From: "Rich Cummings" <rich@hbgary.com>
To: "'Aaron Barr'" <aaron@hbgary.com>; "'Ted Vera'" <ted@hbgary.com>; "'Greg Hoglund'" <greg@hbgary.com>
Sent: Saturday, January 30, 2010 12:33 PM
Attach: HBGary SEAL v5.pptx
Subject: FW: Con Call with McAfee SE Team

Guys,

This is the presentation I'm giving to 120 McAfee sales engineers on Monday about our DDNA integration. Even if 25% of them get it we now have 40 more technical people pitching DDNA. This is how REAL companies scale out. Grrrrrrr!

Have a good weekend.

Rich

-----Original Message-----
From: Namit_Arora@McAfee.com [mailto:Namit_Arora@McAfee.com]
Sent: Friday, January 29, 2010 9:25 PM
To: rich@hbgary.com; John_Klassen@McAfee.com
Cc: Eric_Renner@McAfee.com; penny@hbgary.com
Subject: RE: Con Call with McAfee SE Team

Rick, here is the final ... I just added titles on two slides (with screenshots). Thanks, and I look forward to your presentation on Monday!

Namit Arora
Sr. Manager, Marketing, SIA
McAfee, Inc.
Direct: +1.408.346.5208

-----Original Message-----
From: Rich Cummings [mailto:rich@hbgary.com]
Sent: Thursday, January 28, 2010 10:10 PM
To: Klassen, John
Cc: Renner, Eric; Arora, Namit; penny@hbgary.com
Subject: RE: Con Call with McAfee SE Team

John,

Thank you very much for the feedback I really think it's come together well! I've added in your 3 slides and thanks for doing the work there too. Here is the latest version attached.

I will go through this again tomorrow morning and let you all know if I've made any edits. I believe I'll be able to do the current presentation in the allotted 20 minutes without any problems as I have only a couple key points to touch on per slide.

Feel free to send me any more suggestions or improvements.

We're fired up to work with you all!

Best,
Rich

-----Original Message-----
From: John_Klassen@McAfee.com [mailto:John_Klassen@McAfee.com]
Sent: Friday, January 29, 2010 12:21 AM
To: rich@hbgary.com
Cc: Eric_Renner@McAfee.com; Namit_Arora@McAfee.com; penny@hbgary.com
Subject: RE: Con Call with McAfee SE Team

Rich,

This is a really good presentation, really hits the mark for what SEs need to know!

Suggestions:

Slide 4 - the build isn't quite right, the ovals appear to early. I fixed it in the attached PPT.

Slide 10 - I *LOVE* the side-by-side comparison. In the table, let's change "McAfee EPO" to "McAfee Total Protection for Endpoint" (ToPS Endpoint) because ePO is the management framework, not the security products that provide anti-malware protection (VirusScan Enterprise, HIPS, etc.). I adjusted the size as well.

Slide 15 - The Red for ePO Server box is not McAfee Red, too bright. Change "ePO Agents" to "McAfee Agents" to match the McAfee product naming (I know, it's not clear why ePO = ePO Server + McAfee Agent but that's the current standard). I made these changes in the attached PPT too so you could see what I mean.

Otherwise only praise, especially for the "on disk" vs. "in memory image" slides -- brilliant!

-jkk

John Klassen
Technology Director, Security Innovation Alliance McAfee, Inc.
Mobile: 510.290.8900

-----Original Message-----
From: Rich Cummings [mailto:rich@hbgary.com]
Sent: Thursday, January 28, 2010 6:47 PM
To: Arora, Namit; penny@hbgary.com
Cc: Renner, Eric; Klassen, John
Subject: RE: Con Call with McAfee SE Team

Thank you Namit,

I really like what you've done, it looks really good on your background. Great suggestions as well, I've made most of the changes you recommended I believe. I will take another quick look in the morning and send it over if I make any edits.

Penny please review and let me know your thoughts.

Thanks again,
Rich

-----Original Message-----
From: Namit_Arora@McAfee.com [mailto:Namit_Arora@McAfee.com]
Sent: Thursday, January 28, 2010 6:39 PM
To: rich@hbgary.com; penny@hbgary.com
Cc: Eric_Renner@McAfee.com; John_Klassen@McAfee.com
Subject: RE: Con Call with McAfee SE Team

Thanks Rich,

The slides look good. I apologize for not mentioning that this needs to be in the McAfee template. So I went ahead and transferred the contents - see attached deck. Please review it to make sure there are no formatting glitches. After this call, we'll use it as the primary HBGary presentation in the Sales Resource Center for use by our Reps/SEs in customer environments.

Here are some changes I made: combined slides 4 and 5 in your deck, replaced the ecosystem diagram. I also added slide #23.

What would be nice is a statement of the customer problem you have set out to solve. This could go on slide #3. It would be good to have titles for slides #12-#15, a descriptor for what we are looking at. Really like slide #10. Please add contact details on slide #23.

Also, would it be possible to recast slide #22 summary as customer benefits of the integration, rather than only technical capabilities of Digital DNA? The SEs would want to take away a couple of key nuggets on why they should care, when they should think of you, etc.

It may be challenging to cover 23 slides and also take questions in 20 minutes but I'll leave it to you whether you want to shorten the presentation a bit. That's all I have. John is reviewing this as well and might have some suggestions.

Thanks,

Namit Arora
Sr. Manager, Marketing, SIA
McAfee, Inc.
Direct: +1.408.346.5208

-----Original Message-----
From: Rich Cummings [mailto:rich@hbgary.com]
Sent: Thursday, January 28, 2010 12:38 PM
To: Arora, Namit; penny@hbgary.com
Cc: Renner, Eric
Subject: RE: Con Call with McAfee SE Team

Hi Namit,

Please find attached my draft of the presentation for Monday. I'll give you a call in a couple minutes to see if we can chat. If I don't reach you please feel free to call me on my cell (703-999-5012) anytime until we get this finalized to everyone's satisfaction.

We're really look forward to the Sales Engineering call on Monday and winning some business together.

Best,
Rich

Rich Cummings | CTO | HBGary, Inc.
Office 301-652-8885 x112
Cell Phone 703-999-5012
Website: www.hbgary.com |email: rich@hbgary.com

-----Original Message-----
From: Namit_Arora@McAfee.com [mailto:Namit_Arora@McAfee.com]
Sent: Tuesday, January 26, 2010 10:44 PM
To: rich@hbgary.com; penny@hbgary.com
Cc: Eric_Renner@McAfee.com
Subject: RE: Con Call with McAfee SE Team

Rich, checking in to see if you are on track to send me a draft presentation by tomorrow, Wed?

The SE call is from 1-2 PM PST on Monday. I'll forward the meeting invite later this week. Thanks.

Namit Arora
Sr. Manager, Marketing, SIA
McAfee, Inc.
Direct: +1.408.346.5208

-----Original Message-----
From: Arora, Namit
Sent: Wednesday, January 20, 2010 2:41 PM
To: Renner, Eric; Rich Cummings; 'Penny Leavy'
Subject: RE: Con Call with McAfee SE Team

Thanks, Eric.

Rich,
I'll be happy to help you develop a presentation for the SE call. Basically what we need is a deck with about 10-12 slides. It should provide an overview of HBGary and its products/solutions and then talk about our joint solution and its customer benefits. Screen shots that illustrate the joint integration tend to work really well. Since the audience here is SEs, it is Ok to be technical.

I'm not sure if the total time of 20 mins will allow a live demo but if you feel confident of finishing your entire presentation in 20 mins, go ahead.

Ideally you should get through the slides and the demo in a bit under 20 mins, leaving 3-4 mins for any Q&A.

Please send me a draft presentation by Tuesday next week (Jan 26th), which should give us time to review and request edits as appropriate. I'll send you call-in details later next week. This will be a LiveMeeting call and you will get presentation control. Over 80 North American SEs generally attend.

Let me know if you have any questions.

Namit Arora
Sr. Manager, Marketing, SIA
McAfee, Inc.
Direct: +1.408.346.5208

-----Original Message-----
From: Renner, Eric
Sent: Tuesday, January 19, 2010 1:07 PM
To: Rich Cummings; 'Penny Leavy'; Arora, Namit
Subject: RE: Con Call with McAfee SE Team

Penny, thank you for the introduction.

Hi Rich, great to meet you and looking forward to your participation on this McAfee SEAL Team Call with our SEs. Namit is lining this up, so he'll coordinate with you on all the details.

Thanks again,

Eric

Eric Renner
Director, Business Development - SIA
McAfee, Inc.
Direct: 408.346.5451

-----Original Message-----
From: Rich Cummings [mailto:rich@hbgary.com]
Sent: Tuesday, January 19, 2010 12:41 PM
To: 'Penny Leavy'; Renner, Eric; Arora, Namit
Subject: RE: Con Call with McAfee SE Team

Hi Eric and Namit,

I look forward to the call. Please feel free to call my cell anytime. The number is 703-999-5012.

Thanks,
Rich

Rich Cummings | CTO | HBGary, Inc.
Office 301-652-8885 x112
Cell Phone 703-999-5012

Website: www.hbgary.com |email: rich@hbgary.com

-----Original Message-----
From: Penny Leavy [mailto:penny@hbgary.com]
Sent: Tuesday, January 19, 2010 3:30 PM
To: Rich Cummings; eric_renner; namit_arora@mcafee.com
Subject: Con Call with McAfee SE Team

Rich,

Met Eric Renner. Eric is our POC for the ePO initiative. Today, we will be signing the sales agreement that allows HBGary and McAfee to jointly sell our DDNA for ePO solution. On 2/1/10 thre is a call with 80-120 SE's. They would like HBGary to participate. The call will be for 20 minutes and answer

WHo we are
Our Core Technology
Functional ePO integration
What Customers get with integration
Demo of product

The session will be recorded and archived for all of McAfee. Please work with Eric and Namit to schedule. Eric, Rich's phone is 703-999-5013 or he is at ext 112

--
Penny C. Leavy
HBGary, Inc.

