



## **Seamless Security using: GuardIT® for FLEXnet® Publisher**

**October 22<sup>nd</sup>, 2008**

*Vince Arneja  
Director, Product Management  
Arxan Technologies  
&  
John Frame  
Senior Director, Product Management  
Acesso Software*

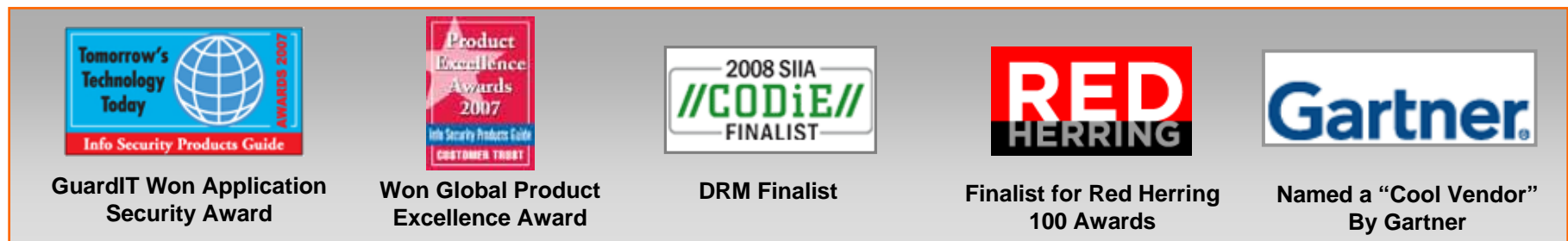
- About Arxan Technologies
- Software Piracy Problem/IP Protection
- GuardIT - Proven Technical Solution exists today
- Acreesso and Arxan Partnership (LM Fortification)
  - What does it mean
  - What are the benefits
- Arxan YTS
- Summary
- Q&A

# Arxan At-A-Glance



- **History:** Core technology was conceived in 1998 out of an NSA Center of Excellence (CERIAS) located at Purdue University; Department of Defense pedigree; leading Anti-tamper solution since 2001
- **Research:** Advanced R&D group focused on next wave of solutions
- **Current Standing:** Grown revenues more than 100% per year for last 3 years; privately held, VC backed, well-funded
- **Offering:** Application hardening solutions that secure code and keys to actively protect software from tampering, piracy and reverse engineering.
- **Customer Value:** Business-critical software NOW has built-in/embedded security features. Network security, identity and access management alone are insufficient.

Offices in Bethesda (MD), San Francisco, W Lafayette (IN) plus Sales offices



- **Piracy:** Building or using unauthorized and/or unpaid for copies of proprietary software, for internal use or for external sales. Also, enabling disabled/unpaid for proprietary functionality for internal use or sale.
- **Reverse engineering:** Determining the logic structure and run-time control of software, in order to extract proprietary intellectual property in the form of algorithms or for the purposes of effective tampering.
- **Insertion of exploits:** Insertion of viruses or other malware into software (pirated or legitimate).
- **Tampering:** Altering proprietary distributed software at the binary level to achieve piracy objectives, to insert exploits, or to aid in reverse engineering.

# Software Piracy Headlines: Alarming



Two-thirds of software, costing \$200B, will be pirated over next 5 years



Hackers bypassing Symantec; using their software tools as gateway into corporate servers



“EDA-Software vendors are taking software protection seriously”



“Chinese pirates busted with \$500 million of software”



“Successful iPhone Hack”



“Huawei lifted... software code” from Cisco router



(DRM) Licensees neglected to encrypt decryption key



Pystar’s \$399 Mac clone can run Apple OS and software



US Atty General - Piracy threatens national security, funds terrorism



“Microsoft’s DRM Hacked”



Hacks distributed by competitor cost smart card company \$90M



NDS quote – All companies reverse-engineer competitor technology



SonyBMG sued by small software company for piracy

# Software IP Theft and Piracy = Revenue Leakage



- Software delivered outside of corporate firewalls are **completely exposed** to:
  - ⇒ Reverse engineering resulting in IP theft!
  - ⇒ Binary level hacking:
    - ✓ Works around license management to enable piracy
    - ✓ Allows non-payment for features
    - ✓ Modifies behavior
- Legal protections against such activities are important... and taken alone, are not sufficient to deter software theft.
- In many situations, good technical protection defense does not need to be perfect or entirely impenetrable.
- Software products are available **today** that can virtually stop software IP theft and piracy, and such technology can be easily applied to binary software prior to market delivery.

