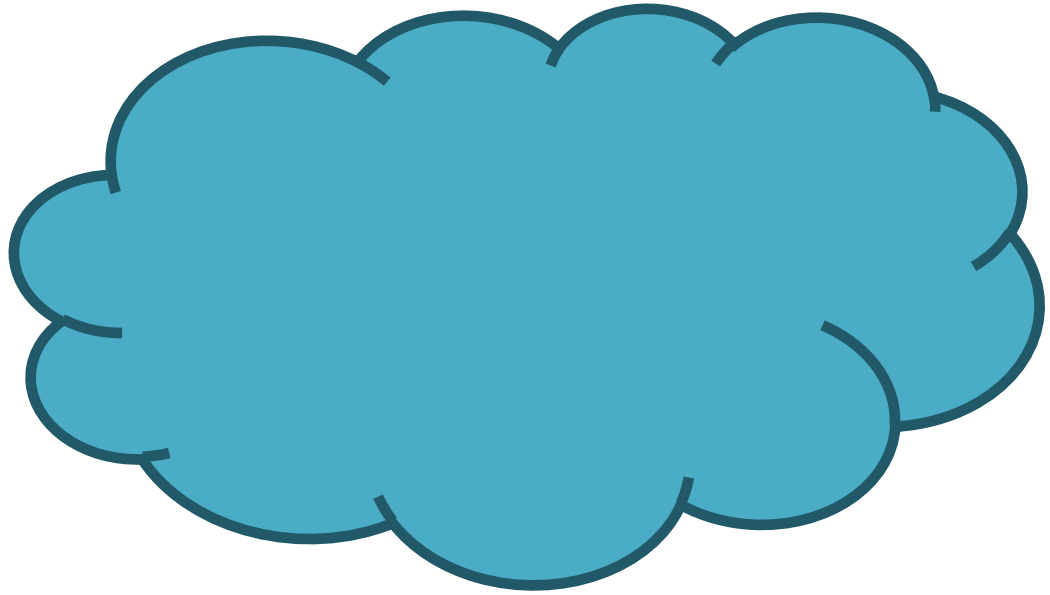
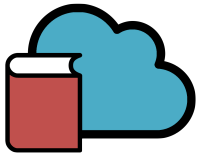
Definition of Cloud Computing

Cloud Computing is…



a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)

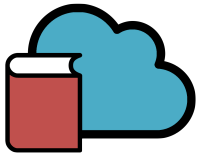


Definition of Cloud Computing

Cloud Computing is…

convenient, on-demand shared configurable resources

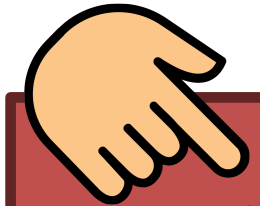
that can be rapidly provisioned and released with minimal management effort or service provider interaction



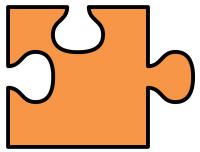
Definition of Cloud Computing

Cloud Computing is…

convenient, on-demand shared configurable resources, rapidly provisioned with minimal effort



Note: The cloud computing industry represents a large ecosystem of many models, vendors, and market niches. This definition attempts to encompass all of the various cloud approaches.



Cloud Characteristics Quiz

Given our definition of cloud computing fill in the 5 essential cloud characteristics.

On demand self service

Broad or wide network access

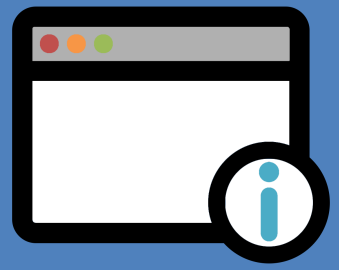
Resource pooling or sharing

Measured service

Rapid elasticity

Cloud Service Models

Software As A Service



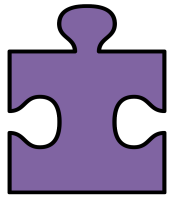
- Use the provider's applications running on a cloud infrastructure

Platform As A Service

- Consumer-created applications using programming languages and tools supported by the provider

Infrastructure As A Service

- Capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources

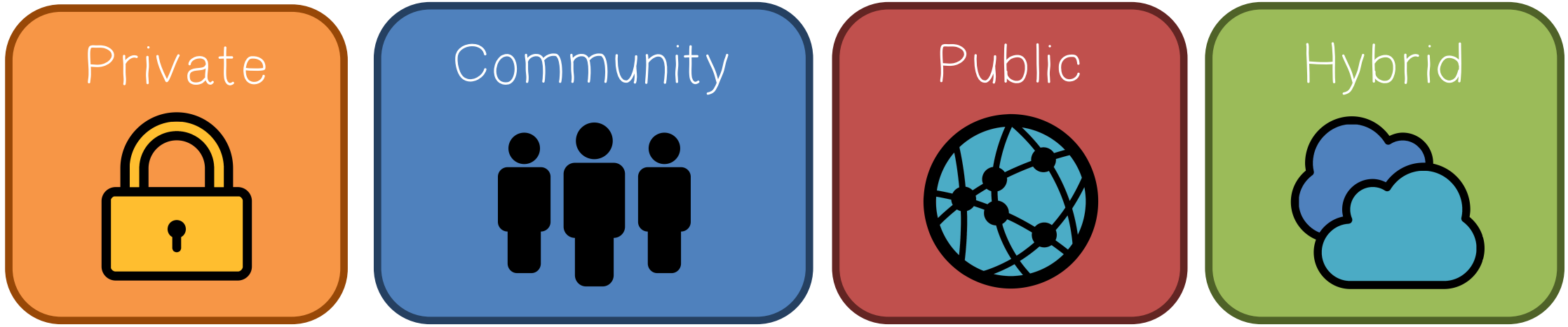


Services Quiz

Given the definitions of SaaS, IaaS, PaaS determine the service category for each of the products listed:

PaaS	Google Apps
IaaS	Amazon Web Services
PaaS	Salesforce
SaaS	Knowledge Tree
IaaS	Microsoft Azure

Cloud Deployment Models



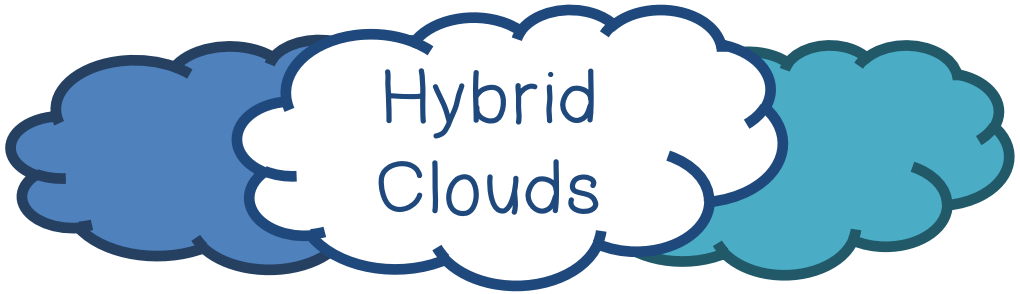
- The cloud infrastructure is operated solely for an organization.
- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns
- The cloud infrastructure is made available to the general public or a large industry group
- The cloud infrastructure is a composition of two or more clouds (private, community, or public)

Common Cloud Characteristics Quiz

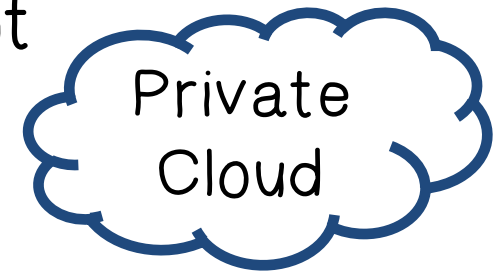
List some of the characteristics that all four cloud models share:

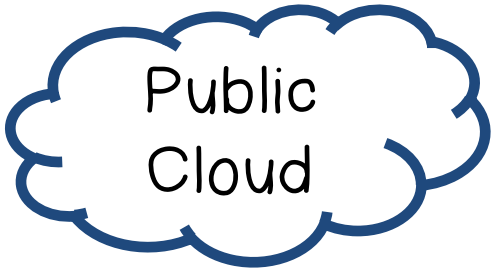
Massive scale
Homogeneity
Virtualization
Resilient computing
Low cost software
Geographic distribution
Service orientation
Advanced security technologies

NIST Cloud Definition Framework



Deployment Models:

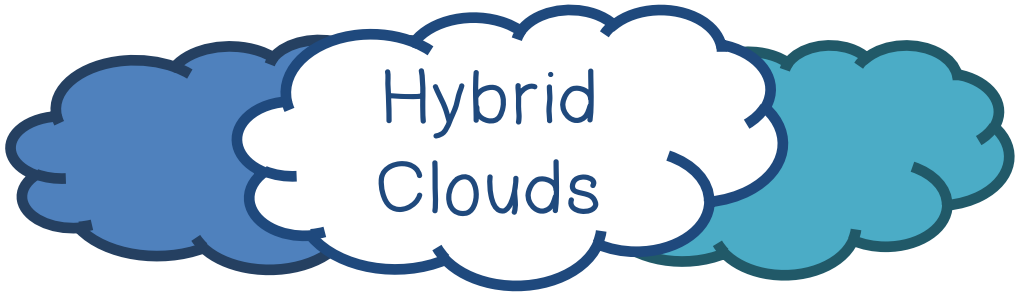




Service Models:

Source: Based upon original chart created by Alex Dowbor - http://ornot.wordpress.com

NIST Cloud Definition Framework

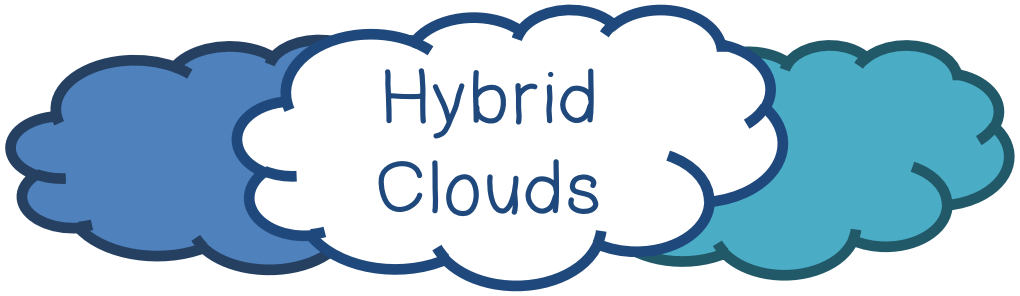


Essential Characteristics:

- On Demand Self-Service
- Broad Network Access
- Rapid Elasticity
- Resource Pooling
- Measured Service

Source: Based upon original chart created by Alex Dowbor - http://ornot.wordpress.com

NIST Cloud Definition Framework



Common Characteristics:

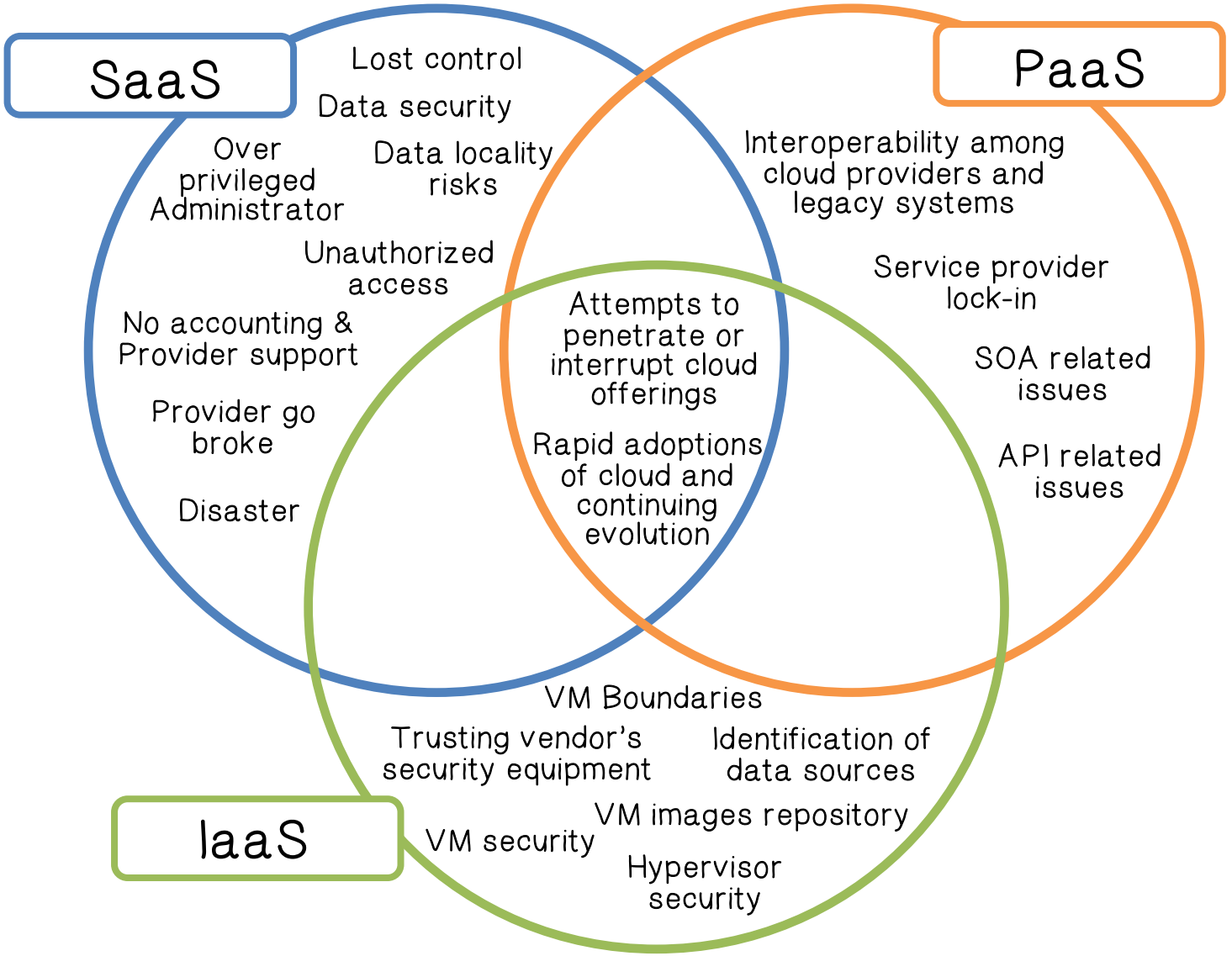
- Massive Scale
- Resilient Computing
- Homogeneity
- Geographic Distribution
- Virtualization
- Service Orientation
- Low Cost Software
- Advanced Security

