

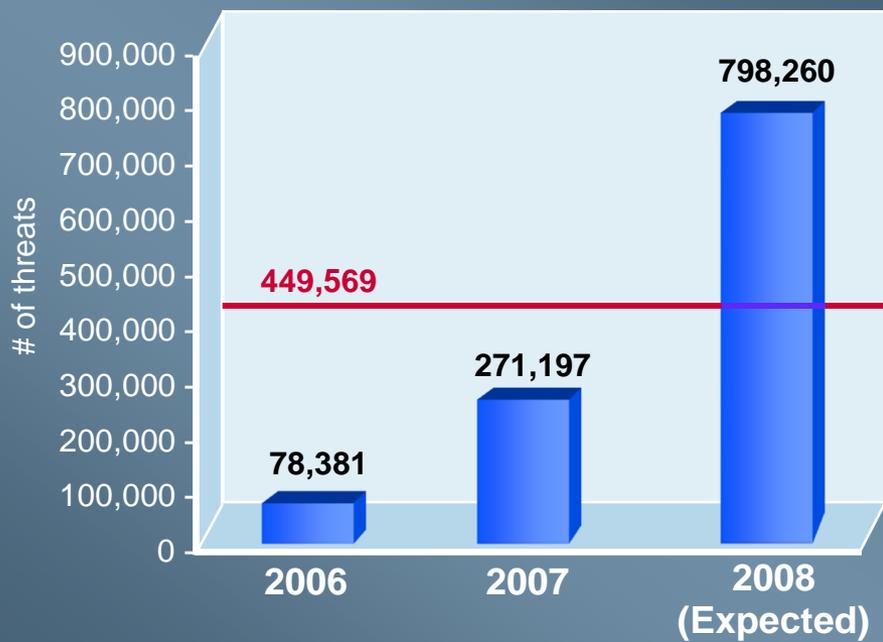


Protect what you value.

Combating Today's Cyber Threats— Inside Look at McAfee's Security

Charles Ross, Director Sales Engineering Public Sector

Altering Threat Landscape



- 246% growth from '06 to '07
- 300% growth projected from '07 to '08
- YTD greater than '06 and '07 combined
- Over 3500 updates added to DAT file per day