HBGary-McAfee Integration

An Overview Presentation

Rich Cummings, CTO, HBGary

February 11, 2011

Agenda

- Who is HBGary –
- SIA Partnership – Theft and Forensics
- HBGary Digital DNA –
  - What is it?
  - How it works
  - How it complements McAfee End Point Protection
- Existing Customers
- Questions and Answers

HBGary Background

- Founded in 2003 by Greg Hoglund – Founder of Rootkit.com
  - First 4 years spent on
    - Government Services Contracts
    - Advanced Government Research Projects
  - 2007 – Commercial Products and Solutions focused
    - Responder Pro – Memory Forensics & Malware Analysis
    - Digital DNA – Enterprise Malware Detection System

R&D Funding

Air Force Research Labs

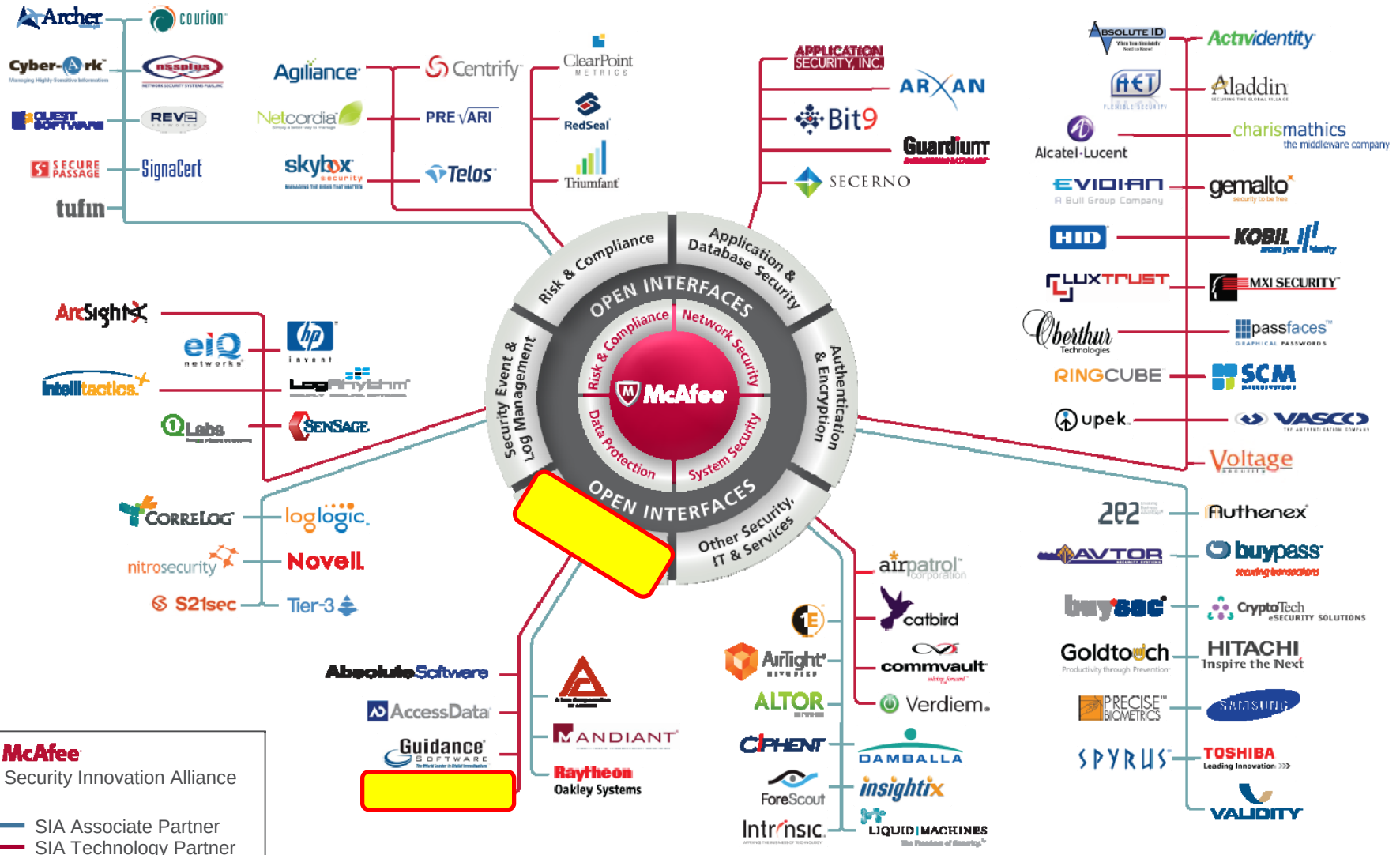
- Next Generation Software Reverse Engineering Tools
- Kernel Virtual Machine Host Analyzer
- Virtual Machine Debugger

Dept Homeland Security (HSARPA)

- Next Generation Botnet Detection and Mitigation
- H/W Assisted System Security Monitor
  - Subcontractor to AFCO Systems Development

Where HBGary Fits in the SIA Program

Incident Response & Forensics



McAfee
Security Innovation Alliance

- SIA Associate Partner
- SIA Technology Partner (McAfee Compatible)

Who is HBGary?

HBGary

HBGary specializes in developing advanced computer analysis products to detect, diagnose, and respond to advanced malware, targeted threats and other cybercrime activities. HBGary's flagship product, Digital DNA™, performs unparalleled detection coupled with Responder™ post-exploitation forensics with dynamic analysis of malware of live running software.

Through this partnership, Digital DNA™ is now integrated with ePO™ so that McAfee customers can deploy Digital DNA, scan physical memory for malicious and unauthorized code, and report results to McAfee ePO console for optimal corrective action. Read the solution brief for more details.

McAfee Compatible solution: HBGary Digital DNA 1.7 and McAfee ePO 4.0.

What is Digital DNA?

- **Digital DNA is:**
  - A Software and Malware Classification System
  - A Learning System - gets smarter over time
  - A programming language with logic used to create rules for Computer RAM
  - A system to identify all executable code in RAM and predict it's behaviors so analysts can quickly identify if a machine has unauthorized or unwanted executable code running on Windows Workstations and Servers.

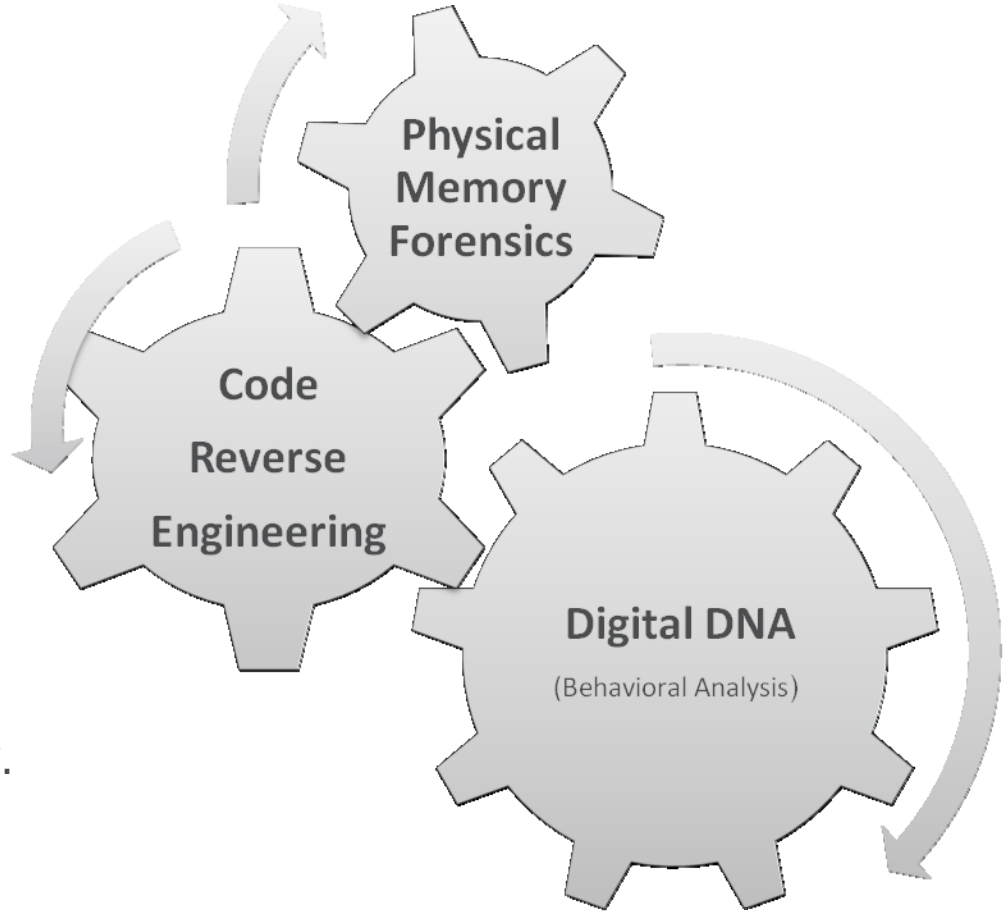
What is Digital DNA

A System designed to:

- Detect Zero Day or Unknown Malware - Passively
  - *Below the operating system – memory forensics*
  - *No protection or prevention or blocking - reactive*
- Detect Malware regardless of how it was packaged
  - *"MD5's are useless in memory at runtime"*
- Report Code Capabilities and Behaviors to the Analyst
  - *"Reverse Engineering for Dummies"*
  - *Programming techniques identified with clear descriptions*
- Easily Identify variants across the Enterprise
  - *Fuzzy Searching/Percentage of Match*

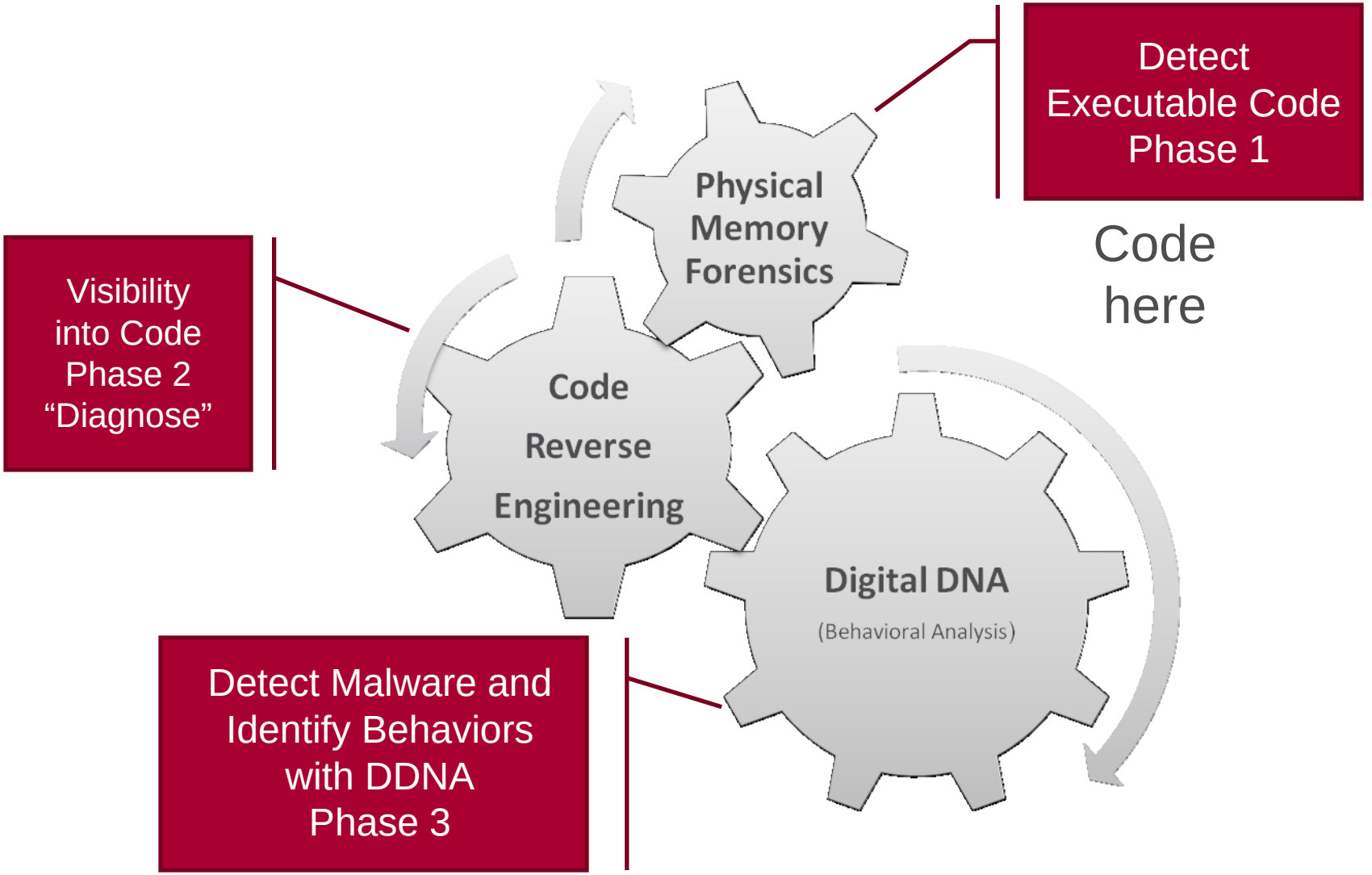
DDNA Core Technologies

GOALS: Gain the lowest level of diagnostic visibility in order to detect malware and malicious behaviors



To obtain our goals we combined the latest advances in Memory Forensics & Reverse Engineering technology. The result was Digital DNA.

How DDNA Works?



How DDNA Complements ePO

Malware Detection Techniques	McAfee Total Protection for Endpoint	HBGary DDNA
Active Protection for Malware	Yes	No
Scans Live Windows machines for malware in memory	Yes	No
Scan's Computer Hard disks and static files for malware	Yes	No
Prevents infection by USB/CDROM	Yes	No
Memory Forensics "Like Crash Dump Analysis" "Offline Analysis of RAM"	No	Yes
Rebuilds "Runtime" State of workstation and servers from a memory image snapshot or image	No	Yes
Automated Reverse Engineering with Responder Pro & REcon	No	Yes

What Digital DNA Looks Like

Ranking Software Modules by Threat Severity

Digital DNA Sequence	Module	Process	Severity	Weight
0B 8A C2 05 0F 51 03 0F 6...	iimo.sys	System		92.7
0B 8 02 21 3D 00 08 63	ipfltdrv.sys	System		13.0
	intelppm.sys	System		11.0
57 42 00 7E 1...	ks.sys	System		-10.0
1C FD 00 08 63	ipnat.sys	System		-13.0

