

Get In Control – Stay In Control



Implementing State of the Art Security for a Process Control DCS

Ernest A. Rakaczky

Program Manager – Control Systems Cyber Security
Invensys Operation Portfolio Management Team

Charles Ross

Sr. Director, Sales Engineering Public Sector
McAfee, Inc.

April 7, 2010



AGENDA



Evolving Threat Landscape



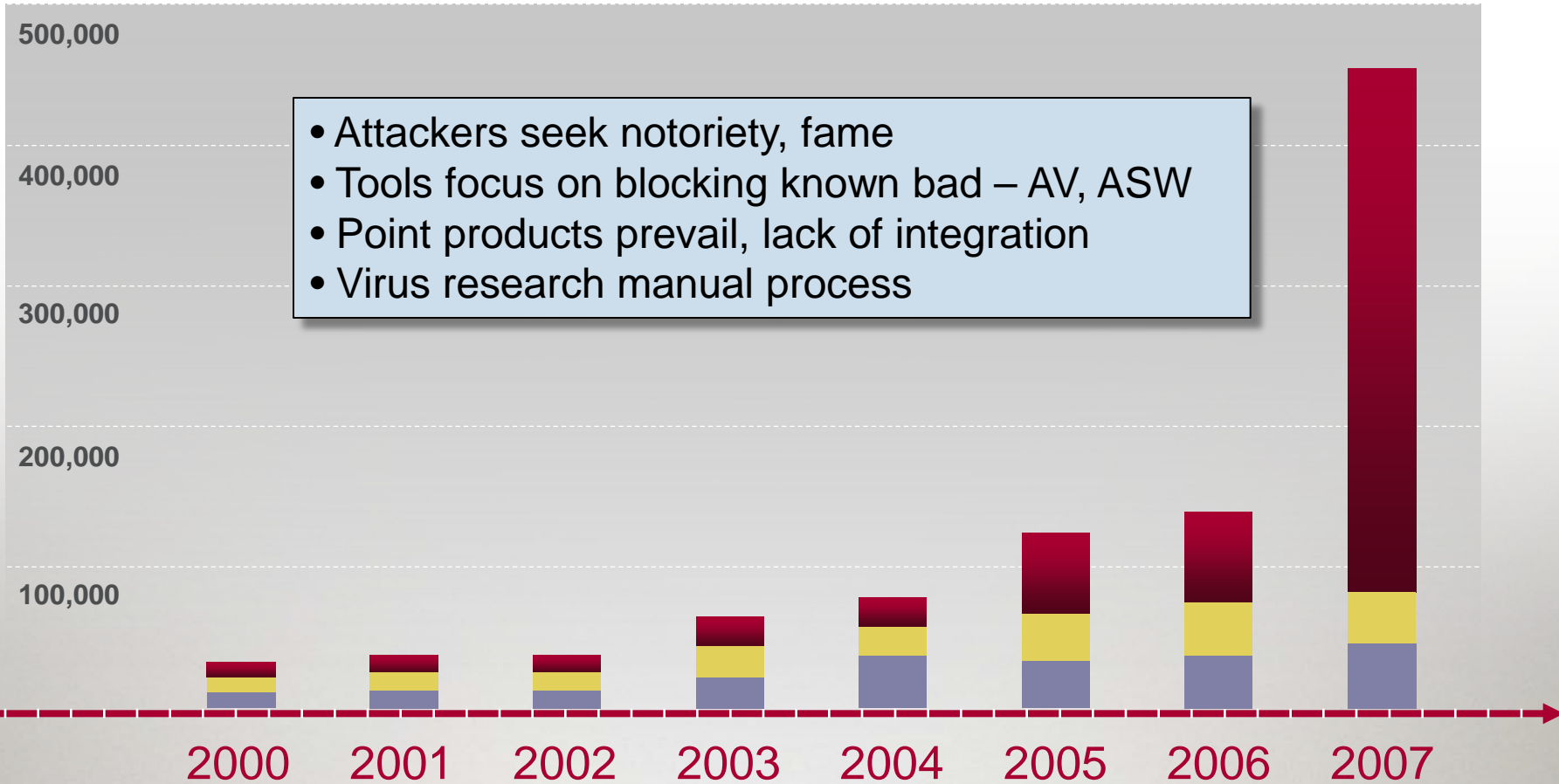
Invensys Case Study



McAfee Energy Security System Solutions (ES³)

