Cyber Security 0101

RMUTT

CH5
Securing Hosts and Data

CompTIA Security+

0100010101111000011100000110110001101111011100100110100101101
1100110011100100000010000110110111101101110011101000111001001
1011110110110000100000010101000111100101110000011001010111001
1100100000011000010110111001100100001000000100110101100101
0111010001101000011011110110010001110011

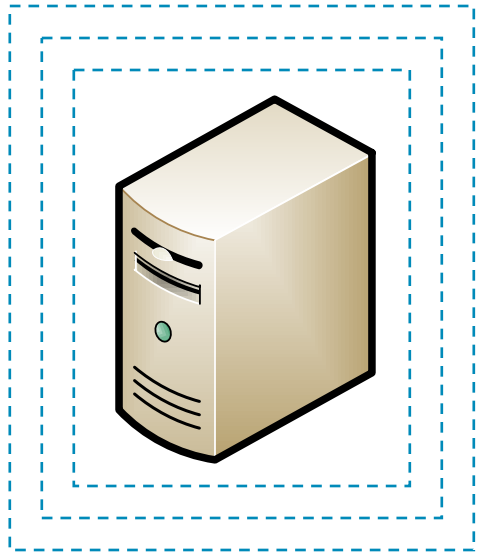
Introduction

1. Implementing secure systems
2. Summarizing cloud concepts
3. Deploying mobile devices securely

Implementing Host Security

- **Least functionality** ต้นแบบสิทธิ์
  - Disabling unnecessary services
    - Improves security posture
    - Reduces attack surface
    - Reduces risks from open ports
  - Disabling unneeded applications
  - Disabling unnecessary accounts
  - Keeping systems up-to-date

อัพเดท สม่ำเสมอ

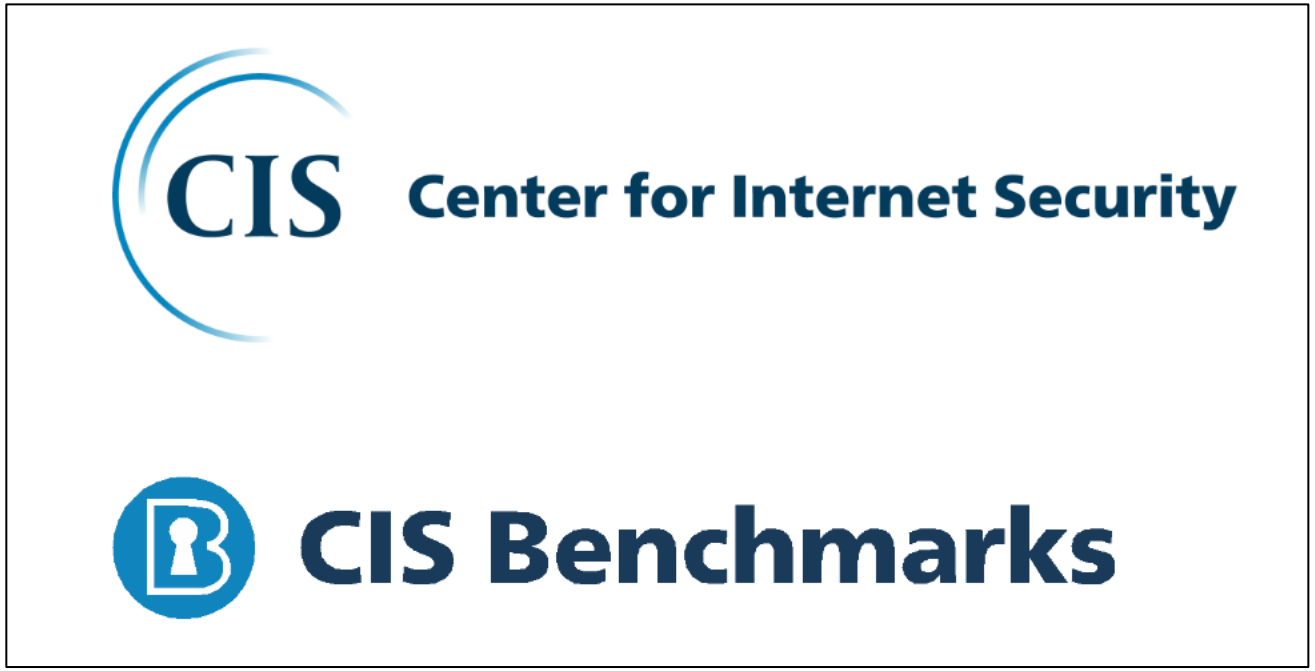


Admin
web service1
web service2

แบ่งสิทธิ์ที่จำเป็นให้

Window จะมี Guest เป็น Default
ต้อง Disable ทิ้ง

Baselines



https://downloads.cisecurity.org

Baselines

Using Baselines

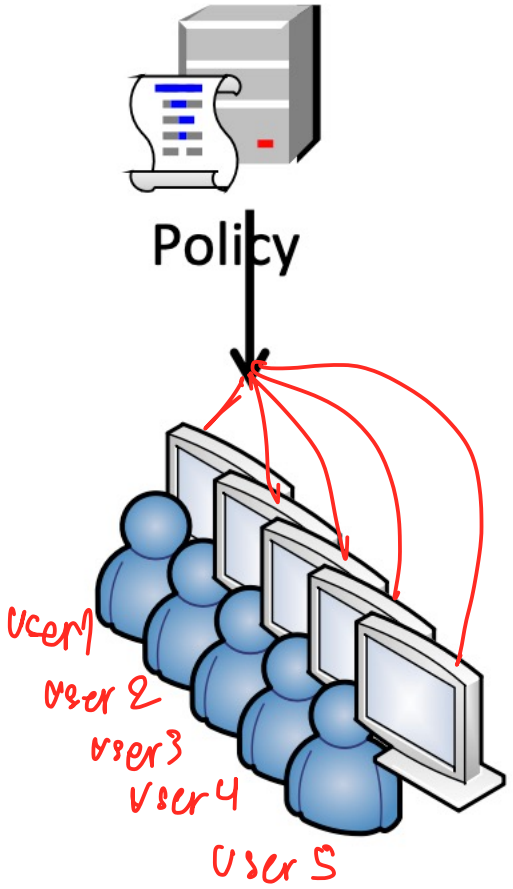
- Improve overall security posture
- Three steps

1. Initial baseline configuration Start in secure state
2. Continuous security monitoring Scan for and detect changes
3. Remediation Isolate or quarantine modified systems

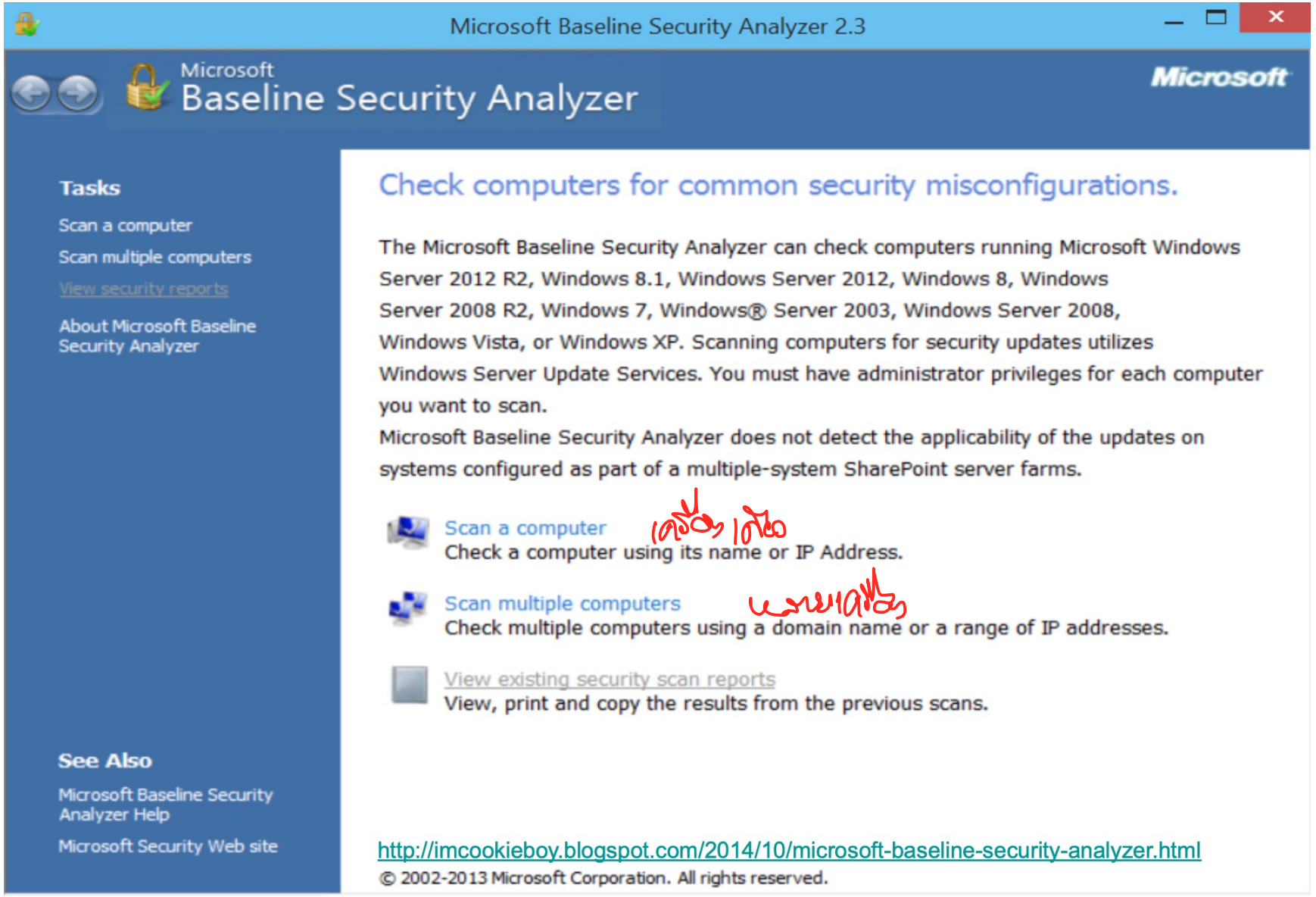
Baselines

- Enforce with Group Policy
- Standardize system configuration
- Standardize security settings
- Enforce strict company guidelines
- Easily apply security settings to multiple computers

