NETWORK DETECTIVE PRO™

MANAGING UNSUPPORTED OPERATING SYSTEMS AND SOFTWARE

Unsupported operating systems and software have known vulnerabilities that can easily be exploited by hackers. Computers running unsupported operating systems and software aren't protected against ransomware and data breaches. Yet most businesses don't replace old software to protect themselves, ultimately hampering their efforts to eliminate risk, comply with cybersecurity regulations and legal requirements.

WHY IT IS CRUCIAL

Everyone understands the importance of installing security patches and updates in a timely manner. Despite this, older versions of operating systems and software linger on networks and can no longer receive security updates.

When a product is no longer supported by its developer, there are limits on the measures that will be effective in protecting it against new threats. Over time, new vulnerabilities will be discovered that can be exploited by relatively low-skilled attackers - as per the *United Kingdom's cybersecurity guidance.*

Developers have lifecycles for software and expect it to be uninstalled when it no longer qualifies for patches and security updates. However, this leads to three problems:

1. Vendors don't always communicate upcoming end-of-support status to their users.
2. When it is communicated, users don't act because they don't understand the risks involved in using software that can't be patched.
3. The software keeps working as if there's nothing wrong, even though it becomes a growing risk the day the security updates stop.

Microsoft used to release an operating system and continually patch and upgrade software until its end-of-support date (usually about 10 years from its introduction).

However, with its new "*Modern Lifecycle*," Microsoft releases "feature updates;" for example, Windows 10 version 1909. The feature update receives security patches for 18 months and then must be fully replaced with a current feature update. If you continue to use Windows 10 version 1909 after 18 months, it becomes a growing risk as new Windows 10 vulnerabilities are identified and patched in current versions. You can search for Microsoft's lifecycle by software version *here*.

HOW NETWORK DETECTIVE PRO CAN HELP

Network Detective Pro creates two reports to identify unsupported operating systems and software. The Client Risk report lists Active Computers and their operating systems while the Full Detail report lets you review software programs listed in the Major Applications list. The report even gives you a roadmap to devices running old software.

It flags software known to be unsafe, like Adobe AIR and old versions of Microsoft products. Since the software has a lifecycle of 10 years, you just need to add 10 to Microsoft Office 2007 to know that it became unsupported in 2017.

Learn how Network Detective Pro helps you quickly identify and address risks posed by unsupported software.

SIGN UP FOR A FREE DEMO NOW