Evolving Threat Landscape

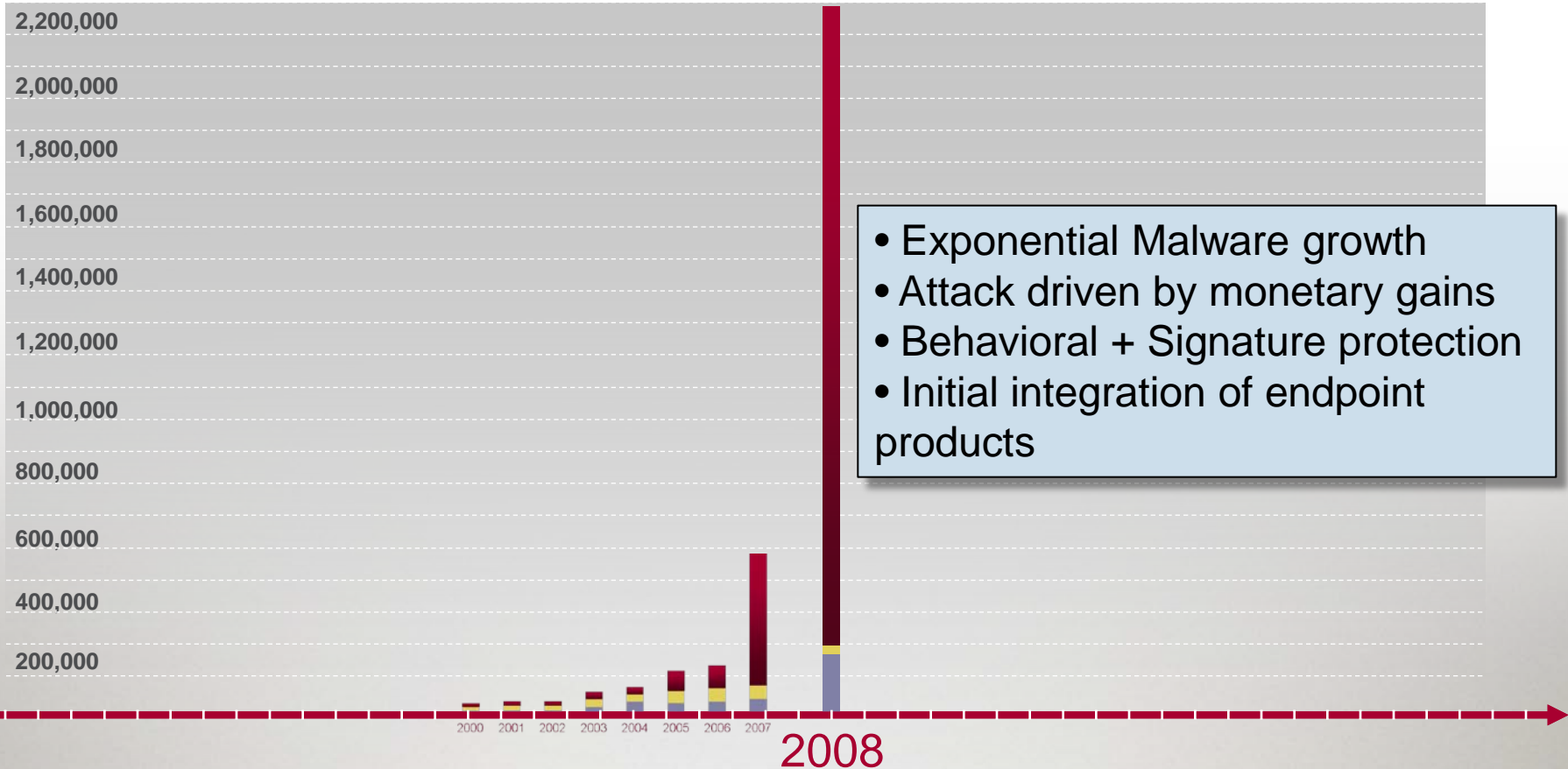
■ Virus and Bots ■ PUP ■ Trojan



Malware Growth (Main Variations)

Evolving Threat Landscape

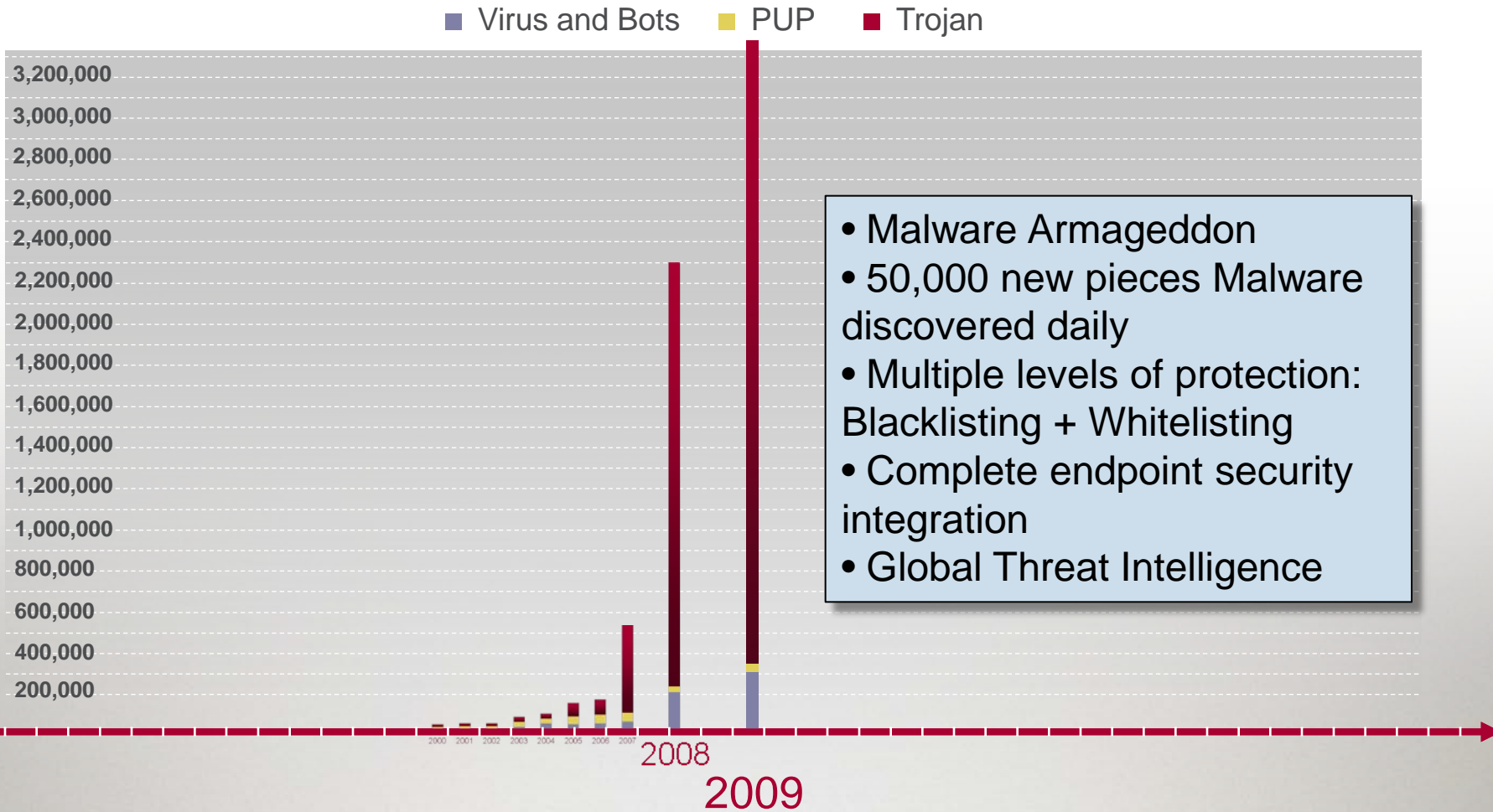
■ Virus and Bots ■ PUP ■ Trojan



- Exponential Malware growth
- Attack driven by monetary gains
- Behavioral + Signature protection
- Initial integration of endpoint products