- Account Policies
- Local Policies
- System Services
- Software Restrictions

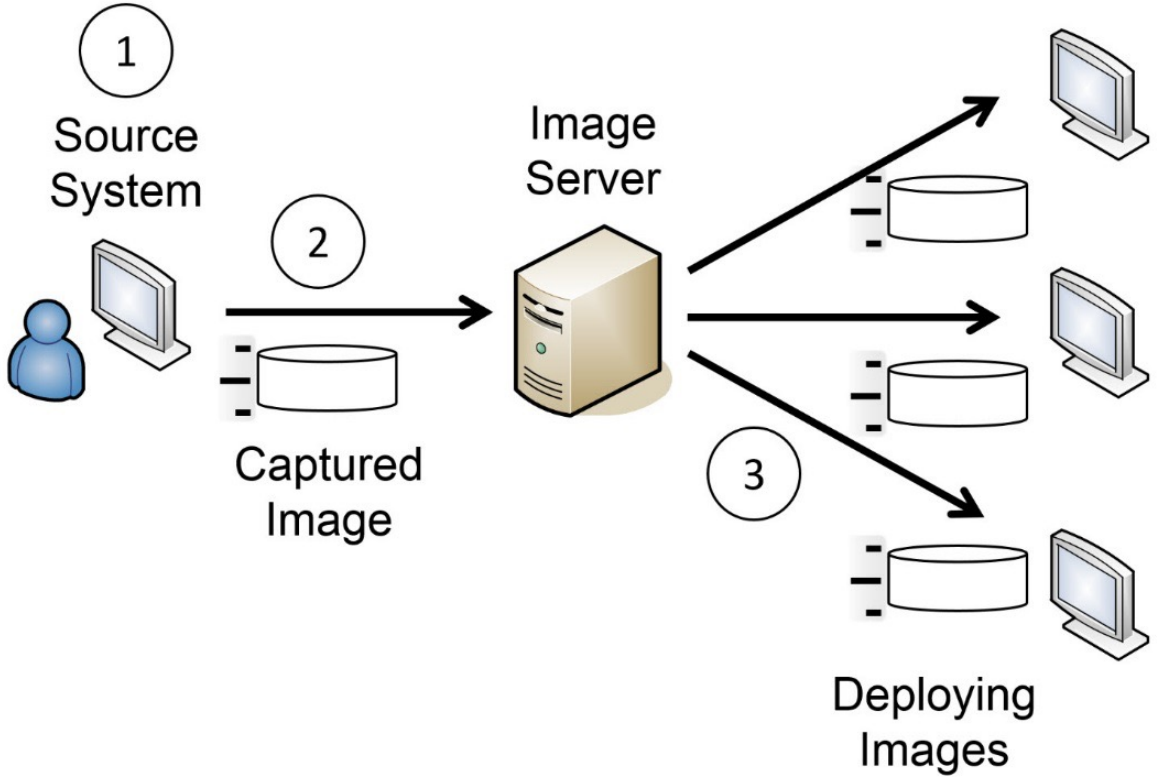


Scan Baselines



Using Master Images

- Provides secure starting point
- Reduces costs



Backup vs Snapshot

Image backup vs Snapshot

These are two different concepts.

- An image backup refers to a semi-traditional backup where data is being backed up from disk to (probably) tape. The only difference is that the data is being backed up via the raw device instead of via the filesystem.

- A snapshot on the other hand, could be considered a type of mirror that is different than a traditional backup. It is on disk and appears to be another copy of your filesystem or device. However, in most cases, it is a virtual copy, that relies on the original for data.

Implementing Secure Systems

- **Patch management**
  - Ensure that systems are up-to-date but delay (If not urgent)
  - Protects system against known vulnerabilities
  - Test patches in a test environment that mirrors the production environment
  - Automated deployment
  - Testing, deploying and verifying updates
  - Verify an update that compatibilities with service software

Implementing Secure Systems

Change management

- Helps ensure changes to IT systems do not result in unintended outages
- Provides an accounting structure or method to document all changes
- Changes are proposed and reviewed before implementation

Implementing Secure Systems

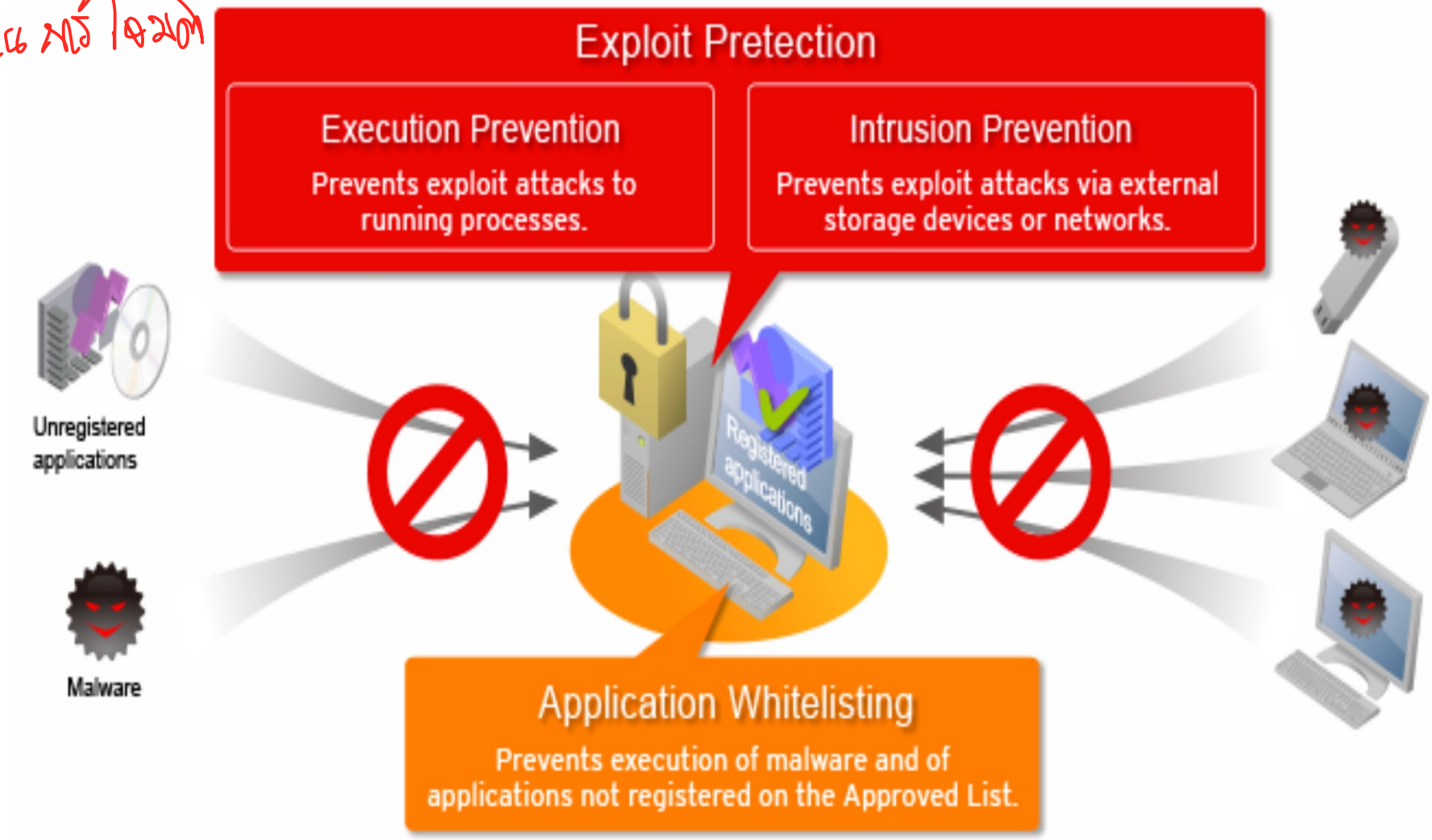
- **Restrict Unauthorized software**
  - Can include malware

- **Compliance violations**
  - Licenses

Whitelisting vs Blacklisting

- Application whitelisting
  - Identifies authorized software for workstations, servers, and mobile devices
  - Prevents users from installing or running software that isn’t on the list
- Application blacklisting
  - A list of prohibited applications
  - Prevents users from installing or running software on the list

