Week 12

An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 12: Modern Enterprise Security (Part 1)

Final Examination

Time travel to January 2036 (15 years from now) and explain in a 1500-word essay the following:

1. What are the major cyber security threats that are facing the world.
2. What are the major cyber security protections being used to address cyber risk.
3. What are your recommendations to global leaders to reduce cyber risk.

Final Examination – Typical Outline

Title: State of Global Cyber Security – 2036

your name

Introduction (150 words)

During the last fifteen years, since 2021, the globe has seen . . .

Major Cyber Security Threats (450 words)

The major cyber security threats facing our globe can be grouped into the following X categories . . .

Major Cyber Security Protections (450 words)

The major cyber security protections protecting our globe today can be grouped into . . .

Recommendations (450 words)

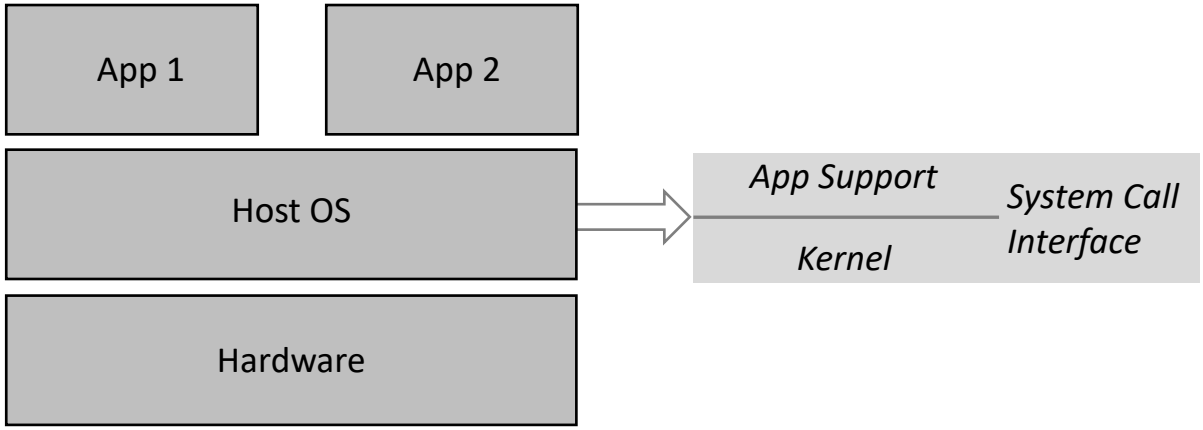
My recommendations for world leaders today in 2036 include . . .

What is Virtualization in Computing and Why is it Relevant to Security?

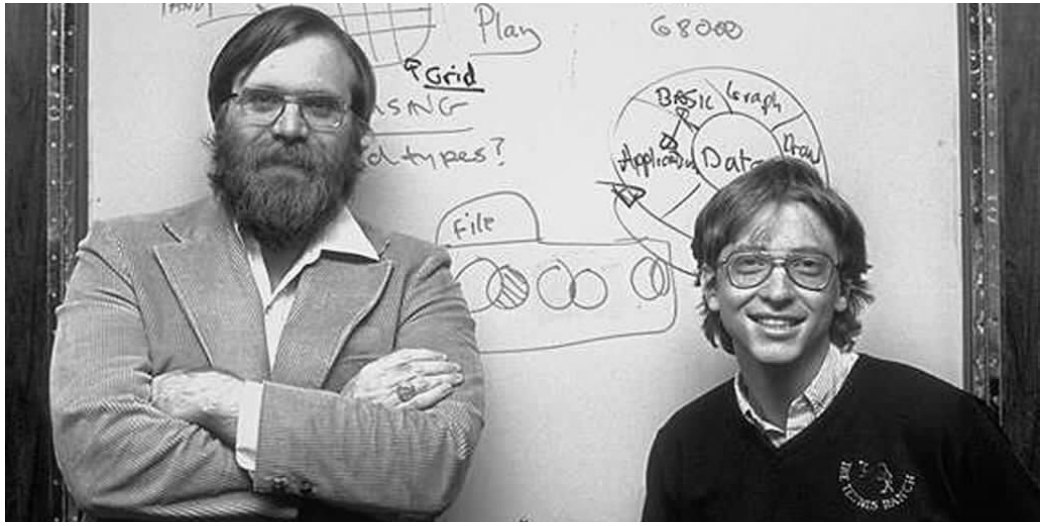
Making One Thing into Multiple Virtual Copies

Week 12

Early Operating System (OS) Model in Computing



Traditional Model



Week 12

Multi-Boot Operating System Model in the 1990's

Week 12

Five Types of Modern Computing Virtualization

- **Desktop Virtualization**
  - Desktop OS runs as a VM on a physical server with other virtual desktops (e.g., VDI services)

Week 12

Five Types of Modern Computing Virtualization

- **Desktop Virtualization**
  - Desktop OS runs as a VM on a physical server with other virtual desktops (e.g., VDI services)
- **Application Virtualization**
  - Application packages in single executable to run in sandbox environment
  - One copy of application on server with many client desktops (e.g., streaming)

Week 12

Five Types of Modern Computing Virtualization

- **Desktop Virtualization**
  - Desktop OS runs as a VM on a physical server with other virtual desktops (e.g., VDI services)
- **Application Virtualization**
  - Application packages in single executable to run in sandbox environment
  - One copy of application on server with many client desktops (e.g., streaming)
- **Server Virtualization**
  - Many VMs run on a single physical server to optimize resources through hypervisor software

Week 12

Five Types of Modern Computing Virtualization

- **Desktop Virtualization**
  - Desktop OS runs as a VM on a physical server with other virtual desktops (e.g., VDI services)
- **Application Virtualization**
  - Application packages in single executable to run in sandbox environment
  - One copy of application on server with many client desktops (e.g., streaming)
- **Server Virtualization**
  - Many VMs run on a single physical server to optimize resources through hypervisor software
- **Storage Virtualization**
  - Grouping of physical storage into multiple virtual storage devices

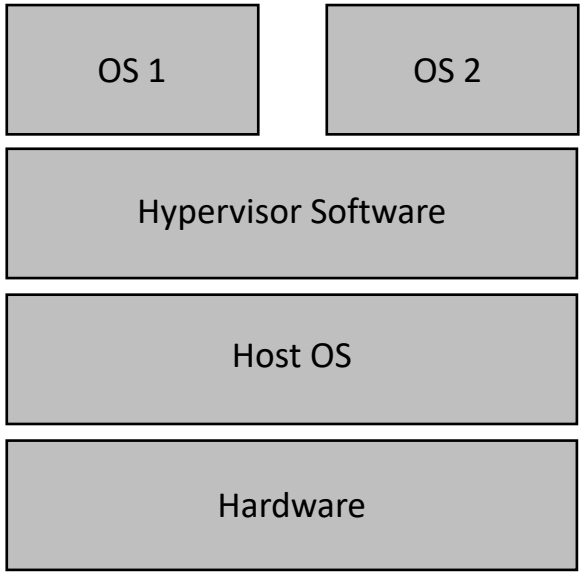
Week 12

Five Types of Modern Computing Virtualization

- **Desktop Virtualization**
  - Desktop OS runs as a VM on a physical server with other virtual desktops (e.g., VDI services)
- **Application Virtualization**
  - Application packages in single executable to run in sandbox environment
  - One copy of application on server with many client desktops (e.g., streaming)
- **Server Virtualization**
  - Many VMs run on a single physical server to optimize resources through hypervisor software
- **Storage Virtualization**
  - Grouping of physical storage into multiple virtual storage devices
- **Network Virtualization**
  - Decouples virtual networks from underlying hardware
  - Management and control through software-defined switches

Week 12

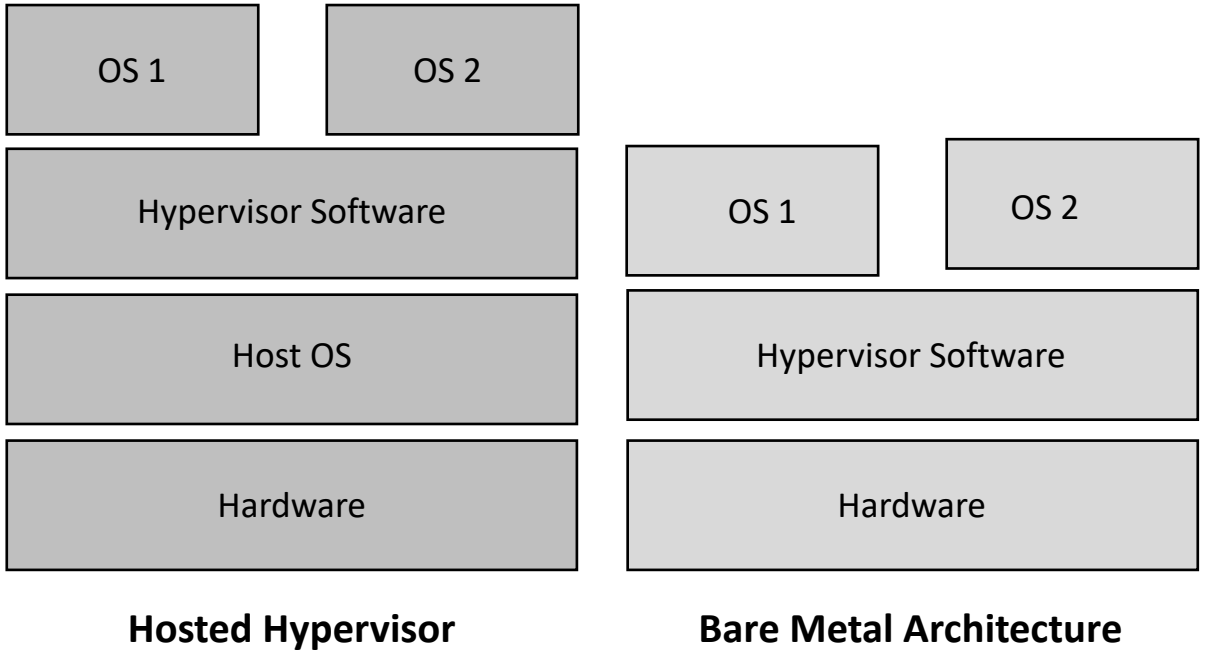
Popular Server Virtualization Models



Hosted Hypervisor

Week 12

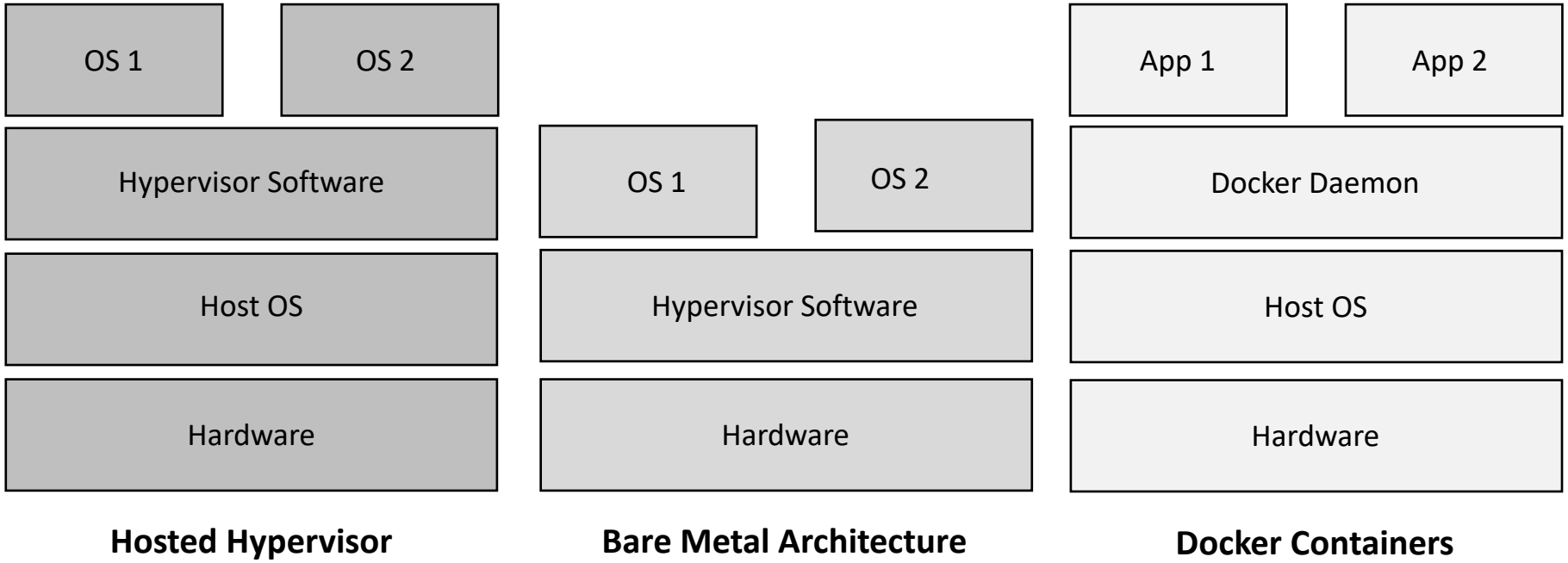
Popular Server Virtualization Models



Hosted Hypervisor **Bare Metal Architecture**

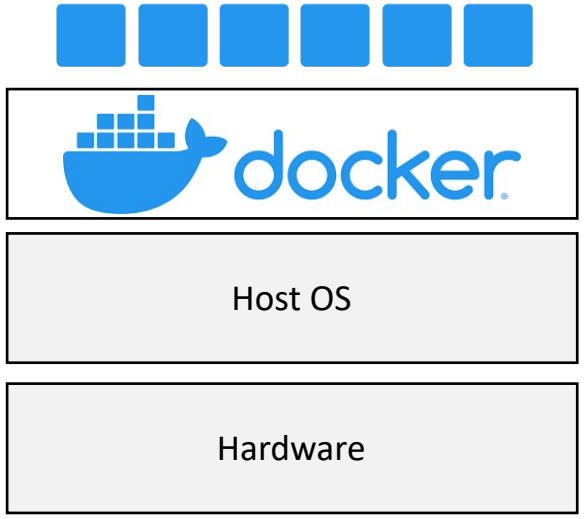
Week 12

Popular Server Virtualization Models



Week 12

Docker Containers



Docker Container Deployment

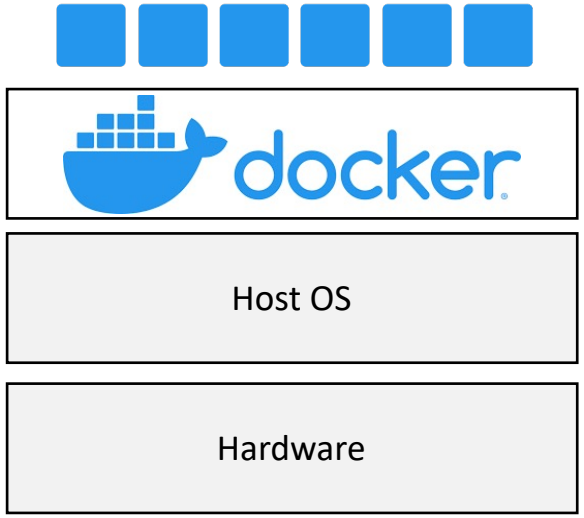
Platform-as-a-Service (PaaS)
Delivers Software in Containers

Containers Share Single Host OS
Use Fewer Resources than VMs

Originated in 2010 as Y-Combinator Project
Released as Open Source in 2013

Week 12

Docker and Kubernetes

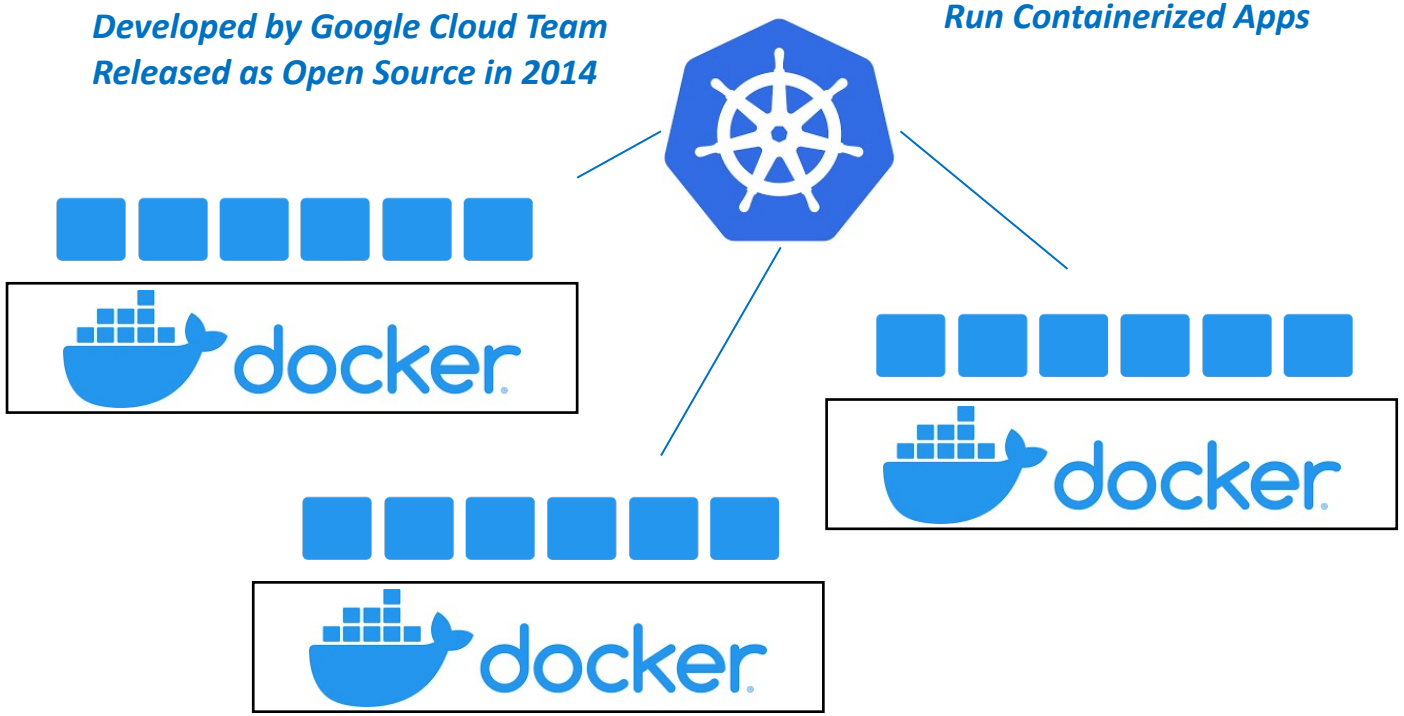


Docker Container Deployment

Docker Runs as a "Single Node"

Developed by Google Cloud Team
Released as Open Source in 2014

Kubernetes and Docker Coordinate to Build and Run Containerized Apps



Docker Container and Kubernetes Deployment

Kubernetes Coordinates Clusters of Nodes

Week 12

China Trade Monitor
News and analysis of China's economic relations with the world