Malware Growth (Main Variations)

Evolving Threat Landscape



Malware Growth (Main Variations)

McAfee In the Crossfire Report (2010)



- Survey of 600 IT and security executives from critical infrastructure enterprises across seven sectors in 14 countries
- Reported cost of downtime from major cyber attacks to Critical Infrastructure exceeds **U.S. \$6 million per day**
- Intangible costs – **critical operational failures, loss of life, loss of reputation**, etc. difficult to calculate
- More than half of respondents said they had experienced **Large-scale denial of service attacks** by high level adversary like organized crime, terrorists or nation-state (e.g. like in Estonia and Georgia)
- 59% respondents believed that representatives of **foreign governments had already been involved in targeted infiltrations of critical infrastructure**

Invensys : Challenge & Cyber Protection Goals

Challenge

- Provide cyber protection for Control systems manufactured by Invensys
- Preserve business continuity and Operational productivity
- Prevent unknown 0-day threats, reduce patch frequency/urgency
- Protect data confidentiality
- Simplify regulatory compliance

Control System - Cyber Protection Goals

- Adopt holistic view on applying cyber security measures for a control system
- View security with both management & technical perspective
- Ensure security is addressed from both an IT and operational perspective
- Design and develop multiple layers of network, system and application security
- Ensure industry, regulatory & international standards/guidance are understood and adopted where applicable
- Incorporate both Adaptive and Pervasive cyber security measures within the operating plant and control networks



Invensys : Security Requirements

Security Requirements

Control Device/System

- Password changeability
- Tight application control – minimal services, least privilege
- Strong access control & tracking
- Application identification and requirements
- Embedded Anti-virus & Malware protection
- Ability to implement security updates/patches

Delivery Processes

- Software validation & testing
- SAT & FAT specific security requirements – baseline
- Remote support requirements
- Life-Time support requirements
- Antivirus & Malware protection updates
- Clear software patch validation & implementation process
- Personnel clearance, tracking & validation



Invensys : Security & Compliance Requirements

Security Requirements (cont.)

Cyber Security Program

- Risk assessment
- Security gap analysis
- Definition of security policy and procedures
- Access controls and measures
- Defining Defense-in-Depth, Layers of protection
- Creating Data Isolation & Control, DMZ's/Secure Zones
- Site security management requirements



Compliance Requirements

- NERC CIP Compliance Program
- CFATS – Chemical Facility Anti-terrorism Standards
- NIST SP800
- ISAS99 – ISCI (Security Compliance Institute)
- Common Procurement Program with DHS
- CSSP Program within DHS – National Labs
- Industry Specific Roadmaps to Secure Control Systems
- IEC-62351 & IEC62443, IEEE-1402
- IAEA & NRC Nuclear Requirements

I/A Series® Security Enhancements Project

- Distributed Control I/A Series® Upgrade Project (Initiated in 2008)

Mission

- Provide enhanced security measures into DCS
- Help facilitate DCS customers to comply with standards (NERC, DHS, etc.)

Primary Goals

- Add anti-spyware to anti-virus software
- Add configurable host-based firewall
- Add control of hardware ports
- Add control of removable media
- Ability to centrally manage all of above
- Ability to expand into other products (e.g. Application White-listing, NAC)



The Solution:



McAfee's Endpoint Security Solutions

McAfee's Energy System Security Solution (ES³)



Currently deployed in InvenSYS DCS

Future deployment in InvenSYS DCS

Most comprehensive security platform for DCS environments

- Controls endpoints against most complex, targeted, zero-day malware
- Massive scalability & interoperability to support complex DCS operating environments

Trusted solution of the US Department of Defense

- Protection for over 5 million endpoints of the Army, Air Force, Navy, Marine Corps and US Intelligence communities

Single, integrated management for diverse environments

- Controls endpoints (Windows, Linux and Mac), mobile phones, virtual machines, storage, legacy OS's, embedded systems and servers with common policies under a single management console

Capabilities

Modules

• Security

- Signature protection
- Behavioral protection
- Firewall
- Application White-listing
- File Integrity Monitoring
- External device protection



- Host Intrusion Prevention Software (HIPS)
- Application Control
- Change Control
- Anti-Virus / Anti-Spyware
- Device Control Module (DCM)

• Auditing

- Host compliance check
- Rogue system identification
- Network admission control



- Policy Auditor (PA)
- Rogue System Detection Module (RSD)
- Network Access Control

• Reporting

- Centralized agent, console security management
- Event propagation/correlation



- ePolicy Orchestrator

Invensys I/A Series System Architecture

I/A Series System Architecture

Intra-Enterprise Level

- Plant Intelligence**
- Plant Asset Management
 - Simulation/ Modeling
 - Enterprise Historian
 - Plant Information Portal
 - Batch Management



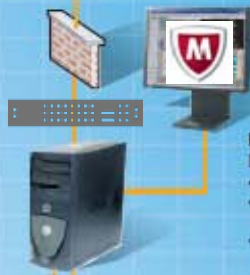
Secure Control Information Network



- Operator Environment**
- Visualization
 - Alarm/Alert Management
 - Historian
 - Real-time Performance Management



- Engineering Environment**
- System Configuration
 - Control Strategy Development
 - Display Configuration
 - Field Device Management
 - Advanced Control
 - Batch Execution



- Maintenance Environment**
- Asset Management
 - Alarm Analysis & Optimization
 - Condition Monitoring & Diagnostics



Wireless Handheld

Fault-Tolerant 1-gb Mesh Control Network

- Intelligent Field Integration**
- Fieldbus I/O
 - Remote I/O
 - Conventional I/O
 - Safety Systems
 - PLC



