SRI KRISHNA COLLEGE OF ENGINEERING AND TECHNOLOGY

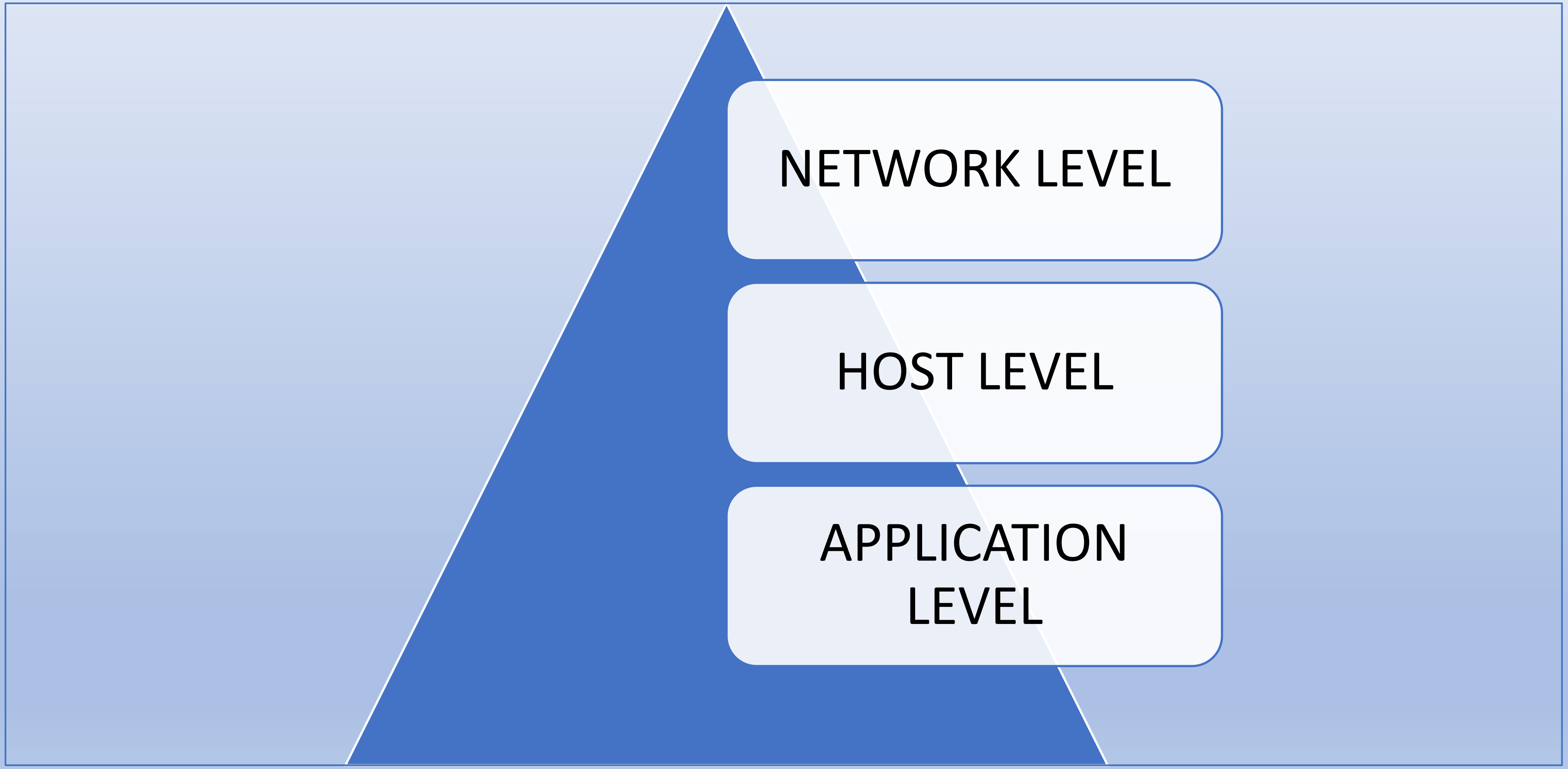
An Autonomous Institution | Approved by AICTE | Affiliated to Anna University | Accredited by NAAC with A++ Grade
Kuniamuthur, Coimbatore – 641008
Phone : (0422)-2678001 (7 Lines) | Email : info@skcet.ac.in | Website : www.skcet.ac.in

