The Impact of Automated Software Updates and Security Patches

Nile takes care of all software updates and security patches so customers can experience an always-on, secure network.

Overview

Devices such as laptops, iPhones, TVs, tablets, and other IoT instruments have been around for decades, requiring software updates to continue delivering the experience we expect. Yet, when we see an alert indicating a software update is available, we defer it every time. Why? There is the fear of disrupting our user experience, wasting time out of our schedules, waiting while the update happens.

It is the same for the network. Our network requires regular maintenance to ensure reliable connectivity and to reduce security vulnerabilities. Software updates and security patches are a critical part of this maintenance, and like our personal devices, are delayed and pushed off. Why? These updates are beneficial to an organization's network but come with uncontrollable consequences. IT teams must consider if it's too risky to implement, will the update break something, or will business continuity be impacted if the network goes down. That can cost millions of dollars to repair and is a monumental task for IT to resolve.

For so long, the network has grown in complexities from time-consuming configurations to complex updates and patches limiting business continuity and the user experience. Nile eliminates this complexity with a service set out to fundamentally change the way networks are maintained. By providing an agile approach to software upgrades, security patches, and lifecycle management, Nile ensures the network is concrete in reliability and untouchable in security.

Implications of Software Updates

Technology is rapidly evolving in today's enterprise environment with so many new introductions of applications, devices, and infrastructure. Enhanced security, newer features, and more productivity are all results of a successful software update. Although this may sound like an ideal scenario for every business – the reality of software updates is that they are time-consuming, fear-inducing, and costly.

Businesses, small or large, must keep in mind the impact the update may have on the network and even more importantly, the user experience. Imagine if you had 20 to 25 branch offices, each requiring software updates. If something breaks or the software update is incompatible with other

technologies on your network, business continuity is hampered, the user experience is interrupted, and the organization's success is at stake. This fear steers organizations away from executing these software updates leaving employees without the tools they need to successfully collaborate with peers and the network susceptible to security threats.

> **Avoiding software updates was easier than dealing with the consequences. It's a risk due to the potential impact on network performance. The auditor finally mandated the software updates to meet compliance.**

Enhanced Security

The number one reason to implement a software update is security.[1] Within each software update, security pockets are patched to protect the network and its data. The longer software updates are delayed, the more vulnerable the network is to malware, security breaches, and other malicious threats (social engineering, man-in-the-middle, rogue devices).

Newer features and better productivity

Access to new technologies and features is a huge benefit to software updates – giving companies the opportunity to stay ahead of the competition. Without software updates, applications may contain bugs, and security flaws, and can impact network performance and business continuity.

Nile automates software updates for better performance and better security

Agility and simplicity is what Nile achieves when it comes to securing and optimizing the network for each customer. Unlike the tradition of cyclical quarterly or semi-annual software updates, Nile manages and automates the software upgrade and security patch process *for* customers. It's completely automatic and done as part of the subscription to the Nile service and happens **without impacting network uptime**. Once the software has been updated, AI-based software bots in the cloud automatically verify and validate the performance of Nile service elements and end devices. There is no longer a fear of the update impacting multiple branch offices, taking the entire network down, or leaving any vulnerable areas for malware to make its way into. There is no longer a need to plan for a time to implement the update nor a reason to have people and resources coordinated.

The Impact of Security Patches

The explosion of IoT devices and cloud applications have created more and more opportunity for security attacks. These new trends have created a network that is always on the defensive – and without protection, persistent attackers will find vulnerable areas to exploit leaving your network, data, and people vulnerable.

Companies release security patches to strengthen network security and eradicate vulnerable areas to protect the network from these malicious attacks. But if these patches are not immediately implemented, it leaves hackers with the perfect opportunity to exploit security holes and gain access to your network. 60% of breaches involve unpatched vulnerabilities[2].

As we are living through a mobile and hybrid workforce, our essential files and data are digitized. Security patches are a way to mitigate security threats and ensure that your technology is compliant with security standards, and facilitates business continuity. Similar to looking through a sea of SKUs, the complexity continues on with implementing security patches. In a recent study

polling answers from enterprise administrators, 71% found that patching is “overly complex and time-consuming” and 62% said getting patches tested and installed often takes a back seat to other tasks.[3]

Patch management is a priority for CIOs which includes identifying, prioritizing, remediating, and reporting on security vulnerabilities[4]. It’s crucial to ensure security patches are implemented across the entire network consistently.

Introducing the Era of Automated Security Patches

Avoid the compromise between network performance and network security

Nile is inherently secure, and the way the network limits entry and exit points uniquely protects the network from unauthorized access or malicious actors. Security patches are another way the network is protected – to improve security parameters and to ensure malicious actors can’t code their way in. From a tamper-resistant physical design to enforcing zero trust security outside and inside the network, social engineering, rogue devices, and security breaches are no longer threats to your network’s data or the end user.

Automation is a key element of the Nile experience – offloading software updates and security patches from IT teams so they can invest time into value-added activities. It goes beyond network connectivity and trickles down to the way the network is managed.

With Nile, your network comes with deep instrumentation that is continuously monitoring the network, and fine-tuning the network for optimal performance. As part of your subscription to the Nile Access Service, the lifecycle of your network, including the software updates and security patches, is automatically managed, ensuring that it is always-on and always-secure.

[1] Security is the number one reason to update software
[2] Cyber Security Trends in 2021
[3] Admins: Patch management is too complex and cumbersome
[4] Patch Management