## ***Historical Attacks:***

- Determine method to generate valid keys
  - Reverse engineer key creation, or find keys that can be reused.
- Spoof the presence of valid licenses
  - For example, by cloning a license server that has been enabled through a purchase transaction to serve as legitimate keys.

## ***Modern Binary Level Attacks:***

- Bypass license management
  - Tamper with decision making routines in the binary code.
- Modify code to enable/disable/modify functionality
  - Tamper with internal parameters, tamper with enabled/disabled decision making code, or insert operational changes.
- Reverse engineer product components
  - Extract IP-rich routines for competitive value and usage.

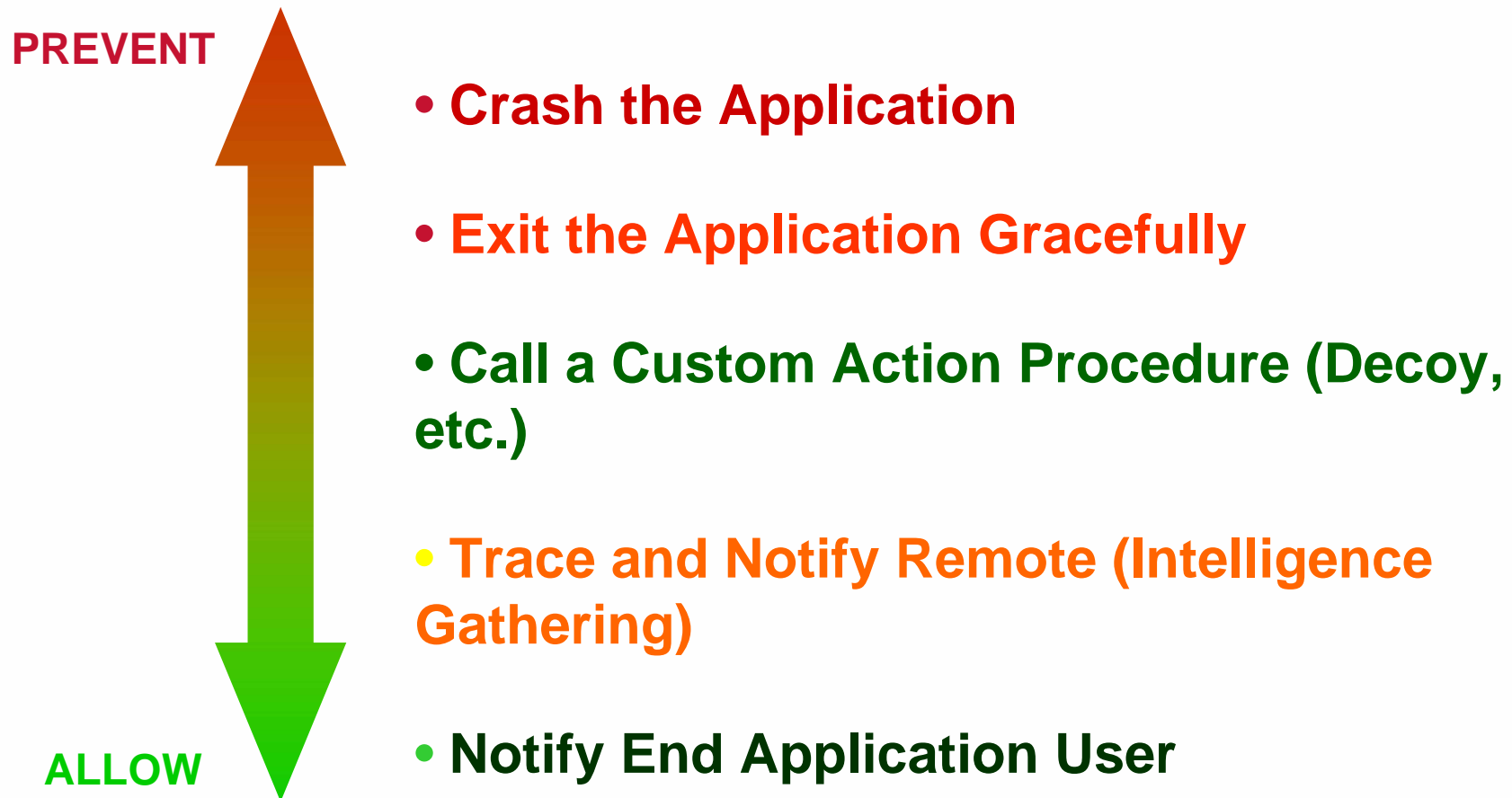
# GuardIT® = RLP (Revenue Leakage Prevention)