Infrastructure Security

Infrastructure Security

- Infrastructure security in cloud computing refers to the practices, technologies, and policies used to protect the foundational components of a cloud environment at the network, host, and application levels.
- Information security practitioners commonly use this approach; therefore, it is readily familiar to them.
- We discuss this infrastructure security in the context of SPI service delivery models (SaaS, PaaS, and IaaS).

Infrastructure Security



NETWORK LEVEL

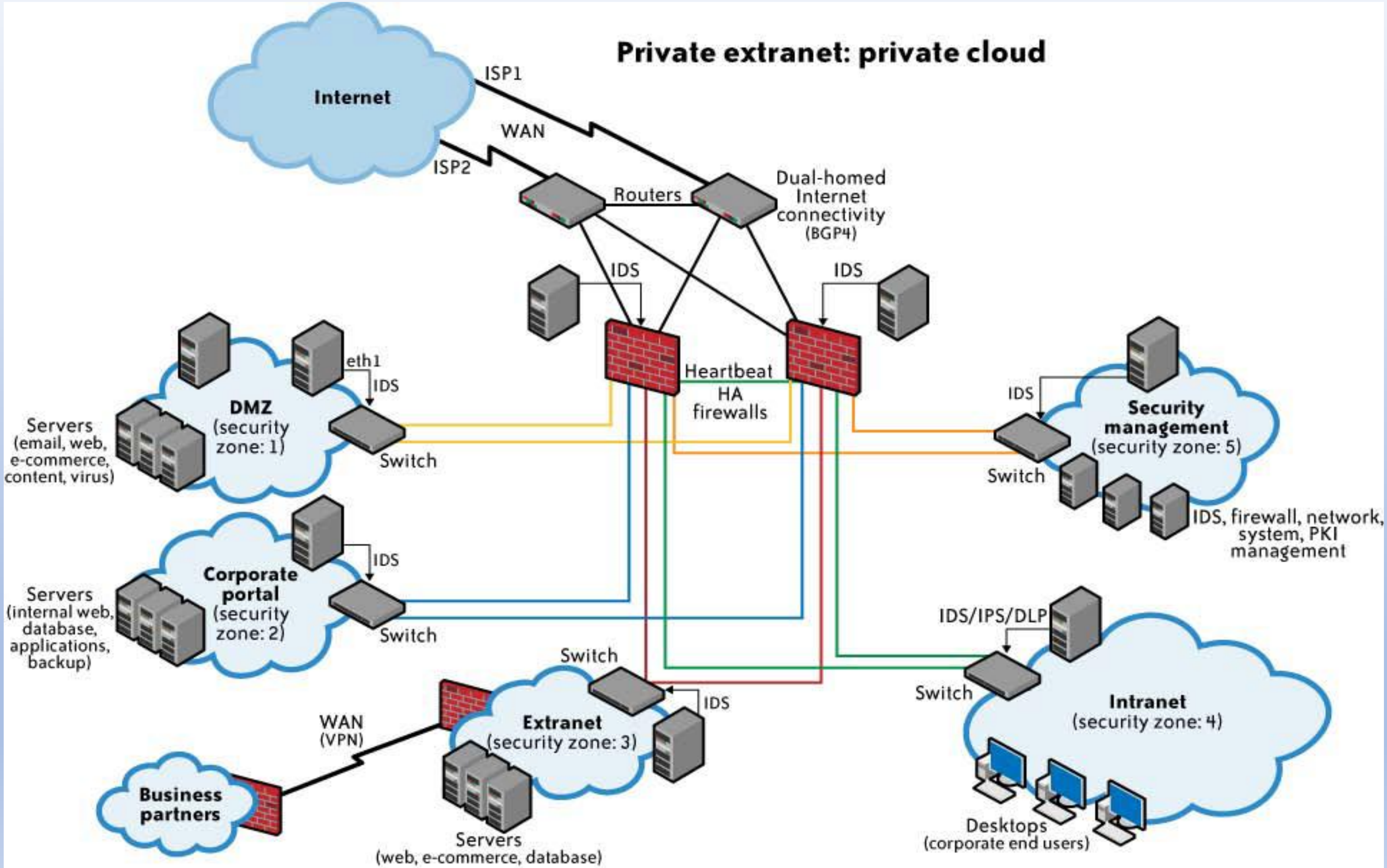
HOST LEVEL

APPLICATION LEVEL

NETWORK LEVEL

- When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds.
- With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider.
- Although your organization’s IT architecture may change with the implementation of a private cloud, your current network topology will probably not change significantly.
- The security considerations you have today apply to a private cloud infrastructure, too.
- And the security tools you have in place (or should have in place) are also necessary for a private cloud and operate in the same way.

NETWORK LEVEL


Private extranet: private cloud
Internet
ISP1
WAN
ISP2
Routers
Dual-homed Internet connectivity (BGP4)
IDS
IDS
Heartbeat
HA firewalls
eth1
IDS
DMZ (security zone: 1)
Servers (email, web, e-commerce, content, virus)
Switch
IDS
Security management (security zone: 5)
Switch
IDS, firewall, network, system, PKI management
IDS
Corporate portal (security zone: 2)
Servers (internal web, database, applications, backup)
Switch
IDS/IPS/DLP
Switch
Intranet (security zone: 4)
Desktops (corporate end users)
Switch
IDS
Extranet (security zone: 3)
Servers (web, e-commerce, database)
WAN (VPN)
Business partners

NETWORK LEVEL

- ❑ Illustrates a private extranet architecture using a private cloud setup, which integrates multiple security zones connected via high-availability (HA) firewalls and intrusion detection systems (IDS).
- ❑ Internet traffic from two ISPs is routed through redundant routers with dual-homed connectivity, feeding into HA firewalls that distribute traffic to distinct security zones.