Source: McAfee Avert Labs

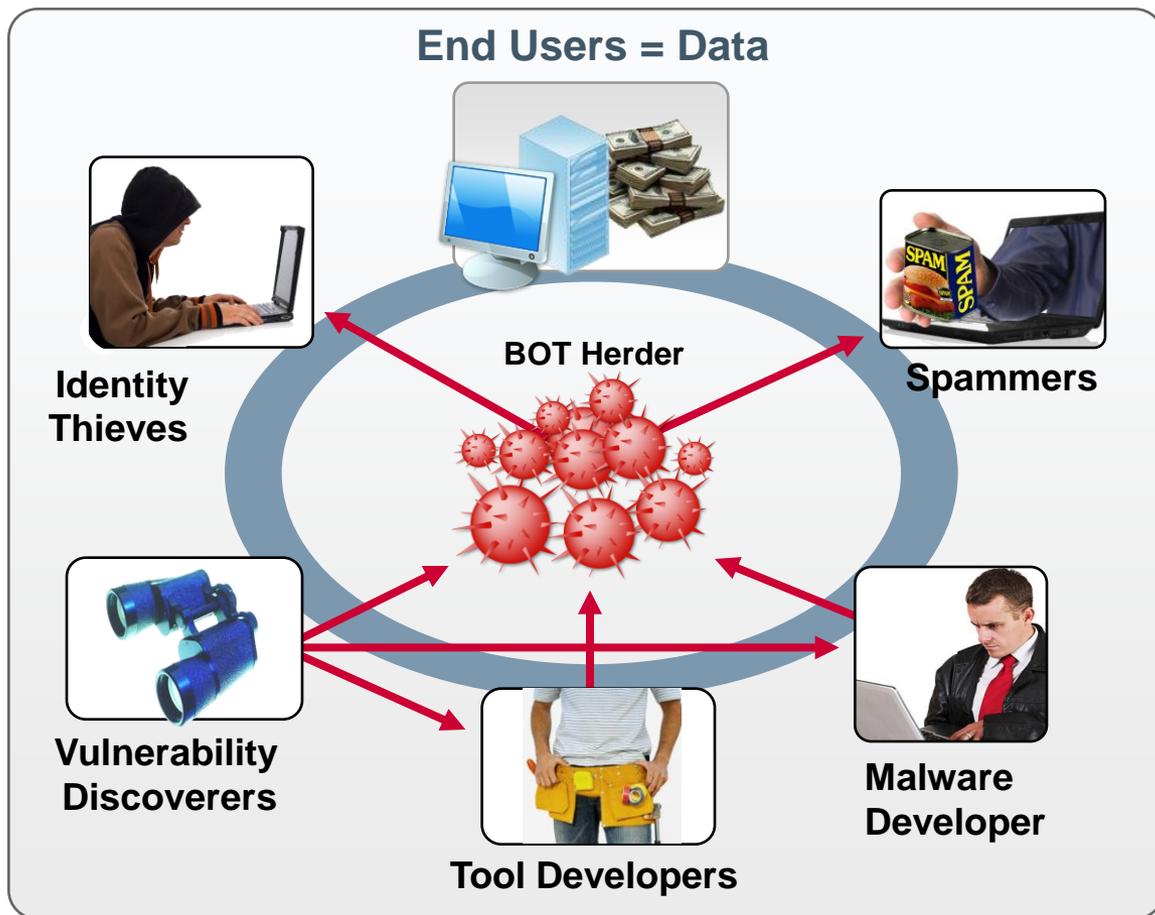
McAfee



Protect what you value.

Altering Threat Landscape (cont.)

Attacker "Ecosystem"



- Change in motivation – monetary gain, not fame
- Traditional malware tools being used to steal data
- 80% of attacks financially motivated; up from 50% two years ago

McAfee



Protect what you value.

Challenges McAfee Internally Faces

- **New Security Era** – Hackers prioritize attacks based on cost/benefit analysis, organizations need to catch up
- **Business Partnership** – Strong security countermeasures are predicated on a strong knowledge of business risk
- **Economic Pressures** - Executives need to understand why they are investing in security – expressed in financial terms
- **Demonstrable Security** - Risk needs to be objectively evaluated and quantitatively measured to be managed effectively



