Welcome Back to SECURITY+ Day 02

Michael Shannon
and
Irfan Ahmed

Class will begin at 10:00 am
Central Standard Time

THREAT ACTORS AND VECTORS

Objectives

- Compare threat actor types, attributes, and motivations
- Explore social engineering and common attack surfaces
- Look at supply chain vulnerabilities
- Examine application, O/S-based, web-based vulnerabilities
- Learn about hardware, virtualization, cloud, and mobile device vulnerabilities

THREAT ACTORS (AGENTS)

- Threat agents (or actors) are the persons, methods, operations, techniques, systems, or entities that act (or have the potential to act) with intent to initiate, transport, carry out, or in any way support a particular threat or exploit
- Threats are not realized without an agent or catalyst
- Can be comprised of an individual or a group
- The attacks can also be totally automated (bots)

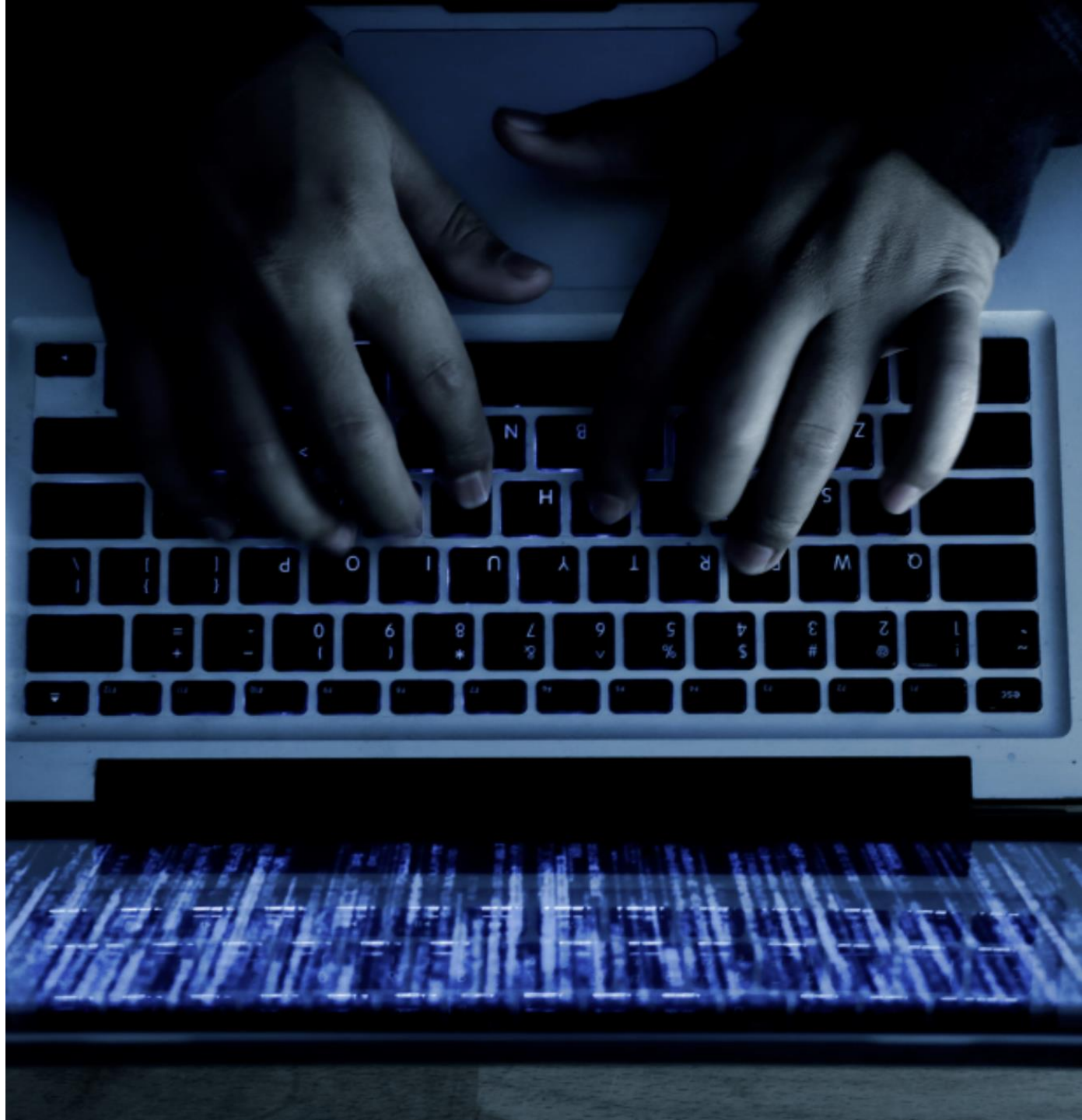
STRUCTURED	UNSTRUCTURED
Planned	Accidental
Organized	Non-malicious
Persistent	Drive-by web surfing
Multi-phased	No acceptable use policy (AUP)
Can be internal or external	Email and webmail
Exploit kits, zero-days, modules, ransomware	USBs and personal electronics

UNSKILLED ATTACKERS (SCRIPT KIDDIES)

- These originate from the combination of inexperienced crackers using script viruses and prepackaged malicious code (exploit kits and Malware as a Service [MaaS] campaign)
- The most common script viruses are spread via email attachments using preformed scripts and modules from exploit kits
- Newer techniques are often learned on YouTube and other social media sites in the dark web through ToR browsing
- These represent the lowest level of attacker sophistication and capability levels

HACKTIVISTS

- Hacktivism unofficially began in the late 1980s when viruses and worms spread messages of protest (e.g., "Worms Against Nuclear Killers")
- The term "hacktivism" was coined by the Cult of the Dead Cow, which also gave birth to "Hacktivismo," a group of international crackers protesting human rights abuses
- They are responsible for DoS, DDoS, ransomware, hijacking and defacing websites, and other cyber attacks to raise awareness



ORGANIZED CRIME SYNDICATES

- Organized cybercrime is a well-funded, multi-billion-dollar-a-year industry that affects all sectors of government and the economy
- They are the main contributors to advanced persistent threats (APTs)
- They perform cost-benefit analysis and other research before carefully choosing targets
- The campaigns may last months or years
- Example: The ALPHV/BlackCat ransomware operation

STATE-BASED ATTACKS

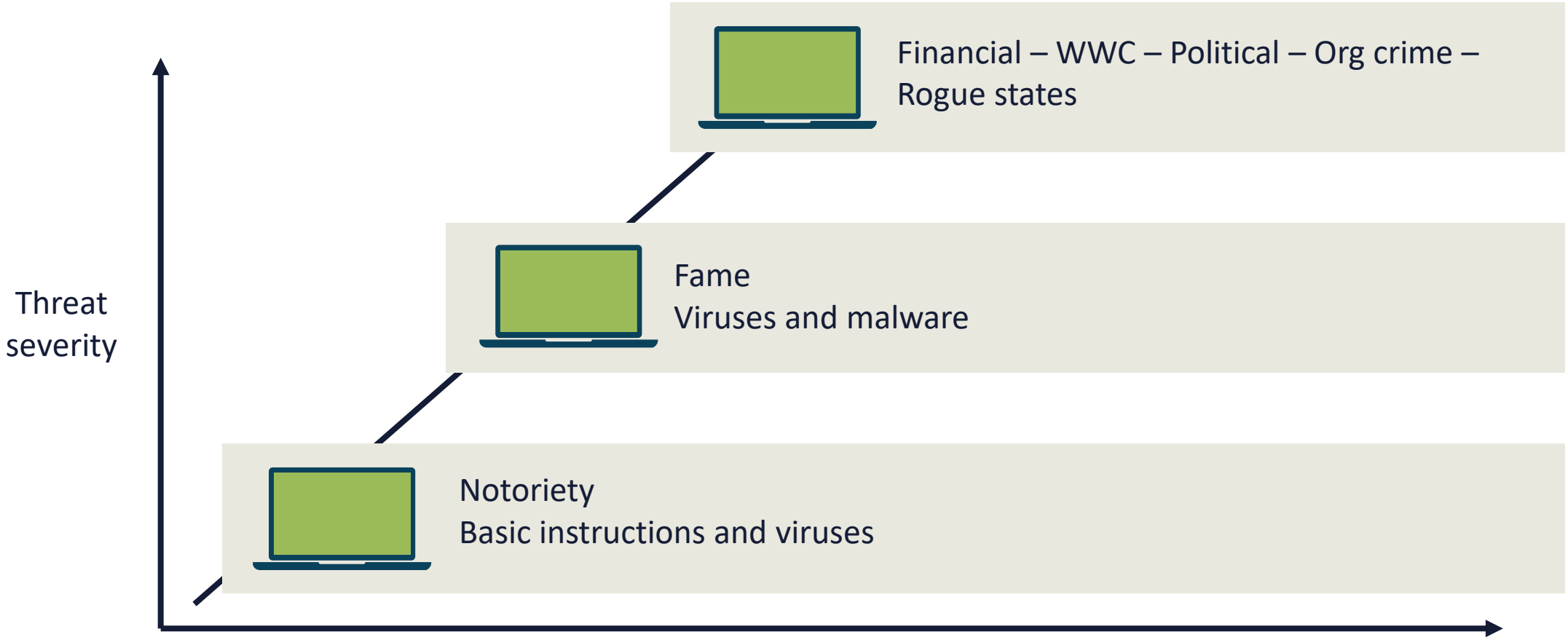
- The nation-state actor has a "license to hack" since they work for a government or military to disrupt or compromise target governments, organizations, or individuals to gain access to valuable data or intelligence
  - They might be part of a semi-hidden "cyber army" or "password crackers for hire" for companies that are aligned with the aims of a government or dictatorship
- They can create incidents and false flag operations that have international significance
- The nation-state actor has developed (along with criminals) many zero-day malware exploits that are waiting to be activated (e.g., a logic bomb)

Many security industry analysts and experts contend that the world has already entered a third world war in the form of a cyber war known as WWC (World War Cyber)

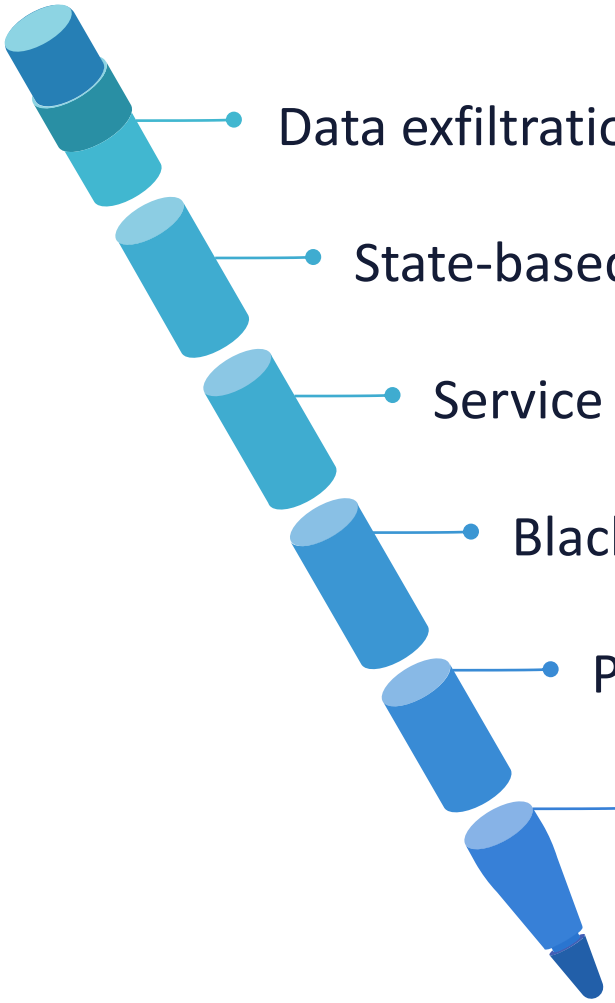
COMPROMISED PRIVILEGED INSIDERS

- These existing and recently released employees or contractors should be considered "public enemy number one"
- They can often have unfettered and elevated access and are the most likely to leave backdoors and other covert channels upon exit from the organization
- The term "compromised" is more accurate than "disgruntled" since there are several factors that can put an employee in a compromised position without being dissatisfied with the organization or other personnel

INTENT AND MOTIVATION



THREAT ACTOR MOTIVATIONS



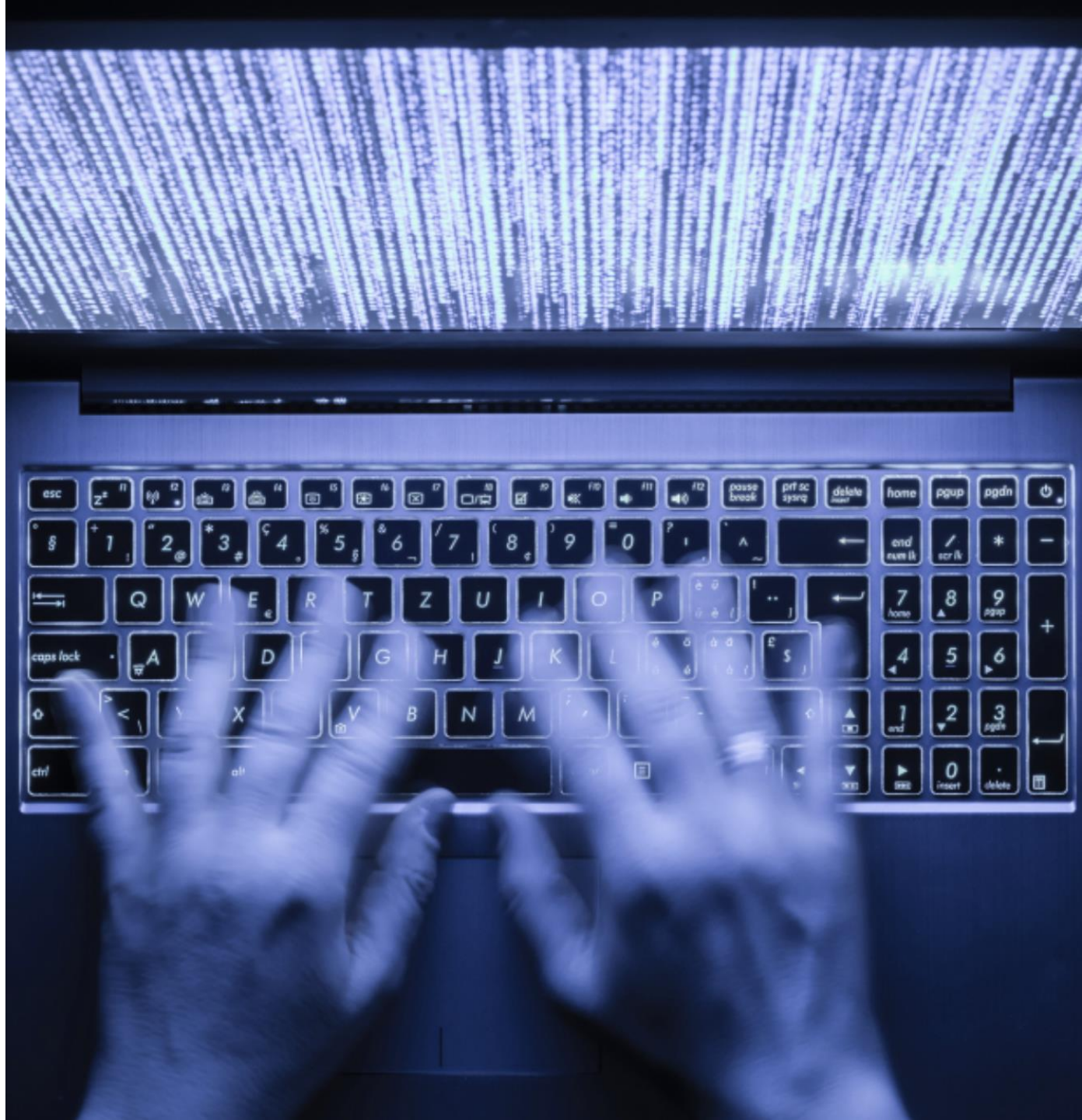
- Data exfiltration for financial gain
- State-based or corporate espionage
- Service disruption
- Blackmail and extortion
- Political activism or ethical issues
- Revenge or act of war

THE DARK WEB

- The dark web is the veiled collective of Internet sites that are not indexed and are only accessible by a specialized web browser such as ToR, Freenet, or Subgraph OS
- It is considered a part of the deep web
- It is a vast repository of Malware as a Service (MaaS) campaigns and resources

THE DARK WEB

- It is used for keeping Internet activity anonymous and private, which can be helpful in both legal and illegal applications
- While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity, such as purchases of contraband and child pornography



PHISHING ATTACKS

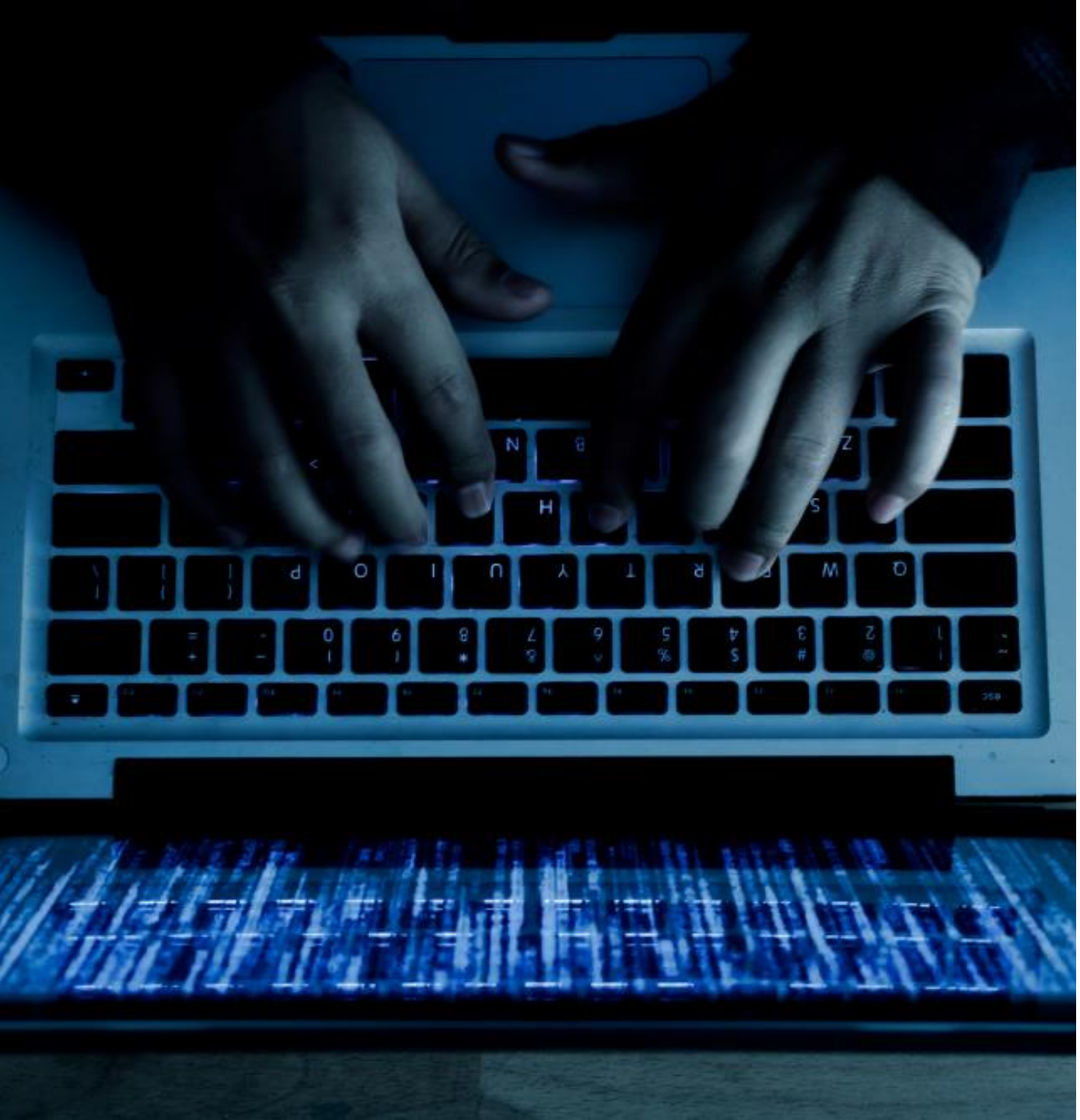
- Email phishing attacks or hoaxes are one of the most common exploit vectors available to crackers
- Phishing is a cyber attack that uses disguised email and webmail as a vector
- The goal is to trick the recipient into believing that the message is legitimate so they will click a link or download an attachment
- Common indicators are vague salutations, suspicious domains, wrong paths or hypertext, awkward grammar, urgency, lack of contact info, and spoofed headers/logos

PHISHING VARIANTS

- **Spear phishing** is a select, targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons
- **Whaling** is a spear phishing attack against high-level and highly privileged employees
- **Smishing** is using various text messaging formats (i.e., SMS) as a vector
- **Vishing** uses a voice over IP or telephony as the hoax vector

BUSINESS EMAIL COMPROMISE (BEC)

- Business email compromise (BEC) is a form of attack that targets companies that outsource, conduct wire transfers, and process invoices, often abroad
- It is often an elaborate advanced persistent hoax that targets corporate email accounts of high-level employees
- They are either spoofed or compromised through keyloggers or phishing attacks, often to perform fraudulent wire and cyber currency transfers
- Some attackers have successfully spoofed large vendors and customers, lawyers, CPAs, and even government officials (e.g., IRS)



SOCIAL ENGINEERING

- Eliciting information and reconnaissance
  - Shoulder surfing
- Dumpster diving
  - Credential harvesting
- Hoaxes and impersonation
- Identity fraud and invoice scams
  - Pretexting using a fabricated story, or pretext, to gain a victim's trust; brand impersonation
- Disinformation and influence campaigns
- Watering hole attacks

REASONS FOR SOCIAL ENGINEERING EFFECTIVENESS

Lack of proper security and awareness training

Inadequate acceptable use policy (AUP)

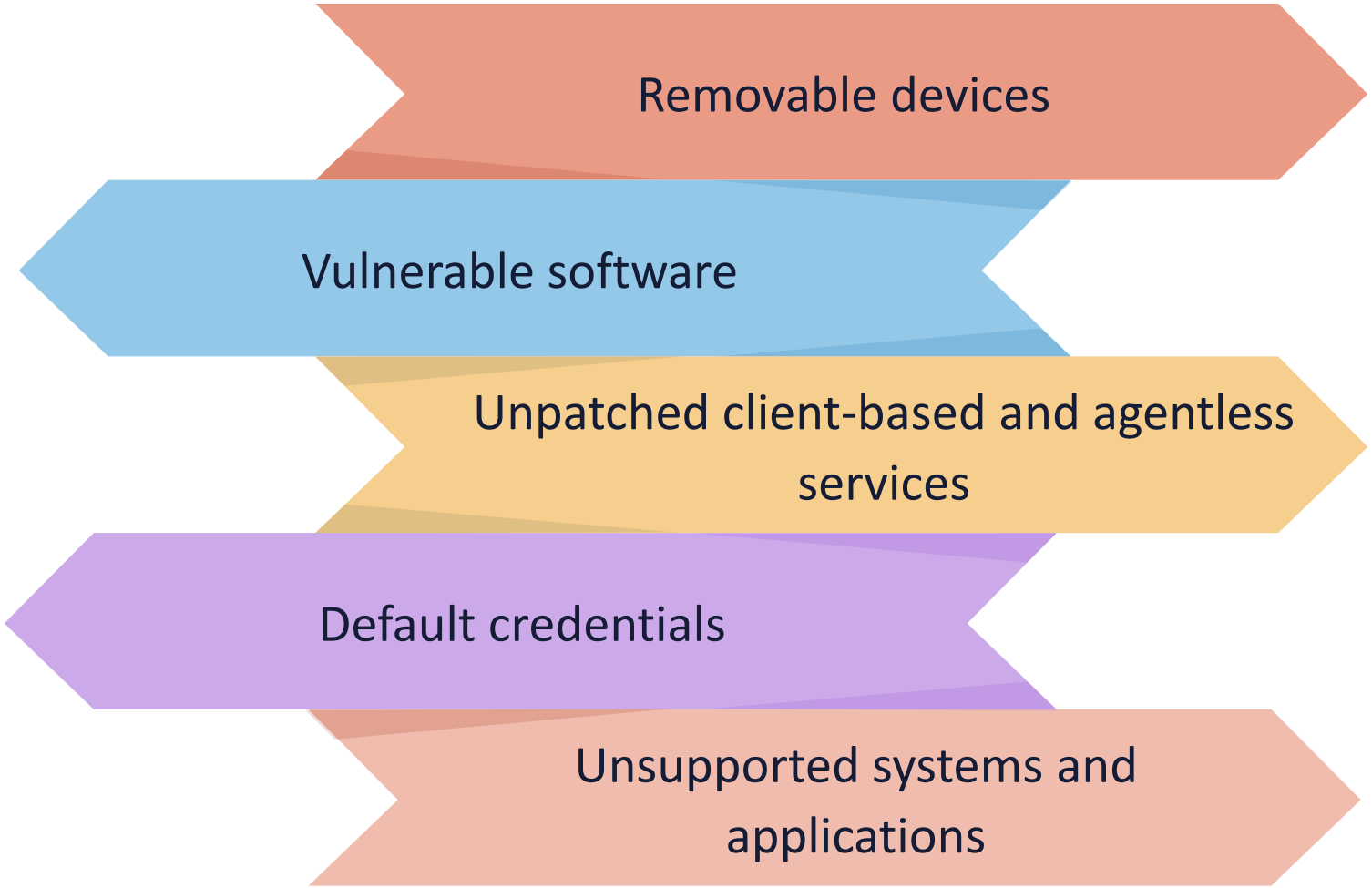
No buy-in from management and employees for prevention measures

No enforcement of policies – no carrot and no stick

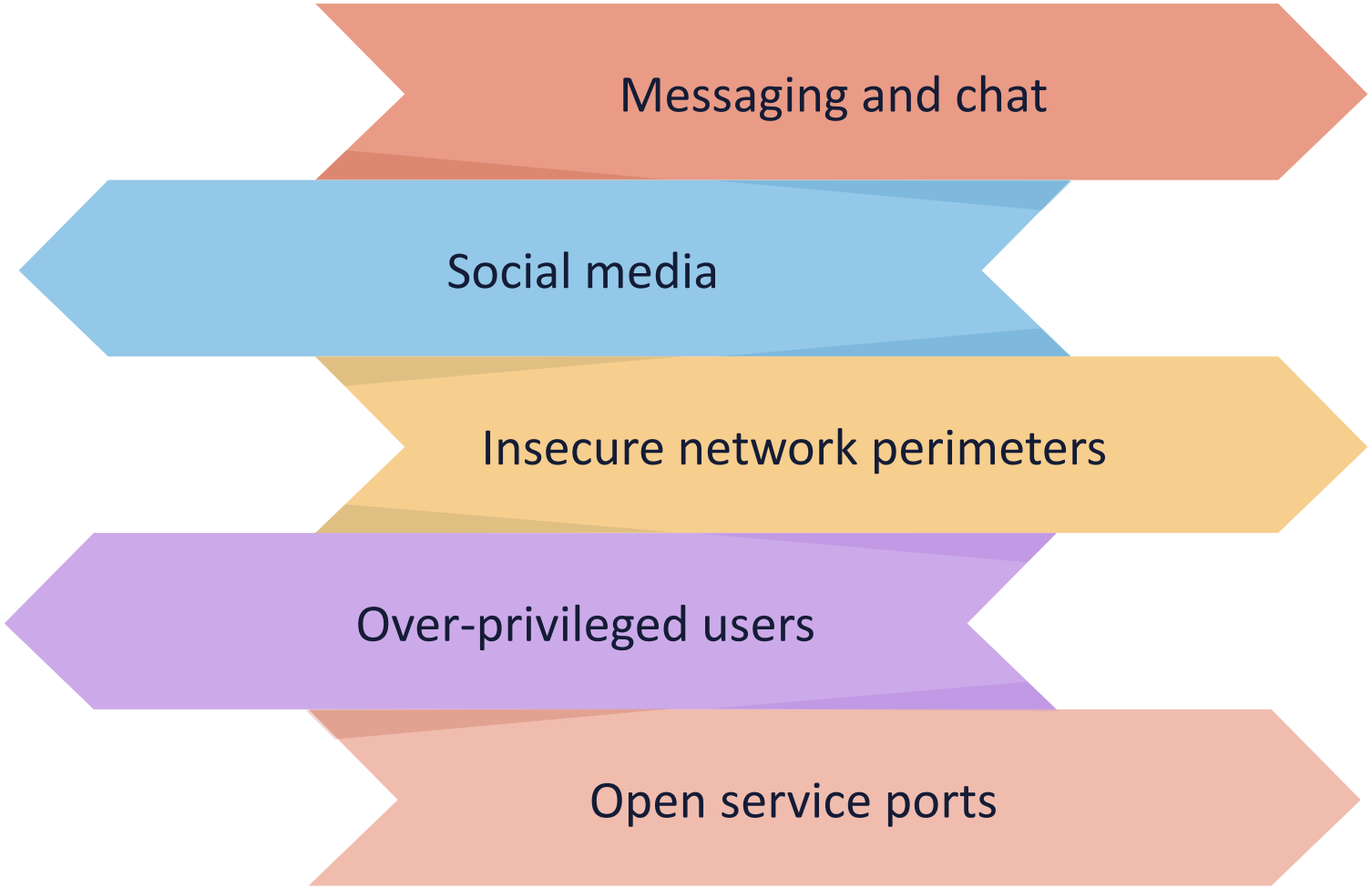
Outdated antivirus, DLP, and mobile device and application management tools

Poor perimeter security controls for email, messaging, telephony, and web activities

COMMON ATTACK SURFACES



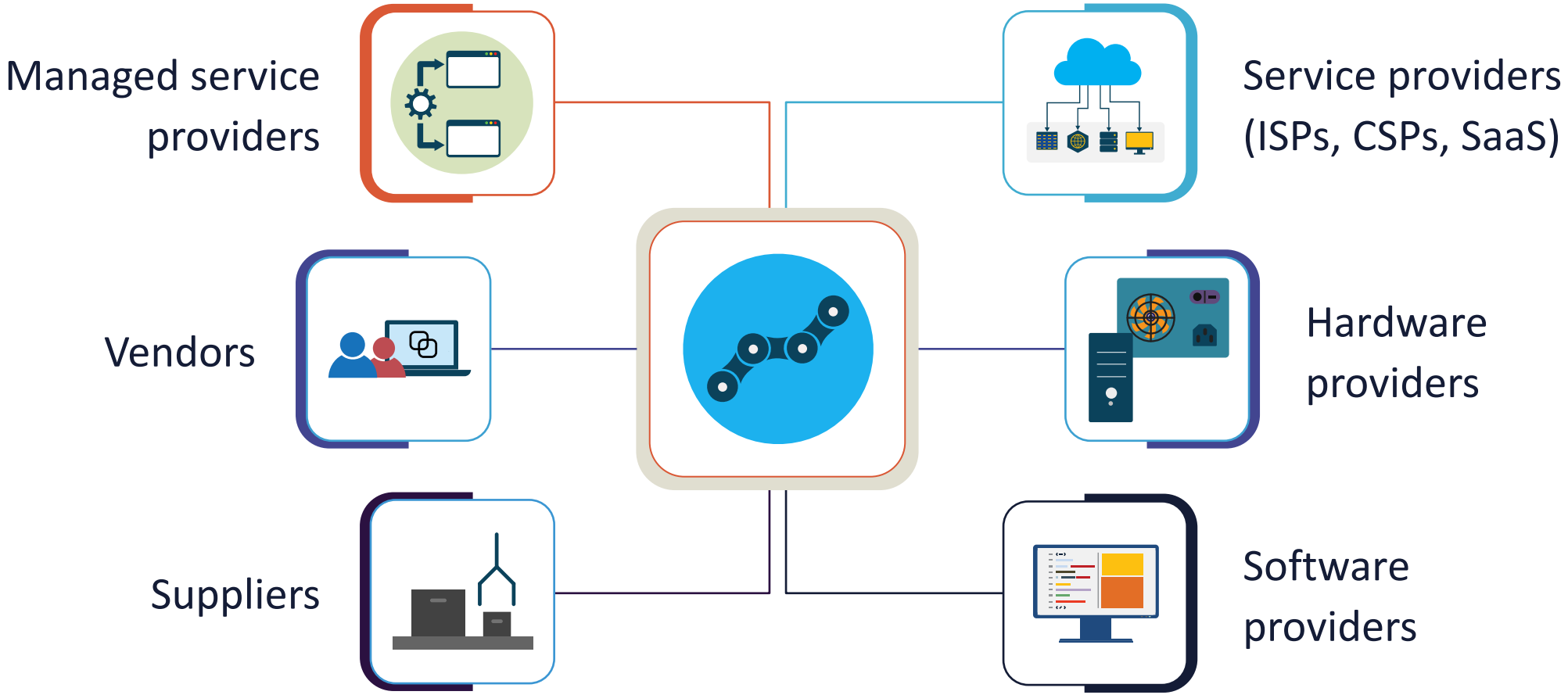
COMMON ATTACK SURFACES



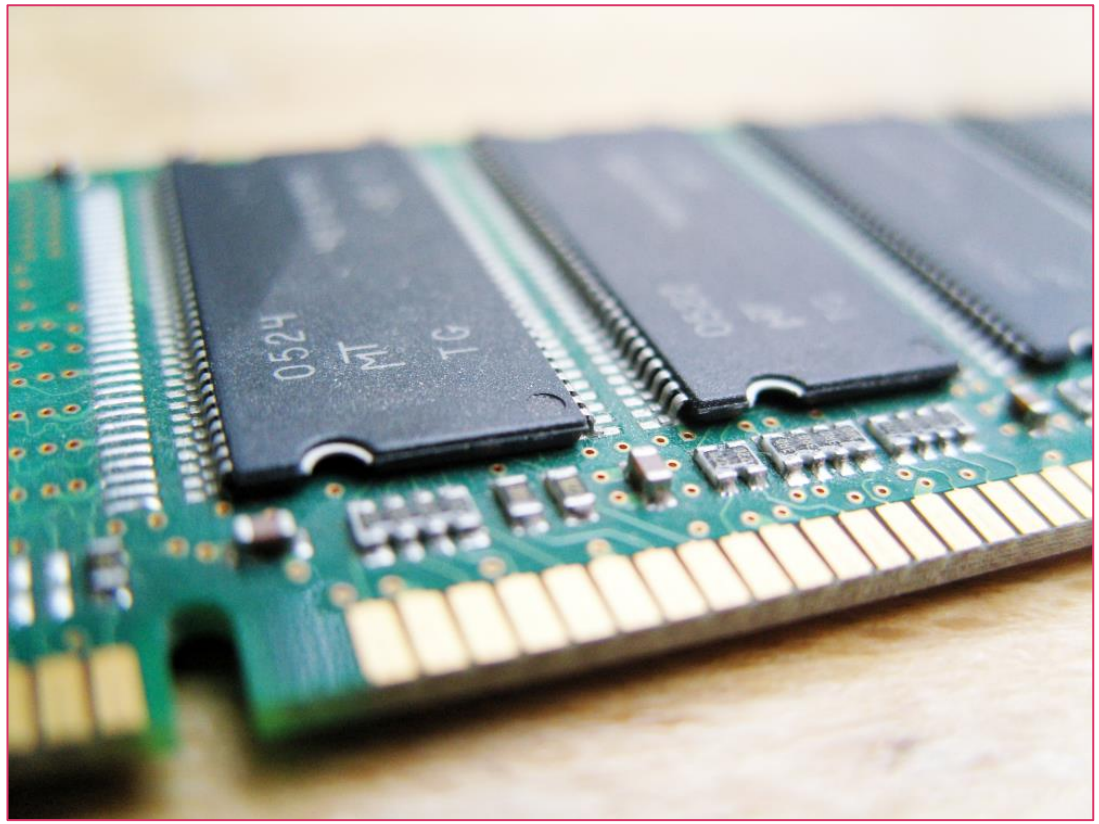
SUPPLY CHAIN VULNERABILITIES

- Software supply chain security continues to be a growing risk for organizations
- Experts predict this will only continue to rise, and damages could exceed 15% growth year-over-year for the foreseeable future
- Many organizations allow third-party organizations to have access to their networks and systems
- When an attacker exploits a vendor or partner, they can leverage this trust relationship to gain access to the organization’s infrastructure
- Zero trust initiatives are a powerful countermeasure to supply chain vulnerabilities

