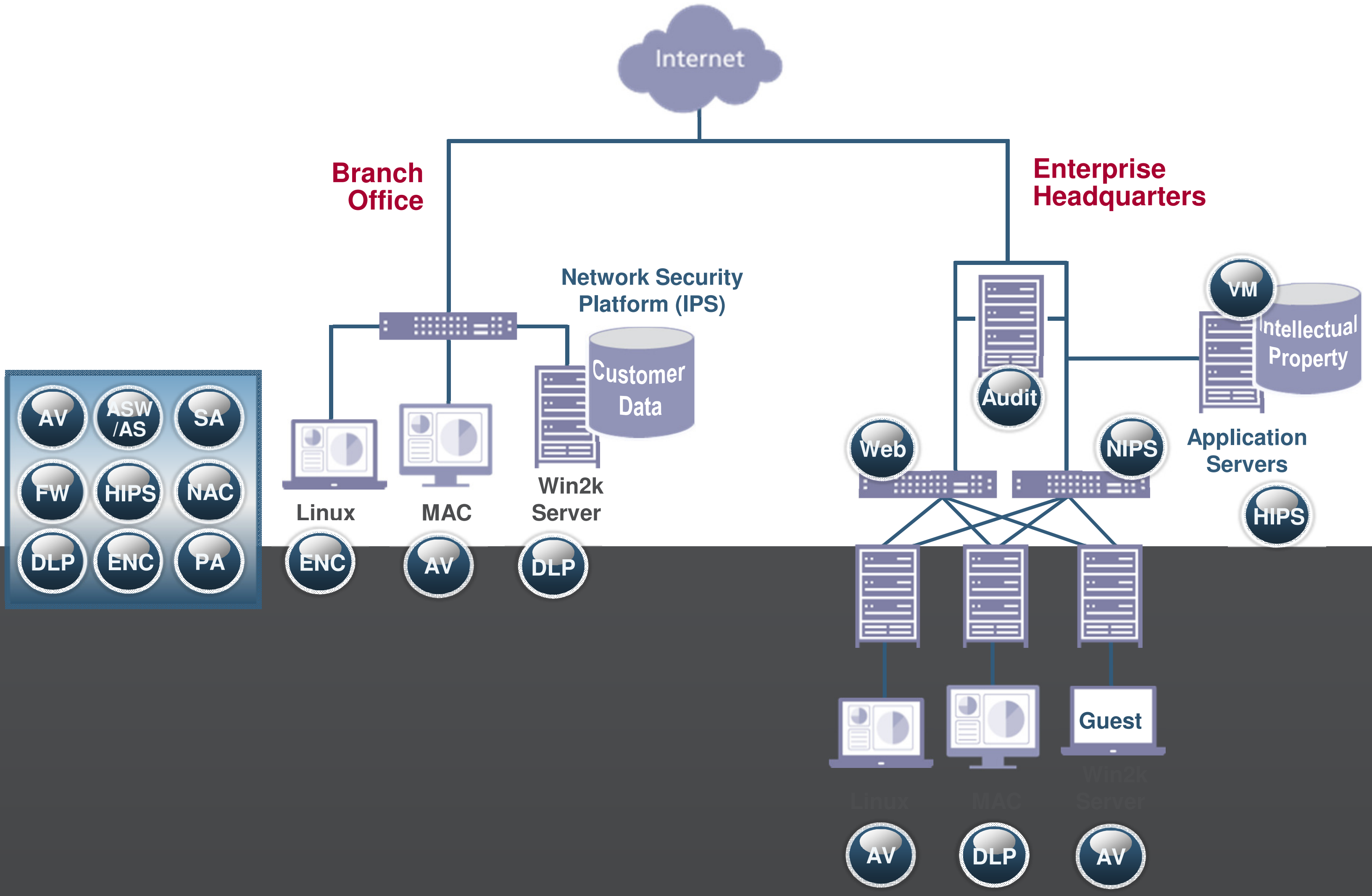
A Better Way

What if…

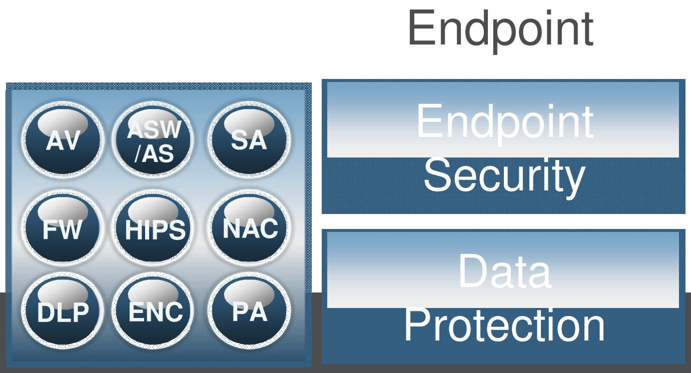
- Operational management costs were reduced?
- Security infrastructure costs could be cut?
- Patching new vulnerabilities was less urgent?
- Event management and escalations were streamlined?
- Compliance was a natural result of your security investment?