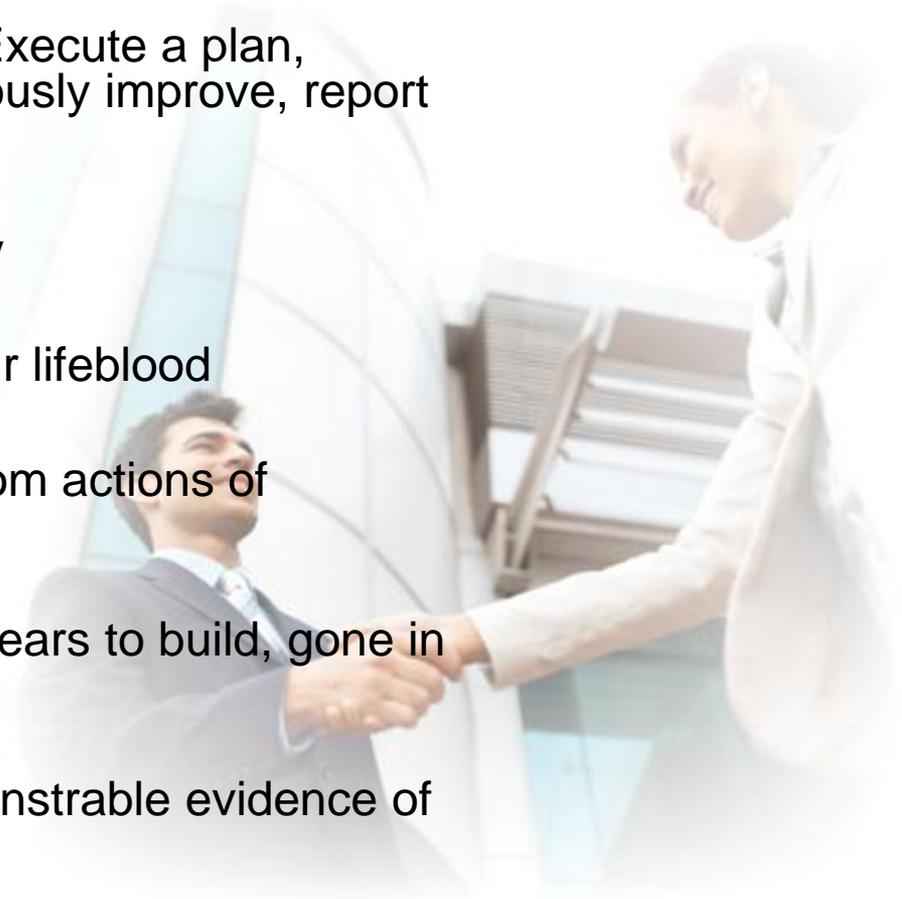
McAfee



Protect what you value.

McAfee's Security Objectives

- **Running security as a “business”** – Execute a plan, provide services, track metrics, continuously improve, report progress
- **Maintain business system availability**
- **Protect intellectual property** – IP is our lifeblood
- **Limit corporate liability** – Insulation from actions of employees
- **Safeguard the corporate brand** – 18 years to build, gone in an instant
- **Ensure compliance** – Simplified, demonstrable evidence of security effectiveness



McAfee

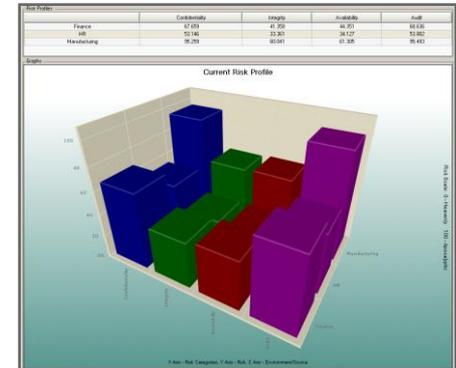


Protect what you value.

Managing Business of Security

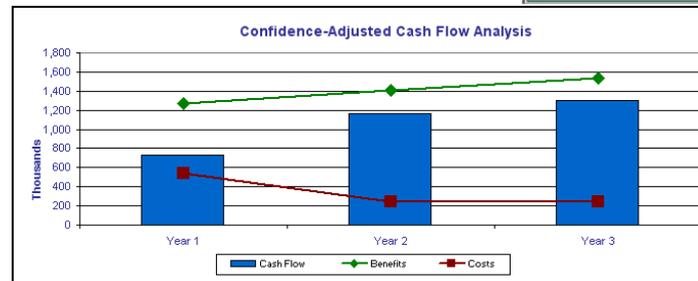
Quantitative Risk Assessments

- Benchmark performance in IT governance, risk, compliance
- Identify areas that require improvement
- Communicate results in clear, crisp business language



Accountability for Results

- Defend proposed budget
- Influence decisions on strategy
- Gain credibility by demonstrating efficiencies/cost savings



	Year 1	Year 2	Year 3	Total	NPV
Return on Investment (ROI)	299%				
Payback period (months)	9				
Total Return (\$)	\$734,080	\$1,164,520	\$1,297,441	\$3,196,041	\$2,604,546
Total Benefit Savings	\$1,273,499	\$1,406,419	\$1,539,340	\$4,219,258	\$3,476,585
Total Costs	\$539,419	\$241,899	\$241,899	\$1,023,217	\$872,040