Source: Based upon original chart created by Alex Dowbor - http://ornot.wordpress.com

NIST Risk Identified Quiz

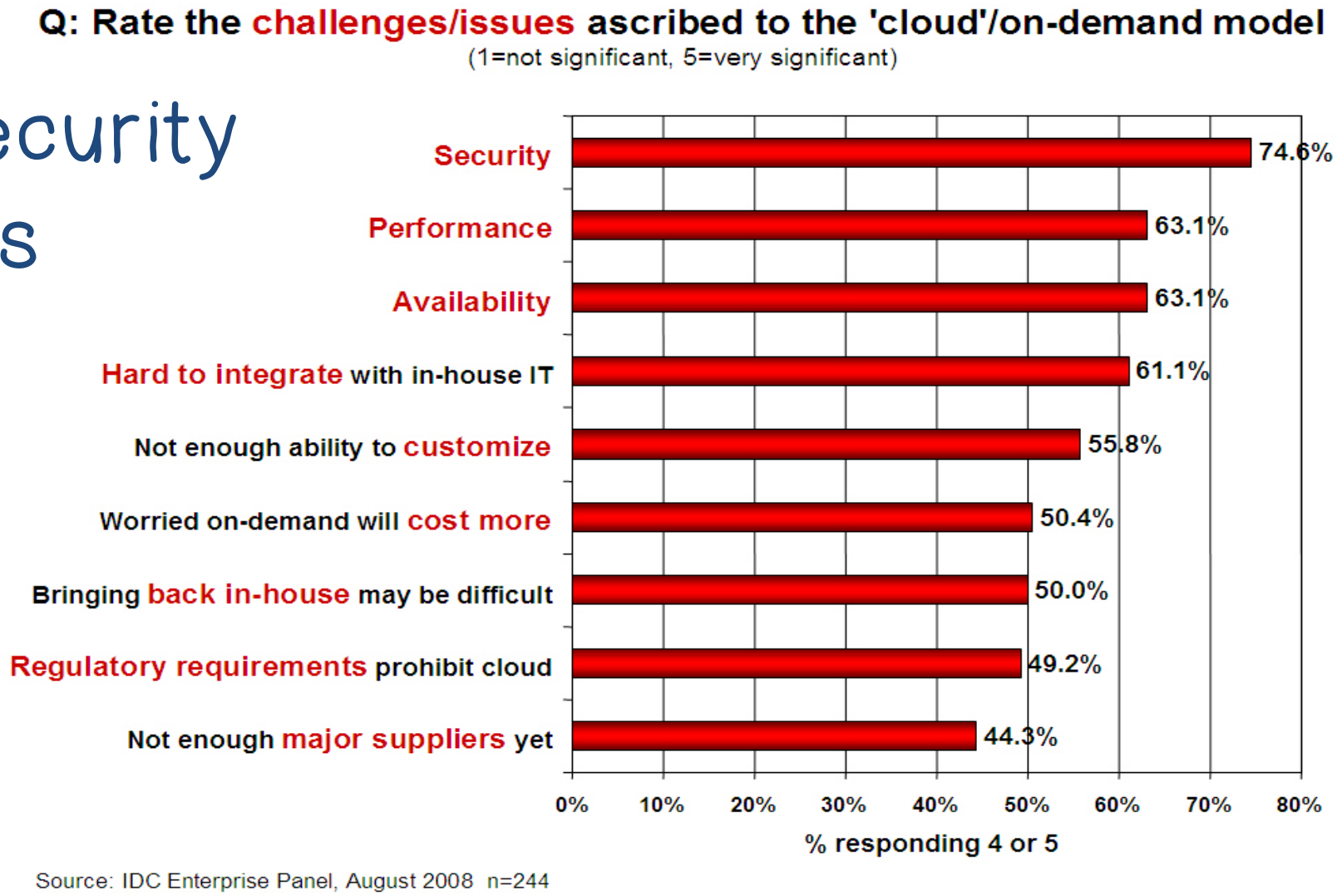
Given the risks, determine which mode belongs to each circle:

(Write PaaS, SaaS, or IaaS in the text boxes)



Cloud Security Concerns

Security and Data Privacy: Critical Barriers to Adopting Cloud Computing



Analyzing Cloud Security

Key Issues:

- Trust, multi-tenancy, encryption, compliance

Clouds are massively complex systems

- Simple primitives and common functional units

Cloud security is a tractable problem

- There are both advantages and challenges

Analyzing Cloud Security

Cloud security advantages

- Shifting public data to an external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery

Analyzing Cloud Security

Cloud security challenges

- Trusting vendor's security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can't be examined
- Loss of physical control

Security Relevant Cloud Components

- Cloud Provisioning Services
- Cloud Data Storage Services
- Cloud Processing Infrastructure
- Cloud Support Services
- Cloud Network and Perimeter Security
- Elastic Elements: Storage, Processing, and Virtual Networks

Provisioning Services

Advantages	Challenges
• Rapid reconstitution of services • Enables availability • Provision of multiple data centers • Advanced honeynet capabilities	• Impact of compromising the provisioning service

Data Storage Services

Advantages	Challenges
• Data fragmentation and dispersal • Automated replication • Provision of data zones (e.g., by country) • Encryption at rest and in transit • Automated data retention	• Isolation management / data multi-tenancy • Storage controller • Single point of failure / compromise? • Exposure of data to foreign governments

Security Cloud Components

Cloud Processing Infrastructure

✔ Advantages	! Challenges
• Ability to secure masters and push out secure images	• Application multi-tenancy • Reliance on hypervisors • Process isolation / Application sandboxes

Security Cloud Components

Cloud Support Services

Advantages	Challenges
• On demand security controls (e.g., authentication, logging, firewalls…)	• Additional risk when integrated with customer applications • Needs certification and accreditation as a separate application • Code updates

Security Cloud Components

Cloud Network and Perimeter Security

✔ Advantages	! Challenges
• Distributed denial of service protection • VLAN capabilities • Perimeter security (IDS, firewall, authentication)	• Virtual zoning with application mobility

Cloud Security Advantages

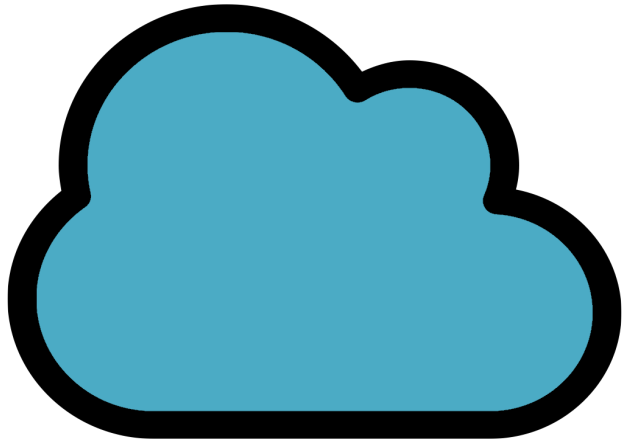
- Data Fragmentation and Dispersal
- Dedicated Security Team
- Greater Investment in Security Infrastructure
- Fault Tolerance and Reliability
- Greater Resiliency
- Hypervisor Protection Against Network Attacks
- Possible Reduction of C&A Activities *(Access to Pre Accredited Clouds)*

Cloud Security Advantages

- Simplification of Compliance Analysis
- Data Held by Unbiased Party (cloud vendor assertion)
- Low-Cost Disaster Recovery and Data Storage Solutions
- On-Demand Security Controls
- Real-Time Detection of System Tampering
- Rapid Reconstitution of Services
- Advanced Honeynet Capabilities

Cloud Security Challenges

- Data dispersal and international privacy laws
  - EU Data Protection Directive and U.S. Safe Harbor program
  - Exposure of data to foreign government and data subpoenas
  - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees



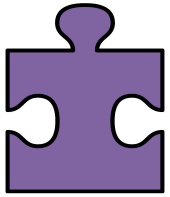
Cloud Security Challenges

- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Public cloud vs internal cloud security
- Lack of public SaaS version control

Cloud Security Challenges

Encryption needs for cloud computing

- Encrypting access to the cloud resource control interface
- Encrypting administrative access to OS instances
- Encrypting access to applications
- Encrypting application data at rest



Cloud Security Quiz

Which of the following statements are true?

- [x] Most data in transit is encrypted
- [ ] Most data at rest is encrypted
- [ ] All data at rest should be encrypted

Additional Issues

Issues with moving PII and sensitive data to the cloud

- Privacy impact assessments

Using SLAs to obtain cloud security

- Suggested requirements for cloud SLAs
- Issues with cloud forensics

Additional Issues

Contingency planning and disaster recovery for cloud implementations

Handling compliance

- FISMA
- HIPAA
- SOX
- PCI
- SAS 70 Audits

Cloud Security Architectures

Clouds typically have a single security architecture but have many customers with different demands

- Clouds should attempt to provide configurable security mechanisms

Organizations have more control over the security architecture of private clouds followed by community and then public

- This doesn't say anything about actual security

Higher sensitivity data is likely to be processed on clouds where organizations have control over the security model

Foundational Elements of Cloud Computing

Primary Technologies

- Virtualization
- Grid technology
- Service Oriented Architectures
- Distributed Computing
- Broadband Networks
- Browser as a platform
- Free and Open Source Software

Foundational Elements of Cloud Computing

Other Technologies

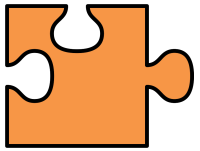
- Autonomic Systems
- Web 2.0
- Web application frameworks
- Service Level Agreements

Virtualization Quiz

Fill in the blanks with regards to cloud computing virtualization.

Virtualization requires at least **one** instance(s) of an application or resource that is to be shared by different organizations.

Sharing between organizations is accomplished by assigning a **logical name** to the resource and then giving each request a **pointer** to the resource.



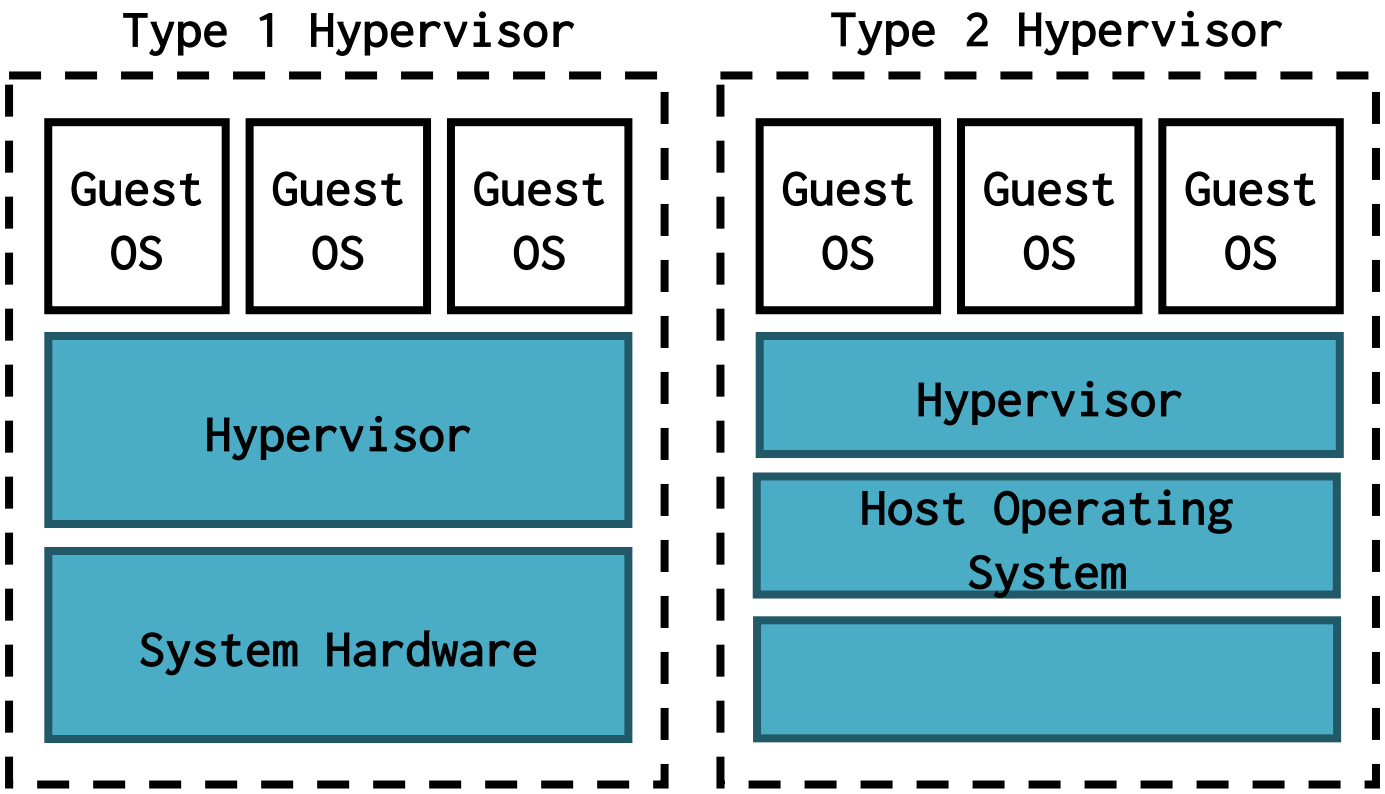
Virtualization Quiz 2

Fill in the blanks with regards to Cloud computing virtualization:

Virtualization involves creating a virtual machine using existing hardware and operating systems. The virtual machine is logically isolated from the host hardware.