SUPPLY CHAIN VULNERABILITIES



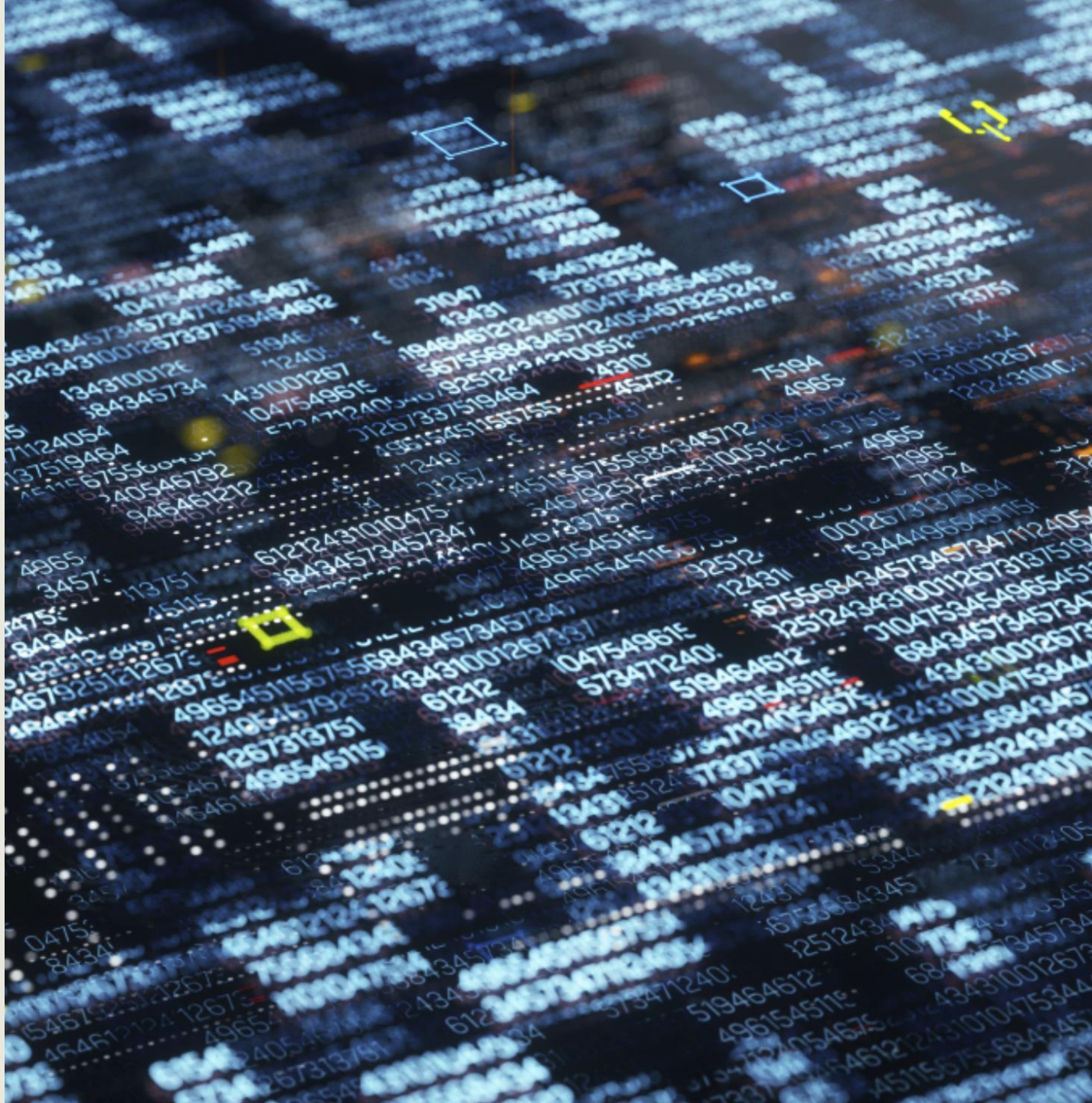
APPLICATION VULNERABILITIES: MEMORY INJECTION



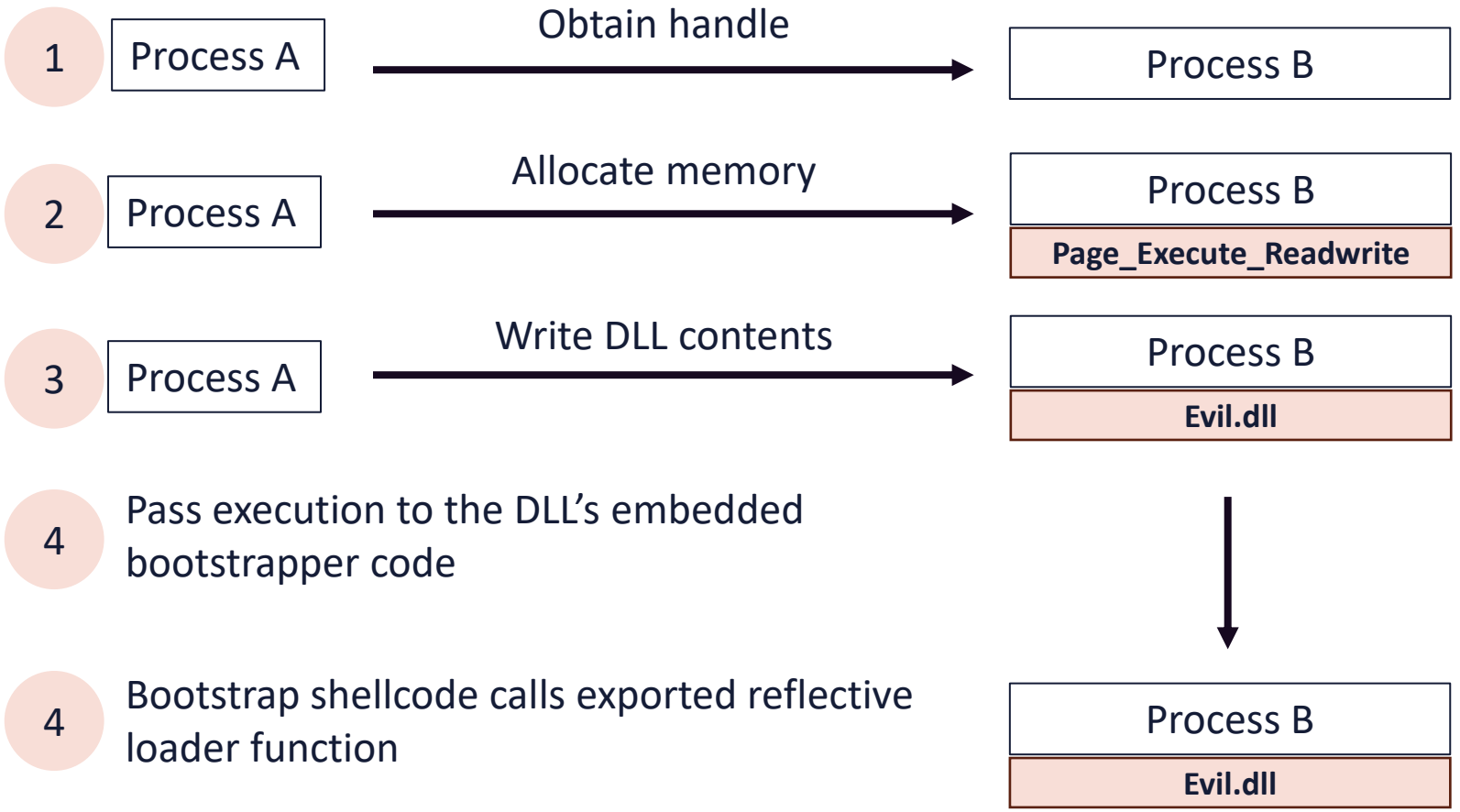
- **Shellcodes** are a small stub of code used as a payload
- A **DLL** is a shared library of functions that multiple programs can access
- A **process** is an instance of a program being executed
- A **thread** is a small sequence of instructions or a component of a process
- Windows API protocols allow interaction with the Windows OS
  - VirtualAllocEx reserves or changes a region of memory
  - WriteProcessMemory writes data to an area of memory in a specified process
  - CreateRemoteThread creates a thread in the address space of another process

APPLICATION VULNERABILITIES: EXAMPLES OF MEMORY INJECTION

- Shellcode injects malicious code into a running application of PowerShell, which is regularly used in attempts to execute in-memory attacks
- Process hollowing starts a legitimate process whose sole purpose is to be a container for malicious code - it delivers the process in a "suspended" state, then rewrites the content with the required code in memory, and continues to execution
- Reflective DLL injection is where contents of a rogue DLL are loaded into memory



REFLECTIVE DLL INJECTION

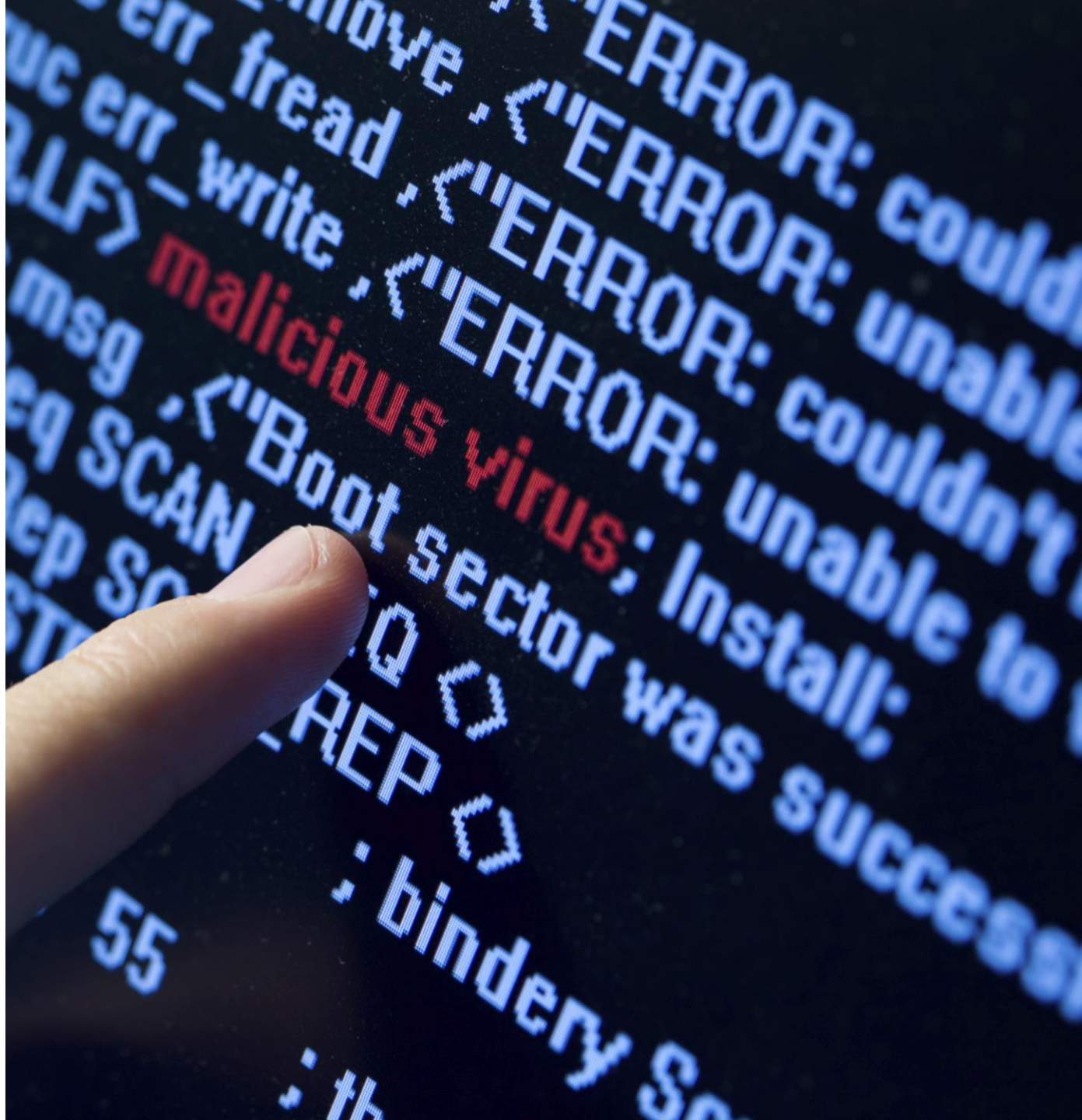


BUFFER OVERFLOWS

- In a buffer overflow attack, the attacker sends a larger-than-expected input
- For instance, when a front-end web server accepts it and writes it to memory areas
- Associated buffers are filled, and the adjacent memory is overwritten as a result
- This "overwrite" may contain malicious instructions or code that crash the server or runs a persistent remote access trojan
- These attacks are often delivered by **malicious updates** from vendors who do not perform software assurance or **zero days** – the first day the malware is discovered

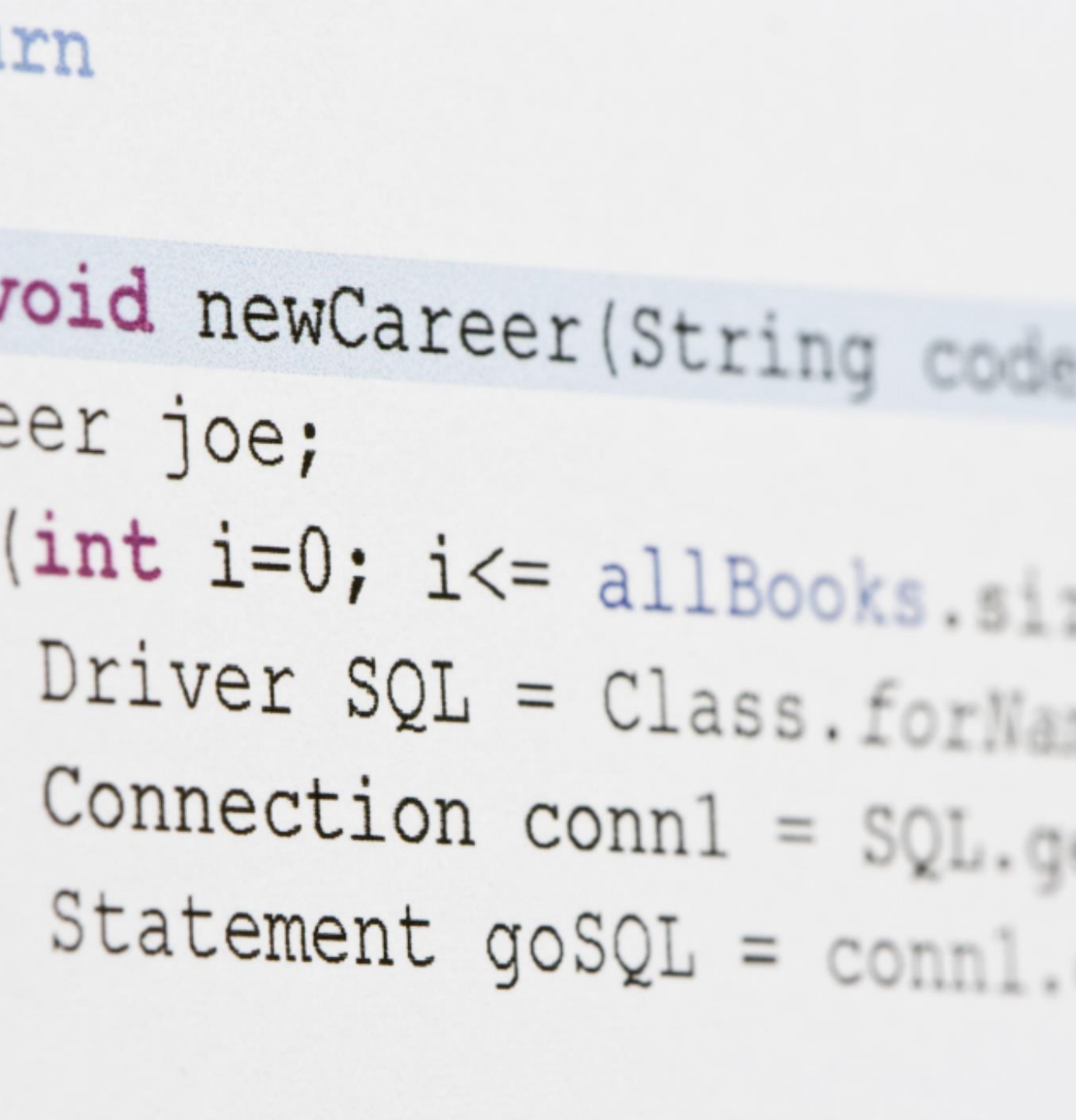
OTHER APPLICATION VULNERABILITIES

- **Race conditions** occur when a device or system attempts to perform two or more operations at the same time; but because of its functionality, the operations must be done in the correct sequence to be done properly
- **Time-of-check (TOC)/Time-of-use (TOU)** happens when an app checks the state of a resource before using the resource, but the resource's state can change between the check and the use in a way that invalidates the results of the check
  - This can cause the product to perform invalid actions when the resource is in an unexpected state



OS-BASED AND WEB-BASED VULNERABILITIES

- One of the most prevalent misconfiguration habits is leaving debugging features enabled in production environments
- It is critical to make sure that debugging functionality is disabled or properly secured in production environments
- Another common misconfiguration comes from the use of default or weak credentials for various system components such as operating systems, databases, network devices, or application interfaces
- All systems should use tested patch management and look for outdated code

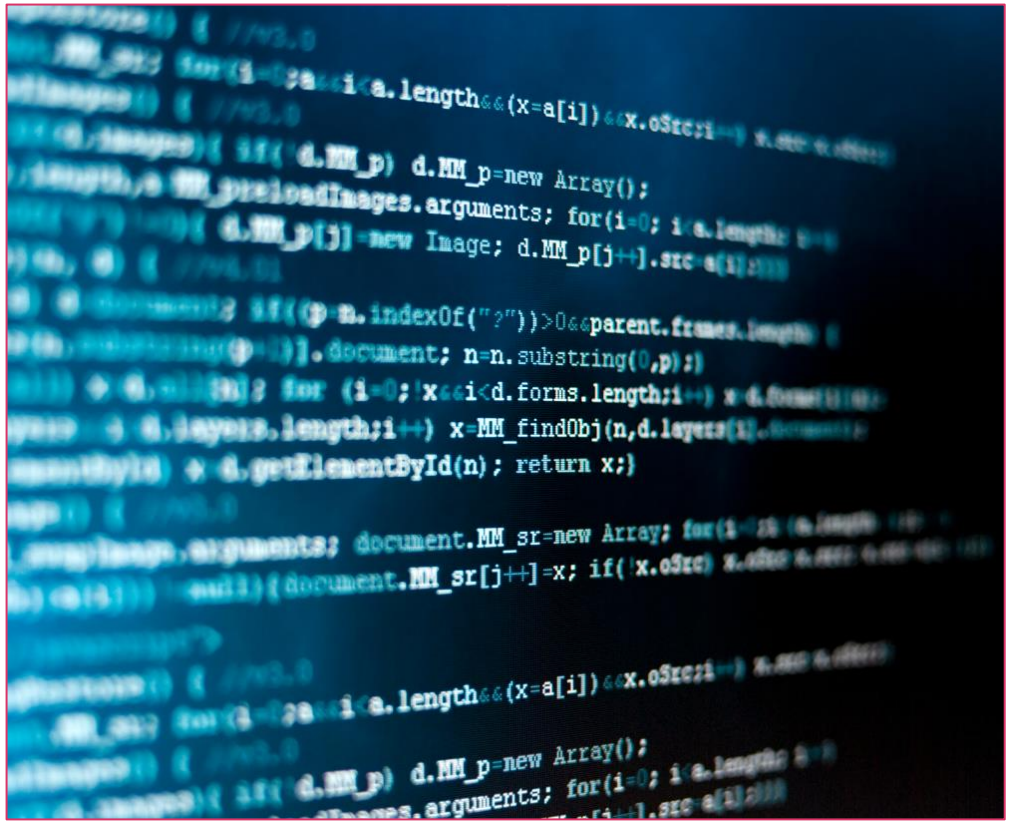


SQL INJECTION (SQLI)

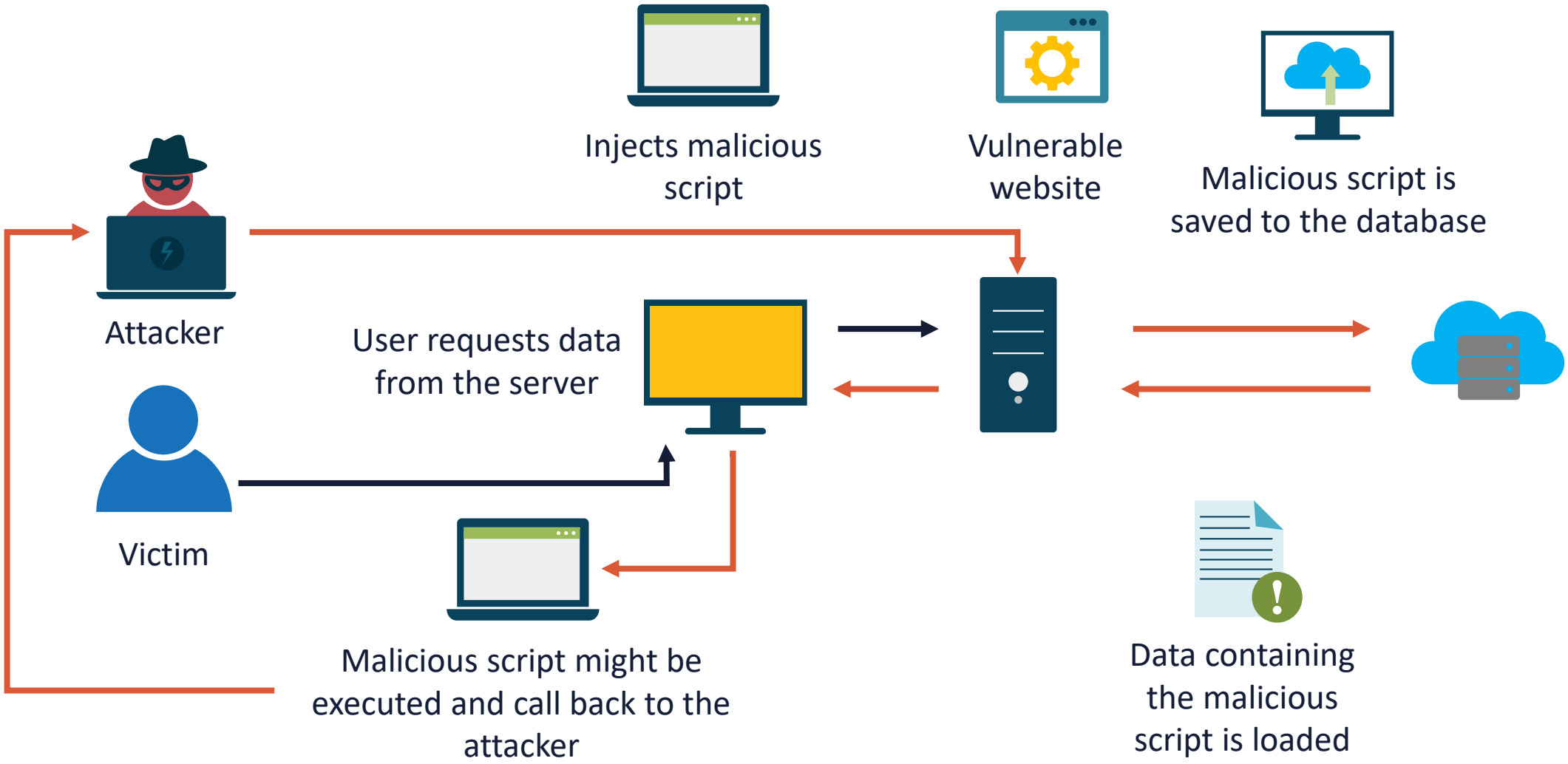
- This common attack has been run against front-end services like web servers and Microsoft SharePoint that use SQL as a database repository
- It involves inserting a SQL query through input data from client-to-server applications:
  - Read sensitive database data (SELECT FROM)
  - Change database data (INSERT, UPDATE, DELETE)
  - Execute administrative functions (e.g., shut down DBMS)
  - Get the contents of files on a database management system (DBMS)
  - Run commands on an operating system

CROSS-SITE SCRIPTING (XSS)

- Flaws in pages rendered by web servers and not the web server code itself (i.e., Apache, IIS) where malicious scripts or code are injected into trusted or innocent website pages
- Malicious scripts can steal cookies, session tokens, or other sensitive data stored by the browser and used with the site
- Attacker typically sends browser-side scripts to end user
- Can occur anytime a web program uses user input within the output it generates without validating or encoding

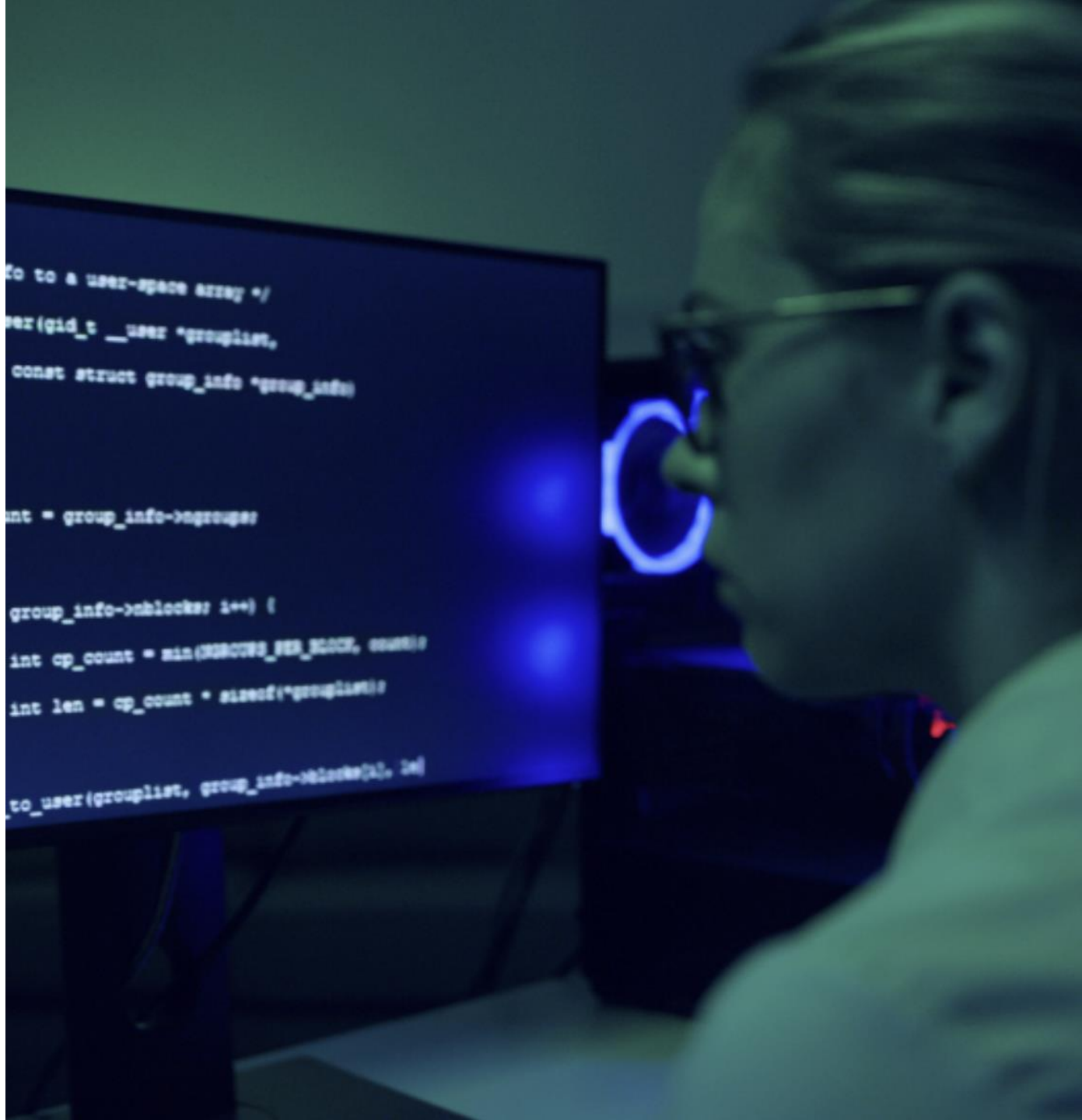


CROSS-SITE SCRIPTING (XSS)



XSS VARIANTS

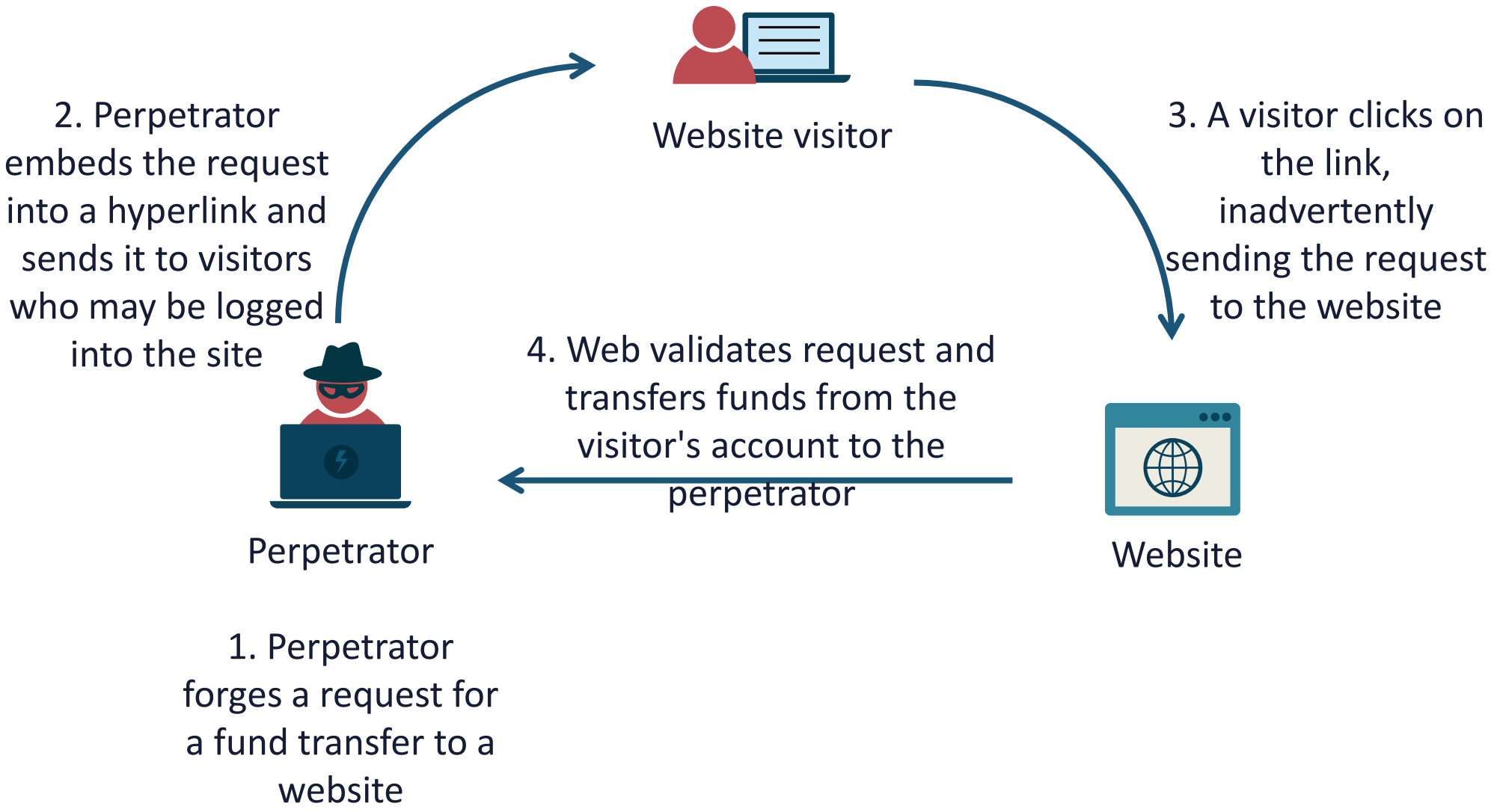
- **DOM-based** is also called local XSS or type 0
  - It does not involve vulnerable web servers but rather insecurely written HTML pages on the end user's system or local gadgets and widgets (Widgets – Apple, Nokia, Yahoo; Gadgets – Microsoft and Google
- **Reflected XSS** (Nonpersistent or Type 1)
  - This is a classic input trust vulnerability where the application is expecting some input (i.e., a query string), and the attacker sends something the developer did not expect
- **Stored XSS** (Persistent or Type 2)
  - This is a variant of type 1 where, rather than reflecting the input, the web server persists the input
  - The difference is an intermediate phase where the untrusted input is stored in a file or a database before unloading on the victim – often found in blogs and review/feedback web application