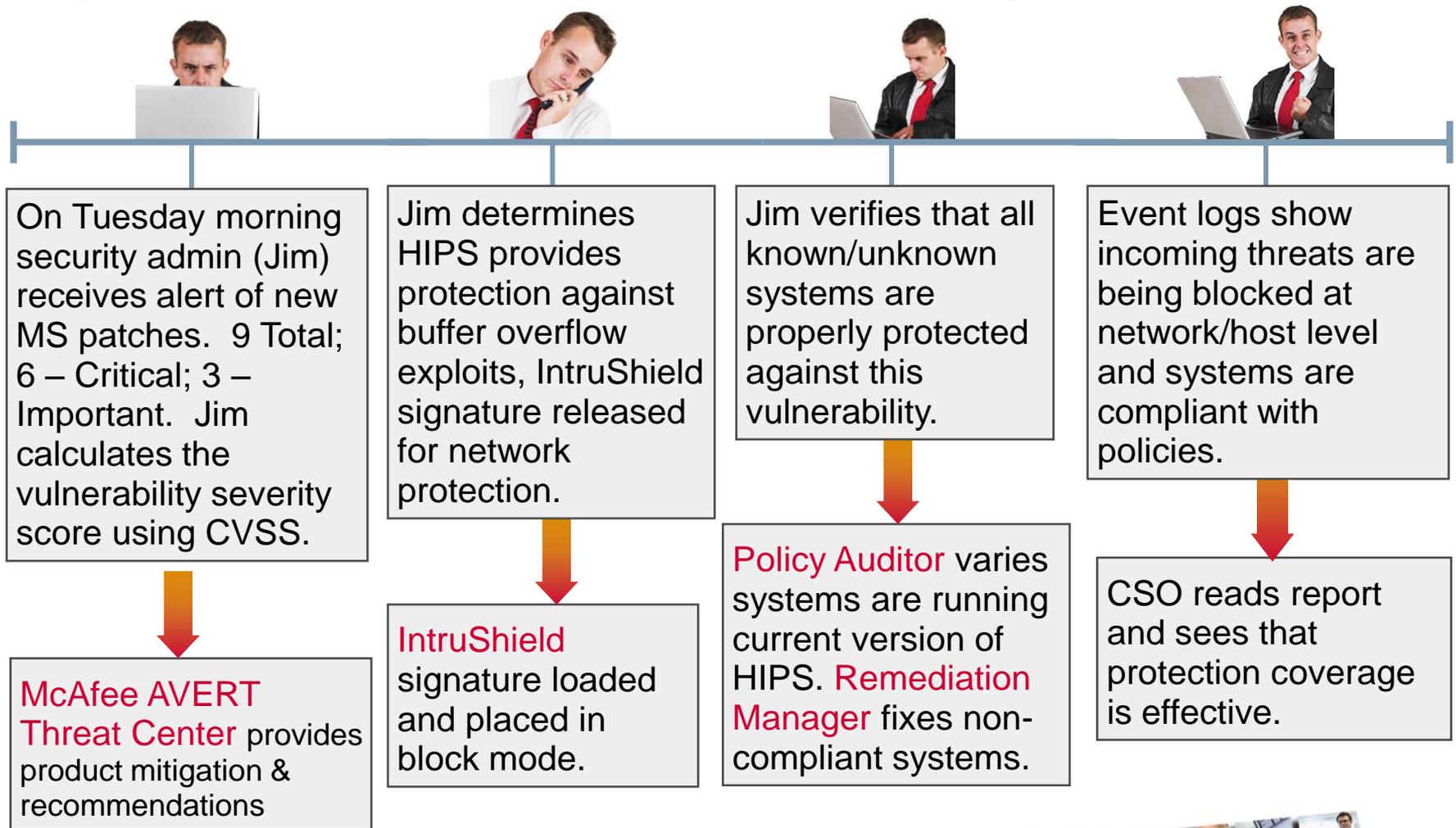
McAfee



Protect what you value.

A Day in the Life – McAfee Threat Mitigation Process

Organizational confidence achieved without patching



McAfee



Protect what you value.

McAfee@McAfee Patch Optimization

Non-Optimized Environment

Exposure: 9 Days

McAfee Optimized Environment

Exposure: 0 Days

McAfee on McAfee

	2005	2006	2007
Number of Vulnerabilities (CVE)	4,933	6,608	6,515
Number of McAfee 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



Protect what you value.

