1. Source code access (Linux kernel/windows OS)
2. Identifying & maintenance of the distribution with patches
3. User management & security
4. Non-technical staff handling configuration changes on Linux systems
5. Inbuilt tools for handling security & their support
6. Data Management- Private information disclosure
7. Vulnerability management, Incident Response, Anti-virus
8. Ease of injecting or developing malware for Linux systems
9. Regular Scanning tools & support
10. Sensitive data (ex: Auditing info)
11. Cloud support
12. Disaster management
13. Linux System & Interfaces hardening
14. Cryptographic algorithms handling & implementation
15. Authentication & Authorization

Reference- [Linux vs Windows | Find Out The 9 Most Amazing Differences (educba.com)](https://www.educba.com/linux-vs-windows/)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Features | Linux Behavior | Windows Behavior |
| 1 | Source code access (Linux kernel/windows OS) | Source code is accessible for modifications and any changes. | Windows does not have access to source code. |
| 2 | Identifying & maintenance of the distribution with patches | Searching, finding, validating & merging the patches with complete ownership by admin. | Completely managed by Microsoft. |
| 3 | User management & security |  |  |
| 4 | Non-technical staff handling configuration changes on Linux systems | As Linux is a command line interface, it is difficult to handle configuration changes. | Only admin can change the configuration settings. |
| 5 | Inbuilt tools for handling security & their support | Linux provides some inbuilt tools for | Provided by Microsoft (ex: Windows Defender) |
| 6 | Data Management- Private information disclosure |  |  |
| 7 | Vulnerability management, Incident Response, Anti-virus | Linux has segmented working environments which secure it from the attack of virus. | Windows OS is not much segmented and thus it is more vulnerable to threats. |
| 8 | Ease of injecting or developing malware for Linux systems | Limited access is given to the users and hence in case of any virus attacks, only a part of the system will be damaged. The virus won’t be able to affect the whole system as Linux does not run as root by default. | Users have full admin access over the accounts. Thus, when a virus attacks the system, it quickly corrupts the whole system. So, everything is at risk in case of Windows. |
| 9 | Regular Scanning tools & support | Linux has inbuilt scanning tools and has many advantages compared to windows |  |
| 10 | Sensitive data (ex: Auditing info) | No built-in auditing support. | Supports auditing. |
| 11 | Cloud support | Need to download from 3rd party | Inbuilt cloud support (ex: onedrive) |
| 12 | Disaster management |  |  |
| 13 | Linux System & Interfaces hardening |  |  |
| 14 | Cryptographic algorithms handling & implementation | kernel cryptography | Microsoft crypto application programming interface |
| 15 | Authentication & Authorization |  |  |