Remote Field Network



Safety System



Existing I/A Series Installation



Legacy System Migration

- Bailey
- Fisher
- Honeywell
- Moore
- Spectrum
- SPEC200
- Westinghouse

Layered Approach to System Security

Application	Core Functionality	Protection Profile
Application White-Listing	Dynamic Whitelisting, Memory Protection, Image Comparison	<ul style="list-style-type: none"> • Highest protection for low change / low overhead environments • Prevents unauthorized or accidental system changes • Protects against zero day vulnerabilities / targeted threats
Host Intrusion Prevention	Host Signature/Behavior Protection/Stateful Firewall	<ul style="list-style-type: none"> • Controls traffic flows • Prevents remote attacks and data/application outflows • Protects against zero day vulnerabilities • Shields trusted applications
Network Intrusion Prevention	Network Signature/Behavior Protection	<ul style="list-style-type: none"> • Distributed Denial of Service protection • Protects networks without agents • Detects/prevents anomalous network traffic • Protects against zero day vulnerabilities
Anti-Virus	Blacklisting	<ul style="list-style-type: none"> • Cleans and kills malware before it installs • Requires regular updating

Host Intrusion Prevention

Prevention of exploits results in less patch cycles

invenys

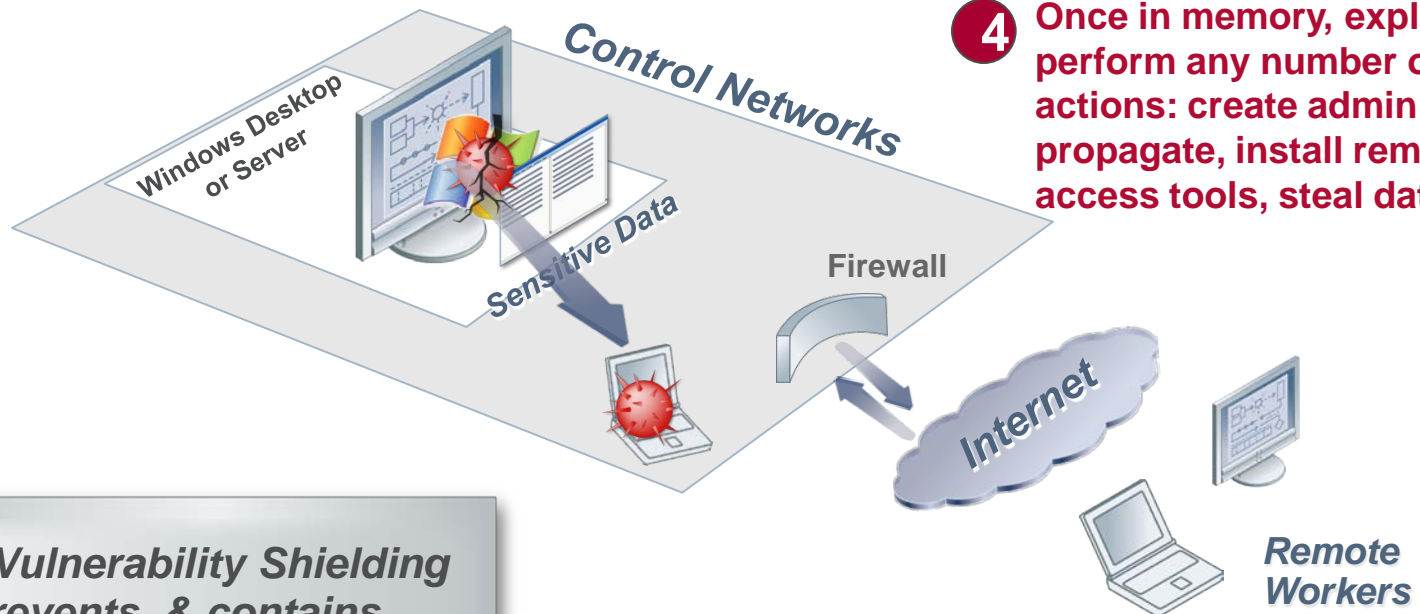


1 Exploit is written to take advantage of application vulnerability

2 Exploit overflows buffer

3 ...and writes code to memory

4 Once in memory, exploit can perform any number of actions: create admin users, propagate, install remote access tools, steal data...