McAfee Helps You Achieve an Optimized Endpoint Security Architecture

McAfee



McAfee Helps You Achieve an Optimized Endpoint Security Architecture



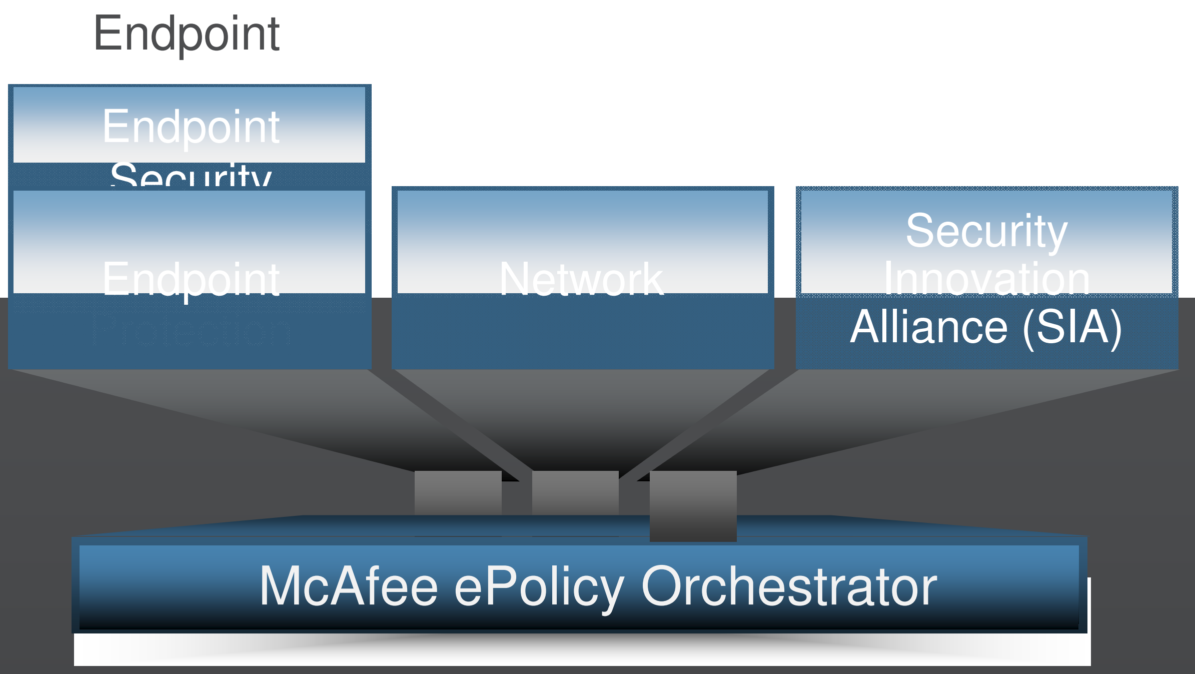
Endpoint

AV
ASW /AS
SA
FW
HIPS
NAC
DLP
ENC
PA

Endpoint Security