- GuardIT is a GUI based software product that hardens applications to track and/or prevent binary code modification.
- GuardIT enables you to quickly and easily implement a deep intricate layered protection by embedding a collection of interdependent protection routines, called Guards, into a program at the binary level and obfuscating the result.
- The Guards, which appear to be normal code:
  - Enable the program to **DEFEND** itself,
  - To **DETECT** if it is attacked,
  - To **REACT** if it is modified
- Differentiating benefits of GuardIT include:
  - Fine-grained control over protection
  - Layered protection
  - Low performance impact, low development impact







# GuardIT – Flagship Product Coverage



## GuardIT Family of Products:

- **GuardIT for Windows 32/64 bit**
  - Desktop
  - Server
- **GuardIT for Linux 32/64 bit**
  - Desktop
  - Server
  - Embedded
- **GuardIT for Microsoft .NET Framework**
- ***GuardIT for FLEXnet Publisher***

## GuardIT Specifications:

### Supported languages

- C, C++; both native and mixed mode images,
- C#, VB.NET for managed code applications

### Supported executable file formats

- PE,
- ELF

### Supported compilers

- Visual Studio 2002, 2003, 2005(SP1) and 2008 (SP1),
- GCC 3.4.4.2, 3.4.6, 4.1.0

### Supported Development (Host) Platforms

- Windows XP SP2 32 bit and 64 bit,
- Windows Vista Enterprise 32 and 64 bit,
- Windows Server 2003 R2 64 bit

### Supported Deployment (Target) Platforms

- Windows XP SP2 32 bit and 64 bit,
- Windows Vista Enterprise 32 and 64 bit,
- Red Hat Enterprise Linux 4,
- Red Hat Enterprise 5