NATIONAL SECURITY

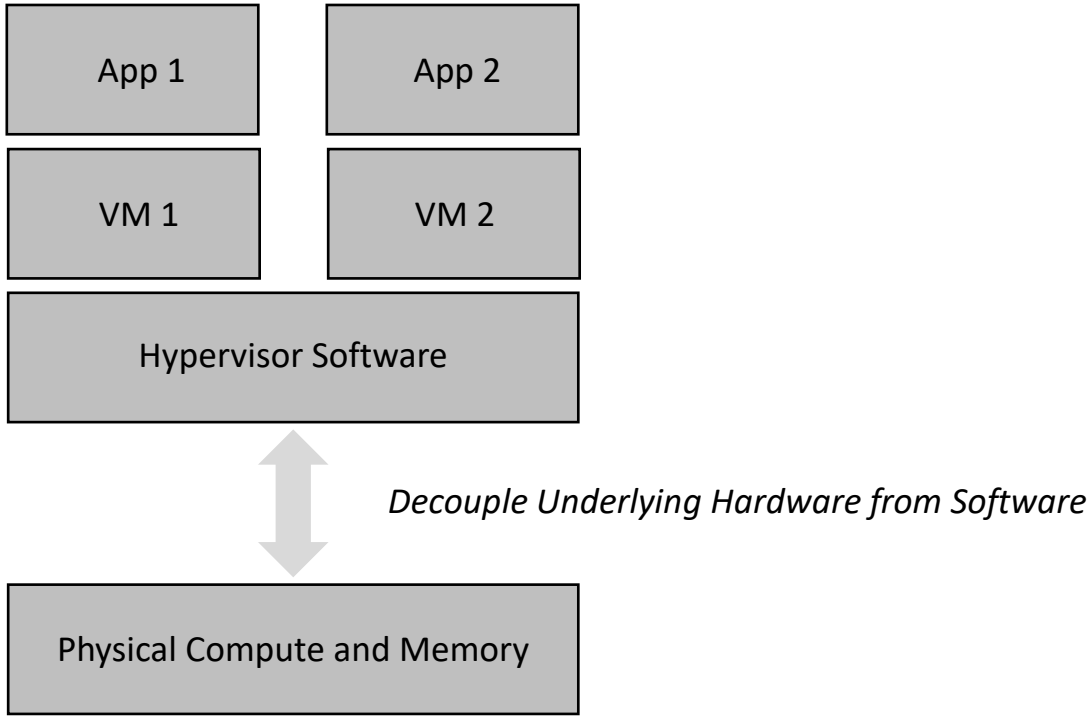
Three U.S. Senators Call For Penalties Against Chinese "Internet of Things" Company

By **Simon Lester** - September 12, 2021

On September 9, U.S. Senators Marco Rubio (R-FL), Rick Scott (R-FL), and Tom Cotton (R-AR) sent a letter to Treasury Secretary Janet Yellen expressing concern about Chinese "Internet of Things" (IoT) company Tuya, and asking the Treasury Department to add Tuya to a "Chinese Military-Industrial Complex Companies List," which would restrict U.S. persons from purchasing and

Week 12

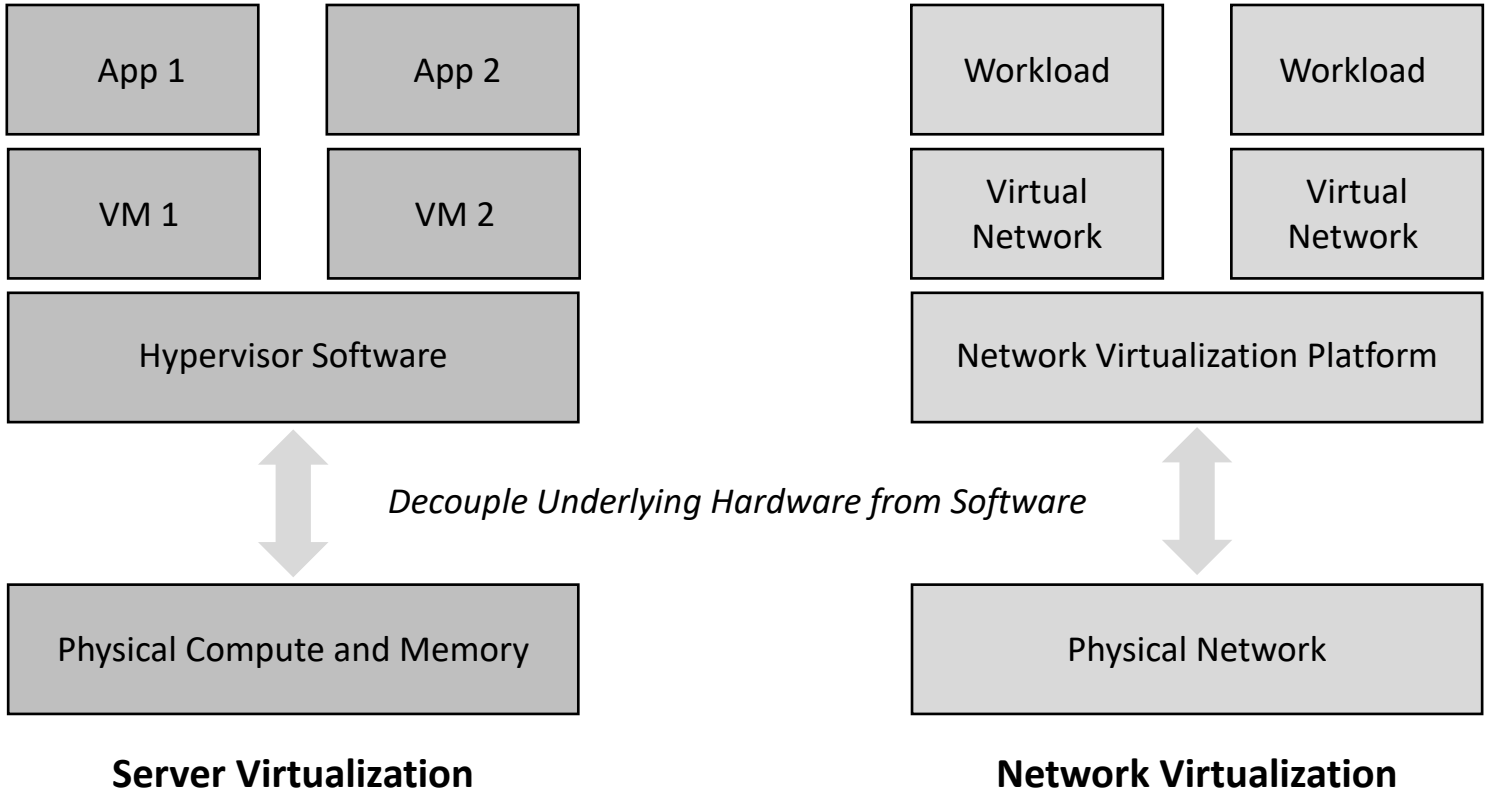
Decoupling Hardware and Software

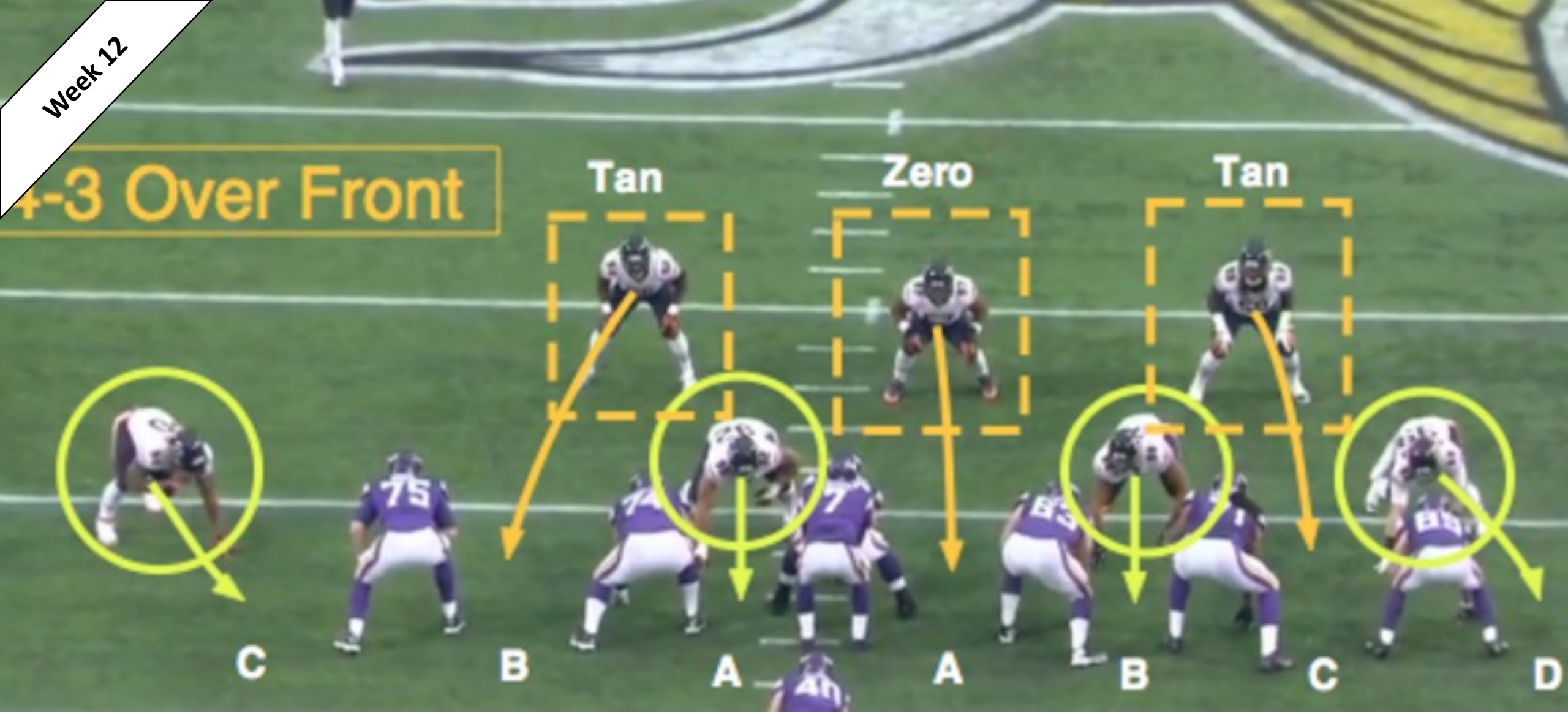


Server Virtualization

Week 12

Decoupling Physical Infrastructure from Virtual Networks





Key Concept: Virtual Systems Can Dynamically Reconfigure During an Attack

What is Cloud Computing and Why is it Relevant to Security?

Week 12

What is Cloud Computing?

- **Delivery of on-demand computing services over the Internet**
  - Servers, storage, databases, networks, software, analytics
  - Pay for what you use (lowers operating costs)

Week 12

What is Cloud Computing?

- **Delivery of on-demand computing services over the Internet**
  - Servers, storage, databases, networks, software, analytics
  - Pay for what you use (lowers operating costs)
- **Supports flexibility, ubiquity, scale, and rapid innovation**
  - Shared model runs infrastructure efficiently and at lower cost
  - Eliminate expense of buying hardware

Week 12

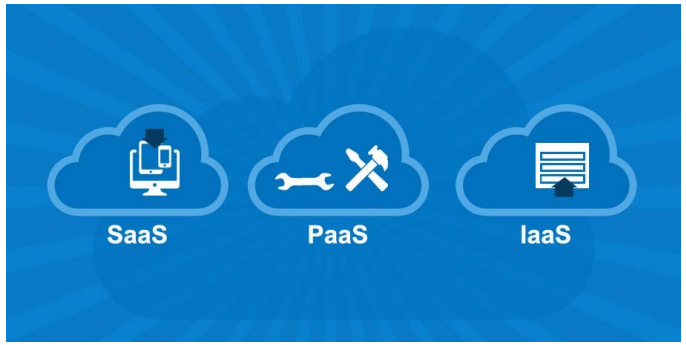
What is Cloud Computing?

- **Delivery of on-demand computing services over the Internet**
  - Servers, storage, databases, networks, software, analytics
  - Pay for what you use (lowers operating costs)
- **Supports flexibility, ubiquity, scale, and rapid innovation**
  - Shared model runs infrastructure efficiently and at lower cost
  - Eliminate expense of buying hardware
- **Cloud computing approaches**
  - Public Cloud – third-party delivery by cloud provider
  - Private Cloud – operated by sponsoring organization
  - Hybrid Cloud – combination of public and private

Week 12

Common Cloud Service Types

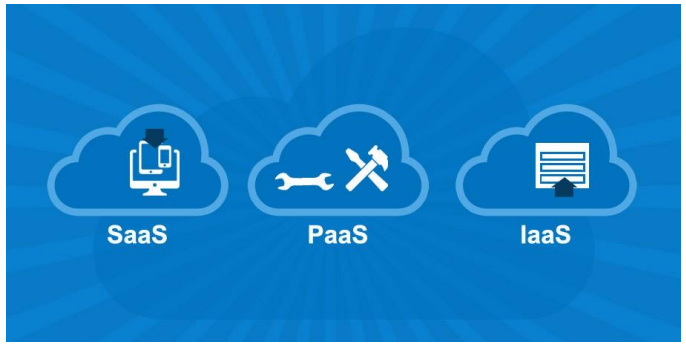
- **Infrastructure as a Services (IaaS)**
  - Pay for IT infrastructure on pay-as-you-go basis
  - Servers, virtual machines, storage, networks, operating systems



Week 12

Common Cloud Service Types

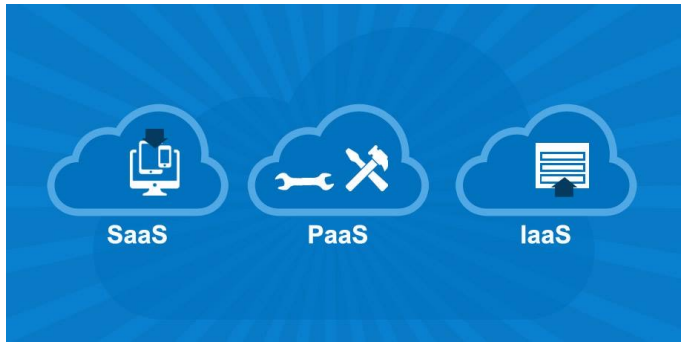
- **Infrastructure as a Services (IaaS)**
  - Pay for IT infrastructure on pay-as-you-go basis
  - Servers, virtual machines, storage, networks, operating systems
- **Platform as a Service (PaaS)**
  - Provides on-demand support for software apps
  - Allows development, test, and management of apps



Week 12

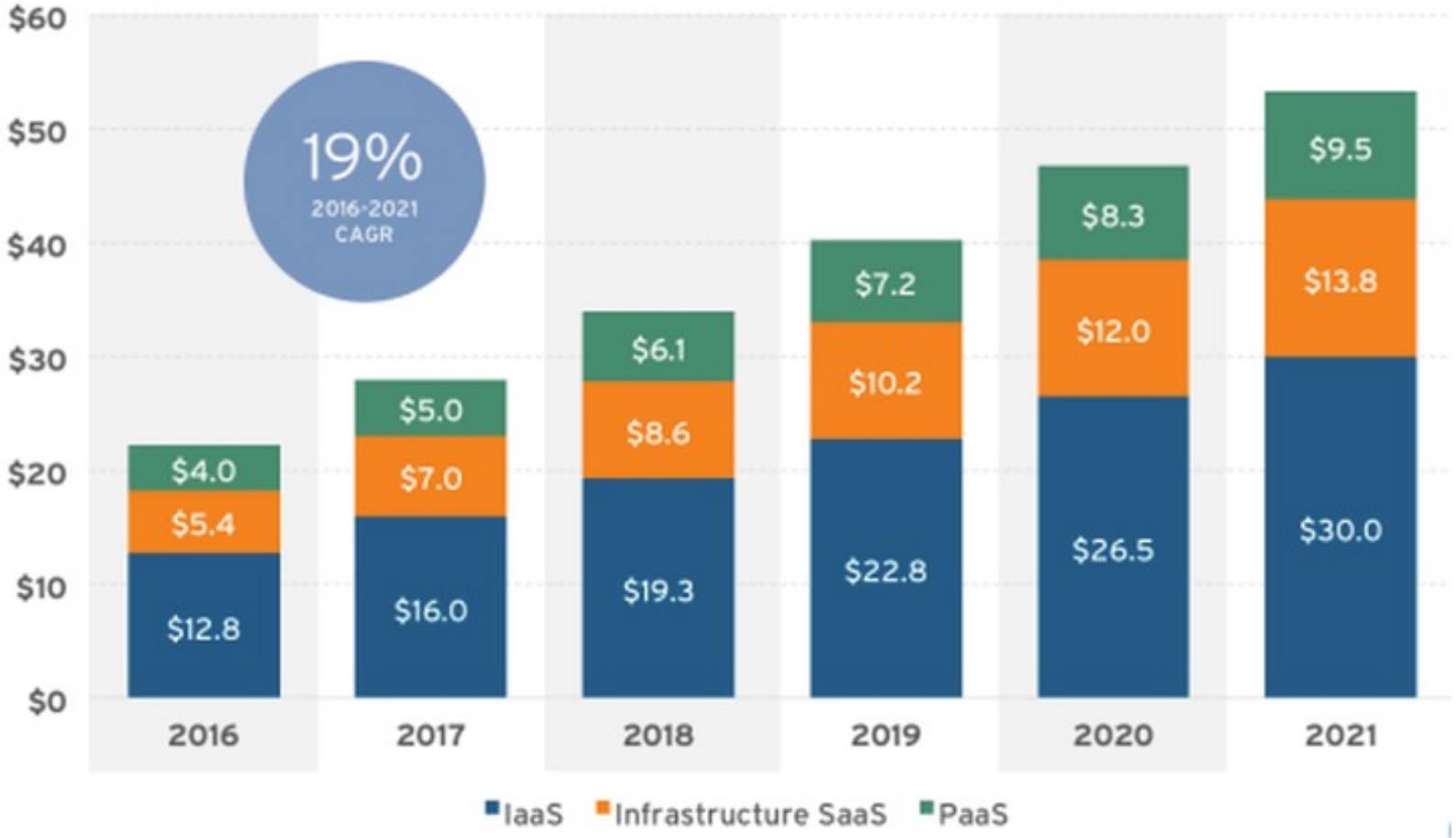
Common Cloud Service Types

- **Infrastructure as a Services (IaaS)**
  - Pay for IT infrastructure on pay-as-you-go basis
  - Servers, virtual machines, storage, networks, operating systems
- **Platform as a Service (PaaS)**
  - Provides on-demand support for software apps
  - Allows development, test, and management of apps
- **Software as a Service (SaaS)**
  - Delivers software apps on-demand, over the Internet
  - Users typically access SaaS apps via subscription



Week 12

Cloud Computing Growth



Source: 451 Research's Market Monitor: Cloud Computing, November 2017

Week 12

Comparing Public Cloud Services

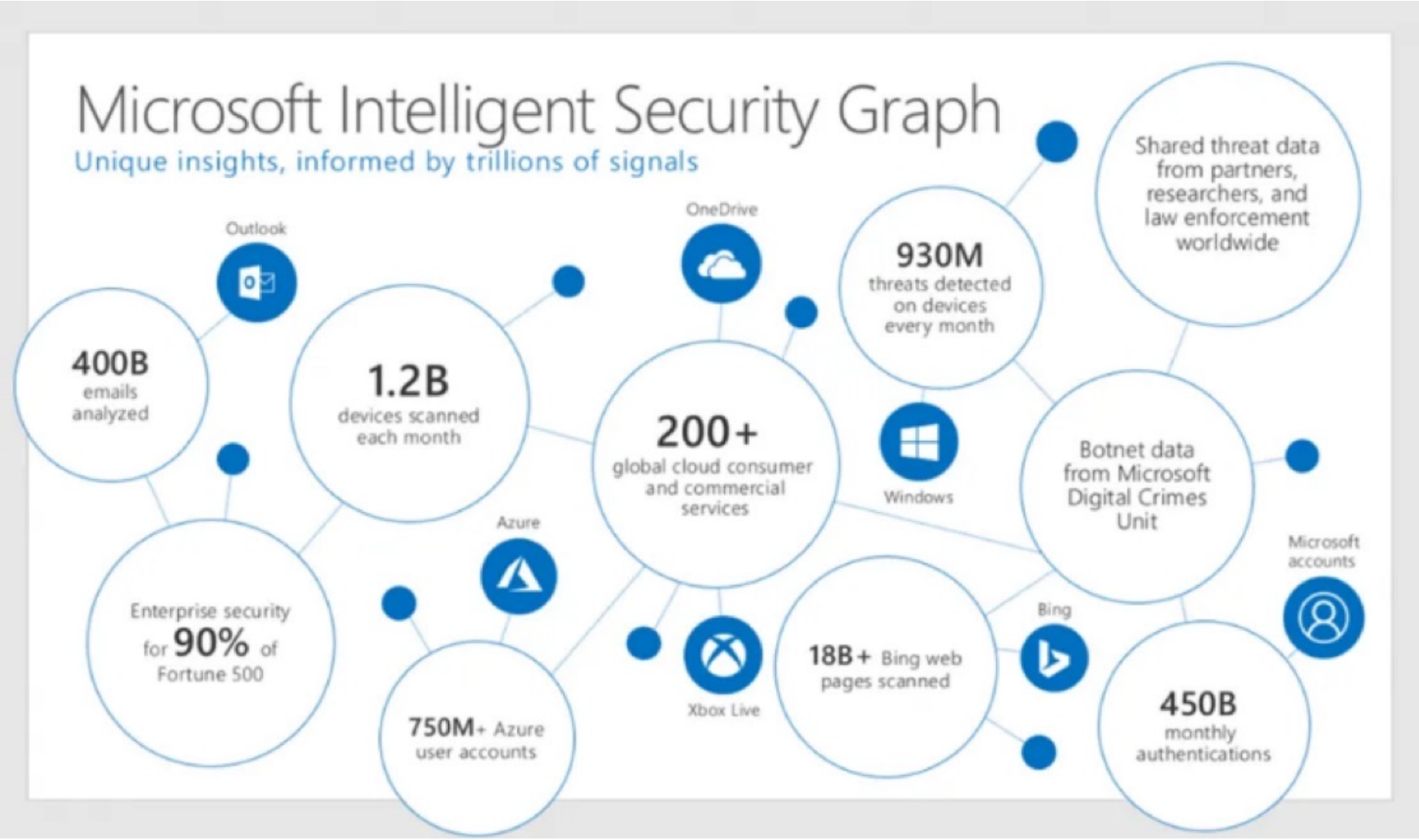
	aws	Azure	Google Cloud
Compute	Elastic Cloud Compute (EC2)	Virtual Machines	Compute Engine
App Hosting	Elastic Beanstalk	Cloud Services	App Engine
Serverless	AWS Lambda	Azure Functions	Cloud Functions
Container	ECS/EKS Containers	AKS Container	Kubernetes Engine
Storage (File)	S3 Storage	Azure Storage	Cloud Storage
Storage (Block)	Elastic Block Storage	Azure Blob	Persistent Disc
Backup	AWS Glacier	Azure Backup	Cloud Storage
Orchestration	Data Pipeline	Data Factory	Cloud DataFlow
Management	AWS Redshift	SQL Data Warehouse	Google BigQuery
NoSQL DB	AWS DynamoDB	Cosmos DB	Cloud DataStore

Can This Baseball Team Beat the New York Yankees?