Data Protection

McAfee Helps You Achieve an Optimized Endpoint Security Architecture



Endpoint

Endpoint Security

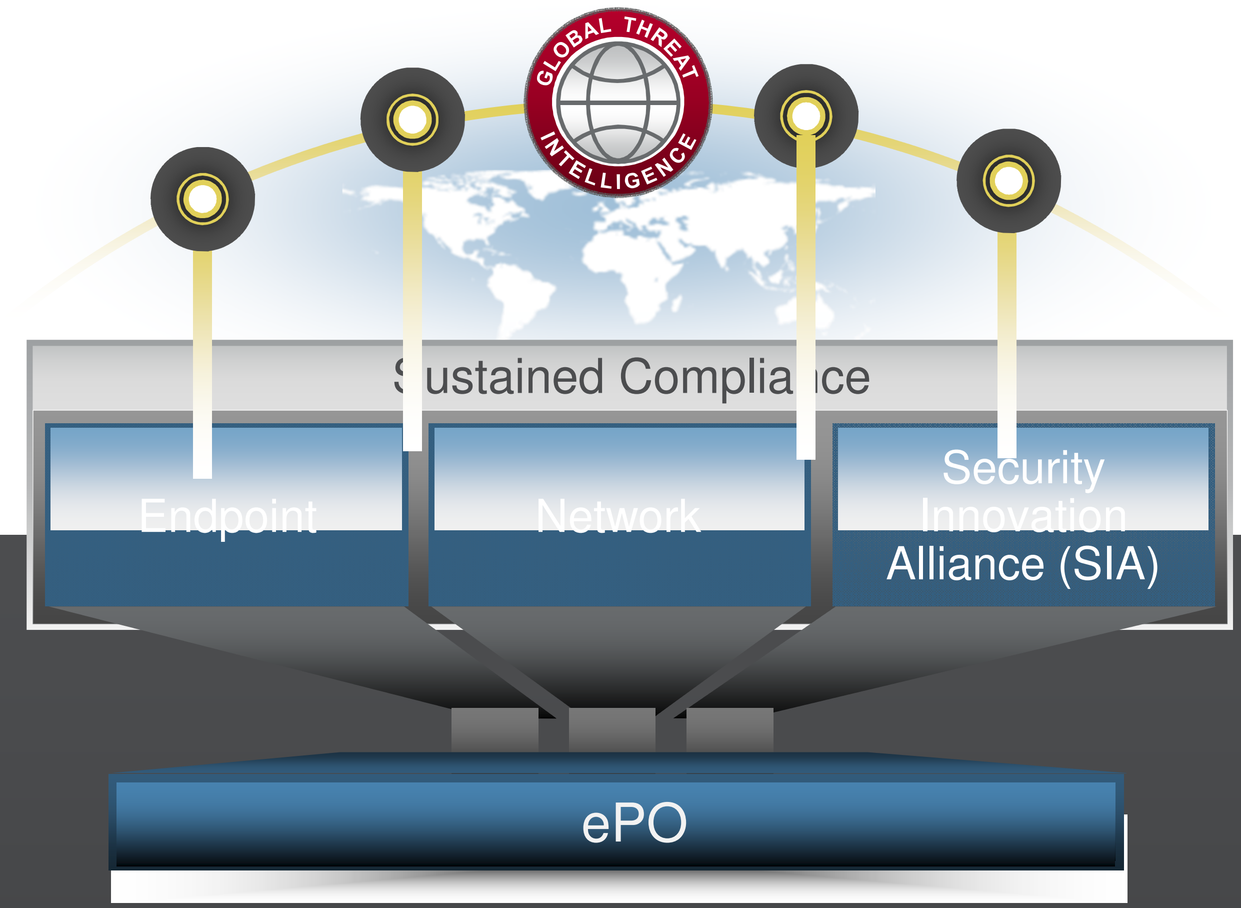
Endpoint Protection

Network

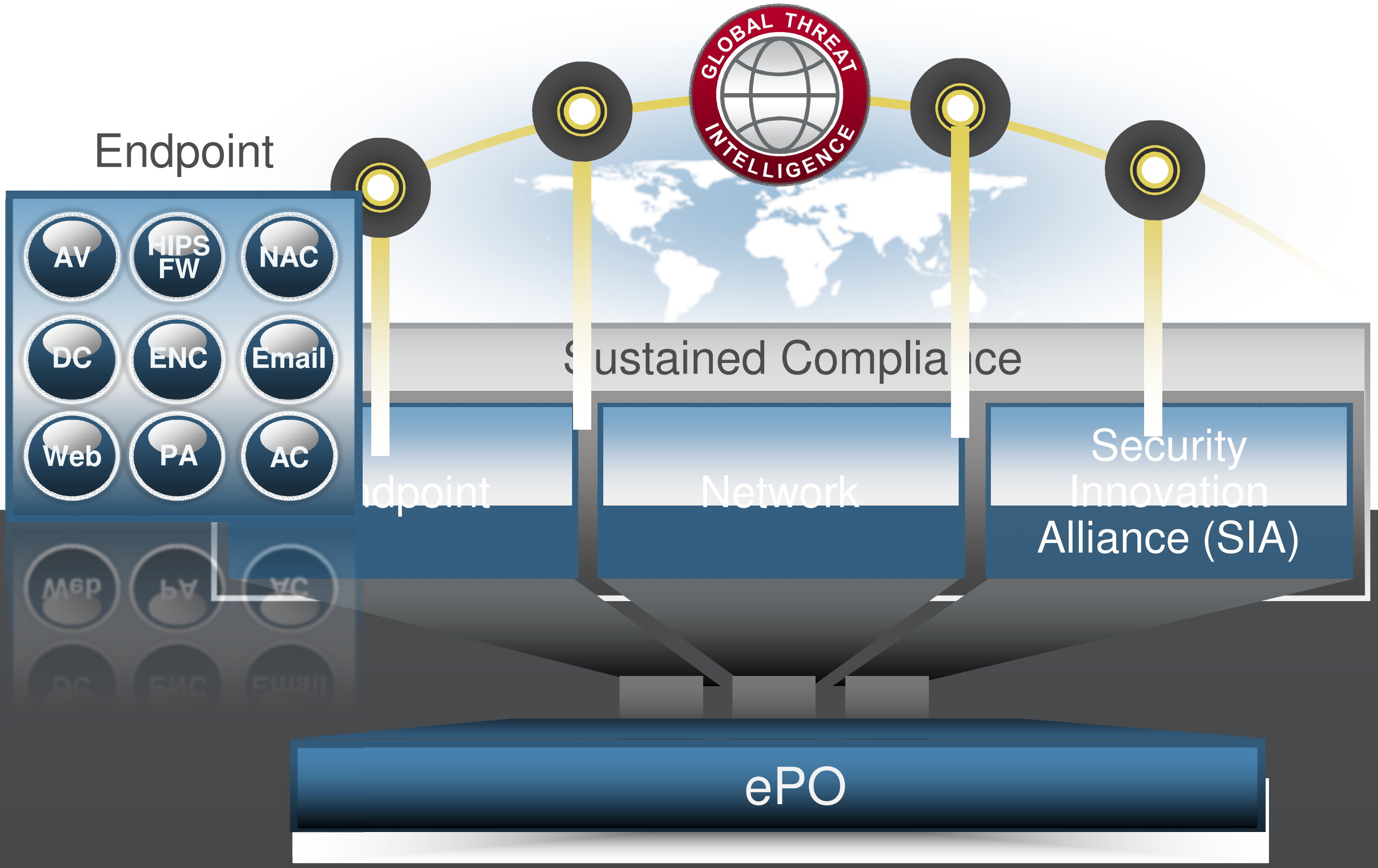
Security Innovation Alliance (SIA)