0B 8A C2 05 0F 51 03 0F 64 27 27 7B ED 06 19 42 00 C2 02 21 3D 00 63 02 21

8A C2

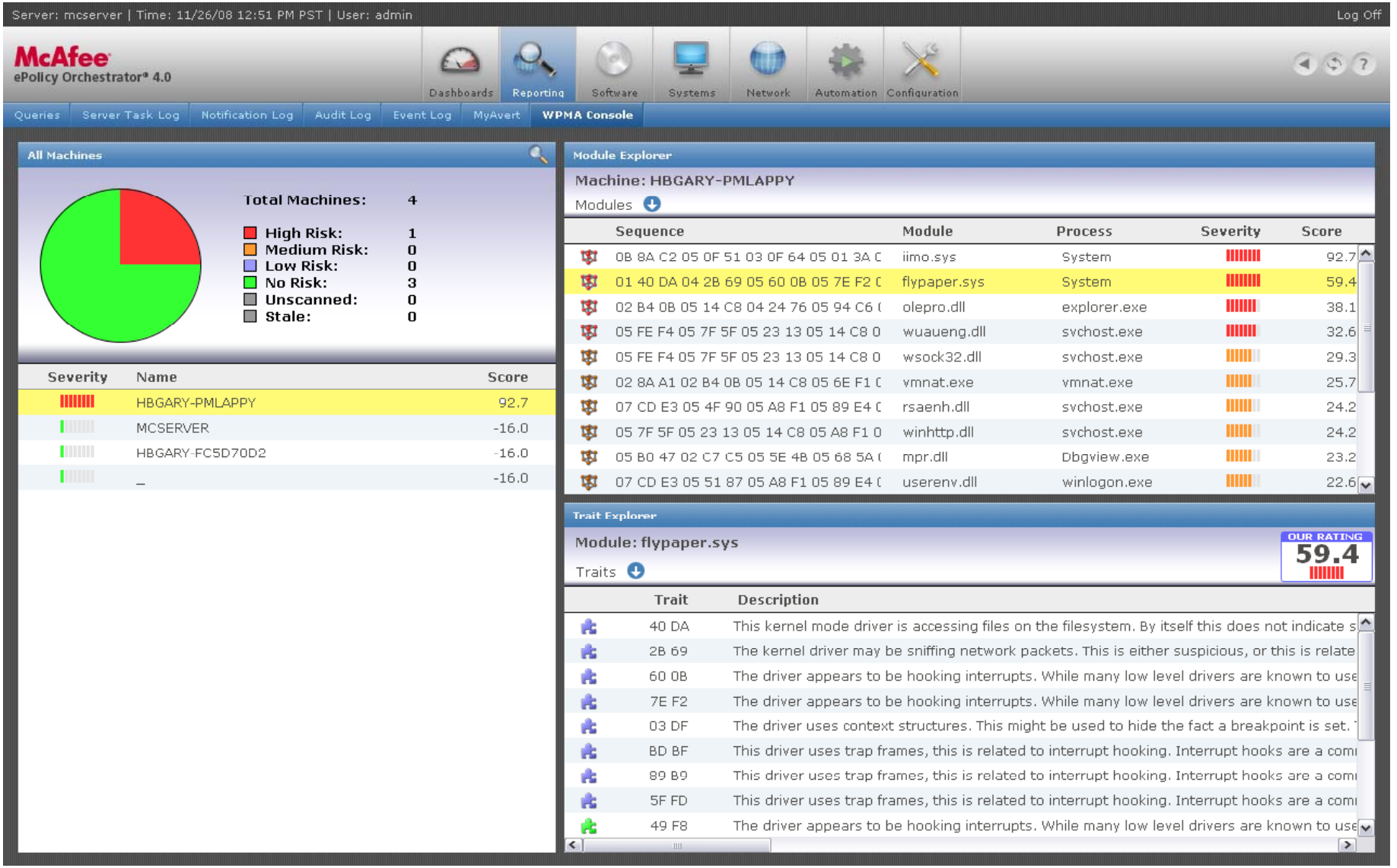
0F 51

0F 64

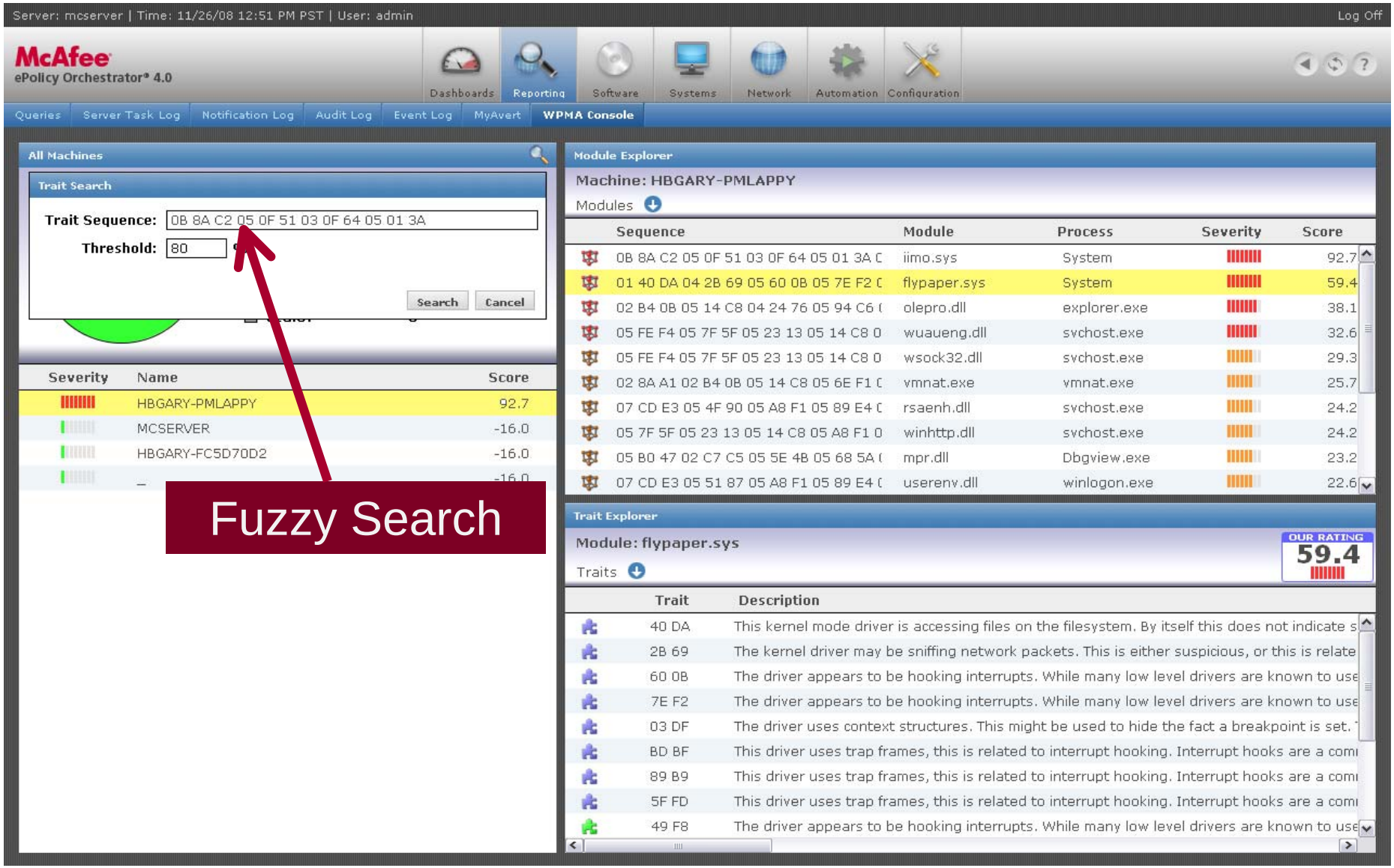
Trait	
Trait:	8A C2
Description:	The driver may be a rootkit or anti-rootkit tool. It should be examined in more detail.
Trait:	0F 51
Description:	There is a small indicator that detour patching could be supported by this software package. Detour patching is a known malware technique and is also used by some hacking programs and system utilities.
Trait:	0F 64
Description:	The driver has a potential hook point onto the windows TCP stack. This is common to desktop firewalls and also a known rootkit technique.

Software Behavioral Traits

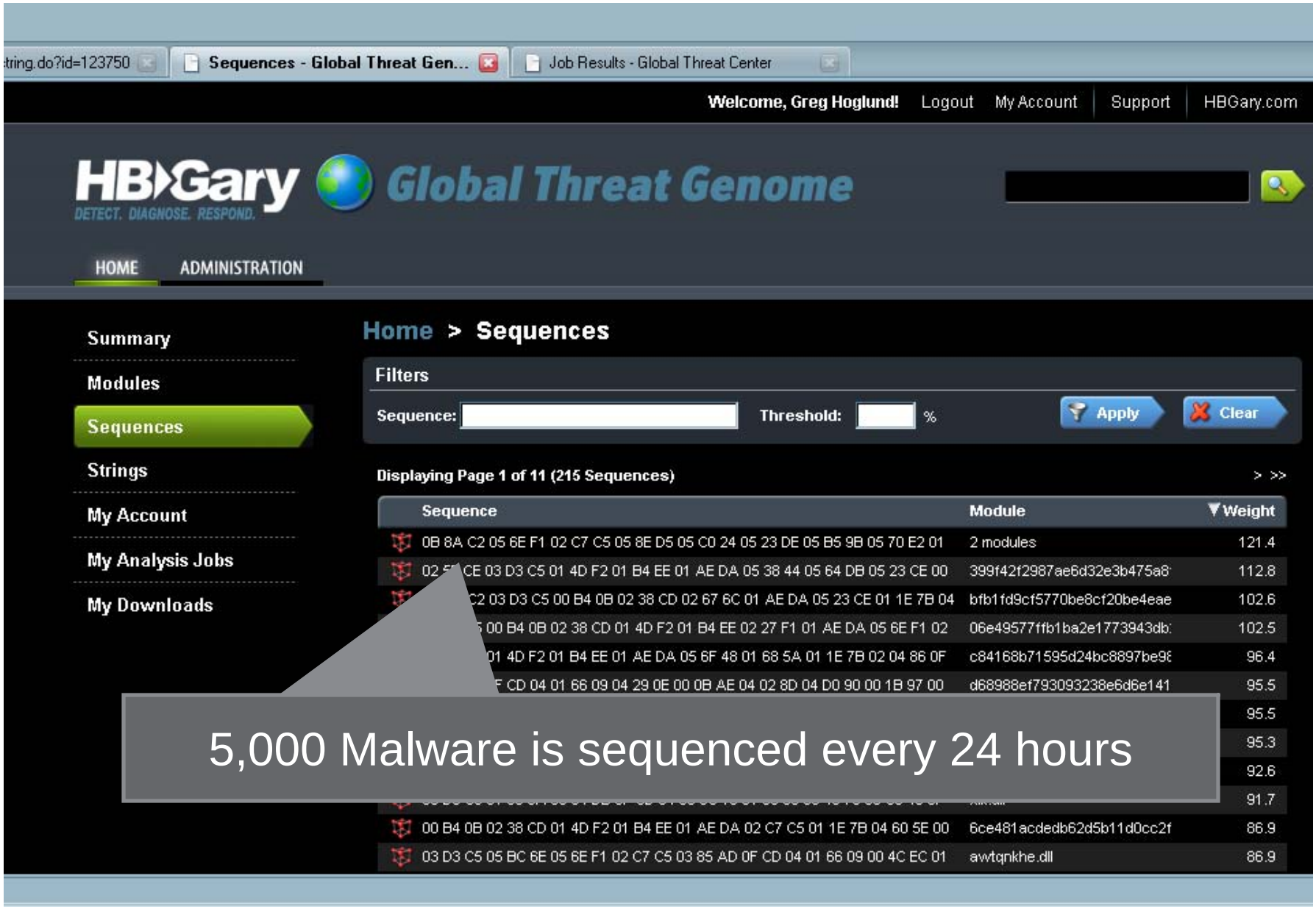
Digital DNA Threat Reporting in ePO



Digital DNA Threat Reporting in ePO



HBGary Portal – Risk Intelligence & Updates



Mapping The Malware Genome

Over 5,000 Traits are categorized into Factor, Group, and Subgroup.

This is our "Genome"

We expect to have 10,000 Traits by end of year

Malware Analysis Factors

Installation/ Deployment
Information Security
Defensive
Development
Communications

HBGary Malware Analysis Factors

Development Factors

- In what country was the malware created?
- Was it professionally developed?
- Are there multiple versions?
- Is there a platform involved?
- Is the a toolkit involved?
- Are there multiple parts developed by different groups or developers?

Command and Control Factors

- How is the malware controlled by its master?
- Do commands come from a cutout site?
- What commands are supported?
- Sniffing, logging, search file system, Attack
- Poison Pill - Self-destruct?

Defensive Factors

- Signs of packing or obfuscation
- AV Sabotage
- Does it have self-defense?
- Does it use rootkit techniques/stealth?
- Does it bypass the operating system?

Communication Factors

- Where does it connect to on the Internet?
- Drop points, Update Sites, C&C,
- IP addresses or DNS names
- incoming or outbound connections?
- Does it use encryption?
- Does it use Steganography?