Can This IT Security Group Beat the Russian Military?

Week 12

Microsoft Invests $1B/Year in Cyber Security



What is Software Defined Networking and How is it Used for Security?

Week 12

What is Software Defined Networking (SDN)?

- **Software Defined Networking (SDN) is a network architectural model**
  - Popular to virtualize data centers
  - Important aspect of Tier One carrier network infrastructure including 5G

Week 12

What is Software Defined Networking (SDN)?

- **Software Defined Networking (SDN) is a network architectural model**
  - Popular to virtualize data centers
  - Important aspect of Tier One carrier network infrastructure including 5G
- **Improves control, orchestration, management, and securing of network resources**
  - Support programmable features versus manual configuration
  - *Security comes from improved visibility and ease of control*

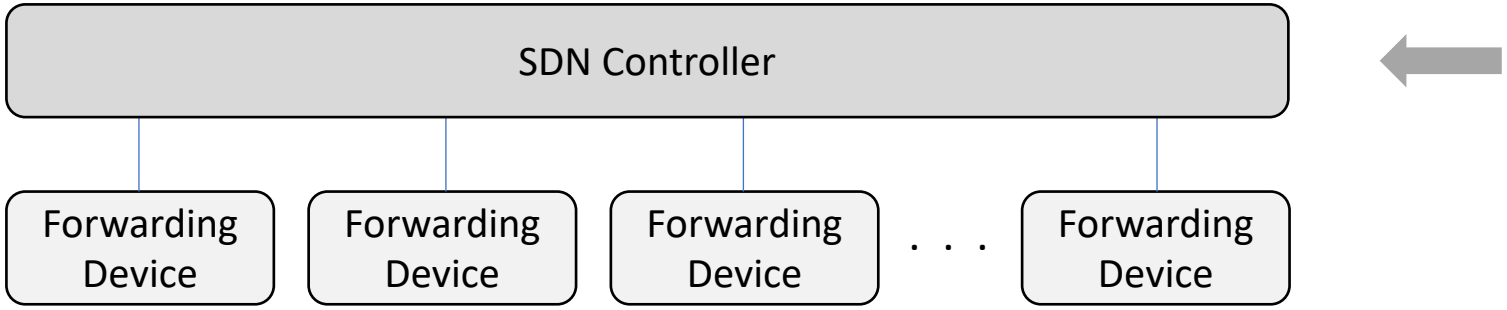
Week 12

What is Software Defined Networking (SDN)?

- **Software Defined Networking (SDN) is a network architectural model**
  - Popular to virtualize data centers
  - Important aspect of Tier One carrier network infrastructure including 5G
- **Improves control, orchestration, management, and securing of network resources**
  - Support programmable features versus manual configuration
  - *Security comes from improved visibility and ease of control*
- **Separates and decouples data and control plane using a centralized SDN control function**
  - SDN involves centralized control versus distributed router configuration
  - Network resources can be configured and secured at scale

Week 12

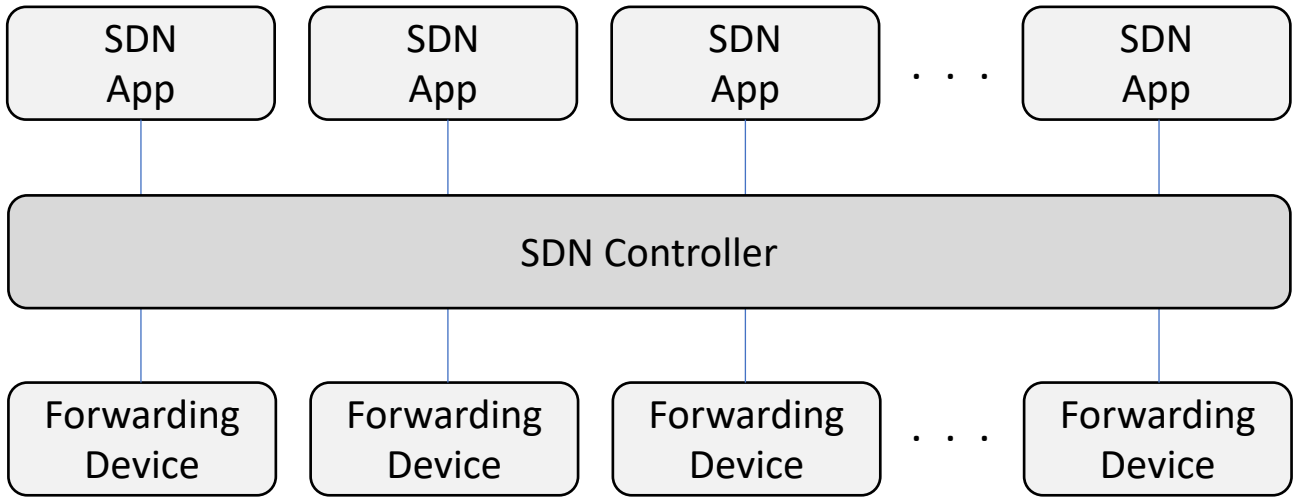
SDN Controller Configuration



Replaces Top of Rack Router in a Traditional Data Center

Week 12

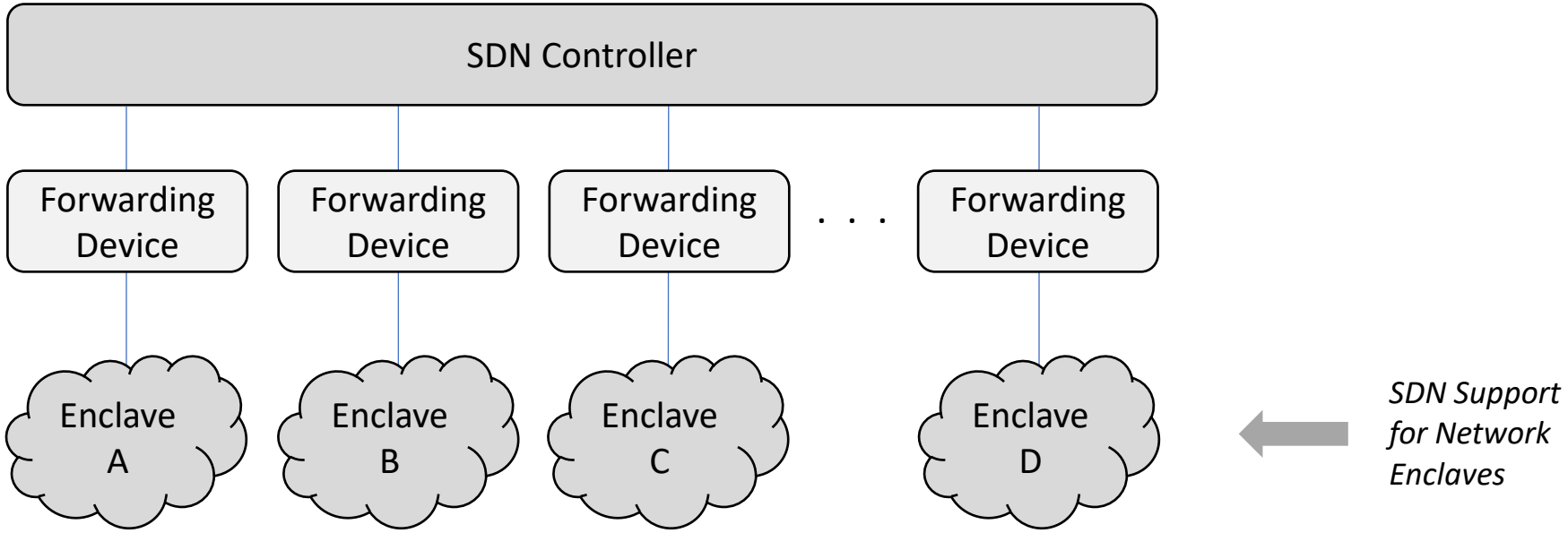
SDN Controller Configuration



SDN Security Apps Provide Extensible Protection (e.g. Analytics)

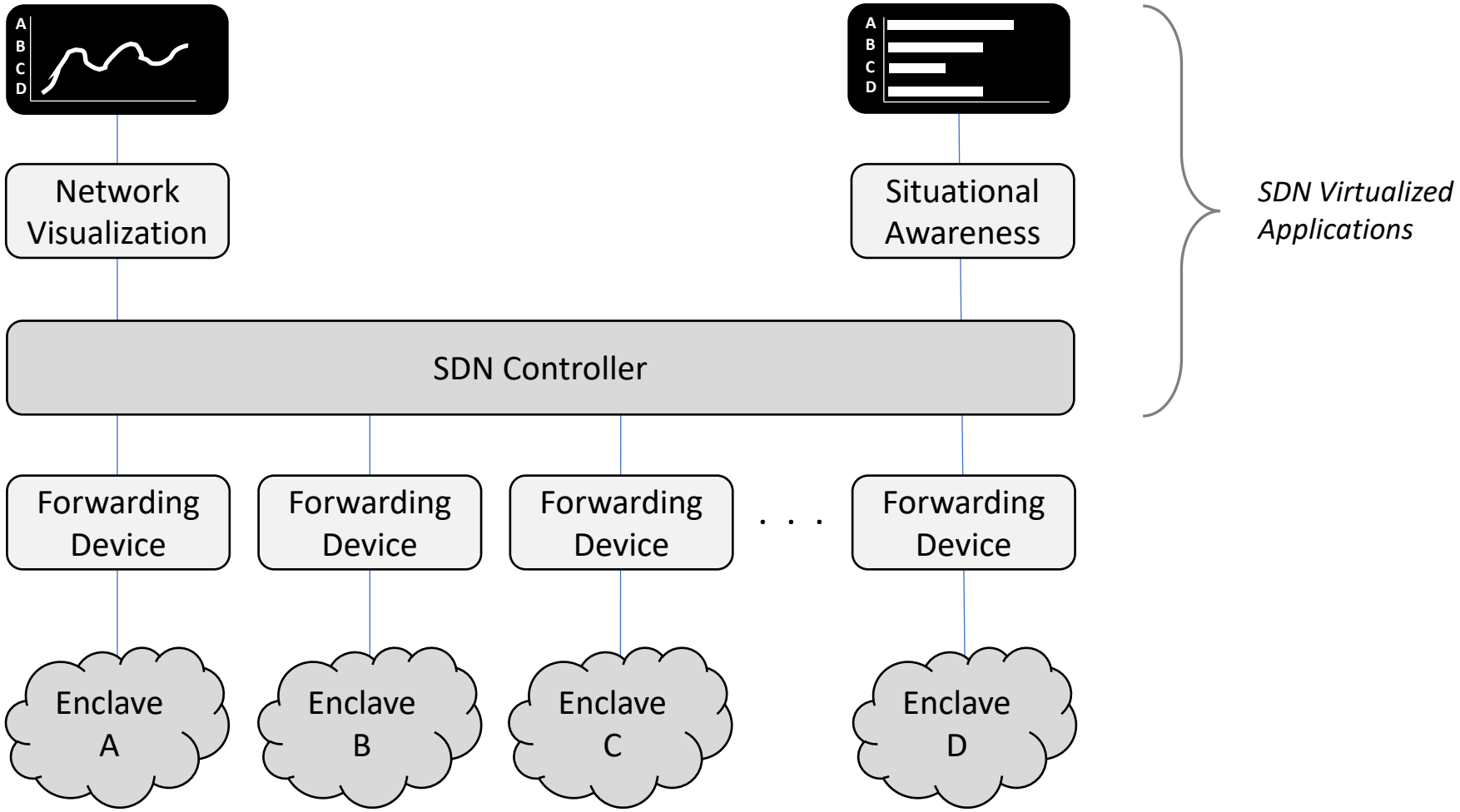
Week 12

SDN-Based Network Visualization and Situational Awareness



Week 12

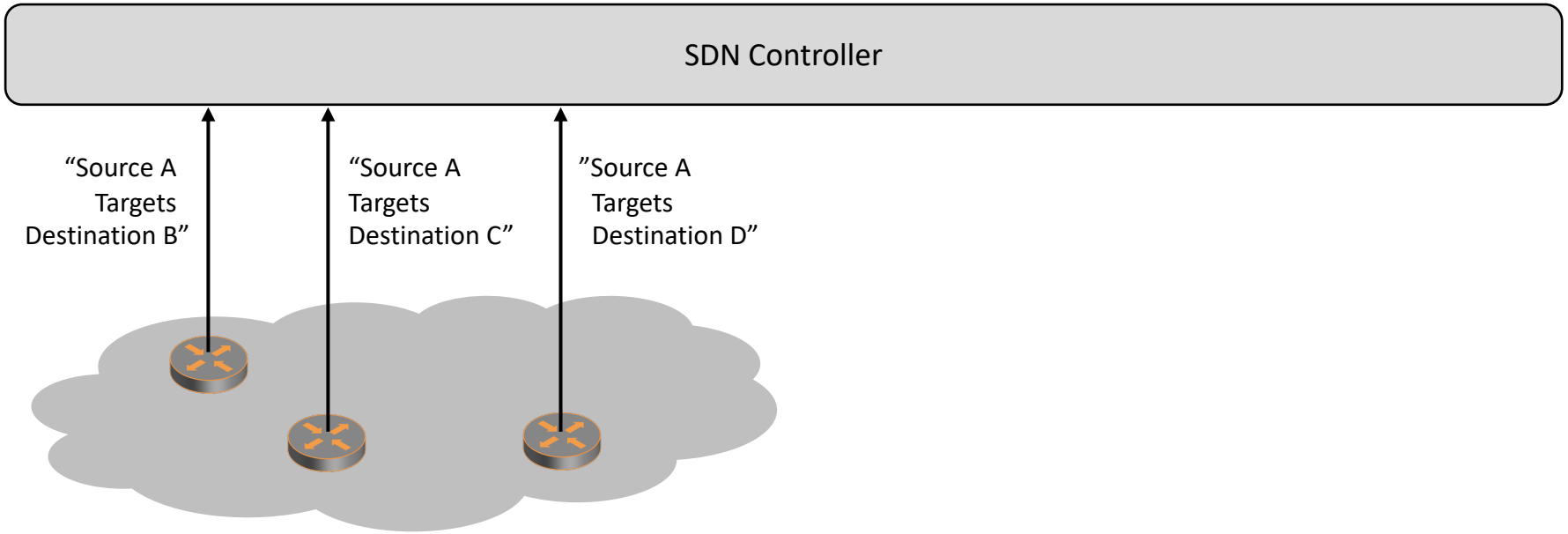
SDN-Based Network Visualization and Situational Awareness



Week 12

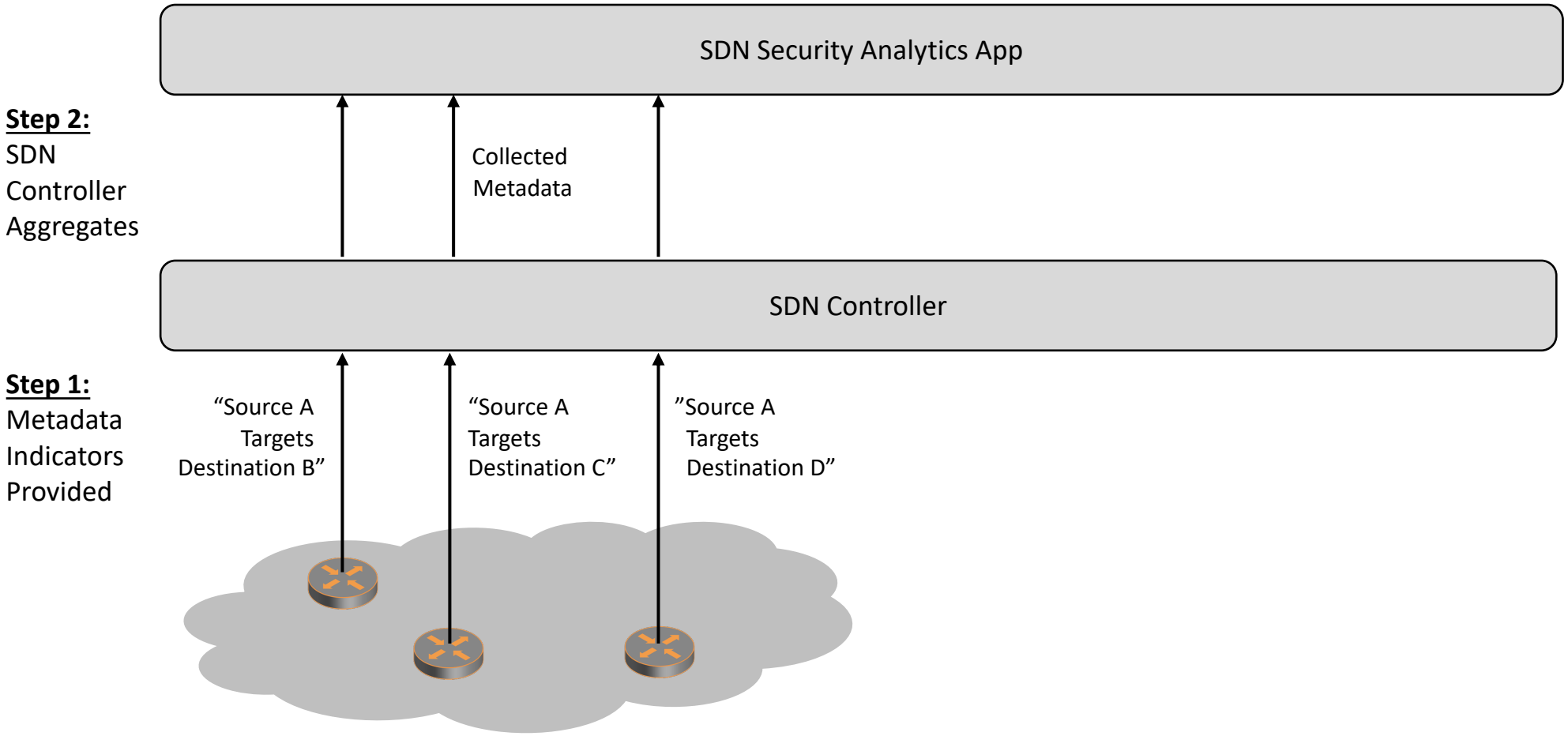
SDN Detection and Response (SDN-DR)