- ❑ The DMZ (Zone 1) hosts public-facing servers (email, web, virus scanning), while the Corporate Portal (Zone 2) manages internal services like databases and backups. A secure Extranet (Zone 3) connects to business partners via VPN, and the Intranet (Zone 4) serves corporate end users. All zones are monitored with IDS/IPS/DLP systems.
- ❑ The Security Management zone (Zone 5) oversees system-wide controls, including firewalls, PKI, and network security, ensuring layered protection and isolated access across the infrastructure.

NETWORK LEVEL

- If you have a private extranet in place (e.g., for premium customers or strategic partners), for practical purposes you probably have the network topology for a private cloud in place already.
- However, if you choose to use public cloud services, changing security requirements will require changes to your network topology.
- You must address how your existing network topology interacts with your cloud provider’s network topology.
- There are three significant risk factors in this use case:

NETWORK LEVEL

- **Ensuring the confidentiality and integrity** of your organization’s data-in-transit to and from your public cloud provider.
- **Ensuring proper access control** (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- **Ensuring the availability of the Internet-facing resources** in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers

NETWORK LEVEL MITIGATION

- ❑ First, note that network-level risks exist regardless of what aspects of “cloud computing” services are being used (e.g., software-as-a-service, platform-as-a-service, or infrastructure-as-a-service).
- ❑ The primary determination of risk level is therefore not which *aaS is being used, but rather whether your organization intends to use or is using a public, private, or hybrid cloud.
- ❑ Although some IaaS clouds offer virtual network zoning, they may not match an internal private cloud environment that performs stateful inspection and other network security measures.