Host IPS Vulnerability Shielding blocks, prevents, & contains exploits

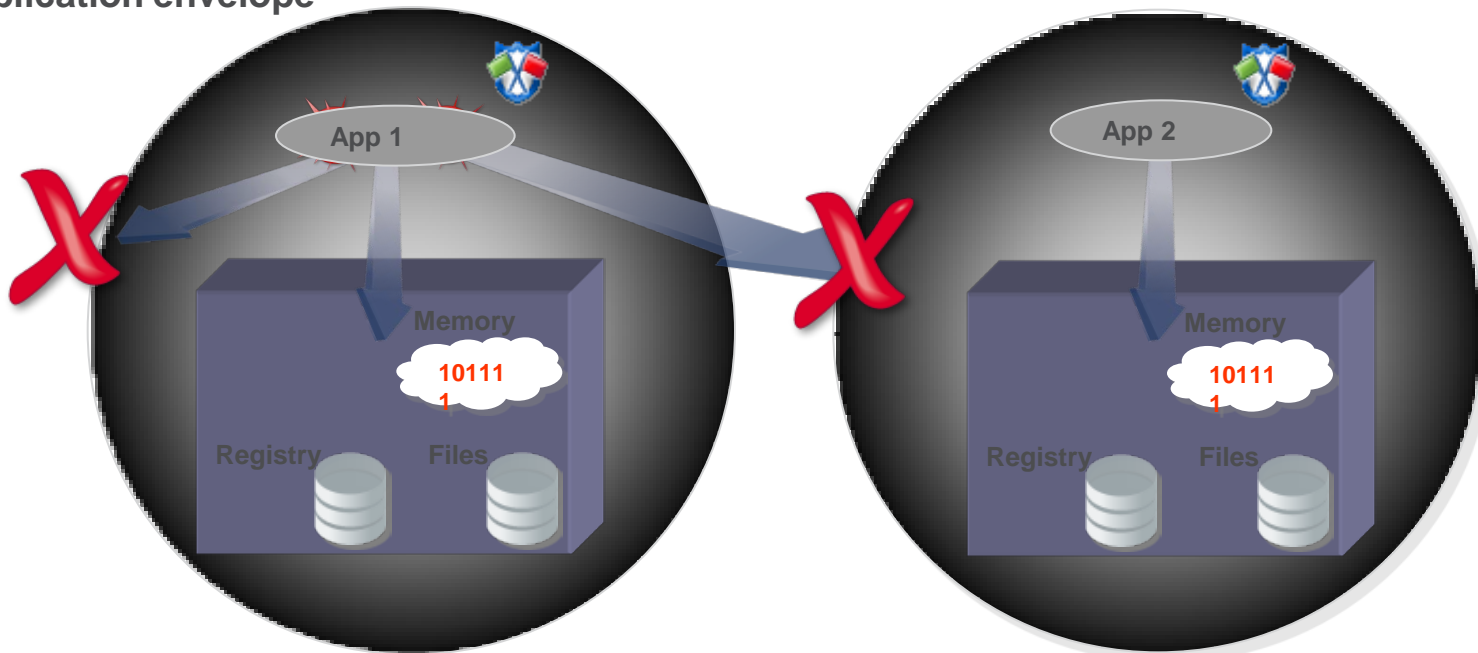
Host Intrusion Prevention

Application Shielding & Enveloping

1 Applications are allowed to access their own files, data, registry and services

3 Enveloping – Applications are not permitted to access data, registry and services outside their own application envelope

2 Shielding - Applications, registry and services are locked down against malicious activity



Host Intrusion Prevention

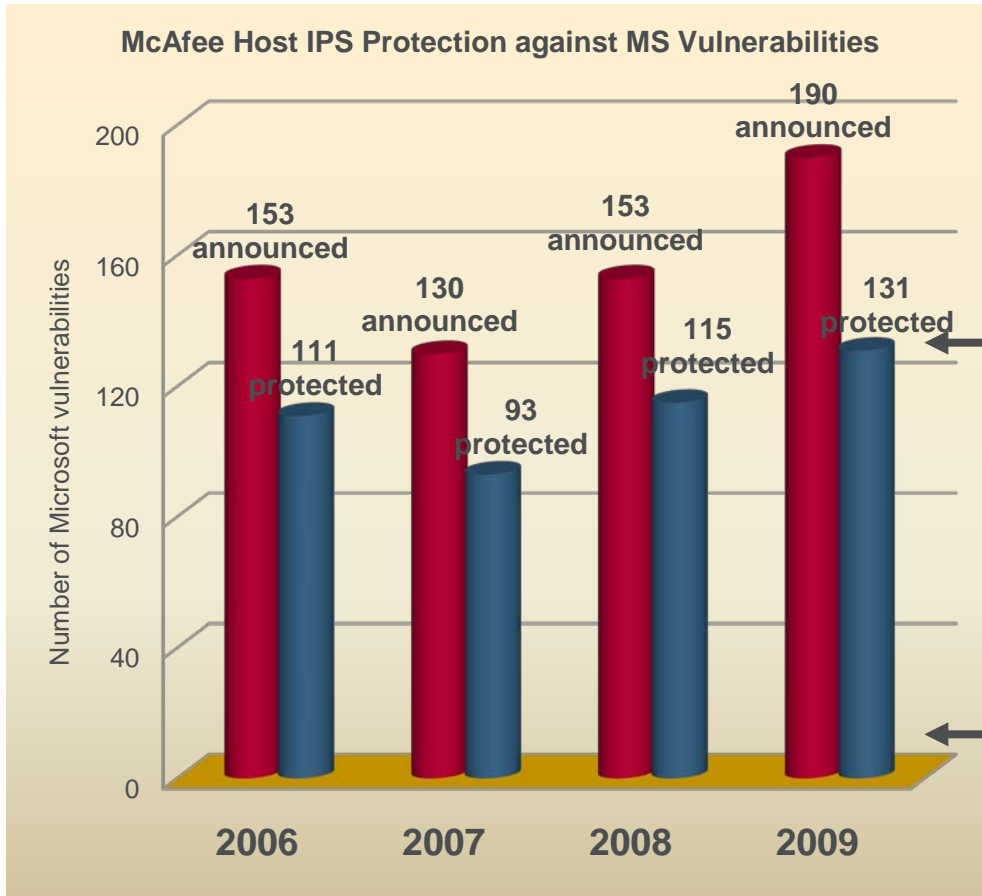
Adaptive Policy Tuning

- Define what traffic should be allowed
- Select a default policy type as template – modify with your rules
- Assign policy in Adaptive Mode to representative end nodes to tune
 - Exceptions created automatically
 - Exceptions reported to ePO as Client Rules
- Refine policy



Host Intrusion Prevention

Patch Planning vs. Reacting to "Patch Tuesday"



McAfee Host IPS: 90% zero-day protection out-of-the-box on "Black Tuesday"

Vulnerability Gap

...while classic **antivirus** protection alone is **not enough**

*Average

Application Change Control

Maximizing Business Reliability for Mission-Critical Systems

invenys



RUN-TIME CODE AUTHORIZATION

- Only authorized code can run
- Every code load/launch event gated by software inventory check
- Covers all types of software on protected systems: binary, script, ...

AUTHORIZED CODE PROTECTION

- Authorized code files are protected from change, deletion, tampering
- Extensible to configuration data or any other files you wish to protect

PROCESS PROTECTION

- Running code is protected run-time tampering, insertion, hijacking

FILE READ/WRITE and COPY PROTECTION

- Protect sensitive data files from being viewed, altered or copied



Application Change Control

Change Management Trust Model

Authorized Change Processes



Production Mode



Hardened Production environment



Scheduled Update Windows



Update Windows defined via Authorized Administrators



Authorized Updaters
(Tivoli, SMS, SW Agents, etc)