Step 1:
Metadata
Indicators
Provided



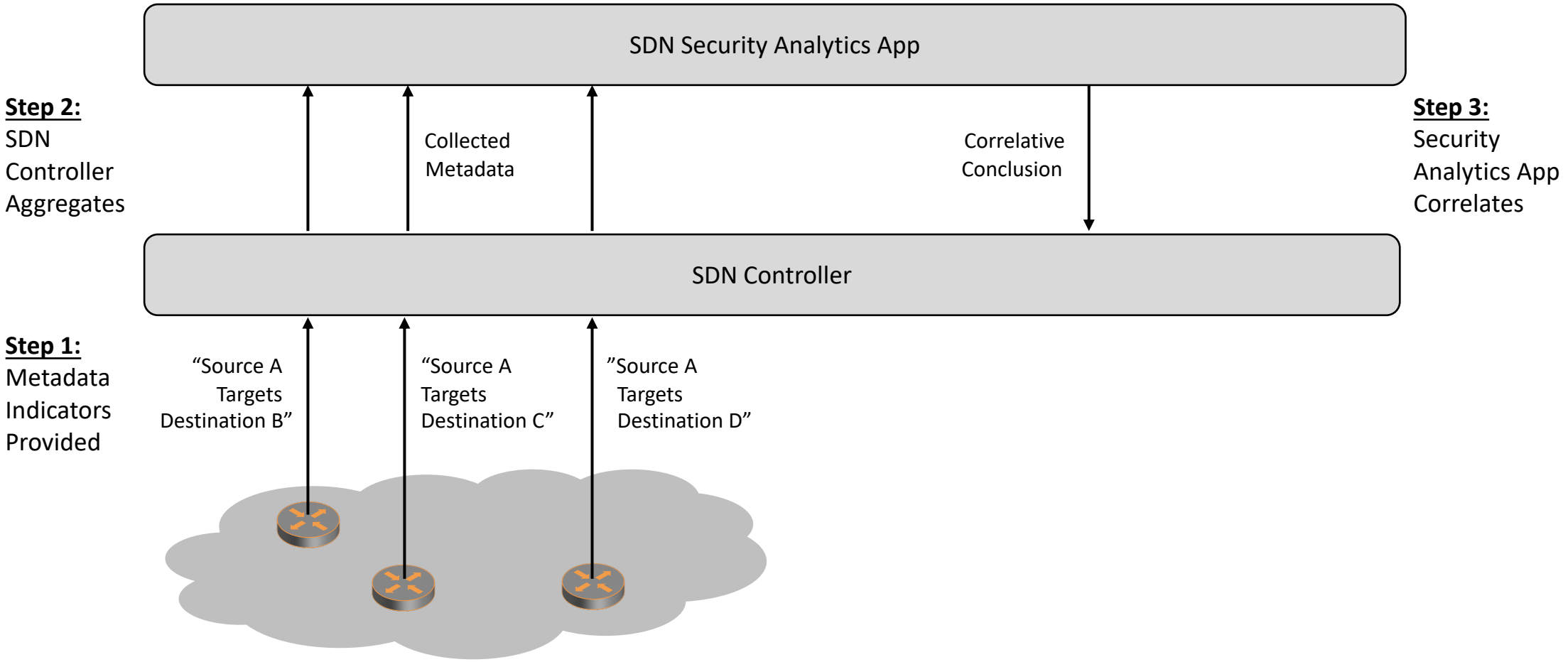
Week 12

SDN Detection and Response (SDN-DR)



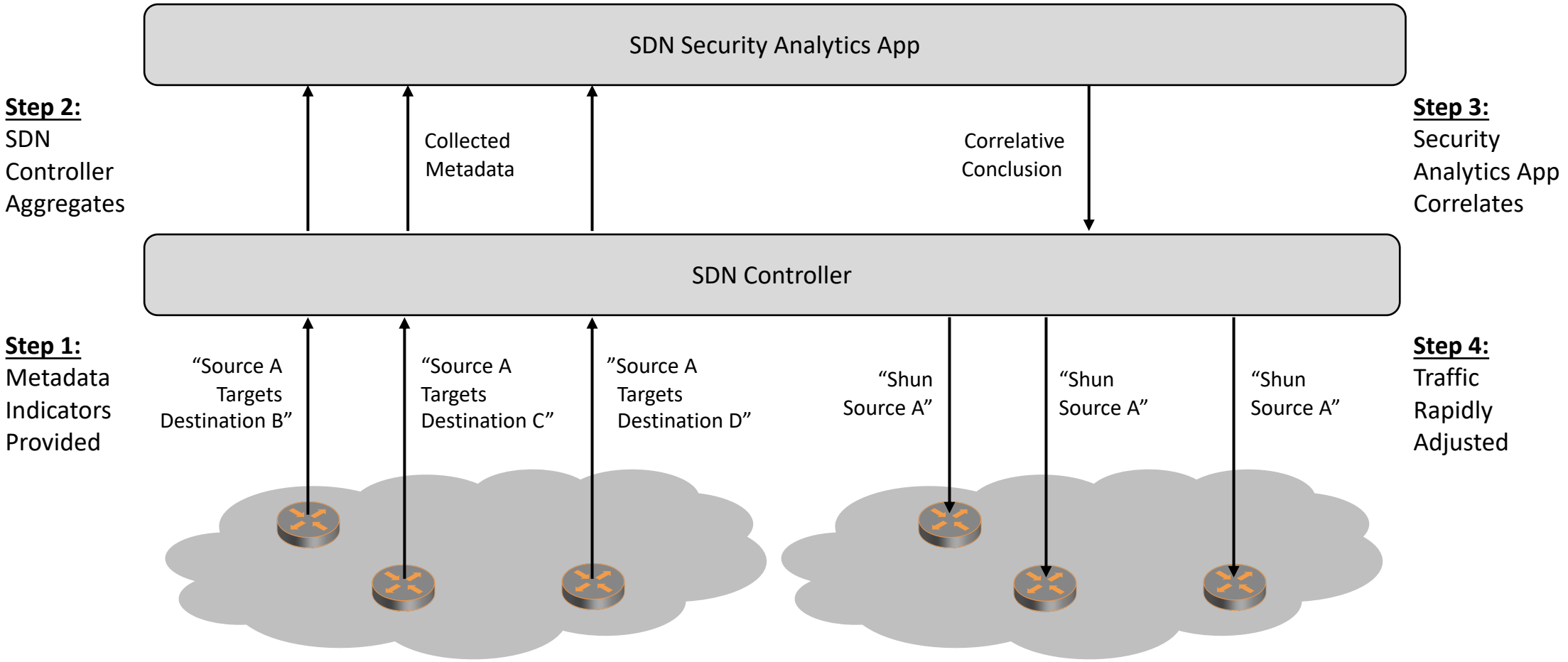
Week 12

SDN-Based Detection and Response (SDN-DR)



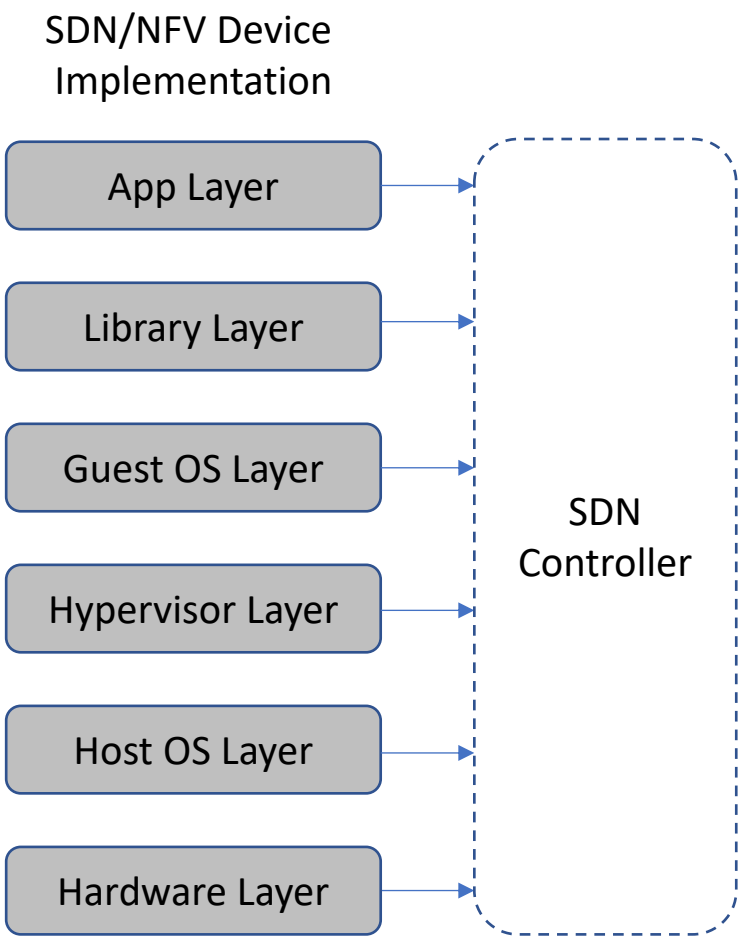
Week 12

SDN-Based Detection and Response (SDN-DR)