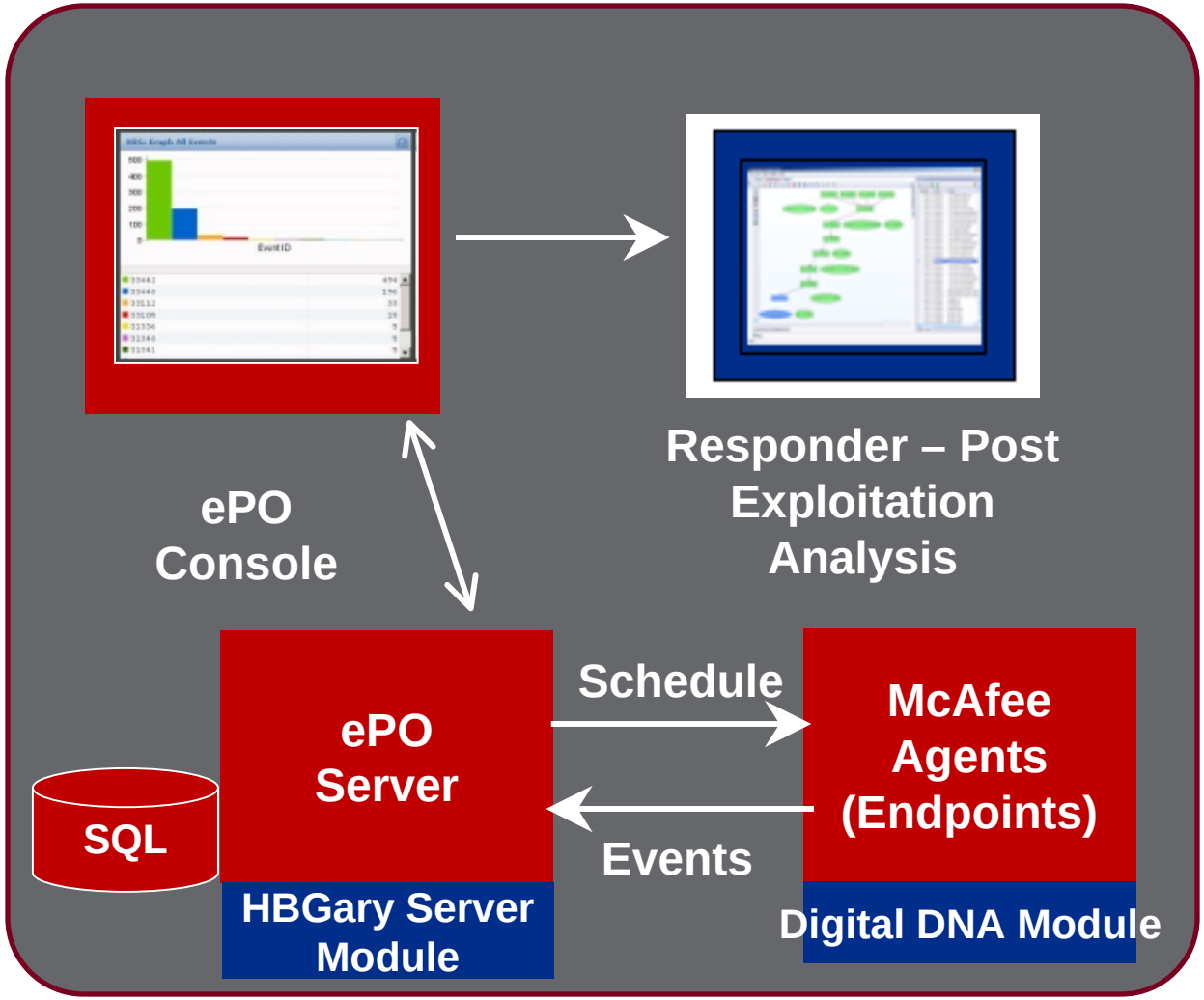
Installation and Deployment Factors

- Does it use the registry?
- Does it drop any files?
- Autorun.inf? USB? Open shares?
- Does it sleep and awaken later?
- JavaScript? Flash?
- Infection Point/Attack Vector

Information Security Factors

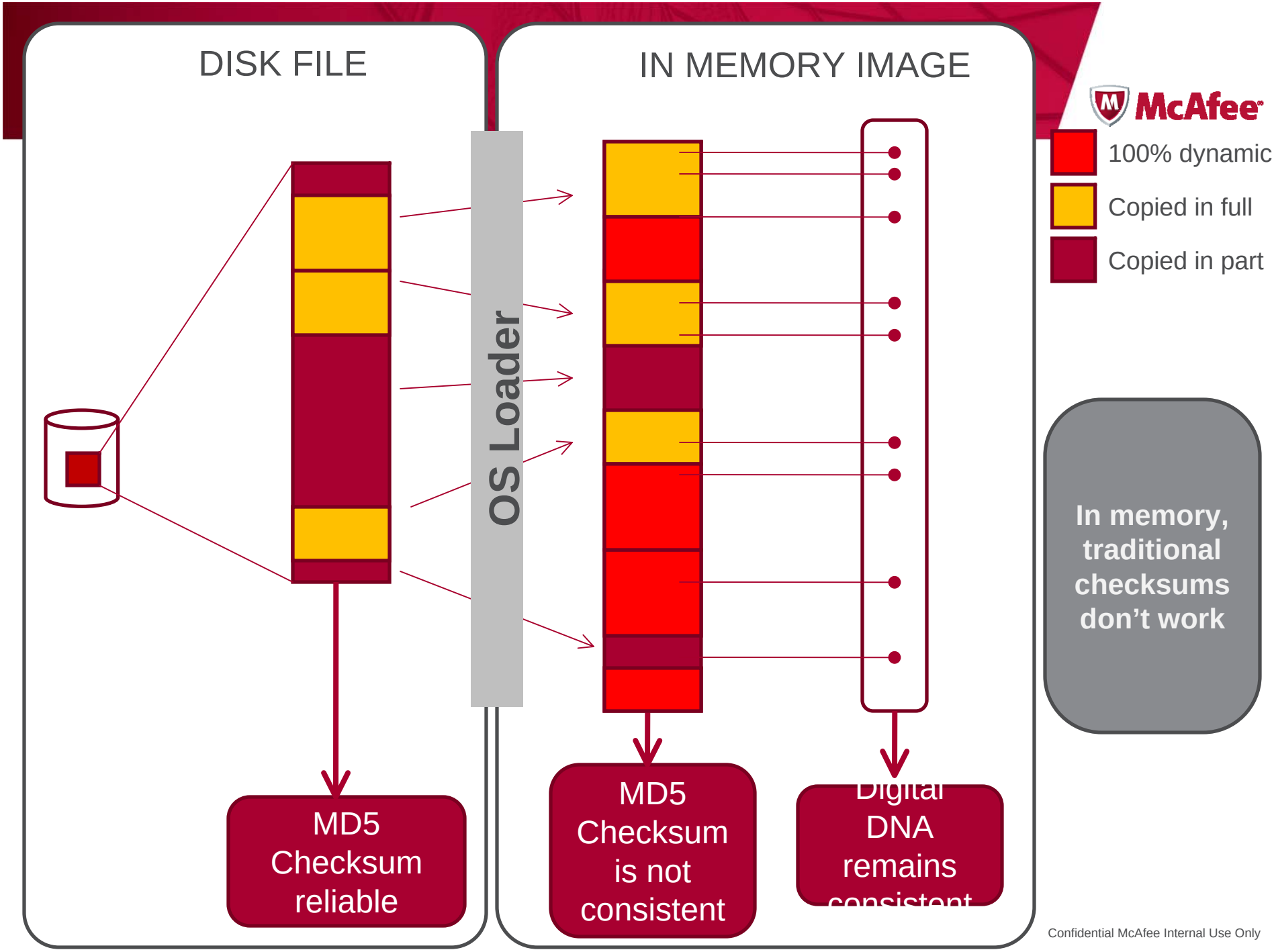
- Identify the risks associated with the binary
- What does it steal?
- Does it sniff keystrokes, passwords, 2 factor authentication tokens?
- Can it destroy data?
- Can it alter or inject data?
- Does it download additional tools?

