V20PCA107 - IT INFRASTRUCTURE MANAGEMENT 2.0

UNIT - III_WEEK - 9

Infrastructure Computer Security

Infrastructure security is the practice of protecting critical systems and assets against physical and cyber threats. From an IT standpoint, this typically includes hardware and software assets such as end-user devices, data centre resources, networking systems, and cloud resources.

Benefits of Infrastructure Security

Enterprises depend on their technology assets to maintain operations, so protecting technology infrastructure is protecting the organization itself. Proprietary data and intellectual property (IP) provide many companies significant competitive advantages in the market, and any loss of or disruption of access to this information can have profound negative impacts to a company's profitability.

Common Security Threats to IT Infrastructure

Cyber threats to technology infrastructure range from phishing attempts and ransomware attacks to distributed denial of service (DDoS) exploits and Internet of Things (IoT) botnets. Physical dangers include natural disasters such as fires and floods, civil unrest, utility outages, and theft or vandalism of hardware assets. Any of these have the potential to cause business disruption, damage an organization's public reputation, and have significant financial consequences.

Options For Securing IT Infrastructure

Typical elements of physical protection include access control, surveillance systems, security guards, and perimeter security. To protect their digital perimeter, organizations will implement firewalls, penetration testing, network monitoring, virtual private networks (VPNs), encryption technologies, and training programs to teach

employees how to identify and respond to phishing emails and other attempts to steal their network credentials.

1. Fundamentals of Computer Security

- **Confidentiality**: Ensuring that sensitive data is only accessible to authorized individuals.
- **Integrity**: Protecting data from being altered or tampered with by unauthorized users.
- **Availability**: Ensuring that systems and data are available to authorized users when needed.
- **Authentication**: Verifying the identity of users or devices accessing the system.
- **Authorization**: Controlling the access levels and permissions of authenticated users.

2. Types of Threats

- **Malware**: Viruses, worms, ransomware, spyware, and other malicious software.
- **Phishing**: Fraudulent attempts to obtain sensitive information via deception.
- **Denial of Service (DoS)**: Attacks that disrupt the availability of services.
- **Man-in-the-Middle (MITM)**: Intercepting and altering communication between two parties.
- **Insider Threats**: Security risks posed by employees or trusted individuals.

3. Security Policies and Protocols

- **Security Policy Development**: Defining organizational security protocols, incident response, and acceptable use policies.
- **Access Control Policies**: Determining user rights and levels of access (e.g., Role-Based Access Control).
- **Network Security Protocols**: Secure communication methods such as SSL/TLS, VPNs, firewalls, and intrusion detection systems (IDS).
- **Encryption**: Using cryptographic techniques to secure sensitive information during transmission and storage.

4. Security Technologies

- **Firewalls**: Hardware or software systems that block unauthorized access to or from a network.

- **Antivirus and Antimalware**: Software designed to detect and remove malicious code.
- **Intrusion Detection/Prevention Systems (IDS/IPS)**: Tools that monitor network traffic for signs of suspicious activity.
- **Data Loss Prevention (DLP)**: Technology designed to prevent unauthorized sharing of sensitive data.
- **Endpoint Security**: Securing devices like laptops, smartphones, and other endpoints connected to a network.

5. Incident Management and Response

- **Incident Response Plan (IRP)**: Steps to follow in case of a security breach or cyberattack.
- **Forensics**: Investigating security incidents to understand their causes and impacts.
- **Disaster Recovery and Business Continuity**: Plans and systems to restore operations in the event of a major security incident.

6. Emerging Threats and Trends

- **Zero-Day Vulnerabilities**: Exploits that occur before a patch or fix is available.
- **Advanced Persistent Threats (APT)**: Prolonged and targeted attacks, often backed by well-funded adversaries.
- **Cloud Security**: Ensuring the safety of data stored in and accessed from cloud environments.
- **IoT Security**: Protecting Internet of Things devices, which are increasingly targeted by cybercriminals.