NETWORK LEVEL MITIGATION

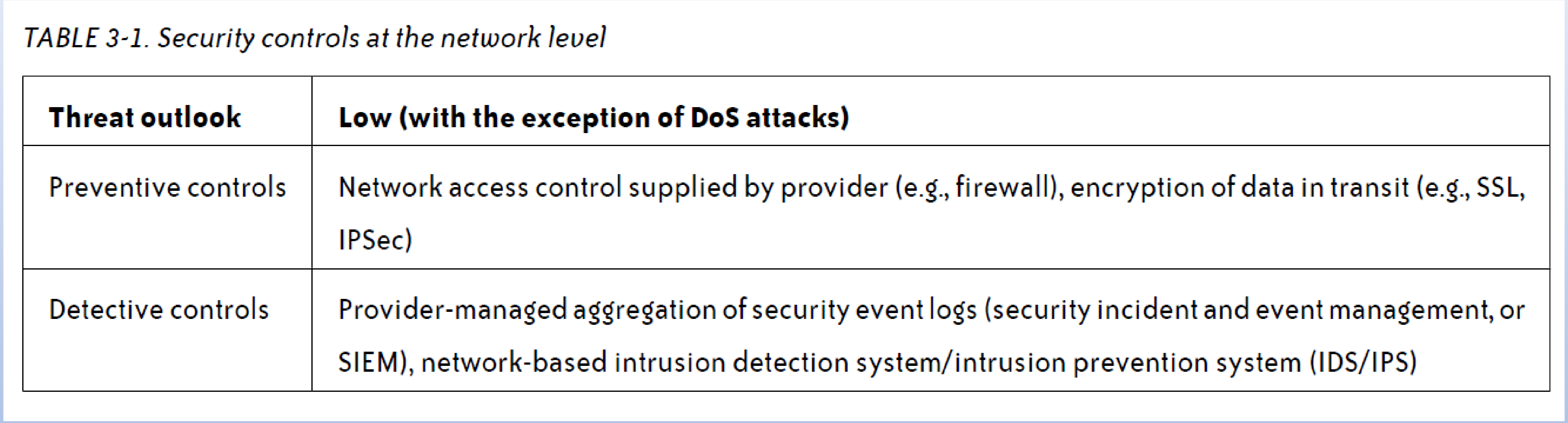


TABLE 3-1. Security controls at the network level

Threat outlook	**Low (with the exception of DoS attacks)**
Preventive controls	Network access control supplied by provider (e.g., firewall), encryption of data in transit (e.g., SSL, IPSec)
Detective controls	Provider-managed aggregation of security event logs (security incident and event management, or SIEM), network-based intrusion detection system/intrusion prevention system (IDS/IPS)

