

**Threat Detection Tools**

Version 1.0

**Contents**

[**Network Intrusions Detection (NIDS) Tools** 3](#_Toc83738959)

[**Firewall** 3](#_Toc83738960)

[**Anti-Virus and Anti-Malware\*** 3](#_Toc83738961)

[**Intrusion Detection System (IDS)** 3](#_Toc83738962)

[**Intrusion Prevention Systems (IPS)** 4](#_Toc83738963)

[**Proxys** 4](#_Toc83738964)

[**Bastion Host** 4](#_Toc83738965)

[**Password Auditing Tools** 4](#_Toc83738966)

[**Vulnerability Assessment** 5](#_Toc83738967)

[**Penetration Testing** 5](#_Toc83738968)

[**Managed Detection Services** 5](#_Toc83738969)

# **Network Intrusions Detection (NIDS) Tools**

Intrusion detection systems look for patterns in network activity to identify potentially malicious activity. Whilst initial strategies deter and block malicious activity, cyber criminals have become increasingly sophisticated, and attacks are still on the rise.

# **Firewall**

A firewall is a network security system that monitors and controls incoming and outgoing network traffic. The ‘rules’ used by the firewall decide whether to allow or block connections and these may be pre-configured or set by the user. A firewall acts as a gatekeeper to put a barrier between your school network and the Internet.

There are software and hardware firewalls. A hardware firewall is an actual device, such as a router. A software firewall is a program on your device. Many devices have built-in software firewalls, and these should be enabled (turned on) and updated regularly.

# **Anti-Virus and Anti-Malware\***

\*Malware refers to malicious software, which viruses are one example.

Antivirus software looks at a variety of data such as files, software applications, and webpages your users access. It searches for known threats and monitors the behaviour of all programs, alerting you to suspicious or unusual activity and quarantining suspicious files.

As well as actively monitoring, products allow users to run full system scans if they are concerned about a potential threat or compromise.

More information is available from the [NCSC](https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product) website.

# **Intrusion Detection System (IDS)**

An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator, or collected centrally using a security information and event management system. Known as a ‘burglar alarm for your network’.

It looks for unusual and suspicious network traffic and bad patterns of access.

[Police cyber alarm](https://cyberalarm.police.uk) is a free IDS tool available for schools.

The easy to install network traffic collector has minimal system requirements and alerts schools to potential threats. Evidence of an attack can be made available to the police in a court ready format.

No personal data is collected and so there is no data protection implication or intrusive monitoring of user activity.

# **Intrusion Prevention Systems (IPS)**

An Intrusion Prevention System (**IPS**) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

It is a ‘burglar alarm with teeth’ and instead of simply issuing an alert, it alerts and also attacks the intrusion.

There is a risk of false positives which may cause a self-inflicted DoS and it can be weaponised against you.

# **Proxys**

In computer networking, a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources. (An intelligent firewall that works at a high level).

Proxy servers can be called web application filters.

# **Bastion Host**

A bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. Designed to be put in a high risk area.

# **Password Auditing Tools**

Minimum password complexity requirements can be set across a network, but this is often not used in schools with young pupils, due to the difficulty in getting pupils individual logons. Therefore, many schools rely on documented policy.

Password auditing tools are also used to look at the security of your school by attempting to break passwords to gain access to the school network. Auditing tools utilise common attacks to discover the password of a user account.

An auditing tool can help you to assess whether users are following school password policy requirements for length, complexity, and system specific access.

Also see [password policy advice](https://www.ncsc.gov.uk/collection/passwords/updating-your-approach) from the NCSC.

# **Vulnerability Assessment**

Vulnerability testing or vulnerability assessment is a process of evaluating security risks to reduce the possibility for intruders/hackers to get unauthorised access to systems.

Vulnerability scanning allows you to detect and remediate potential risk, helping you to identify and map all your assets – hardware and software, and obtain a report on potential vulnerabilities. This allows you to prioritise resources on your highest risk areas.

Also see [Vulnerability Scanning Tools](https://www.ncsc.gov.uk/guidance/vulnerability-scanning-tools-and-services) and Services information from the NCSC.

# **Penetration Testing**

Penetration testing (pen testing) simulates a cyber-attack against your school network. It is designed to find vulnerabilities that could lead to unauthorised access or attempts to gain access.

Penetration tests may form part of a full security audit and help your school gain assurance against your vulnerability assessment.

Further information on [Penetration Testing](https://www.ncsc.gov.uk/guidance/penetration-testing) is available from the NCSC.

# **Managed Detection Services**

Managed Detection and Response (MDR) services are managed by a third-party provider. An MDR service provides intelligence on threats, security monitoring, incident analysis, and incident response.

Some IT providers incorporate managed MDS. Be sure that contracts cover monitoring provisions, carry out due diligence, and understand how reporting mechanisms work. You can’t outsource accountability.