7. Regulations and Compliance

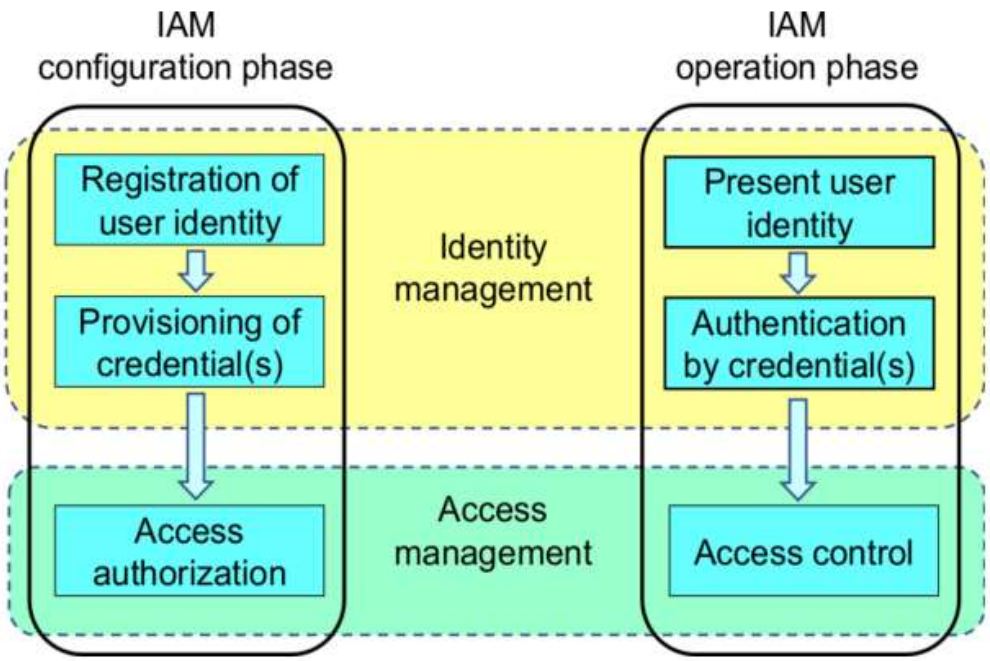
- **GDPR (General Data Protection Regulation)**: Governing data privacy in the EU.
- **HIPAA (Health Insurance Portability and Accountability Act)**: Protecting sensitive patient data in healthcare.
- **PCI DSS (Payment Card Industry Data Security Standard)**: Ensuring secure handling of credit card information.
- **ISO/IEC 27001**: An international standard for managing information security.

These are essential components of **computer security in IT infrastructure management**, ensuring that systems are resilient to attacks and downtime while maintaining the confidentiality, integrity, and availability of data.

Identity Management

Identity management (IDM), also known as identity and access management (IAM or IdAM), is a framework of policies and technologies to ensure that the right users (that are part of the ecosystem connected to or within an enterprise) have the appropriate access to technology resources. IDM systems fall under the overarching umbrellas of IT security and data management. IDM addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

Identity management (ID management) – or identity and access management (IAM) – is the organizational and technical processes for first registering and authorizing access rights in the configuration phase, and then in the operation phase for identifying, authenticating and controlling individuals or groups of people to have access to applications, systems or networks based on previously authorized access rights. Identity management (IdM) is the task of controlling information about users on computers. Such information includes information that authenticates the identity of a user, and information that describes data and actions they are authorized to access and/or perform. It also includes the management of descriptive information about the user and how by whom that information can be accessed and modified. In addition to users, managed entities typically include hardware and network resources and even applications. The diagram below shows the relationship between the configuration and operation phases of IAM, as well as the distinction between identity management and access management.



Access control is the enforcement of access rights defined as part of access authorization.

Digital identity is an entity's online presence, encompassing personal identifying information (PII) and additional information. It can be interpreted as the codification of identity names and attributes of a physical instance in a way that facilitates processing.

Function

In the real-world context of engineering online systems, identity management can involve five basic functions:

1. The pure identity function: Creation, management and deletion of identities without regard to access or entitlements;
2. The user access (log-on) function: For example: a smart card and its associated data used by a customer to log on to a service or services (a traditional view);
3. The service function: A system that delivers personalized, role-based, online, on-demand, multimedia (content), presence-based services to users and their devices.
4. Identity Federation: A system that relies on federated identity to authenticate a user without knowing their password.
5. Audit function: Monitor bottlenecks, malfunctions and suspect behavior.

An identity-management system refers to an information system, or to a set of technologies that can be used for enterprise or cross-network identity management.
The following terms are used in relationship with "identity-management system":

- Access-governance system
- Identity and access management system
- Entitlement-management system
- User provisioning system

Identity management, otherwise known as identity and access management (IAM) is an identity security framework that works to authenticate and authorize user access to resources such as applications, data, systems, and cloud platforms. It seeks to ensure only the right people are being provisioned to the right tools, and for the right reasons. As our digital ecosystem continues to advance, so does the world of identity management.

