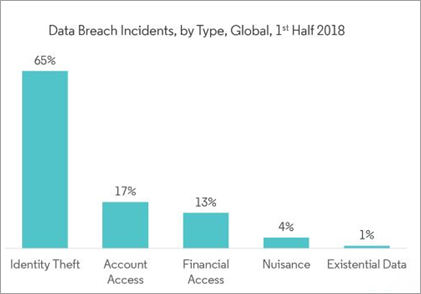
**Firewall software:**

**An Overview**

The types of data breaches that businesses are most concerned about and seek for firewall protection are illustrated in the following infographic:



Looking at the above infographic, we can see that identity theft is by far the biggest concern for businesses seeking cyber and firewall protection today. But, what makes firewall protection so important or in other words ‘so useful’?

Perhaps, the best way to find it out is through the answers to the frequently asked questions about the firewall software which we have covered in the upcoming section.

**Frequently Asked Questions About Firewall**

Enlisted below are the most commonly asked questions about Firewalls.

**Q #1) What is a Firewall?**

**Answer:** A shield or barrier protecting a private network from unauthorized access, a firewall secures devices connected to the internet or another network such as a local area network (LAN).

The purpose of having a firewall installed on a PC, phone, or tablet is to protect users from the data-based malware threats that exist on the internet or other connected networks.

In the cyberspace, data transfers between your PC and servers & routers. This data, which is transferred in packets, is monitored by a firewall to identify and block any unwanted traffic.

The firewall accomplishes this by checking the data packets against the rules that have been set up. If the data packets are in line with these rules, then they are accepted by the firewalls. If they fail to meet the rules, then the firewall rejects or blocks them.

Today, firewalls are helping to protect the PCs and other connected devices across the globe whether they belong to individual users, large corporations, or the government.

**Q#2) How does a Firewall work?**

**Answer:** To explain it simply, firewalls work by monitoring the information traffic to accept or allow the ‘good data’ while rejecting or blocking the ‘bad or harmful data’. However, if we get into the details, then the firewall uses one of the three methods or combinations of these to control the traffic that flows in and out of the network.

**The three methods used by a Firewall to protect a PC, tablet, or other devices are:**

1. Packet Filtering
2. Proxy Service
3. Stateful Inspection

Involving the use of a pre-determined set of rules to create filters, packet filtering is the most basic form of firewall protection. The firewall will not allow a data packet to enter a network if it is flagged by the filters. All data packets, except those that make it through the filters, are discarded.

An application that serves as an intermediary between systems, a firewall proxy retrieves information from the internet and then sends it to the requesting system. The firewall’s application layer is where the Firewall Proxy Servers function.

This is the point where it is mandatory for both ends of a connection to use a proxy to conduct the session. A process that reflects a service that would run on the end host is created and run by the proxy servers on the firewall. As a result, all data transfer for an activity is centralized for scanning to the firewall.

The third and final method used by a firewall to protect a device or system is a stateful inspection. The most advanced firewall scanning, stateful inspection keeps information attributes of each connection for the duration of the session in a database.

Collectively referred to as the connection’s ‘state’, these attributes include important information such as the connection’s port and IP addresses and the sequence in which the data packets are being transferred. Relevant information held in the database is compared to the data being transferred by the firewall.

The firewall allows the information to go through if the comparison yields a positive match. Otherwise, the entry of the information or data packet is denied.

**Q#3) What are the Different Types of Firewall Software?**

**Answer:** There are two basic types of Firewall i.e. Appliance Firewalls and Client-based Firewalls. A firewall software, a client-based firewall is installed on a device for tracking the information traffic on that particular device.

On the other hand, the appliance firewall is a physical or hardware-based version of the firewall which includes a device that is placed between a user’s network and an outside network such as the internet.

Often, the appliance firewalls are used for network environments with several devices that share the same network or internet connection. On the other hand, client-based or software firewalls are best for customizing the levels of protection and setting up firewall permissions for individual users or a group of users.

**Q#4) How do Firewalls Protect from Hackers?**

**Answer:** Firewalls protect from hackers by blocking their access to your PC via Wi-Fi and the internet.

To access your PC and steal sensitive data such as your browsing history, bank details, passwords, and other such information, hackers make use of the keylogging software and Trojan viruses to record your sessions and monitor your keystrokes. By keystrokes, we mean what you enter onto your PC or another device.

Hackers can run illicit activities using your computer even without your knowledge. The good news is that firewalls can help to stop them.

***How can firewalls protect your computer from hackers?*** By blocking all unauthorized connections to your system.

Additionally, a firewall allows you to choose programs on your computer which can access the internet. This ensures that you never connect to the internet unknowingly. This stops the hackers and other cybercriminals in their tracks as they use a Wi-Fi network or an internet connection to enter your computer.

**Q#5) Can a Firewall be Hacked?**

**Answer:** It is a rarity, that a firewall can be hacked. Cybercriminals can easily hack a firewall if it is not properly tuned. Although a firewall is meant to protect your computer from hackers, the security of your system can be compromised if you misconfigure or inappropriately maintain a firewall.

