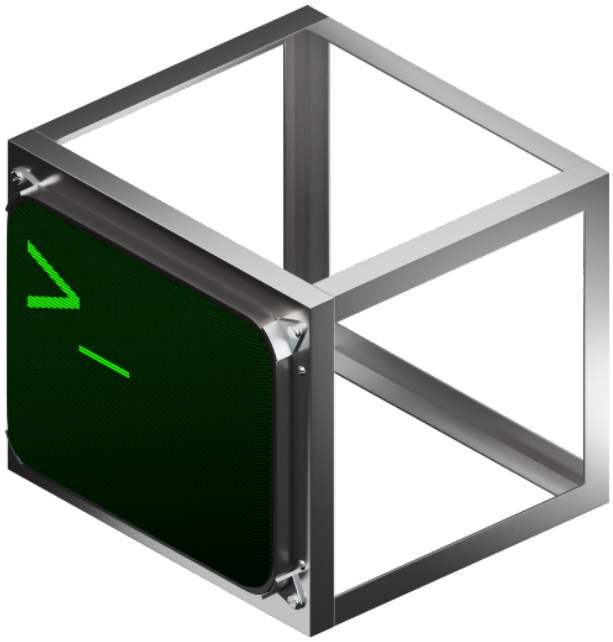
AME Privacy+ .apbx

Methodology Report

June 2025



Contents

Introduction

Despite being the leading global platform for desktop software, Windows collects excessive personally identifiable information (PII) and often compromises system stability with frequent, untested updates. The release of Privacy+ addresses these issues by providing an environment focused on maximizing privacy and ensuring reliable operation. Under direction of the Privacy+ playbook, AME client executes a removal process that surgically deletes specific core Windows components and services, including Windows Update. Unlike similar system modifications that merely disable services via scripts, Privacy+ deletes their executables from the system.

The testing methodology outlined in this document focuses on validating the removal of key services and features by the Privacy+ playbook, and represents the internal validation process by which stability, software compatibility, and privacy standards are measured during its development. The services targeted for deletion by this process have been identified as possessing the ability to add or remove data and system components at any time during the system's operation, without specific user knowledge or consent.

The goal of Privacy+ is to provide the best, and most comprehensive privacy and stability enhancement modifications for the Windows platform, packaged in an easy-to-use playbook for the AME client. Furthermore, maintaining software and hardware compatability, despite these heavy modifications to the core system, is a top priorty.

Key Features

Privacy Enhancement

- Removal of Edge & Internet Explorer, OneDrive, Windows Update, Windows Defender, AppLocker, Server Initiated Healing, Microsoft Store, DiagTrack, cloudidsvc, AgentService, InstallService, and many other smaller services
- Specialized firewall rules for Settings, Explorer, Start Menu Search, and cryptsvc
- Hundreds of privacy-related changes to the registry
- Overall reduction of network traffic by over 95% compared with a regular Windows system
- Replacement of many core apps with open-source alternatives

Reliable Operation

- Removal of Windows Update ensures an unaltered system state
- Removal of Windows Defender reduces utilization spikes
- A focus on disabling / removing various network traffic incurring services eliminates the possibility of alterations to the system without user consent

Quality of Life

- Optional improvements to the Windows UI
- Included Privacy+ Settings companion app for managing system settings
- Retained compataility with most Win32 programs and games

Overview

AME Beta, developed by Amelabs, is a versatile tool designed to customize Windows environments through modular configuration files known as playbooks. The Privacy+ playbook stands out by targeting privacy and stability, removing core Windows components and services such as Windows Update and DiagTrack that harvest PII and introduce instability through untested updates or background activity. By deleting these components executables rather than merely disabling them, Privacy+ ensures a permanent reduction in data transmission and a more reliable system. This section explores how AME Beta and Privacy+ work together to deliver a robust solution for users seeking a privacy-focused, stable Windows experience.

The Challenge

Windows, by default, engages in extensive automated interactions with Microsoft servers, including telemetry, diagnostic data, update checks, and cloud synchronizations. These processes often transmit PII without explicit user consent, compromising privacy. Additionally, frequent updates sometimes inadequately tested can destabilize the system, leading to crashes, performance issues, or hardware incompatibilities. Privacy+ tackles these challenges head-on by identifying and eliminating components that enable unwanted data transmission and erratic system behavior, ensuring users retain control over their data and system reliability.