### Supported Target chipsets

- Intel Compatible x86 (32-bit),
- 64-bit chipset,
- PPC

### Build integration

- Command line interface allows seamless integration into any build environment

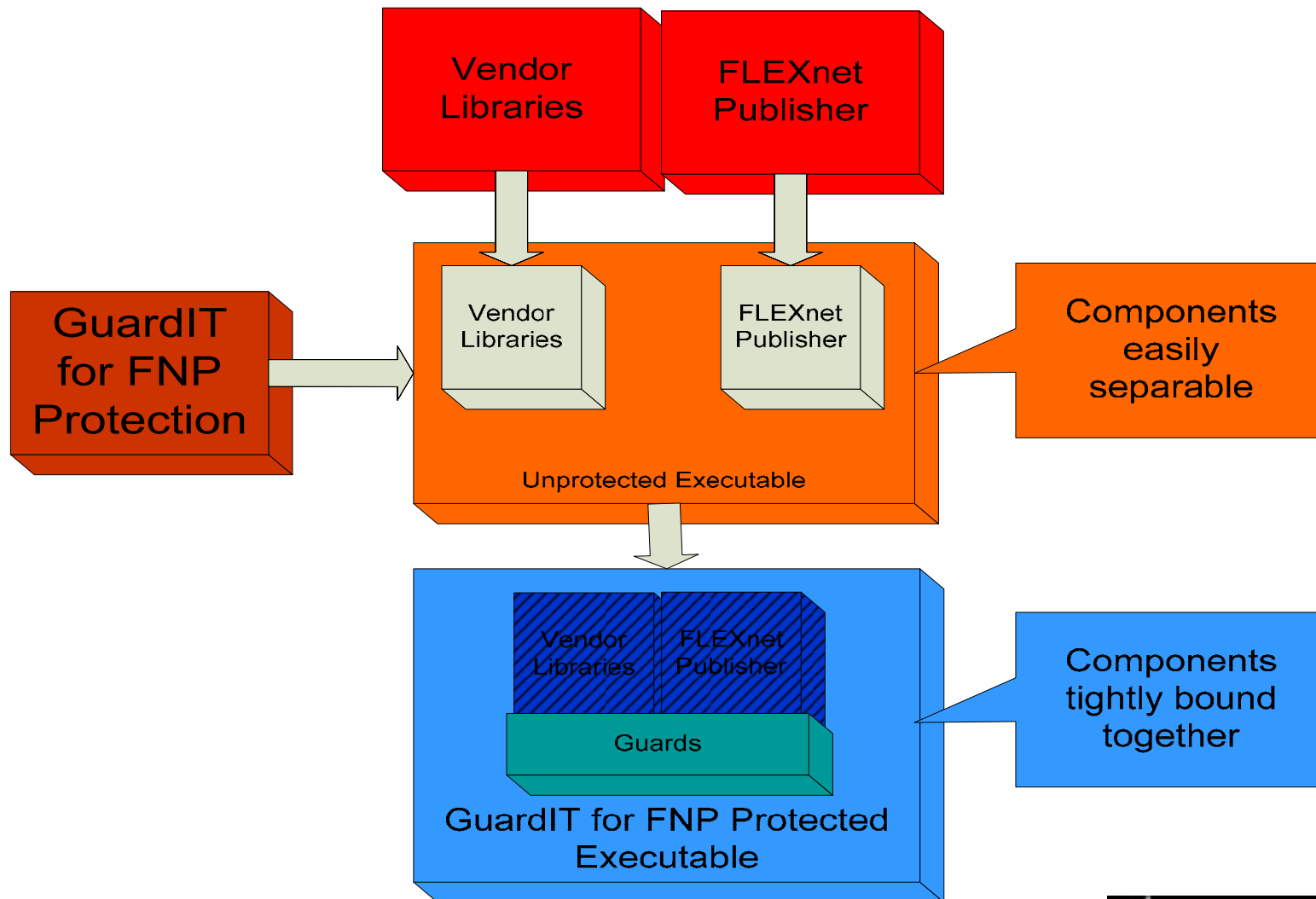
# The Acresso-Arxan Partnership



- The combination of **FLEXnet Publisher licensing technology** and Arxan's application hardening solution enables producers to:
  - protect and secure their applications against tampering and piracy
  - eliminate the inappropriate use of software, preserve revenue and brand value
- **GuardIT for FLEXnet Publisher** - a rich product combination that safeguards application files and the integrity of licensing solutions against tampering and piracy:
  - **Provides** intricate and layered protection to mitigate LM piracy and tampering
  - **Provide** durable and customized binary-based protection against sophisticated threats
  - **Deploy** software protection rapidly via an automated and easy-to-use solution
  - **Exercise** predetermined control over specific software areas
  - **Designed** for high security and low application impact protection
- **GuardIT for FLEXnet Publisher** is specifically designed to protect FLEXnet libraries and application calls to the FLEXnet libraries. The protection is extensible, easy-to-use and can be deployed as a seamless part of your existing build process.



# Power of the Partnership

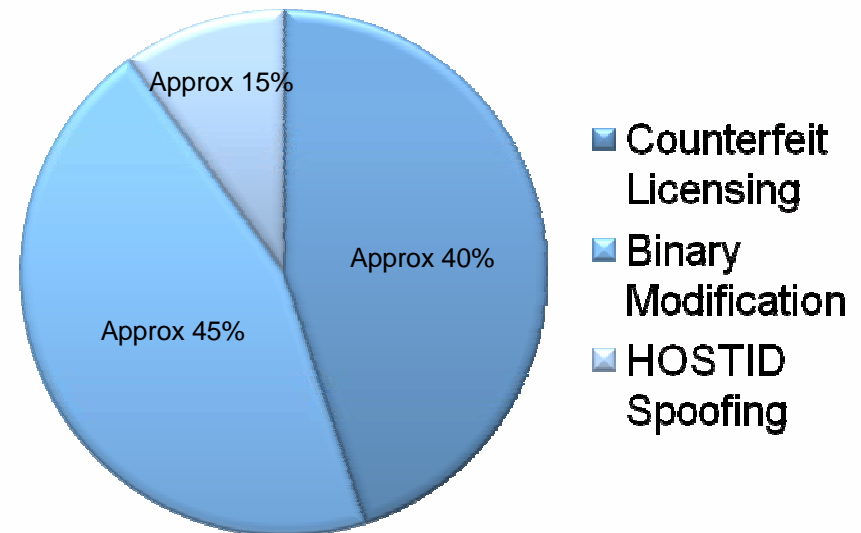


# Three Basic Forms of LM “Piracy”



- **Counterfeit Licensing**
  - Majority of piracy used to take this form
  - Acrecco added increased encryption via Tamper Resistant Licensing (TRL/CRO)
- **Binary Modification**
  - Current weakest link
  - GuardIT for FLEXnet Publisher
- **HOSTID spoofing**
  - Very easy to “spoof” (clone) PC hardware IDs
  - Mitigated with Composite HostIDs and Dongles
  - Doesn’t facilitate “large-scale” piracy