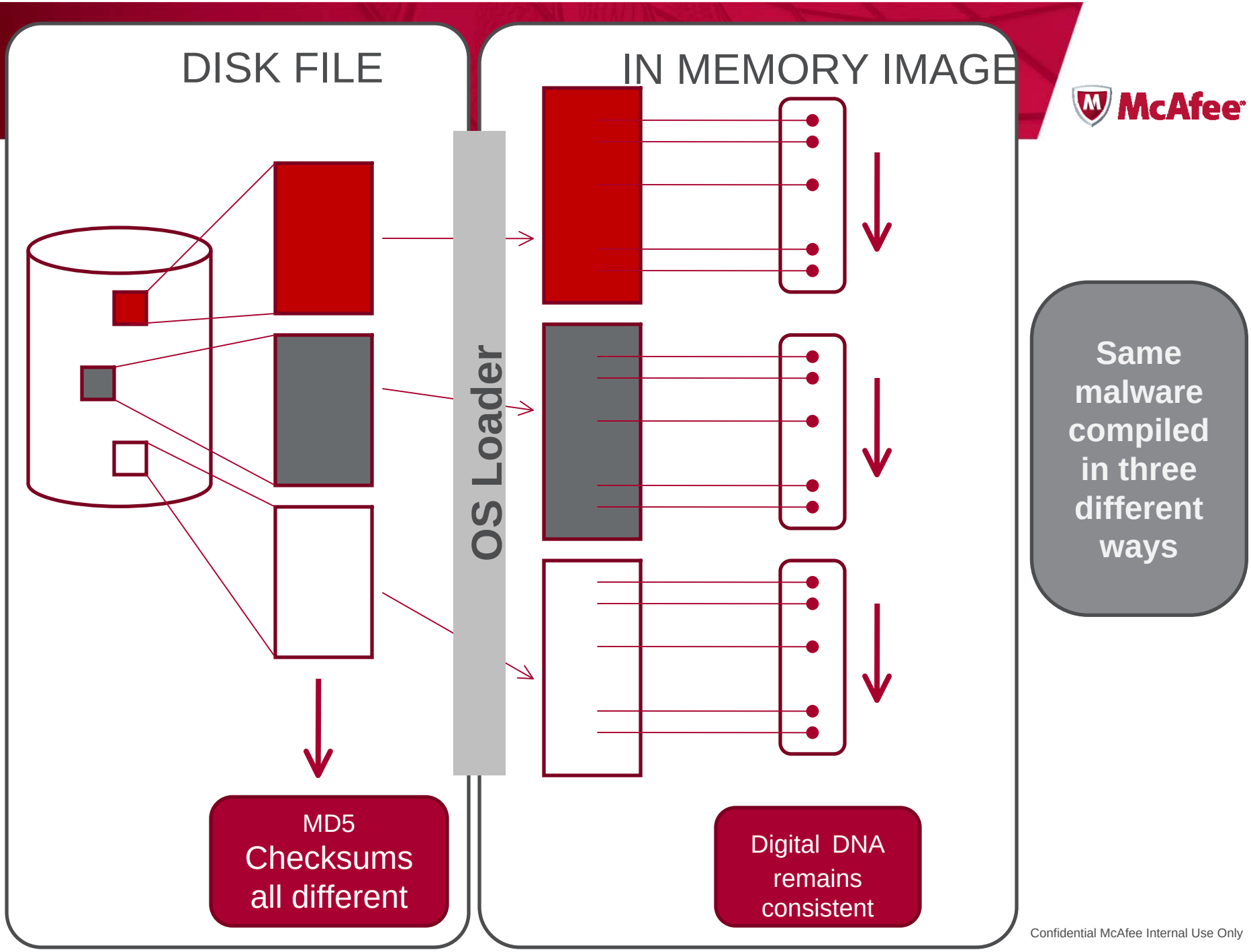
Easy Installation and Work Flow



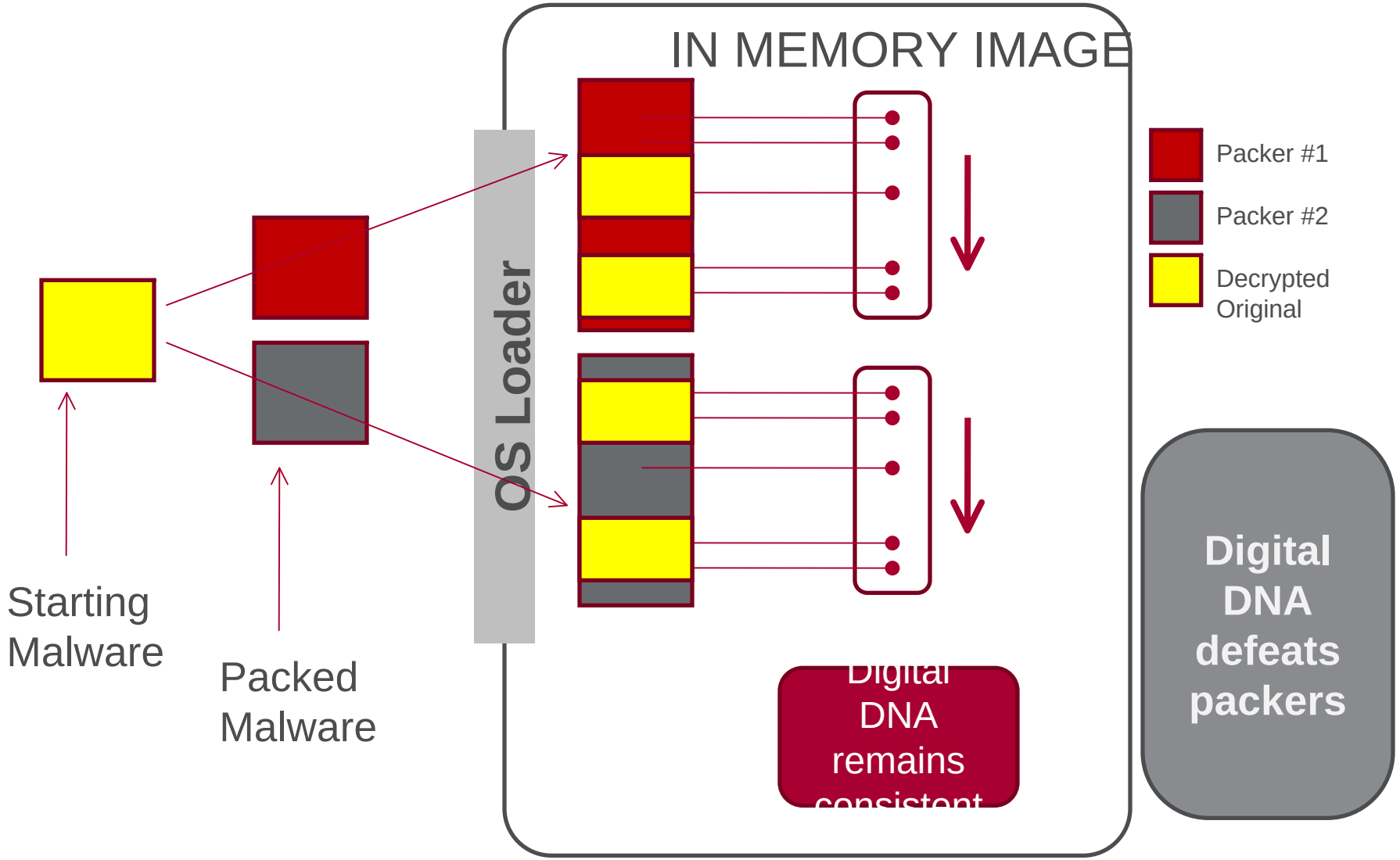
Why MD5's Don't Work in Memory

- In memory, once executing, a file is represented in a new way that cannot be easily be back referenced to a file checksum
- Digital DNA™ does not change, even if the underlying file does
  - Digital DNA is calculated from what the software DOES (it's behavior), not how it was compiled or packaged

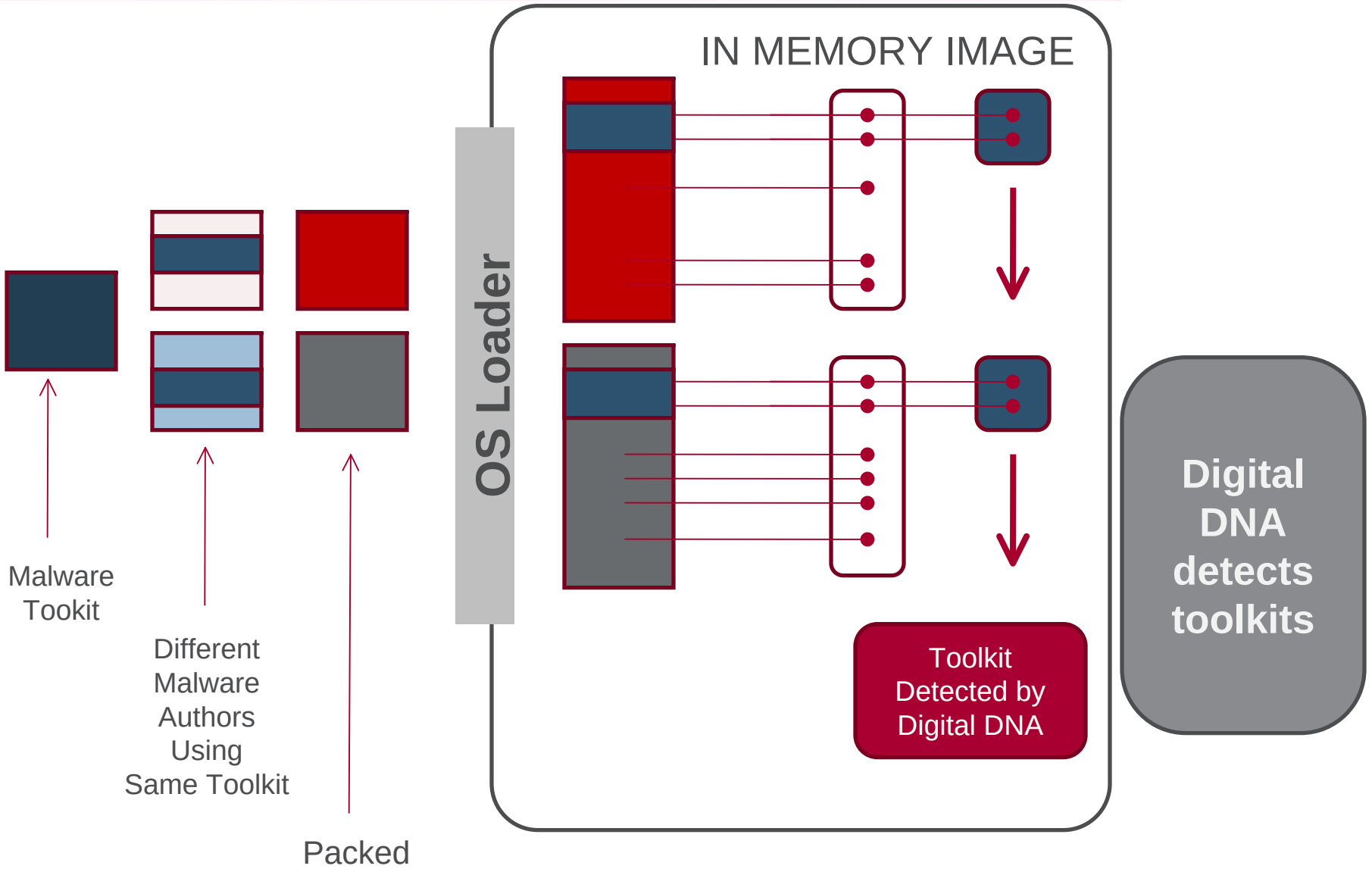




Digital DNA Defeats Packers



Digital DNA Detects Malware Toolkits



Customer Benefits of Integrated Solution

1. The McAfee ePO/HBGary Integrated solution provides organizations with a military grade Defense-In-Depth posture
   - Precision Strike Response with Unprecedented End-Point Visibility
2. Digital DNA detects the Advanced Persistent Threat (APT) hiding in Computer RAM
   - The Memory Forensics approach augments McAfee's proactive threat protection with law enforcement grade diagnostics for deep detection
   - Detected Malware can be sent to Avert Labs for Rapid Virus Signature creation
3. Rapidly Understand The Malware's Intentions and Capabilities
   - What is being stolen, Who it communicates with, How the malware installs itself, Command and Control Channels
4. Use this Risk Intelligence for enterprise policy changes and to identify scope of breach
   - IP Addresses, URL's are blocked at the IPS/Gateway
   - Registry keys and files are searched