Whitelisting vs Blacklisting



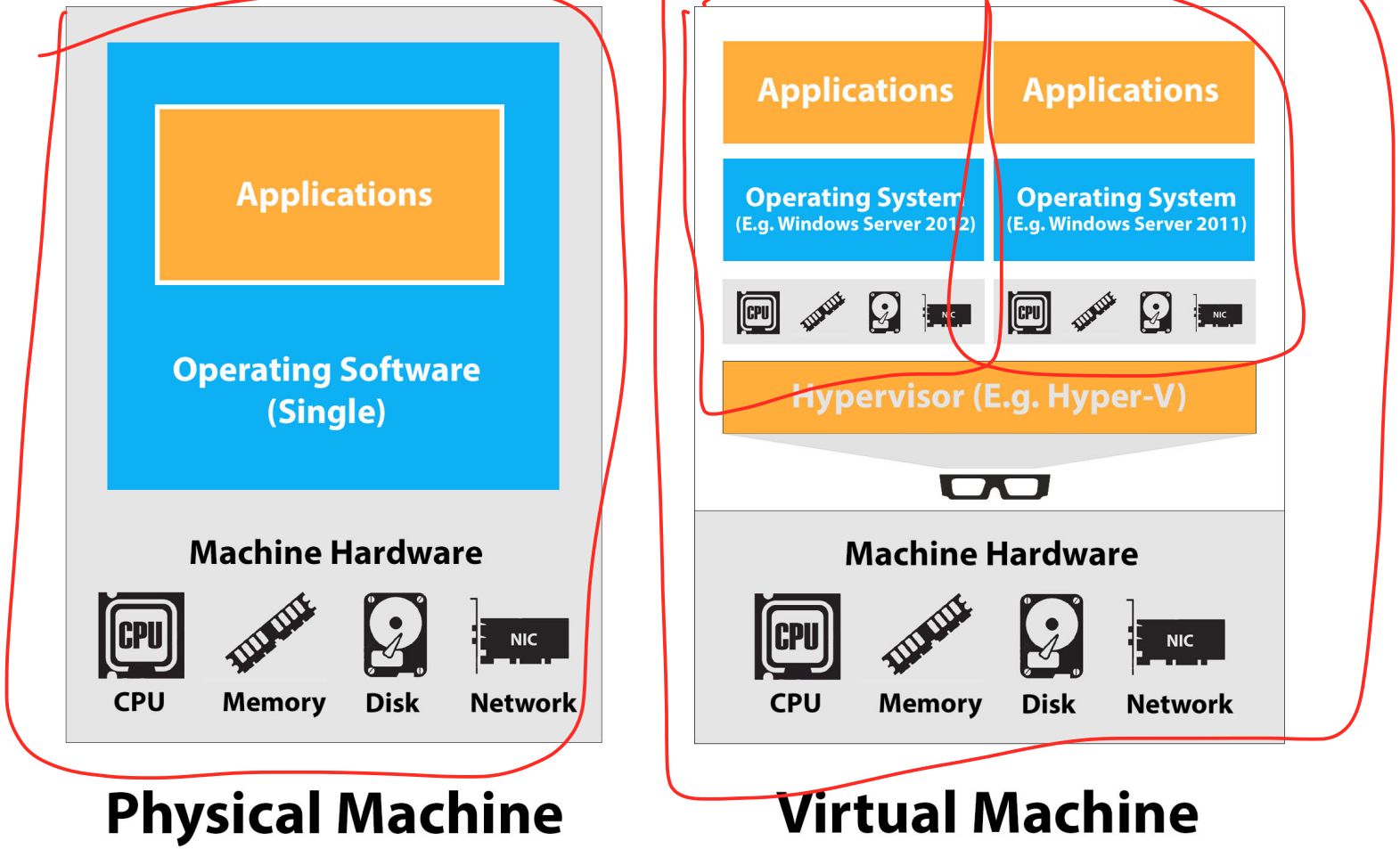
http://apac.trendmicro.com/apac/enterprise/tmsl/

Whitelisting vs Blacklisting

http://apac.trendmicro.com/apac/enterprise/tmsl/

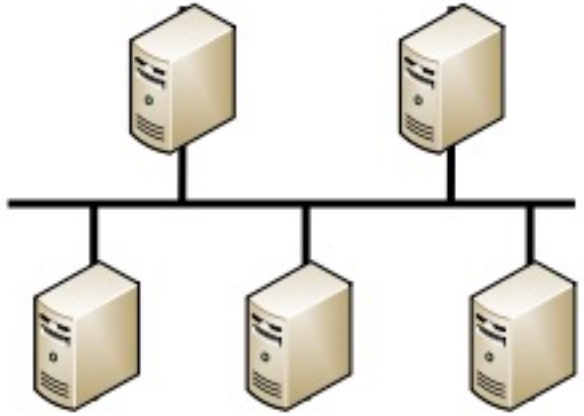
Hypervisor

A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware or hardware that creates and runs virtual machines.



Understanding Virtualization

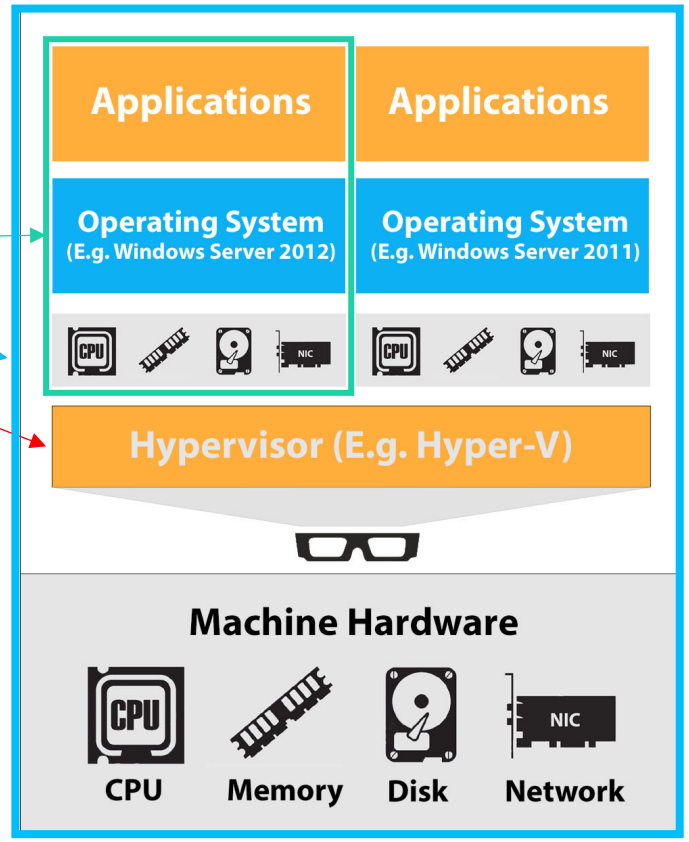
- Multiple virtual systems hosted on physical host system
- Increased availability
- Lower costs
- High level of flexibility
- Used to test security controls, updates, and patches



Understanding Virtualization

Virtualization Concepts

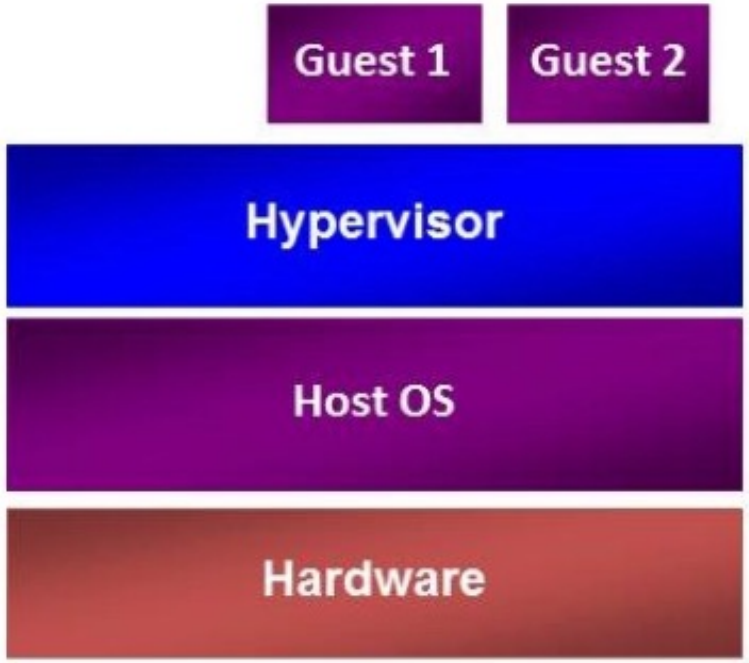
- Hypervisor
- Host
- Guest
- Patch compatibility
- Host availability/elasticity
- Snapshots
- Sandboxing



Hypervisor Design:

Two approaches

(Hosted)
Type 2 Hypervisor



Examples:

- Virtual PC & Virtual Server
- VMware Workstation
- KVM

(Bare metal)(Native)
Type 1 Hypervisor

ไม่มี OS = ประสิทธิภาพสูงกว่า

Examples:

- Hyper-V
- Xen
- VMware ESX

http://sahinerbay.com/author/sahinerbay/page/2/

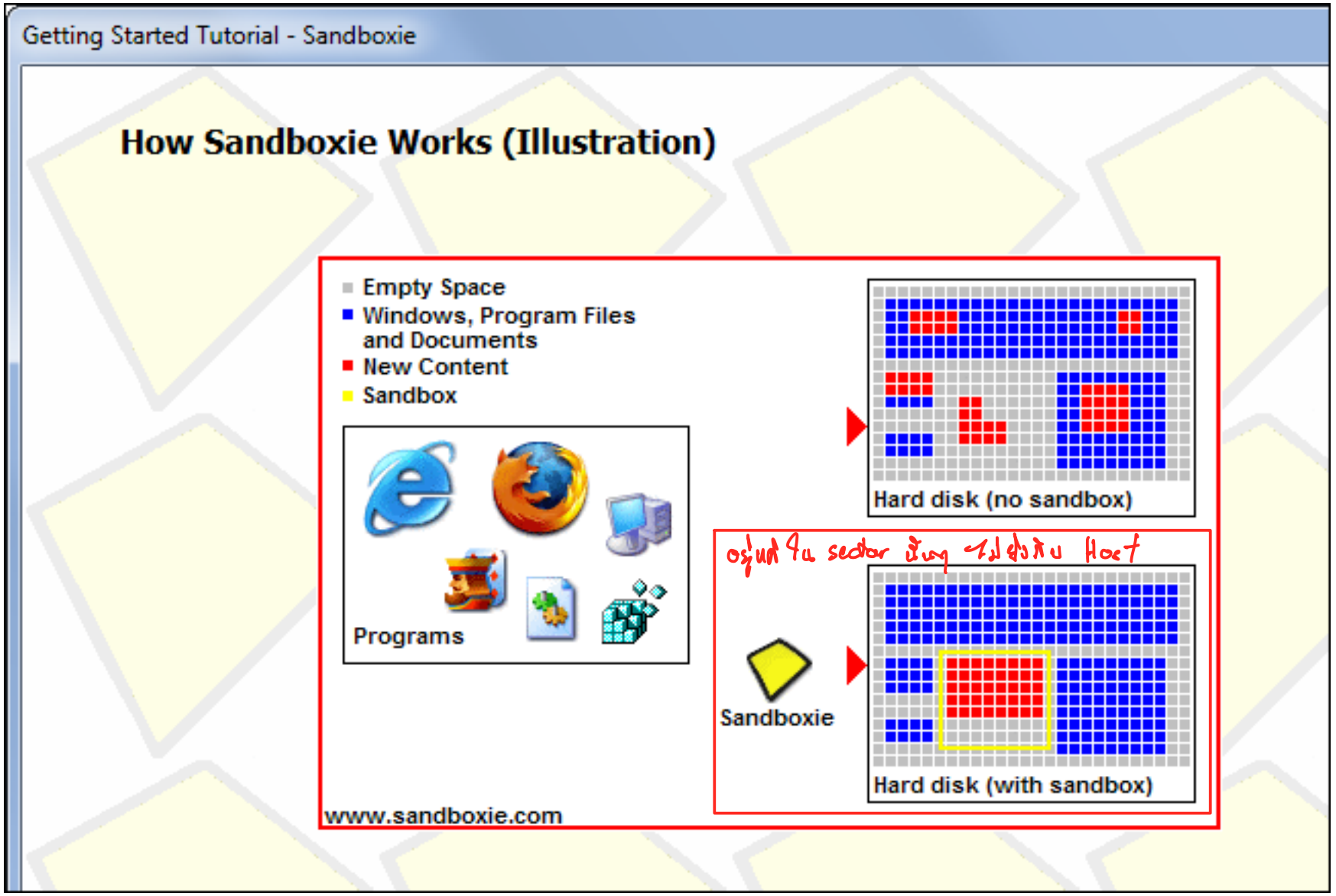
Secure Staging and Deployment

Sandbox อะไรสักอย่างหนึ่ง

- Used for testing
- Isolated area on a system

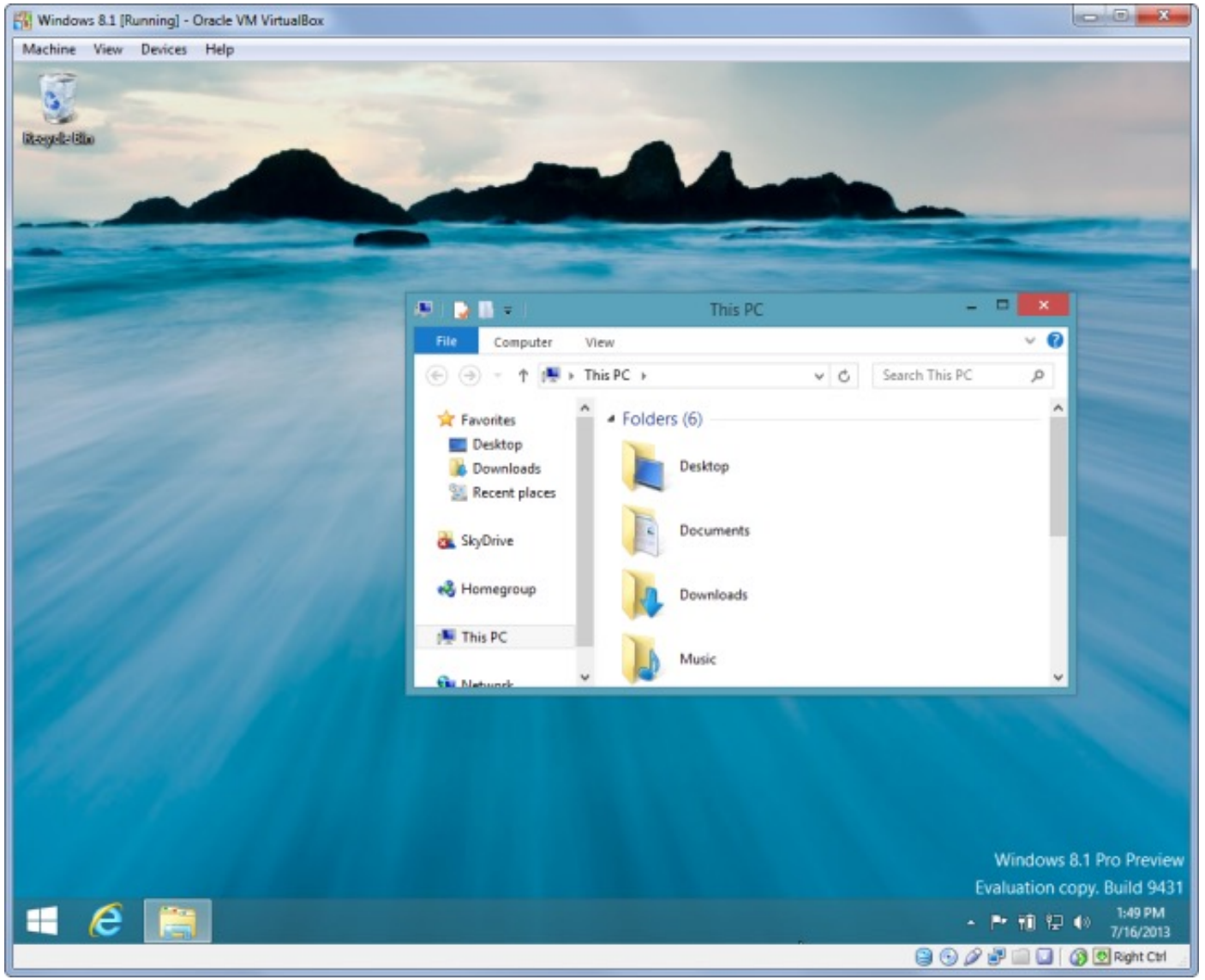
Secure Staging and Deployment

Sandbox



Secure Staging and Deployment

Sandbox



Secure Staging and Deployment

Development (Dev)

- App created in a development environment

System Integration testing (SIT)

- App Integration testing after develop

Test/User appetence test (UAT)

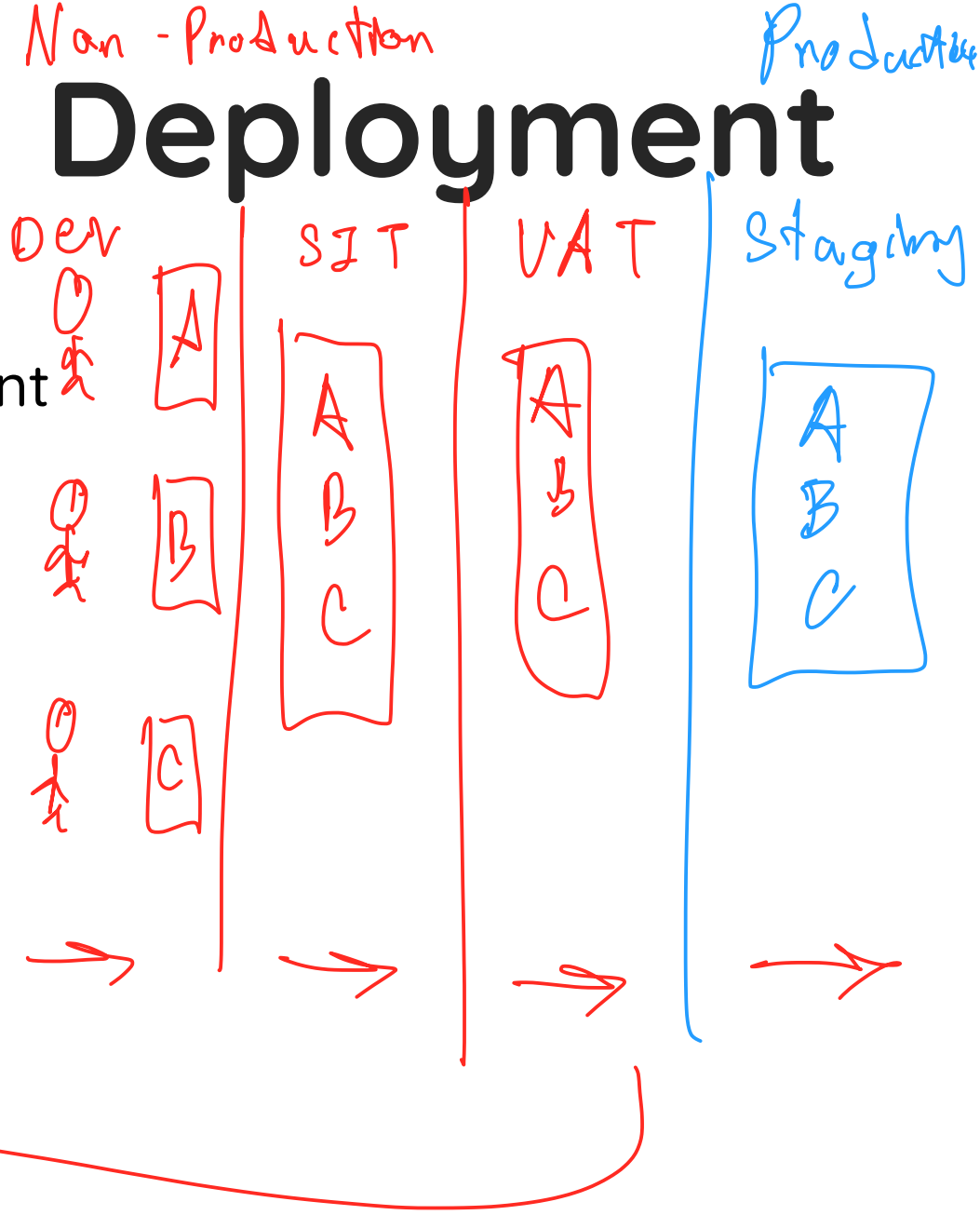
- App tested in a testing environment

Staging

- Simulates production environment

Production (PRD/PROD)

- Final product



Patch Management

- Automated deployment
- Controlled deployment
- Scheduling patch management
- Testing, deploying and verifying updates

Static Environments

- SCADA systems
- Embedded systems
- Mobile systems (Old)
- Mainframes
- Game consoles
- In-vehicle computing systems

Protecting Static Systems

- Redundancy and diversity
- Network segmentation
- Security layers
- Application firewalls
- Manual updates
- Firmware version control
- Wrappers (TCP wrappers)