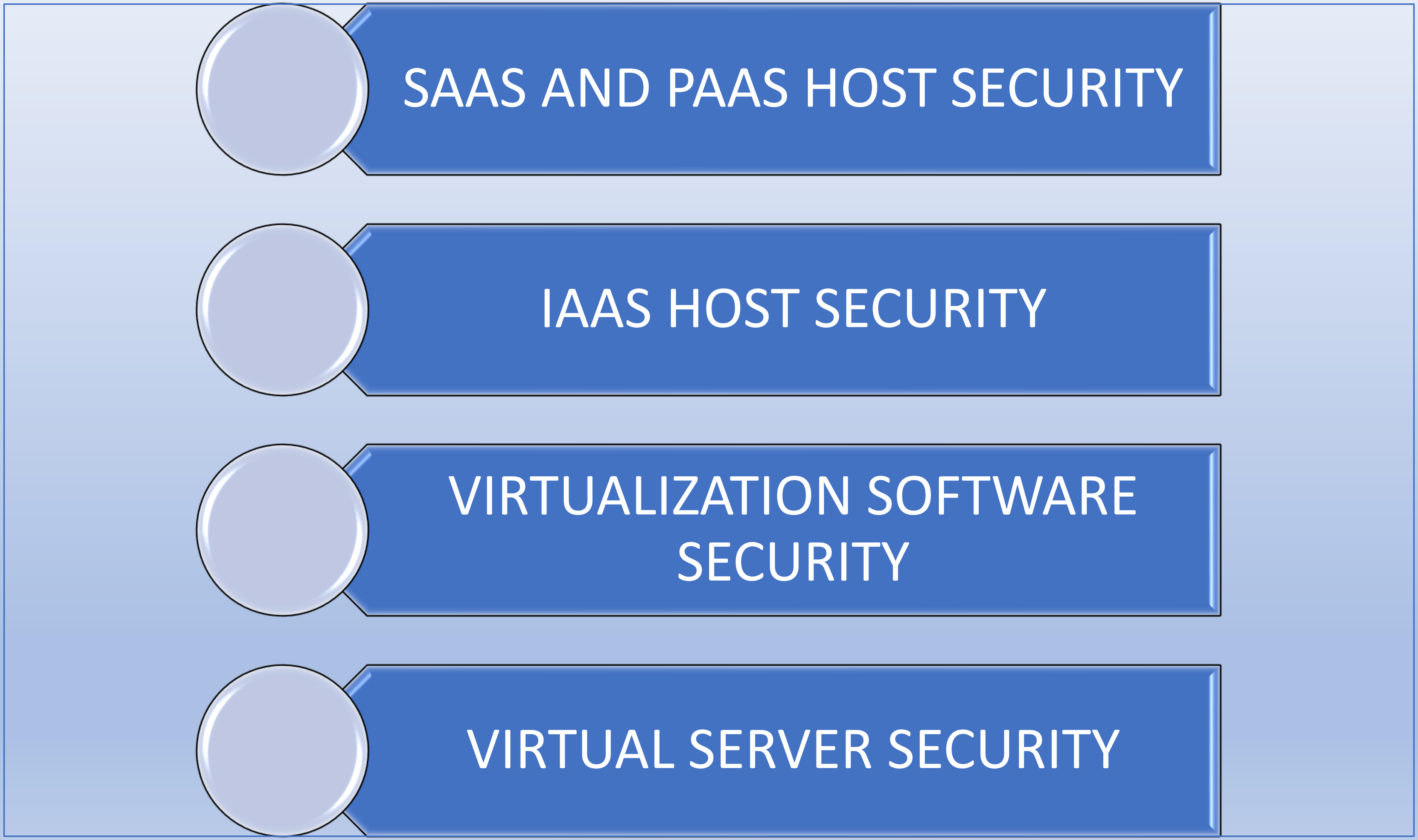
HOST LEVEL

- ❑ Consider cloud service models (SaaS, PaaS, IaaS) and deployment models (public, private, hybrid) when evaluating host security.
- ❑ No new host-specific threats exist in cloud, but virtualization threats like VM escape, configuration drift, and insider attacks persist.
- ❑ Weak access control to hypervisors increases risk, especially in public cloud setups.
- ❑ Cloud’s elastic nature introduces new security management challenges due to rapid provisioning and short-lived VM instances.
- ❑ Traditional patching methods struggle due to the high rate of change in cloud environments.

HOST LEVEL

- Massive scale and uniform operating systems in cloud can accelerate the spread of attacks—this is known as the “velocity of attack.”
- Clear understanding of trust boundaries is essential—know what you are responsible for securing.
- Compare your responsibilities with those of the cloud service provider (CSP) to ensure complete coverage of host infrastructure security.

HOST LEVEL



- SAAS AND PAAS HOST SECURITY
- IAAS HOST SECURITY
- VIRTUALIZATION SOFTWARE SECURITY
- VIRTUAL SERVER SECURITY

SAAS AND PAAS HOST LEVEL

- ❑ CSPs do not publicly disclose detailed host platform or OS security measures to avoid aiding attackers.
- ❑ In SaaS (e.g., Salesforce, Workday) and PaaS (e.g., Google App Engine, Force.com), host security is fully managed by the cloud service provider.
- ❑ Customers cannot directly view or control the host-level security in SaaS and PaaS models.
- ❑ To gain assurance about host security, customers can request details through a Non-Disclosure Agreement (NDA) or third-party controls assessment frameworks like SysTrust or ISO 27002.