"Identity management" and "access and identity management" (or AIM) are terms that are used interchangeably under the title of identity management while identity management itself falls under the umbrella of IT security and information privacy and privacy risk as well as usability and e-inclusion studies.

There are three components of Identity and Access Management (IAM):

- Access management/Single sign-on to verify users' identities before they can access the network and applications
- Identity governance to ensure that user access is being granted according to appropriate access policies for onboarding and role/responsibility changes
- Privileged access management to control and monitor access to highly privileged accounts, applications and system assets

These technologies can be combined using identity governance, which provides the foundation for automated workflows and processes.

Purposes for Using Identity Management Systems

Identity management systems are concerned with the creation, the administration and the deployment of:

- Identifiers: Data used to identify a subject.
- Credentials: Data providing evidence for claims about identities or parts thereof.
- Attributes: Data describing characteristics of a subject.

The purposes of identity management systems are:

- Identification: Who is the user – used on logon or database lookup
- Authentication: Is this the real user? Systems needs to provide evidence!
- Authorization and non-repudiation: Authorization of documents or transaction with e-ID and most often with digital signature based on e-ID. Generates non-repudiation and receipts.

Commercial Solutions

Identity-management systems, products, applications, and platforms are commercial Identity-management solutions implemented for enterprises and organizations. Technologies, services, and terms related to identity management include Microsoft Windows active directory, service providers, identity providers, Web services, access control, digital identities, password managers, single sign-on, security tokens, security token services (STS), workflows, OpenID, WS-Security, WS-Trust, SAML 2.0, OAuth, and RBAC.

1. **Identity Management Fundamentals**
   - **Identity**: A unique representation of a user, system, or application within an organization.
   - **Authentication**: The process of verifying the identity of users trying to access a system (e.g., via passwords, biometrics, or multi-factor authentication).
   - **Authorization**: Granting the appropriate access and privileges based on the user's role or identity within the organization.
   - **Federated Identity**: A method where a user's identity is shared across multiple systems or organizations without needing multiple credentials (e.g., Single Sign-On - SSO).

2. Components of Identity Management

- **User Identity Lifecycle Management**: Involves the creation, maintenance, and removal of user accounts as they join, change roles, or leave the organization.
- **Single Sign-On (SSO)**: A user can authenticate once and gain access to multiple systems without needing to log in separately for each one.
- **Multi-Factor Authentication (MFA)**: A security process requiring multiple verification methods (e.g., password + code sent to a mobile device) before granting access.
- **Password Management**: Ensuring secure password policies, storage, and reset mechanisms (e.g., complex password requirements, self-service password resets).

3. Access Control Mechanisms

- **Role-Based Access Control (RBAC)**: Permissions are assigned based on the user's role within the organization (e.g., admin, manager, employee).
- **Attribute-Based Access Control (ABAC)**: Permissions are assigned based on user attributes like department, location, or clearance level.
- **Least Privilege Principle**: Ensuring that users have the minimum level of access necessary to perform their job functions.
- **Just-In-Time (JIT) Access**: Temporary access permissions granted to users for a limited time to minimize risk.

4. Identity Management Technologies

- **Identity and Access Management (IAM) Systems**: Centralized tools used to manage identities and control access across multiple systems. Examples include Okta, Microsoft Azure Active Directory, and IBM Security Identity Manager.
- **Directory Services**: Databases that store user identities and credentials, such as **Active Directory (AD)** or **Lightweight Directory Access Protocol (LDAP)**.
- **Identity Governance and Administration (IGA)**: Solutions focused on managing the identity lifecycle, ensuring that access rights are appropriate and compliant with regulations.
- **Identity Providers (IdPs)**: Systems that authenticate users and provide identity information to other applications (e.g., Google, Facebook as third-party IdPs in web apps).

5. Identity Federation and Single Sign-On (SSO)

- **Federated Identity Management**: Enables users to authenticate across different networks or domains without needing multiple sets of credentials. Technologies such as **SAML (Security Assertion Markup Language)** and **OAuth** are commonly used in federated identity management.
- **SSO Benefits**: SSO simplifies the user experience by reducing the need for multiple logins, improving security by centralizing authentication management, and enhancing productivity.