Methodology

To achieve its privacy and stability goals, Privacy+ relies on a meticulous analysis process to identify and target problematic components. This section outlines the tools and methodology used to detect unwanted data transmissions and unstable services, achieving two core objectives: enhancing the playbook's efficiency and privacy protections through continuous iteration, and demonstrating its edge over rival solutions via robust benchmarking. To achieve this, we employ a structured process supported by industry standard tools like Wireshark for detailed network traffic analysis, Network Monitor for real-time system insights, and AME Beta for seamless playbook deployment and testing. These tools collectively enable us to monitor, analyze, and refine system performance with a high degree of accuracy.

Network Analysis

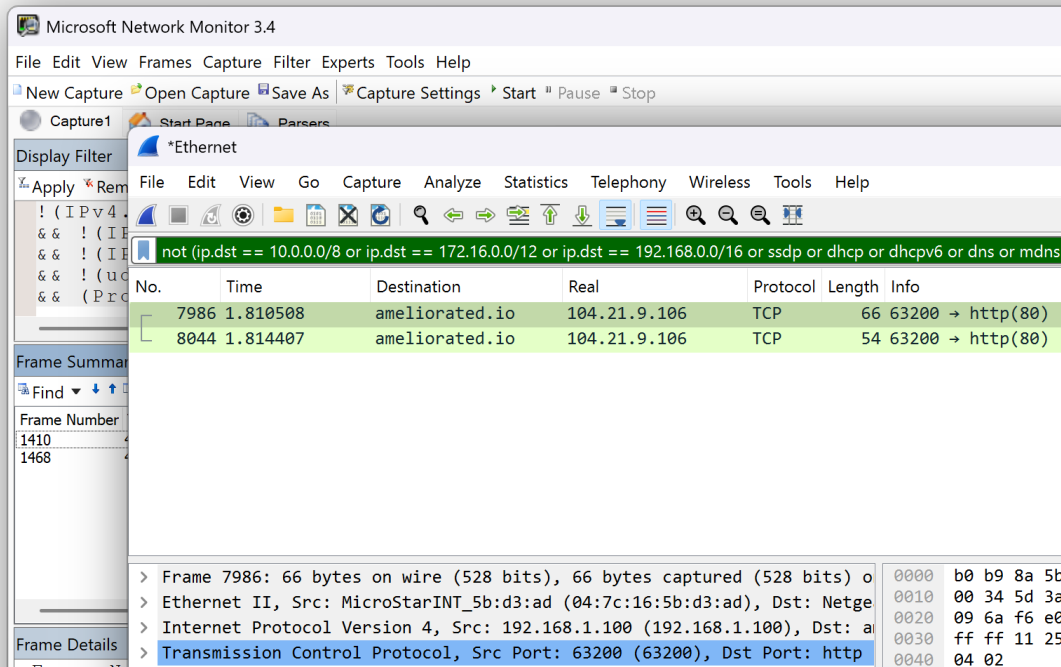
The analysis follows a structured approach: First, network traffic is captured with Wireshark to detect unwanted transmissions. These transmissions are then traced to specific processes or services using Network Monitor. Next, the privacy impact and stability risks of each identified component are assessed. Finally, appropriate elimination techniques are selected to remove or block the offending components. This methodology ensures Privacy+ achieves a near-silent network profile and a stable system state.

Wireshark: Capturing Network Packets

Wireshark, an open-source network protocol analyzer, captures real-time network packets to identify privacy-infringing transmissions. It reveals contacted domains, unencrypted data, and connection frequency, enabling Privacy+ to pinpoint and eliminate telemetry and update-related traffic.

Network Monitor: Tracing Processes

Network Monitor 3.4 complements Wireshark by tracing packets to their originating processes or services. This step is vital for identifying components like Windows Update or DiagTrack that compromise both privacy and stability, allowing Privacy+ to target them for deletion.