SAAS AND PAAS HOST LEVEL

- ❑ CSPs are responsible for implementing preventive and detective controls on their host infrastructure and validating them via third-party or standards-based assessments.
- ❑ Virtualization technologies such as Xen and VMware are commonly used to optimize host resource utilization.
- ❑ Customers should understand how the CSP secures the virtualization layer as part of host infrastructure.
- ❑ In SaaS, this abstraction layer is only accessible to developers and CSP operations staff but in PaaS, customers can indirectly interact with the host abstraction layer via platform APIs.

SAAS AND PAAS HOST LEVEL

- Security of the host is the CSP’s responsibility, but customers still bear the responsibility of managing their own data securely.
- The main advantage for customers is reduced responsibility and cost in managing host-level security.
- Despite offloading host security, customers must ensure that the CSP maintains adequate security hygiene through documentation or audit assurances.

IAAS HOST LEVEL

- Host security in IaaS is divided into two categories: virtualization software security and customer guest OS (virtual server) security.
- **Virtualization Software Security:**
- This layer sits on bare-metal hardware and enables virtual instance creation.
- Virtualization methods include: OS-level virtualization (e.g., Solaris containers, BSD jails, Linux-VServer)Paravirtualization (e.g., certain Xen and VMware versions)Hardware-based virtualization (e.g., Xen, VMware, Microsoft Hyper-V)
- Securing this layer is critical as it separates hardware from virtual machines. In public IaaS, customers cannot access or secure this layer—this is managed solely by the CSP.

IAAS HOST LEVEL

- ❑ **Customer Guest OS or Virtual Server Security:**
- ❑ This is the virtual operating system instance (e.g., Linux, Windows, Solaris) that customers deploy.
- ❑ Customers have full control and responsibility for securing these virtual servers.
- ❑ These instances are internet-facing and thus must be hardened by the customer (patches, firewalls, access control, etc.).

VIRTUALIZATION SOFTWARE SECURITY

- ❑ If a hypervisor is compromised, the attacker could potentially impact all customer VMs on that host making security vital.
- ❑ There is an ongoing "arms race" between attackers and defenders in the virtualization security space.
- ❑ Example: A major breach at Vaserv.com occurred when hackers exploited a zero-day vulnerability in HyperVM, affecting 100,000 websites.
- ❑ The attack allowed destructive commands like rm -rf to be executed, leading to complete data loss for many customers.
- ❑ Many affected Vaserv users had no backups due to choosing unmanaged services, highlighting the severity of hypervisor-level breaches.

VIRTUALIZATION SOFTWARE SECURITY

- ❑ CSPs must implement strict physical and logical access controls for hypervisors and virtualization infrastructure.
- ❑ IaaS customers should seek to understand the CSP’s hypervisor security practices to evaluate compliance with internal policies and regulations. However, CSPs generally lack transparency in this area, often forcing customers to trust the provider’s security assurances.

VIRTUAL SERVER SECURITY

- ❑ IaaS customers have full control over their virtual machines (VMs) and are fully responsible for their security and ongoing management.
- ❑ Public IaaS providers (e.g., Amazon EC2) offer APIs for VM provisioning, decommissioning, and replication.
- ❑ Virtual servers are often accessible from the Internet, increasing their attack surface.
- ❑ Network access must be restricted to minimize exposure—typically, CSPs block all ports except essential ones (e.g., port 22 for SSH).Customers should ensure network-level controls (firewalls, access lists) are configured correctly on each VM.

VIRTUAL SERVER SECURITY

- **Common host-level security threats in public IaaS include:**
- Account hijacking due to weak or missing passwords on standard user accounts.
- Attacks on systems lacking proper host-level firewall configurations.
- Insertion of Trojans or malicious code into VM software or operating system images.