McAfee ePolicy Orchestrator

McAfee Helps You Achieve an Optimized Security Architecture

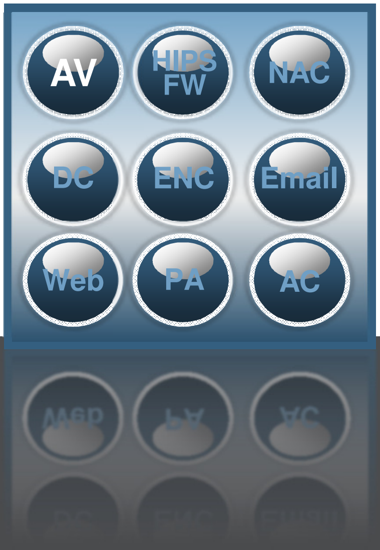

GLOBAL THREAT INTELLIGENCE
Sustained Compliance
Endpoint
Network
Security Innovation Alliance (SIA)
ePO

Protect the Endpoint



Protect the Endpoint

Endpoint

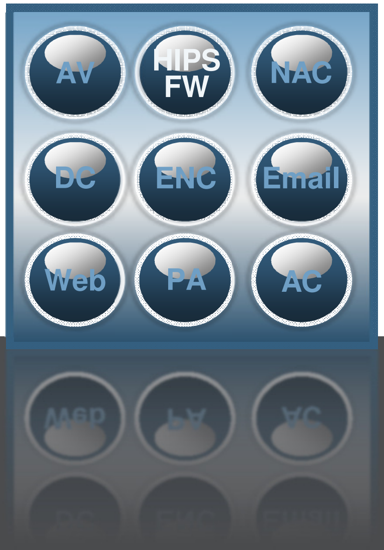


Anti-Malware Protection

- Stops known and unknown malware, spyware, rootkits, key-loggers and more
- Over 99% detection rate
- Proactive, real-time Artemis technology
- Windows, Macintosh and Linux supported
- Broad protection across endpoints, servers and mobile devices

Protect the Endpoint

Endpoint



Host Intrusion Prevention for Desktop with Integrated Firewall

- Protects against unknown malware and zero-day vulnerabilities
- Delivered zero-day protection for ~90% Microsoft vulnerabilities from “06 to ‘10
- Reduces patching urgency
- Integrated firewall changes protection based on location (i.e. coffee shop vs. office)

Protect the Endpoint

Endpoint

AV
HIPS FW
NAC
DC
ENC
Email
Web
PA
AC

Network Access Control (for Managed Endpoints)

- Ensure endpoint compliance prior to and after network access
- Prevent users from disabling security tools
- For unmanaged (guest) endpoints, integrates with McAfee NAC Appliance and NAC Add-on to Network Security Platform

Protect the Endpoint

Endpoint

AV
HIPS FW
NAC
DC
ENC
Email
Web
PA
AC

Device Control

- Protects against accidental/malicious data leaks and unauthorized device usage
- Removable drives, thumb drives
- Real time prevention

Protect the Endpoint

Endpoint

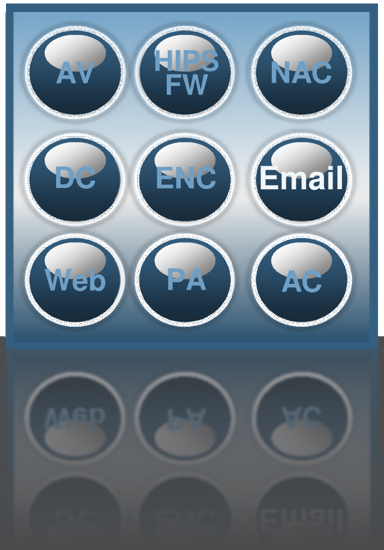
AV
HIPS FW
NAC
DC
ENC
Email
Web
PA
AC

Endpoint Encryption

- Encrypts confidential information:
  - Full-disk
  - File and folder
  - Mobile device and Smart Phone
  - Removable Media
  - USB devices
- Helps meet regulatory compliance if laptop is lost