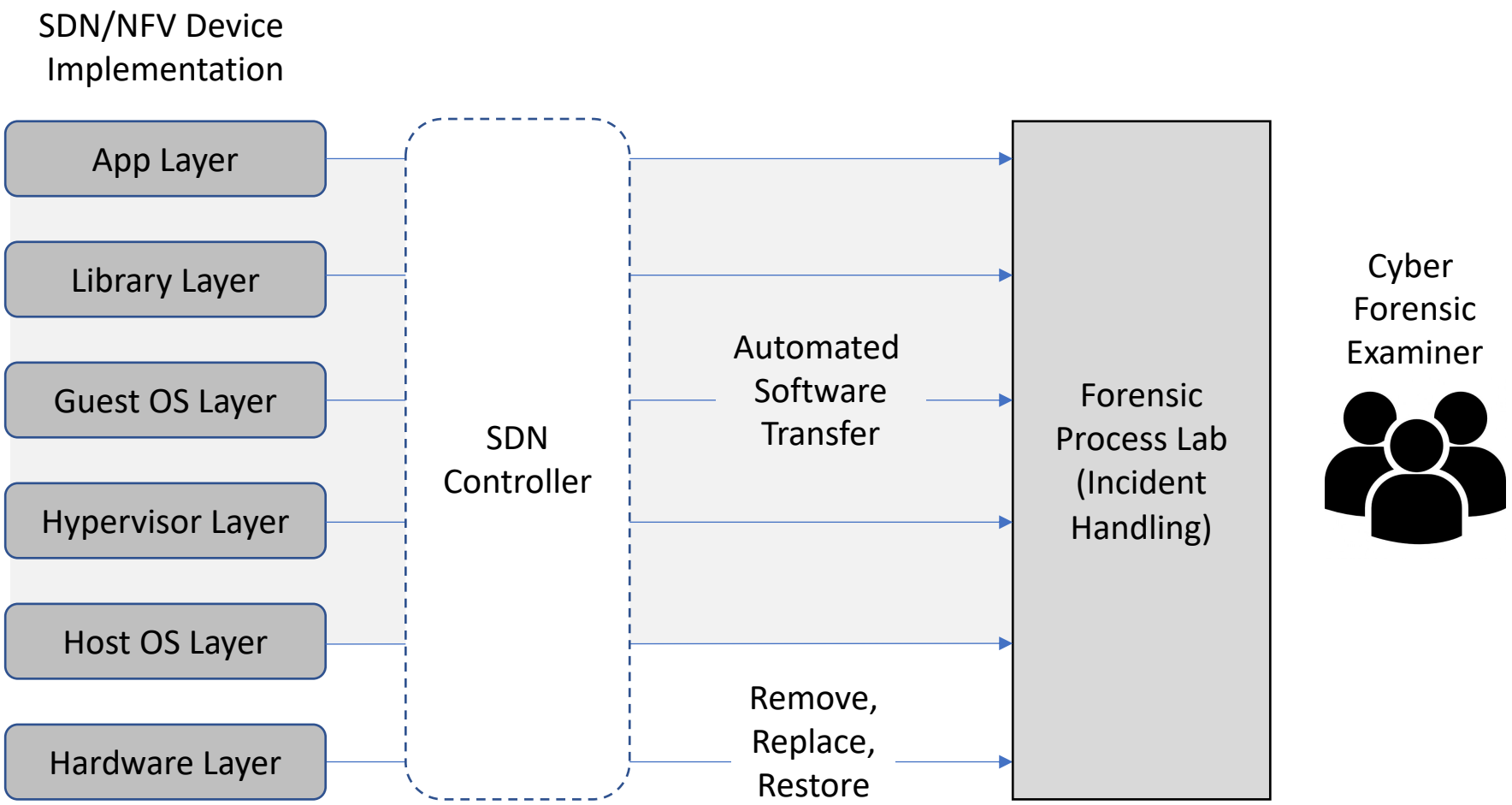
Week 12

Delivery of Forensic Artifacts via SDN



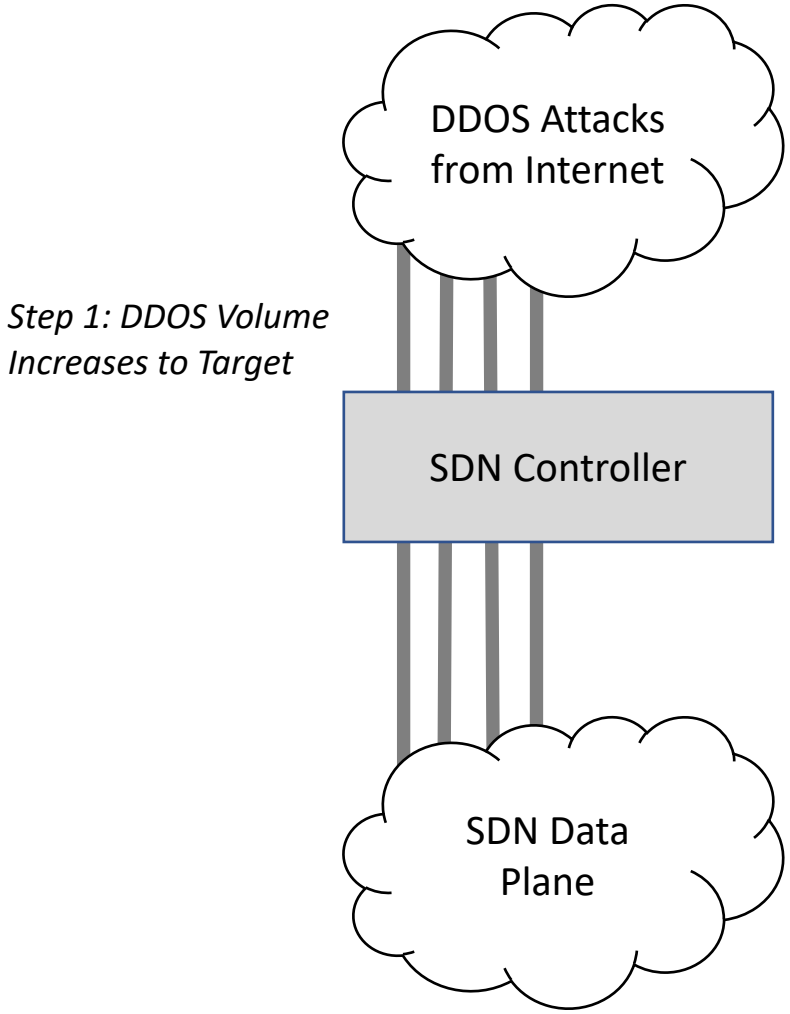
Week 12

Delivery of Forensic Artifacts via SDN



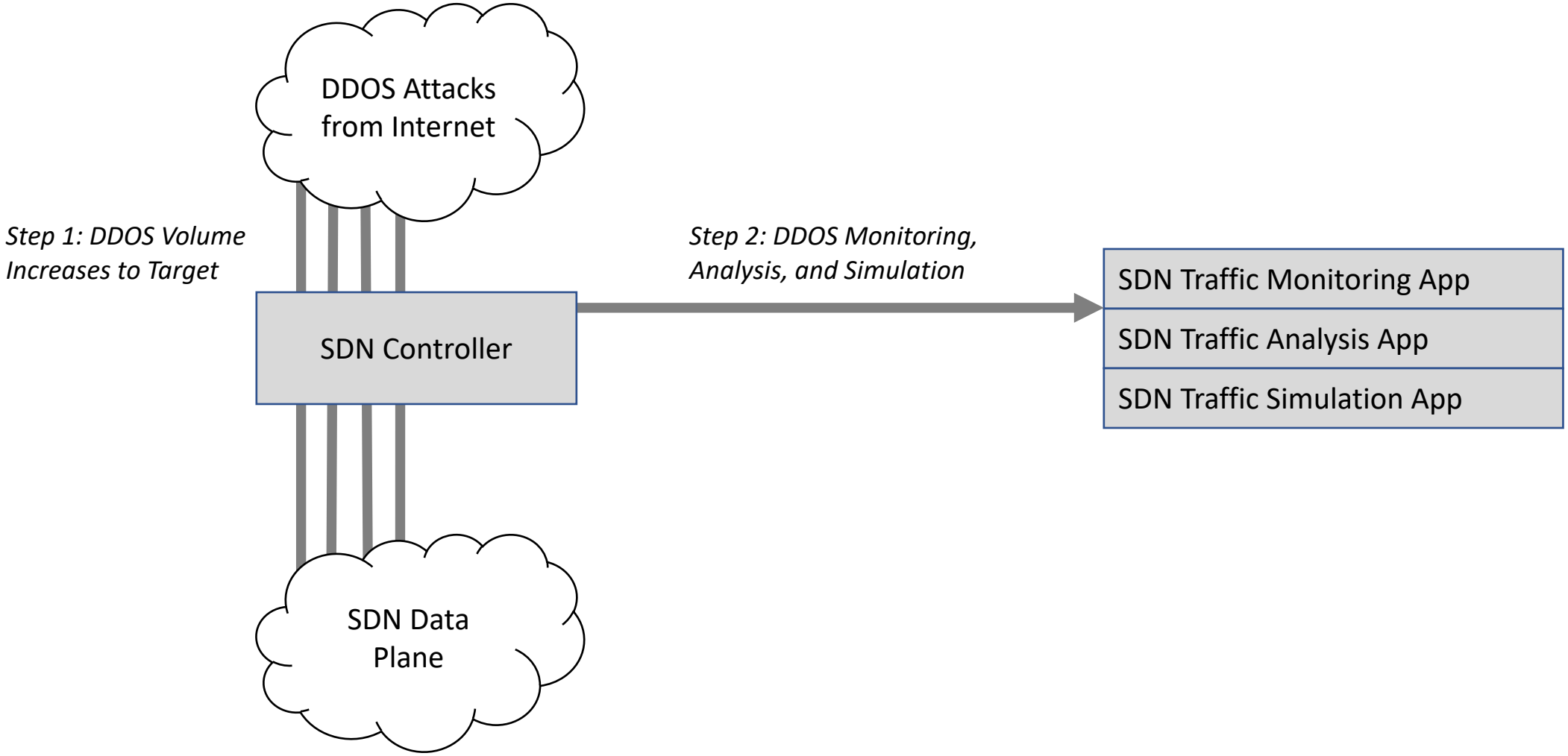
Week 12

Potential DDOS Delivery via SDN



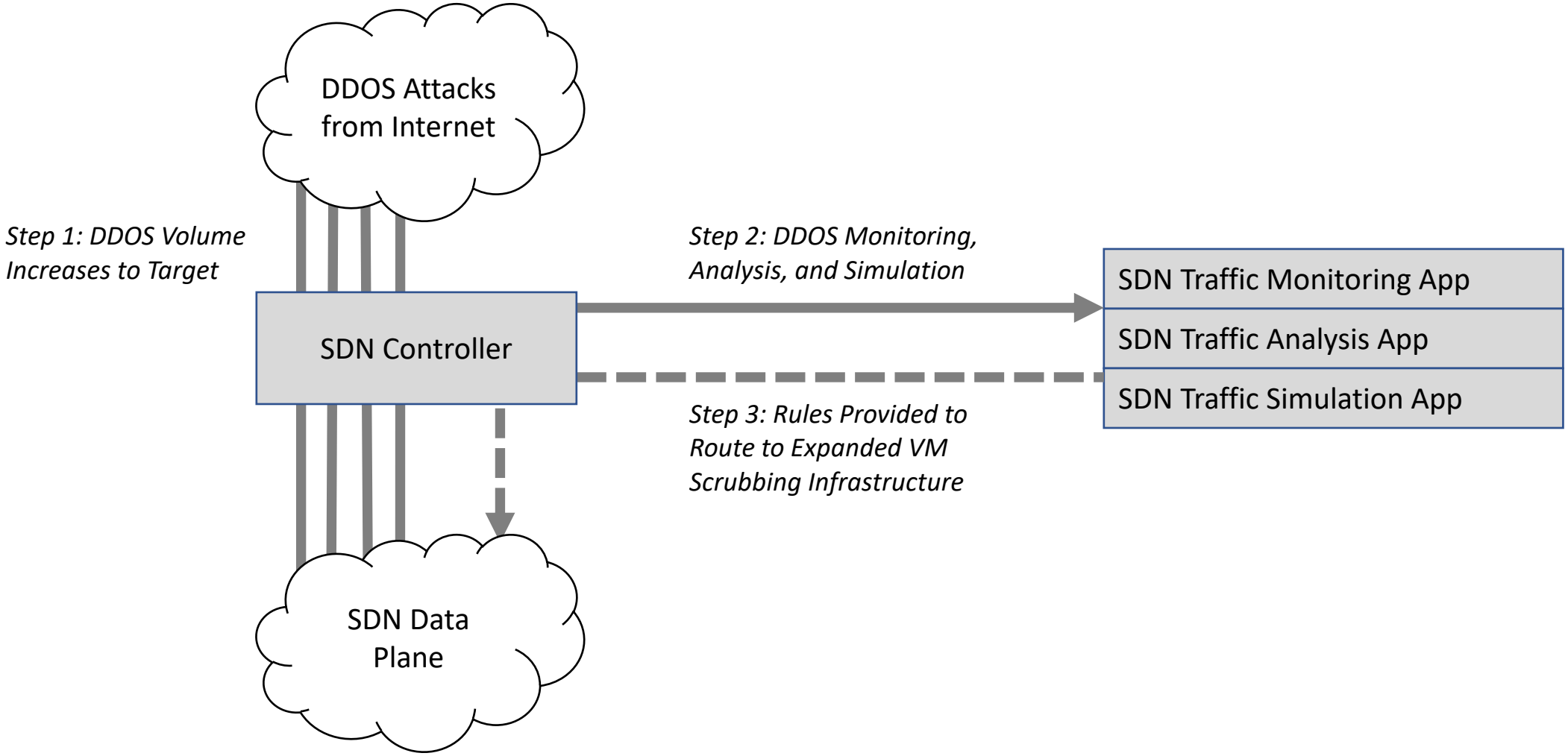
Week 12

Potential DDOS Delivery via SDN



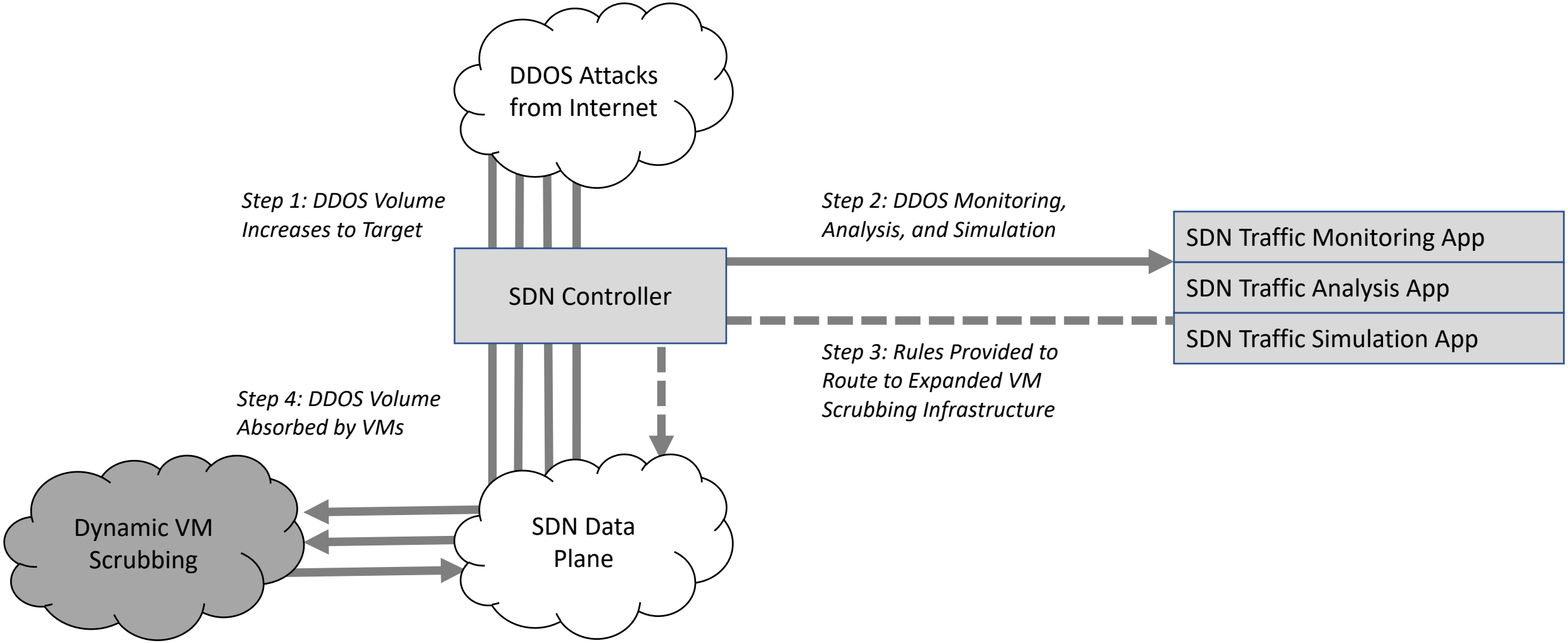
Week 12

Potential DDOS Delivery via SDN



Week 12

Potential DDOS Delivery via SDN

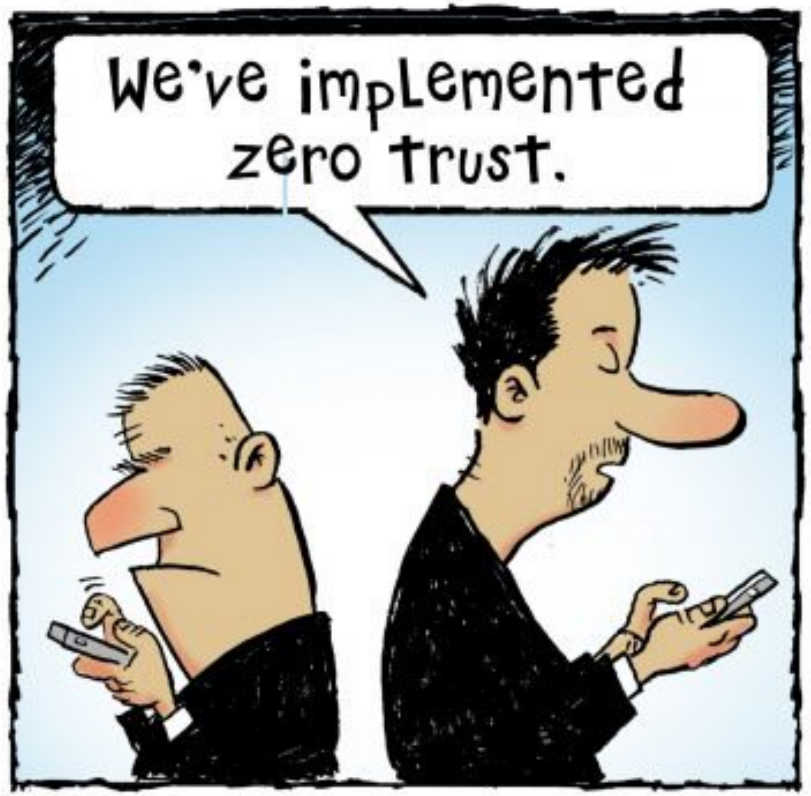


SDN Enables Dynamic, Expandable DDOS Attack Absorption

What is Zero Trust?

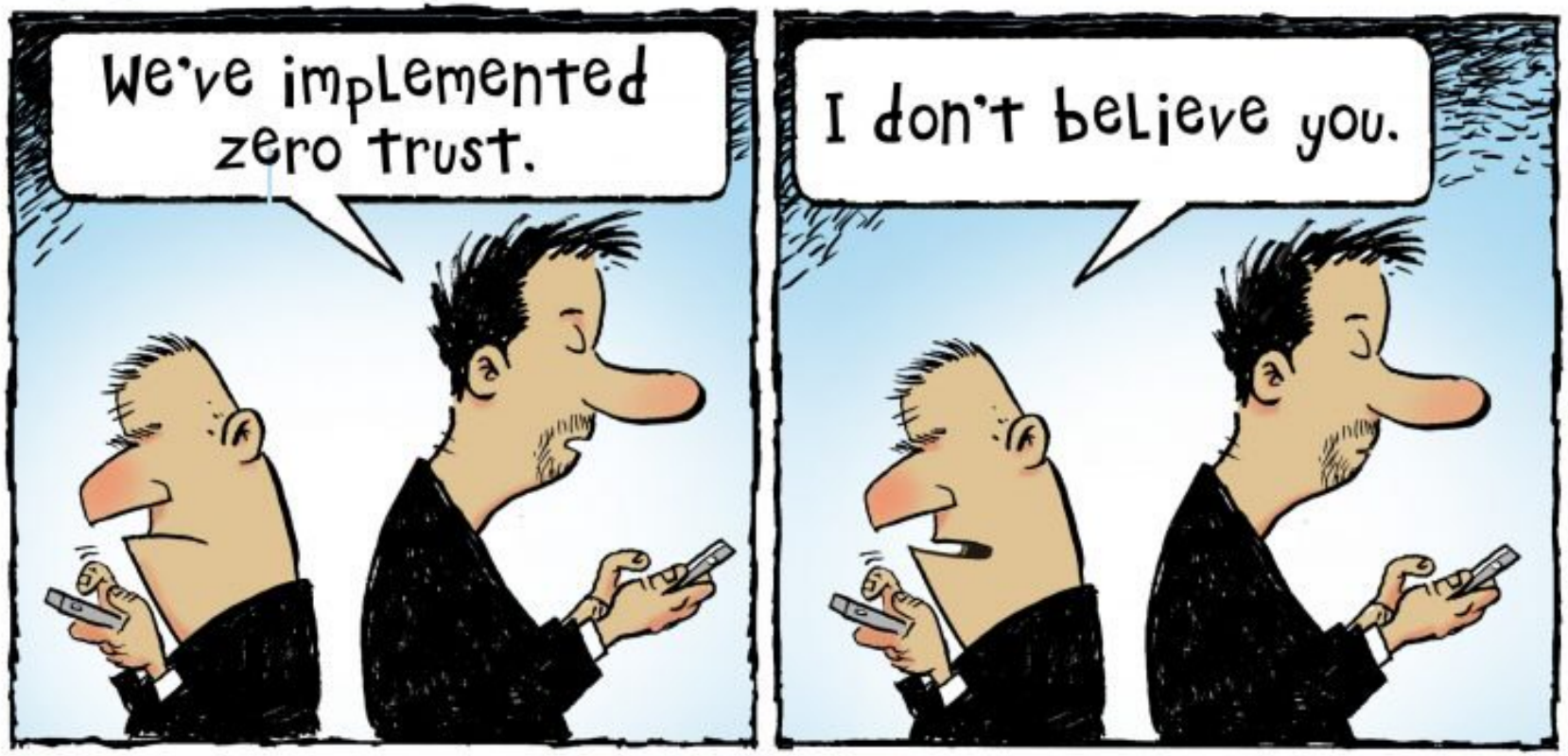
Week 12

Charlie Ciso



Week 12

Charlie Ciso



Week 12

Charlie Ciso

Week 12

What is Zero Trust?

- **Conceptual cyber security model for protection of apps and data**
  - Introduced by Forrester in 2010 (possibly earlier by Jericho Forum)

Week 12

What is Zero Trust?

- **Conceptual cyber security model for protection of apps and data**
  - Introduced by Forrester in 2010 (possibly earlier by Jericho Forum)
- **Identity verification versus perimeter protection**
  - Endpoint workloads are authenticated and authorized based on identity

Week 12

What is Zero Trust?

- **Conceptual cyber security model for protection of apps and data**
  - Introduced by Forrester in 2010 (possibly earlier by Jericho Forum)
- **Identity verification versus perimeter protection**
  - Endpoint workloads are authenticated and authorized based on identity
- **Trust no longer established by enterprise perimeter**
  - Firewall perimeters no longer a primary control in Zero Trust

Week 12

Perimeter Vulnerability: Target's 2014 Incident

40 Million Credit Cards Stolen from Target

- Hacked third-party vendor access unnoticed from 12/2/13 to 1/16/14
- CEO and CIO of Target apologized and resigned
- Remediation/legal costs: $162M (Target) and $200M (Banks)

Week 12

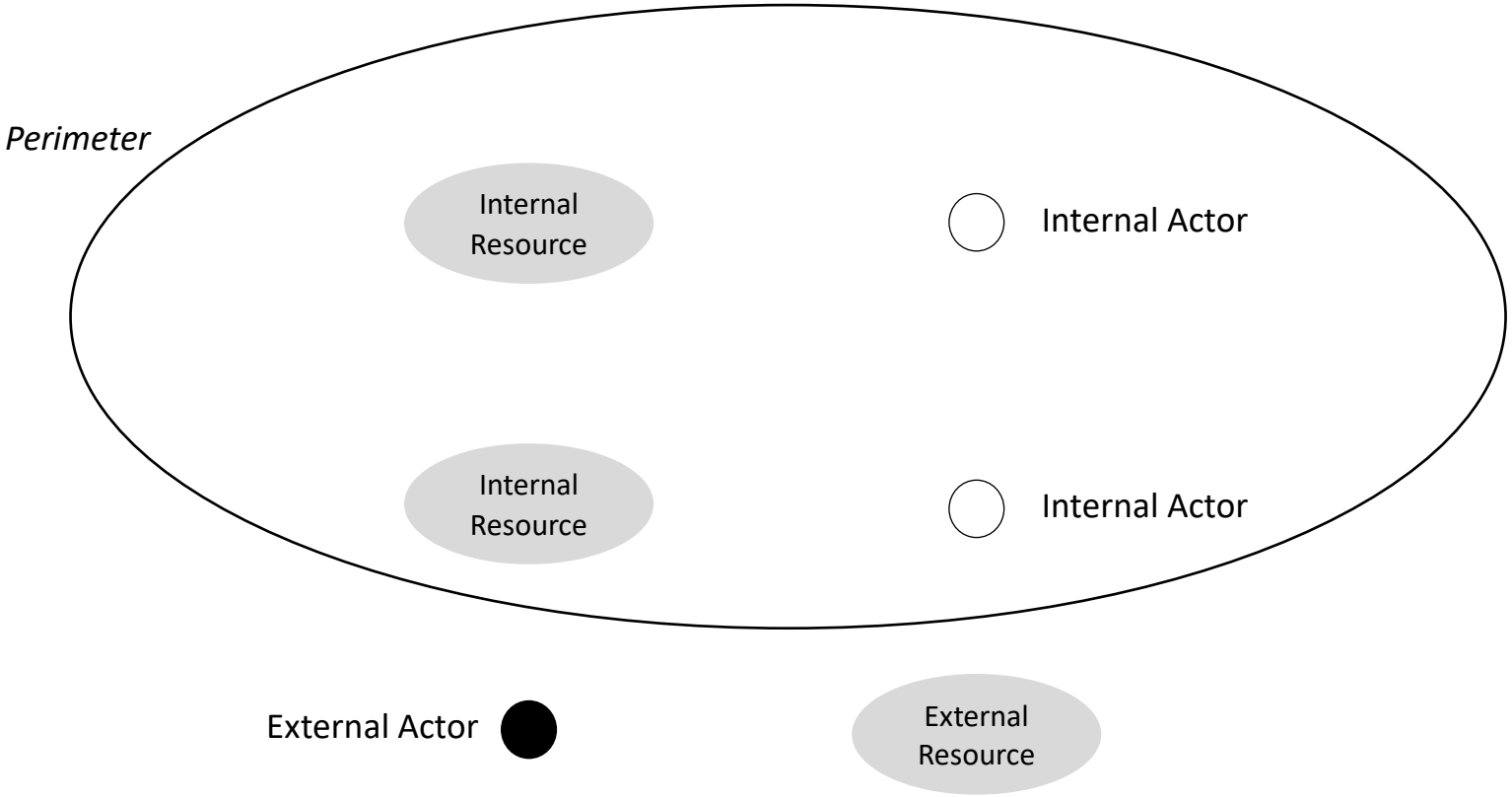
Perimeter Vulnerability: Home Depot's 2014 Incident

Five Month Undetected Attack at Home Depot

- Compromised 56 million customer payment cards
- CEO apologized publicly after the cyber attack
- Famous security budget retort from ex-employee: "We sell hammers."