CROSS-SITE REQUEST FORGERY (CSRF/XSRF)

- Attacks force an end user to perform undesirable actions in a web application in which they are authenticated
- An effective CSRF/XSRF attack can force users to perform state-changing requests:
  - Transferring funds
  - Changing their email address
  - Changing their password
- If the victim is an administrative account, the CSRF attack can compromise the entire web application

CROSS-SITE REQUEST FORGERY (CSRF/XSRF)



HARDWARE VULNERABILITIES

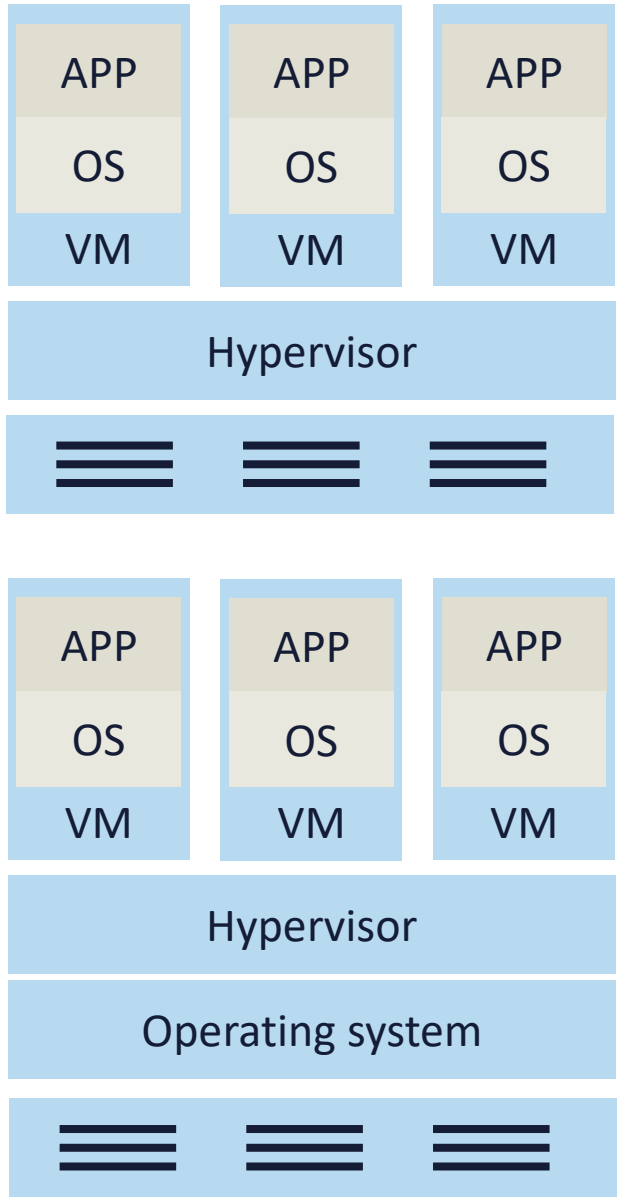
- Some of the dominant factors that contribute to vulnerabilities and flaws in hardware are
  - Vendors going out of business
  - Original equipment manufacturers (OEMs) cutting corners
  - Product becoming end-of-support and/or end-of-life with few or no alternatives
  - The usage of outdated and legacy systems
  - Unsecure and unsigned device drivers

FIRMWARE VULNERABILITIES

- Firmware is software that is embedded within hardware devices and provides low-level control and functionality
- Some firmware can be remotely reprogrammed and may be accessed by attackers through remote code execution (RCE)
- Common firmware exploits are authentication bypass, buffer overflows, and injection flaws
- The rapid emergence of the Internet of Things (IoT) and smart devices has introduced more security vulnerabilities

HYPERVISORS

- The virtual machine manager software system that runs and controls virtual machines
- It allocates and shifts resources as well as manages the interaction between the VMs and the hardware
- Type I – bare metal or native
  - Runs directly on the underlying hardware
  - XenServer, KVM, Hyper-V, ESXi
- Type II – hosted
  - Runs on the OS installed on the hardware
  - Oracle VirtualBox 6, VMWare Player/Workstation



HYPERVISOR VULNERABILITIES

- **VM sprawl** – involves having no centralized control of hypervisors and virtual machines
- **VM hopping** – when administrators do not enforce the partitioning of guests from each other
- **VM escape** – a flaw in the hypervisor that allows a guest to access the underlying hypervisor or even the hardware that it runs on
- **Hyperjacking** – a scenario where a privileged insider installs malware, such as a rootkit, on the hypervisor to conduct unauthorized activities

THE CLOUD SECURITY ALLIANCE (CSA) TREACHEROUS 12

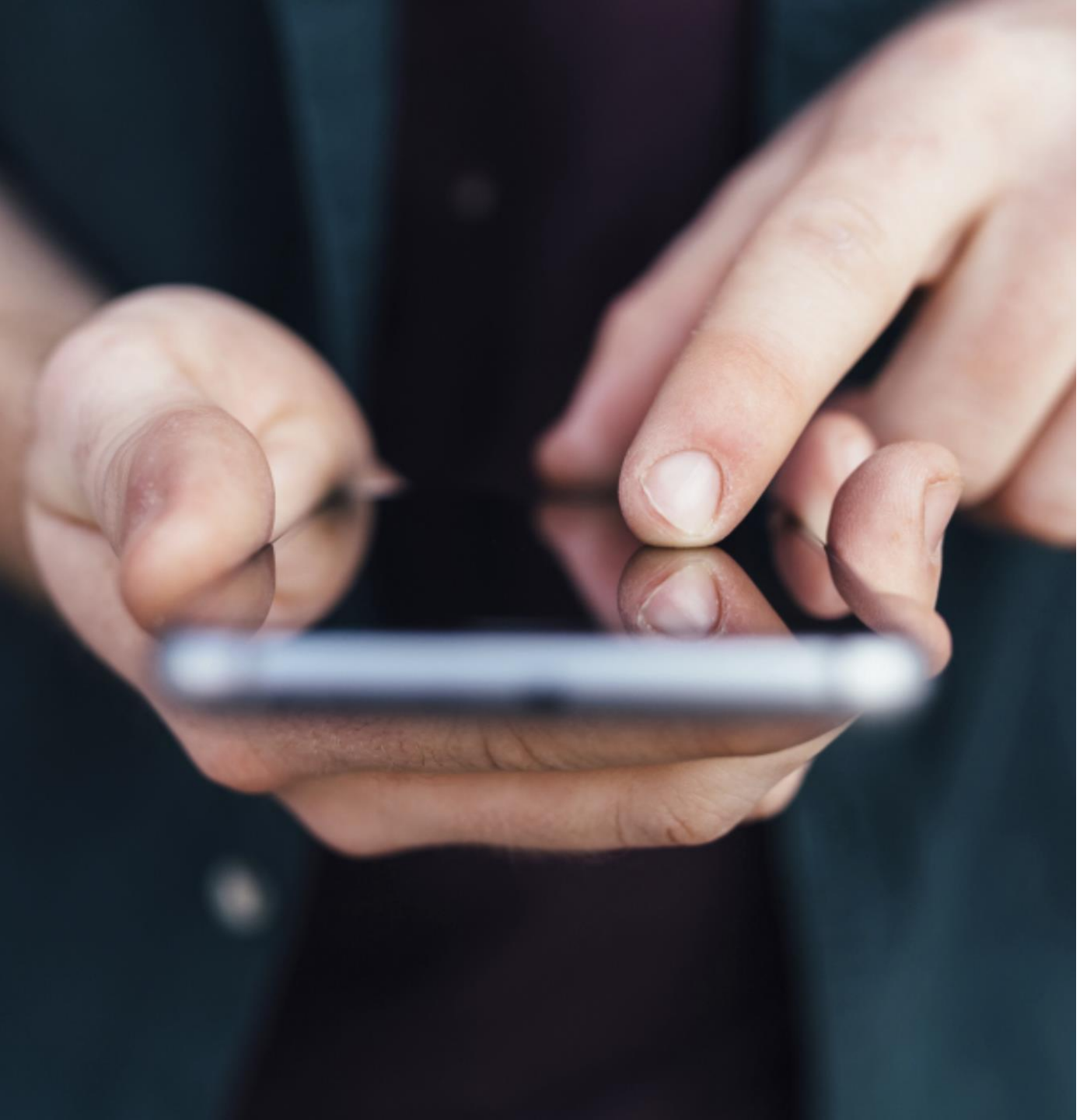
- *The Treacherous 12 – Cloud Computing Top Threats* report plays a vital role in the CSA research ecosystem
- The goal of the report is to offer organizations an up-to-date, expert-informed understanding of cloud security issues so that educated risk management decisions can be made concerning cloud adoption strategies
- The report reflects the current consensus among security experts in the CSA community about the most significant security issues in the cloud

THE CSA TREACHEROUS 12

1. Data breaches
2. Weak identity, credential, and access management
3. Insecure APIs
4. System and application vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats (APTs)
8. Data loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. Denial of service
12. Shared technology vulnerabilities

MOBILE DEVICE VULNERABILITIES

- There are several classic vulnerabilities with mobile devices – most of which have been addressed with vendor updates
- **Side loading**, in the context of smartphones, involves installing a compatible app for an Android or iOS device that is not available, approved, or at least monitored and maintained by your device platform's official app store



MOBILE DEVICE VULNERABILITIES

- **Jailbreaking is the act of exploiting the flaws of a locked-down electronic device (iPhone)** to install software other than what the manufacturer has made available for that device
- **Rooting is the process of unlocking usually an Android** smartphone or tablet
  - A rooted device gives the user much more freedom to customize the device and achieve more administrative control
  - It allows the device owner to gain full access to the root of the operating system and access all the features

ENTERPRISE MOBILITY MANAGEMENT (EMM)

- Organizations should employ the most robust authentication mechanisms feasible (biometrics, QR codes, trusted platform modules)
- This is accomplished through enterprise mobility management initiatives:
  - Mobile device management (MDM)
  - Mobile application management (MAM)

SURVEY OF MALICIOUS ACTIVITIES

Objectives

- Examine malware and physical attacks
- Explore network and application attacks
- Learn about cryptographic and password attacks
- Look at Indicators of Compromise (IoC)

MALWARE ATTACKS

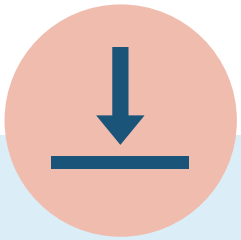
- A malware attack is a common cyberattack where malware (typically malicious software) executes unauthorized actions on the victim's system
- The malicious software (AKA virus or worm) encompasses many different types of attacks such as ransomware, spyware, command and control, and more
- Like other types of cyber attacks, some malware attacks end up with mainstream news coverage due to their severity
- An example of famous malware is the WannaCry ransomware attack

All security incidents can be considered an exploit, but not all exploits involve the usage or delivery of a malicious software (malware) payload

RANSOMWARE

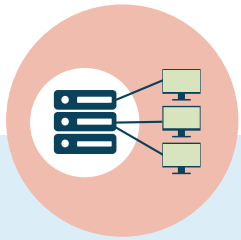
- This is a popular form of malware that encrypts key files and holds them for "ransom"
- Usually committed for cryptocurrencies such as Bitcoin (over 90%) or Monero
- Ransomware evolved from misleading "fix" apps to fake AV tools and bogus "fine" websites
- The average ransom demand has more than doubled since 2020
- Over 30% of victims are in the U.S.
- The newest trend is Ransomware as a Service (RaaS) on the dark net, which is a subset of Malware as a Service (MaaS)

RANSOMWARE CAMPAIGN



1. Installation

Crypto-ransomware installs itself after boot up



2. Contacting headquarters

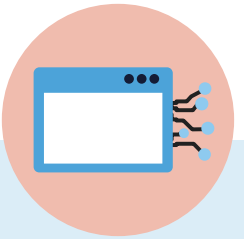
Malware contacts a server belonging to an attacker or group

3. Handshake and keys

The ransomware client and server "handshake" and the server generates two cryptographic keys

4. Encryption

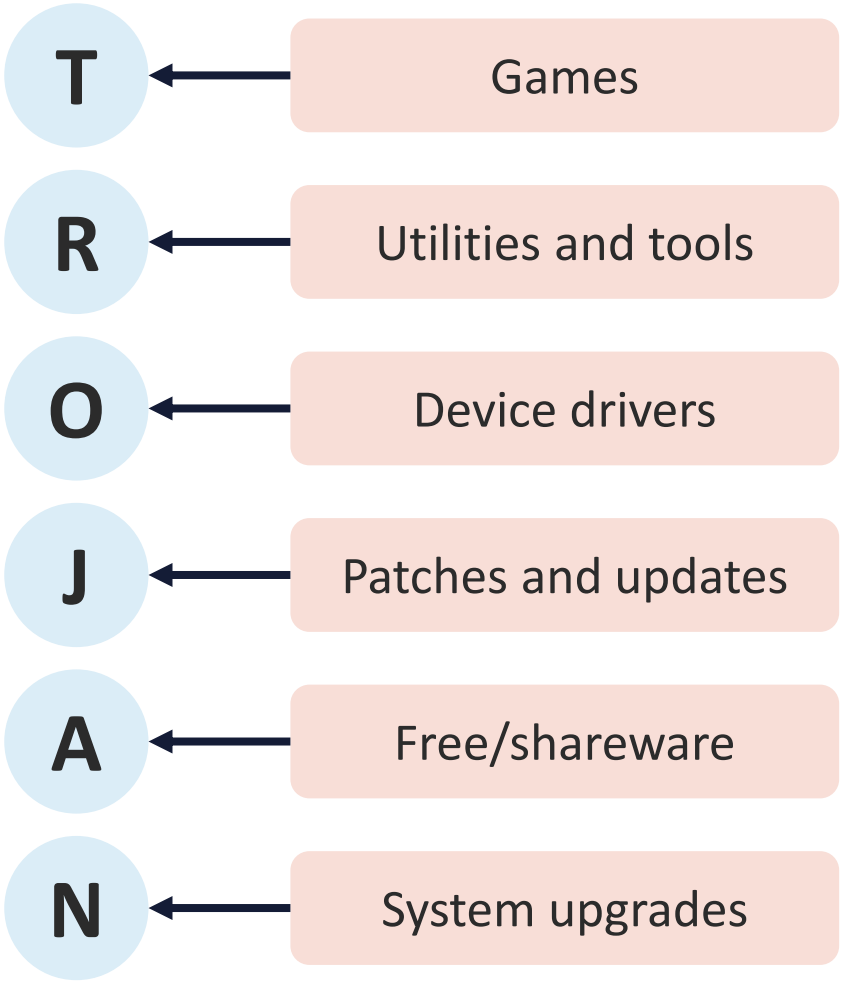
The ransomware starts encrypting every file it finds with common file extensions



5. Extortion

A screen displays, giving a time limit to pay up before the criminals destroy the key the decrypt the files

TROJANS

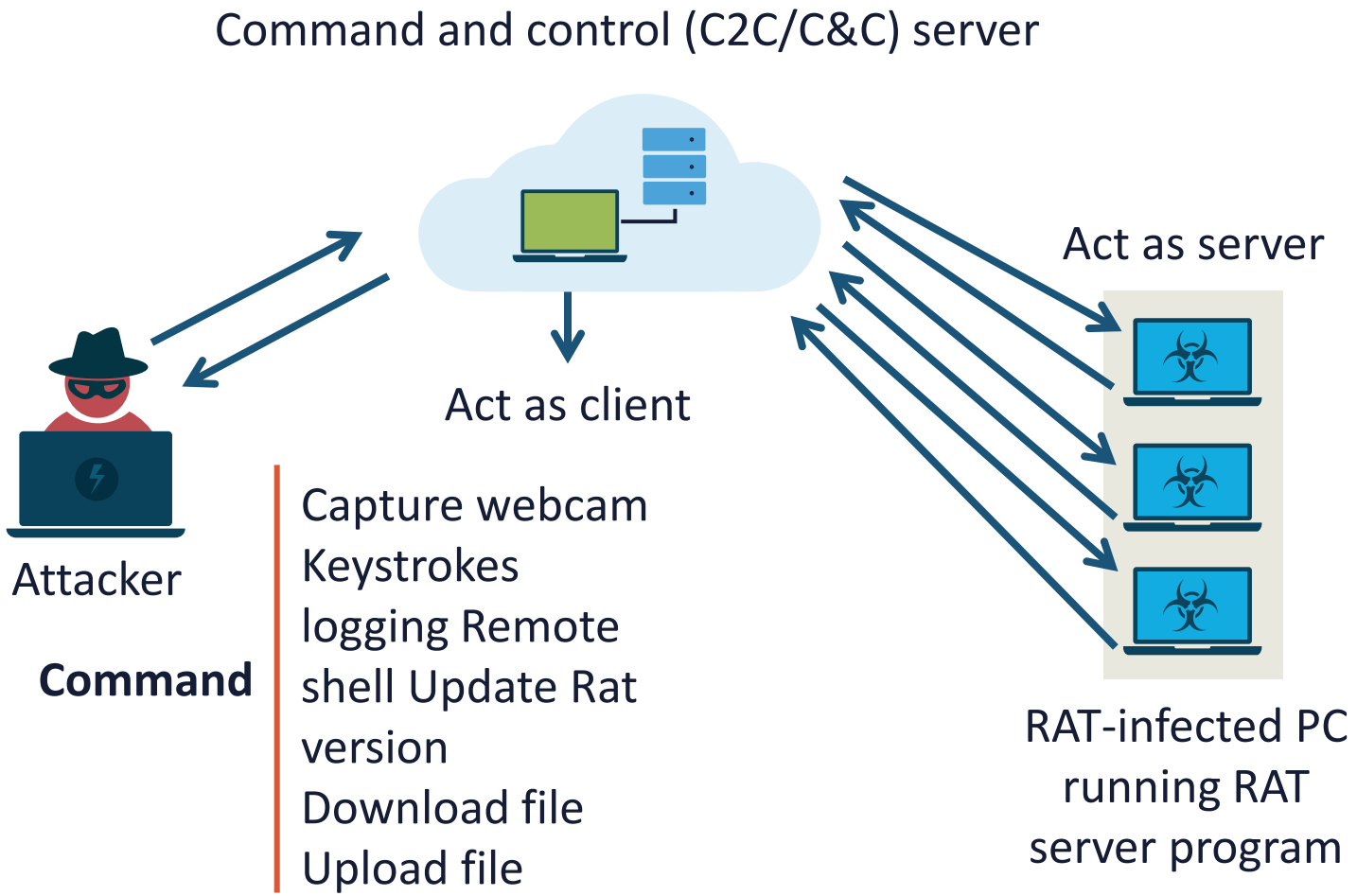


- Trojans are malicious code and programs that masquerade as legitimate applications or are embedded in real programs
- Trojan horses have no replicating abilities like viruses or worms
- They can either be a re-named benign program or the trojan code can exist in an operable application
- Trojans can also be part of a more elaborate distributed denial-of-service or botnet attack

REMOTE ACCESS TROJANS (RATS)

- Remote access trojans (RATs) are a variant of trojan malware engineered to permit an attacker to remotely control an infected computer
- Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response
- The server can be a command-and-control server that is part of an automated botnet

REMOTE ACCESS TROJANS



VIRUSES

A computer virus is a type of malware that spreads between computers and causes damage to data and software

Viruses are distinctive in that they typically attach to executable files to disrupt systems, cause major operational issues, and result in data loss and leakage

The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments

WORMS

Worms are a special form of self-replicating virus (malware) that generally spreads without user action

They distribute complete copies (possibly modified) of themselves across networks

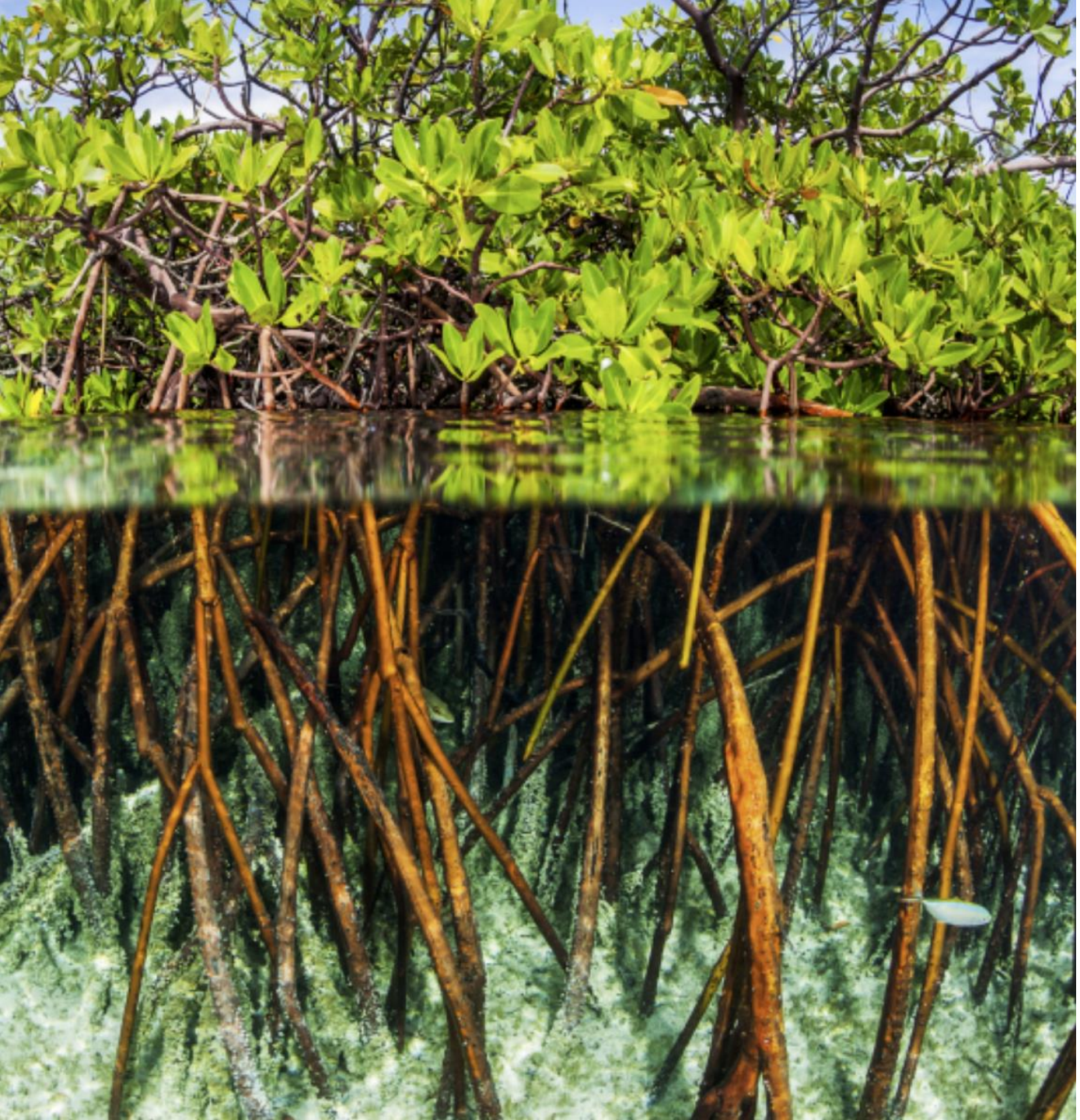
A worm can consume resources, infiltrate data, or simply cause the CPU on the system to waste cycles, resulting in a computer becoming unresponsive

SPYWARE AND BLOATWARE

- **Spyware** is often defined as malware intended to penetrate a device, collect personal data, and then send it to a third party without permission
- Spyware can also refer to legitimate software that monitors data for commercial purposes like advertising
- Technically speaking, practically all smart devices and IoT components are spyware
- **Bloatware** is unwanted and potentially harmful software preloaded onto new devices
- It is preinstalled by vendors, manufacturers, or carriers as a form of marketing to put services directly in front of customers

KEYLOGGERS

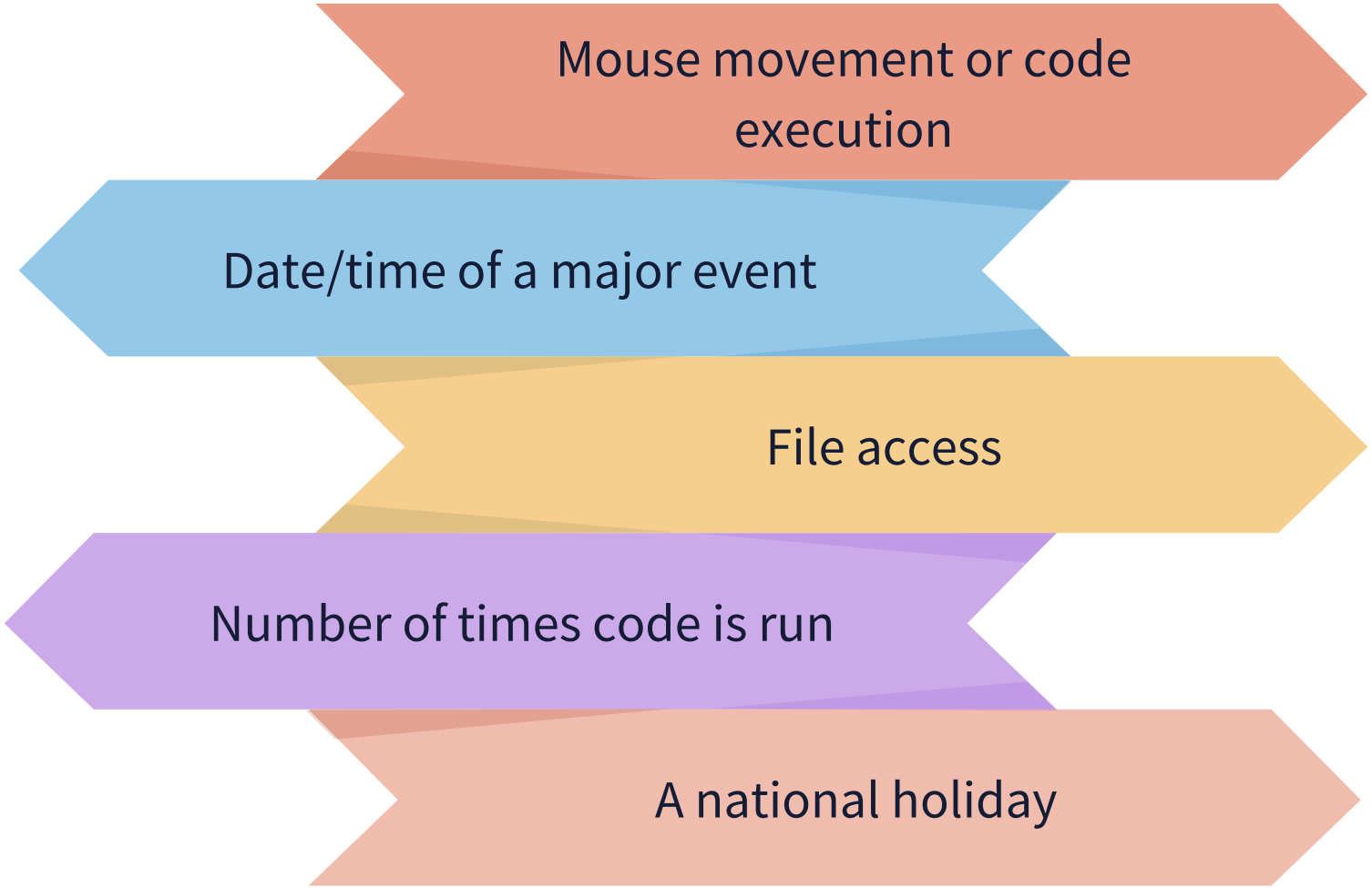
- Keystroke logging is typically done by malicious code that records keystrokes and sends data back to command-and-control servers
- Spyware uses keyloggers to capture passwords, credit card information, or other personally identifiable information (PII)
- Software can also be used to track employees or family members to adhere to acceptable use
- Keylogger detectors are special mitigation tools
- Examples: PAL KeyLogger Pro and KeyGhost



ROOTKITS

- Rootkits are a type of malware that can give a threat actor control of systems user consent or knowledge
- "Root," "admin," "superuser," or "system admin" are all interchangeable terms
- They are dangerous because they are designed to hide their presence
- A threat actor who has placed a rootkit onto a machine (often via phishing email) can remotely access and control it to deactivate the antivirus software, spy on activities, steal sensitive data, or execute other malware

LOGIC BOMBS ARE TRIGGERED BY EVENTS



PHYSICAL ATTACKS

- Safes and other containers are rated based on the amount of time a tool would take to penetrate with brute force
- Doors and windows of all types are also common targets of brute force attacks
- Although considered a preventative mechanism, locks are a delay component since all could be overcome by brute force

RFID CLONING

- RFID and NFC devices are vulnerable to a variety of physical attacks
- Crackers can clone credit and debit cards by stealing the name, account number, expiration date, and 3-digit code
- Data stored on RFID chips can be stolen, skimmed, and scanned by anyone with easily obtained RFID readers
- Skimming uses devices that overlay an ATM or point-of-sale scanner to steal the information from the victim

ENVIRONMENTAL ATTACKS

- Any environmental system that is not air-gapped can be compromised
- Many systems and sensors are "smart" or remotely accessible with IP
- They can be hacked to shut down systems, overload them, and hijack to change temperature or humidity
- If the environmental system connects to other networks, they can represent potential backdoors
- There should be a zero-trust policy and high visibility when considering these critical systems

DENIAL-OF-SERVICE ATTACKS (DOS)

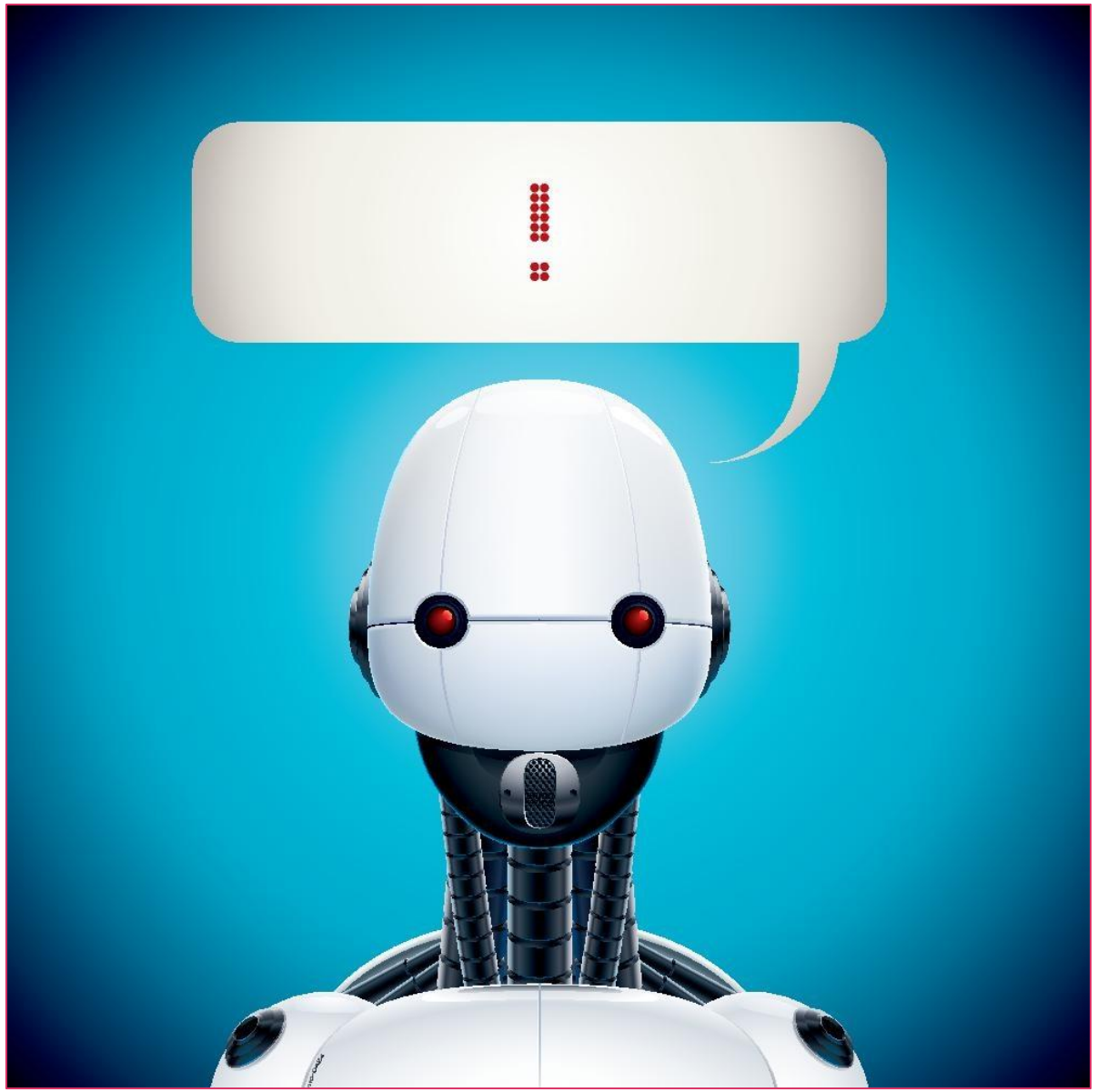
- A DoS attack happens when a malicious cyber threat actor prevents legitimate subjects from accessing information systems, infrastructure devices, or other network resources
- Affected services include email/webmail, websites, personal cloud storage, online accounts (e.g., banking), or other services that depend on a server or network
- A denial-of-service condition is accomplished by flooding the targeted host or network with traffic (i.e., ICMP, TCP, UDP) until the target cannot respond or simply crashes, preventing access for legitimate users

DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

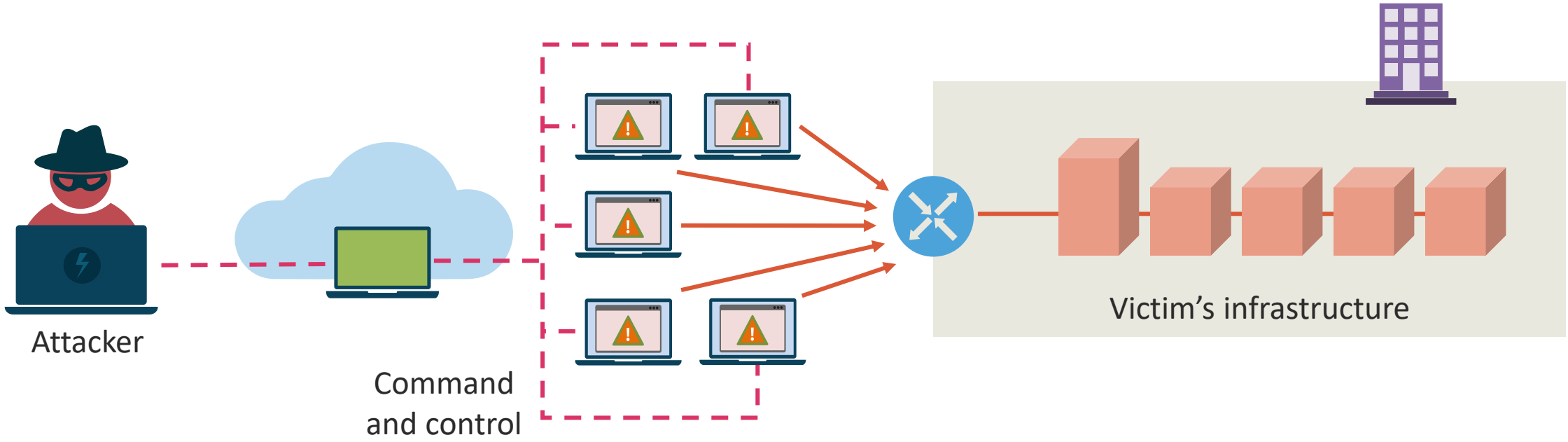
- DDoS floods a server with Internet traffic to prevent users from accessing connected online services and sites
- Some attacks are launched by hacktivists overloading an organization’s servers to make a statement or express displeasure
- Other DDoS attacks are financially motivated by competitors or involve extortion, in which perpetrators attack a company and install ransomware on their servers
- The most common form of DDoS attack is robot networks (botnets)

BOTNETS

- The most common form of DDoS attack today
- The robot network (botnet) consists of a zombie computer and a master command and control server to remotely control victims, and many victims are unaware
- The communication often occurs over Internet Relay Chat (IRC), encrypted channels, bot-centric peer-to-peer networks, and even social media
- Bots can exfil data, log keystrokes, scan memory, force a system to participate in mining cyber currency, and more



DDOS BOTNETS



DNS ATTACKS

DoS and DDoS

Attacker targets the root or down-level DNS servers to overwhelm the systems with a large amount of UDP queries

Cache poisoning

Attacker attempts to modify the DNS cache in the wrong way so that all DNS requests return an incorrect response

DNS hijacking

Similar to poisoning, the attacker often sets up a cloned site to redirect hijacked users to steal data or deliver malware

DNS spoofing

An attacker will represent a domain name and IP mapping to trick users or poison caches

DNS ATTACKS

NXDOMAIN attack

Attempts to make servers disappear from the Internet by flooding the DNS server with requests for invalid or nonexistent records

DNS flooding

This is considered a variant of the UDP flood attack, since DNS servers rely on the UDP protocol for name resolution

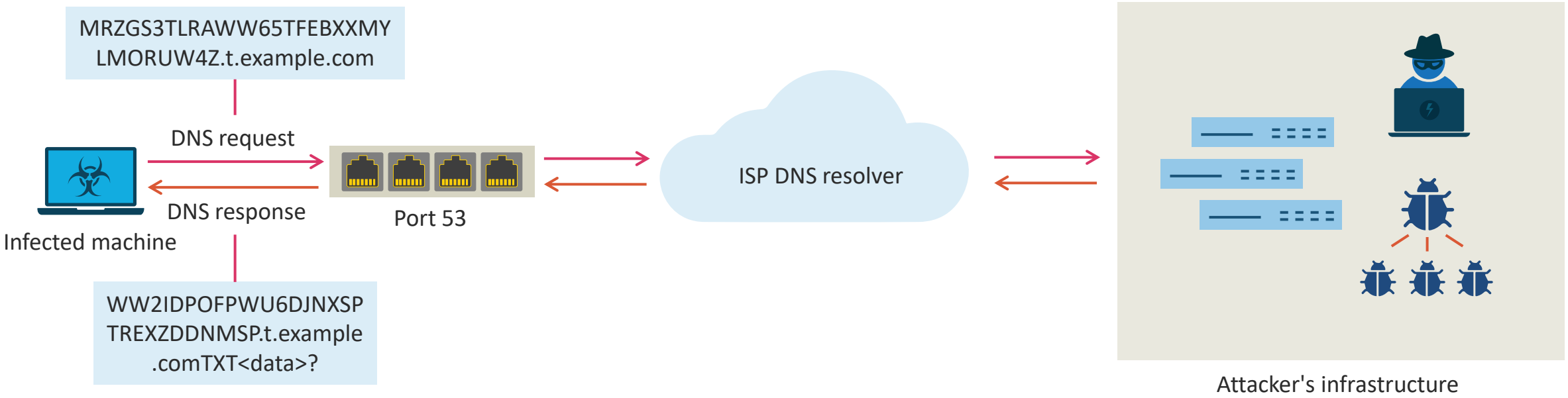
Amplification attack

A reflection-based DDoS attack in which an attacker leverages the functionality of open DNS resolvers to overwhelm a target server or network with an amplified amount of traffic

DNS tunneling

Exploits the DNS protocol to tunnel malware and other data by registering a domain server that points to the attacker's server, where a tunneling malware program is installed

DNS TUNNELING



WIRELESS ATTACKS

- Rogue access points and evil twins spoof real wireless LAN devices
- DHCP starvation uses up real leases so that a rogue server can be introduced
- Attacks target management and control frames (disassociation or de-authentication) used for roaming devices
- On-path attacks used to be called man-in-the-middle, where rogue devices inject into TCP connections and other communications
- Jamming is a form of denial-of-service attack towards access points (APs) and wireless controllers

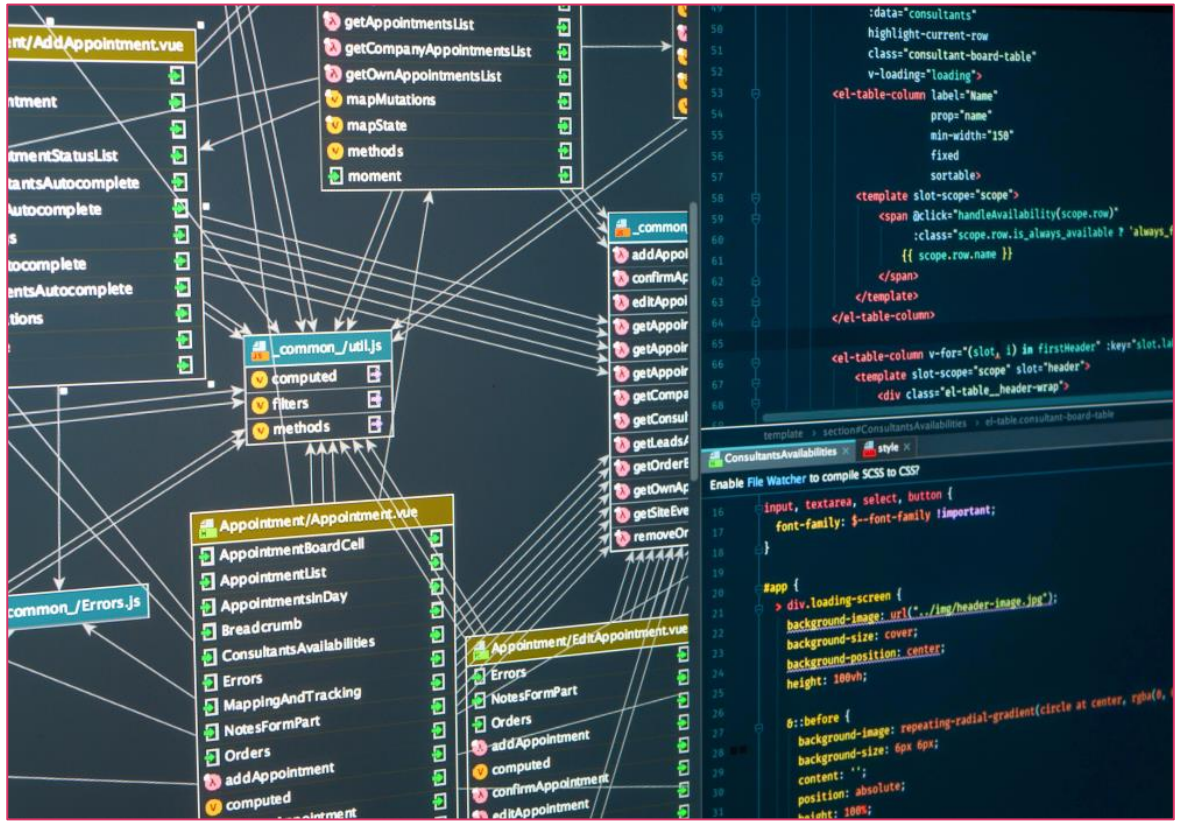
CREDENTIAL REPLAY

- A credential replay attack involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of generating an unauthorized effect or gaining unauthorized access
- Attackers will also perform other reconnaissance attacks, dumpster diving, and various social engineering to harvest the internal usernames of an organization

SQL INJECTION (SQLI)

Involves inserting a SQL query through input data from client to server application and can allow for several exploits

- Read sensitive database data (SELECT FROM)
- Change database data (INSERT, UPDATE, DELETE)
- Execute administrative functions (e.g., shutdown DBMS)
- Get the contents of files on database a management system (DBMS)
- Run commands on the operating system



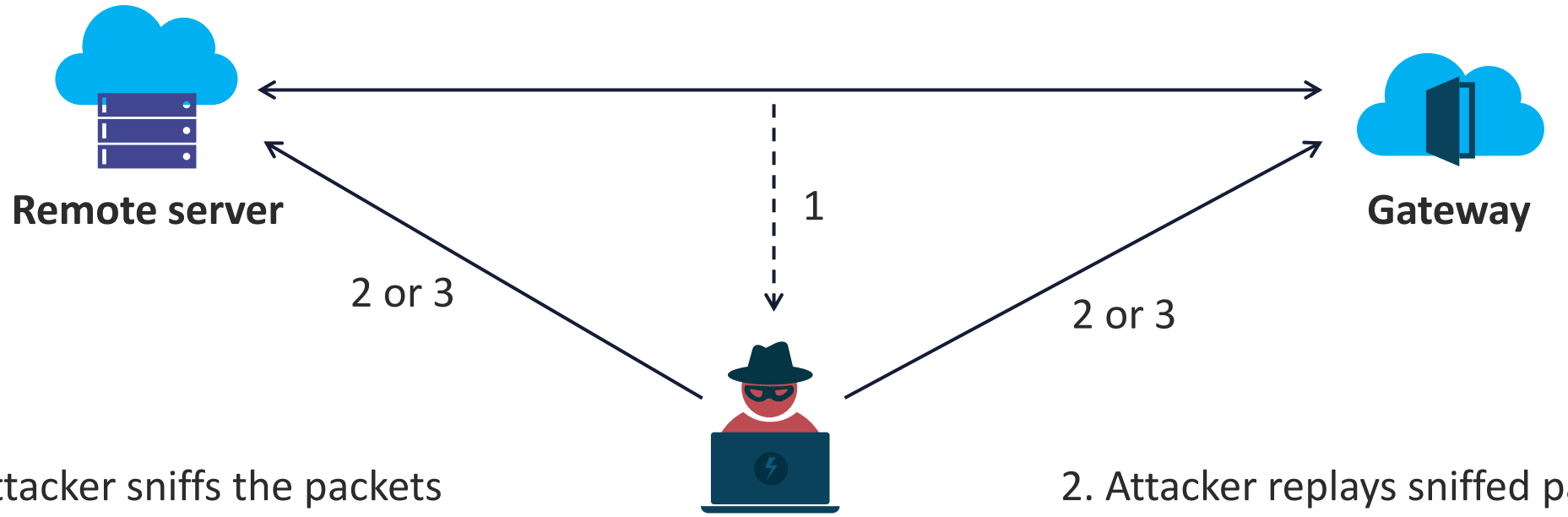
BUFFER OVERFLOWS

- The buffer overflow attacker manipulates coding errors to compromise affected applications running on critical servers
- It changes the program's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data
- It usually involves violating programming languages and overwriting the bounds of the buffers they exist on when code
  - Is reliant on external data to control its behavior
  - Is dependent on data properties that are enforced beyond its immediate scope
  - Is so complex that programmers are not able to predict its behavior accurately

REPLAY ATTACKS

- A replay attack happens when an attacker snoops on a secure network communication, intercepts it, and then deceptively delays or resends it to misdirect the receiver into doing what the cracker wants
- The added challenge of replay attacks is that a script kiddie does not need advanced skills to decrypt a message after capturing it from the network
- The attack could be successful simply by resending the entire communication

REPLAY ATTACK



1. Attacker sniffs the packets exchanged between the gateway and the remote server

2. Attacker replays sniffed packets at a different time interval

3. Attacker modifies and sends sniffed packets or forges new packets

PRIVILEGE ESCALATION

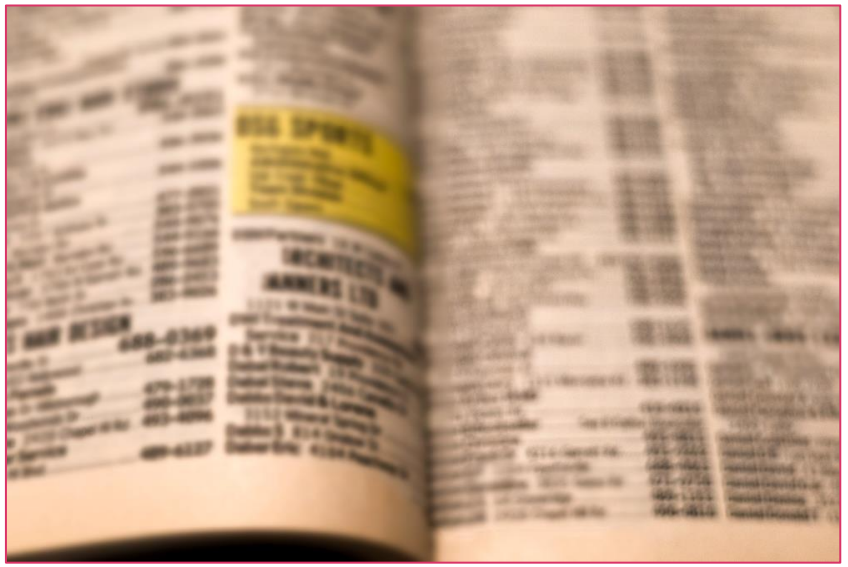
- Attackers exploit human misconfiguration, design flaws, or omissions in web applications
- This is closely related to lateral movement — tactics by which an attacker moves deeper into a network looking for sensitive assets
  - The result is an internal or external user with unauthorized system privileges
- Depending on the extent of the attack, bad actors can do minor or major damage
- It might be a simple unauthorized email or a ransomware attack on vast amounts of data

FORGERY AND DIRECTORY TRAVERSAL ATTACKS

Cross-site request forgery (CSRF) is an attack that tricks authenticated users into inputting a request to a web application

CSRF attacks exploit the trust a web application has in an authenticated user

It exploits a vulnerability in a web application if it cannot differentiate between a request generated by an end user and a request generated by a user without their consent



Directory (or path) traversal (or climbing) is a type of HTTP exploit where the attacker leverages the web server software to access data in a directory other than the server's root directory

The threat agent, usually a browser, can view restricted files or execute commands on the server

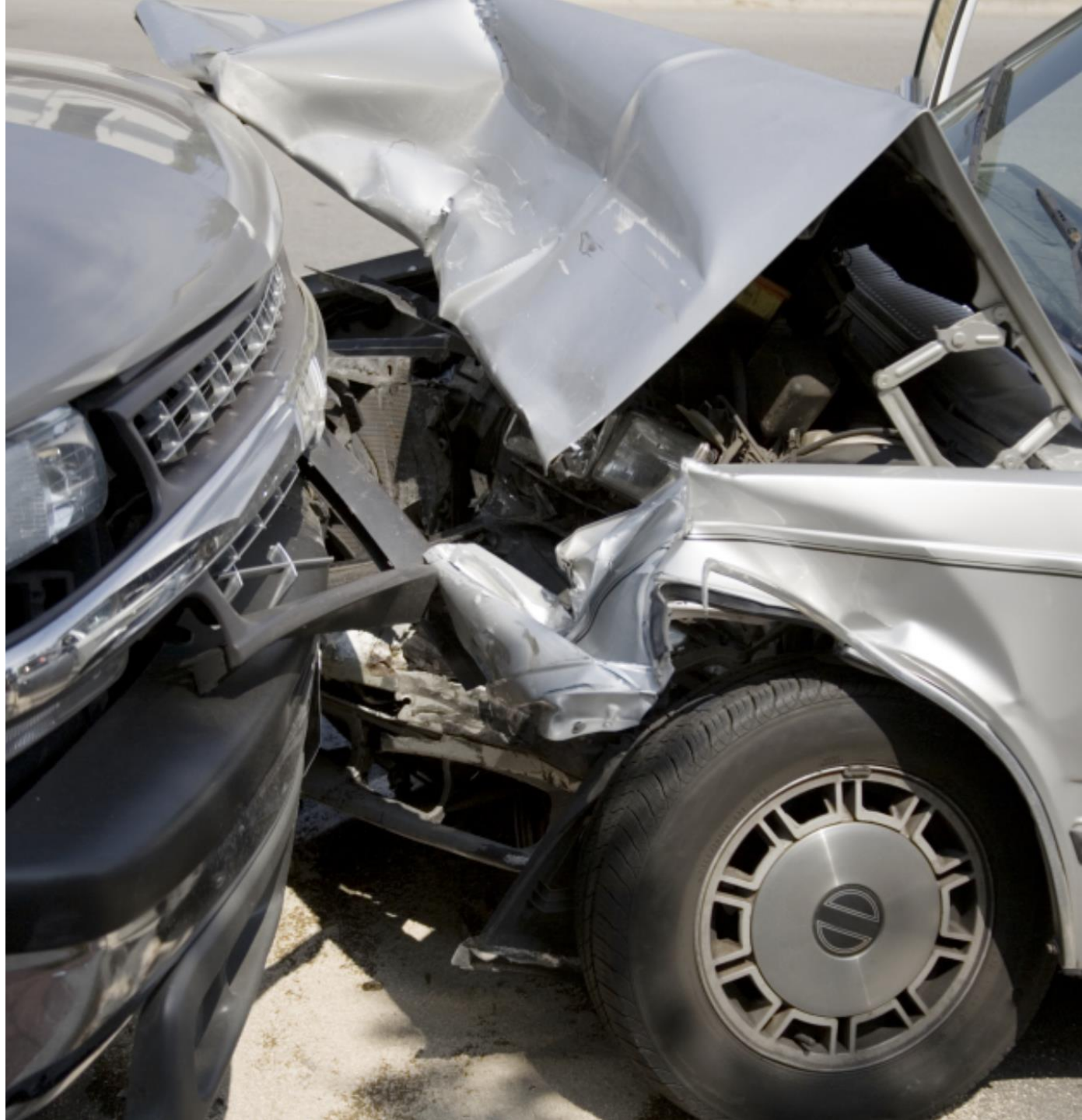
Any server that fails to validate input data from web browsers is vulnerable to a directory traversal attack

CRYPTOGRAPHIC DOWNGRADE ATTACK

- In a downgrade attack, the attacker attempts to force two hosts on a network (typically a browser and web server) to use an insecure or weakly protected data transmission protocol
- The downgrade is often HTTP instead of HTTPS or SSL instead of TLS
- If a downgrade attack is successful, the attacker can exploit connection vulnerabilities to intercept and read transmitted data
- It is considered a type of on-path

COLLISION ATTACKS

- To be considered trustworthy, a cryptographic hashing mechanism must be "collision-resistant"
- This means that two different inputs should never produce the same fingerprint or digest
- This collision can then be exploited by any application that compares two hashes together, such as password hashes, file integrity checks, and others
- MD5 is no longer considered collision-resistant



CRYPTOGRAPHIC BRUTE FORCE ATTACKS

- A brute force attack, also known as an exhaustive search, is a cryptographic hack that depends on guessing all possible combinations of a targeted password until discovered
  - If the password is weak, it could take mere seconds with hardly any effort
- A brute force attack is time and processor-intensive and may be impossible or absurd from a physics standpoint
- It can also relate to trying all possibilities in a cryptosystem keyspace, which is why the larger bit size or modulus is preferred

SIDE CHANNEL ATTACKS

- A side channel attack is enabled by leakage of information from a physical cryptosystem such as a smart card or cryptoprocessor
- Attributes that can be exploited in a side-channel attack, including timing, power consumption, and electromagnetic and acoustic emissions
- Wireless WPA3 had an early side-channel vulnerability in its Dragonfly protocol

DEMO: EXPLORING PASSWORD ATTACKS

In this demo…

We will explore password attacks and tools at:

https://www.google.com/search?client=firefox-b-1-d&q=password+attack+tools

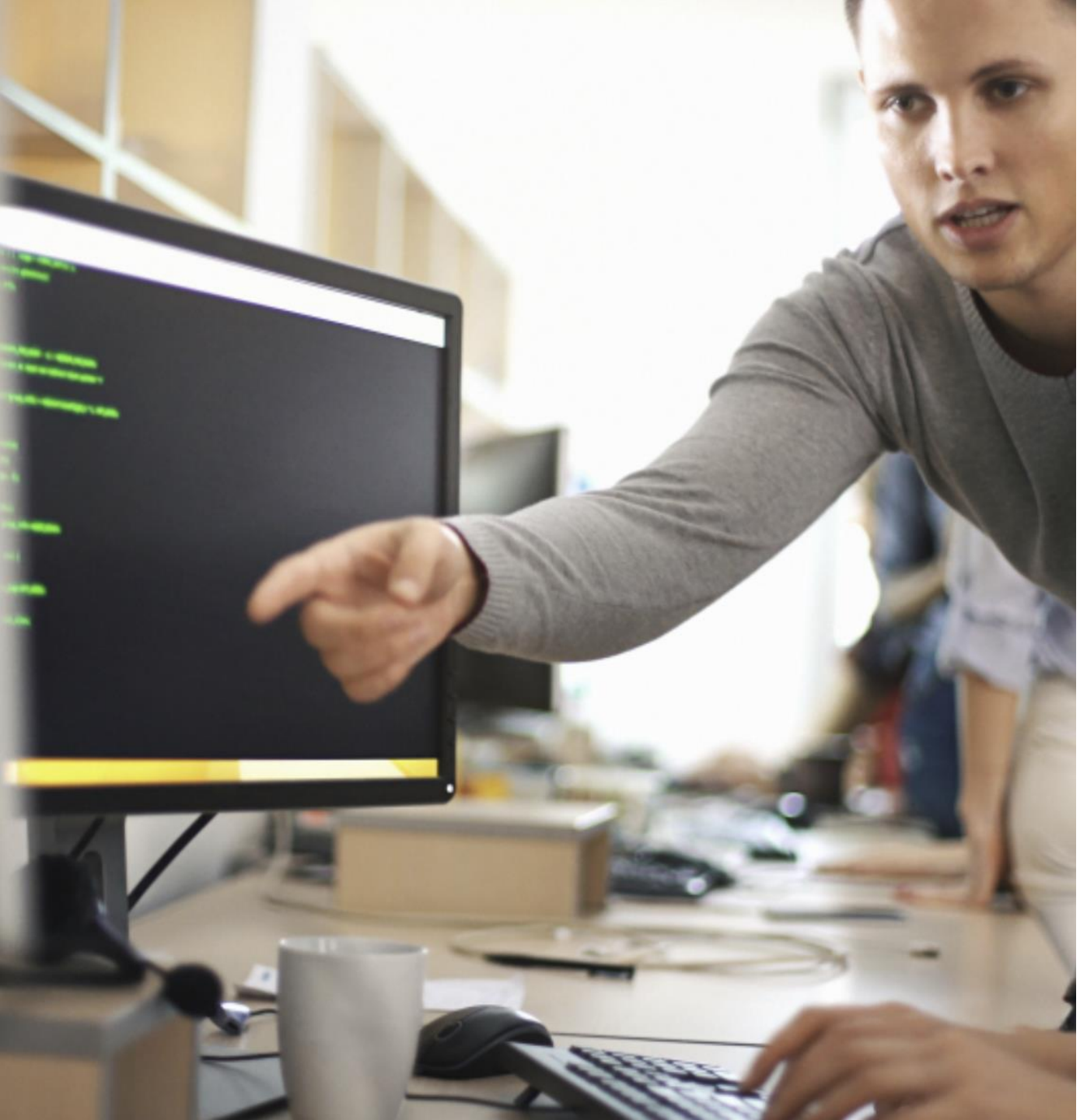
INDICATORS OF COMPROMISE (IOCS)

These are network or host-based cyber observables

Forensic artifacts of an incursion or disturbance

A measurable event or stateful property in the cyber domain

Registry entries, files on disk and in-memory, etc.



INDICATORS OF COMPROMISE

- Account lockout
- Concurrent session usage
- Blocked content
- Impossible travel
- Resource consumption
- Out-of-cycle logging
- Missing logs

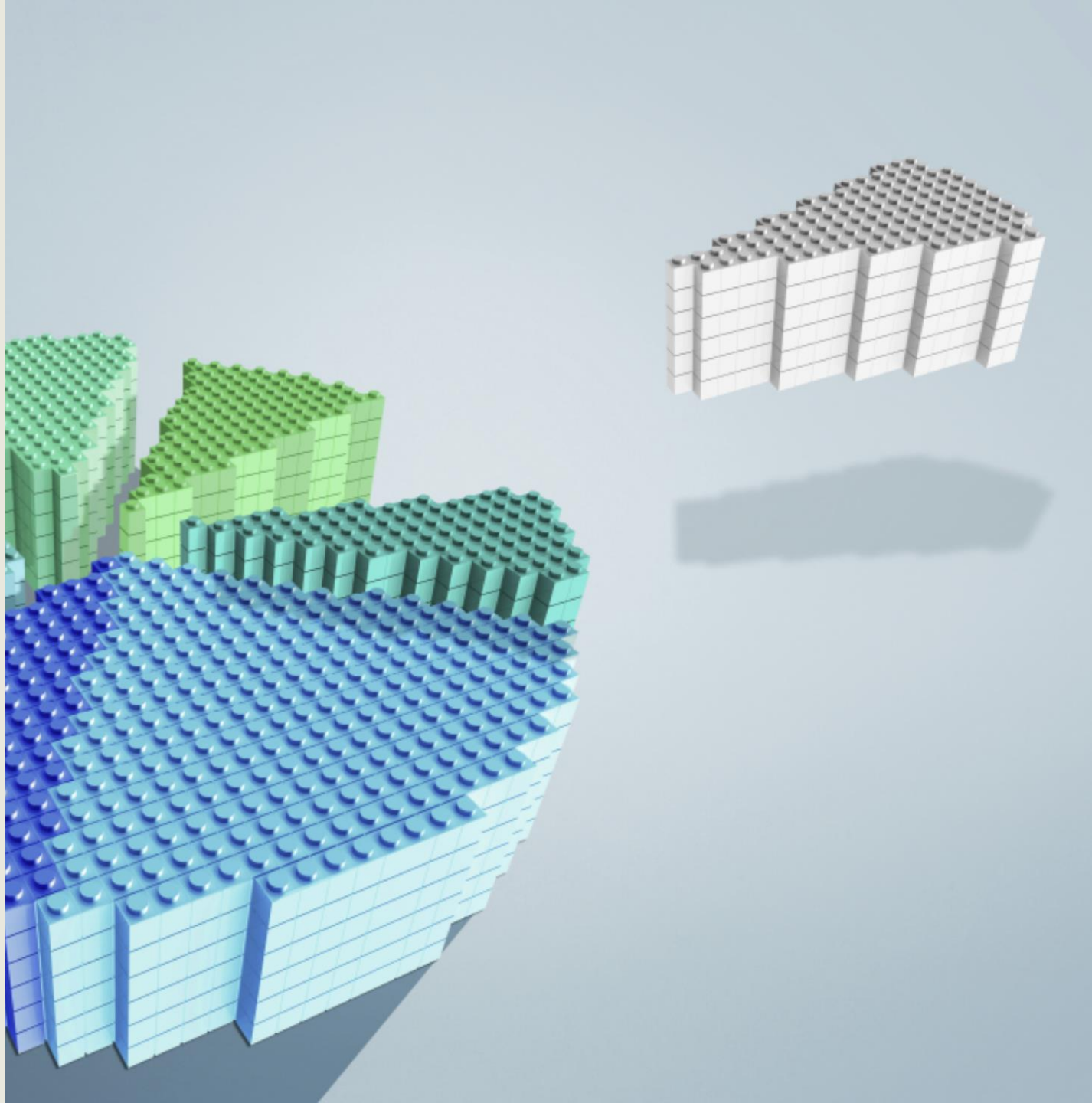
MITIGATION TECHNIQUES

Objectives

- Examine segmentation, isolation, and access control models
- Compare configuration and patch management
- Explore least privilege and separation of duties
- Look at encryption for access controls, monitoring, and visibility
- Learn about decommissioning and offboarding
- Compare hardening techniques

SEGMENTATION AND ISOLATION

- Segmentation divides a computer network into smaller parts
- The purpose is to improve network performance and security
- Other terms that often mean the same thing are network segregation, network partitioning, and network isolation
- Segmentation and isolation are logically and physically accomplished in network infrastructures using zoning
- Zoning (segmentation) is a logical design approach used to control and restrict access

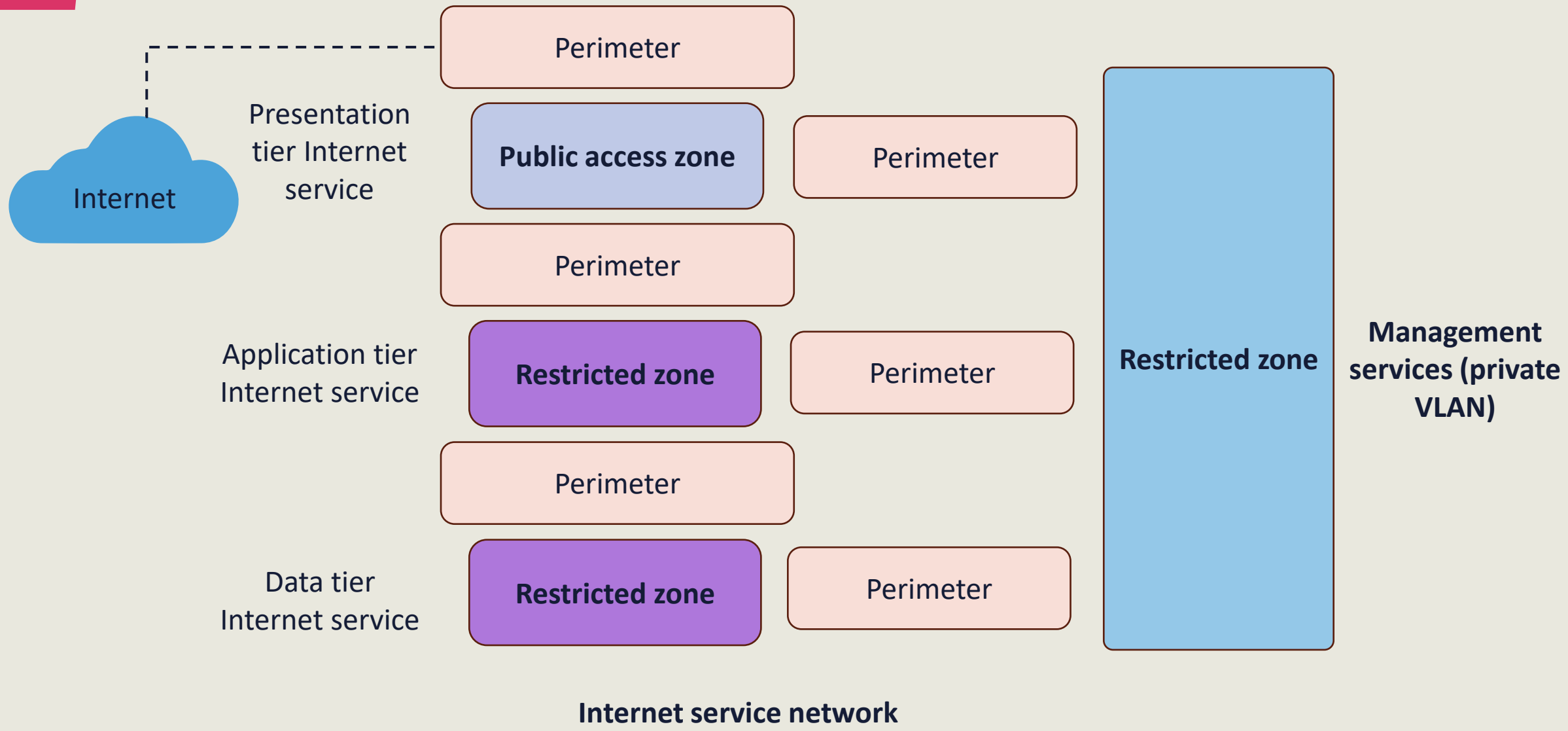


SEGMENTATION AND ISOLATION

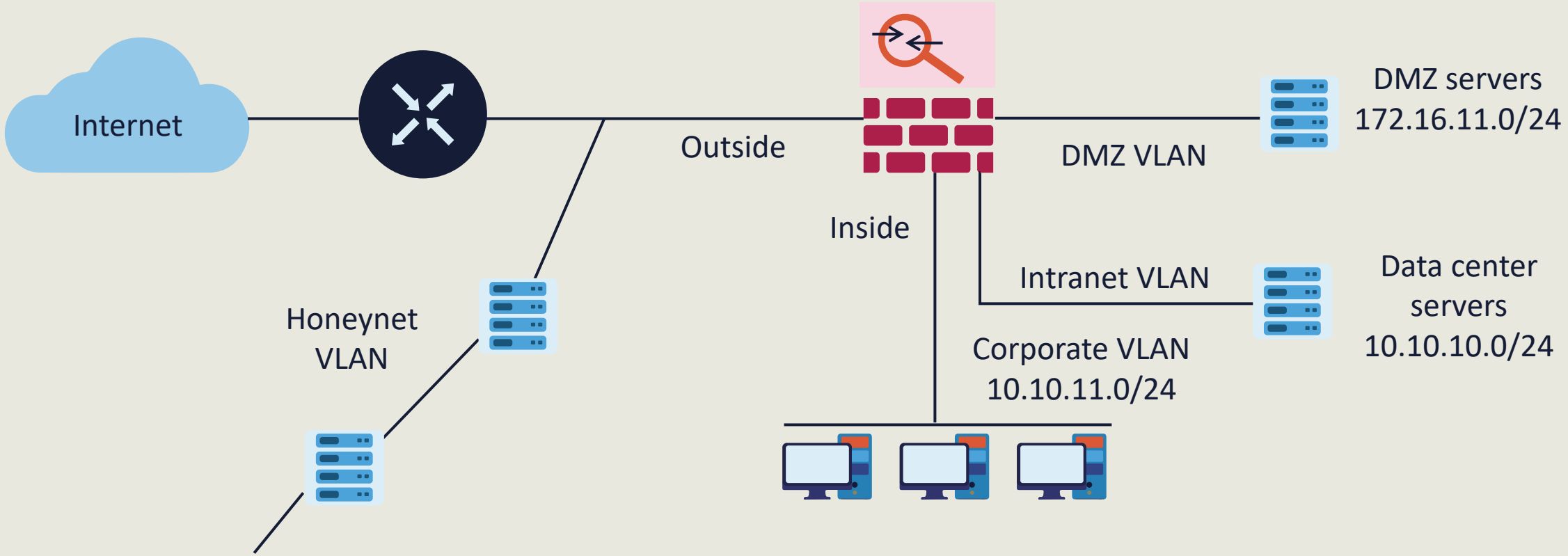
Each zone has fundamental characteristics defined by the security:

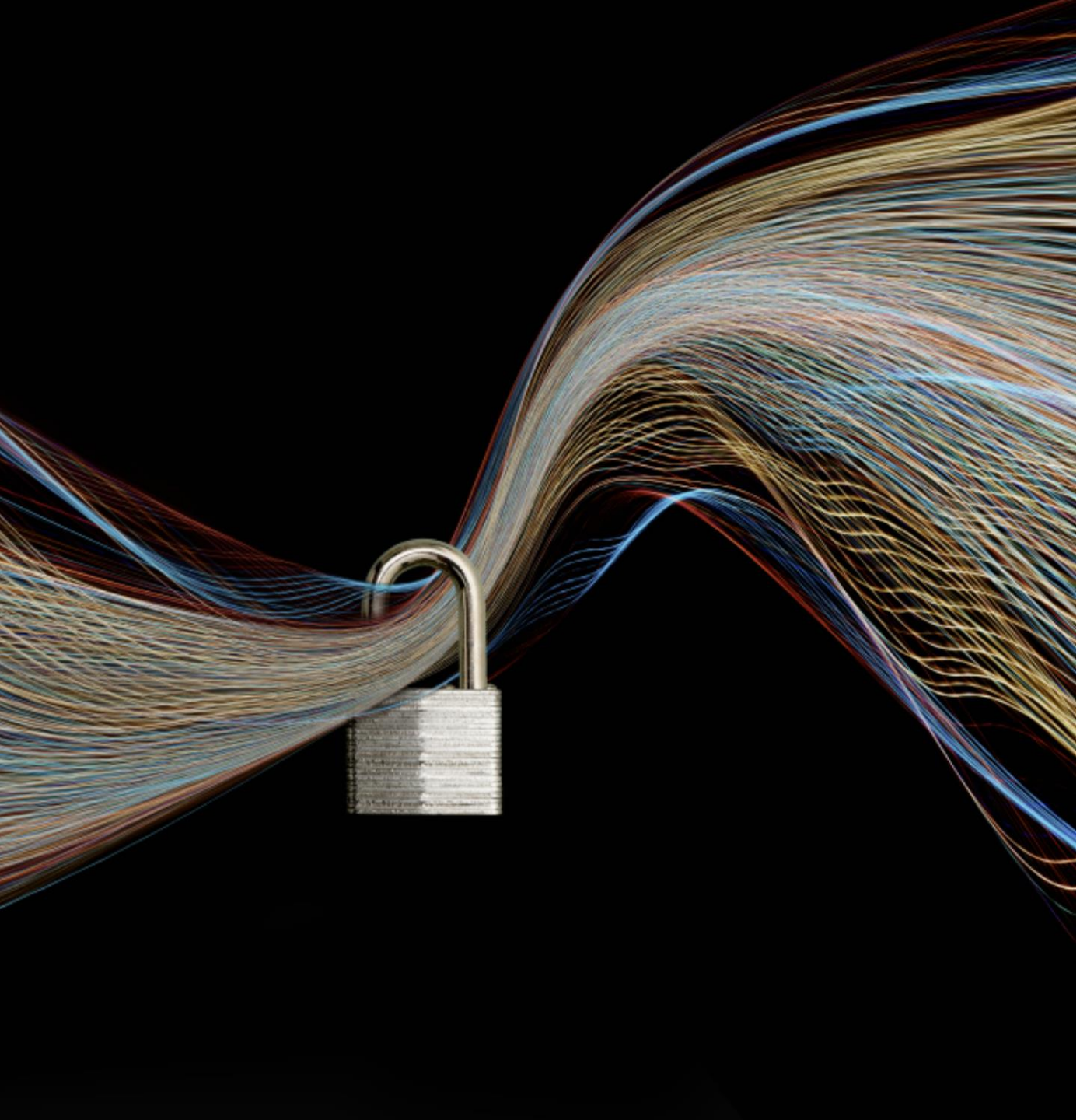
- Every zone contains one or more separate, routable networks
- Every separate, routable network is contained within a single zone
- Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs)
- The only zone that may connect to the public zone is the public access zone (PAZ) (DMZ)

LOGICAL ZONING



PHYSICAL/LOGICAL ZONING





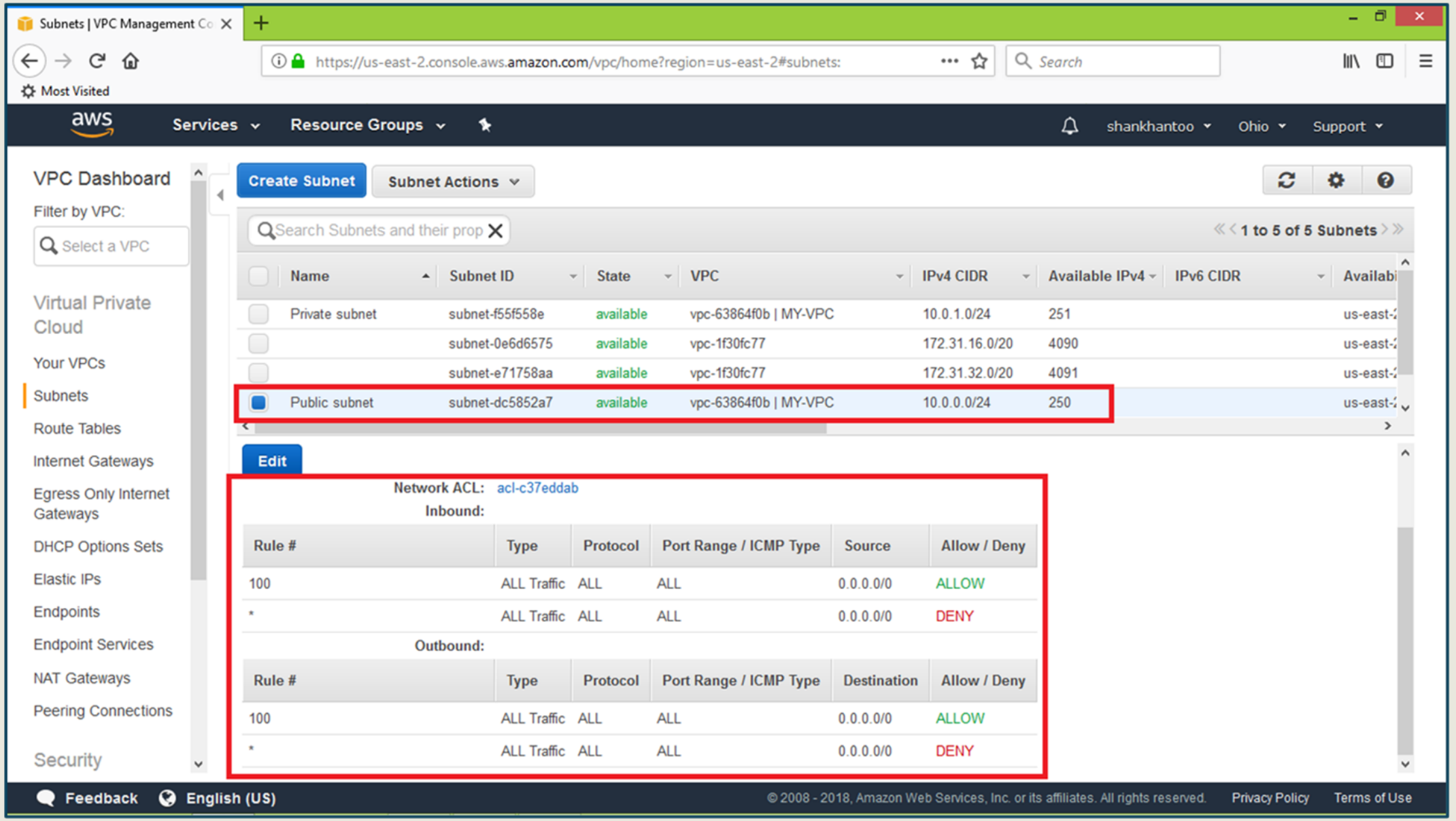
ACCESS CONTROL LISTS (ACLS)

- Allow stateless (static) traffic filtering and management of IPv4 and IPv6 traffic to and from a network interface or virtual local area network (VLAN)
- Contain ordered rules or access control entries (ACEs) to permit (allow) or deny (block) based on Internet Protocol (IP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) services and ports, as well as Internet Control Message Protocol (ICMP) messages and codes
- Function as additional infrastructure defense-in-depth mechanisms
- Have an implicit deny-all as the last entry applied if nothing matches

NETWORK ACCESS CONTROL LISTS (NACLS)

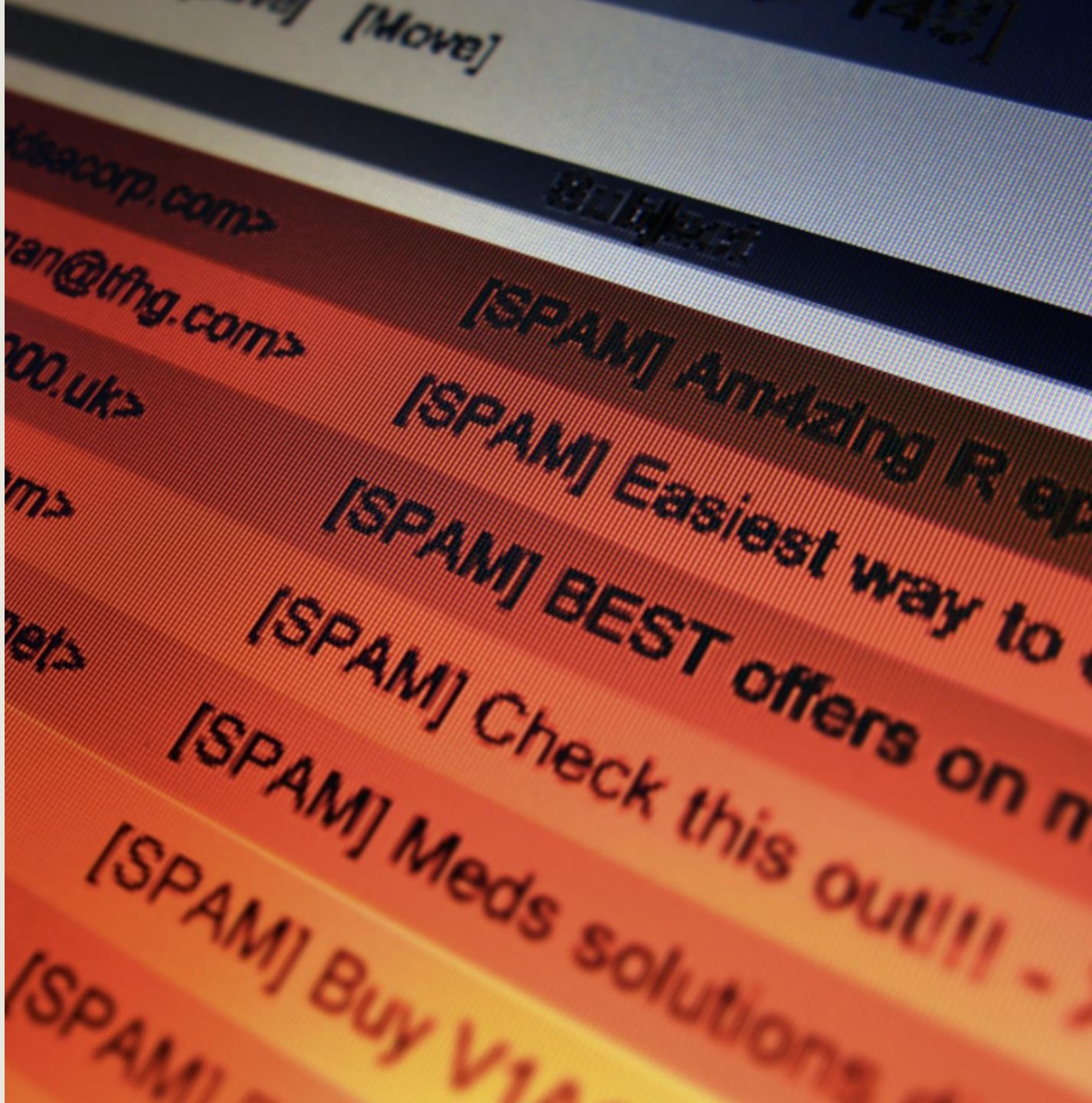
- Are most often static inbound and outbound access lists applied to virtual networks or virtual private clouds
- Apply to all instances, containers, appliances, etc. in the virtual network (VNet)
- Are typically configured with the same techniques as traditional access lists

NACLs at AWS

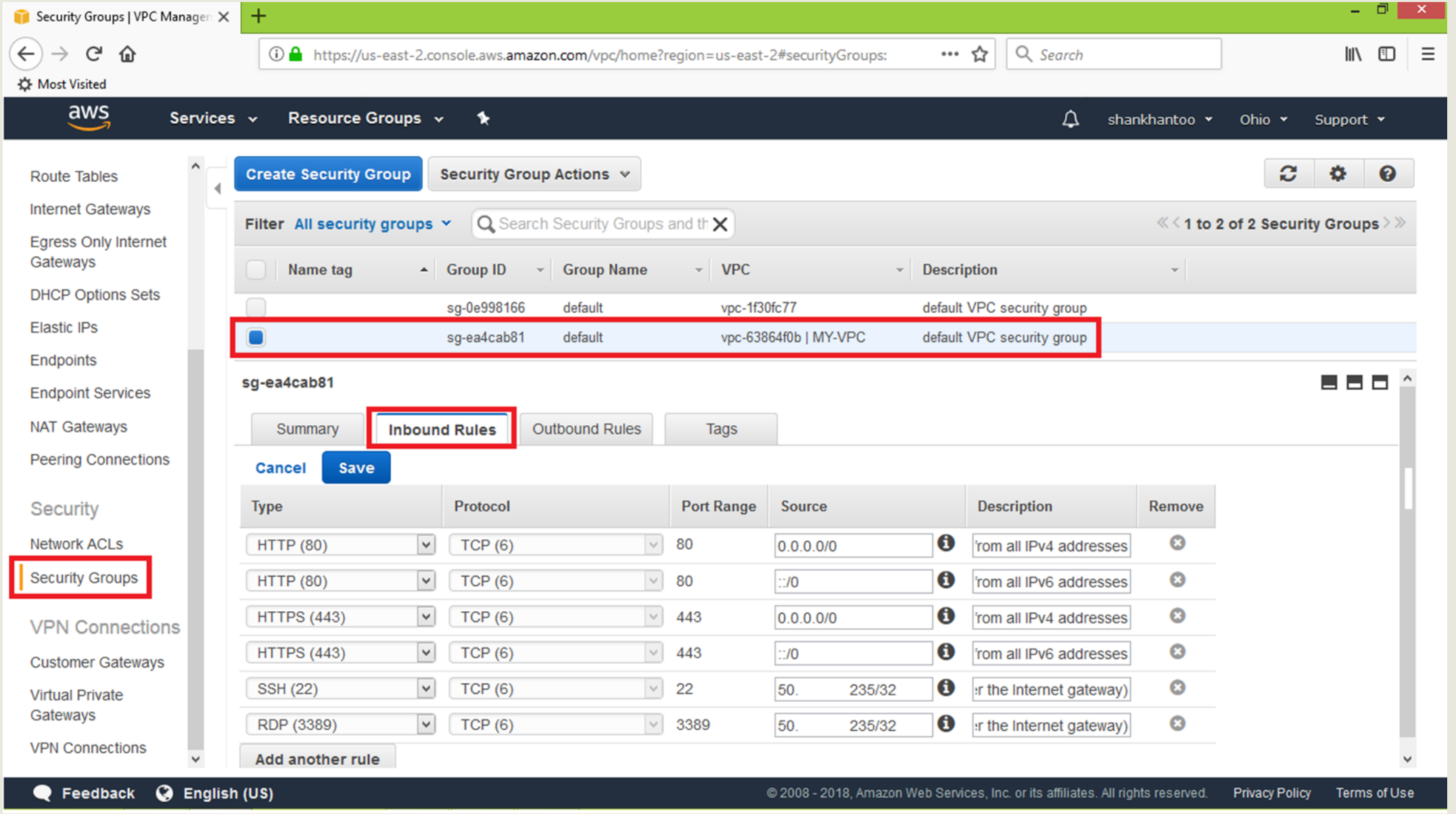

Subnets | VPC Management Co
https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#subnets:
Search
Most Visited
aws
Services
Resource Groups
shankhantoo
Ohio
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Create Subnet
Subnet Actions
Search Subnets and their prop
1 to 5 of 5 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Private subnet subnet-f55f558e available vpc-63864f0b | MY-VPC 10.0.1.0/24 251
subnet-0e6d6575 available vpc-1f30fc77 172.31.16.0/20 4090
subnet-e71758aa available vpc-1f30fc77 172.31.32.0/20 4091
Public subnet subnet-dc5852a7 available vpc-63864f0b | MY-VPC 10.0.0.0/24 250
Edit
Network ACL: acl-c37eddab
Inbound:
Rule # Type Protocol Port Range / ICMP Type Source Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
* ALL Traffic ALL ALL 0.0.0.0/0 DENY
Outbound:
Rule # Type Protocol Port Range / ICMP Type Destination Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
* ALL Traffic ALL ALL 0.0.0.0/0 DENY
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

SECURITY GROUPS

- Are commonly stateful "allow-list" firewalls that apply to layer 3 and layer 4 network traffic
- Can be applied to a virtual load balancer and instance virtual interface:
  - These operate at the hypervisor level attached to the virtual elastic network interfaces (eth0)
- Are called network security groups (NSGs) if applied to an entire virtual network
- Have no explicit deny rules like NACLs, but rather have an implicit deny if nothing matches the "allow-list"
- Evaluate all rules before a decision is made



Security Groups at AWS



PERMISSIONS

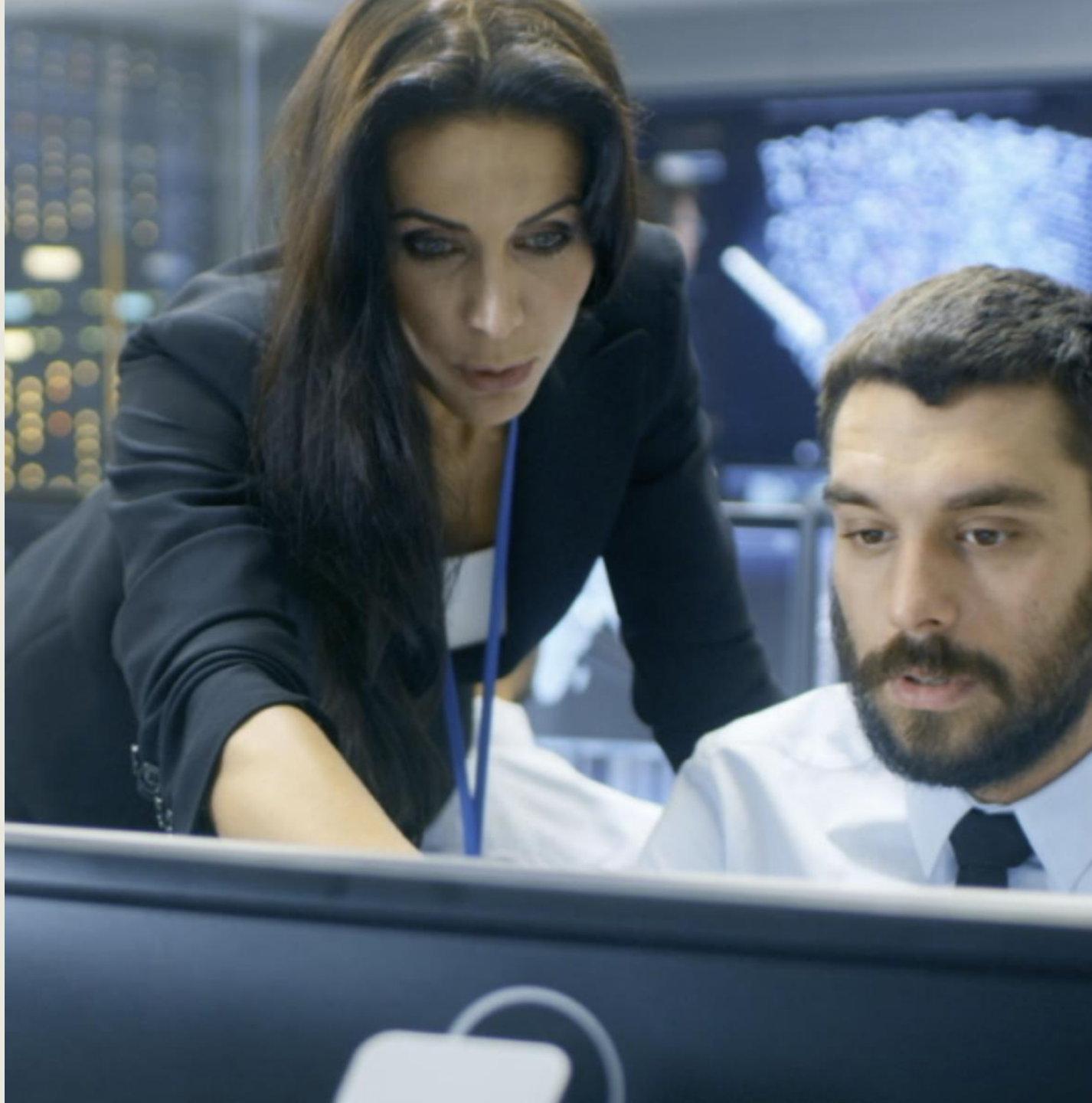
- Permissions that principals have can be dictated and enforced by the network operating file system (Linux or Windows) or using a directory service as in:
  - **Read** (r) permission to access the file's contents
  - **Write** (w) permission to modify or change the contents of a file
  - **Execute** (x) permission to execute the contents of a file
- One can change a Linux file and directory permissions with the **chmod** command, which stands for "change mode"

CONFIGURATION MANAGEMENT

- The goal of configuration management (CM) is to ensure that accurate and meaningful information is readily available regarding the configuration of applications and services along with the configuration items (CI) that support them
- It includes all relationships and dependencies between the CIs:
  - Objects include hardware, software, networks, sites, vendors, suppliers, and people

CONFIGURATION MANAGEMENT

- CM is a governance and systems life cycle process for ensuring consistency among all assets (configuration items) in an operational environment:
  - Classifies and tracks individual CIs
  - Documents functional capabilities and interdependencies
  - Verifies the effect a change to one configuration item has on other systems



CONFIGURATION MANAGEMENT

- CM practices offer the required data about assets and their configurations, including their interactions with other assets, which assists administrators and managers with
  - Problem resolution
  - Incident response
  - Network component deployment
  - Strategy formulation
  - Budgetary forecasting
  - Overall decision-making

Configuration Management System (CMS)

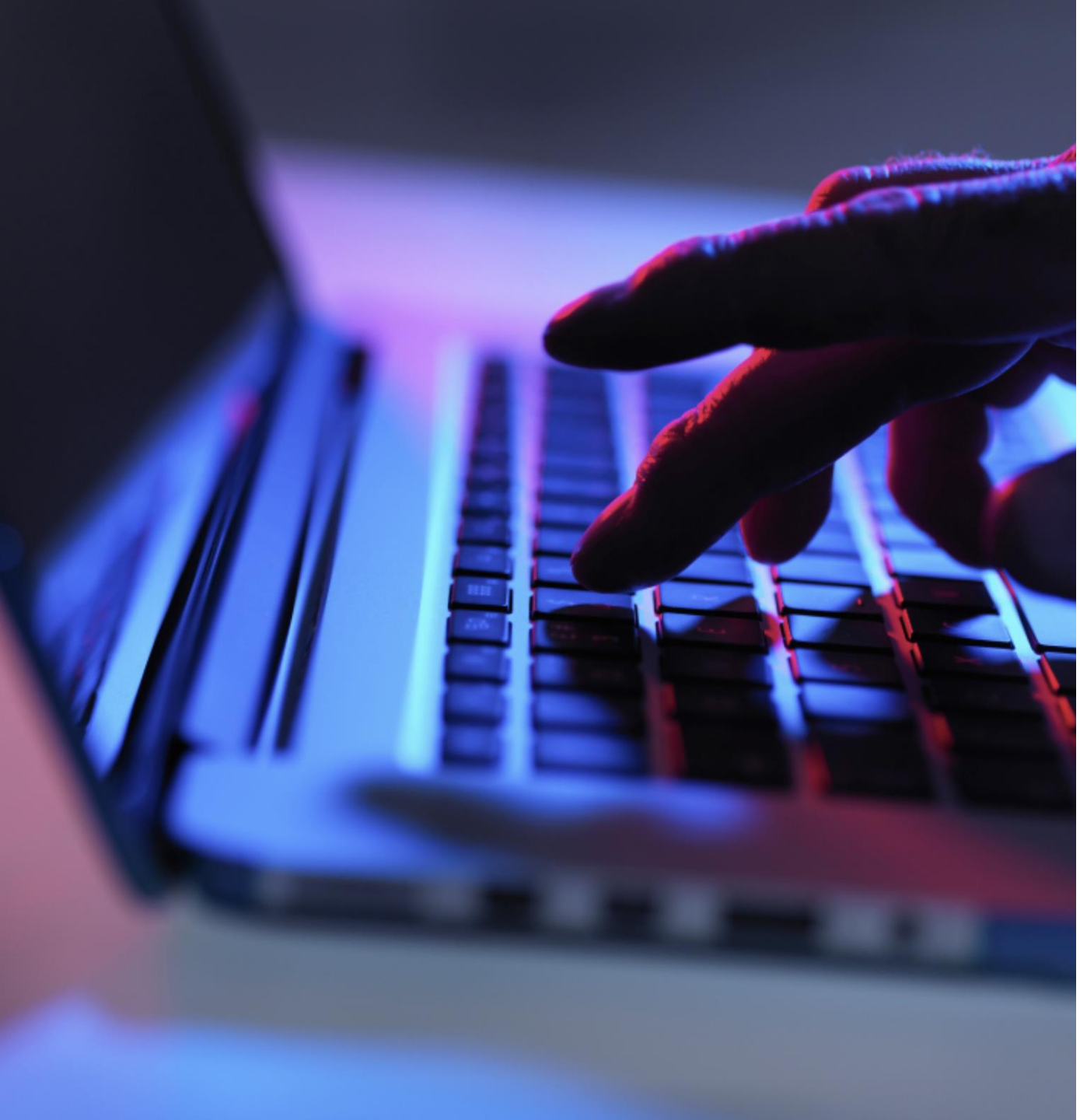
- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
- All information should be tagged and labeled with a common unified schema, preferably using key-value pairs
- This data will populate the configuration management database (CMDB)
- Relational databases have been used historically
- NoSQL/document databases are emerging as a common solution
- A communication service provider (CSP) service such as AWS DynamoDB could be leveraged

PATCH MANAGEMENT

- Patch management is the process of applying (hopefully fully tested) updates to software, drivers, and firmware to protect against vulnerabilities
- Effective patch management helps ensure the best operating performance of systems, boosting productivity
- All systems need to be secured with patches, if possible
- The risks of disregarding patch management can cause exposure of business to leaks and breaches, loss of productivity, and loss of reputation

PATCH MANAGEMENT BENEFITS

- Protects all endpoints from attackers
- Keeps all systems running in an optimized fashion
- Promotes productivity within the organization
- Helps lower the cost of device life cycle maintenance and repair
- Supports laws, regulations, and compliance standards



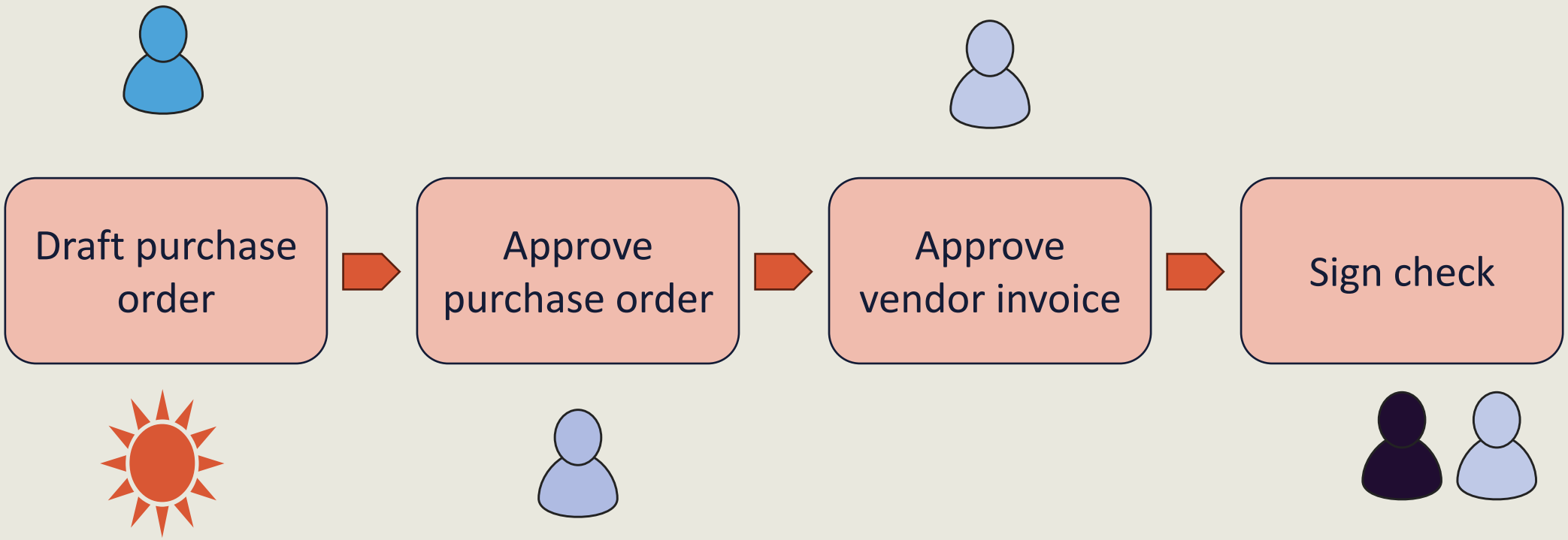
LEAST PRIVILEGE

- Is the principle that users and programs should only have the necessary privileges to complete their tasks, according to the National Institute of Standards and Technology (NIST)
- Is also referred to as "need to know" or staying within one’s "pay grade" or classification level
- Is an aspect of authentications, authorization, and accounting (AAA) and identity and access management (IAM) where the subject has just the proper level or number of permissions and rights to perform the job role or responsibility and nothing more:
  - It should be built into all access control architectures
- Any deviation (escalation or elevation), if allowed, should go through an established change control IT service or service desk implementation

SEPARATION OF DUTIES

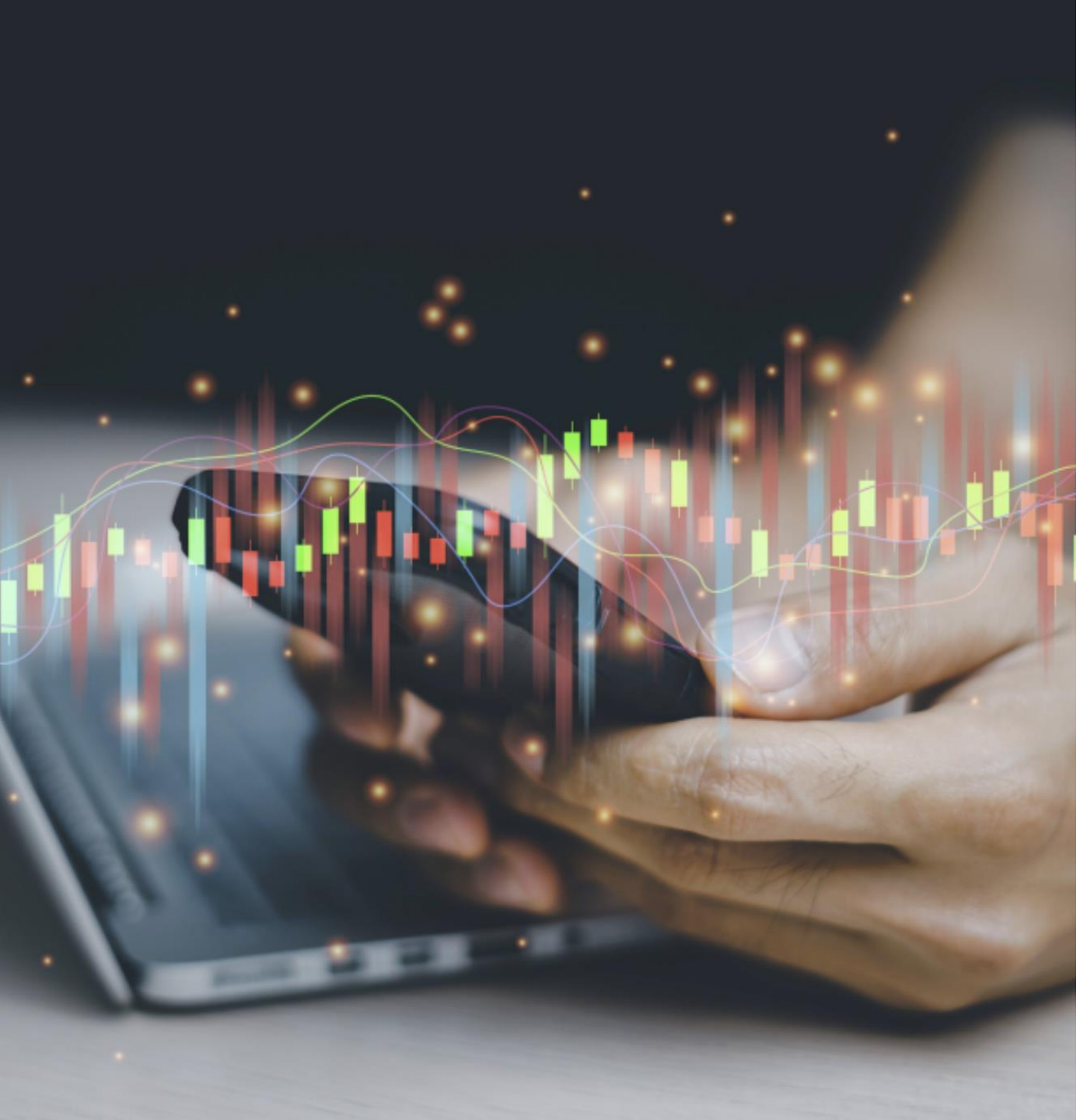
- Separation (also segregation) of duties (SoD) refers to the principle that no user should be given enough privileges to misuse the system on their own:
  - For example, the person authorizing a paycheck should not also be the one who can prepare them
- SoD can be enforced either statically (by defining conflicting roles) or dynamically (by enforcing the control at access time)
- An example of dynamic separation of duty is the two-person rule:
  - The first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first