Secure, signed updates



Users as updaters



Production Mode

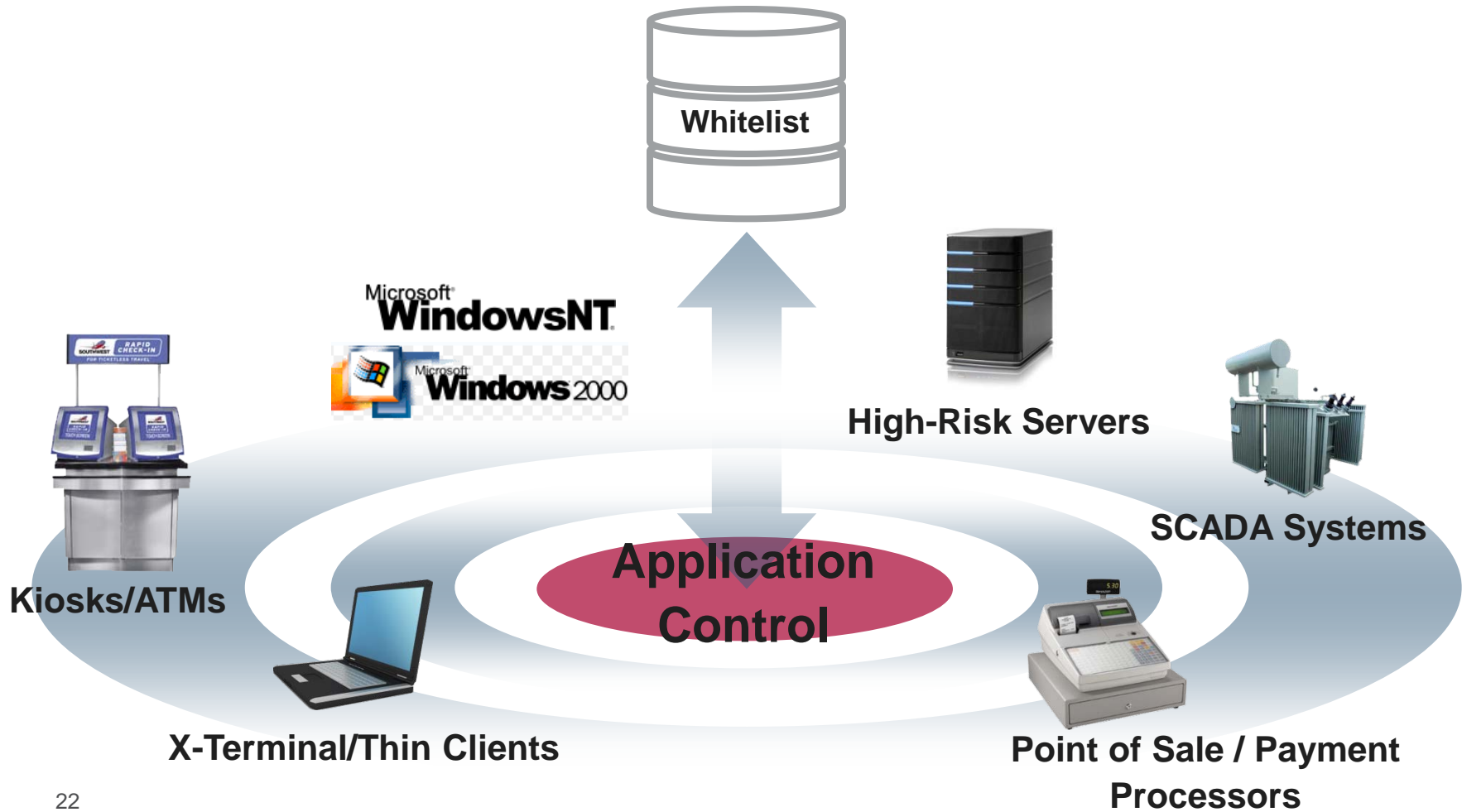


Hardened Production environment

Application Change Control

Extending Coverage to Broader Platforms

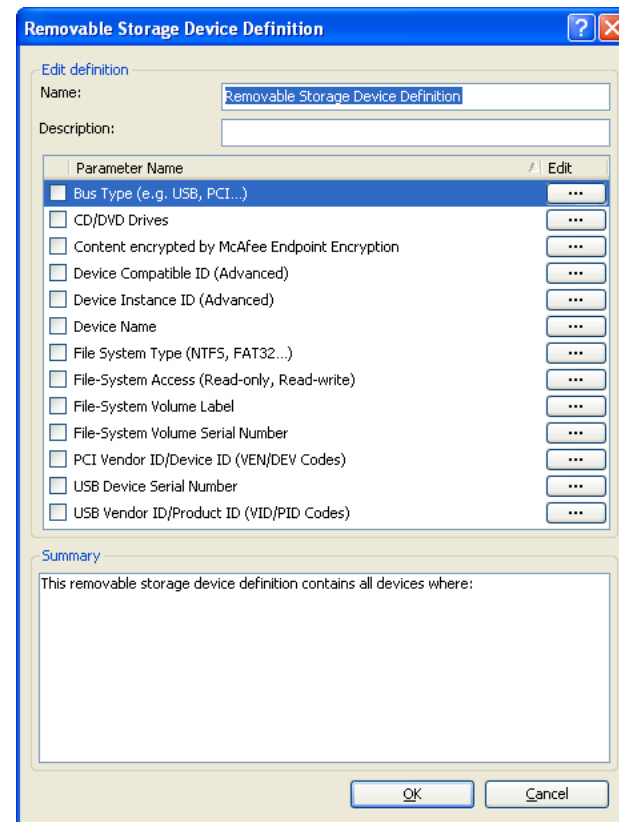
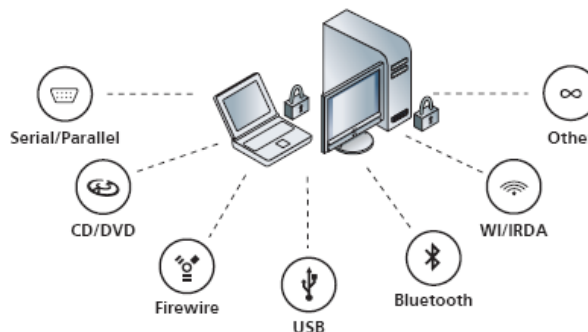
inven5ys



Device Control

Prevent Unauthorized Use of Removable Devices

- Device level management for
 - Removable storage device
 - Plug-and-play devices
- Flexible device definition
 - e.g. by Vendor/Product ID to restrict usage for specific devices only
 - e.g. by Serial Number to restrict to authorized device list only
- Reactions
 - Block
 - Monitor Usage
 - Notify User
 - Read Only



