

Intrusion Detection System (IDS)

Keeping your IT infrastructure secure from malicious actors has never been so important. With businesses increasingly becoming the target of everyday cybercrime, understanding legitimate and illegitimate access to your systems is a vital tool in an ever-growing arsenal of protection measures. So how can an IDS help?

What is an IDS?

An intrusion detection system is a piece of software that monitors a network for malicious activity or policy violations.

Monitored automatically, 24/7/365, if the system detects any instances of malicious activity or violation, the event will be reported using an event management system. This will then be picked up by a dedicated expert who will inspect the issue and put measures in place to mitigate the malicious activity and further protect the network.

Types of IDS

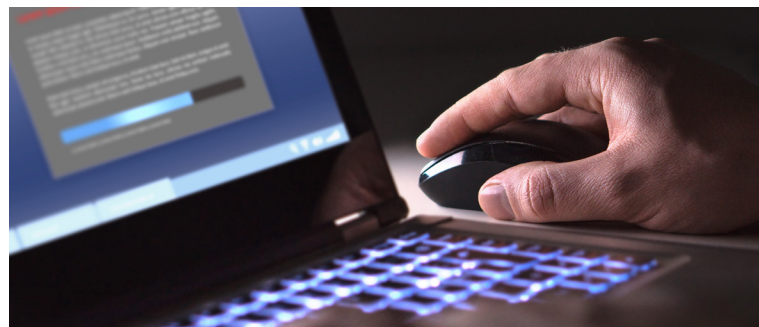
There are a wide array of intrusion detection systems that work on varying levels of security, but the two most common classifications are:

Network intrusion detection system

This is a system that analyses incoming network traffic.

Host-based intrusion detection systems

This is a system that monitors important operating system files.



Why should you use an IDS solution?

With a rapidly changing cybersecurity landscape, it is vital in modern business environments, where information is shared between users and organisations, that the highest level of security is in place. In short, an intrusion detection system acts as an adaptable safeguarding tool for system security, should traditional lines of security fail.

Why should you consider an IDS solution?

- Provides integrated attack detection and vulnerability assessment
- Target aware and able to intelligently adapt to each network
- Accurately identifies real incidents, with fewer false alarms
- Dynamically scores the threat level of all attacks through network threat management
- Automates the IDS analysis process through correlation and heuristic methods
- Fine-tuned and configured for your bespoke solution
- Protects against outbound attacks caused by viruses or malware



Why choose Hyve's IDS solution?

Here at Hyve, security is at the heart of what we do and because of this, we have developed a highly available IDS that provides real-time network-level threat awareness and continuous vulnerability discovery.

Our IDS system highlights critical information and identifies code and application vulnerabilities, leading to better-informed decisions about threats and risk management, and allows for continuous improvement in the base security of any application or infrastructure using it.

Our primary focus is ensuring that our customer's applications and systems are live and accessible 24/7. Unlike intrusion prevention systems (IPS), our IDS does not block traffic, it simply monitors in real-time so that our support engineers are aware of the event anywhere on an application or network. With such an approach, our IDS solution never blocks traffic unless it has been proven to be malicious.