Virtualization Quiz 3

A hypervisor acts as a Virtual Machine Manager.
Given these two diagrams, answer the questions:



Which one does not have any host operating system because they are installed on a bare system?

Type 1

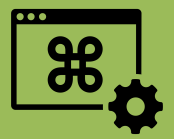
Which one emulates the devices with which a system normally interacts?

Type 2

Platform Virtualization

"[Cloud computing] relies on separating your applications from the underlying infrastructure"

- Steve Herrod, CTO at VMware



Host operating system provides an abstraction layer for running virtual guest OSs

Platform Virtualization

Key is the “hypervisor” or “virtual machine monitor”

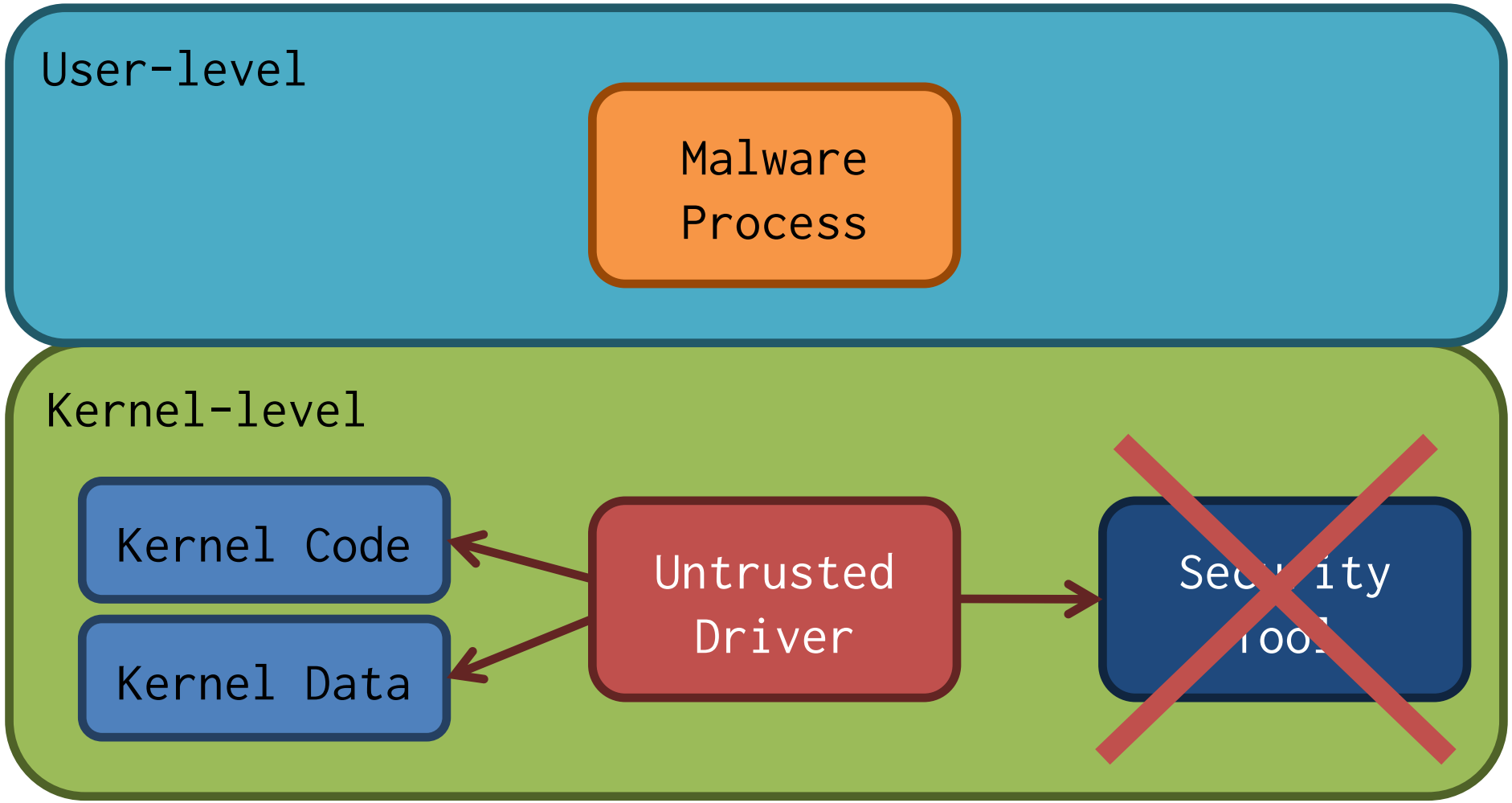
- Enables guest OSs to run in isolation of other OSs
- Run multiple types of OSs

Increases utilization of physical servers

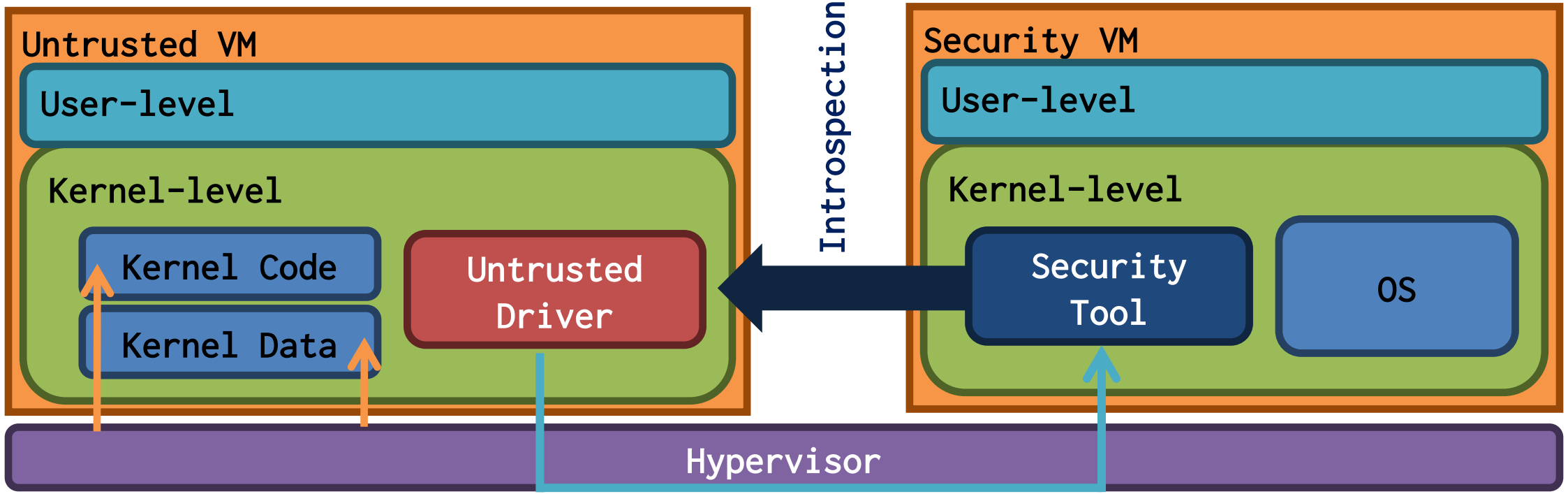
Enables portability of virtual servers between physical servers

Increases security of physical host server

Kernel-Level Attacks and Security Tools



Hypervisor Based Approaches



- Hypervisor has higher privilege than guest kernel
- Security VM is separated from User VM
- Introspection is used to access contents of user VM
- Active monitoring places hooks and invokes security monitor.

VirtualBox Security Quiz

Which of the following steps is considered safe when working with virtual machines?

- [ ] Set the clipboard sharing between the VM and the host to bidirectional.
- [ ] Allow the VM to read and write files on the host machine with the same privileges as the host machine.
- [x] Disconnect the VM from the internet when opening questionable files.

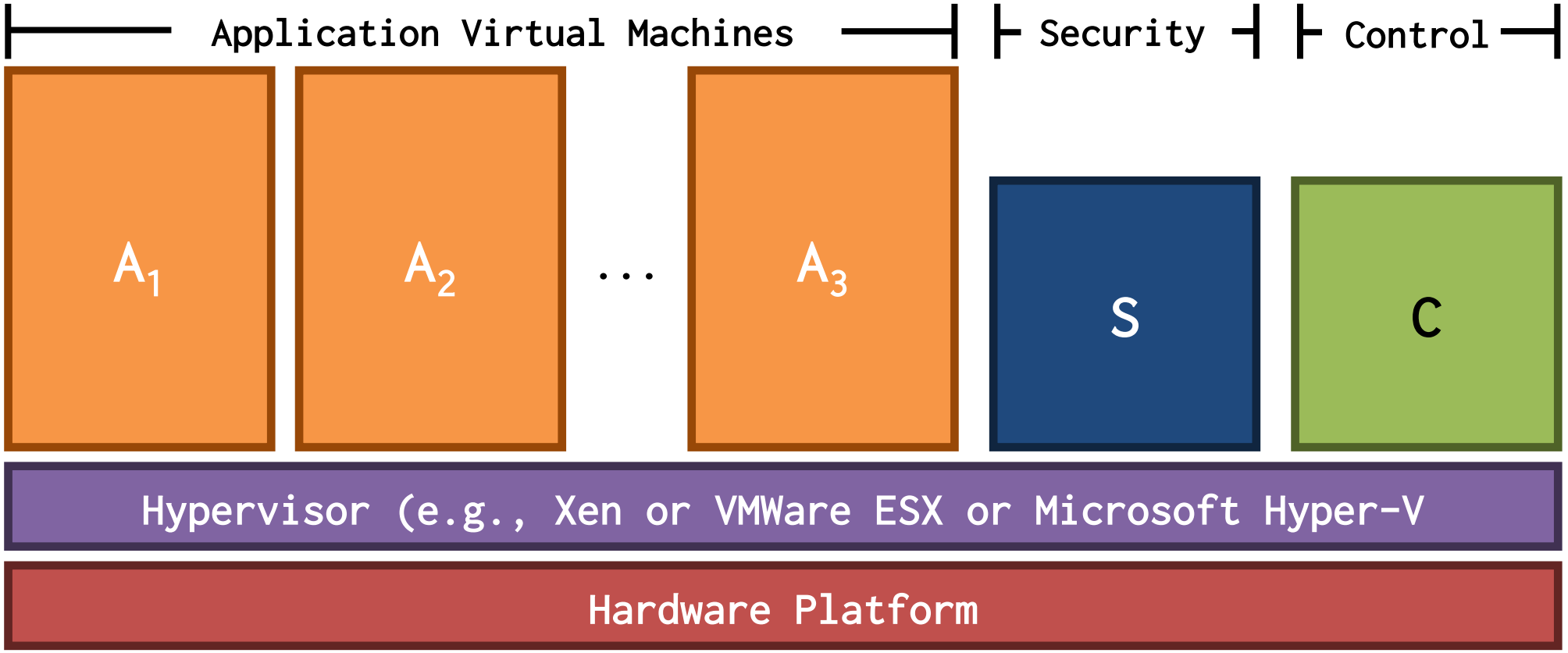
Monitoring Memory

The only reliable source on the current state of a computer system is memory

Nearly endless data for security, forensics, etc

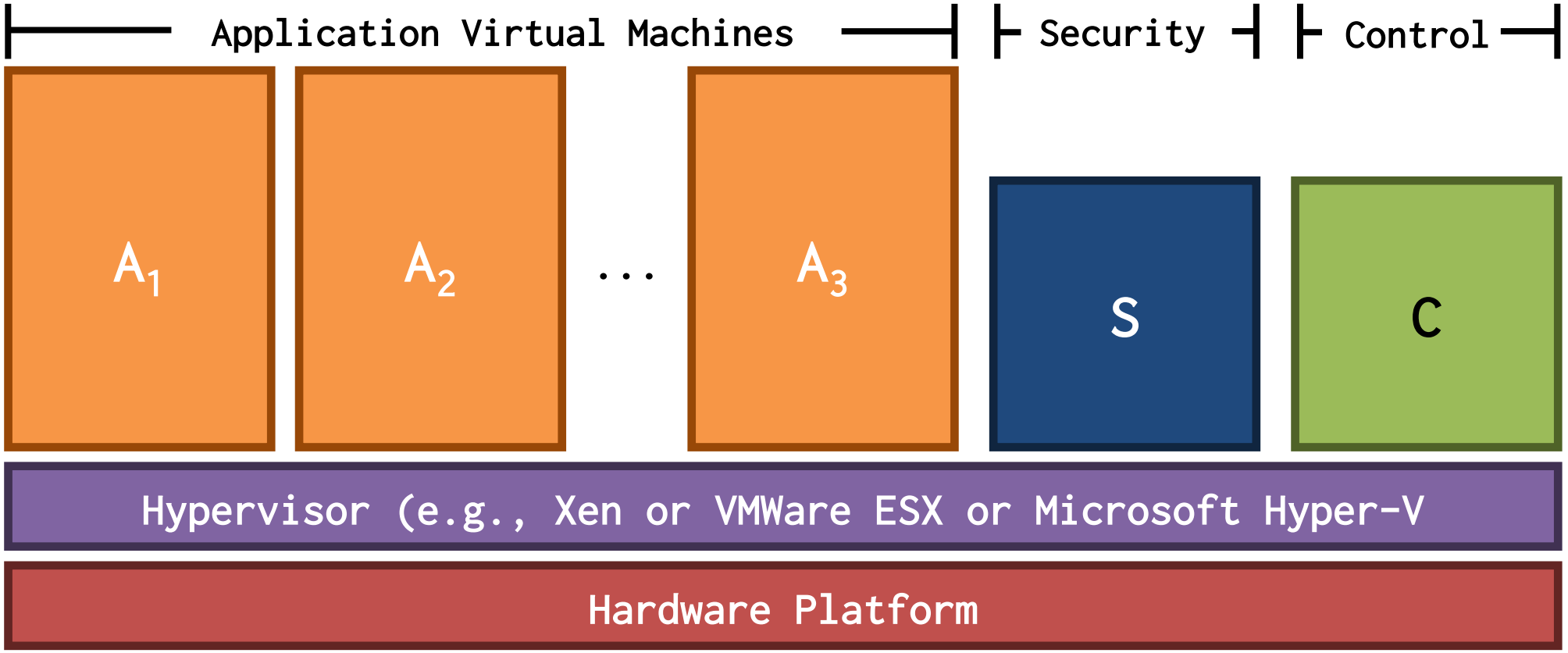
- Running and (some) killed processes
- Encryption keys and decrypted data
- Network sockets and data
- OS-level accounting information
- User input (e.g., key strokes, mouse movement)
- Screen captures and graphical elements
- And much more …