6. Security in Identity Management

- **Zero Trust Security**: A framework where trust is never assumed, and verification is required at every stage. Every user, device, and service must be verified regardless of its location inside or outside the network perimeter.
- **Privileged Access Management (PAM)**: Managing and securing accounts with elevated permissions, such as system administrators or developers with access to critical systems.
- **Identity Threat Detection and Response**: Proactively monitoring for identity-related threats, such as compromised credentials or suspicious access behavior.
- **Biometric Authentication**: Leveraging physical characteristics like fingerprints, facial recognition, or retina scans for identity verification.

7. Compliance and Governance

- **Regulatory Requirements**: Compliance with standards such as **GDPR**, **HIPAA**, **PCI DSS**, and **ISO/IEC 27001** often involves strict identity management protocols to ensure the protection of sensitive data.
- **Audit and Reporting**: Organizations must regularly audit their identity management systems to track access logs, detect anomalies, and generate reports for compliance purposes.
- **Access Reviews**: Periodic evaluations of user access to ensure they only have permissions necessary for their roles.

8. Challenges in Identity Management

- **Identity Sprawl**: The proliferation of user identities across multiple systems, making it difficult to manage and secure them effectively.

- **Password Fatigue**: Users having to remember multiple passwords, leading to poor security practices (e.g., weak passwords, password reuse).
- **Shadow IT**: Users accessing unauthorized applications or systems outside the organization's control, which may pose a security risk.

9. Future Trends in Identity Management

- **Decentralized Identity**: Users own and control their identity through blockchain or other distributed technologies, reducing reliance on centralized identity providers.
- **Passwordless Authentication**: Methods such as biometrics or hardware tokens that eliminate the need for traditional passwords.
- **Artificial Intelligence in Identity Management**: AI and machine learning can be used to analyse access patterns, detect anomalies, and improve security by making real-time decisions based on user behaviour.

Access Control in IT Infrastructure Management

Access control is a fundamental concept in IT infrastructure management, ensuring that only authorized individuals or systems can access resources such as networks, applications, data, and devices. The main objective of access control is to protect the confidentiality, integrity, and availability (CIA) of information by managing and limiting who can use or interact with a given resource.

Key Elements of Access Control

Identification:

- This step involves recognizing a user or system trying to access the resource.
- Typically implemented using unique identifiers such as usernames, IDs, or email addresses.

Authentication:

- Verifying the identity of a user/system using credentials such as passwords, biometrics, tokens, or multi-factor authentication (MFA).
- Common authentication methods include:

- Password-based authentication

- Biometrics (fingerprints, retina scans, facial recognition)
- Two-factor or multi-factor authentication (MFA)

Types of Access Control Models

Discretionary Access Control (DAC):

- The owner of the resource determines who can access it and what permissions they have.
- Flexible but can be prone to errors due to over-per missioning.

Mandatory Access Control (MAC):

- The system enforces strict access policies defined by a central authority based on security labels.
- Users cannot alter permissions on resources.
- Common in government or high-security environments.

Role-Based Access Control (RBAC):

- Access is based on roles assigned to users within an organization.
- Users inherit permissions associated with their roles.
- This method is scalable and reduces administrative overhead.

Attribute-Based Access Control (ABAC):

- Access is determined by policies that consider attributes (user, resource, and environment attributes).
- More dynamic and fine-grained compared to RBAC.

Access Control Methods

Physical Access Control:

- Involves securing physical access to infrastructure components such as servers, data centres, and network equipment.
- Methods include keycards, biometric readers, and security guards.

Logical Access Control:

- Deals with restricting access to digital resources such as files, databases, applications, and systems.
- Methods include software permissions, encryption, and firewall rules.

Network Access Control (NAC):

- Focuses on controlling access to network resources based on user identity and policies.
- Tools like firewalls, VPNs, and intrusion detection/prevention systems are used.

Best Practices for Access Control in IT Infrastructure

Principle of Least Privilege:

Users should only be granted the minimum level of access necessary to perform their duties.

Regular Audits and Reviews:

Periodic reviews of access permissions help identify and revoke unnecessary privileges.

Multi-Factor Authentication (MFA): Add an extra layer of security by requiring users to verify their identity through multiple factors (e.g., password + OTP).

Separation of Duties: Critical tasks should be divided among multiple individuals to reduce the risk of insider threats and fraud.