Also, regardless of how strong your firewall protection is, hackers can bypass the firewall if there are vulnerabilities in the systems and applications that the firewall protects. For instance, there are several vulnerabilities in Windows which the attackers can utilize to enter into your computer.

All they need to do is convince you to visit an infected web page. This makes it important for you to have an anti-virus and anti-malware software, installed on your PC or systems alongside the firewall.

Also, make sure that all applications and operating systems are patched to the latest version. If you do this, then there’s a little chance of a hacker gaining access to your system.

**Q# 6) What to look for in a Firewall?**

**Answer:** With so many options to choose from, it can be difficult to choose the right firewall for your needs.

**However, you are likely to make the right decision if you consider the following criteria for choosing the best free firewall:**

* Protection and prevention from threats.
* Visibility and control of your applications.
* Streamline security infrastructure.
* Real-time alerts
* Excellent customer support.

The above list is not exhaustive and there are several other factors to consider while choosing the best free firewall.

**List Of the Best Free Firewall**

Enlisted below are the Top Free Firewalls that are available in the market.

| **Tool/Service Name** | **Free** | **Version Features** | **Best For** |
| --- | --- | --- | --- |
| [**SolarWinds Network Firewall Security Management**](https://solarwinds.sjv.io/c/1399142/1679071/17790)  [SolarWinds_Logo](https://solarwinds.sjv.io/c/1399142/1679071/17790) | No | Real-time visibility into network firewall security, Monitoring of firewall protection configuration changes, etc. | Custom filters and sending alerts features. |
| [**ManageEngine Firewall Analyzer**](https://softwaretesthelp.com/NFA-BestFreeFirewall)  [ManageEngine](https://softwaretesthelp.com/NFA-BestFreeFirewall) | Free trial available | Log analytics and policy management software, Network security software | Network and security admins of small, enterprise-scale, private, or government IT infrastructures |
| [**System Mechanic Ultimate Defense**](https://www.jdoqocy.com/click-3783426-14457377)  [System Mechanic Ultimate Defense Logo](https://www.jdoqocy.com/click-3783426-14457377) | No | Protect Online Privacy, Remove malware, Block malware, etc. | To clean and repair your PC. |
| [**Intego**](https://offer.intego.com/Mac-AV_b19sxs7b0)  [Intego](https://offer.intego.com/Mac-AV_b19sxs7b0) | Free trial available | Inbound and outbound protection, Block untrusted connections, Two-way firewall | Mac network protection |
| [**Norton**](https://www.anrdoezrs.net/4k104p-85-7NRVWRSQUNPSSOVXVU?sid=firewall)  [Norton](https://www.anrdoezrs.net/4k104p-85-7NRVWRSQUNPSSOVXVU?sid=firewall) | Yes | Advanced protection against cyberattacks, Blocks phishing websites, Protects and monitors the home network. | Protection against viruses and cyberattacks. |
| [**LifeLock**](https://www.jdoqocy.com/5366ar-xrzEIMNIJHLEGJJIIJLL?sid=STH)  [LifeLock](https://www.jdoqocy.com/5366ar-xrzEIMNIJHLEGJJIIJLL?sid=STH) | Free trial available for 30 days. | Secure VPN, Monitor for threats, Alerts, etc. | Blocking cyber threats. |
| [**ZoneAlarm**](https://www.zonealarm.com/)  [ZoneAlarm](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/08/ZoneAlarm.jpg) | Yes | Free Antivirus + Firewall, Multiple security layers, Customizable interface, Online backup. | 5Gb of free cloud backup, Integration with many other security programs. |
| [**Comodo Firewall**](https://www.comodo.com/home/internet-security/firewall.php)  [Comodo Firewall](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/08/Comodo-Firewall.jpg) | Yes | Adblocker, Custom DNS servers, Virtual Kiosk, Windows 7, 8, and 10 compatible, Timely controls. | Streamlined for security novices, Integration with the Comodo Dragon secure browser. |
| [**TinyWall**](https://tinywall.pados.hu/)  [TinyWall](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/08/TinyWall.jpg) | Yes | No pop-up ads, Powerful scanning option, Customizable options, Wi-Fi protection, Real-time alerts Instant firewall configuration, Dedicated LAN controlling options. | No pop-ups, The auto-learn feature makes it easy to create exceptions. |
| [**Netdefender**](https://www.softpedia.com/get/Security/Firewall/NetDefender.shtml)  [Netdefender](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/08/Netdefender.jpg) |  | Simple and user-friendly interface, No pop-ups, Port scanner, Easy setup, Protection against spoofing ARF. | Simple installation process, A single click of button blocks all unwanted incoming traffic. |
| [**Glasswire**](https://www.glasswire.com/)  [Glasswire](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/08/Glasswire.jpg) | Yes | Discreet alerts, Data usage tracking, Visual network monitoring, Toolbox of network checks, Wi-Fi evil twin detection, Lock Down mode Mini graph. | Easy to use function, Ability to block programs with a single click. |