Monitoring Memory: Production Level Systems



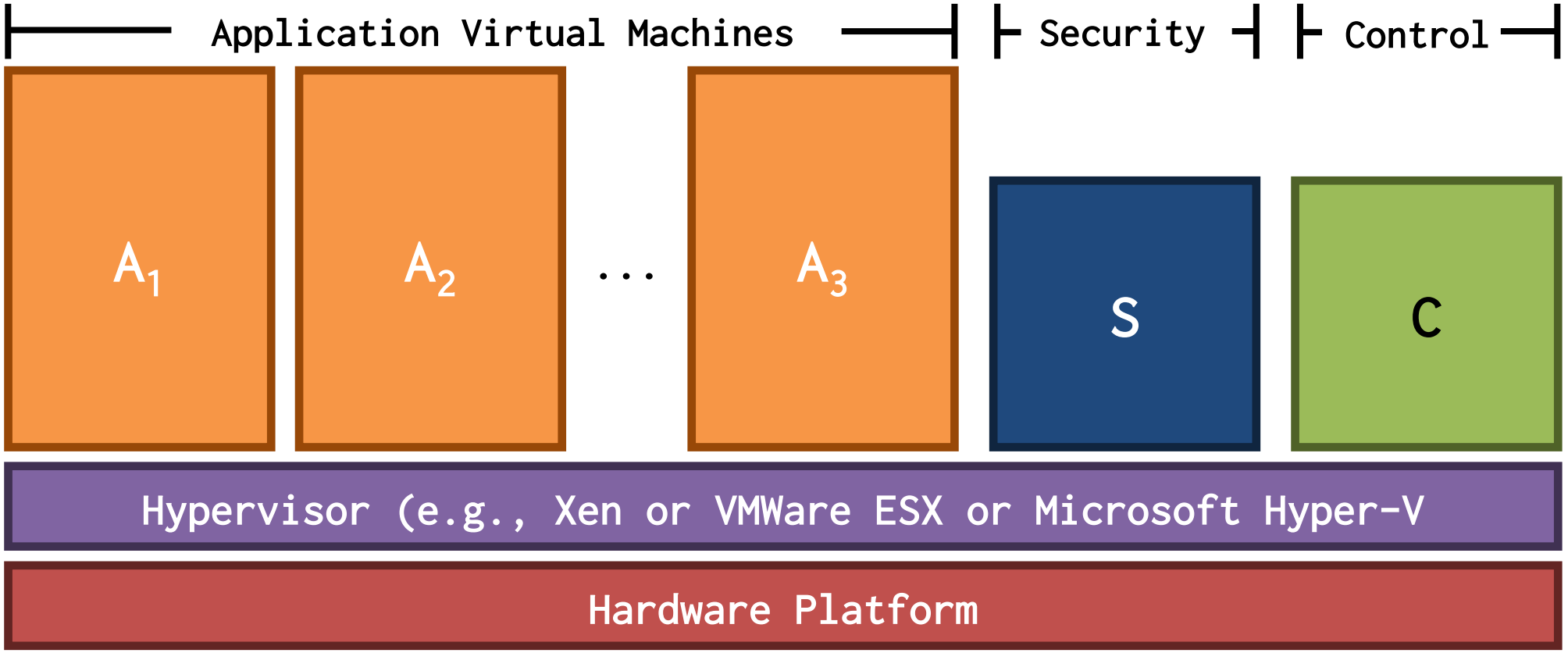
Passive Monitoring: (1) Viewing memory in A_n from S without any timing synchronization between the two virtual machines

Monitoring Memory: Production Level Systems



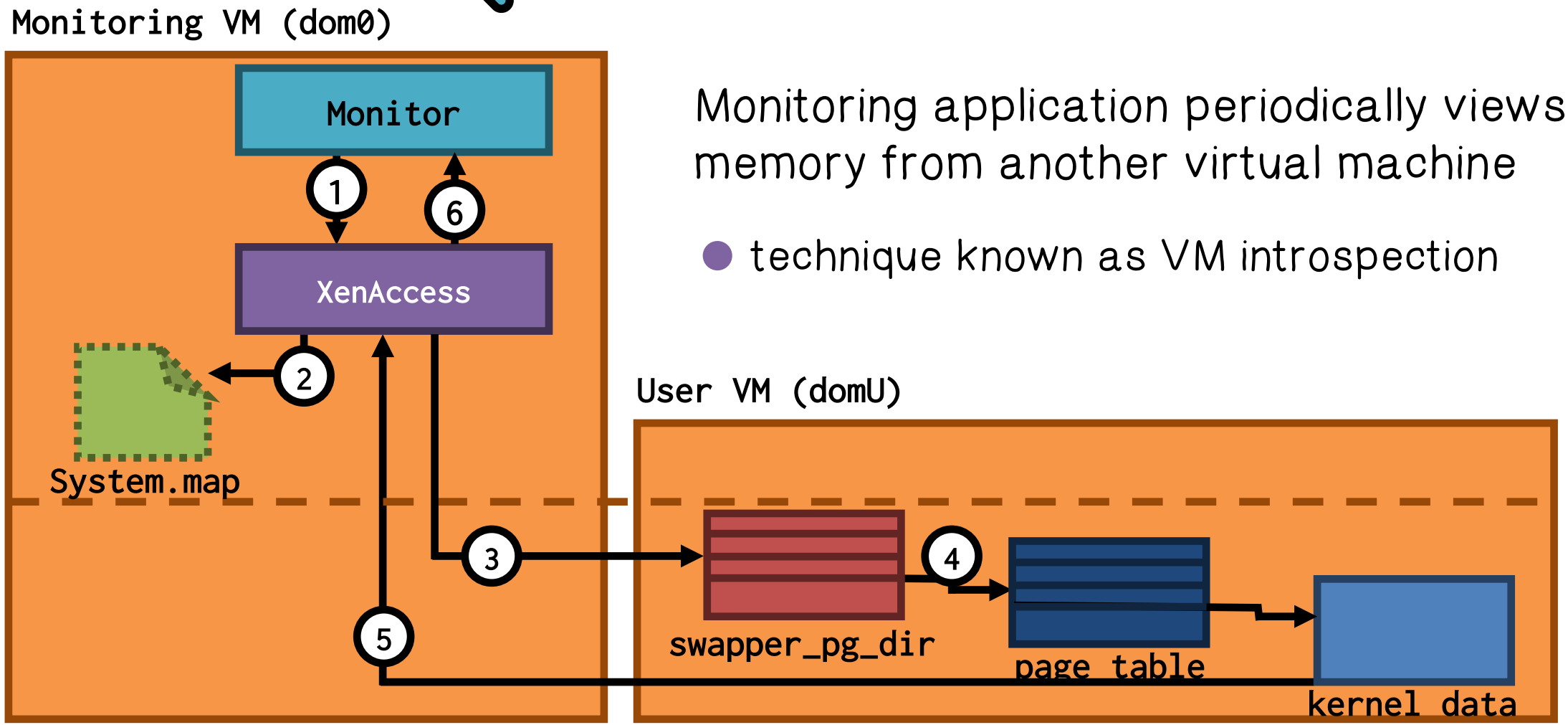
Active Monitoring: Viewing memory in A_n from S with event notification being sent from A_n to S to permit monitoring at relevant times

Monitoring Memory: Production Level Systems



Locating Valuable Data: find critical data structures within the raw memory view for the monitoring task

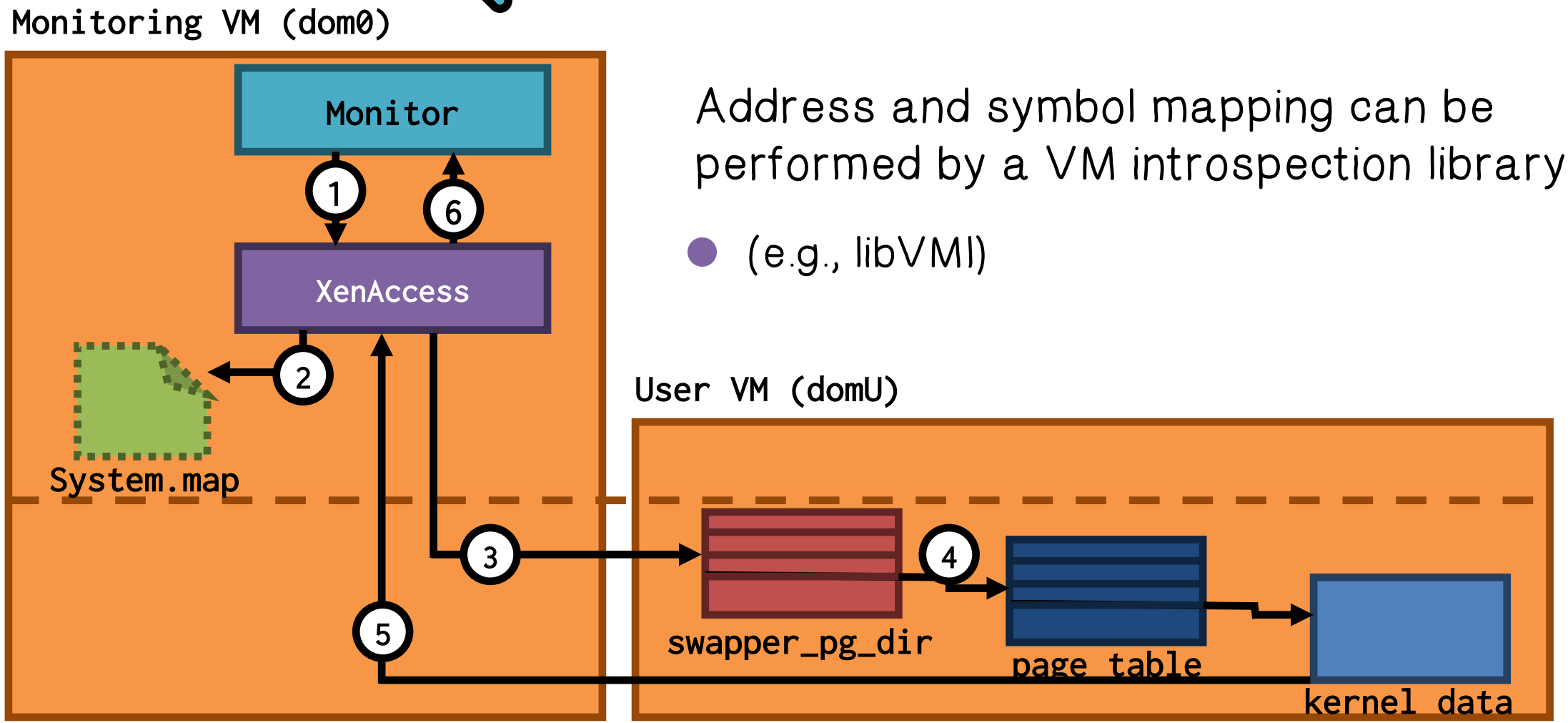
Passive Monitoring



Monitoring application periodically views memory from another virtual machine

- technique known as VM introspection

Passive Monitoring



Address and symbol mapping can be performed by a VM introspection library

- (e.g., libVMI)