SEPARATION OF DUTIES



SoD

- SoD may also involve dual operator principles where two or more subjects are needed to modify or approve:
  - Example: Two signatures or cryptographic keys are required for certain actions
- Rotation of duties is also a related principle:
  - Example: Mandatory time off or forced vacations



ENCRYPTION IN ACCESS CONTROL

- Encryption helps protect private information or sensitive data and can enhance the security of communication between client apps and servers
- In essence, when data is encrypted, even if an unauthorized person or entity gains access to it, they will not be able to read it
- Origin authentication uses symmetric and asymmetric encryption keys in a variety of systems, including digital signatures

ENCRYPTION IN ACCESS CONTROL

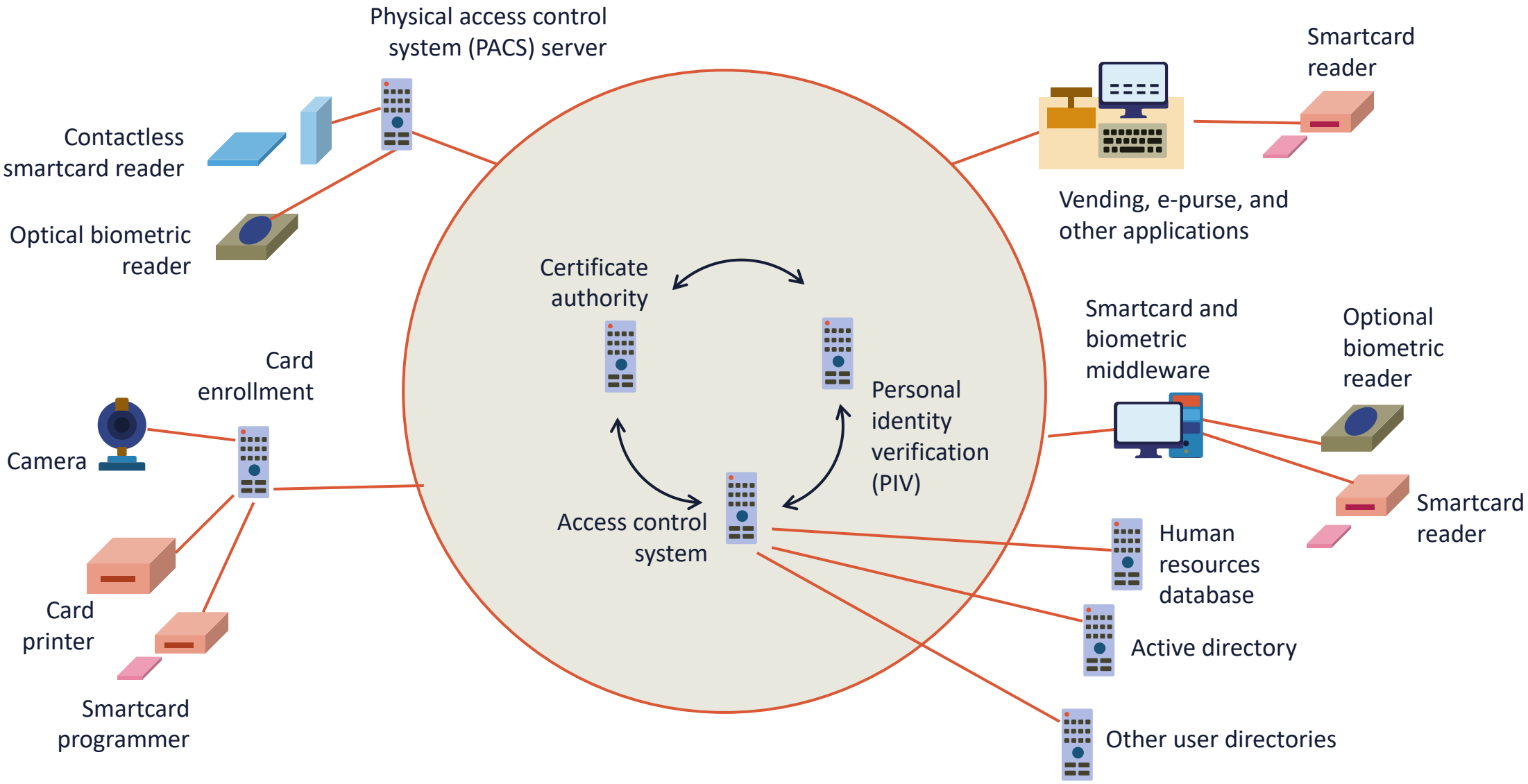
- For example, encryption technologies are involved in shielding private and secret information from unauthorized users, thus safeguarding confidentiality
- This is done by enciphering information in such a way that only authorized users – users with the right key – can access the decrypted data

MONITORING AND VISIBILITY OF ACCESS CONTROLS

- Access controls will determine which subjects have read access or visibility into critical access, such as sensitive data
- This visibility is vital for data in transit over remote channels and data stored at third-party locations like code repositories (Git), personal cloud storage, and cloud-based block, object, and file storage systems
- Access control mechanisms also must be completely visible and always monitored

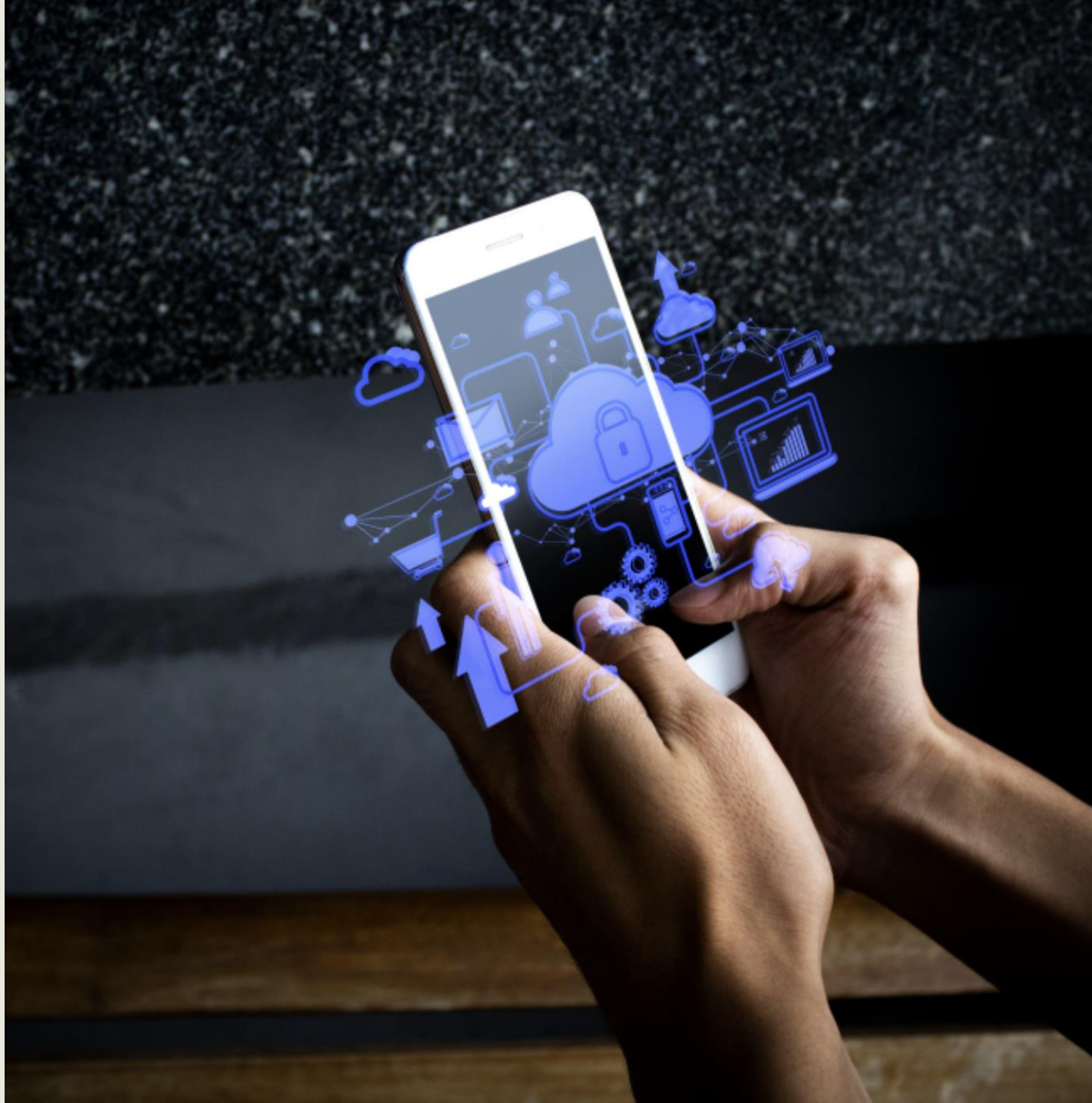
ACCESS CONTROL VISIBILITY

- It is becoming more common to automate monitoring visibility and sending feeds to locations such as security operations centers (SOC) or cloud security information and event management (SIEM)/security orchestration, automation, and response (SOAR) systems like Azure Sentinel
- Audits should be performed regularly to discover gaps or "privilege creep" that can occur with poorly maintained access control and inventory systems
- Other tools that can be used are compliance scanners, PowerShell scanners, vulnerability scanning, and penetration testing


Physical access control system (PACS) server
Contactless smartcard reader
Optical biometric reader
Smartcard reader
Vending, e-purse, and other applications
Certificate authority
Personal identity verification (PIV)
Access control system
Card enrollment
Camera
Card printer
Smartcard programmer
Smartcard and biometric middleware
Optional biometric reader
Smartcard reader
Human resources database
Active directory
Other user directories

DECOMMISSIONING AND OFFBOARDING

- Outgoing employees pose major security risks to organizations
- Security practitioners should make offboarding strategies more resilient
- Without secure off-boarding processes, enterprises expose themselves to a variety of risks, from the harmlessly accidental to the maliciously purposeful
- Risks include data theft, disgruntled leavers, shadow (ghost) IT, unauthorized Software as a Service (SaaS) usage, IT and HR siloed and out-of-sync, access not removed promptly



DECOMMISSIONING AND OFFBOARDING BEST PRACTICES

- Generate solid onboarding policies and processes
- Encourage proactive, interdepartmental collaboration with stakeholders
- Secure corporate assets, devices, and associated credentials
- Make sure there is complete visibility of employees' SaaS, cloud, and third-party access, usage, and permissions
- Monitor for uncommon or even risky behavior of outgoing staff members
- Handle all leavers respectfully and transparently

HARDENING SYSTEMS

- Classic methods of hardening systems involve shutting down TCP and UDP ports and services, including ICMP messages and codes
- Only necessary secured protocols should be used, for example, Secure Shell (SSH) instead of teletype network (telnet)
- Continual patch management initiatives must be implemented for all systems and applications
- Strict least privilege access controls should be used for all administrative users
- Ongoing monitoring and visibility must be instigated

HARDENING SYSTEMS

- Data, systems, and applications can be hardened using symmetric and asymmetric cryptosystems, including data at rest, in transit, and in use
- Endpoints are secured and hardened using trusted platform modules and endpoint detection and response tools:
  - Modern solutions such as Palo Alto Cortex XDR are considered next-generation endpoint detection and host-based intrusion detection and protection

HARDENING TECHNIQUES

Other hardening best practices involve the following tasks:

- Disabling all auto-configure features
- Replacing all default passwords with strong credentials
- Implementing strict password policies or passwordless solutions
- Removing all unnecessary and unauthorized software (personal cloud storage, type 2 hypervisors, exploit kits, etc.)

Architecture and Infrastructure Concepts

Objectives

- Learn about architectural considerations
- Explore cloud computing
- Define Infrastructure as Code, serverless technologies, containers, and microservices
- Examine network infrastructures including centralized vs. decentralized design
- Discover virtualization
- Learn basics of ICS and SCADA
- Define the Internet of Things

RESILIENCE

- Resilience is the ability of a system to continue to:
  - operate under adverse conditions or stress, even if in a degraded or debilitated state
  - maintain essential operational capabilities
  - recover to an effective operational posture in a time frame consistent with mission needs
- Resilience is the ability of a workload to recover from infrastructure or service disruptions
- Administrators should be able to dynamically obtain computing resources to meet demand and mitigate disruptions
  - Disruptions can be misconfigurations or transient network issues

HIGH AVAILABILITY

- Availability is an aspect of resiliency expressed as a percentage of planned and unplanned downtime over an annual period (99.5, 99.9, 99.95, 99.99)
- High availability entails a system, component, or application operating at high capacity, continuously, without intervention, for a defined period of time
- A highly-available infrastructure is designed to deliver quality performance and handle different loads and failures with minimal or zero downtime

HIGH AVAILABILITY

- Reliability is a measure of percentage uptime, considering the downtime due only to faults, whereas Availability is a measure of the percentage uptime, considering the downtime due to faults and other causes such as planned maintenance
  - For two different systems, it is possible for one system to be more reliable but less available than the other

AVAILABILITY VS. DURABILITY

- Availability has historically been achieved through hardware redundancy so that if any component fails, access to data will remain
- Durability, on the other hand, refers to long-term data protection (i.e., the stored data does not suffer from bit rot, degradation, or other corruption)
  - Durability is concerned with data redundancy so that data is never lost or compromised
- **Example**: AWS S3 and Google Cloud are designed for 99.999999999% (11 nines) durability per object and 99.99% availability per year

OTHER ARCHITECTURAL CONSIDERATIONS

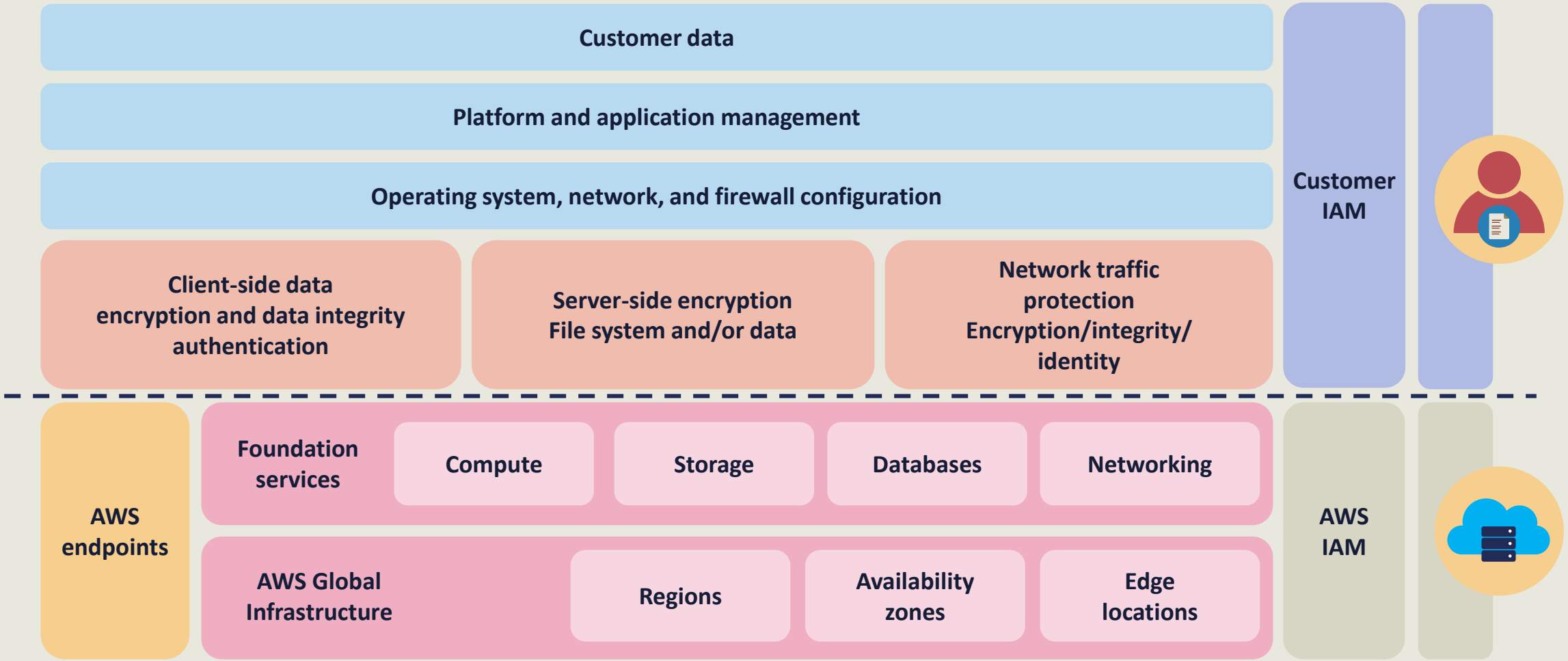
- Cost
- Responsiveness
  - Low latency and performance
- Scalability
  - Scaling out adds physical and virtual instances
  - Scaling up adds compute processor, memory) capacity
- Ease of deployment
  - Infrastructure as Code (IaC)
  - Patching automation
- Risk transference
  - Cloud, insurance, shared disaster sites
- Power

CLOUD COMPUTING: INFRASTRUCTURE AS A SERVICE (IAAS) ACCORDING TO NIST

Infrastructure as a Service is where the "capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, including operating systems and applications.

The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."

INFRASTRUCTURE AS A SERVICE AT AWS



CLOUD COMPUTING: PLATFORM AS A SERVICE (PAAS) ACCORDING TO NIST

Platform as a Service is the when the "capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations."

PLATFORM AS A SERVICE

Development and software development kit (SDK) platforms for Java, PHP, Python, etc.

Container services for Docker and Kubernetes

Managed and fully managed relational and document databases

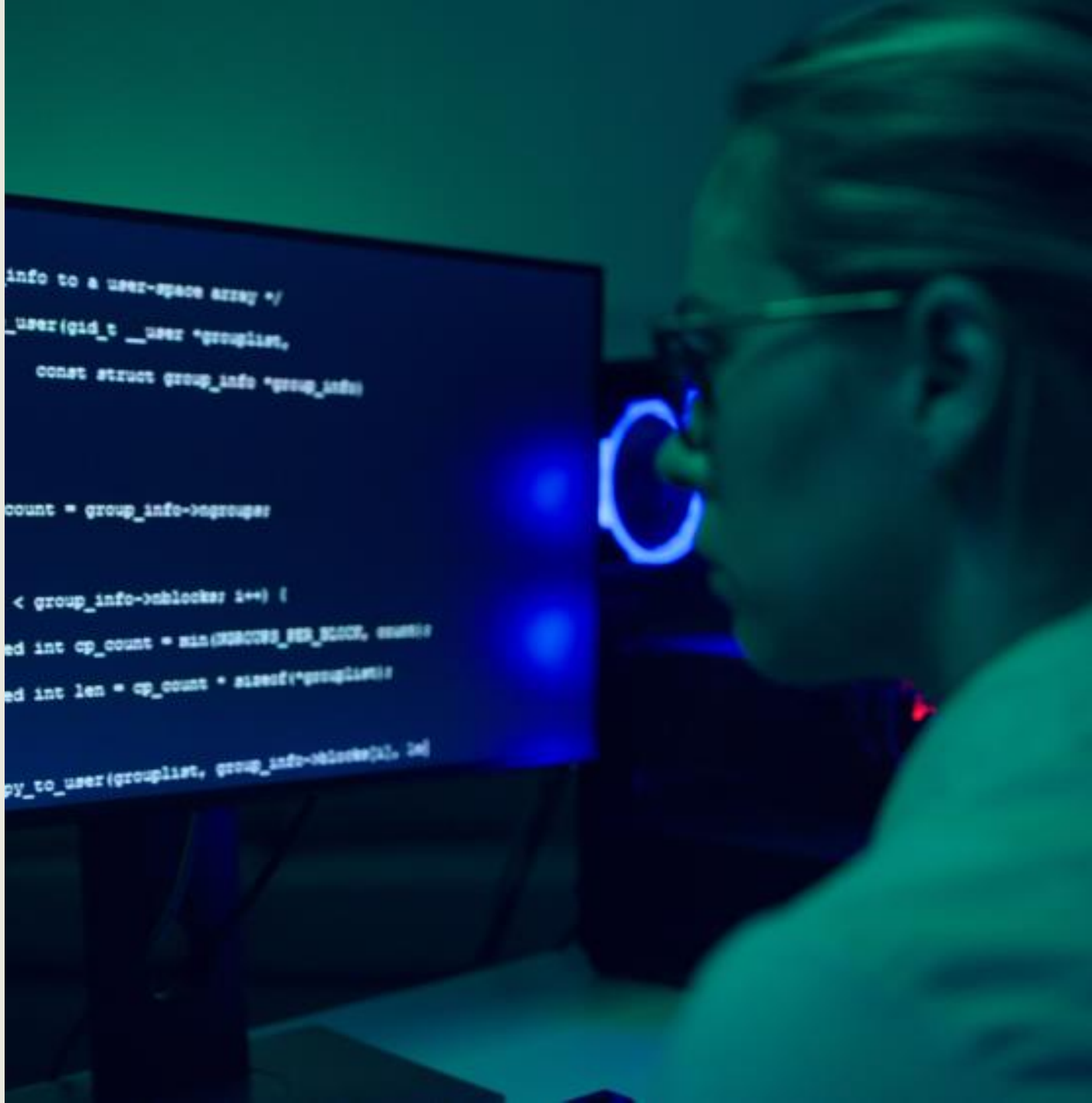
Managed security and threat modeling services

Single sign-on (SSO), machine learning (ML), artificial intelligence (AI), Internet of Things (IoT), blockchain, media services

CLOUD COMPUTING: SOFTWARE AS A SERVICE (SAAS) ACCORDING TO NIST

Software as a Service is when the "capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

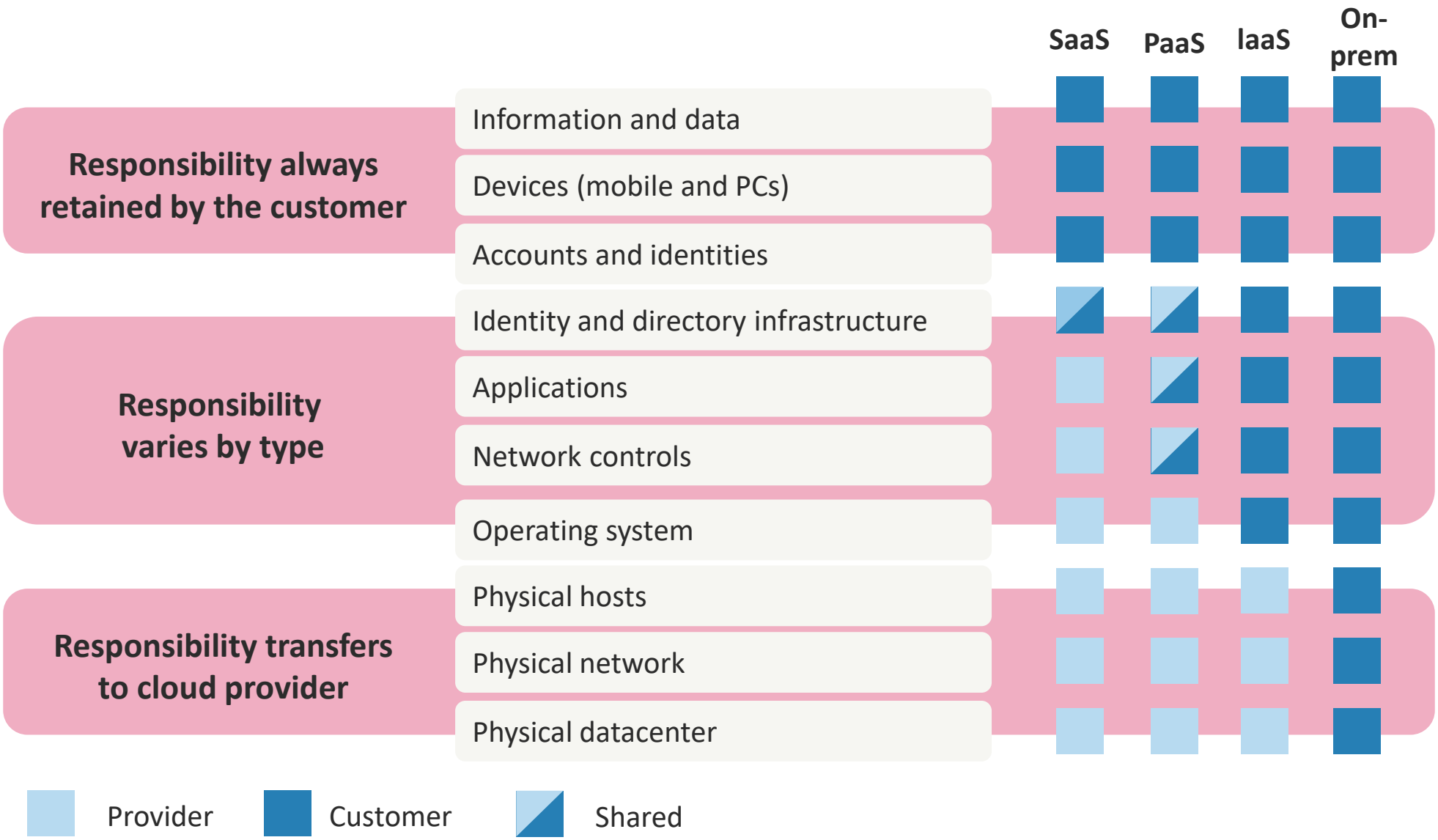
The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."



SOFTWARE AS A SERVICE OFFERINGS

- Customer relationship management (CRM)
- Enterprise resource management (ERM)
- Human resources and workplace tools
- Finance, sales, and marketing services
- Payroll services
- Email, collaboration, and cloud storage
- Help desk and service desk
- Virtual call center
- Business analytics

AZURE CLOUD RESPONSIBILITY MATRIX



CLOUD DEPLOYMENT MODELS

Public Cloud

The organization runs an initiative (DevOps, DB) entirely at the cloud service provider (CSP) or has public customers for its deployed resources (web, E-commerce)

Private Cloud

A cloud scenario that supports a single organization and its internal customers either in the CSP or on-premises

Community Cloud

A consortium that uses a cloud environment for a particular use case (i.e., gaming community, metaverse, financial, healthcare, etc.)

Hybrid Cloud

A combination of the other three options or an edge computing environment – often bursting up during peak seasons

HYBRID CLOUD CONSIDERATIONS

- Hybrid cloud can also be a method for connecting infrastructure and applications between cloud-based resources and other resources that are not placed in the cloud
- The most common type of hybrid deployment is between the provider's public cloud and a standing on-premises enterprise private cloud
- Can be used to migrate, expand, or grow an organization's infrastructure into a cloud solution while linking internal systems to cloud resources
- Often used by organizations to "burst up" to the cloud during peak demand times or special situations

ON-PREMISES (PRIVATE) CLOUD

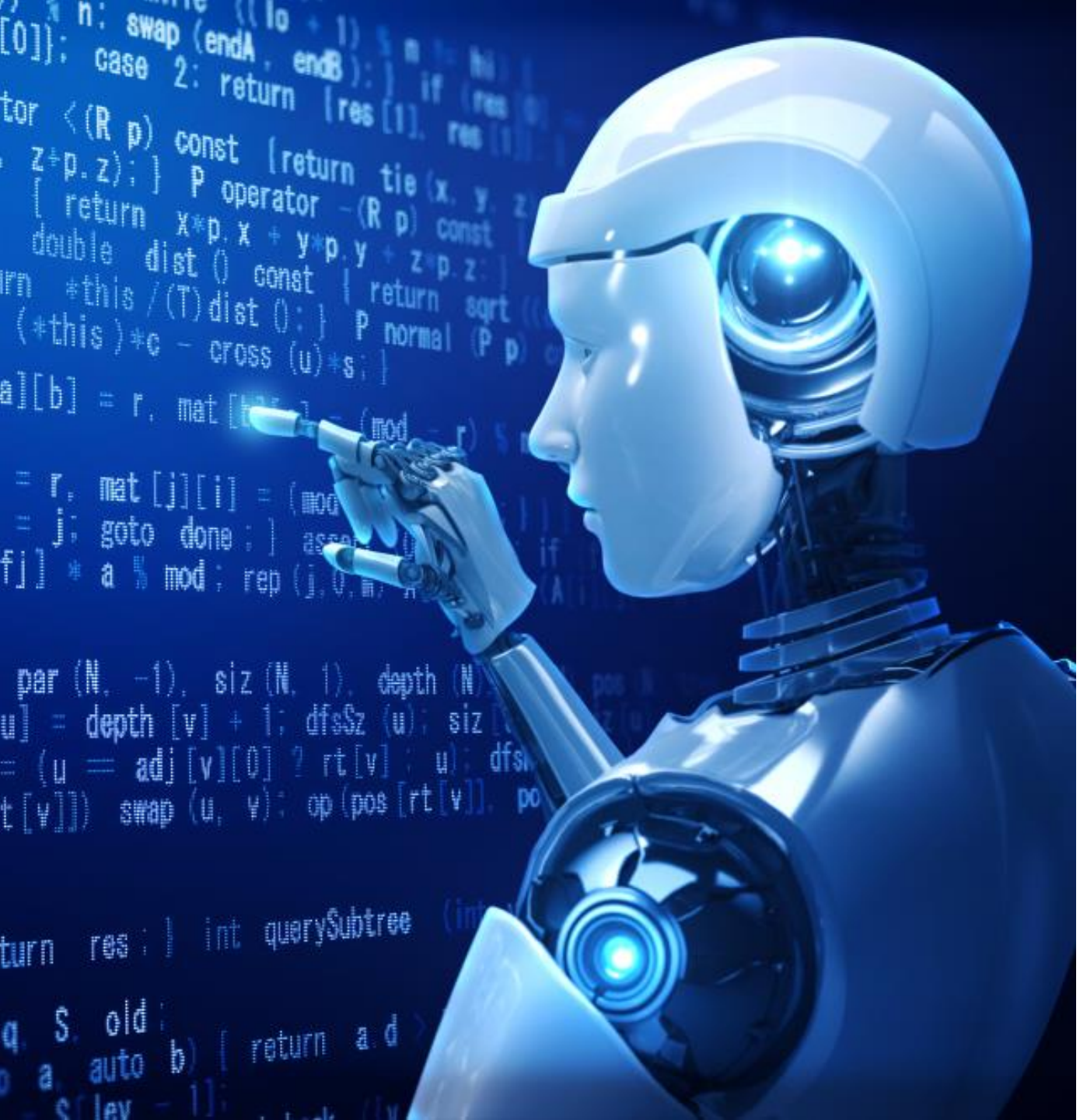
- Involves installing resources on-premises using virtualization and resource management tools, often called private cloud
- On-premises deployment does not provide many of the benefits of cloud computing but is often chosen for its ability to provide dedicated resources
- In most scenarios, this deployment model is the same as legacy IT infrastructure while using application management and virtualization technologies to try and increase resource utilization

THIRD-PARTY CLOUD VENDORS

- **Brokers** – local municipal partners, edge location, reciprocal partners
- **Auditors** – often CSA or SOC certified internal and external auditors
- **MSSP** – managed security service providers such as Fortinet offering cloud-based services (NGFW, NGIPS, EDR, visibility, SIEM+SOAR)
- **CASB** – assisting with SaaS providers for compliance, data loss prevention, and single sign-on
- **Direct Connection** – partners like Direct Connect, Interconnect, and ExpressRoute

INFRASTRUCTURE AS CODE

- IaC is the provisioning and operations of infrastructure using code instead of by manual processes
- Configuration files are created that contain the infrastructure specifications, which makes it easier to edit and distribute configurations
- It also ensures that admins provision the same environment every time
- IaC assists configuration management and helps to avoid undocumented, ad-hoc configuration changes