## Piracy Analysis



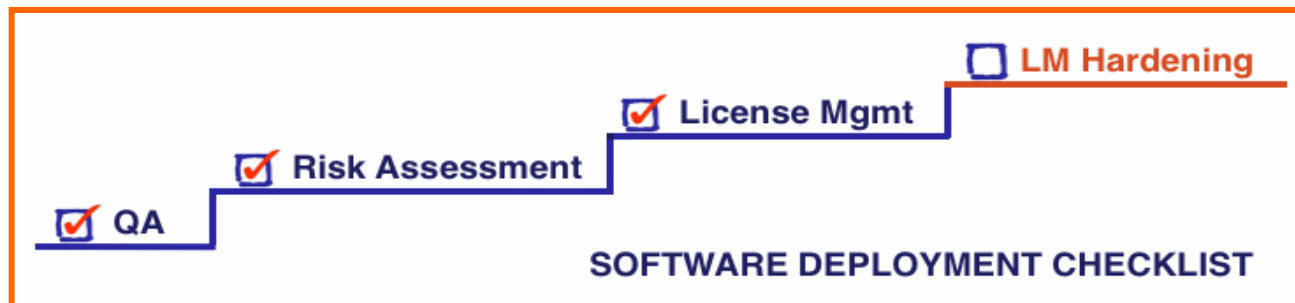
Source: EDAC and Arxan customer feedback



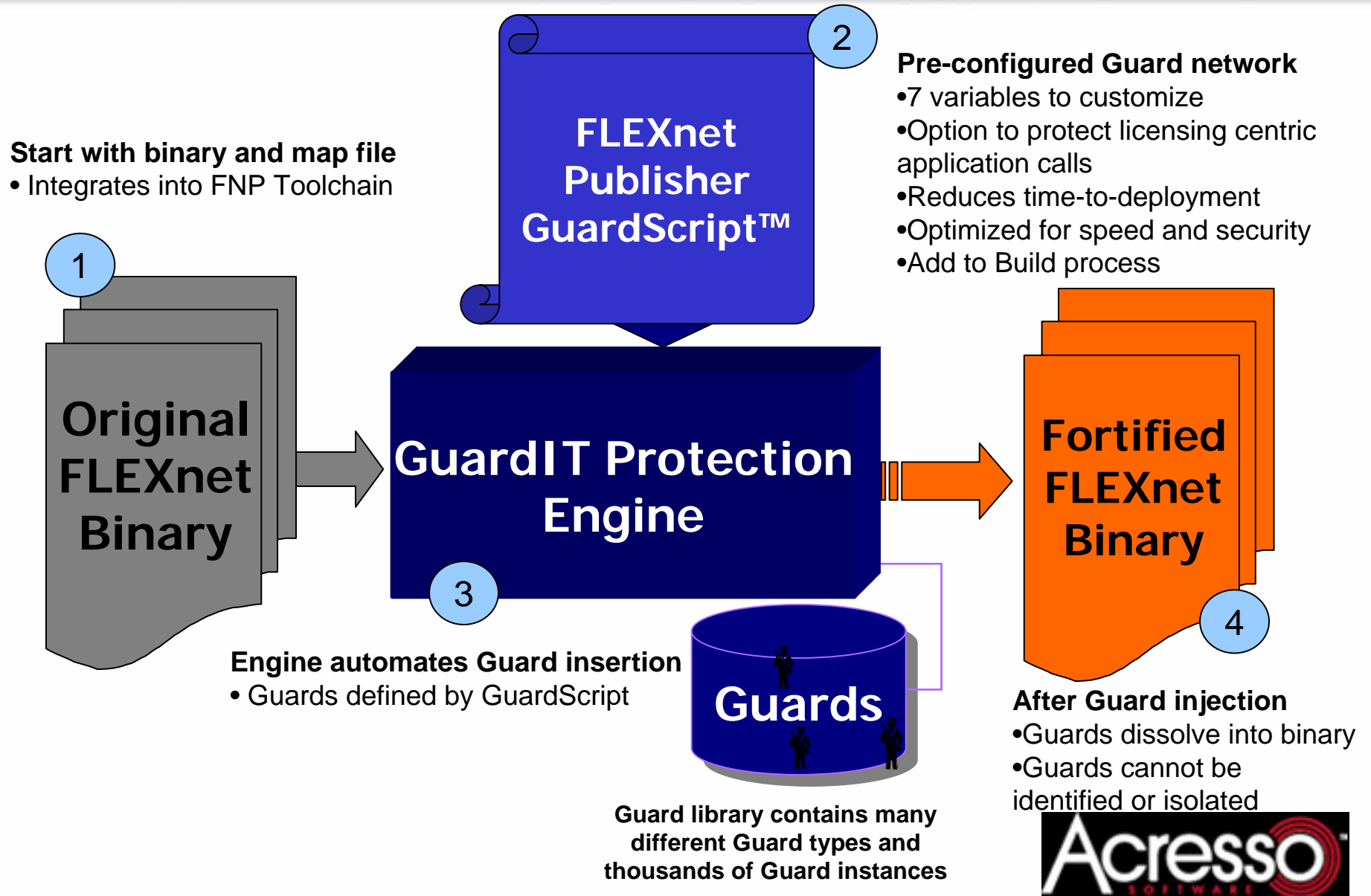
# Why Add a Layer of Protection?