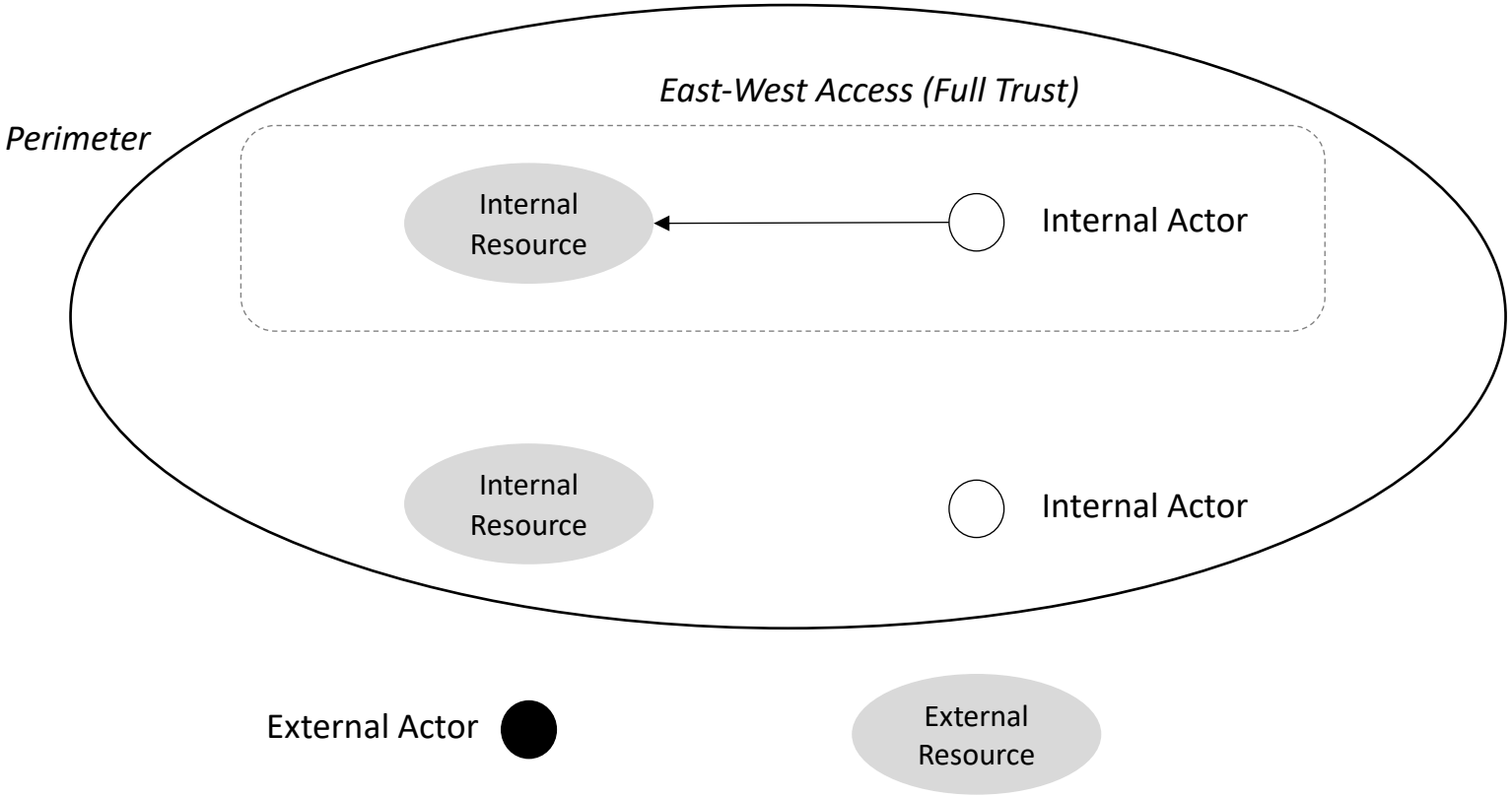
Week 12

North-South Versus East-West Access



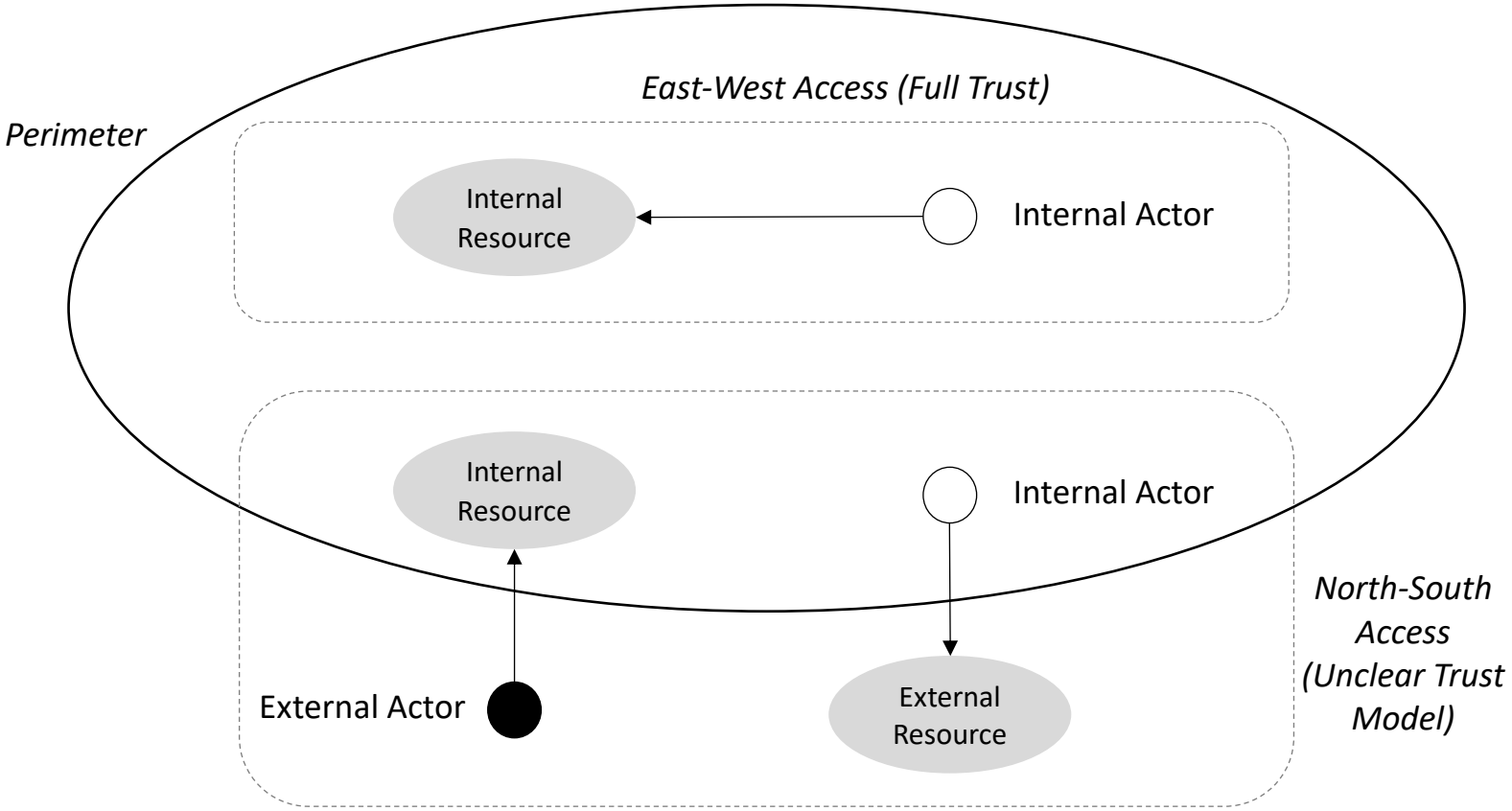
Week 12

North-South Versus East-West Access



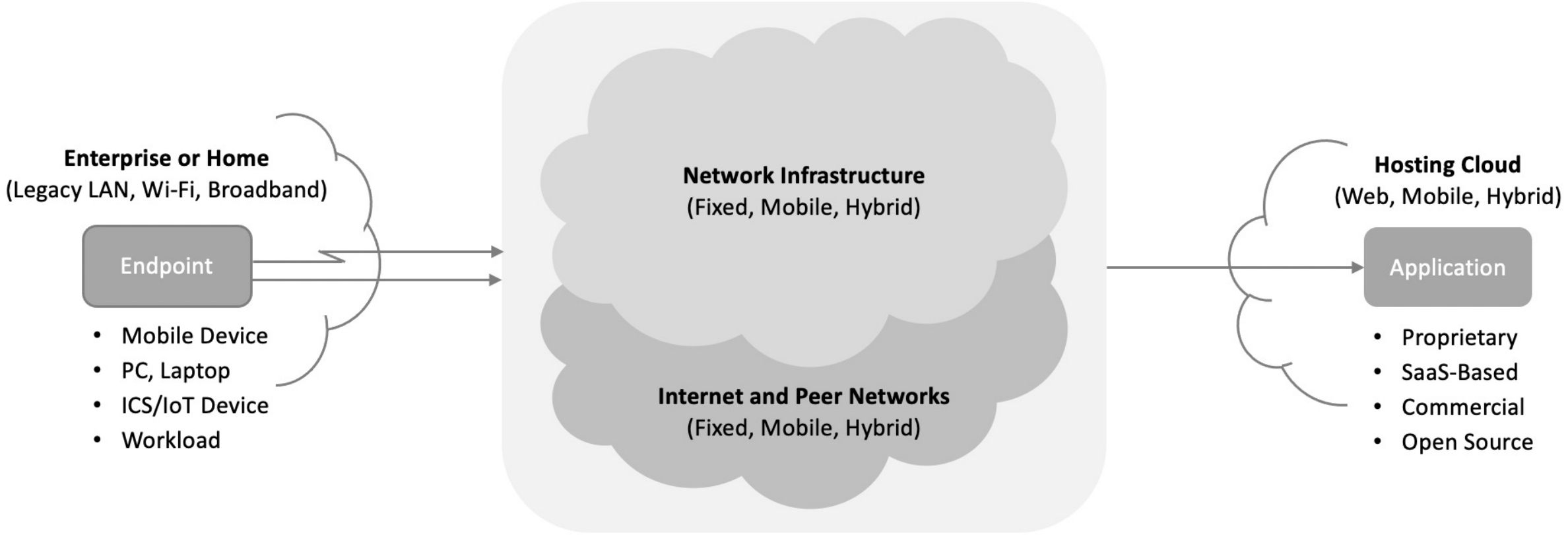
Week 12

North-South Versus East-West Access



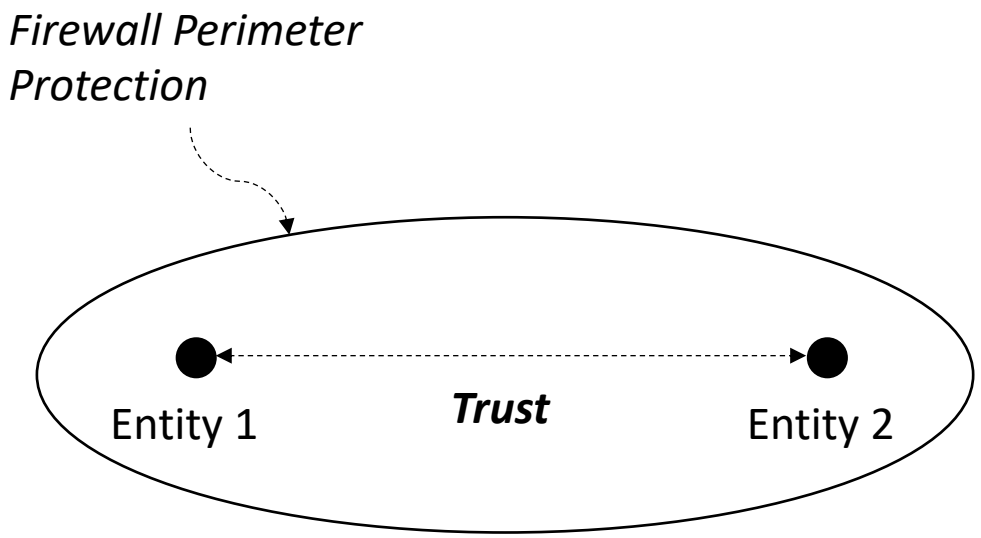
Week 12

Zero Trust Use Case – Endpoint Device to Cloud-Hosted App



Week 12

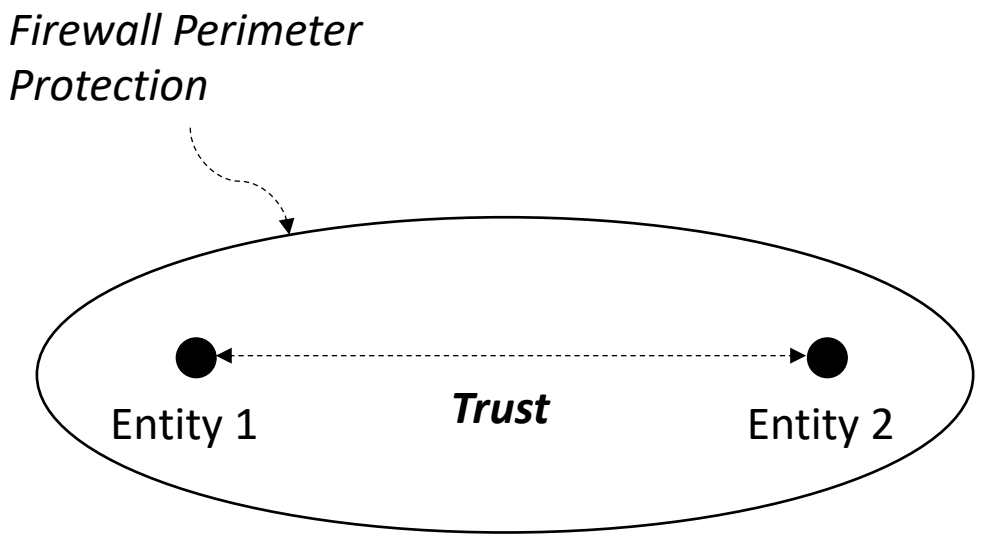
Firewall Perimeter Protection (Opposite of Zero Trust)

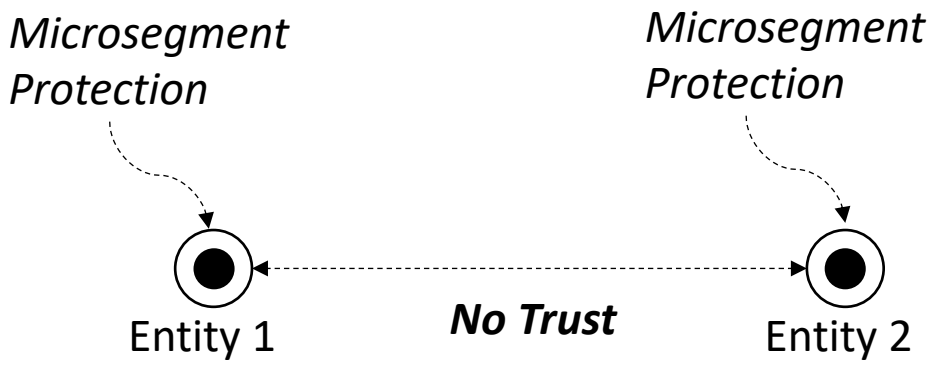


1. Entity 1 and 2 can share freely (bidirectional)
2. No mutual authentication (no 1FA, 2FA, etc.)
3. Shared boundary protection (perimeter)
4. Malware can traverse laterally from 1 to 2

Week 12

Comparison to Zero Trust with No Perimeter



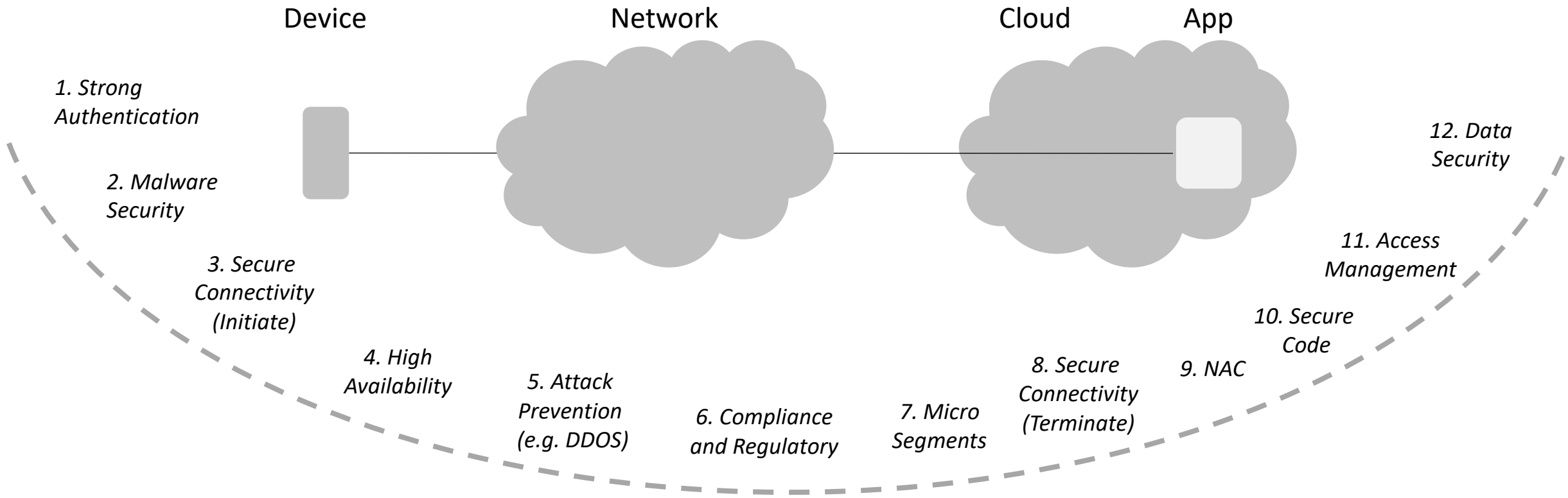


1. Entity 1 and 2 can share freely (bidirectional)
2. No mutual authentication (no 1FA, 2FA, etc.)
3. Shared boundary protection (perimeter)
4. Malware can traverse from 1 to 2 freely

1. Entity 1 and 2 will only share if necessary
2. Mutual authentication (1FA, 2FA, etc.)
3. Local boundary protections (no perimeter)
4. Malware cannot traverse from 1 to 2 freely

Week 12

Components of Zero Trust Network Access (ZTNA)



What are the Dimensions of Modern Data Protection?

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”
- **Data Lakes** – “Have I created large data lakes (likely in cloud) and how are they protected?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”
- **Data Lakes** – “Have I created large data lakes (likely in cloud) and how are they protected?”
- **Data Classification** – “What is the sensitivity of my data and how should it be marked?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”
- **Data Lakes** – “Have I created large data lakes (likely in cloud) and how are they protected?”
- **Data Classification** – “What is the sensitivity of my data and how should it be marked?”
- **Data Access Control** – “Who should be allowed to access what data under which conditions?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”
- **Data Lakes** – “Have I created large data lakes (likely in cloud) and how are they protected?”
- **Data Classification** – “What is the sensitivity of my data and how should it be marked?”
- **Data Access Control** – “Who should be allowed to access what data under which conditions?”
- **Data Encryption** – “What encryption lifecycle processes should be in place to protect my data?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”
- **Data Lakes** – “Have I created large data lakes (likely in cloud) and how are they protected?”
- **Data Classification** – “What is the sensitivity of my data and how should it be marked?”
- **Data Access Control** – “Who should be allowed to access what data under which conditions?”
- **Data Encryption** – “What encryption lifecycle processes should be in place to protect my data?”
- **Data Governance** – “How should the overall data management lifecycle process be governed?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”
- **Data Lakes** – “Have I created large data lakes (likely in cloud) and how are they protected?”
- **Data Classification** – “What is the sensitivity of my data and how should it be marked?”
- **Data Access Control** – “Who should be allowed to access what data under which conditions?”
- **Data Encryption** – “What encryption lifecycle processes should be in place to protect my data?”
- **Data Governance** – “How should the overall data management lifecycle process be governed?”
- **Data Privacy** – “What privacy rights to data owners have and how are they enforced?”

Week 12

Dimensions of Modern Enterprise Data Protection

- **Data Discovery** – “Where is my data located (including cloud and SaaS)?”
- **Data Inventory** – “Do I have an accurate catalog of my data including relevant metadata?”
- **Data Lakes** – “Have I created large data lakes (likely in cloud) and how are they protected?”
- **Data Classification** – “What is the sensitivity of my data and how should it be marked?”
- **Data Access Control** – “Who should be allowed to access what data under which conditions?”
- **Data Encryption** – “What encryption lifecycle processes should be in place to protect my data?”
- **Data Governance** – “How should the overall data management lifecycle process be governed?”
- **Data Privacy** – “What privacy rights to data owners have and how are they enforced?”
- **Data Leakage Prevention** – “How do I make sure my data doesn’t leak to unauthorized users?”

What is Data Leakage Prevention (DLP)?

Week 12

What is Data Leakage Prevention (DLP)?

- **DLP is an enterprise cyber security control designed to prevent sensitive data from leaking out to unauthorized individuals or groups**
  - Often referenced as data leakage prevention, data leakage protection, and data loss prevention (all roughly synonymous)

Week 12

What is Data Leakage Prevention (DLP)?

- **DLP is an enterprise cyber security control designed to prevent sensitive data from leaking out to unauthorized individuals or groups**
  - Often referenced as data leakage prevention, data leakage protection, and data loss prevention (all roughly synonymous)
- **DLP controls address two primary enterprise use-cases**
  - Deliberate and malicious actions by an adversary to intentionally leak data outside a protected enclave
  - Accidental and non-malicious mistaken action where data is inadvertently shared with unauthorized entities

Week 12

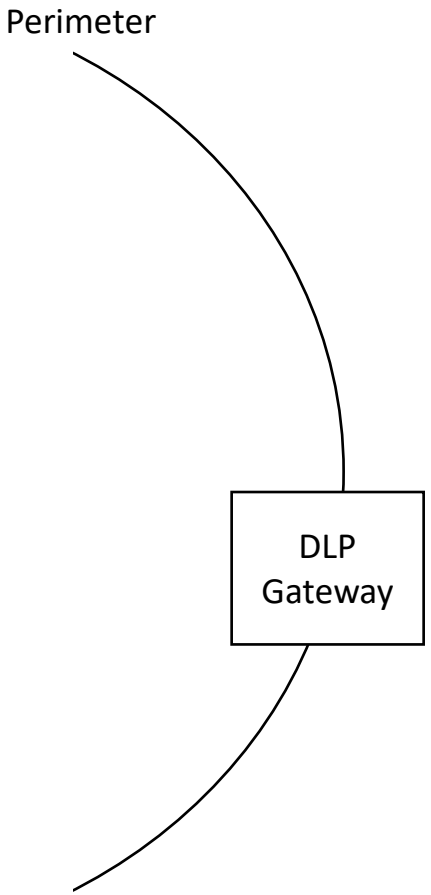
What is Data Leakage Prevention (DLP)?