Protect the Endpoint

Endpoint

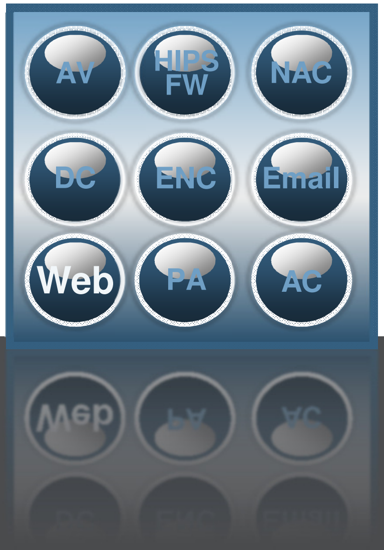


Email Security

- Automated malware filtering at the email server
- Attachment scanning
- Anti-spam filtering
- Leverages proactive Artemis technology to stop new and emerging threats

Protect the Endpoint

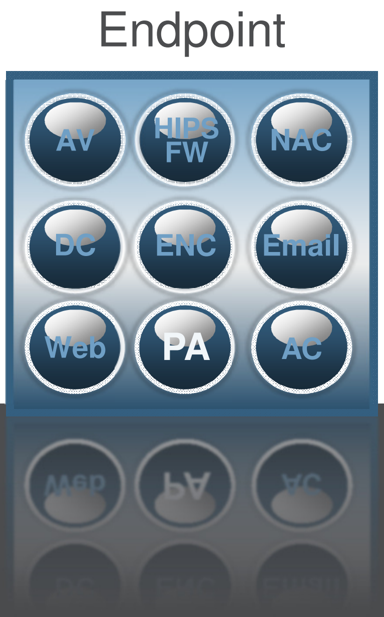
Endpoint



Web Security

- Warn and block employees before they interact with dangerous websites
- Granular user-based policy and reporting on web usage
- Monitor, control and block web content
- Reduce liability and increase employee productivity

Protect the Endpoint

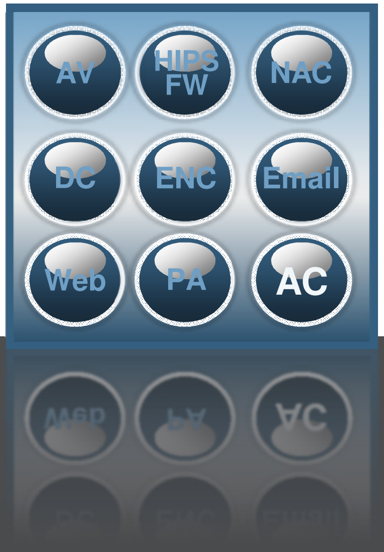


Policy Auditing

- Automates data collection for IT audit reports
- Simplifies compliance with best practice policy templates
- Integrated with McAfee Remediation Manager for endpoint remediation

Protect the Endpoint

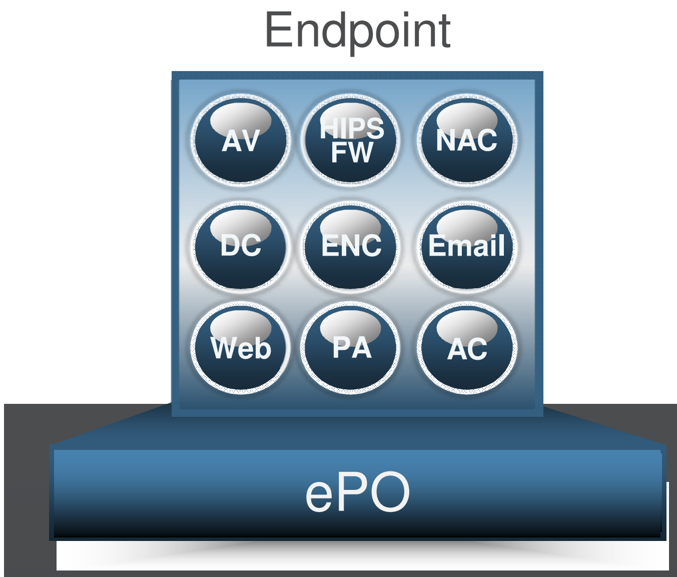
Endpoint



Application Control (Whitelisting)

- Ensures only trusted applications run on endpoints and servers
- Dynamic whitelisting reduces cost of ownership
  - No database, rules or updates needed
- Proactive protection against zero-day threats
  - Comprehensive code coverage that prevents exploits from running