Understanding Memory Contents

0001010111010111010100101100110010111000111010111000111010100011101011111001010
0001101001100010001101000111011101011011001000101011010111010100101100110010100
1100011101011100011101010001110101111001010000110100110001000110100011101110100
0110110010001010110101110101001011001100101110001110101110001110101000111010100
1110010100001101001100010001101000111011101011011001000101011010111010100101100
0011001011100011101011100011101010001110101111001010000110100110001000110100000
1110111010110110010001010110101110101001011001100101110001110101110001110101000
0011101011110010100001101001100010001101000111011101011011001000101011010111010
1010010110011001011100011101011100011101010001110101111001010000110100110001000
0011010001110111010110110010001010110101110101001011001100101110001110101110000
0111010100011101011110010100001101001100010001101000111011101011011001000101011
1101011101010010110011001011100011101011100011101010001110101111001010000110100
0011000100011010001110111010110110010001010110101110101001011001100101110001100
1010111000111010100011101011111001010000110100110001000110100011101110101101100
0100010101101011101010010110011001011100011101011100011101010001110101111001000
1000011010011000100011010001110111010110110010001010110101110101001011001100100
0111000111010111000111010100011101011110010100001101001100010001101000111011100
0101101100100010101101011101010010110011001011100011101011100011101010001110100
0111100101000011010011000100011010001110111010110110010001010110101110101001000
1100110010111000111010111000111010100011101011110010100001101001100010001101000
0011101110101101100100010101101011101010010110011001011100011101011100011101000
1000111010111100101000011010011000100011010001110111010110110010001010110101100
1010100101100110010111000111010111000111010100011101011110010100001101001100000
10001101000111

```
root@bluemoon:/home/bdpayne/
File  Edit  View  Terminal  Tabs  Help
[root@bluemoon examples]# ./process-list 1
[    4] System
[  420] smss.exe
[  468] csrss.exe
[  496] winlogon.exe
[  540] services.exe
[  552] lsass.exe
[  700] svchost.exe
[  760] svchost.exe
[  828] svchost.exe
[  876] svchost.exe
[  924] svchost.exe
[ 1220] spoolsv.exe
[ 1792] alg.exe
[ 1876] wscntfy.exe
[ 1952] explorer.exe
[  140] ctfmon.exe
[ 1924] procexp.exe
[root@bluemoon examp
```

```c
/* initialize the xen access library */
xa_init(dom, &xai);

/* get the head of the list */
xa_read_long_sym(&xai, "PsInitialSystemProcess", &list_head);
memory = xa_access_virtual_address(&xai, list_head, &offset);
memcpy(&next_process, memory + offset + ActiveProcessLinks_OFFSET, 4);
list_head = next_process;

/* print out the first process */
name = (char *) (memory + offset + ImageFileName_OFFSET);
memcpy(&pid, memory + offset + UniqueProcessId_OFFSET, 4);
printf("[%5d] %s\n", pid, name);
munmap(memory, xai.page_size);

/* walk the process list */
while (1){
    /* follow the next pointer */
    memory = xa_access_virtual_address(&xai, next_process, &offset);
    memcpy(&next_process, memory + offset, 4);

    /* if we are back at the list head, we are done */
    if (list_head == next_process){
        break;
    }

    /* print out the next process */
    name = (char *) (memory + offset + ImageFileName_OFFSET -
           ActiveProcessLinks_OFFSET);
    memcpy(&pid, memory + offset + UniqueProcessId_OFFSET -
           ActiveProcessLinks_OFFSET, 4);
    printf("[%5d] %s\n", pid, name);
    munmap(memory, xai.page_size);
}

/* cleanup */
xa_destroy(&xai);
```

libVMI Library

- Open source VM introspection library
- Access to virtual addresses, kernel symbols, and more
- Released in Spring 2006
- Started as XenAccess at Georgia Tech
- https://github.com/libvmi/libvmi

libVMI Library

Read and write VM memory

Virtual memory translation

- Using various methods (DTB, PTD, Kernel Symbol)

Find and map guest OS data structures

Place monitoring event-hooks into the guest

- Exceptions, page faults, etc.

Events on Xen on Intel CPUs

Pause guest and transfer control to callback function (hook)

Memory r/w/x events on defined regions

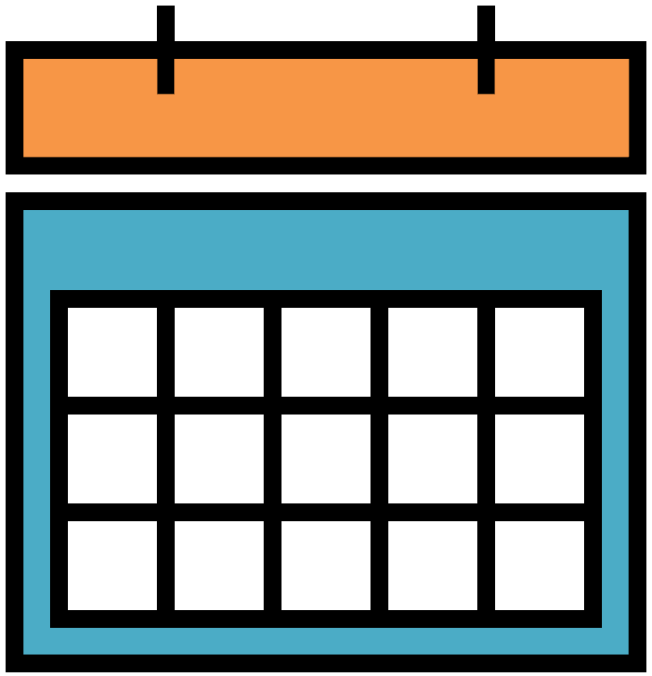
Register r/w events CR0/CR3/CR4/MSR registers

Interrupt events

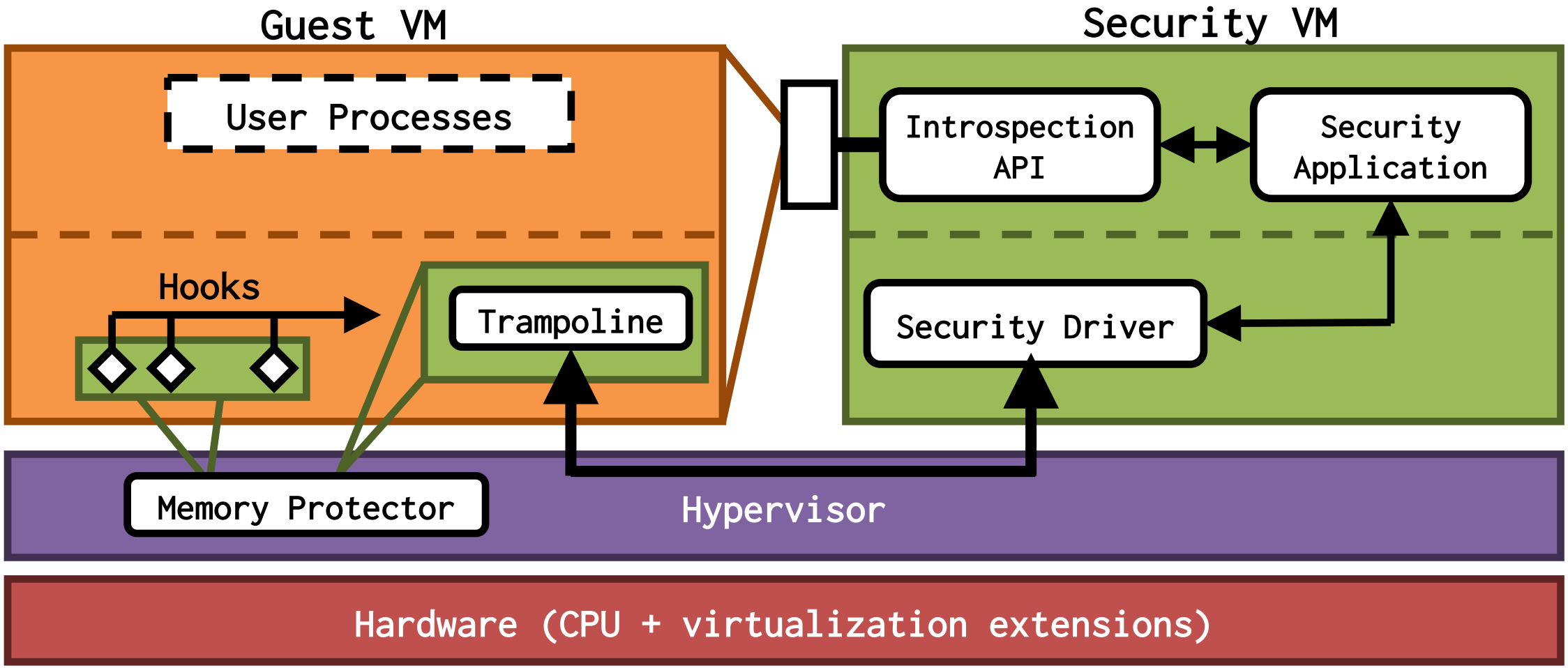
Single step through instructions

Active Monitoring

- Event Driven
  - Enforcing security policy
  - Preventing attacks

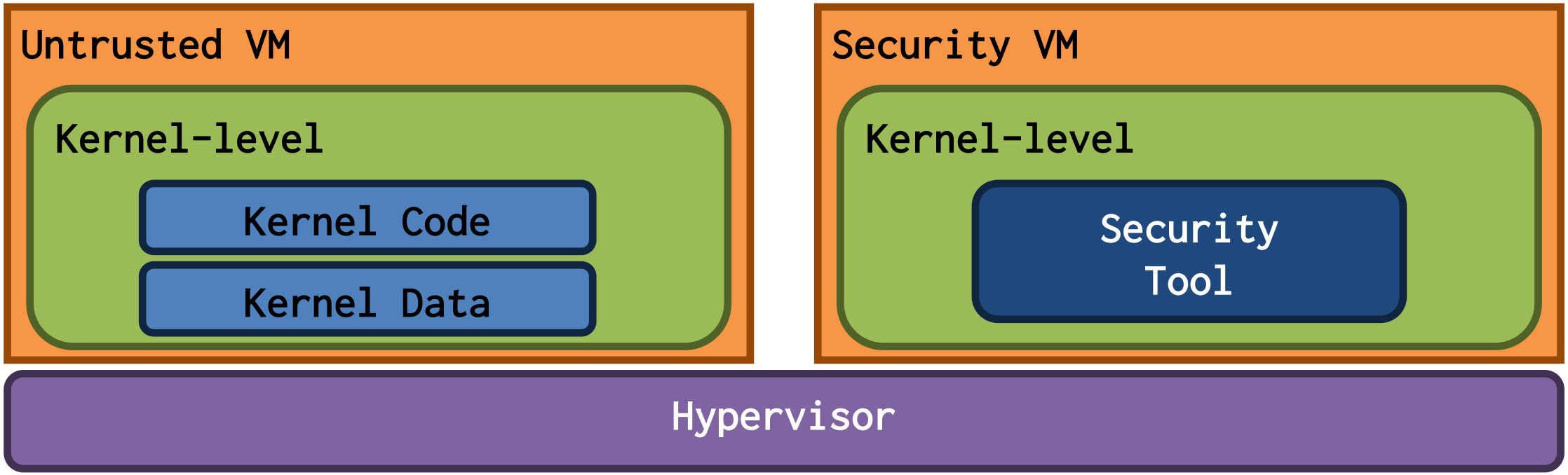


Active Monitoring



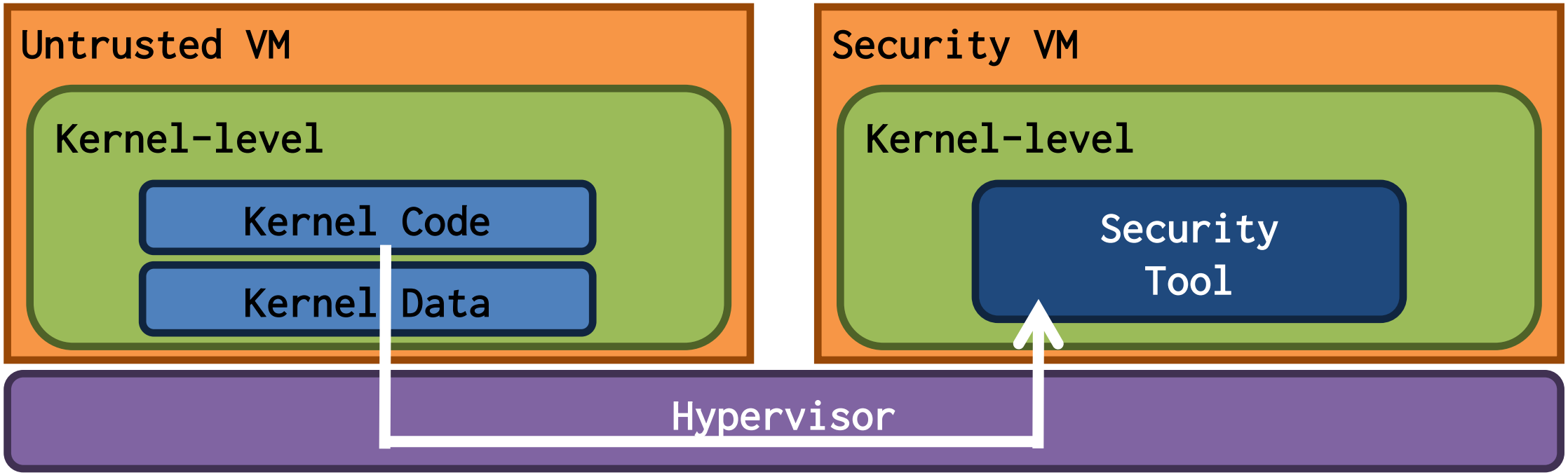
VM Monitoring: Challenge

High Overhead



VM Monitoring: Challenge

High Overhead

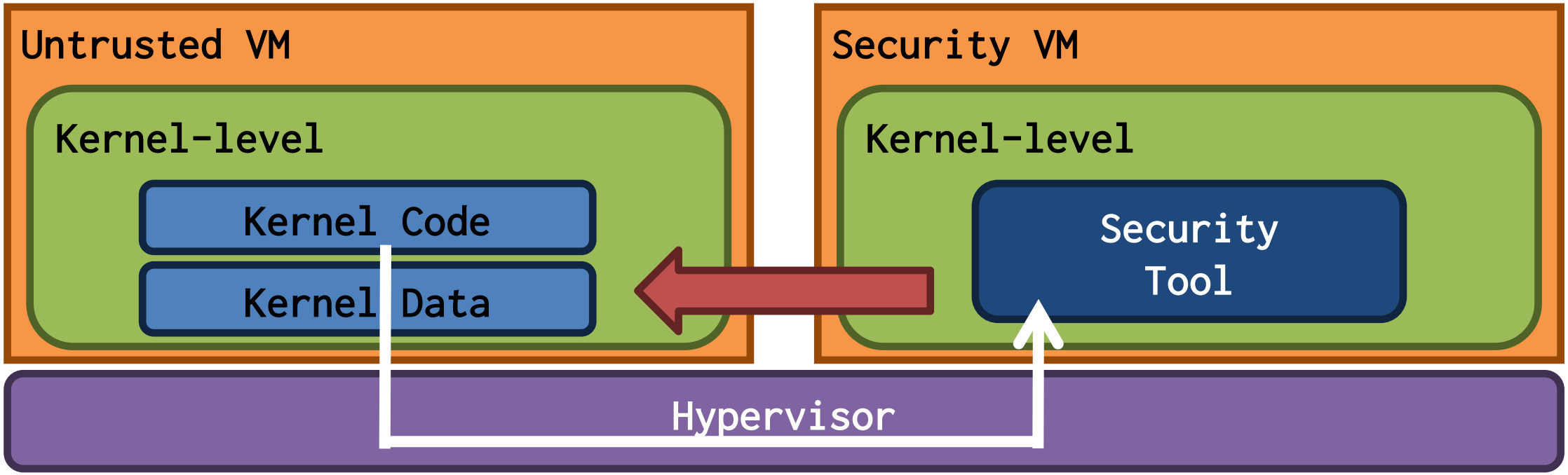


Invocation Cost:

- Requires switching to hypervisor when security tool is invoked
- Especially for fine-grained monitoring

VM Monitoring: Challenge

High Overhead



Introspection Cost:

- Accessing untrusted VM memory requires calls to hypervisor for mapping pages to security VM

Secure In-VM Monitoring (SIM)

Bringing security to traditional in-VM approaches

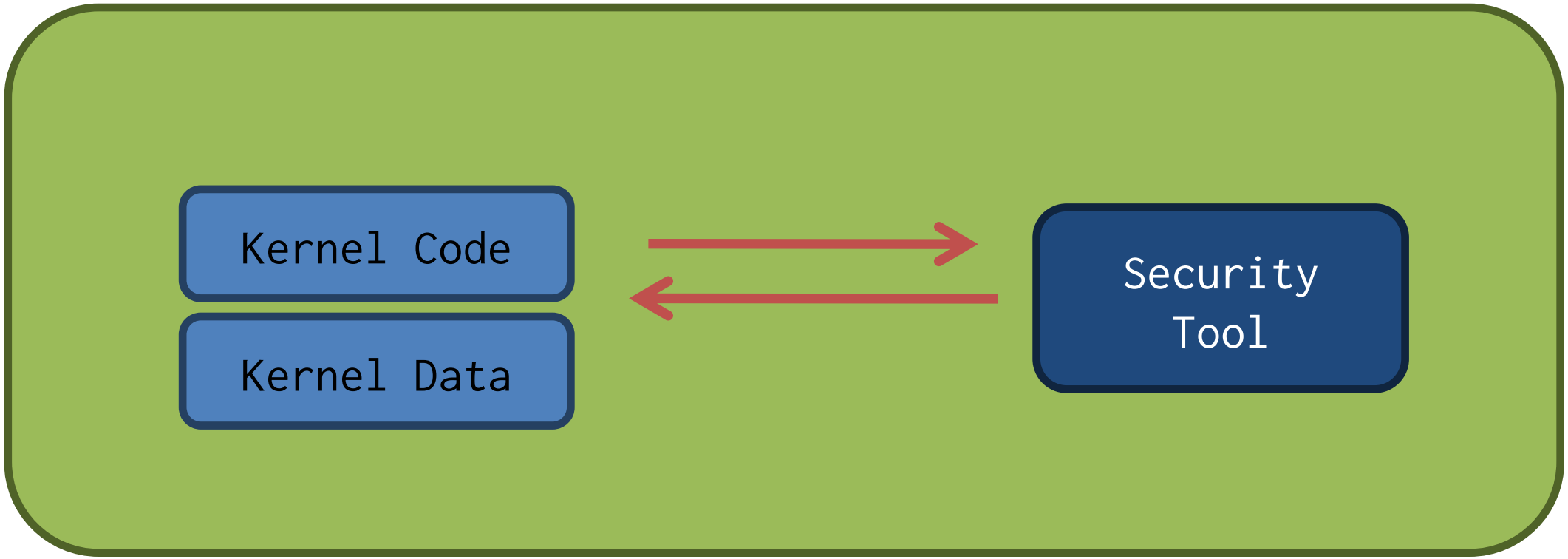
Addresses security and performance requirements together

- Same security as out-of-VM approaches
- Performance close to traditional in-VM approaches

Utilize hardware virtualization features

- No hypervisor intervention during monitor invocation
- Untrusted VM Reads/writes are at native speed

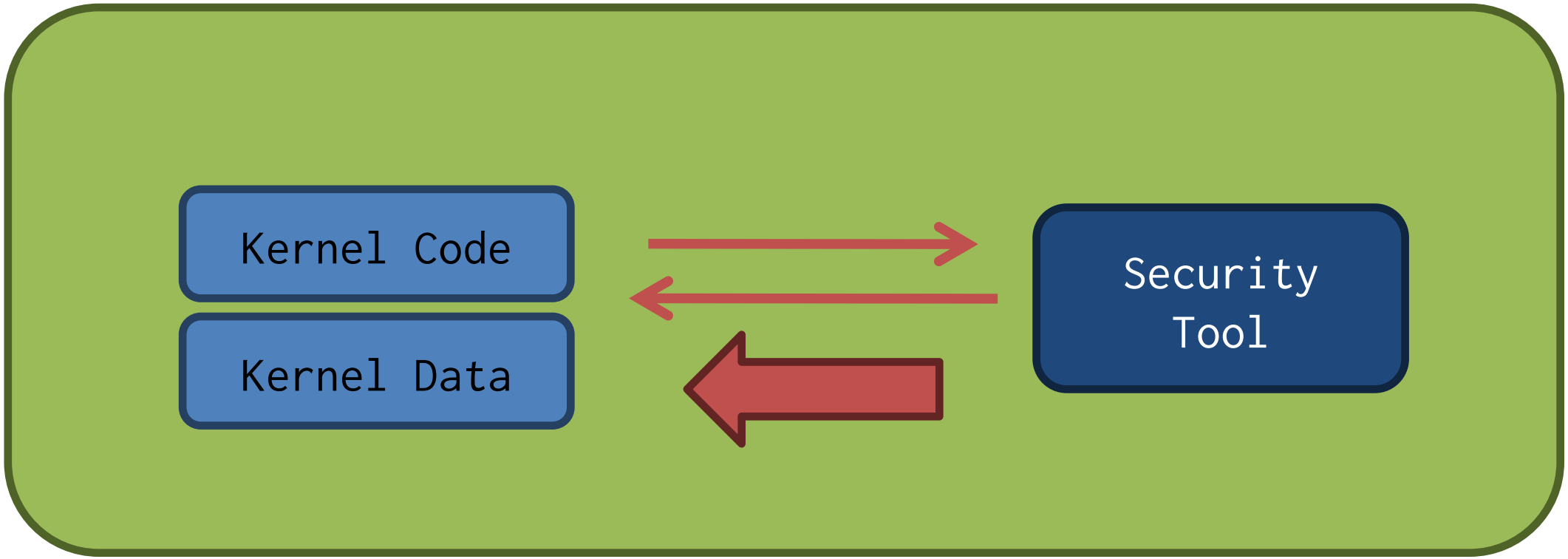
SIM Performance Requirements



Fast Invocation

- Invocation of monitor happens without any privilege changes

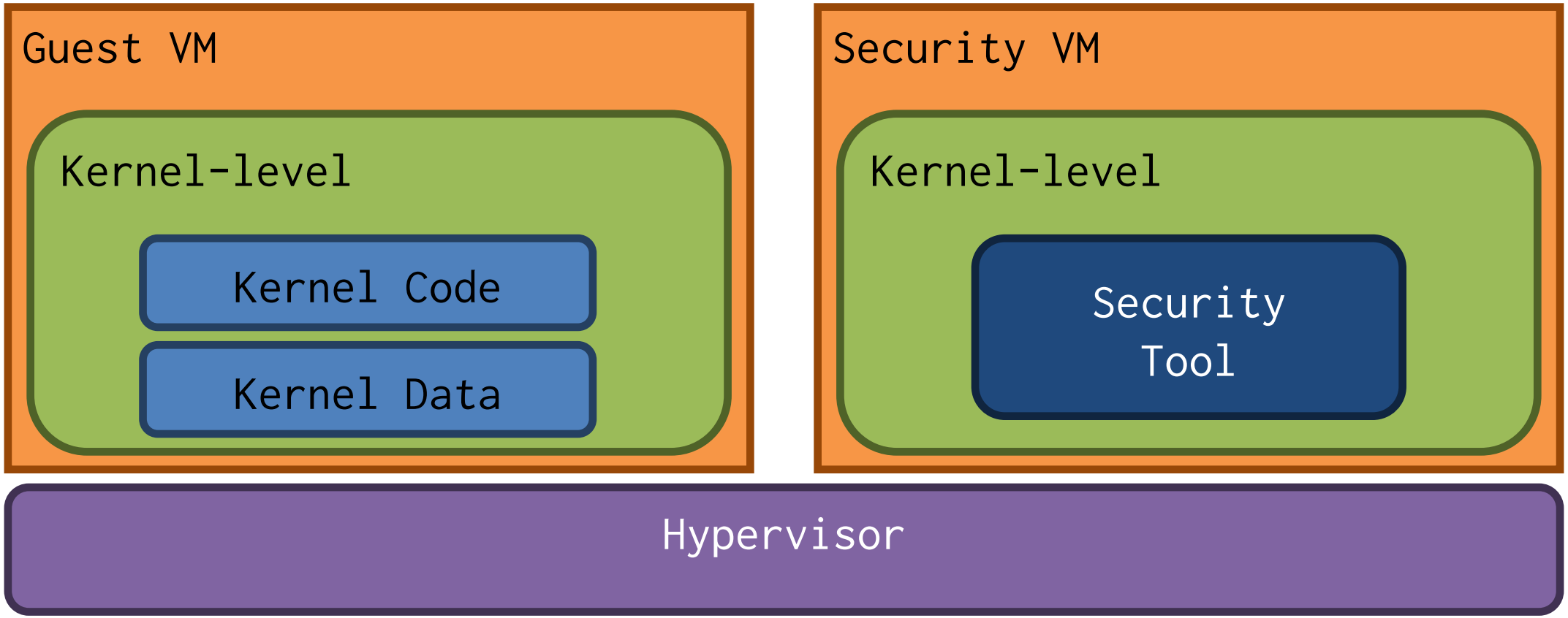
SIM Performance Requirements



Data read/write at native speed

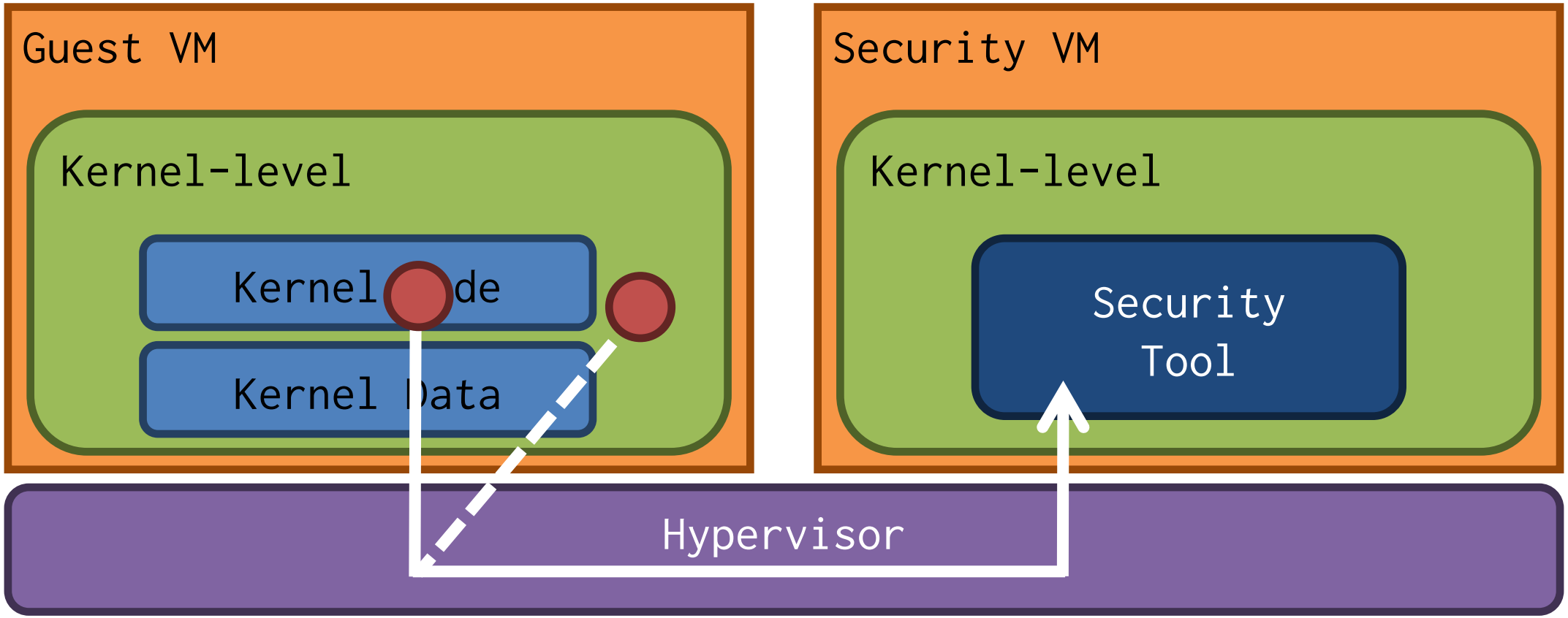
- Native instructions should be able to read/write data directly

