Compare operating systems

You previously explored why operating systems are an important part of how a computer works. In this reading, you'll compare some popular operating systems used today. You'll also focus on the risks of using legacy operating systems.

Common operating systems

The following operating systems are useful to know in the security industry: Windows, macOS®, Linux, ChromeOS, Android, and iOS.

Windows and macOS

Windows and macOS are both common operating systems. The Windows operating system was introduced in 1985, and macOS was introduced in 1984. Both operating systems are used in personal and enterprise computers.

Windows is a closed-source operating system, which means the source code is not shared freely with the public. macOS is partially open source. It has some open-source components, such as macOS's kernel. macOS also has some closed-source components.

Linux

The first version of Linux was released in 1991, and other major releases followed in the early 1990s. Linux is a completely open-source operating system, which means that anyone can access Linux and its source code. The open-source nature of Linux allows developers in the Linux community to collaborate.

Linux is particularly important to the security industry. There are some distributions that are specifically designed for security. Later in this course, you'll learn about Linux and its importance to the security industry.

ChromeOS

ChromeOS launched in 2011. It's partially open source and is derived from Chromium OS, which is completely open source. ChromeOS is frequently used in the education field.

Android and iOS

Android and iOS are both mobile operating systems. Unlike the other operating systems mentioned, mobile operating systems are typically used in mobile devices, such as phones, tablets, and watches. Android was introduced for public use in 2008, and iOS was introduced in 2007. Android is open source, and iOS is partially open source.

Operating systems and vulnerabilities

Security issues are inevitable with all operating systems. An important part of protecting an operating system is keeping the system and all of its components up to date.

Legacy operating systems

A **legacy operating system** is an operating system that is outdated but still being used. Some organizations continue to use legacy operating systems because software they rely on is not compatible with newer operating systems. This can be more common in industries that use a lot of equipment that requires embedded software—software that's placed inside components of the equipment.

Legacy operating systems can be vulnerable to security issues because they're no longer supported or updated. This means that legacy operating systems might be vulnerable to new threats.

Other vulnerabilities

Even when operating systems are kept up to date, they can still become vulnerable to attack. Below are several resources that include information on operating systems and their vulnerabilities.

- [Microsoft Security Response Center (MSRC)](#): A list of known vulnerabilities affecting Microsoft products and services
- [Apple Security Updates](#): A list of security updates and information for Apple® operating systems, including macOS and iOS, and other products
- [Common Vulnerabilities and Exposures (CVE) Report for Ubuntu](#): A list of known vulnerabilities affecting Ubuntu, which is a specific distribution of Linux
- [Google Cloud Security Bulletin](#): A list of known vulnerabilities affecting Google Cloud products and services

Keeping an operating system up to date is one key way to help the system stay secure. Because it can be difficult to keep all systems updated at all times, it's important for security analysts to be knowledgeable about legacy operating systems and the risks they can create.

Key takeaways

Windows, macOS, Linux, ChromeOS, Android, and iOS are all commonly used operating systems. Security analysts should be aware of vulnerabilities that affect operating systems. It's especially important for security analysts to be familiar with legacy operating systems, which are systems that are outdated but still being used.