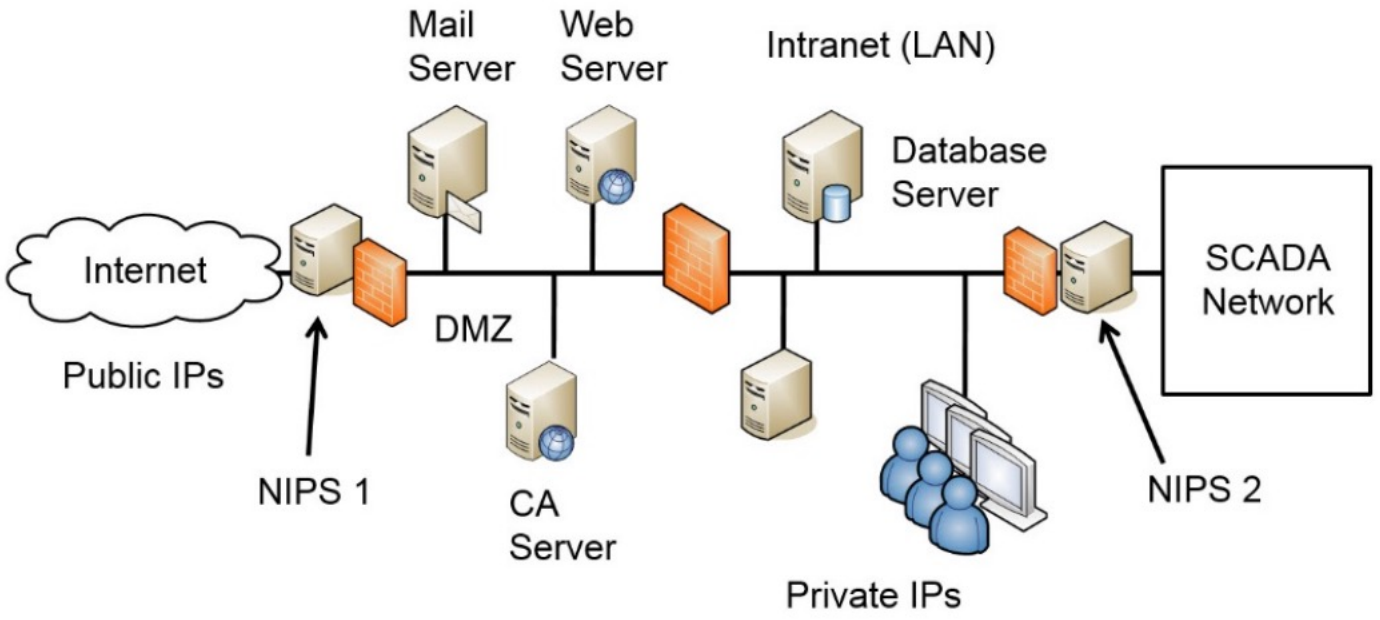
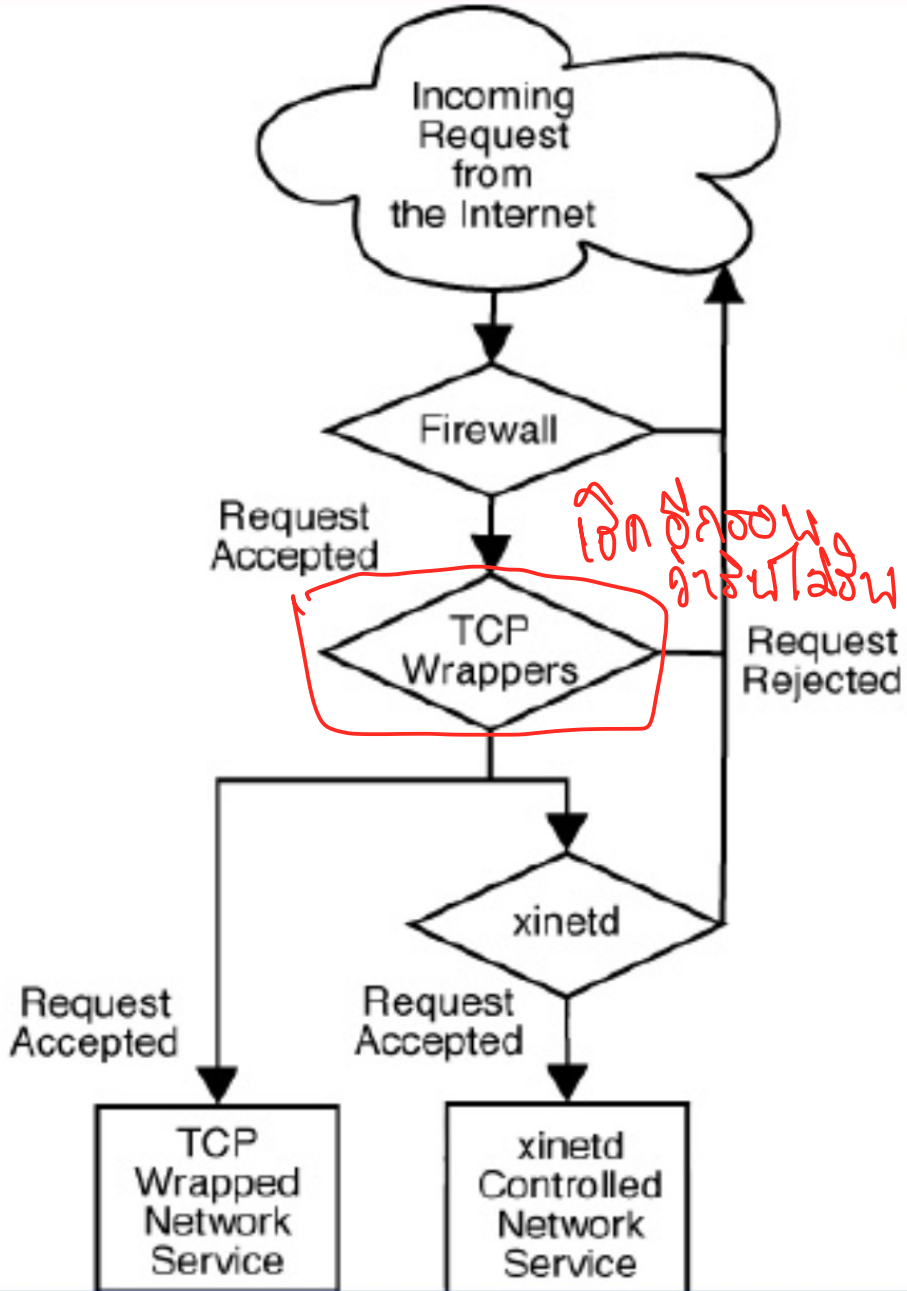


Figure from Chapter 4

What Are TCP Wrappers?

TCP wrappers is installed by default with a server-class installation of Red Hat Linux 8.0, and provides access control to a variety of services. Most modern network services, such as SSH, Telnet, and FTP, make use of *TCP wrappers*, a program that is designed to stand guard between an incoming request and the requested service. Ref: http://www.slideshare.net/Riju_Rocks/networking-51602489