Maintaining System Availability

Proactive Threat Management

- 2007: 6,516 vulnerabilities, 69 MS patches released, **McAfee patched 4 times**
- 0-day protection with network/host IPS

Resilient Security Ecosystem

- Layered defense – “Swiss cheese” model
- Blade server technology - redundancy/transparent failover for web/email security



Securing Emerging Technologies

- Virtualization – Offline VM scanning, “hyperjacking”, injected VM propagation



Protect what you value.

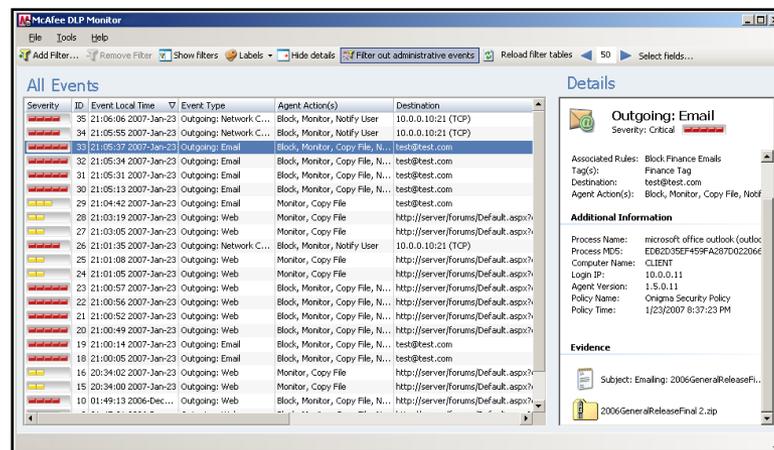
Protecting Intellectual Property

Protecting Data Through It's Lifecycle

- Data at Rest
- Data in Transit
- Data in Use

Prioritized Protection Based on Risk

- Device control / Encrypted USBs – peripheral protection
- Classify data, map location/content, enforce rules, monitor compliance (repeat)
- Full-disk encryption for mobile systems



McAfee



Protect what you value.

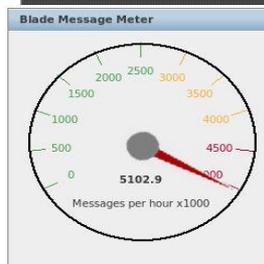
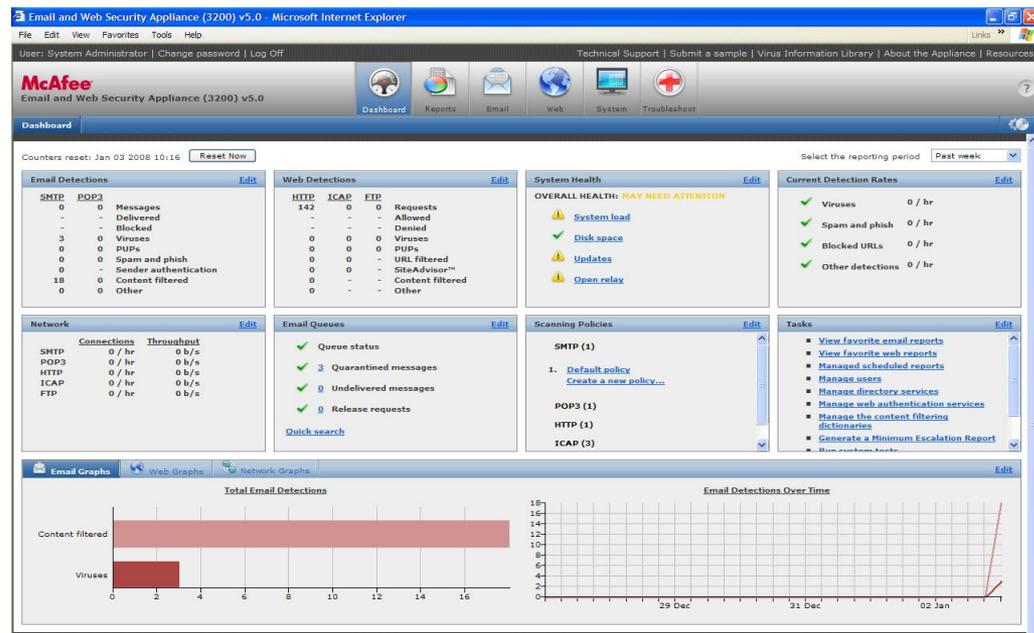
Limiting Corporate Liability