- **DLP is an enterprise cyber security control designed to prevent sensitive data from leaking out to unauthorized individuals or groups**
  - Often referenced as data leakage prevention, data leakage protection, and data loss prevention (all roughly synonymous)
- **DLP controls address two primary enterprise use-cases**
  - Deliberate and malicious actions by an adversary to intentionally leak data outside a protected enclave
  - Accidental and non-malicious mistaken action where data is inadvertently shared with unauthorized entities
- **DLP tools and platforms typically include many types of functional methods**
  - Data classification, content inspection, contextual analysis, incident response, and real-time mitigation

Week 12

Original DLP Methodology

Step 1: Internal actor classifies and explicitly marks internal data



Week 12

Original DLP Methodology

Process is prone to error and poor judgment

Step 1: Internal actor classifies and explicitly marks internal data

Step 1': Internal actor might not classify and explicitly mark some internal data

Perimeter

DLP Gateway

Week 12

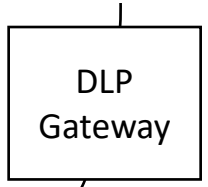
Original DLP Methodology

Step 1: Internal actor classifies and explicitly marks internal data

Step 1': Internal actor might not classify and explicitly mark some internal data

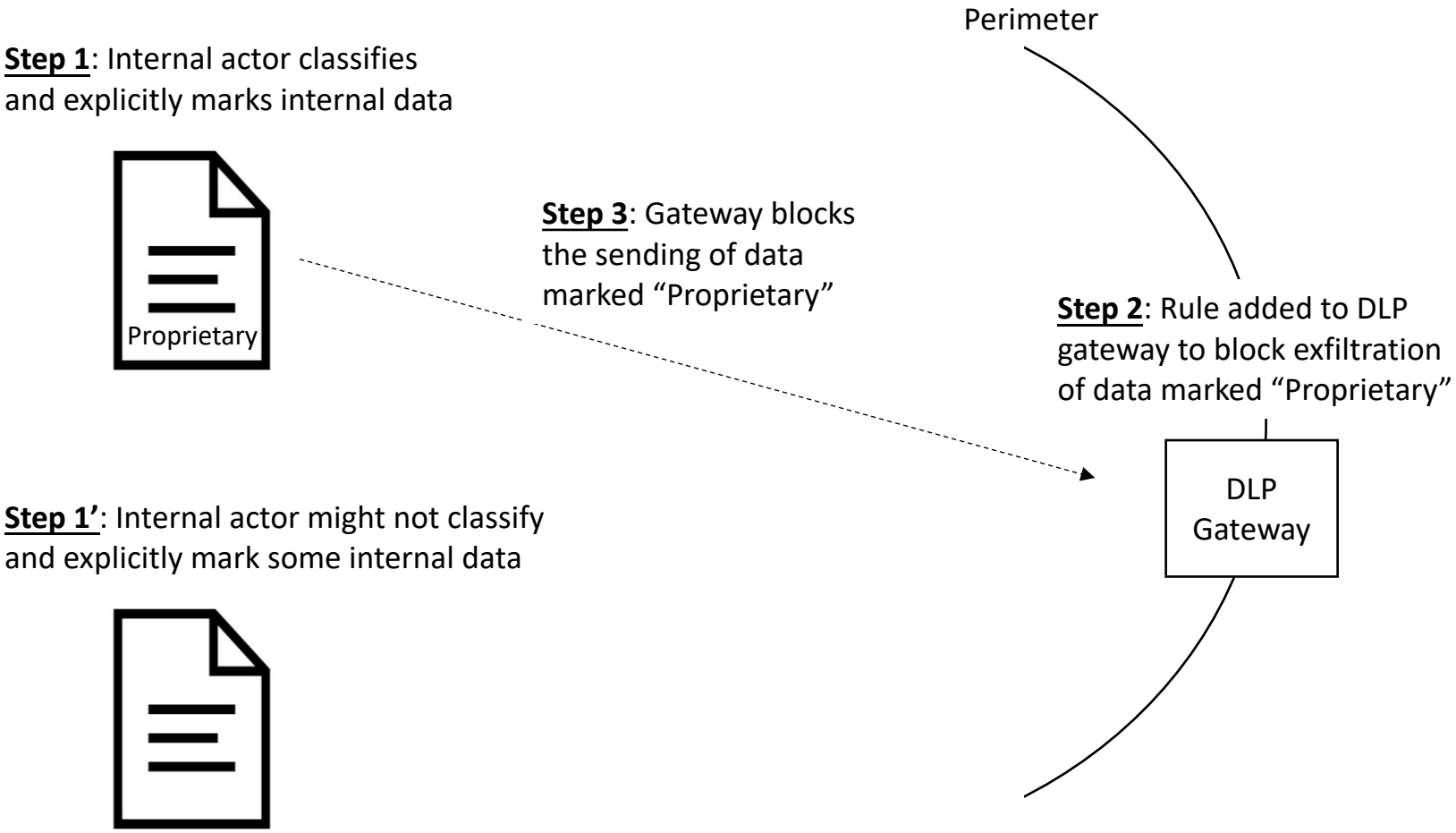
Perimeter

Step 2: Rule added to DLP gateway to block exfiltration of data marked "Proprietary"



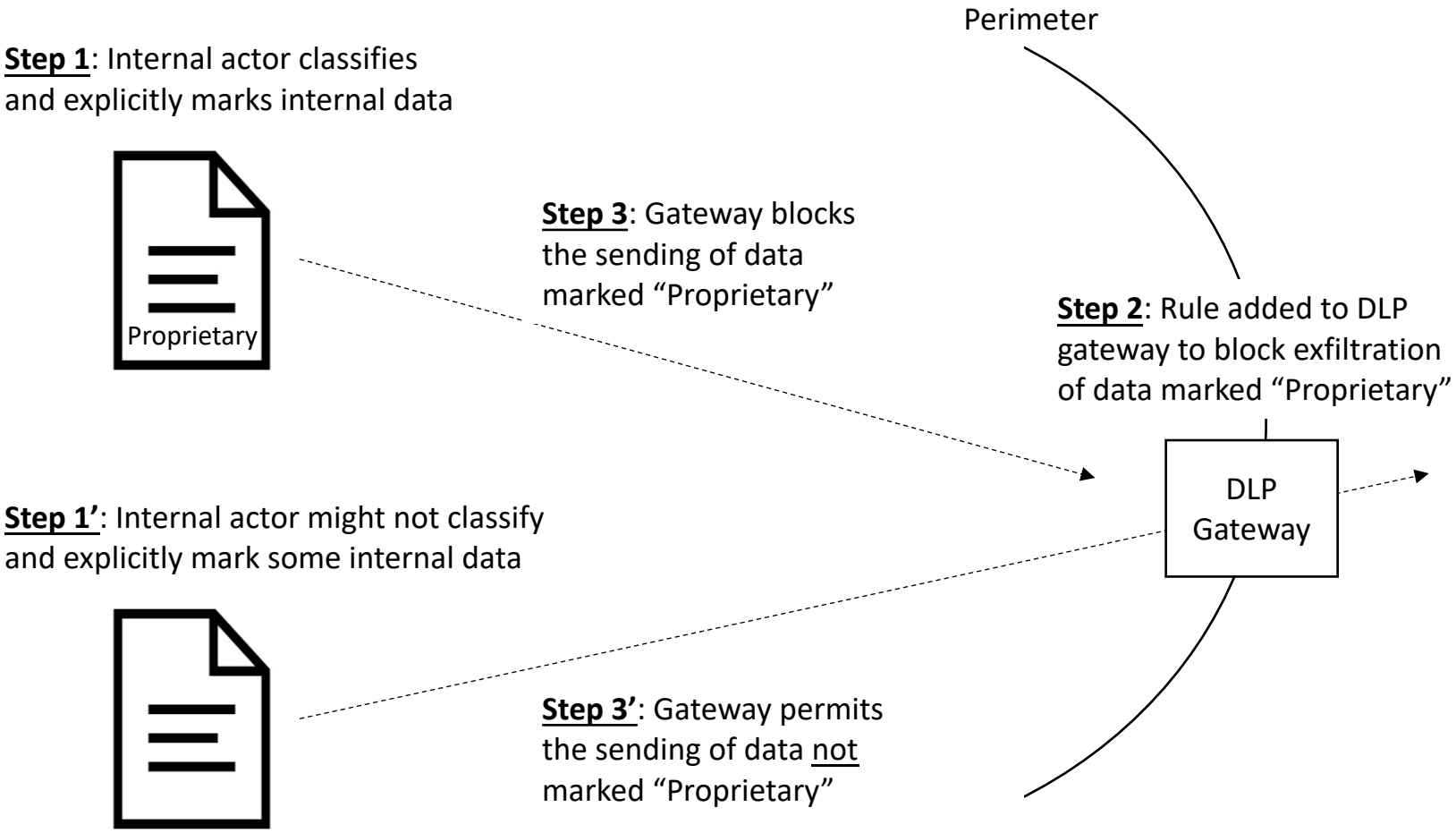
Week 12

Original DLP Methodology



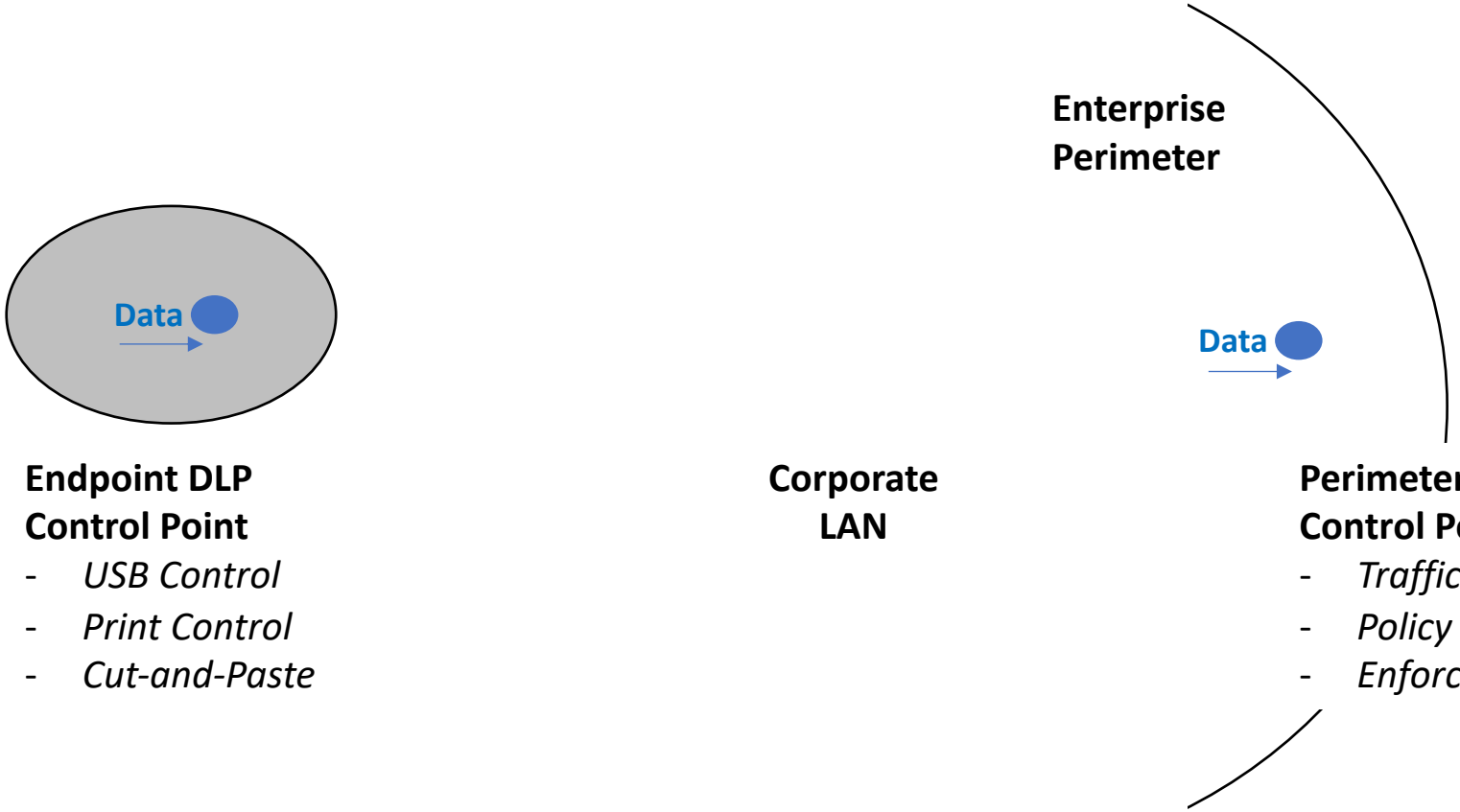
Week 12

Original DLP Methodology



Week 12

Traditional DLP Control Points – First Generation



Endpoint DLP Control Point

- *USB Control*
- *Print Control*
- *Cut-and-Paste*

Corporate LAN

Perimeter DLP Control Point

- *Traffic Scan*
- *Policy Rules*
- *Enforce/Log*

Week 12

Enhanced DLP Control Points – Second Generation

Endpoint DLP Control Point

- *USB Control*
- *Print Control*
- *Cut-and-Paste*
- ***Heuristic Processing***
- ***Behavioral Analytics***
- ***Predictive Security***
- ***UBA Integration***

Corporate LAN

Perimeter DLP Control Point

- *Traffic Scan*
- *Policy Rules*
- *Enforce/Log*
- ***Heuristic Processing***
- ***Behavioral Analytics***
- ***Predictive Security***
- ***UBA Integration***

What is a Secure Web Gateway (SWG)?

Week 12

What is a Secure Web Gateway (SWG)?

- **A Secure Web Gateway (SWG) is a deployed network security system that prevents inbound threats to internal trusted users.**
  - Excellent option for perimeter-based networks with gateway chokepoints to and from data centers.

Week 12

What is a Secure Web Gateway (SWG)?

- **A Secure Web Gateway (SWG) is a deployed network security system that prevents inbound threats to internal trusted users.**
  - Excellent option for perimeter-based networks with gateway chokepoints to and from data centers.
- **Typical SWG functions include URL filtering, malicious code protection, and application-level controls for major web applications.**
  - Increasingly seeing extension to include DLP and other functions as adversary threats have intensified.

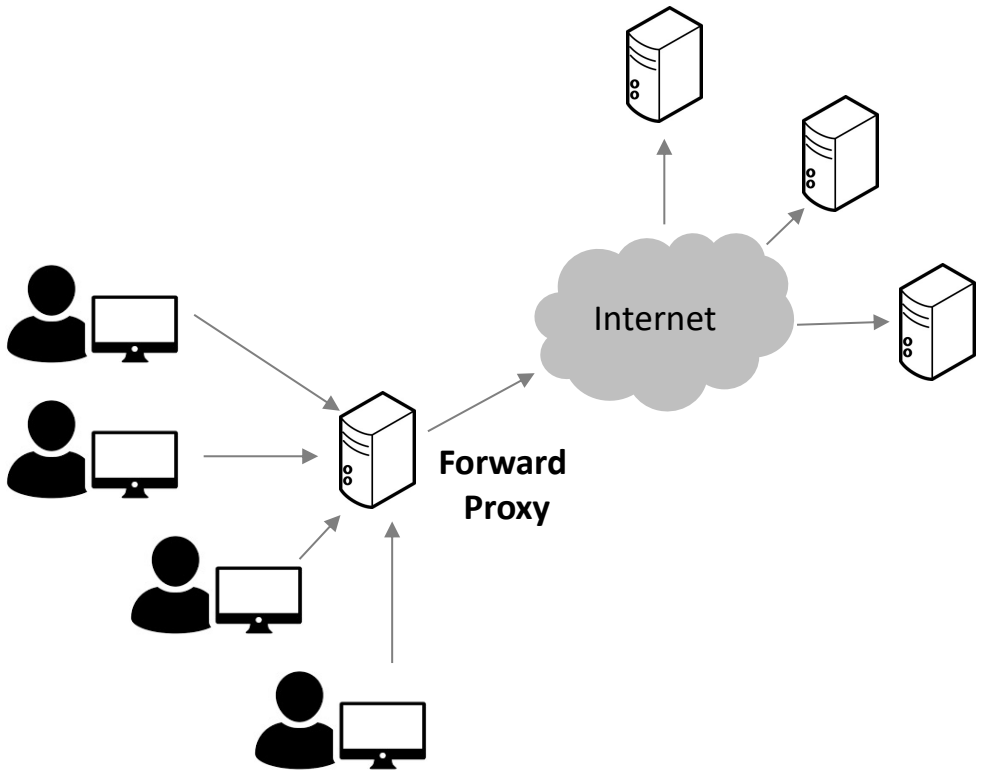
Week 12

What is a Secure Web Gateway (SWG)?

- **A Secure Web Gateway (SWG) is a deployed network security system that prevents inbound threats to internal trusted users.**
  - Excellent option for perimeter-based networks with gateway chokepoints to and from data centers.
- **Typical SWG functions include URL filtering, malicious code protection, and application-level controls for major web applications.**
  - Increasingly seeing extension to include DLP and other functions as adversary threats have intensified.
- **SWGs include many modes of deployed operation such as advisory, discretionary, and mandatory control implementation.**
  - SWG control of access to inappropriate content and improper sites complicates the security mission.

Week 12

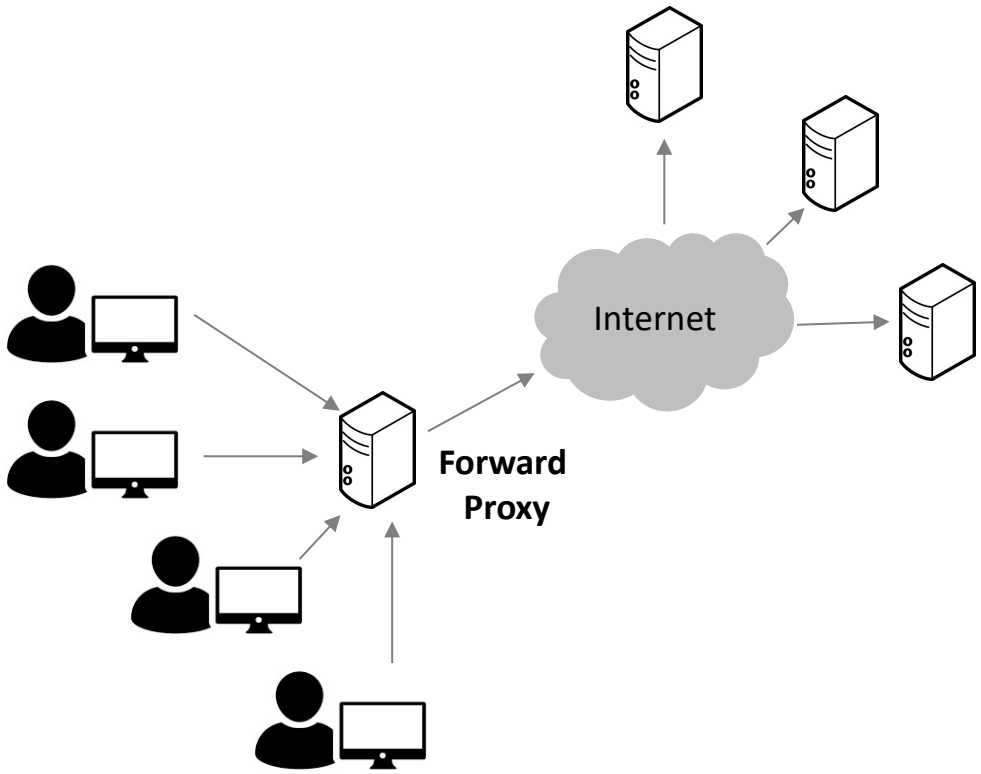
Understanding Proxy Operations



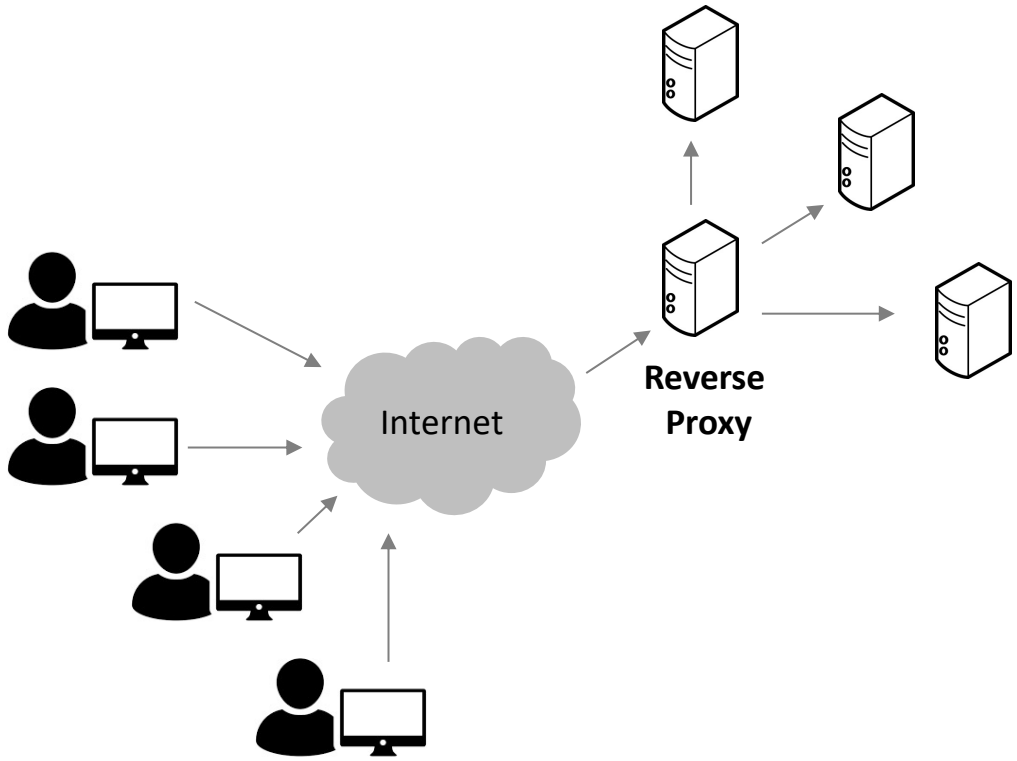
Protects Users from Malicious Content Access (Inbound to Users)