TCP Wrappers and xinetd

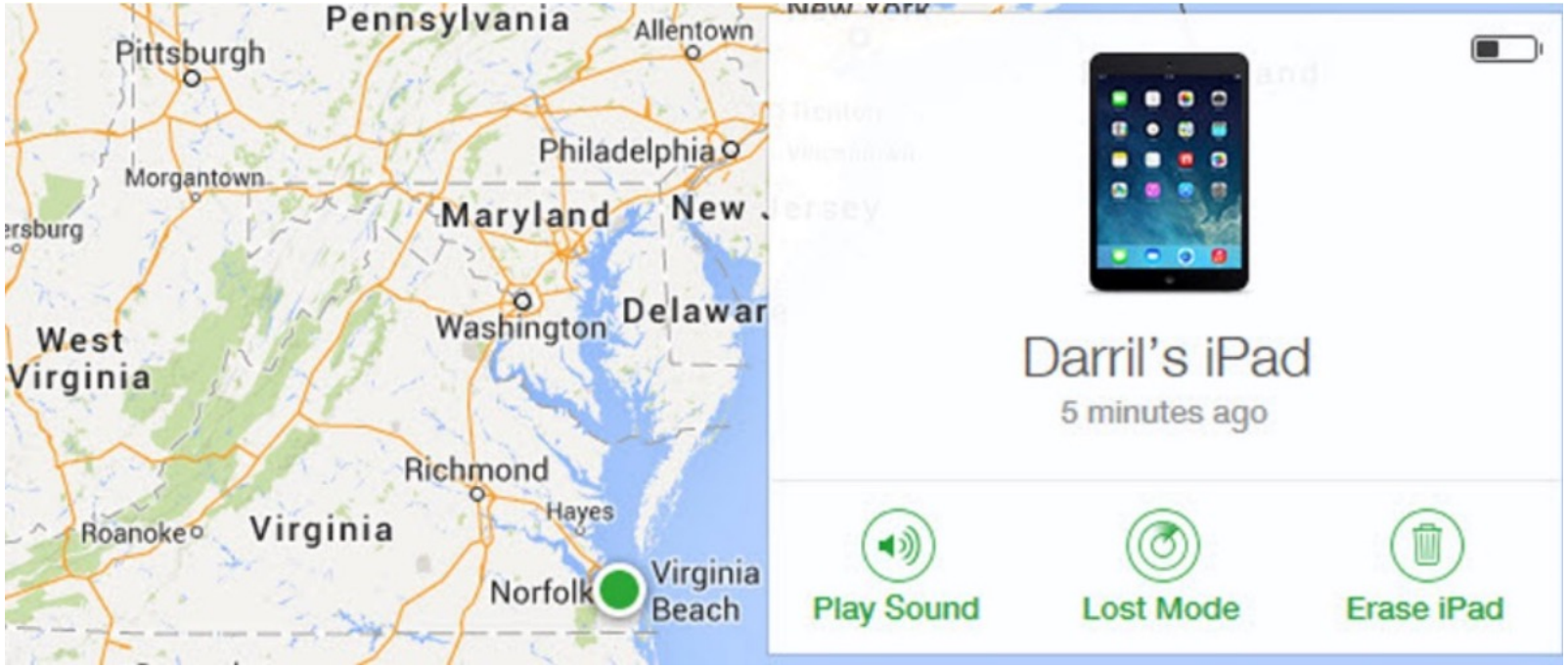


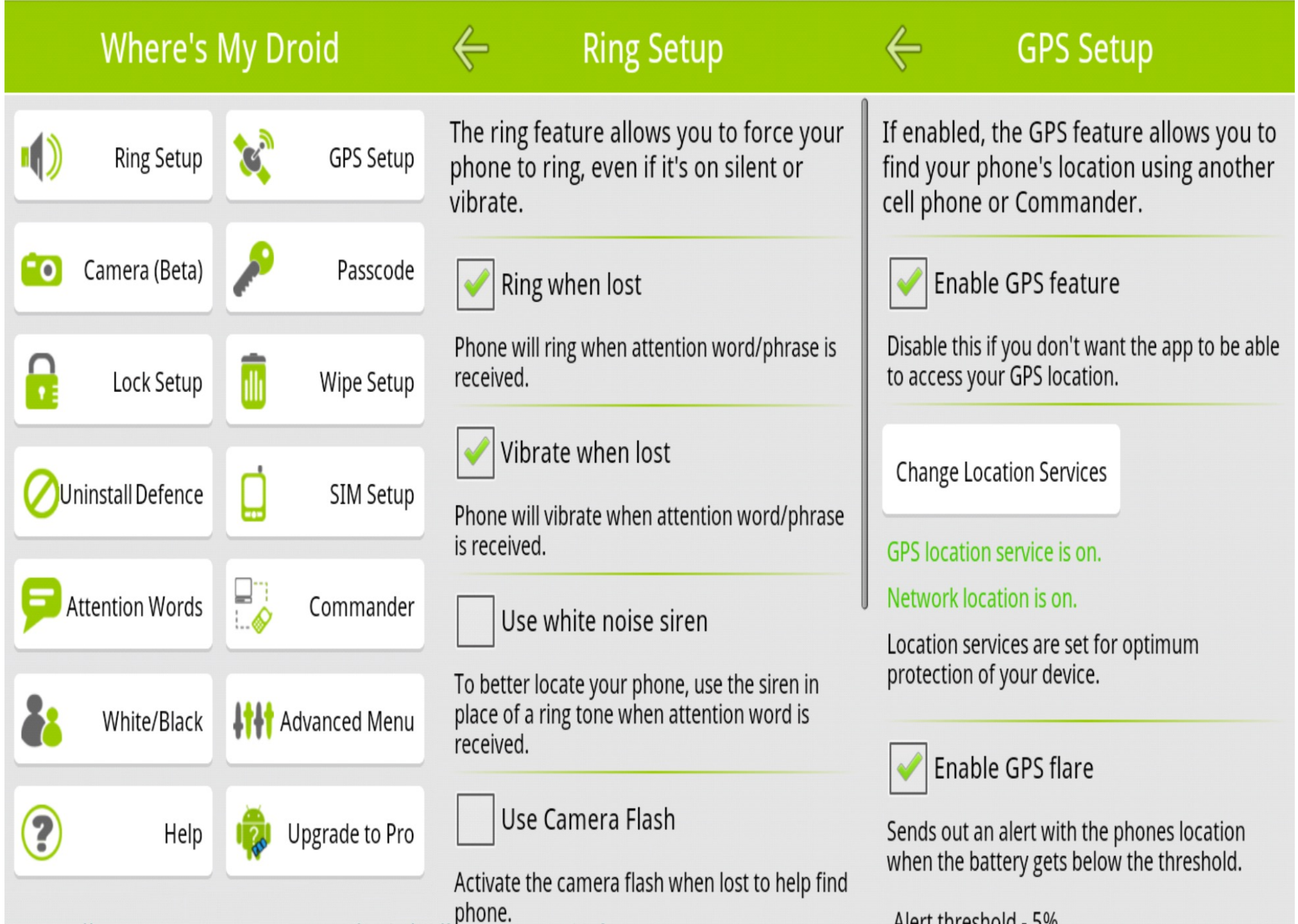
Controlling access to network services is one of the most important security tasks facing a server administrator:

- An `iptables-based firewall` filters out unwelcome network packets within the kernel's network stack.
- `TCP wrappers` add an additional layer of protection by defining which hosts are allowed or not allowed to connect to "wrapped" network services. One such wrapped network service is the `xinetd` super server.

Securing Mobile Devices

- Full disk encryption
- Authentication and device access control
- GPS tracking




Where's My Droid
Ring Setup
GPS Setup
Camera (Beta)
Passcode
Lock Setup
Wipe Setup
Uninstall Defence
SIM Setup
Attention Words
Commander
White/Black
Advanced Menu
Help
Upgrade to Pro
Ring Setup
The ring feature allows you to force your phone to ring, even if it's on silent or vibrate.
Ring when lost
Phone will ring when attention word/phrase is received.
Vibrate when lost
Phone will vibrate when attention word/phrase is received.
Use white noise siren
To better locate your phone, use the siren in place of a ring tone when attention word is received.
Use Camera Flash
Activate the camera flash when lost to help find phone.
GPS Setup
If enabled, the GPS feature allows you to find your phone's location using another cell phone or Commander.
Enable GPS feature
Disable this if you don't want the app to be able to access your GPS location.
Change Location Services
GPS location service is on.
Network location is on.
Location services are set for optimum protection of your device.
Enable GPS flare
Sends out an alert with the phones location when the battery gets below the threshold.

Securing Mobile Devices

- Removable storage
- Storage segmentation
- Screen locks
- Lockout
- Remote wiping
- Disabling unused features

Bring Your Own Device (BYOD)

Bring Your Own Device (employee-owned)

- Acceptable use policy ใช้ได้เฉพาะที่ที่กำหนด
- Adherence to corporate policies
- Privacy
- User acceptance
- Data ownership
- Support ownership

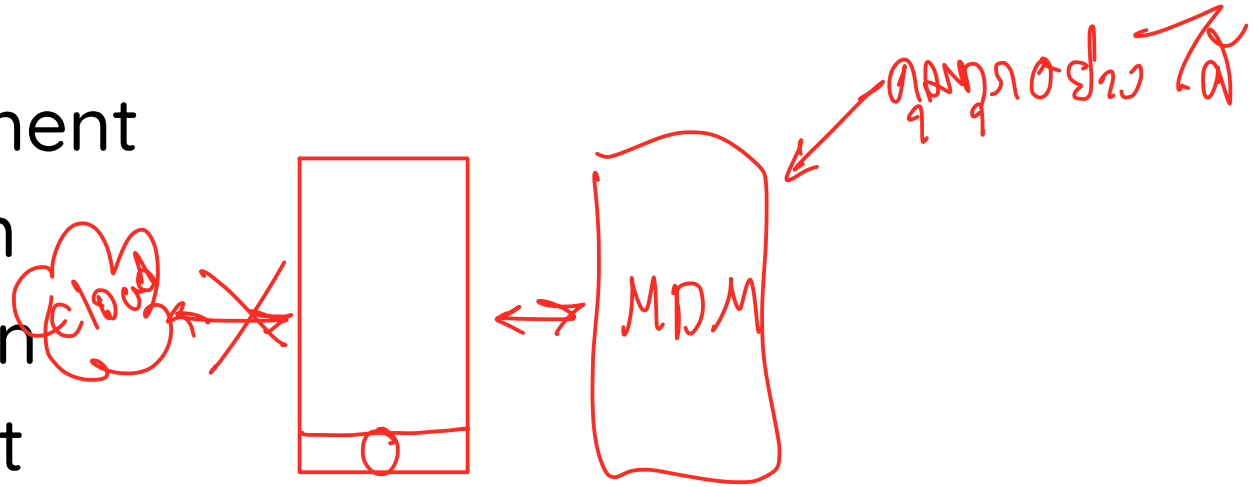
BYOD Concerns

Bring Your Own Device (employee-owned)

- Asset tracking and inventory control
- Architecture/infrastructure considerations
- Forensics
- Legal concerns
- On-boarding/off-boarding
- On-board camera/video

Mobile Device Management (MDM)

- Application management
- Full device encryption
- Storage segmentation
- Content management
- Containerization
- Passwords and PINs
- Biometrics
- Screen locks

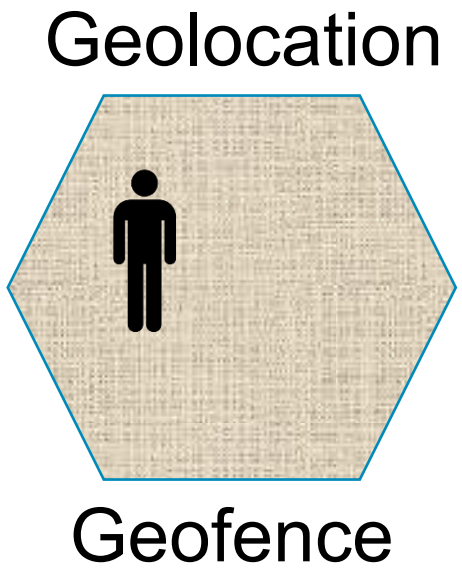


Mobile Device Management (MDM)

- Ensure mobile systems are up to date
  - Current patches
  - Up-to-date antivirus
- Block devices that are not up to date
- Include
  - Patch management
  - Antivirus management
  - Application control

Mobile Device Management (MDM)

- Remote wipe
- Geolocation
- Geofencing
- GPS tagging
- Context-aware authentication
- Push notification services



MDM Enforcement / Monitoring

Unauthorized software

- Third party app stores
- Rooting and jailbreaking
- Updates
- Sideloading
- SMS and MMS
- SMS

Hardware control

- USB OTG cables

Unauthorized connections

- Tethering
- Wi-Fi Direct
- Ad hoc

Protecting Data

Data at rest

- Any stored data
- Hard drives, Mobile phones, USB flash drives, external drives, databases and backups

Data in transit

- Data in motion
- Any data traveling over a network

Data in use

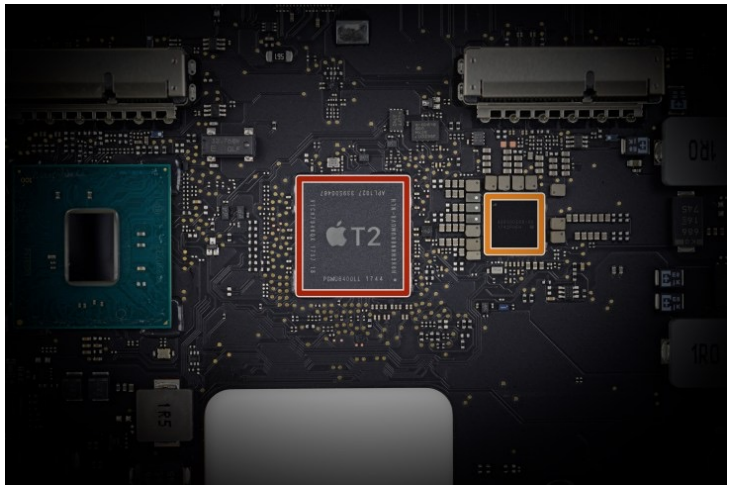
Protecting Confidentiality with Encryption