Managing Content

- Control spam – MFE : 1 mil msgs day, 90% spam, 98% catch rate
- Stop malware
- Safe web surfing practices

Managing Systems

- Centralized endpoint protection
- Network Access Control
- Risk-aware Intrusion Prevention



Blade Status									
Name	State	Load	Active	Connections	Anti-Virus Engine	Anti-Virus DAT	Anti-Spam Engine	Anti-Spam DAT	
thames	Network	0	266	155384	5.2.00	5221	2.1.00	5.12.754	
blade1	OK	40	30	17479	5.2.00	5221	2.1.00	5.12.754	
blade2	OK	51	30	17282	5.2.00	5221	2.1.00	5.12.754	
blade3	OK	32	30	17483	5.2.00	5221	2.1.00	5.12.754	
blade4	OK	25	30	17177	5.2.00	5221	2.1.00	5.12.754	
blade5	OK	46	30	17306	5.2.00	5221	2.1.00	5.12.754	
blade6	OK	43	28	17170	5.2.00	5221	2.1.00	5.12.754	
blade7	OK	51	29	17263	5.2.00	5221	2.1.00	5.12.754	

McAfee

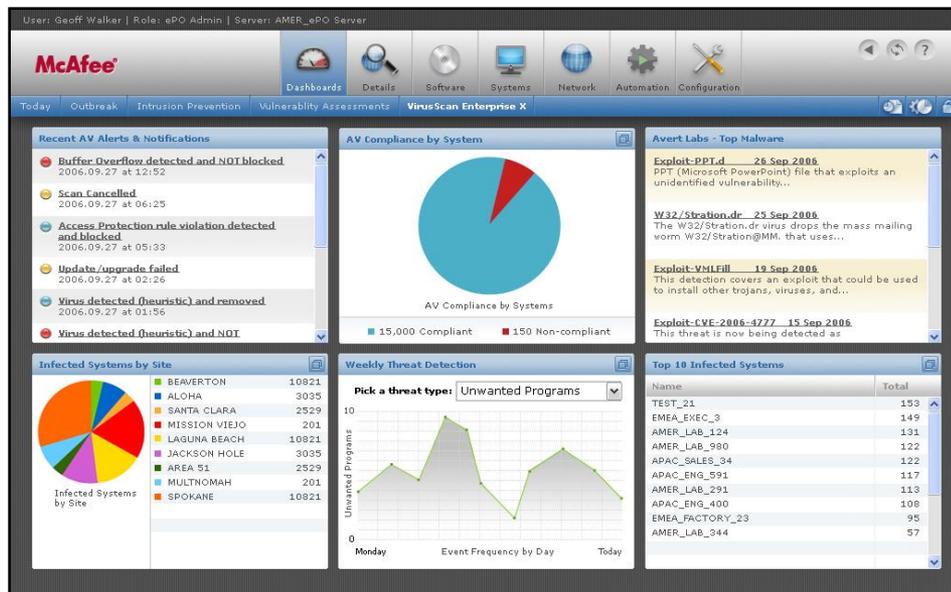


Protect what you value.

Safeguard Corporate Brand

Integrated Security

- One console + one agent + 1.5 FTE's = McAfee's Endpoint Security (~6000 nodes)
- Consolidated reporting identifies problems and correlates security logs quickly
- Trending report data provide leading indicators of suspicious activity
- One of the most attacked websites on the Internet – no outbreaks in 5+ years



McAfee



Protect what you value.

Demonstrating Compliance

Proving Compliance

- Centralized endpoint policy/configuration management
- Enforce and measure compliance against “gold” system standard
- McAfee tracks compliance against 24 regulatory mandates

Increase Auditor Confidence

- Improve assurance by demonstrating continuous control execution
- Customized reporting to satisfy specific audit requirements