- The effort is one of making it harder to:
  - Understand what the licensing software is doing
  - Manipulate what the code is doing so that functionality remains, but licensing hardening is bypassed
- It is **ALWAYS** possible to defeat any technology
  - Customers should understand this, have appropriate expectations
  - Customers should set business metrics
  - Time from release to published exploit (i.e. 6 mo, 1 yr, 5yrs)
  - Ease of use in the exploit



# Hardening FLEXnet Publisher Apps



# Protection Diversity



- Each copy of a protected application can have a different instantiation of the Guard network
- Each Guard type has a large number of instances
- Defeats BORE Attack
- Randomized using seed element
- Example: Imgr.lib



# Demonstration



Come see the demo at the Arxan booth here at SoftSummit

```
C:\> 9. GuardIT for FNP

Finalizing program changes....Lookup of substring '_lc_checkout' returns:
_lc_checkout

..Lookup of substring '_lc_checkout' returns:
_lc_checkout

....Lookup of substring '_lc_checkout' returns:
_lc_checkout

.....
Lookup of substring '_lc_checkout' returns:
_lc_checkout

Patching all of 'I.code("_lc_checkout")' with 0x90 ... Ok.
Warning: The program code protected by guard 'I.Repair_lc_checkout_function' has
just been patched.
Patching images...

Transformed image 'I' written to file 'C:\arxan_demo\workspace\mvsn_composite\p_
mvsn_compex.exe' (2617344 bytes, or 184% of the original image size).
Protection completed successfully.

C:\arxan_demo\workspace\mvsn_composite>
```



# Managing SW Piracy: where to start?



## *Arxan Yellow Team Services:*

Software Theft is Rampant: Proceed With Caution

**Level 1 - Assess the Damage:** determine which of your software products are being hacked and sold for little or no money



**Benefit:** Determine which of your software products are being pirated, and what IP is at risk.

**Level 2 - Determine the Reason:** where are the weak links or vulnerabilities?



**Benefit:** Understand where the weak links or attack exposures may exist.

**Level 3 - Plot your Plan:** what are your options for defense, what are anticipated benefits?



**Benefit:** Determine your general solution for defense. strategy. Assess and choose specific implementation technologies or products.



- EDAC is leveraging Arxan YTS
- Piracy impact on the EDA software industry and enable the EDAC members to make value based decisions for their Anti-Piracy strategies.
- Specific acts of piracy will be validated and categorized by software type, operating system, total time to crack, and attack vector.
- Will execute all levels of the YTS on various EDAC member applications

# Summary



- There is a proven binary based technical product to help combat the piracy problem
- Not all products are created equal
- Synergy with Acreesso and direct customer feedback leads to seamless customer experience
- More product evolution to come
- YTS helps to get started