Software-based encryption

- File/folder-level encryption
- Full disk encryption
- Data base column encryption

Hardware-Based Encryption

- Hardware Security Module (HSM)
  - Removable or external hardware device, (purchased separately)
- Trusted Platform Module (TPM) Secure Module
  - Chip in motherboard (included with many laptops)
  - Apple T1, T2



Data Leakage

Data Loss Prevention (DLP) techniques

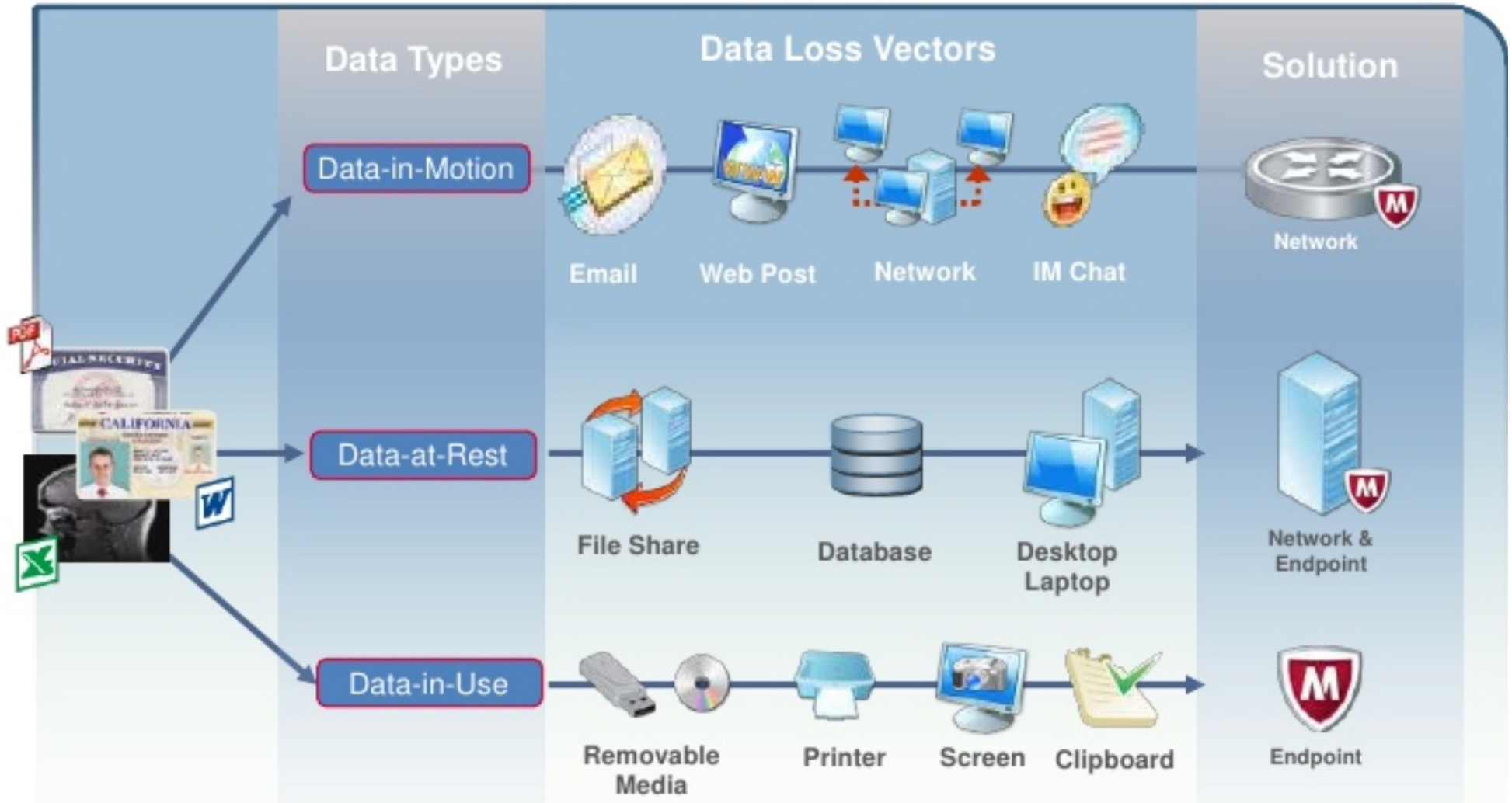
Data-in-motion

- Scans emails and attachments
- Detects outgoing confidential company data

Endpoint Protection

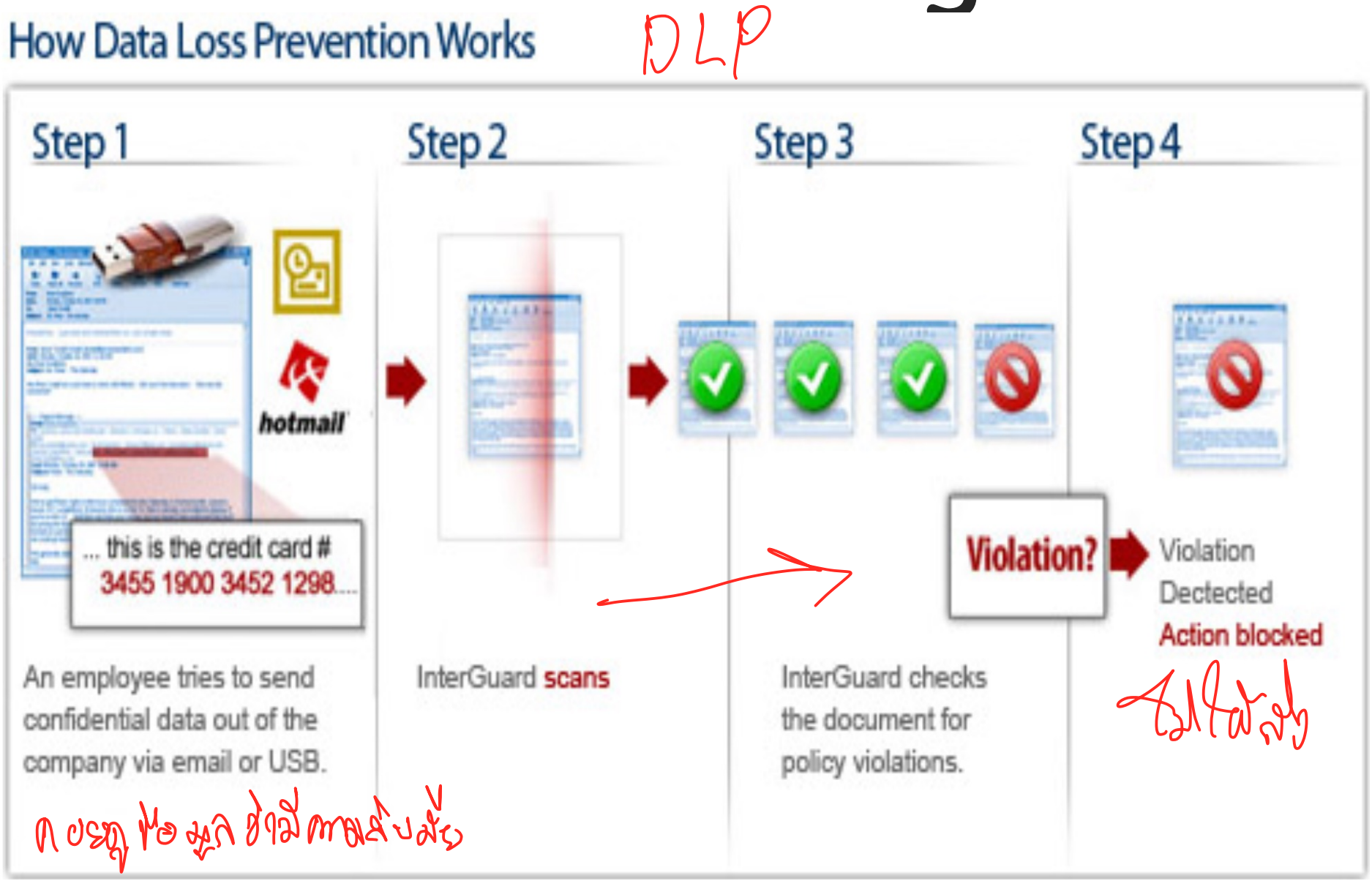
- Scans for content going to devices
- Prevents users from copying certain data to USB drives
- Prevents users from sending certain data to printers

Data Leakage



http://www.slideshare.net/Intel-ASIP/enterprise-api-security-data-loss-

Data Leakage



https://www.awarenesstechnologies.com/products_dlp.html

Understanding Cloud Computing

Software as a Service (SaaS)

- Applications provided over the Internet (such as web-mail accessed with a web browser)