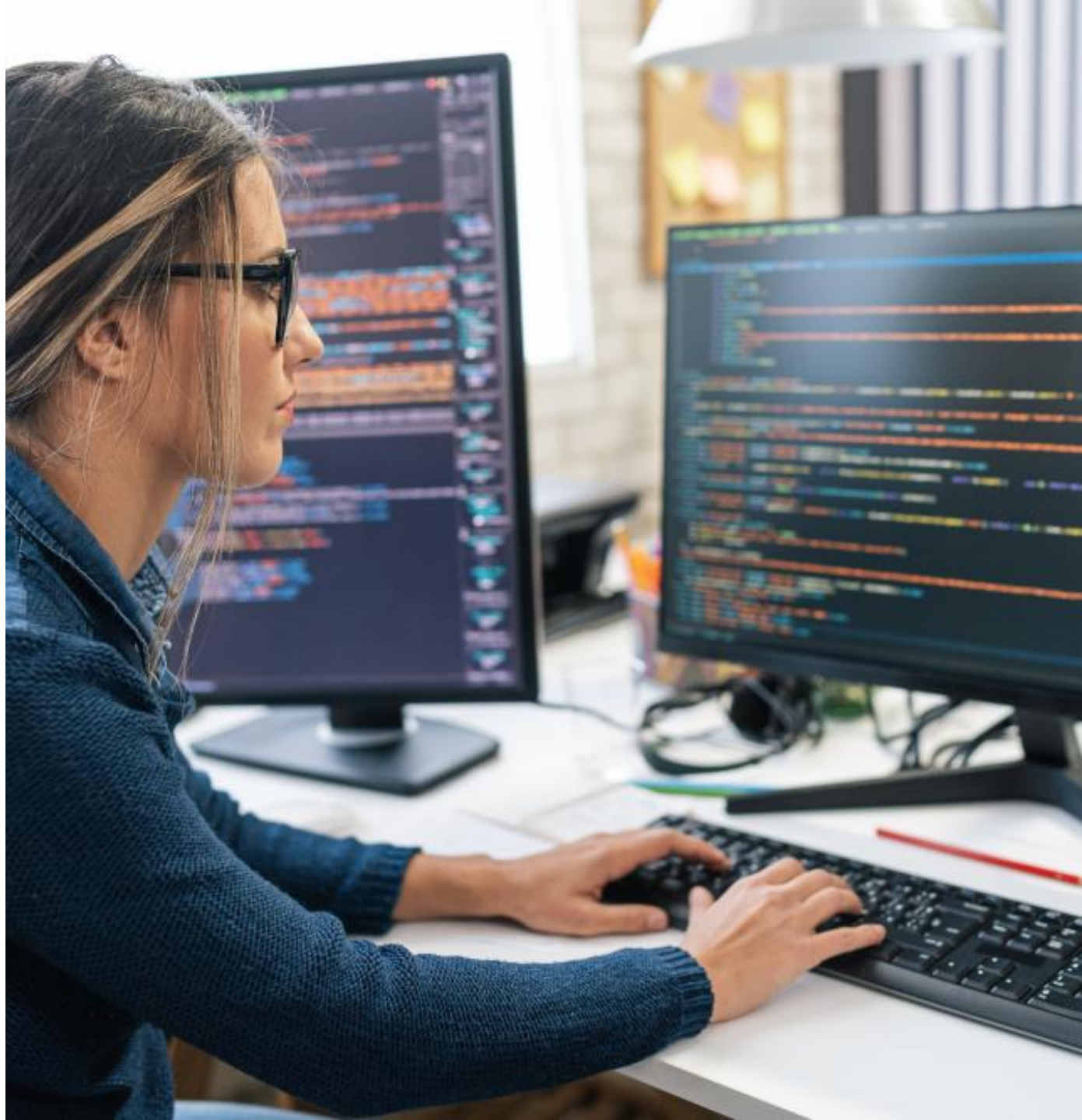


INFRASTRUCTURE AS CODE

- Version control is also an important part of IaC, and all configuration files should be under source control just like any other software source code files
- Deploying with IAC also means that architects can divide their infrastructure into modular components that can then be combined in different ways using automation and orchestration
- This is referred to a generating a "single source of truth" or "terraforming the environment"

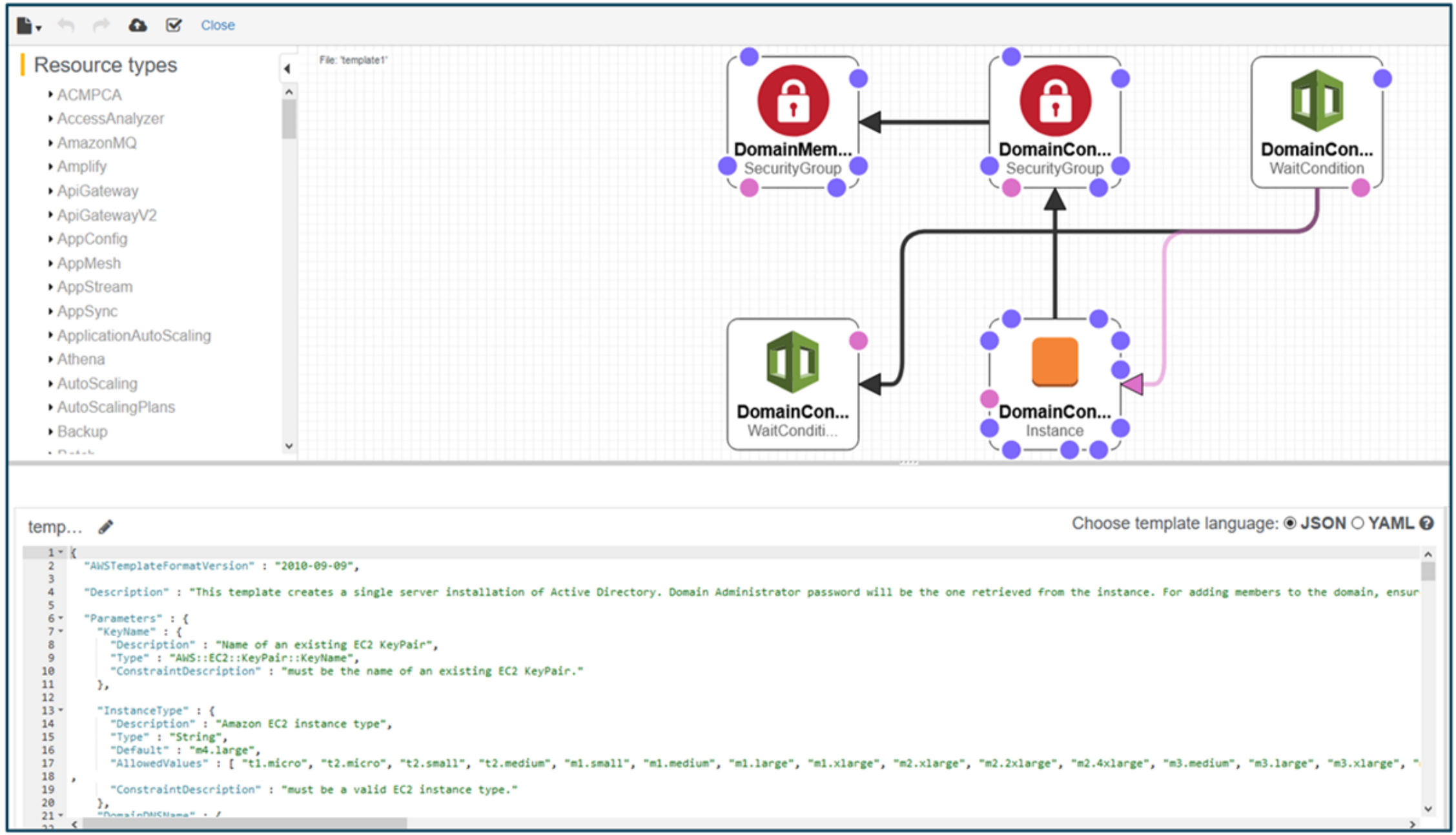
INFRASTRUCTURE AS CODE (IaC)

- Automating with IaC also means that developers do not need to manually provision and manage servers, operating systems, containers, or microservices each time they develop or deploy an application
- Codifying the infrastructure offers a template to follow for provisioning
- An automation tool, such as Red Hat® Ansible® Automation Platform is a common IaC solution



INFRASTRUCTURE AS CODE

- Cloud services such as AWS CloudFormation empower customers to model, deploy, and manage AWS and third-party resources by handling the Infrastructure as Code
- The cloud template language comes in either JSON or YAML formats
- Customers can automate, test, and deploy infrastructure templates with continuous integration and delivery (CI/CD) automations
- Templates can also be used to set up lab environments for learning the cloud


Close
Resource types
ACMPCA
AccessAnalyzer
AmazonMQ
Amplify
ApiGateway
ApiGatewayV2
AppConfig
AppMesh
AppStream
AppSync
ApplicationAutoScaling
Athena
AutoScaling
AutoScalingPlans
Backup
File: 'template1'
DomainMem...
SecurityGroup
DomainCon...
SecurityGroup
DomainCon...
WaitCondition
DomainCon...
WaitConditi...
DomainCon...
Instance
temp...
Choose template language: JSON YAML
{
"AWSTemplateFormatVersion" : "2010-09-09",
"Description" : "This template creates a single server installation of Active Directory. Domain Administrator password will be the one retrieved from the instance. For adding members to the domain, ensur
"Parameters" : {
"KeyName" : {
"Description" : "Name of an existing EC2 KeyPair",
"Type" : "AWS::EC2::KeyPair::KeyName",
"ConstraintDescription" : "must be the name of an existing EC2 KeyPair."
},
"InstanceType" : {
"Description" : "Amazon EC2 instance type",
"Type" : "String",
"Default" : "m4.large",
"AllowedValues" : ["t1.micro", "t2.micro", "t2.small", "t2.medium", "m1.small", "m1.medium", "m1.large", "m1.xlarge", "m2.xlarge", "m2.2xlarge", "m2.4xlarge", "m3.medium", "m3.large", "m3.xlarge",
,
"ConstraintDescription" : "must be a valid EC2 instance type."
},

SERVERLESS TECHNOLOGIES

- Modern serverless solutions leverage modern cloud infrastructures to emulate the network operating system (NOS) environment without the need for a Windows or Linux-based servers
- These are technologies for running code, managing data, and integrating applications, all without managing servers
- They feature automatic scaling, built-in high availability, and a pay-for-use billing model to increase agility and optimize costs
- Functions, containers, and databases are common serverless solutions

CASE STUDY: AWS FARGATE SERVERLESS CONTAINERS

Without Fargate

Build your container image

Define and deploy the EC2 instances

Provision and manage compute and memory resources

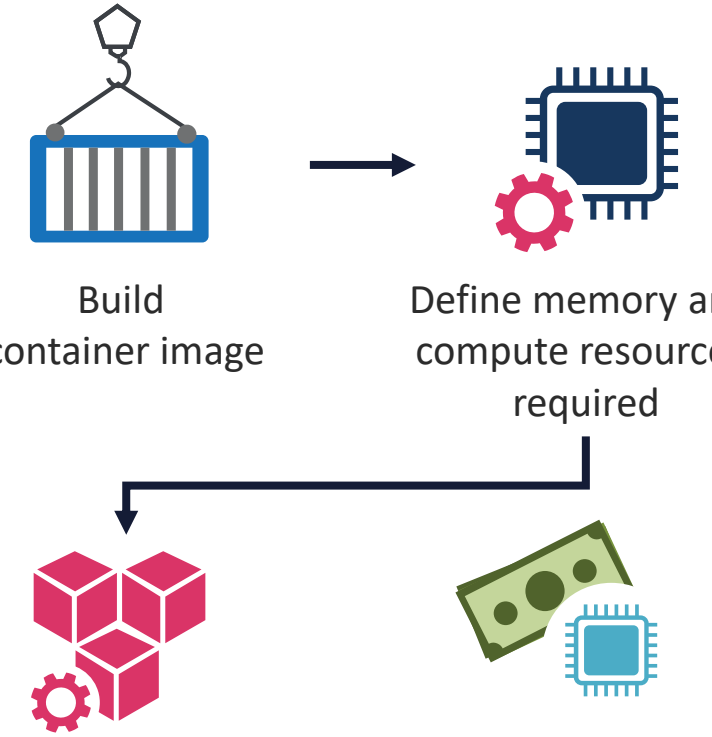
Isolate application in separate virtual machines (VMs)

Define and deploy the EC2 instances

Pay for EC2 instances

AWS Fargate

With Fargate



Build container image

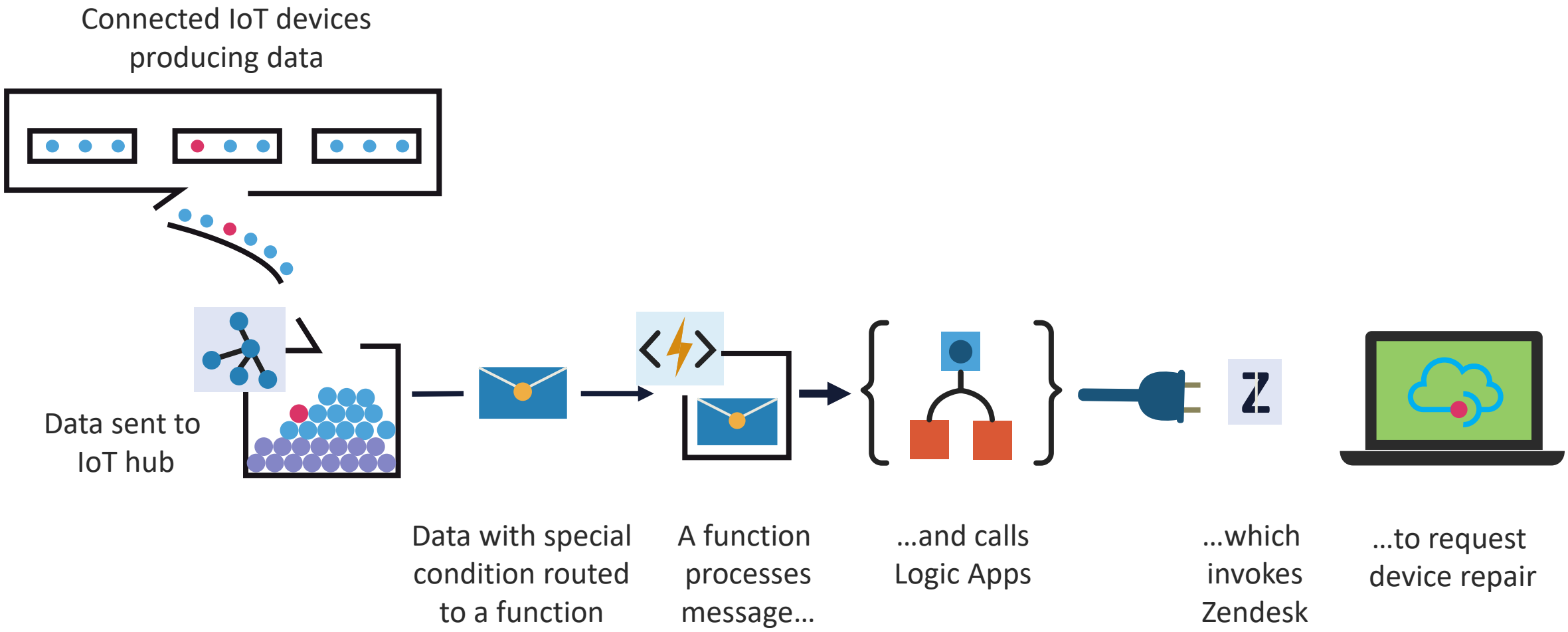
Define memory and compute resources required

Run and mange applications

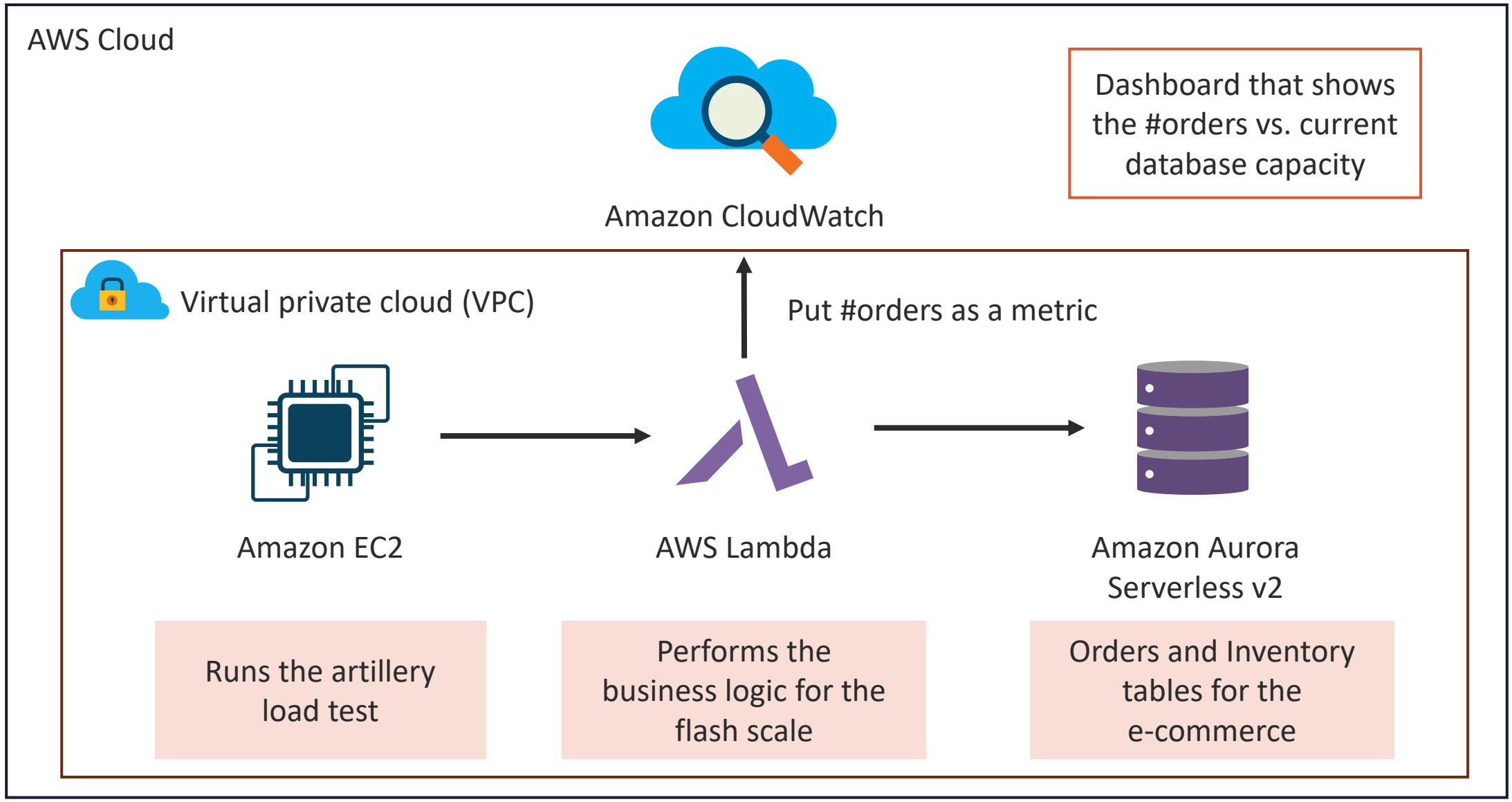
Pay for requested compute resources when used

Applications isolation by design

CASE STUDY: AZURE SERVERLESS FUNCTIONS



CASE STUDY: AWS SERVERLESS DATABASE WITH AURORA



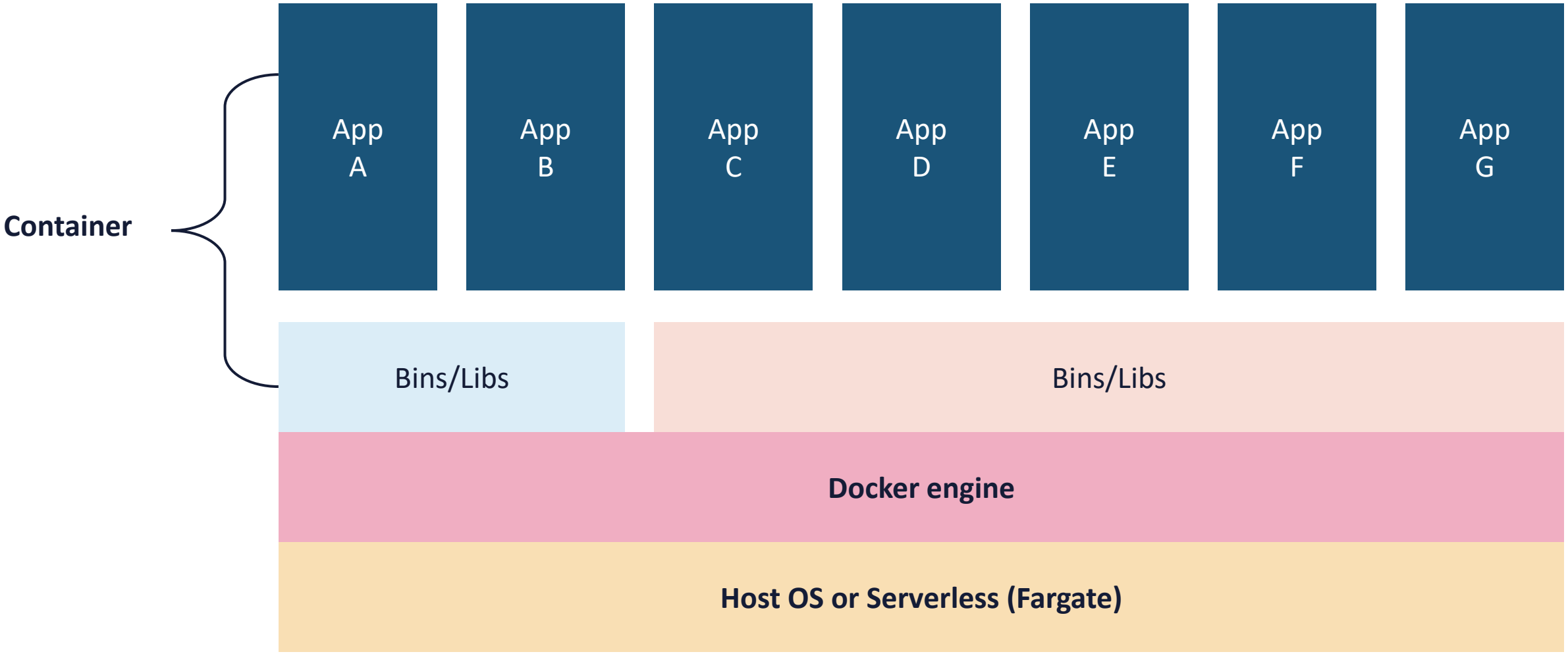
CONTAINERS

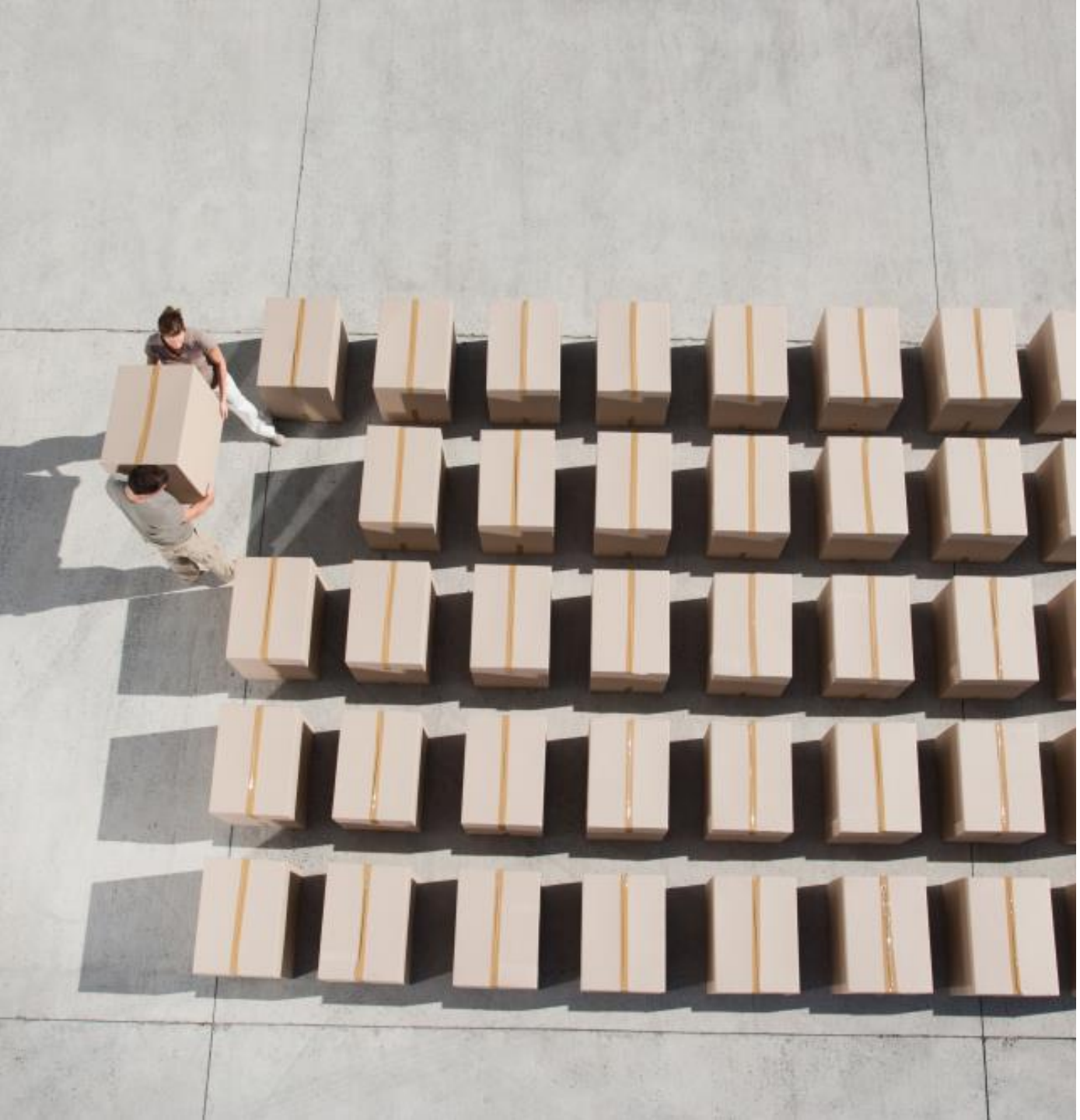
- A container is a discrete environment within an operating system (or a serverless architecture) where one or more applications can run and that is typically assigned all the resources and dependencies needed to function
- It is a modular and portable environment that includes the application binaries, software dependencies, and hardware requirements wrapped up into an independent, self-contained unit

CONTAINERS

- Containers are commonly used for processes and workflows in which there are important requirements for security, reliability, and scalability
- All cloud providers offer managed container development, automation, and orchestration services
- Containers can be server-based or serverless (AWS Fargate)

CONTAINERS

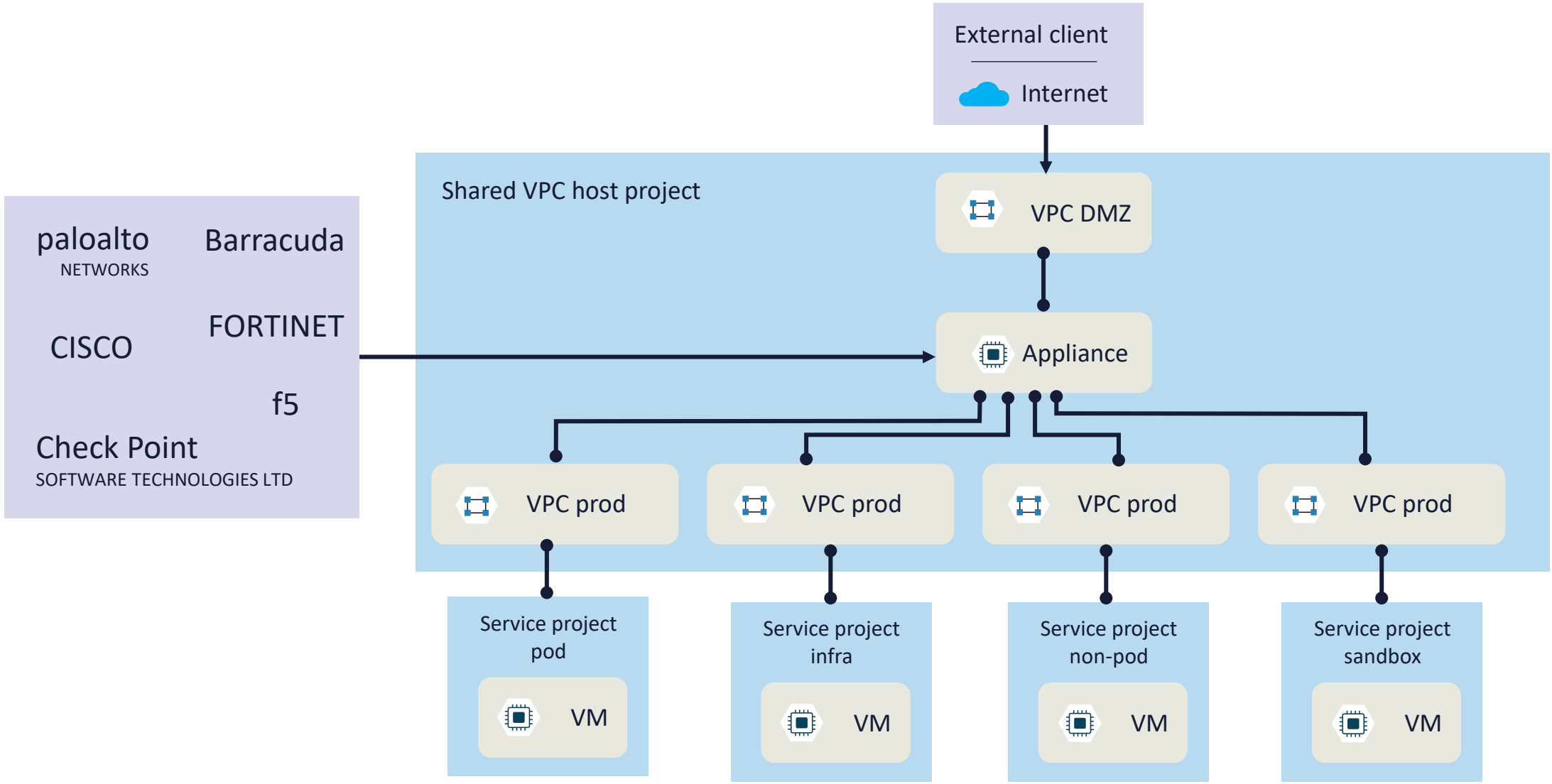

App A
App B
App C
App D
App E
App F
App G
Container
Bins/Libs
Bins/Libs
Docker engine
Host OS or Serverless (Fargate)



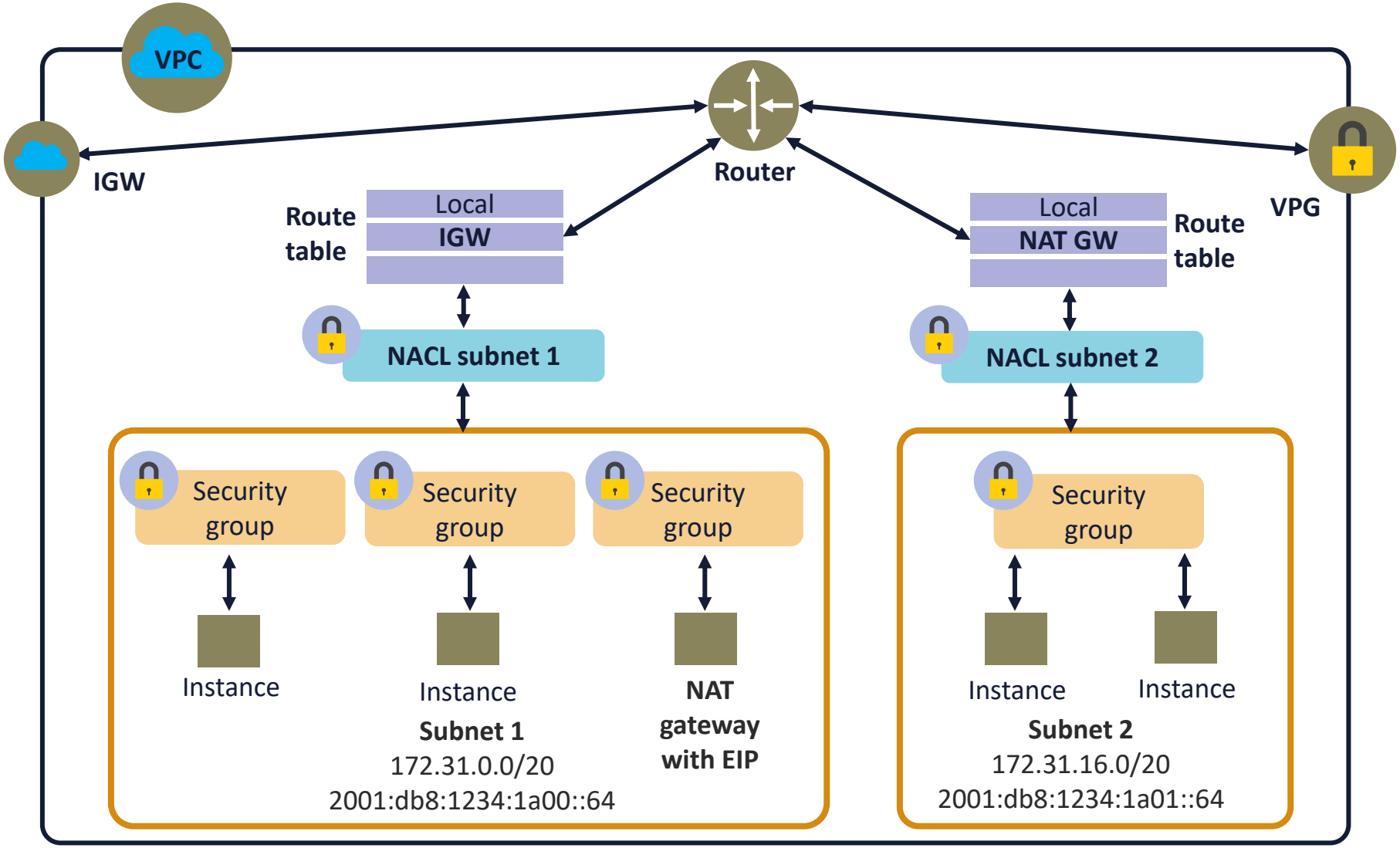
MICROSERVICES

- Microservices are specific service-oriented application components made up of small independent services that communicate over well-defined APIs for notification and process queueing
- They make applications and apps faster to develop and easier to scale by small, self-contained teams of developers
  - Microservices are about the design of software
  - Containers are about packaging software for deployment

CLOUD CUSTOMER NETWORK INFRASTRUCTURE: GOOGLE CLOUD PLATFORM (GCP)