# Thank You

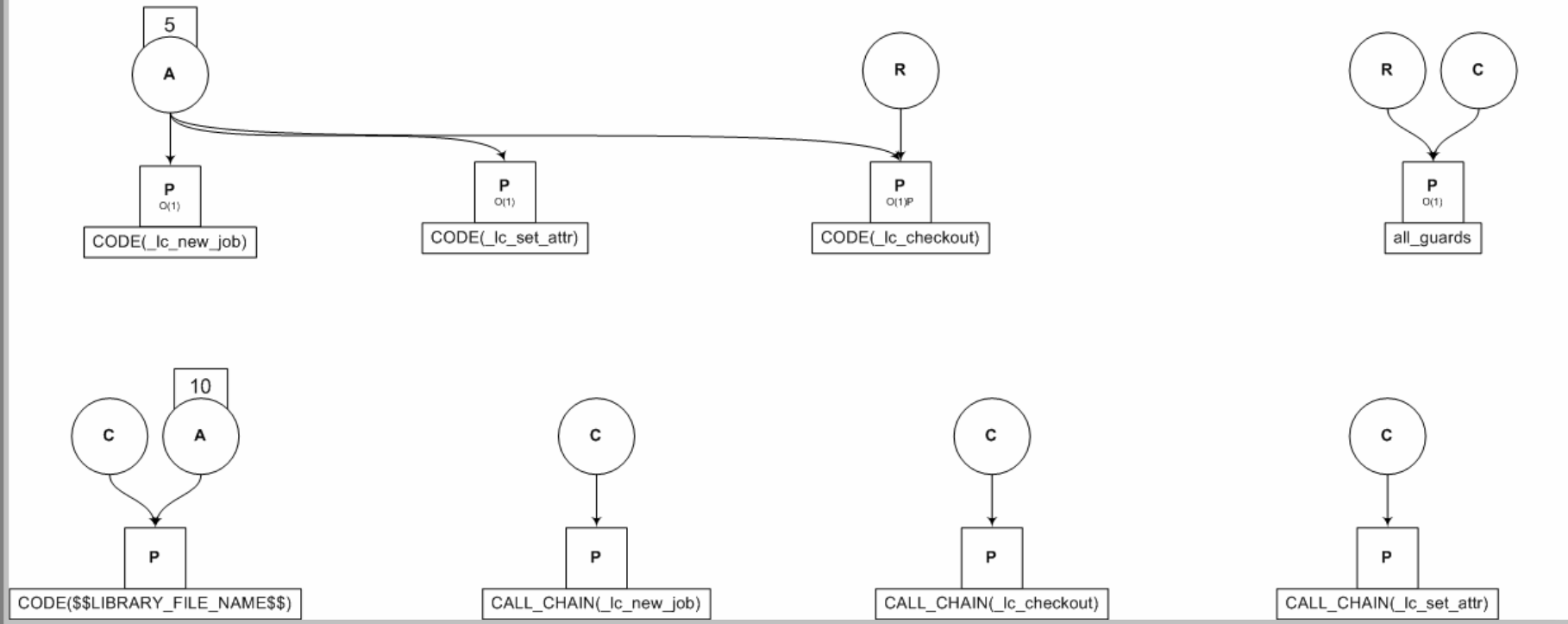
*Vince Arneja*  
*Director, Product Management*  
*Arxan Technologies*  
&  
*John Frame*  
*Senior Director, Product Management*  
*Acesso Software*

# GuardScript Design



Fri Apr 04 14:01:06 2008

guardscript\_template\_windows\_exit\_action.gsml



***You can use any text or XML editor to edit the GuardScript***

- **Specify the location of the XSD (schema) file in the *GuardScript* element**
- **Specify the location of the configuration file in the *config\_cmd* element.**
- **Identify the location of the program to be protected and the directory in which to put the resulting protected program in the *input\_file* and *output\_file* parameters.**
- **Specify the location of the auxiliary files**
- **Specify the location and name of the LMGR libraries**

## Red Teaming

- *Highly skilled/ethical hackers perform a blind security assessment*
  - Model the actions of an adversary
  - Simulate “in the field” malicious attacks
  - Knowledge provided to team is from public sources only

## Blue Teaming

- *Highly skilled security team hired as part of customer’s development team*
  - Has access to priority information i.e. source code, documents, etc.
  - Design, develop, and implement a protection plan
  - Can be performed in parallel with Red Teaming

## Consulting/Training

- CPI/IP identification
- Anti-Tamper planning
- Vulnerability Assessment
- Tool Training