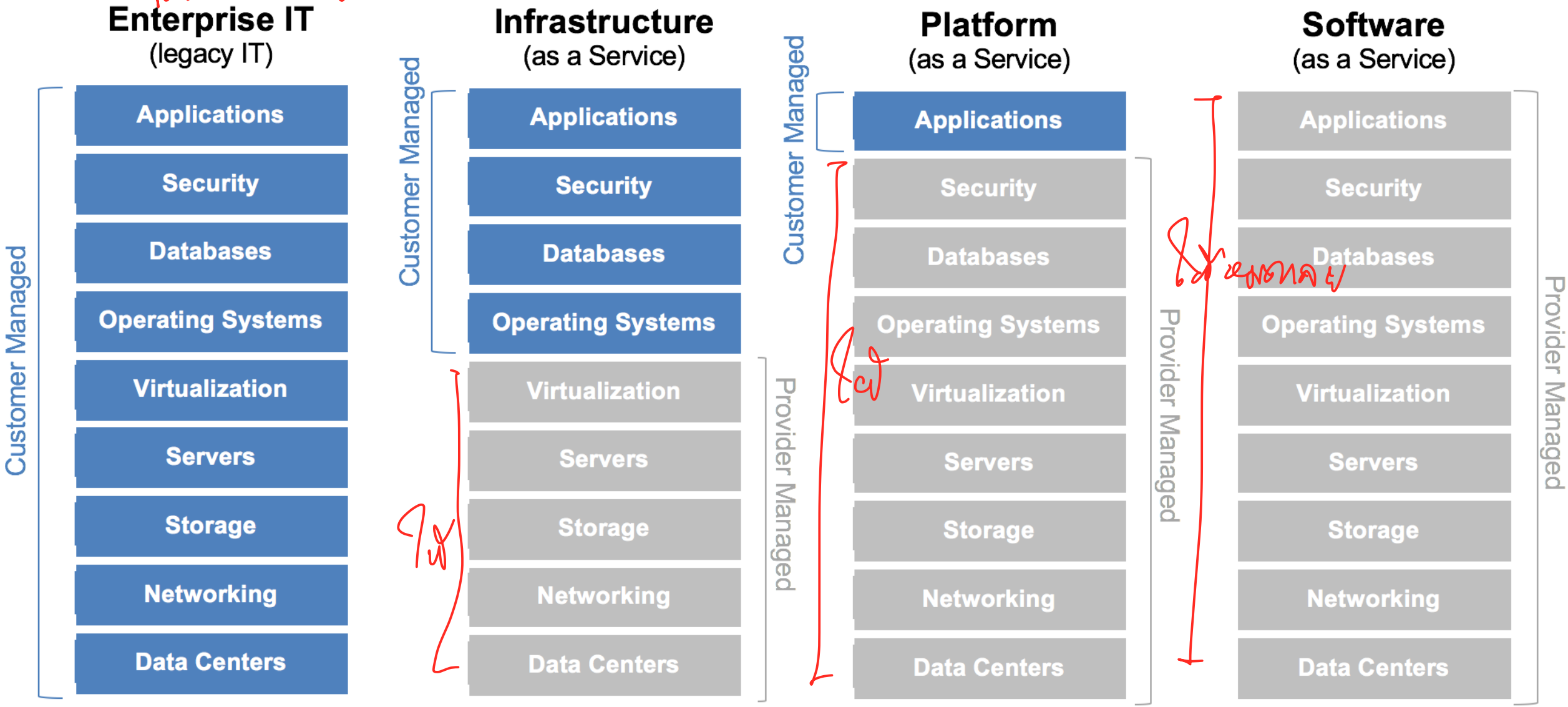
Platform as a Service (PaaS)

- Provides customers with a fully managed platform
- Vendor keeps platform up-to-date

Infrastructure as a Service (IaaS)

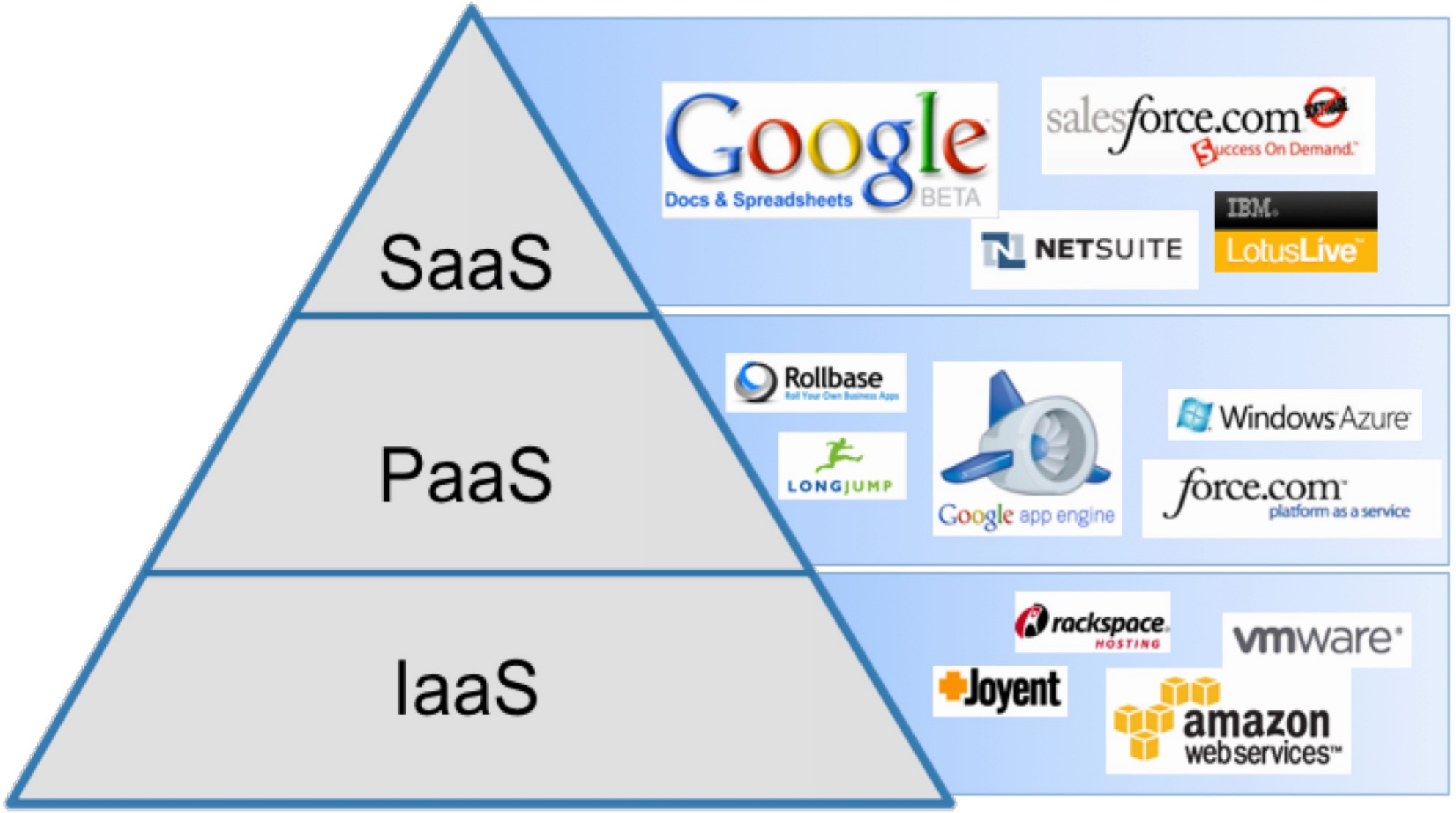
- Provides customers with access to hardware in a self-managed platform
- Customers are responsible for keeping an IaaS system up to date

Understanding Cloud Computing



https://mycloudblog7.wordpress.com/2013/06/19/who-manages-cloud-iaas-paas-and-saas-services

Understanding Cloud Computing



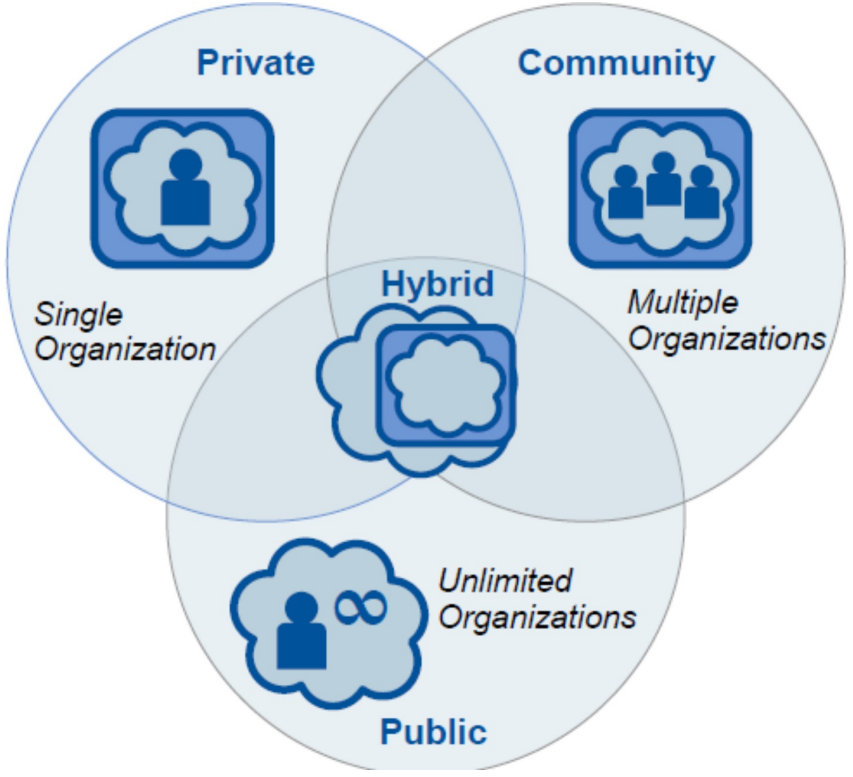
Understanding Cloud Computing

Public – Available to anyone ใครก็ใช้

Private – Only available within a company เฉพาะบริษัท

Hybrid – Combination of public and private ผสมกัน แบบใช้ Public บริษัทใช้ Private

Community – Cloud shared by two or more organizations แชร์กันใช้



File System Security

- Linux permissions

d rwx rwx rwx
- rwx rwx rwx

- = file
d = Directory = floder

File Name	Owner	Group	All Other Users
Success.exe	rwx	rw-	- - -
Study.docx	rwx	rw-	r- -
UCanPass.exe	rwx	r-x	r-x

Group Owner

read
write
execule

Demo

File Name	Number	Owner	Group	All Other Users
Success.exe	760	111	110	000
Study.docx	764	111	110	100
UCanPass.exe	755	111	101	101

4 2 1
rwx
1 1 1
7

4 2 1
rw-x
1 1 0
6

4 2 1
rwx
0 0 0
0

- Chmod

Change modify

Chapter 5 Summary

1. Implementing secure systems
2. Summarizing cloud concepts
3. Deploying mobile devices securely


Q&A