Centralized Security Management

Extending Coverage to Broader Platforms

invenys

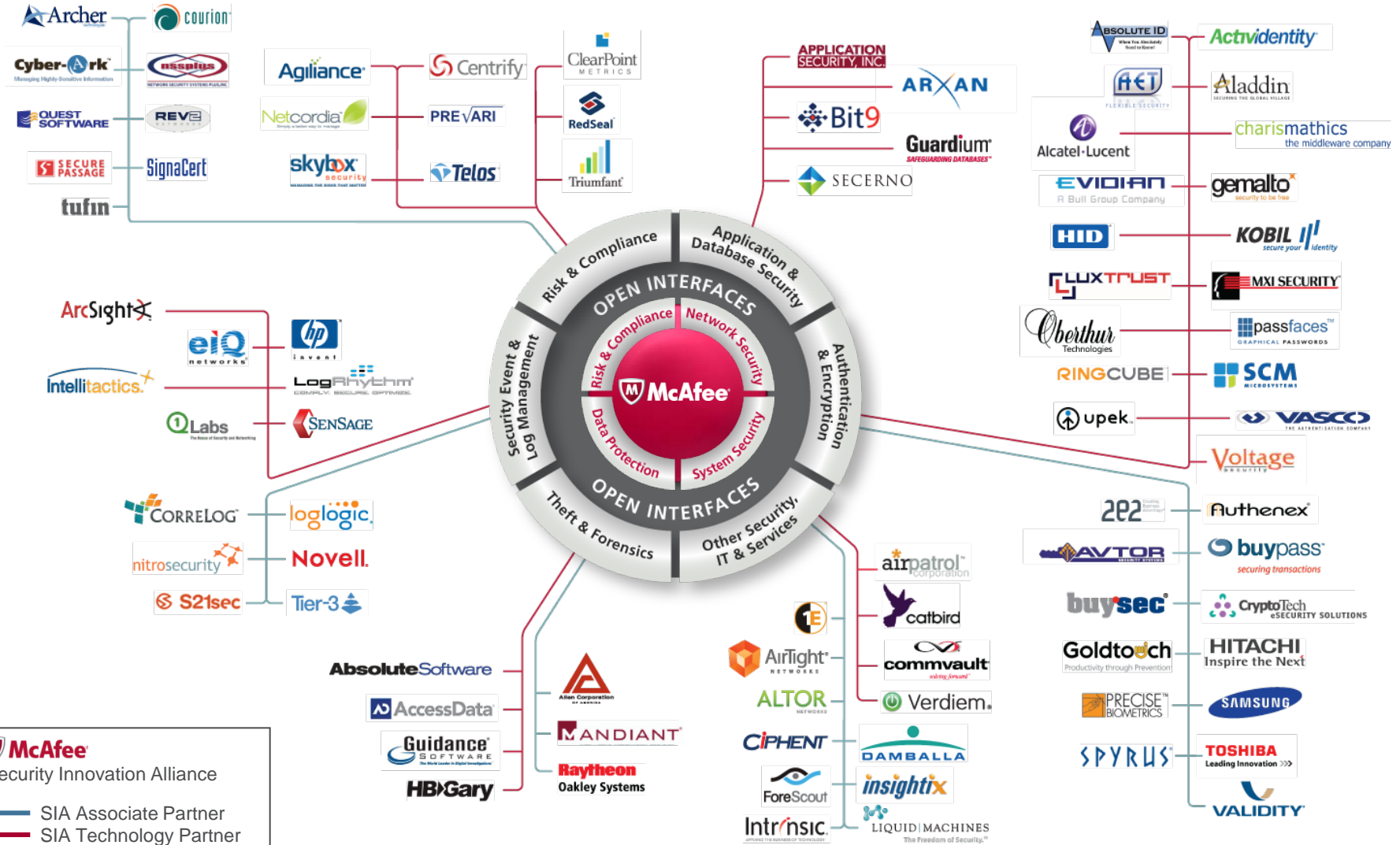


Single Integrated Management Console

- Single agent, single console
- Ease agent deployment and administration
- Manages all endpoint solutions
- Flexible reporting – from one-page executive security summaries to detailed information
- Open Architecture
- Lower operational costs with improved visibility and efficiency

McAfee's Platform for Security Innovation

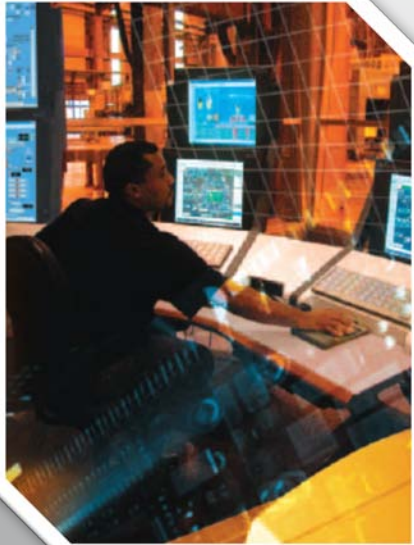
Industry Leadership to Drive Better Protection, Greater Compliance and Lower TCO



Invensys: Lessons Learned

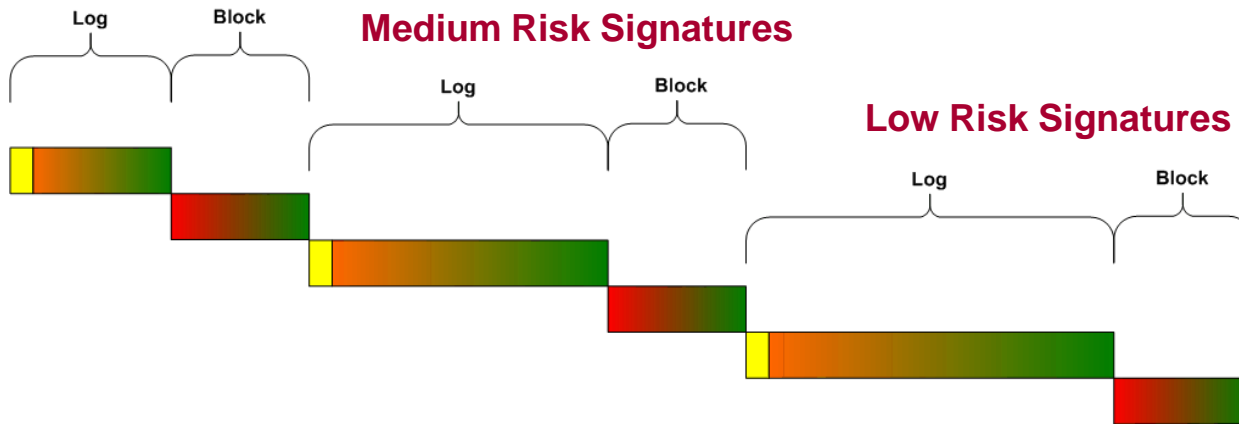
Lessons Learned

- **There was a lot to learn!**
 - Powerful feature set + flexible configuration leads to learning curve
- **How to make it easy for customers**
 - Taking products designed for IT experts and putting them in the hands of process control system personnel
 - Need to education technical support people as well as customers
- **Adequate time for testing/tuning**
 - Many combinations of software and hardware configurations
 - Many policies, rules, settings to test
 - Many test cases to write and execute
 - Having sufficient time and resources to test
- **Making the correct trade-off decisions**