Week 12

Understanding Proxy Operations



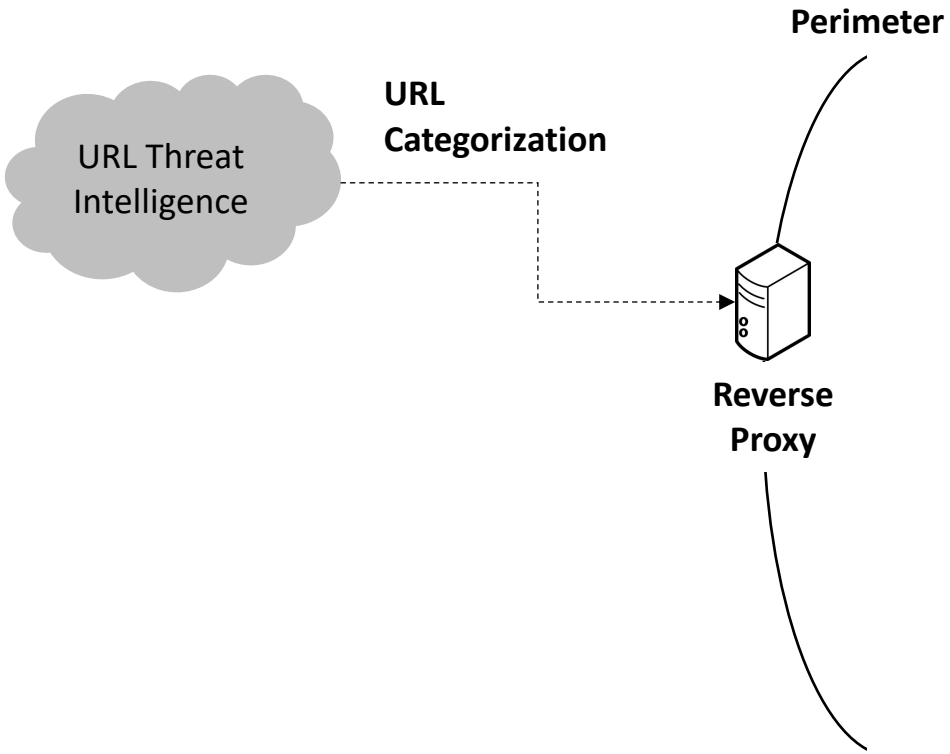
Protects Users from Malicious Content Access (Inbound to Users)



Protects Servers from Malicious Content Access (Inbound to Servers)

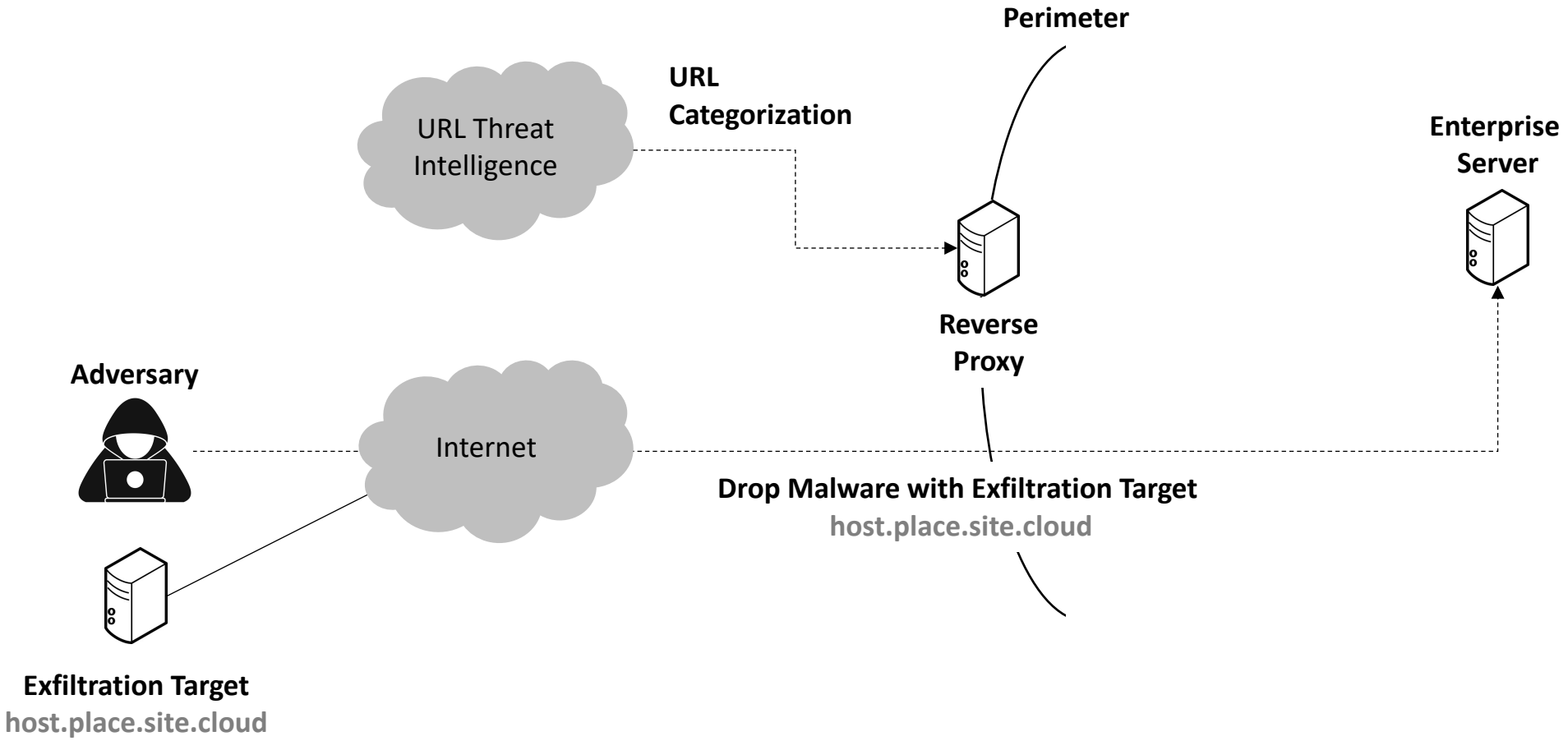
Week 12

Preventing Data Exfiltration with Reverse Proxy



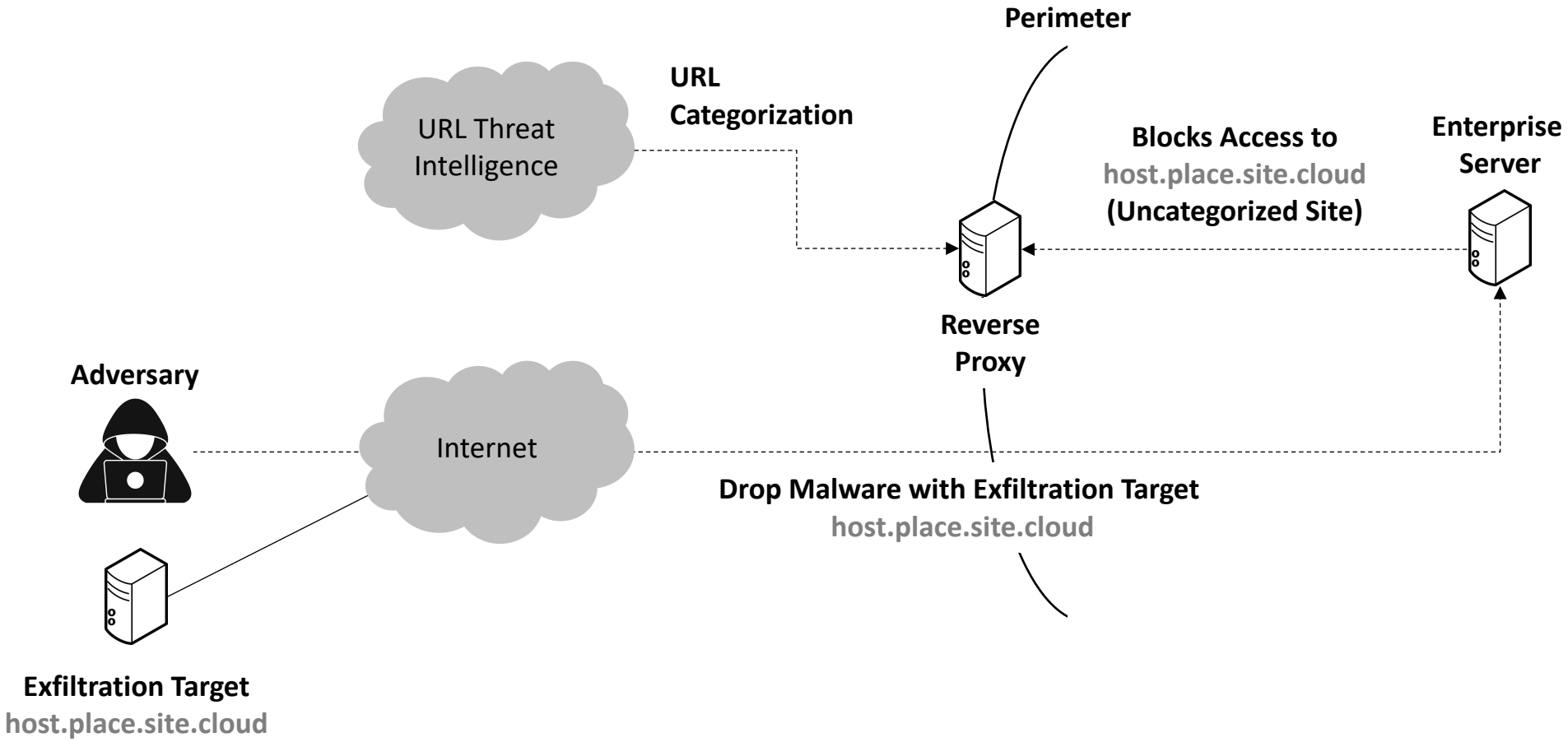
Week 12

Preventing Data Exfiltration with Reverse Proxy



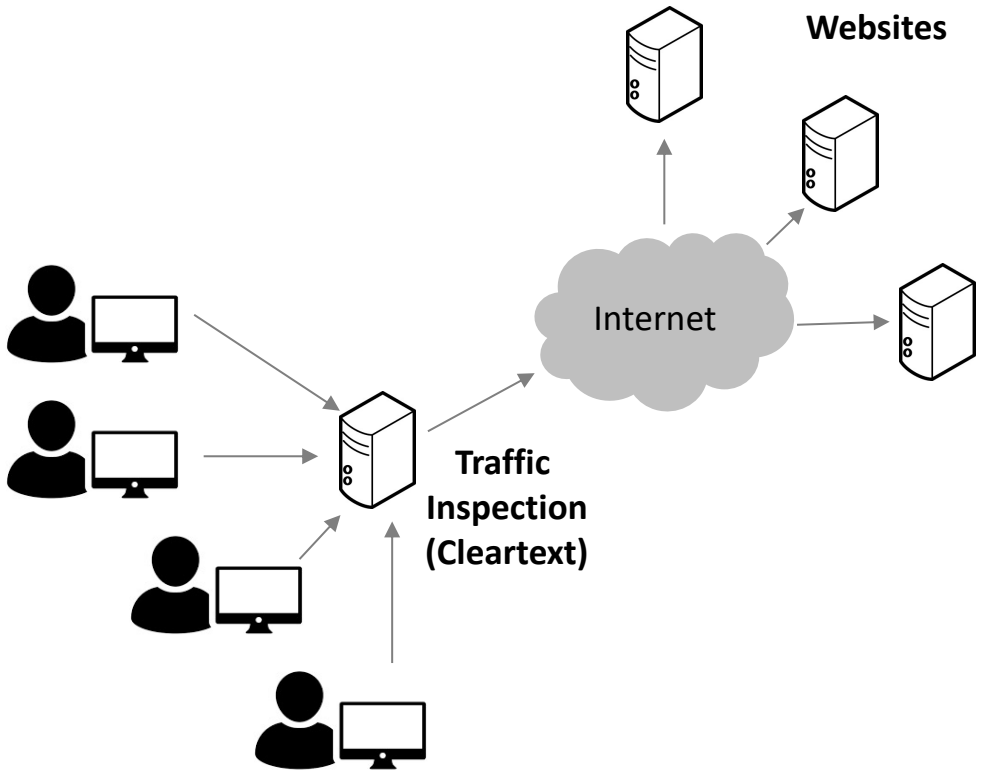
Week 12

Preventing Data Exfiltration with Reverse Proxy



Week 12

Enterprise Traffic Inspection – First Generation

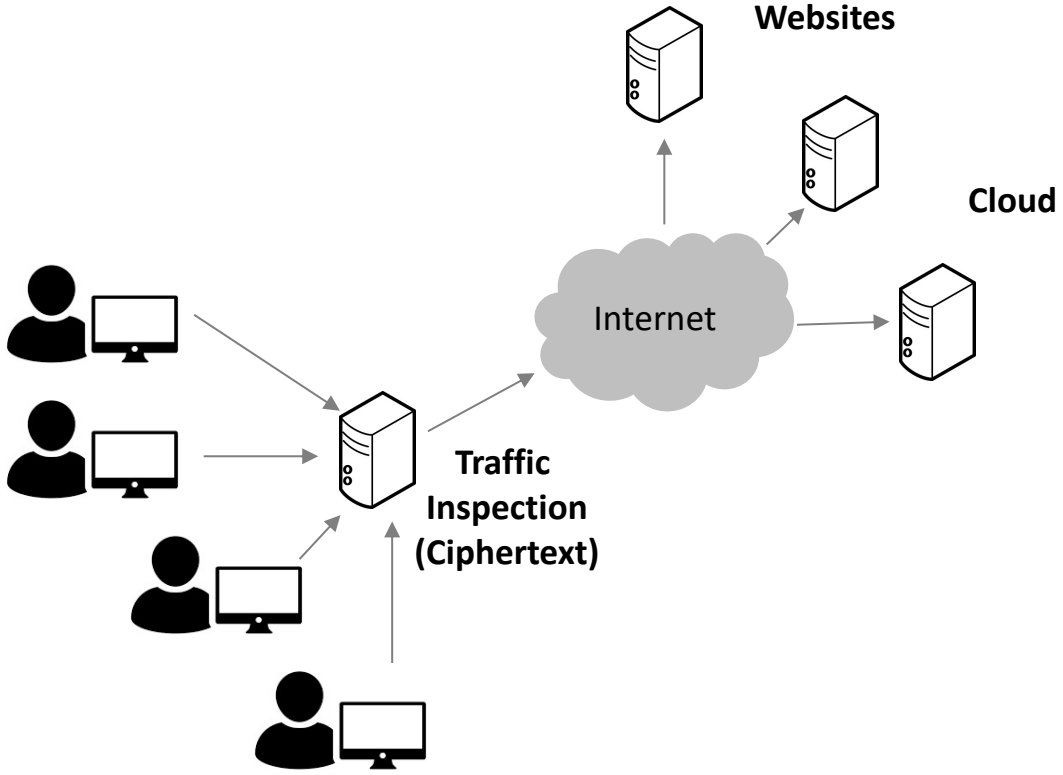


- **Traffic is mostly <u>non-encrypted</u>**
- **Traffic is mostly <u>web-based</u>**
- **Proxy inspection is straightforward**

Requirements for First-Generation SWG in context of Perimeter Architecture

Week 12

Enterprise Traffic Inspection – Next Generation



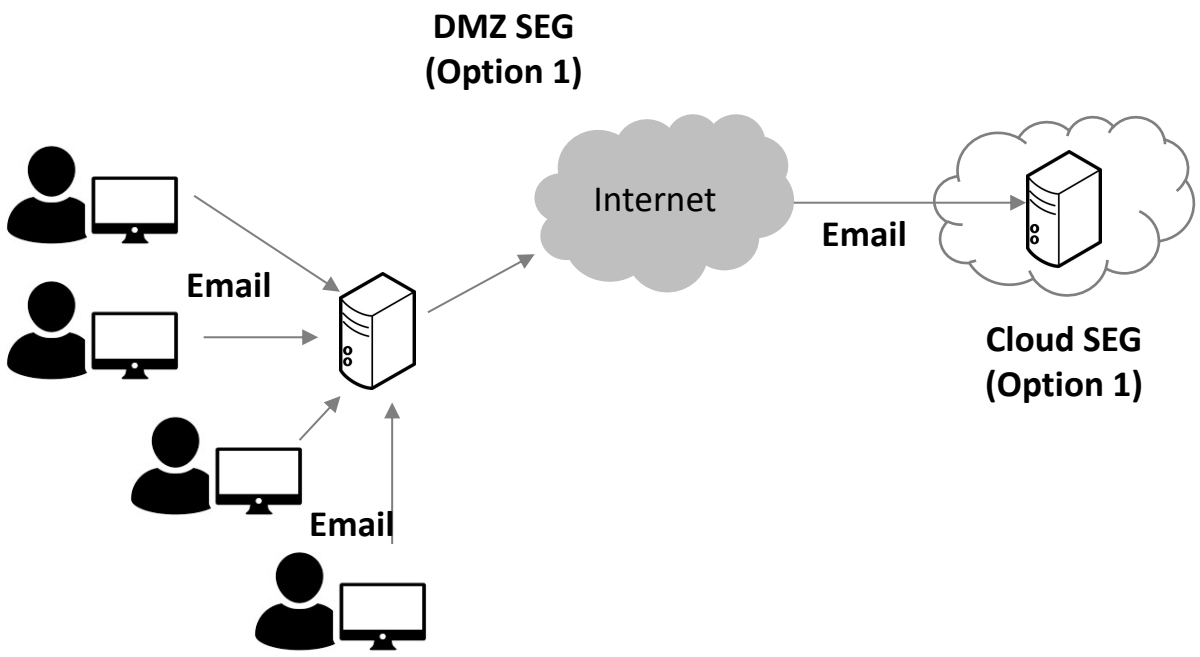
- **Traffic is mostly encrypted**
- **Traffic is >70% cloud-based**
- **Proxy inspection is more complex**

Requirements for Next-Generation SWG in context of SASE Architecture

What is a Secure Email Gateway (SEG)?

Week 12

Understanding Secure Email Gateway (SEG)



- **Email remains important in business**
- **SEGs filter attachments for malware**
- **Reduces SPAM, phishing, and viruses**

Requirements for Next-Generation SEG in context of SASE Architecture

Week 12

Fact: Too Many Malicious Emails Make it Through Commercial SEGs