Call to Action

- Visit the McAfee Sales Resource Center
  - Joint Solution Brief
  - Customer Presentation
  - Sales Teaming Guide (Coming soon)
  - Sales Teaming Cheat Sheet (Coming soon)

- Contact HBGary for detailed product information

  - Name: Rich Cummings
    - Tel: 301-652-8885 x112
    - Email: rich@hbgary.com

  - Website: www.HBGary.com

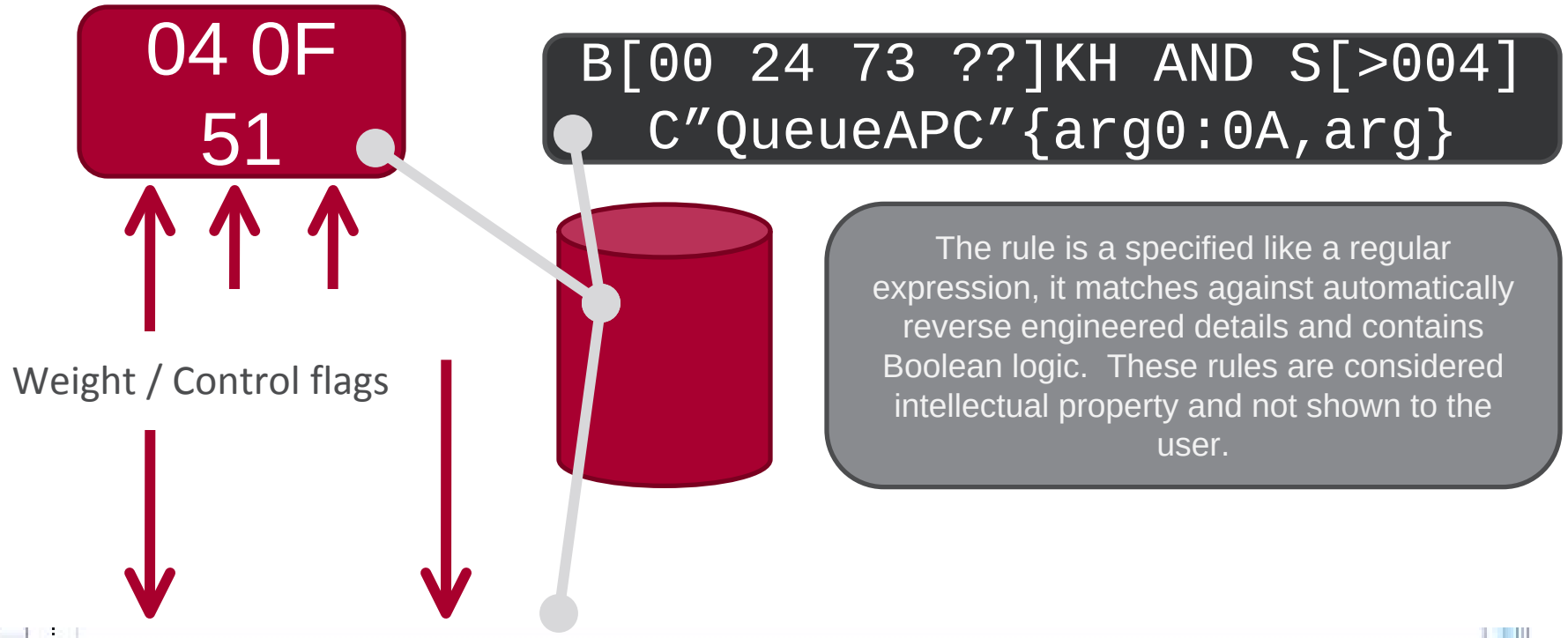
McAfee® COMPATIBLE

Questions?