Path to Prevention – Three phases to Implementation

High Risk Signatures



Medium Risk Signatures

Low Risk Signatures

- | | | |
|---|---------------------|---|
|  | Notification Period | Alert users to exercise critical Applications |
|  | Monitor Period | Monitor logs, Fix (legitimate), Remove (illegitimate) Applications, Create Exceptions |
|  | Acceptance Period | High degree of confidence in outcome of preceding period |
|  | High Alert Period | Be on alert for blocked Applications |

Prevention is an evolutionary process... its build upon TRUST

An IPS must be a highly accurate IDS first!

Invensys : Trade-Off Analysis

Tradeoffs #1 – Balancing business needs and security needs

- “I need security.”
- “I don’t want security.”
- “I want security but don’t want to pay for it.”
- “I need a rich feature set. I want to be able to....”
- “Keep it simple. I don’t want it to get in my way.”
- Must maximize profit and productivity
- Must protect DCS from attacks

Tradeoffs #2 – Finding the optimal security policy

- Balancing act to optimize policies and rules
- Example:
 - “If you tighten the firewall too much, you could break an application at a critical time”
 - “If you loosen the firewall rules too much, your environment could be penetrated by an adversary”
- Question: Which one would you prefer to be called to the corner office for?



Invensys : Results & Next Steps

Results

- Provide customers with a robust, complete set of security tools
- Provide an easy installation experience make security more palatable
- Provide basic default best practices as a jump start
- But, let the customer make the trade-offs appropriate for their site
- Provide a scalable, modular infrastructure so that tools can be updated/added over time
- Expect to be continually enhancing security based on the evolving threat landscape (you are never done)

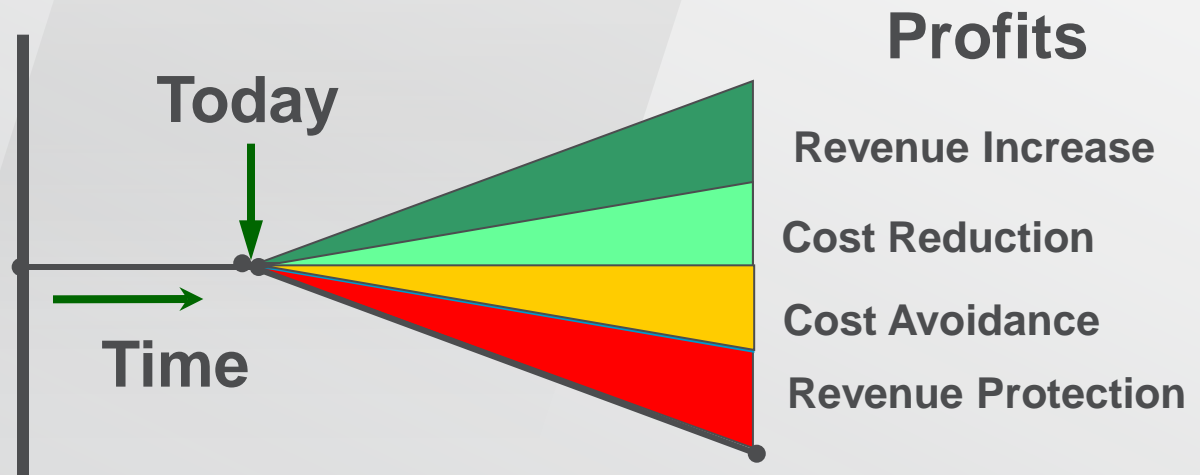


Invensys : Key Financial Benefits

Maintaining Data and the value it brings...



- Maintaining profits...are as important as Increasing profits
- A stronger Cyber Security program for Control systems enable...



Invensys : Key Financial Benefits

Maintaining Data and the value it brings...

Enable process improvements to reduce process costs

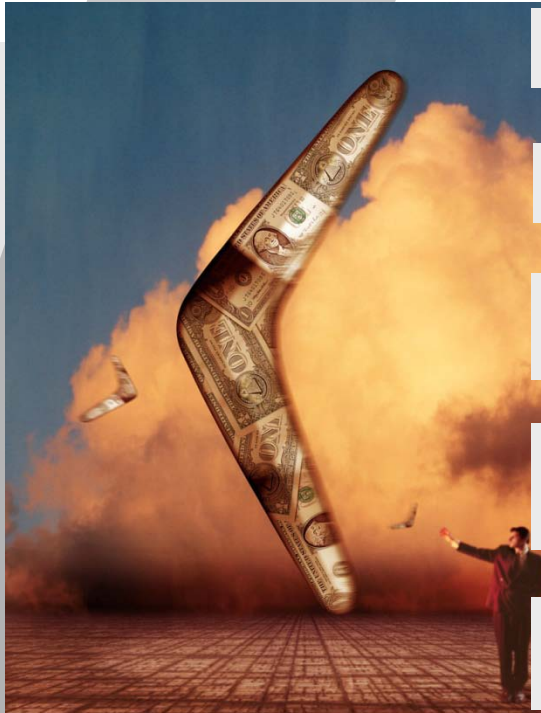
Enable process improvements to increase production

Increased administration capacity by streamlining the security workload

Avoid current and increased costs of regulatory compliance and non-compliance

Protect production from the impact of increasing security intrusions

Protect the plant from a catastrophic event caused by a security intrusion



invenSys

+



McAfee[®]

**Next Generation Security for
Distributed Control Systems**