SIM Security Requirements



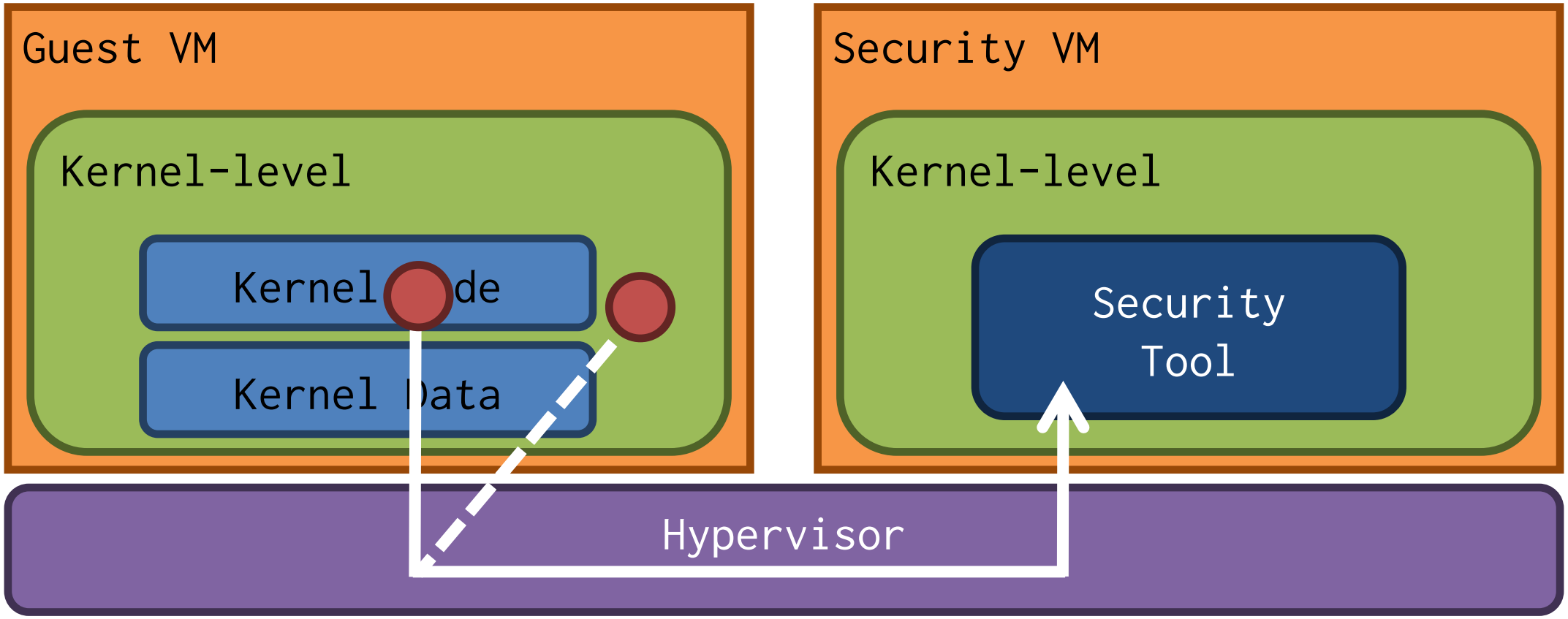
Isolation of monitor code and data

SIM Security Requirements



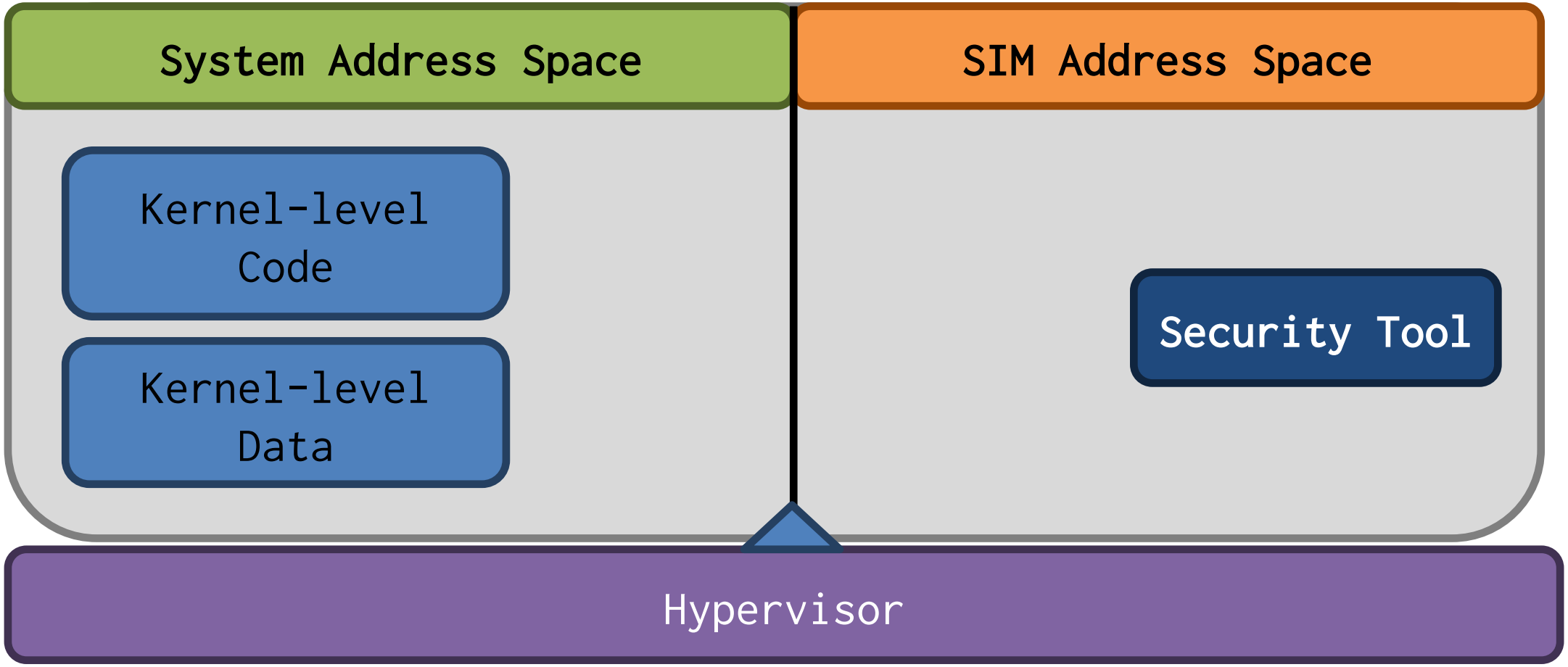
Secure invocation for event-handling

SIM Security Requirements



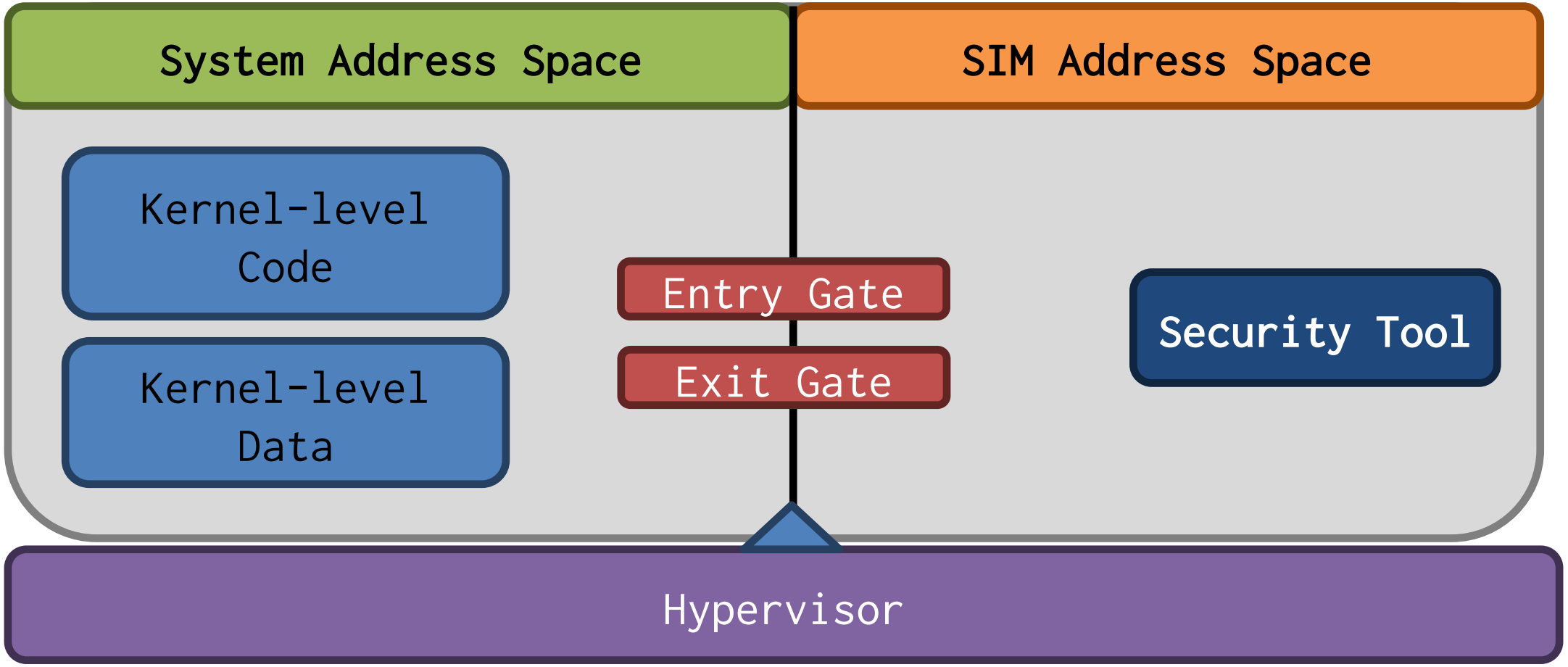
Monitor's execution does not rely on untrusted code and data

SIM Design



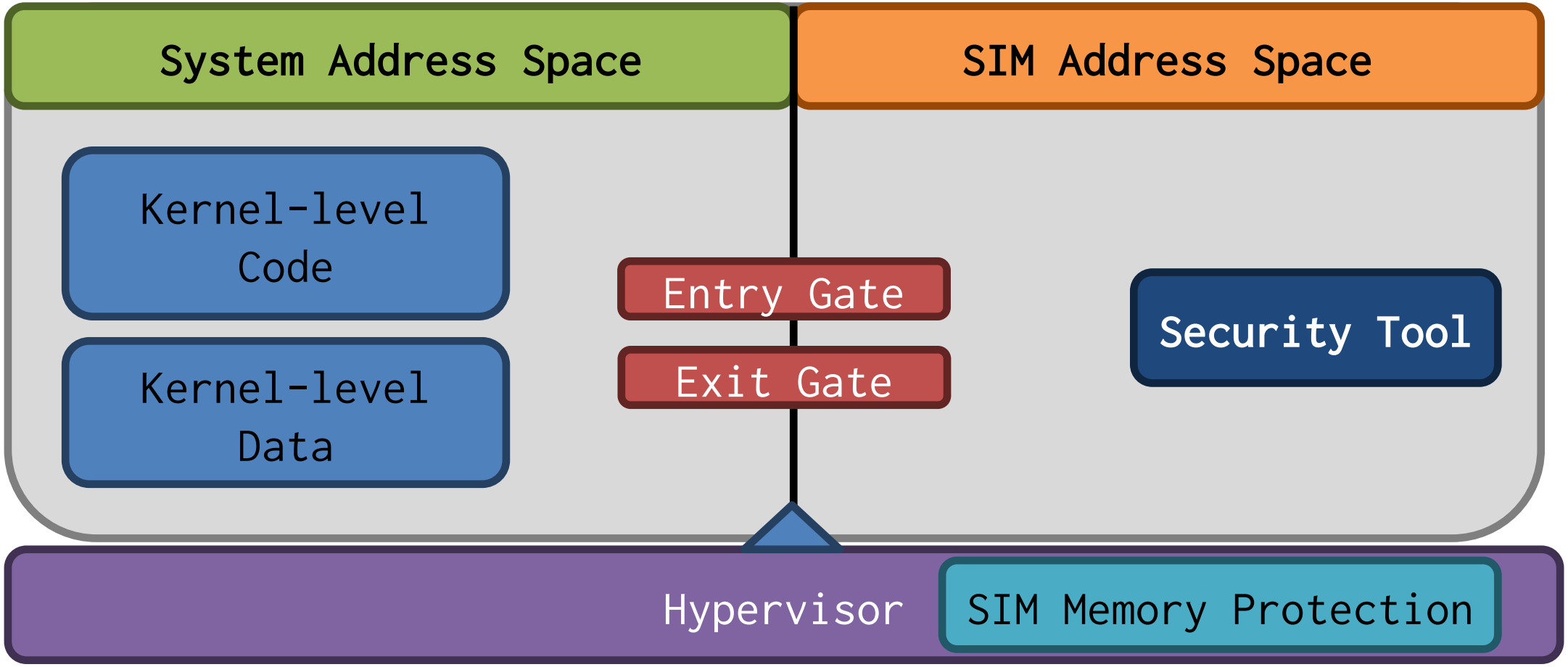
Security Requirement: Isolation – by using separate paged virtual addresses