Access Control Lists (ACLs): Use ACLs to specify who can access particular network resources and what operations they can perform.

Centralized Management: Implement centralized access control mechanisms for easier management and consistency across the organization.

Challenges in Access Control

1. **User Mismanagement:** Over-provisioning access or failure to revoke access for former employees can lead to security breaches.
2. **Complexity in Large Organizations:** As organizations grow, managing access permissions across multiple systems and platforms becomes more complex.
3. **Insider Threats:** Employees with legitimate access can misuse their privileges, leading to data theft or sabotage.
4. **Compliance and Regulations:** Organizations must ensure their access control policies comply with regulations like GDPR, HIPAA, and SOX.

Intrusion Detection System

What is an Intrusion Detection System?

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. The

IDS is also a listen-only device. The IDS monitors traffic and reports results to an administrator. It cannot automatically take action to prevent a detected exploit from taking over the system.

Attackers are capable of exploiting vulnerabilities quickly once they enter the network. Therefore, the IDS is not adequate for prevention. Intrusion detection and intrusion prevention systems are both essential to security information and event management.

Intrusion Detection Systems vs. Intrusion Prevention Systems

The following table summarizes the differences between the IPS and the IDS deployment.

	Intrusion Prevention System	**IDS Deployment**
Placement in Network Infrastructure	Part of the direct line of communication (inline)	Outside direct line of communication (out-of-band)
System Type	Active (monitor & automatically defend) and/or passive	Passive (monitor & notify)
Detection Mechanisms	1. Statistical anomaly-based detection 2. Signature detection: - Exploit-facing signatures - Vulnerability-facing signatures	1. Signature detection: - Exploit-facing signatures

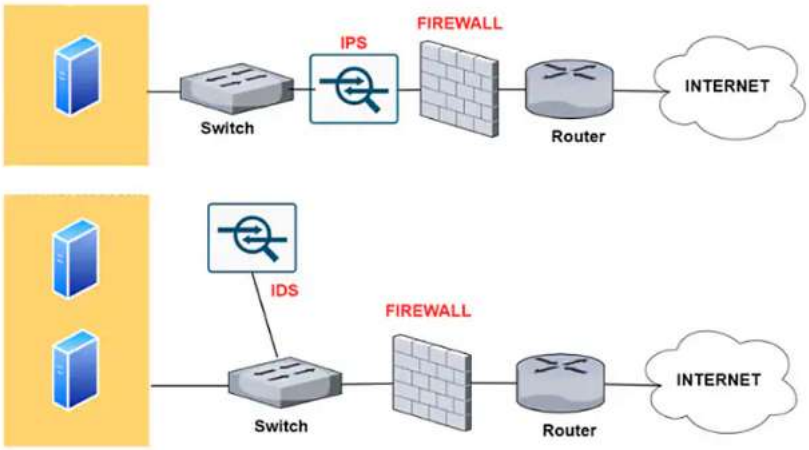


Diagram depicting the difference between an IPS and an IDS

How IDS Works

An IDS only needs to detect potential threats. It is placed out of band on the network infrastructure. Consequently, it is not in the real-time communication path between the sender and receiver of information. IDS solutions often take advantage of a TAP or SPAN port to analyze a copy of the inline traffic stream. This ensures that the IDS does not impact inline network performance.

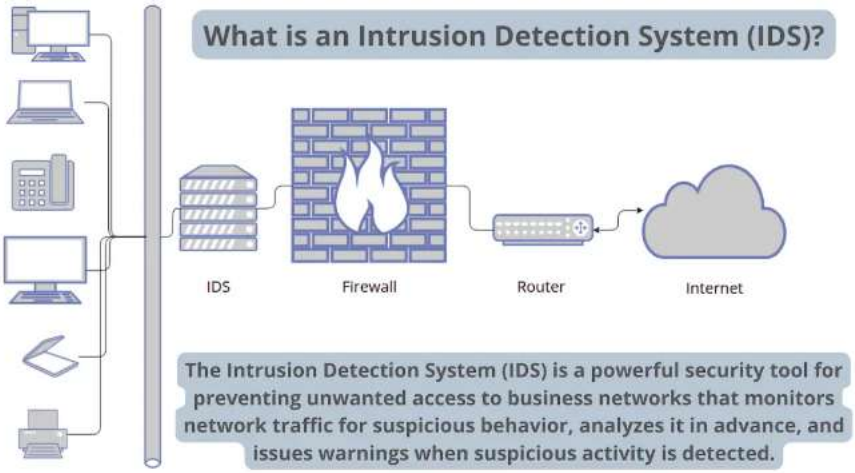


Diagram depicting the functionality of an intrusion detection system

When IDS was developed, the depth of analysis required to detect intrusion could not be performed quickly enough. The speed would not keep pace with components on the direct communications path of the network infrastructure. Network intrusion detection systems are used to detect suspicious activity to catch hackers

before damage is done to the network. There are network-based and host-based intrusion detection systems. Host-based IDSes are installed on client computers; network-based IDSes are on the network itself.