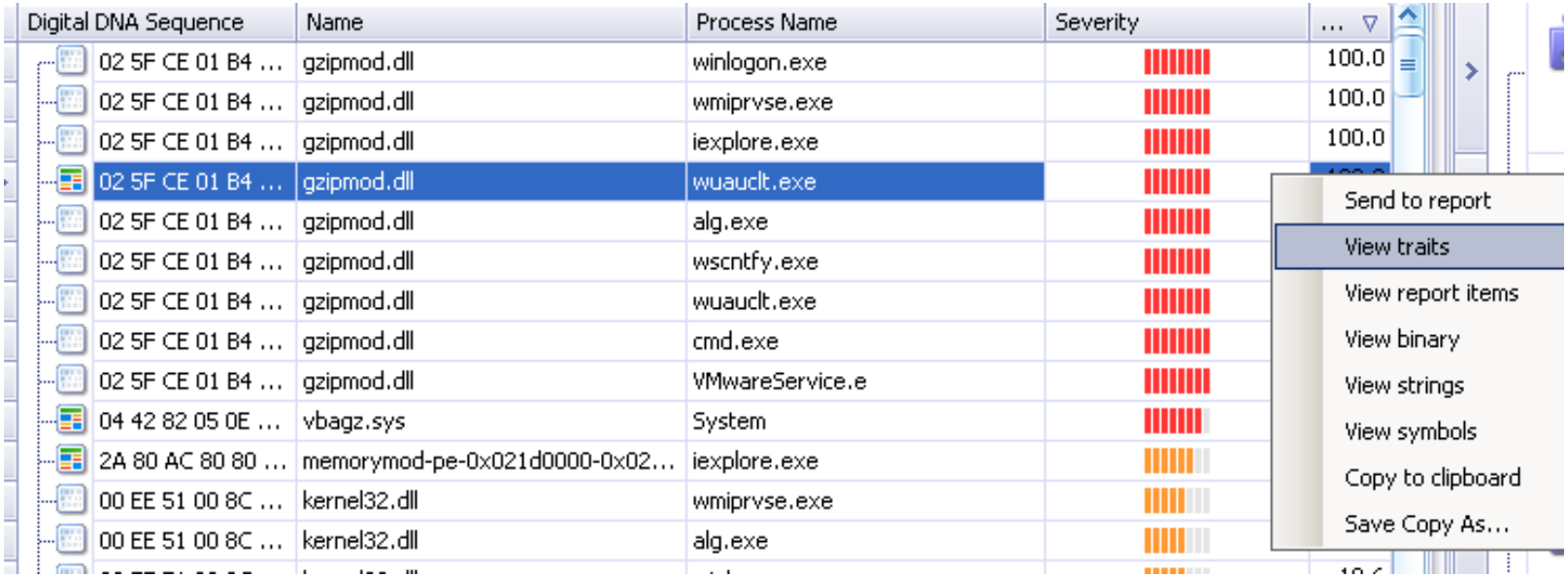
Thank you very much

sales@hbgary.com

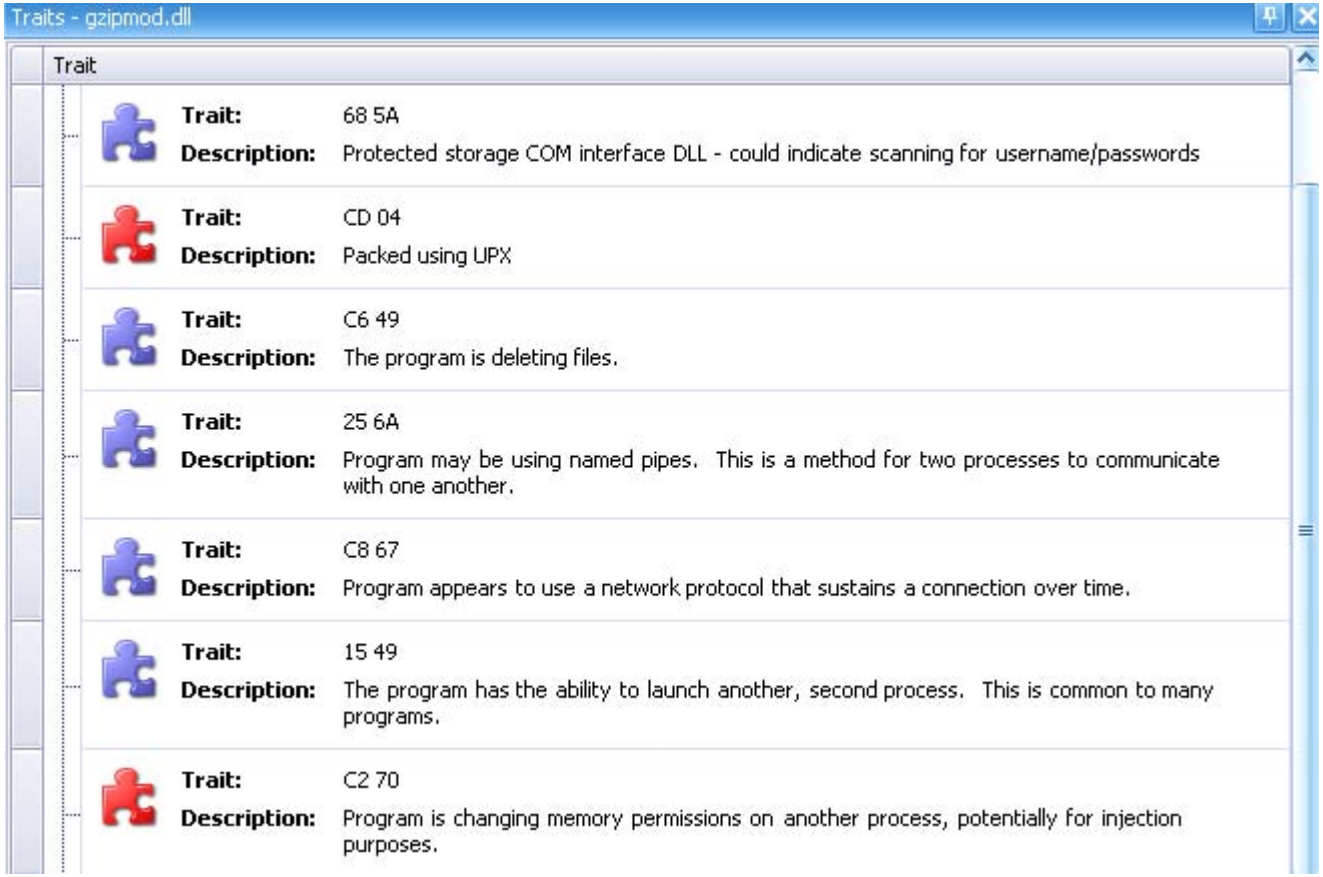
What's in a Trait?



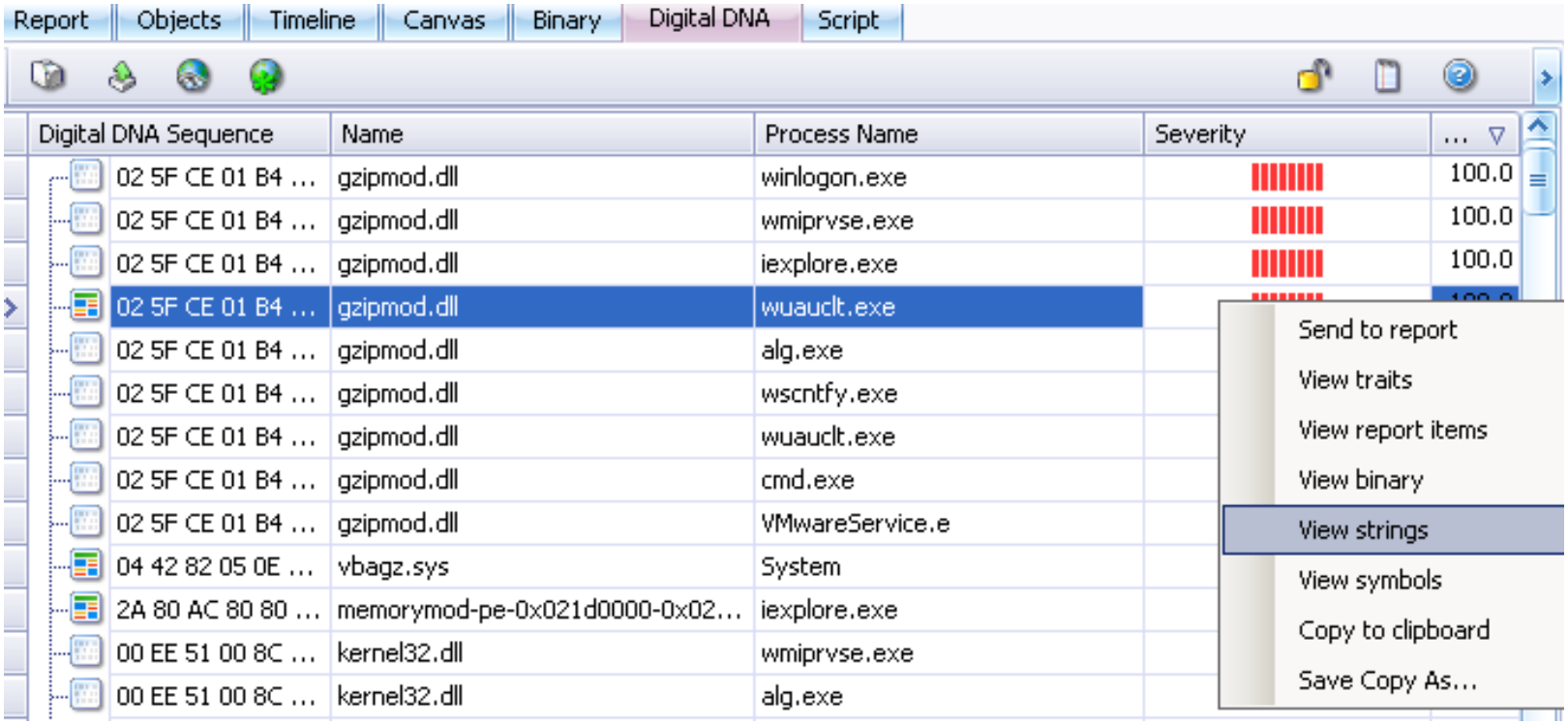
Responder Pro w/DDNA



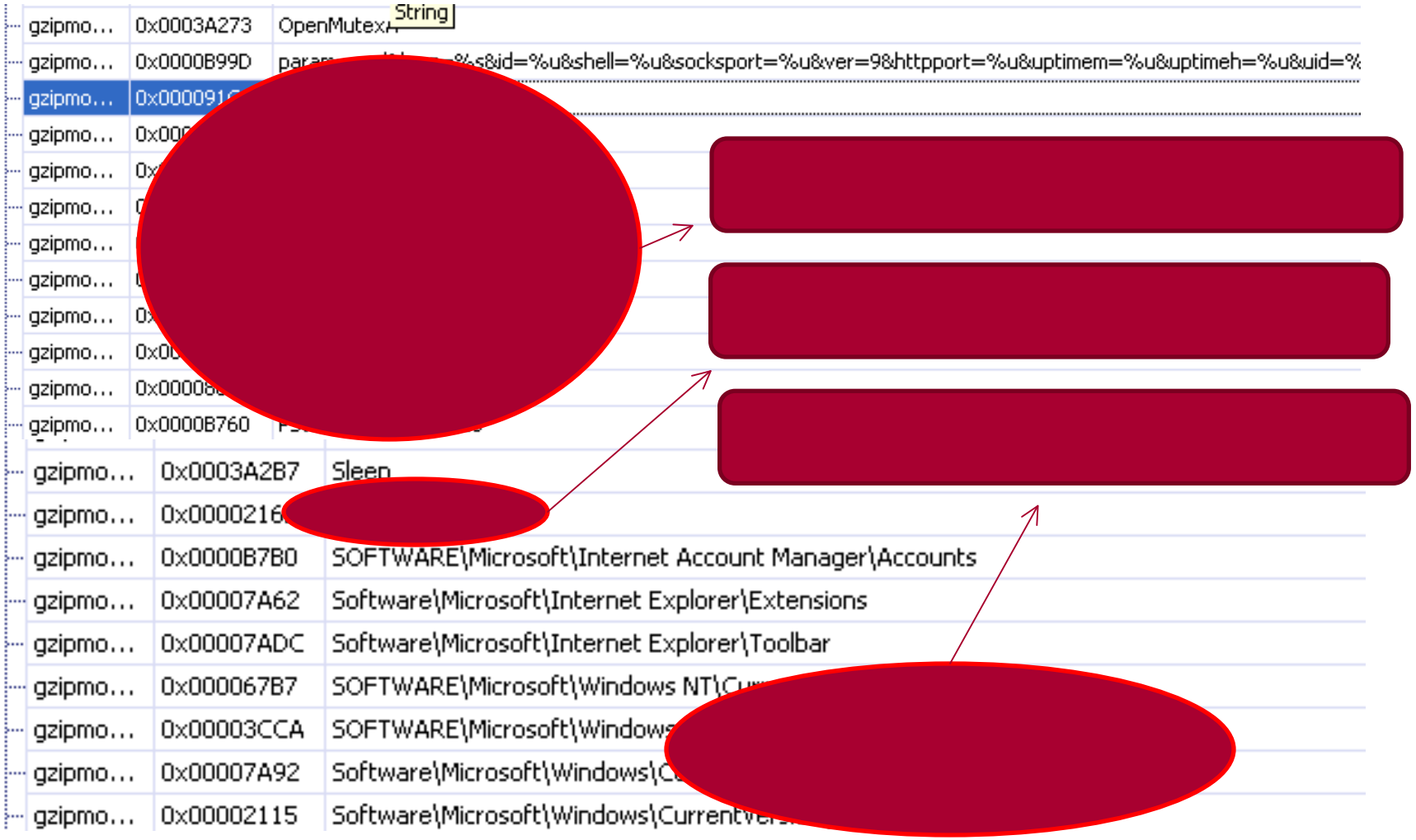
Traits for gzipmod.dll



Malware Analysis- Responder Pro



Actionable Intelligence – Responder Pro




McAfee®