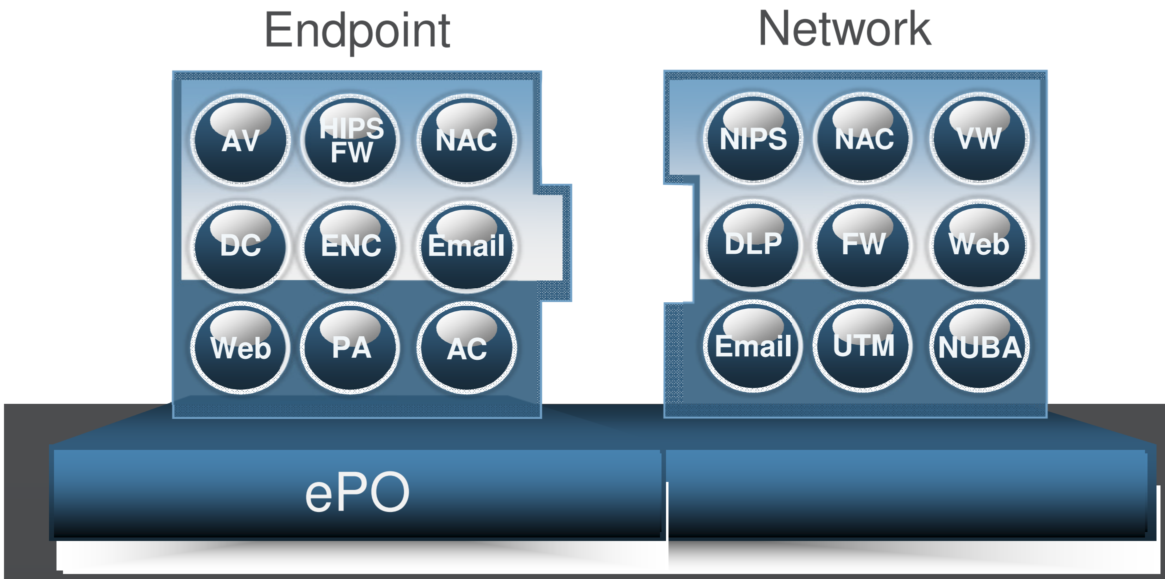
Protect the Endpoint



Single Integrated Management

- Single agent, single console
- Web-based console for access from anywhere
- Open architecture
- Manages all endpoint solutions
- Lower operational costs with improved visibility and efficiency