An IDS works by looking for deviations from normal activity and known attack signatures. Anomalous patterns are sent up the stack and examined at protocol and application layers. It can detect events like DNS poisonings, malformed information packets and Christmas tree scans. An IDS can be implemented as a network security device or a software application. To protect data and systems in cloud environments, cloud-based IDSes are also available.

Types of IDS Detection

There are five types of IDS: network-based, host-based, protocol-based, application protocol-based and hybrid.

1. **Network-based intrusion detection system (NIDS)** - A network IDS monitors a complete protected network. It is deployed across the infrastructure at strategic points, such as the most vulnerable subnets. The NIDS monitors all traffic flowing to and from devices on the network, making determinations based on packet contents and metadata.
2. **Host-based intrusion detection system (HIDS)** - A host-based IDS monitors the computer infrastructure on which it is installed. In other words, it is deployed on a specific endpoint to protect it against internal and external threats. The IDS accomplishes this by analyzing traffic, logging malicious activity and notifying designated authorities.

The remaining three types can be described as such:

3. **Protocol-based (PIDS)** - A protocol-based intrusion detection system is usually installed on a web server. It monitors and analyzes the protocol between a user/device and the server. A PIDS normally sits at the front end of a server and monitors the behavior and state of the protocol.
4. **Application protocol-based (APIDS)** - An APIDS is a system or agent that usually sits inside the server party. It tracks and interprets correspondence on

application-specific protocols. For example, this would monitor the SQL protocol to the middleware while transacting with the web server.

5. **Hybrid intrusion detection system** - A hybrid intrusion detection system combines two or more intrusion detection approaches. Using this system, system or host agent data combined with network information for a comprehensive view of the system. The hybrid intrusion detection system is more powerful compared to other systems. One example of Hybrid IDS is Prelude.

There is also a subgroup of IDS detection methods, the two most common variants being:

1. **Signature-based**
   A signature-based IDS monitors inbound network traffic, looking for specific patterns and sequences that match known attack signatures. While it is effective for this purpose, it is incapable of detecting unidentified attacks with no known patterns.

2. **Anomaly-based**
   The anomaly-based IDS is a relatively newer technology designed to detect unknown attacks, going beyond the identification of attack signatures. This type of detection instead uses machine learning to analyze large amounts of network data and traffic.
   Anomaly-based IDS creates a defined model of normal activity and uses it to identify anomalous behavior. However, it is prone to false positives. For example, if a machine demonstrates rare, but healthy behavior, it is identified as an anomaly. This results in a false alarm.

Why Intrusion Detection Systems are Important

Cyberattacks are always increasing in complexity and sophistication, and Zero Day Attacks are common. As a result, network protection technologies must keep pace with new threats, and businesses must maintain high levels of security. The objective is to assure secure, trusted communication of information. Therefore, an IDS is important

to the security ecosystem. It operates as a defense for systems security when other technologies fail.

- Identify security incidents.
- Analyze the quantity and types of attacks.
- Help identify bugs or problems with device configurations.
- Support regulatory compliance (by means of better network visibility and IDS log documentation).
- Improve security responses (by means of inspecting data within network packets, rather than manual census of systems).

While IDSes are useful, they are extended in impact when coupled with IPSes. Intrusion Prevention Systems (IPS) add the ability to block threats. This has become the dominant deployment option for IDS/IPS technologies.

Better still is the blend of multiple threat prevention technologies to form a complete solution. An effective approach is a combination of:

- Vulnerability protection
- Anti-malware
- Anti-spyware

These technologies combined constitute advanced threat protection. The service scans all traffic for threats (including ports, protocols and encrypted traffic). Advanced threat prevention solutions look for threats within the cyberattack lifecycle, not just when it enters the network. This forms a layered defense — a Zero Trust approach with prevention at all points.