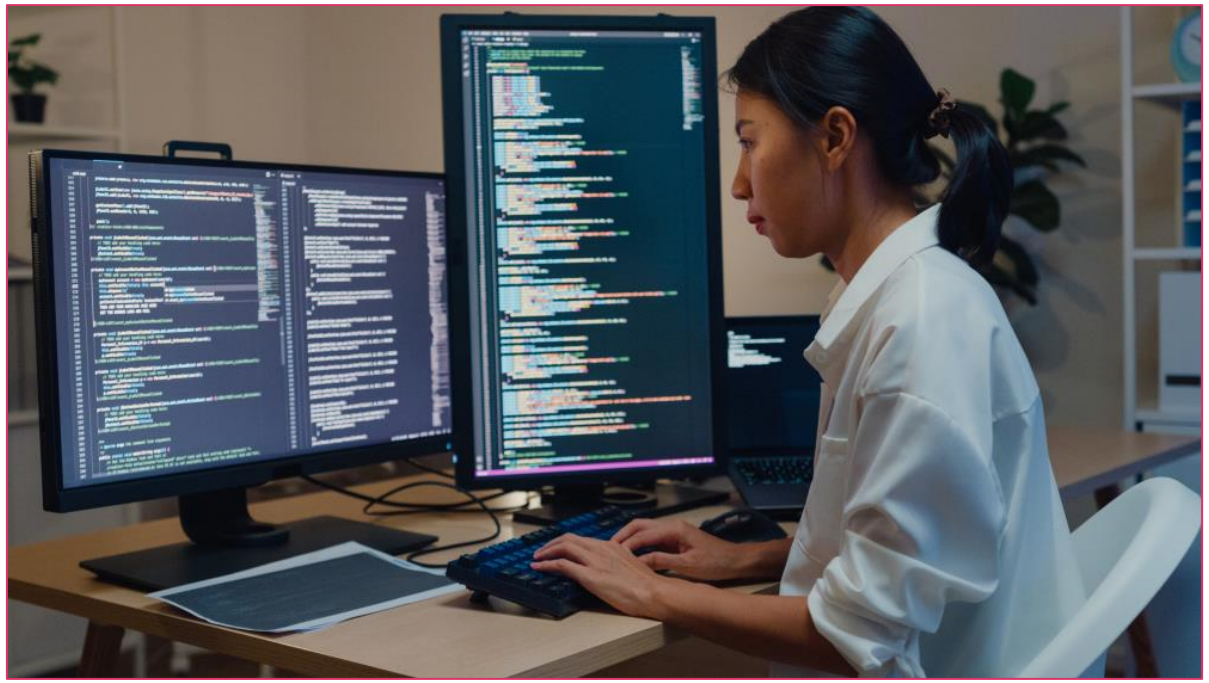


CLOUD CUSTOMER NETWORK INFRASTRUCTURE: AWS



SOFTWARE-DEFINED NETWORKING (SDN)

- Software-defined networking is a framework intended to make a network more flexible and easier to manage, especially with disparate hardware and graphical overlays
- SDN centralizes management by abstracting the control plane from the data forwarding function in the different networking devices

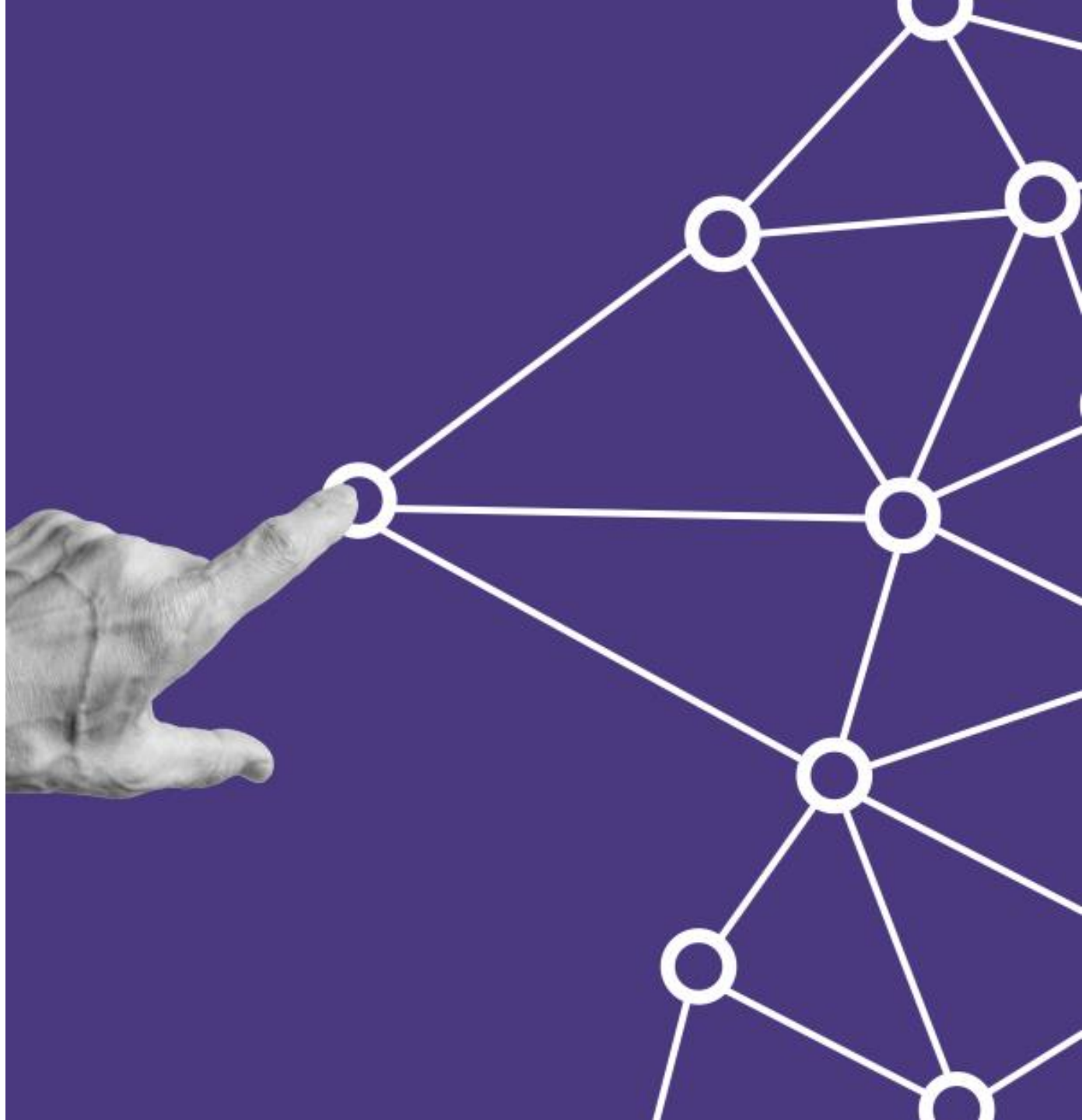


SDN

- An SDN architecture offers a centralized, programmable network consisting of the following:
  - The controller is the essential element of an SDN architecture that assists centralized management and control, automation, and policy enforcement across physical and virtual environments
  - Southbound application programming interfaces (APIs) relay information between the controller and the individual network devices
  - Northbound APIs transmit information between the controller and the applications and policy engines, to which an SDN looks like a single logical network device

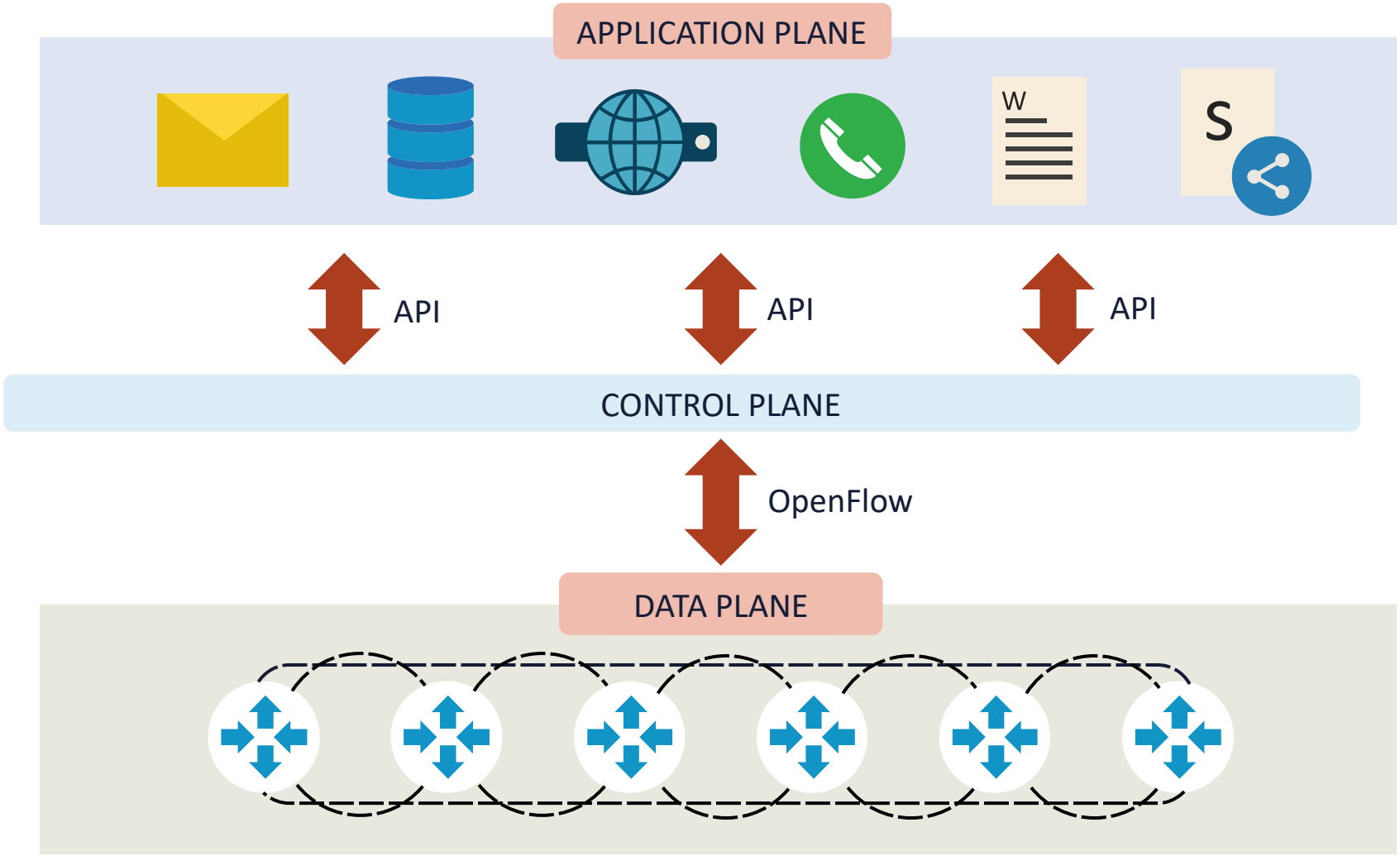
SDN CHARACTERISTICS

- Directly programmable
- Agile
- Centrally managed
- Programmatically configured
- Open standards-based and vendor-neutral



SOFTWARE-DEFINED NETWORKING

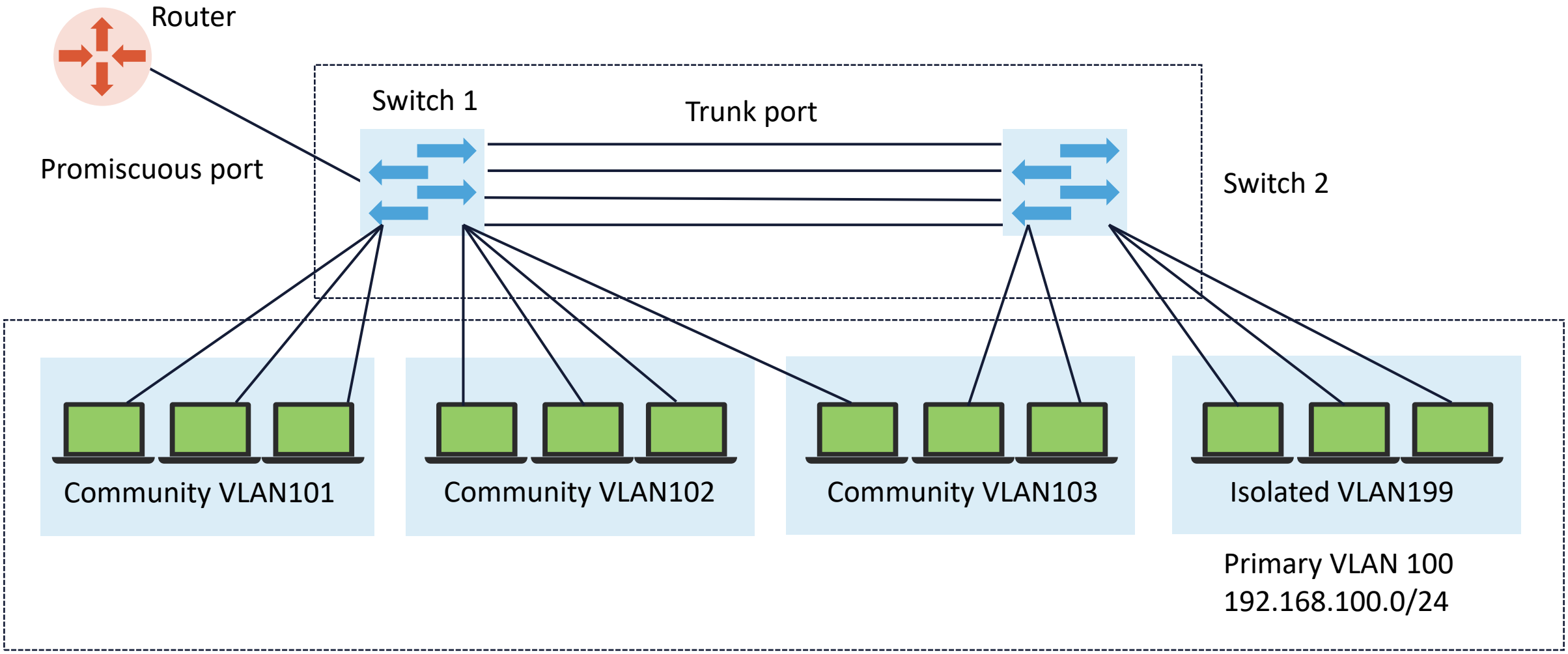
SDN



OTHER NETWORK INFRASTRUCTURE CONCEPTS

- Physical isolation
- Air-gapped
- Logical segmentation

LOGICAL SEGMENTATION



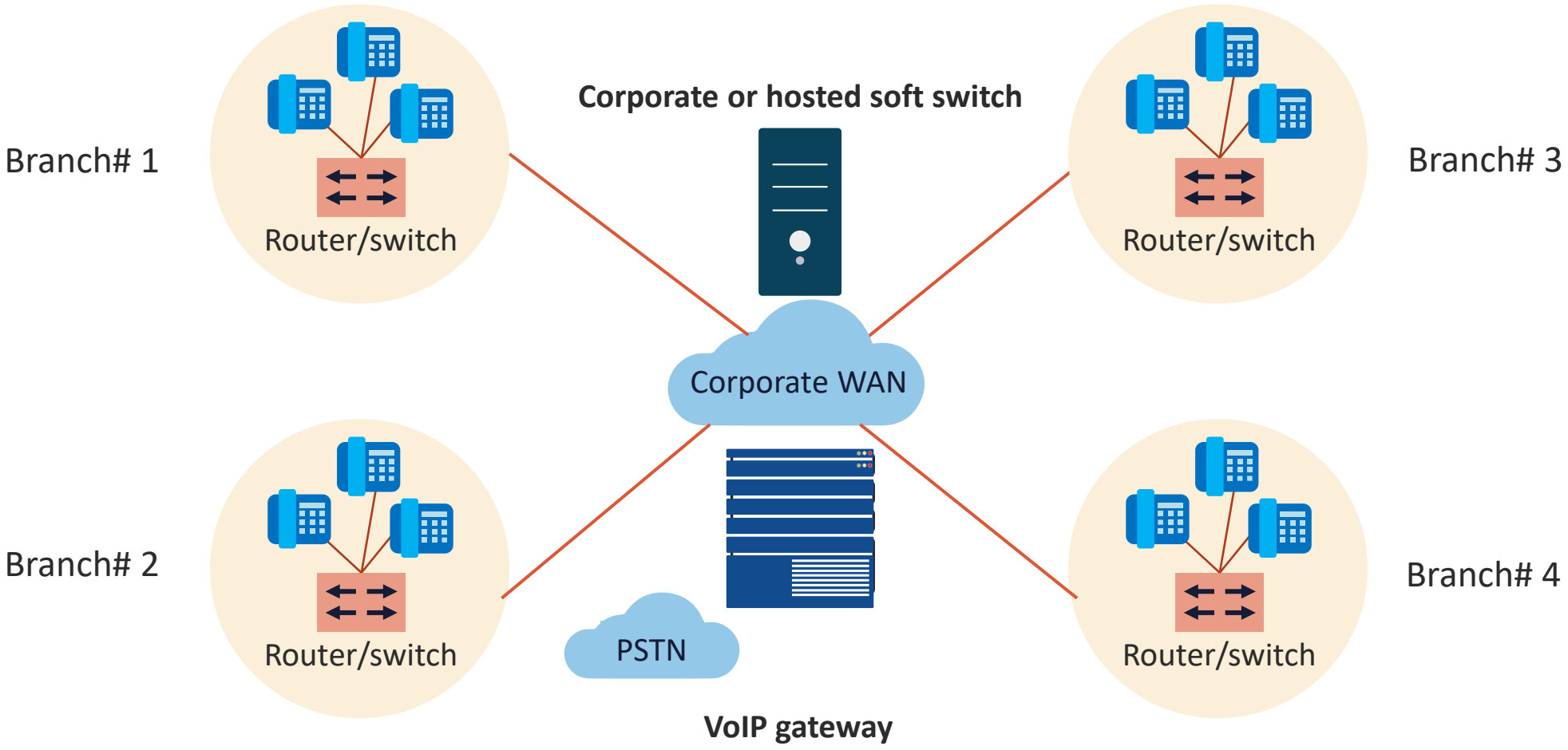
CENTRALIZED DESIGN

- Centralized systems typically deploy a client/server architecture where one or more client node communicates directly (or through a proxy) with a central server either physically or logically
- This is the most common type of system in many organizations where a client sends a request to a corporate intranet and receives a response

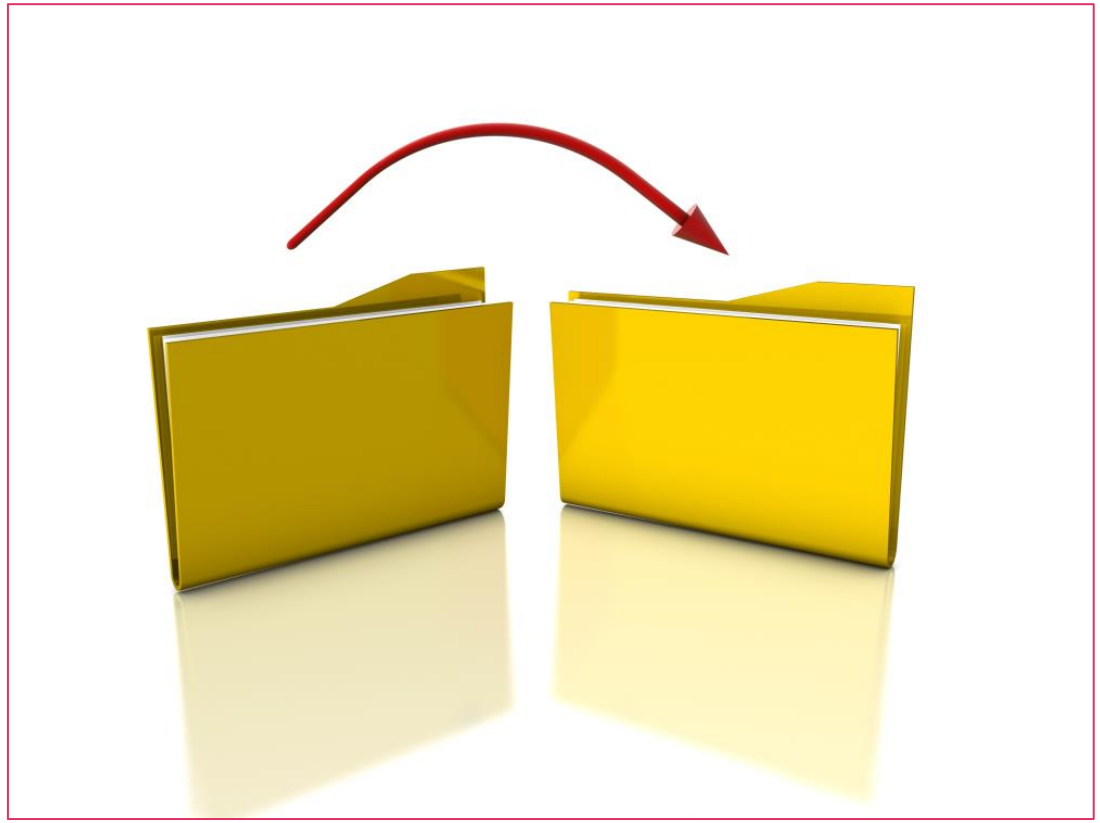
COMMON CENTRALIZED ATTRIBUTES

- Presence of a global clock: all client nodes sync up with the main clock of the central node
- There is one highly available central node that coordinates all the other nodes in the system
- Central node failure causes the entire system to fail because if the server is down, no other entity is there to send/receive responses/requests
- Centralized servers can, in many cases, leverage a hierarchy of intermediate down-level servers

CENTRALIZED WIDE AREA NETWORK (WAN)



DECENTRALIZED DESIGN

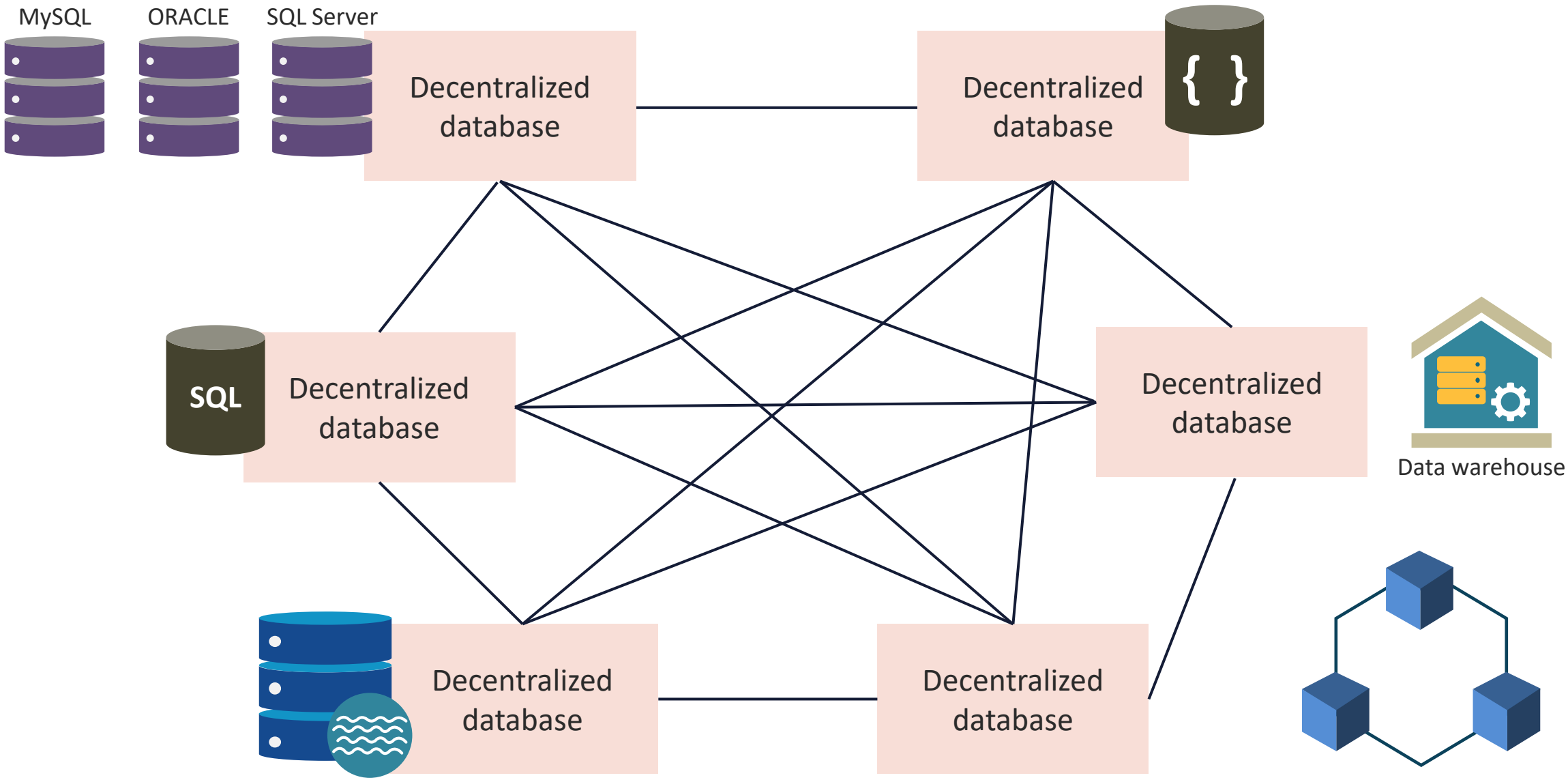


- In a decentralized system, every node makes its own decision
- The final behavior of the system is the aggregate of the decisions of each individual node or host
- There is no single entity that receives and responds to the request
- The requests are broadcasted or multicasted to the decentralized architecture

COMMON DECENTRALIZED ATTRIBUTES

- There is no global clock as each node is independent of each other, and therefore have different clocks that they run and follow
- Decentralized systems have multiple or shifting nodes and more than one unit which can listen for connections from other nodes
- One central node failure causes a part of the system to fail; not the whole system

DECENTRALIZED DATABASE NETWORK



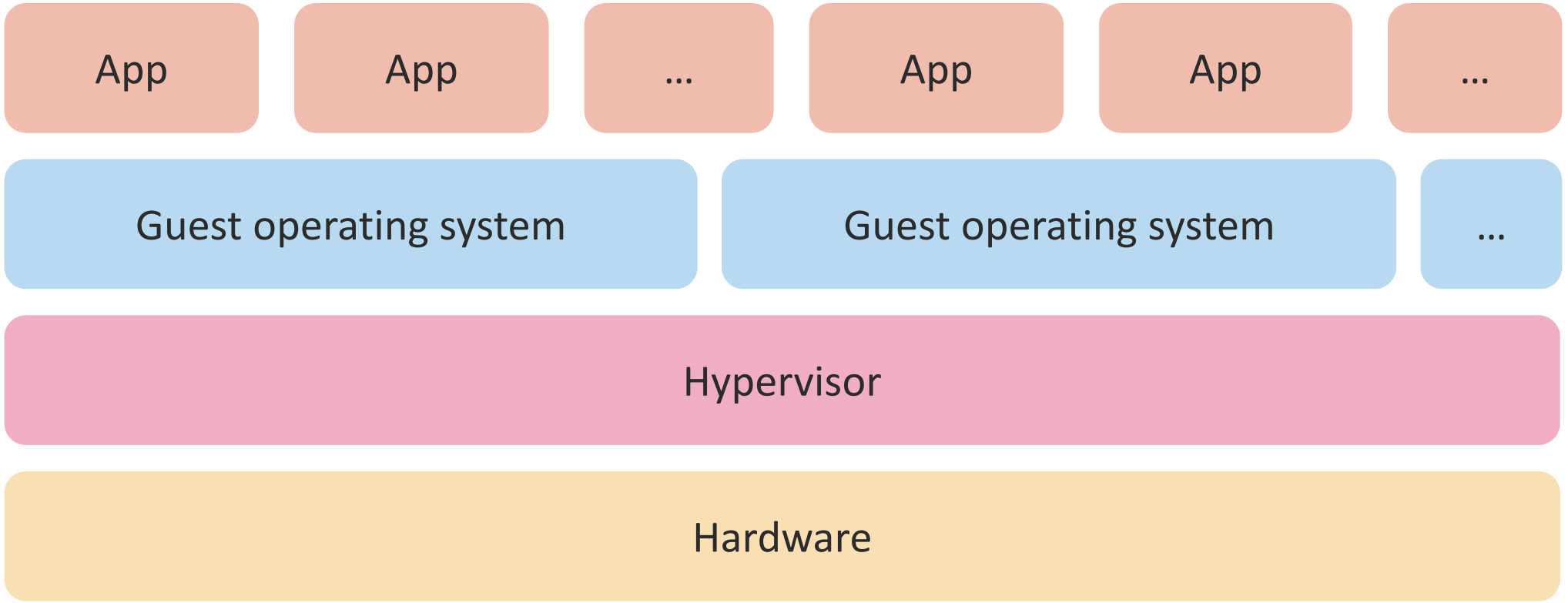
VIRTUALIZATION

- Virtualization is the process of running a virtual instance of a computer system in a layer abstracted from the underlying hardware server
- It most often refers to running multiple operating systems on a computer system simultaneously
- To the applications running on top of the virtualized machine, it can seem as if they are on their own dedicated operating system with libraries, dynamic link libraries (DLLs), and associated programs

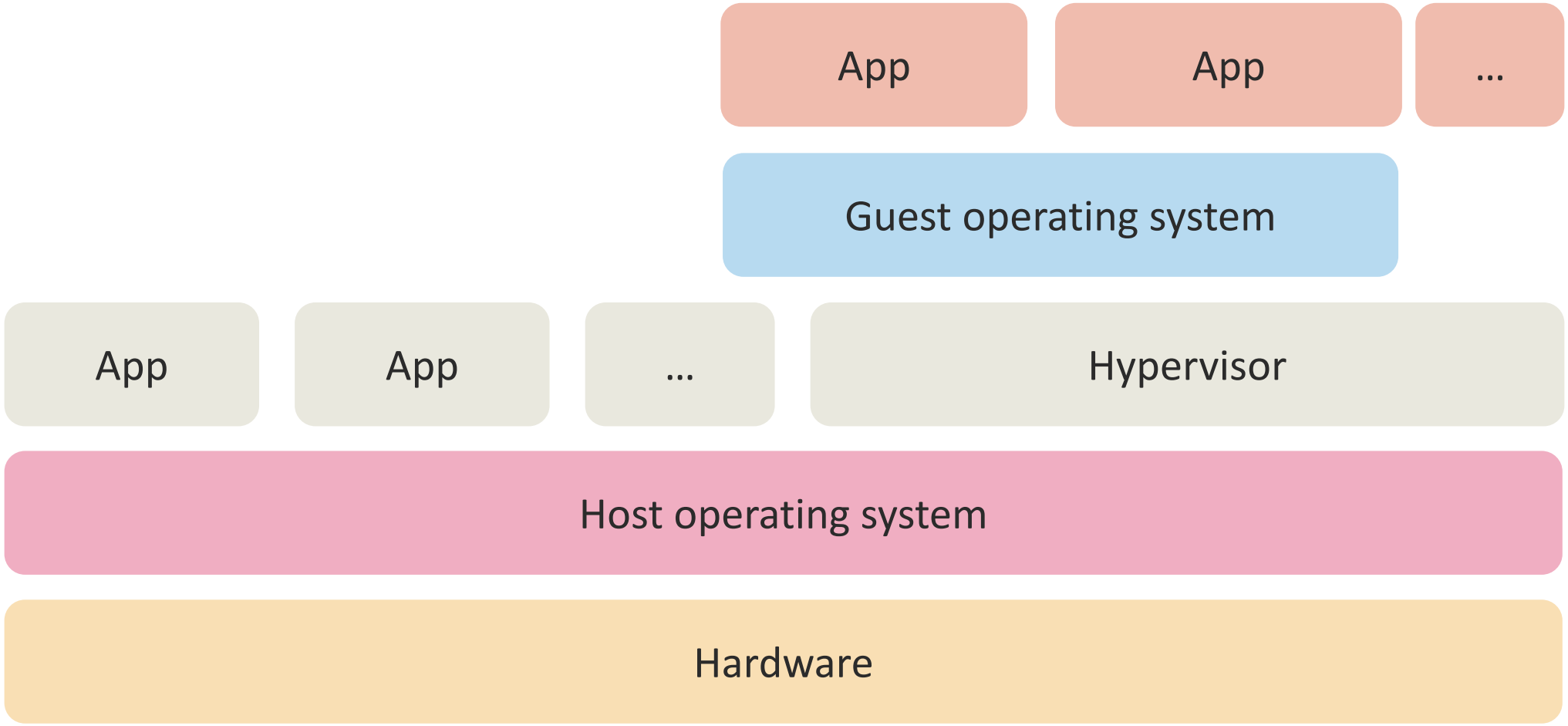
HYPERVISORS

- These are the virtual machine manager system and software that run one or more virtual machines
- It controls the interaction between the VMs and the underlying hardware
- Type I – bare metal or native
  - Runs directly on the underlying hardware
  - XenServer, KVM, Hyper-V, ESXi
- Type II – hosted
  - Runs on the OS installed on the hardware
  - Oracle VirtualBox 6, VMWare Player/Workstation

TYPE 1 HYPERVISORS



TYPE 2 HYPERVISORS



SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

- Supervisory Control and Data Acquisition (SCADA) systems represent the software used to collect and send data to throughout facility systems and to cloud services
- Programmable logic controllers (PLCs) and other embedded systems are common hardware components
- Systems that are not air-gapped introduce various threats

INDUSTRIAL CONTROL SYSTEMS (ICS)

- Industrial control system (ICS) is a combined term that represents varied forms of control systems and related instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial and mechanical processes
- Each ICS typically functions differently and is built to electronically manage tasks efficiently
- Modern devices and protocols used in an ICS are used in nearly every industrial sector and critical infrastructure

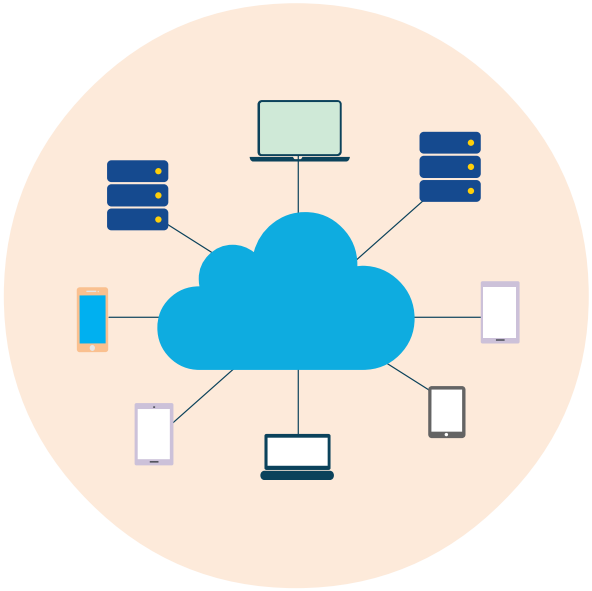
SCADA AND ICS SYSTEMS

- Facility and manufacturing control and management systems
- Water management systems
- Electric/nuclear power grid, solar, and wind farms
- Traffic signals and mass transit systems
- Environmental and manufacturing control systems

INTERNET OF THINGS

- The term IoT refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves
- With the advent of inexpensive computer chips and high bandwidth networking, there are now billions of devices connected to the Internet using IPv4 and IPv6
- Everyday devices like toothbrushes, vacuums, cars, and machines can use sensors to collect data and respond intelligently to users

INTERNET OF THINGS



- Mobile devices
- Cameras
- Farm and ranch equipment
- Sensors
- Smart appliances
- Facility automation
- Medical devices and systems
- Vehicles and aircraft (drones)
- Smart meters
- Embedded devices and real-time operating systems (RTOS)