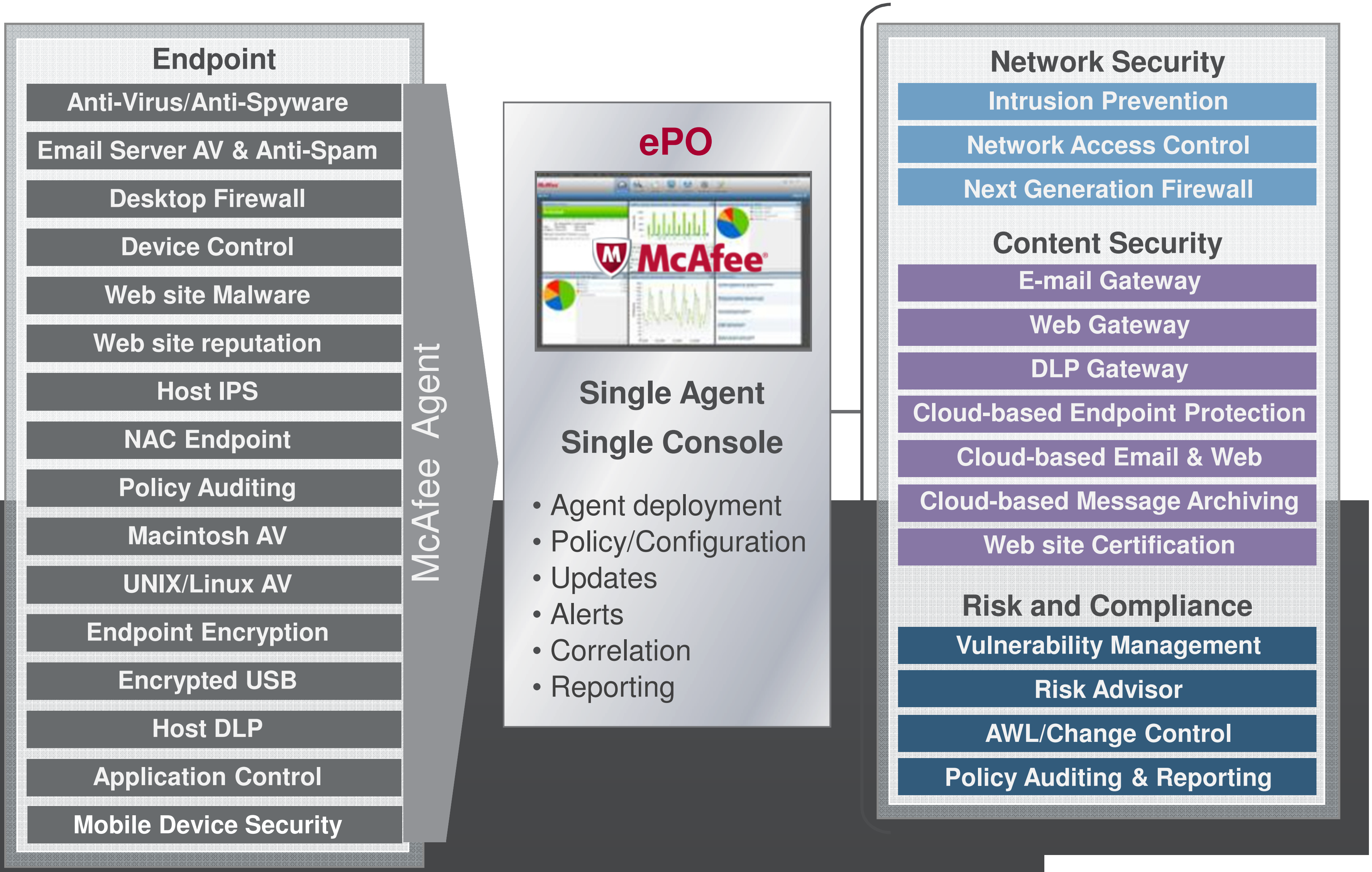
Endpoint and Network Interlock



Reduced compliance and operating costs

- Integrated network and endpoint products
- Simplified administration
- Reduced errors

McAfee Integrated Security Platform



Endpoint

- Anti-Virus/Anti-Spyware
- Email Server AV & Anti-Spam
- Desktop Firewall
- Device Control
- Web site Malware
- Web site reputation
- Host IPS
- NAC Endpoint
- Policy Auditing
- Macintosh AV
- UNIX/Linux AV
- Endpoint Encryption
- Encrypted USB
- Host DLP
- Application Control
- Mobile Device Security

McAfee Agent

ePO

Single Agent

Single Console

- Agent deployment
- Policy/Configuration
- Updates
- Alerts
- Correlation
- Reporting

Network Security

- Intrusion Prevention
- Network Access Control
- Next Generation Firewall

Content Security

- E-mail Gateway
- Web Gateway
- DLP Gateway
- Cloud-based Endpoint Protection
- Cloud-based Email & Web
- Cloud-based Message Archiving
- Web site Certification

Risk and Compliance

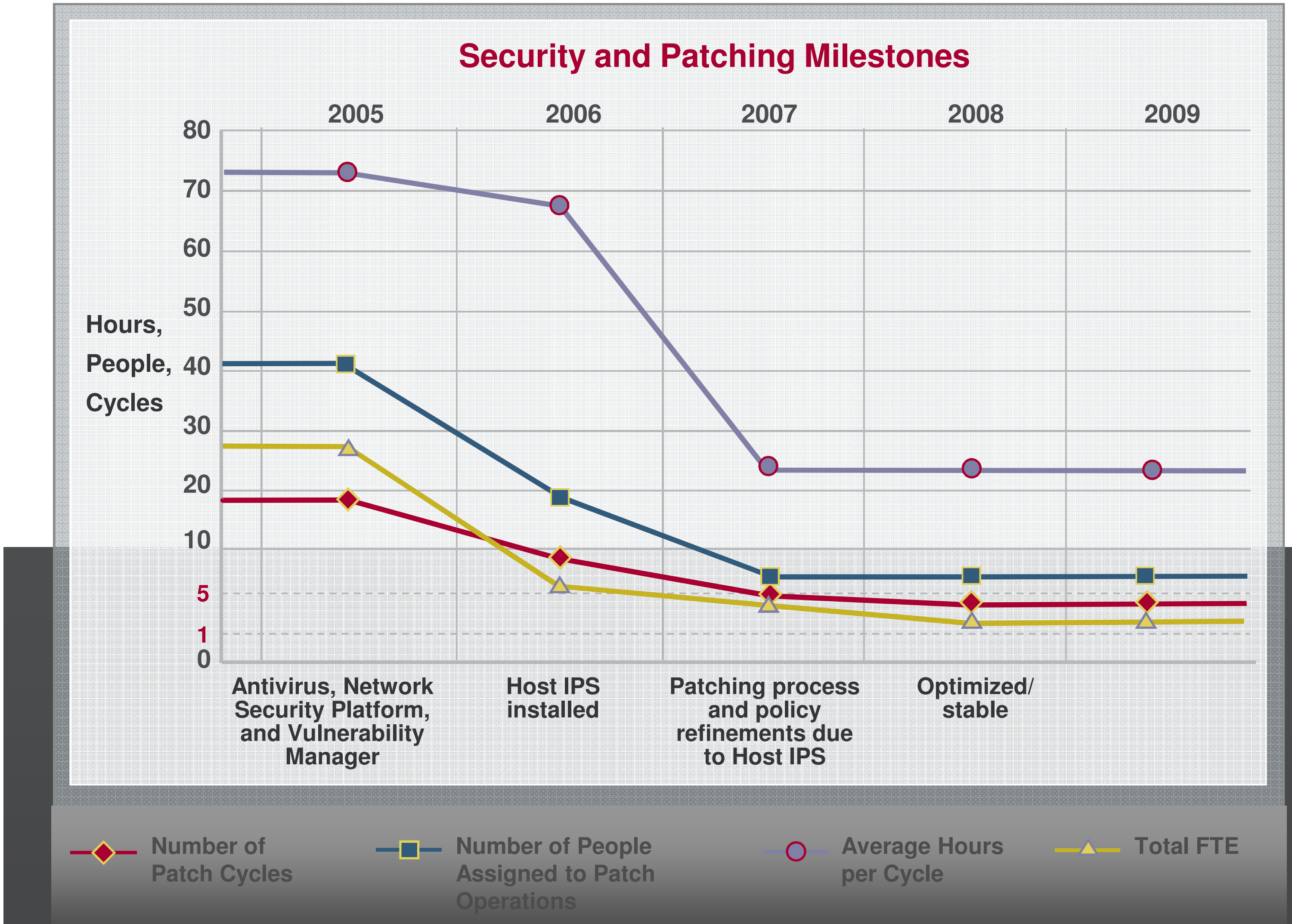
- Vulnerability Management
- Risk Advisor
- AWL/Change Control
- Policy Auditing & Reporting