SIM Design



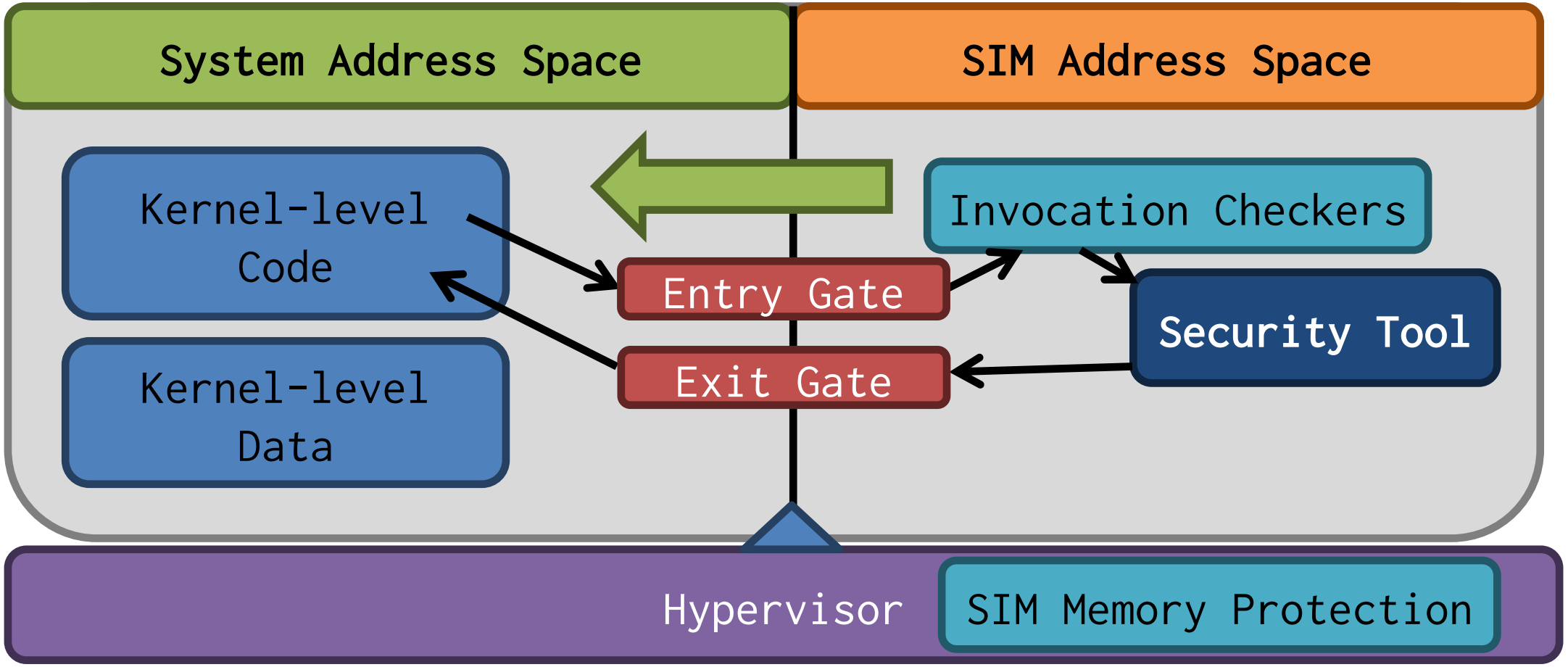
Performance Requirement: Fast invocation – no hypervisor intervention

SIM Design



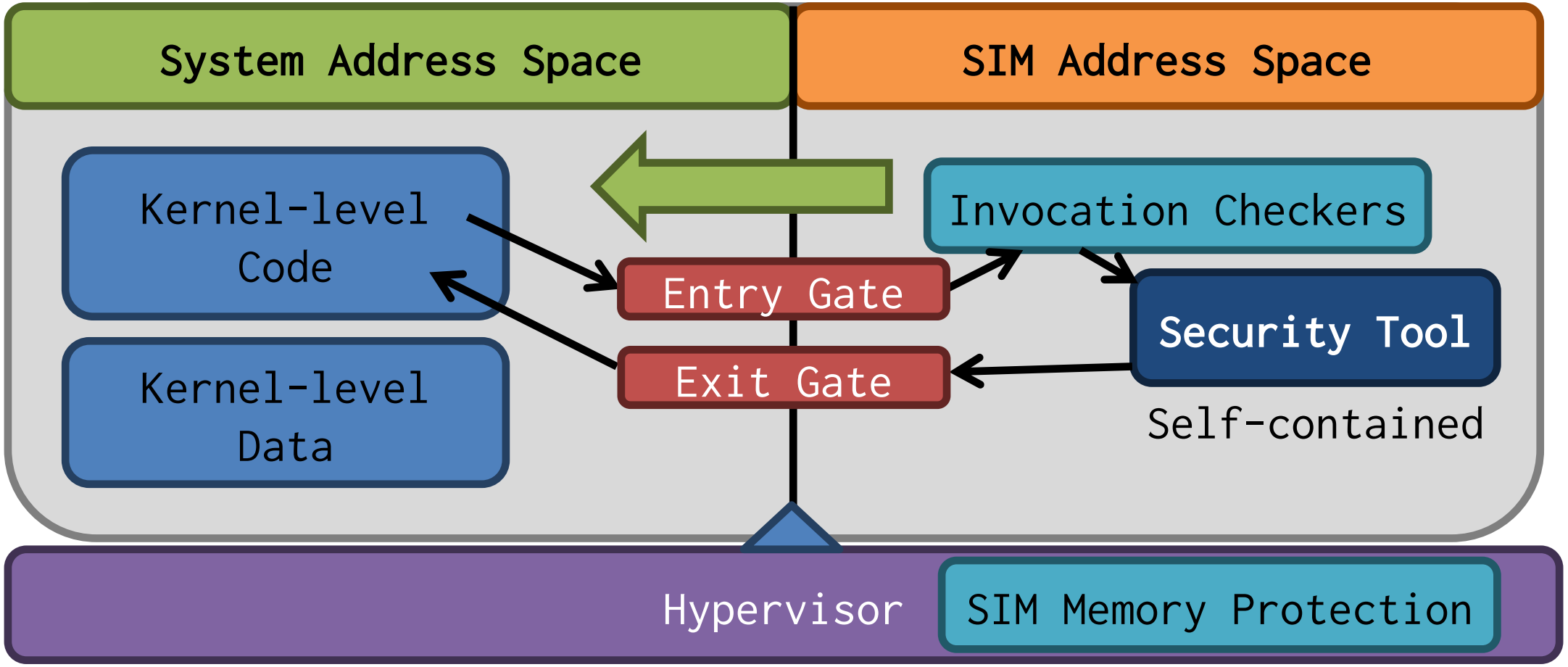
Performance Requirement: Fast invocation – no hypervisor intervention

SIM Design



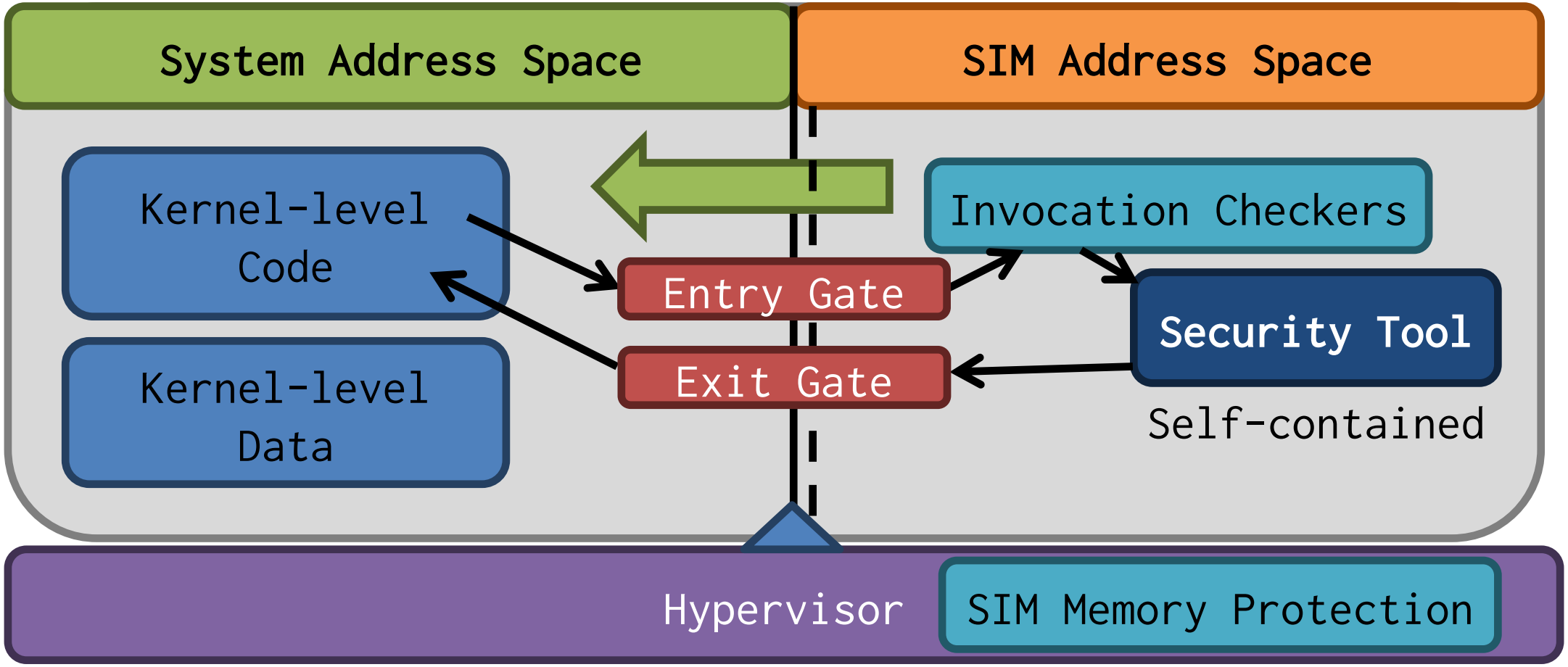
Security Requirement: Secure invocation for event handling

SIM Design



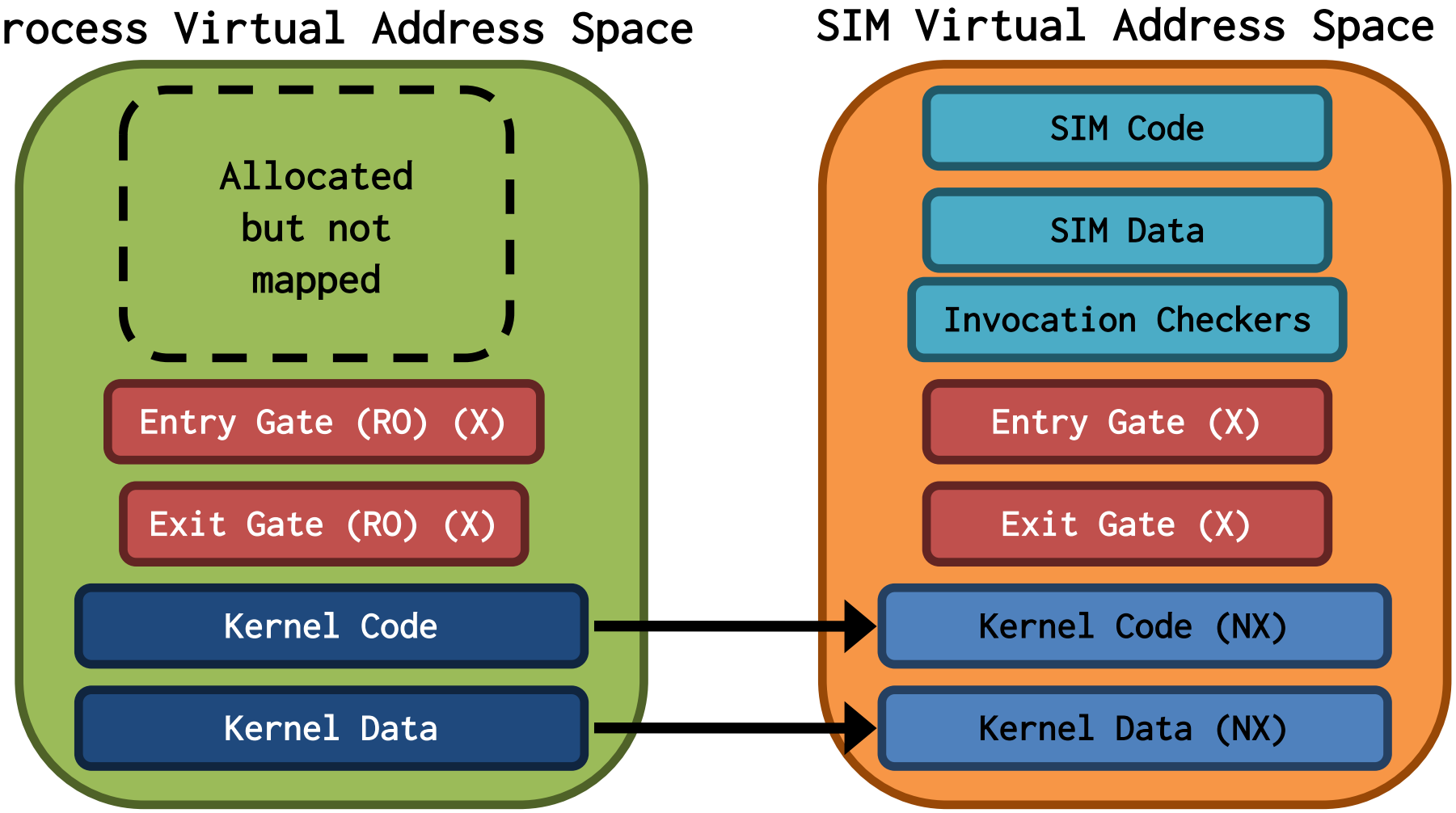
Security Requirement: Monitor's code does not rely on anything untrusted

SIM Design



Performance Requirement: Native read/writes

Protected Address Space Generation



Monitor Invocation Overhead

Micro benchmarking

- Measure time required between executing hook and returning back from SIM monitor
- Use null handlers, so that only switching time is measured

Monitor Invocation Overhead

Monitor Type	Avg. time (u sec)	Std. dev (u sec)
SIM approach	0.469	0.051
Out-of-VM approach	5.055	0.132