Optimized Security in Action – McAfee Risk Advisor

To run this demo, you must have the CARMA_demo.swf file in the presentation directory. Left click on the image to start/stop

Cost Savings Through Planned Patching

McAfee @ McAfee



- FTE dedicated to patching reduced from 27 to 0.3
- Saved $5.5M over 3 years

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

Total Protection Lowers Operational Cost

Spend Less Time
Managing Security

- 38% less time on security reporting
- 41% less time developing security policies

- 30% more endpoints
- 50% less hardware

Manage More Nodes
with Less Hardware

Use Less Admins
More Efficiently

- Admins save about 6 hours per week
- 38% less time to manage security

MSI International, survey of 488 ePO and non-ePO users

Insight Express, survey of 387 ePO and non-ePO customers users

Top Reasons to Upgrade to Total Protection Solutions

1 **Save Money**

By consolidating your security solutions with one vendor, you can gain additional protection at a lower cost.

2 **Deploy Quickly**

Because it’s integrated with McAfee ePO, you can manage it easily from one centralized console.

3 **Protect from every angle**

Total Protection for Endpoint provides advanced protection: integrated anti-spyware, zero-day intrusion prevention, and flexible network access control.

4 **Save Time Every Day**

Integration with ePO means you can add increased protection fast.

5 **Leverage the leader**

McAfee has been an endpoint security leader in the Gartner Magic Quadrant for four years and was selected “best endpoint security solution” by SC Magazine for 2009.

McAfee Endpoint Suites

Protection Tier	Total Protection for Endpoint Enterprise Edition Suite	Total Protection for Secure Business	Endpoint Protection Advanced Suite	McAfee Endpoint Protection Suite	McAfee Total Protection for Server	McAfee Endpoint Protection for Mac
Single management console	●	●	●	●	●	●
Real-time malware protection	●	●	●	●	●	●
Desktop firewall	●	●	●	●		●
Desktop host IPS	●	●	●			
Website security	●	●	●	●		
Email server anti-virus & anti-spam	●	●	●	●		
Host URL filtering	●		●			
Device control	●	●	●	●		
Full disk encryption	●	●				
Email & web gateway anti-malware		●				
Network access control (NAC)	●		●			
Desktop policy auditing	●		●			
Multi-platform anti-virus (Linux, Mac, Mobile)	●				●	
Application & change control					●	

Why McAfee Total Protection for Endpoint

McAfee
ePolicy Orchestrator® 4.0
Dashboards
Reporting
Software
Systems
Network
Automation
Configuration
ePO Summary
Options
McAfee Links
Technical Support for Enterprise Products
Go to the McAfee Enterprise Support home page
Virus Information Library
Find detailed information on various threats
McAfee, Inc. Home Page
Go to the McAfee home page
Master Repository Status
Protected
Quick System Search
ePO: Distributed Repository Status
ePO: Compliance Summary
ePO: Malware Detection History
1,200
1,000
800
600
400
200
0
Events
3 Compliant
1 Non-Compliant
YOURBRAND

This master repository is up-to-date with protection against all known threats.

	My Repository	Latest Available
DAT:	5342.0000	5342.0000
Engine:	5200.2160	5200.2160

Use this text box to search systems by system name, IP address, MAC address, or user name.

Query did not return any results.

- Lowest Operating Cost
- Single integrated management console
- Proactive real-time malware detection
- World-class research and support
- Industry leader

Questions ?