Detailed Testing Steps

To validate Privacy+'s effectiveness, a comprehensive testing process is employed. It begins with setting up a virtual machine (e.g., VMware or VirtualBox) running a clean installation of Windows 11. Once Windows is setup, Network Monitor 3.4 is installed inside the environment. Wireshark is then configured on the host system to capture internet-bound traffic originating from the virtual machine's network adapter (e.g., "VMware Network Adapter VMnet01") and applying a filter to exclude local traffic, such as:

```
not (ip.dst == 10.0.0.0/8 or ip.dst == 172.16.0.0/12 or
ip.dst == 192.168.0.0/16)
```

The capture runs for one hour while Network Monitor simultaneously traces the traffic to specific processes. After stopping both captures, the data is analyzed: Wireshark's display filters isolate Microsoft-related traffic, and Network Monitor's "Process" column links this traffic to processes like svchost.exe. Findings are documented by recording packet counts and unique transmissions for both stock Windows and Privacy+ configurations, allowing for a direct comparison to confirm reductions in traffic and improvements in stability. This process ensures Privacy+'s modifications are thoroughly validated.

Results and Validation

Testing on Windows 11 (Build 22631.3593) in a virtual machine over one hour demonstrates Privacy+'s impact. Privacy+ v0.7 generates only 103 packets and 4 unique transmissions, a stark contrast to stock Windows' 2688 packets and 127 transmissions, and O&O ShutUp10++'s 1104 packets and 57 transmissions. This significant reduction in network activity, paired with maintained system stability and compatibility, validates Privacy+'s approach to enhancing privacy and reliability, outperforming alternative solutions.

	Packets	Transmissions (unique)
Windows 24H2	2688	127
O&O Shutup10++	1104	57
AtlasOS 4.0.0	1109*	15
ReviOS 3.23.12	3331-148*	16-7*
Privacy+ v.0.7	103	4

Testing Footnotes

Testing Environment:
All tests were conducted on a fully updated Windows 11 virtual machine (Build 22631.3593) using an identical snapshot for each capture to ensure consistency. Testing was performed on Friday, May 31, 2024.

Measurement Precision:
The results are based on one-hour captures from system boot to shutdown. While this provides a snapshot of network activity, it may not fully account for periodic or sporadic transmissions. Future studies will incorporate averaged 24-hour measurements for enhanced precision.

Variability in Results:
Minor fluctuations in timing and system state can influence network activity. For instance, ReviOS* Measurement One exhibited higher-than-expected traffic, likely due to Windows Update activity, while Measurement Two showed a more typical, reduced traffic profile. Similarly, AtlasOS* displayed notable variability, potentially stabilized by a subsequent reboot. This variability highlights the significant volatility in network traffic observed with these solutions, in contrast to the consistent, stable performance achieved through Privacy+'s modification approach.

Traffic Filtering:
Internet packet counts exclude local traffic and basic services (e.g., time synchronization) using the following Wireshark filter:
not (ip.dst == 10.0.0.0/8 or ip.dst == 172.16.0.0/12 or ip.dst == 192.168.0.0/16 or ssdp or dhcp or dhcpv6 or dns or mdns or llmnr or ntp) and (tcp or udp)

Unique Transmissions:
This metric groups related packets into a single transmission to reflect distinct connections. For example, 500 packets exchanged with microsoft.com in a short period are considered one unique transmission.

Testing of AtlasOS:
AtlasOS v4.0.0 tested on Windows 11 VM (Build 22631.3593), using the optional "Disable Defender" feature (not default) to further reduce traffic. One-hour capture: 1,109 packets, 15 transmissions. A reboot may stabilize these results, as seen with ReviOS.

Testing of ReviOS:
ReviOS v23.12 tested on Windows 11 VM (Build 22631.3593), using default options. One-hour captures: Measurement One: 3,331 packets, 16 transmissions due to Windows Update. Measurement Two (after subsequent reboot): 148 packets, 7 transmissions.

APPX Removal

Windows comes pre-installed with numerous APPX packages, also known as Microsoft Store apps, many of which connect to Microsoft servers, transmitting telemetry and consuming resources. Privacy+ targets these packages to enhance privacy while preserving essential system functionality.

Non-system APPX packages can be removed using standard commands, such as PowerShell's `Remove-AppxPackage`. However, system packages, like `Client.CBS`, present a challenge. These are flaged as unremovable, preventing standard removal methods.

Introduced with Windows 11, the `Client.CBS` package bundles multiple apps, including `Globals.IrisService` (which drives Windows Spotlight wallpapers) and `WebExperienceHost` (the "Getting Started" app). Removing `Client.CBS` entirely isn't viable, as it includes critical components like File Explorer. Unlike typical packages, its individual apps can't be isolated for removal using conventional methods.

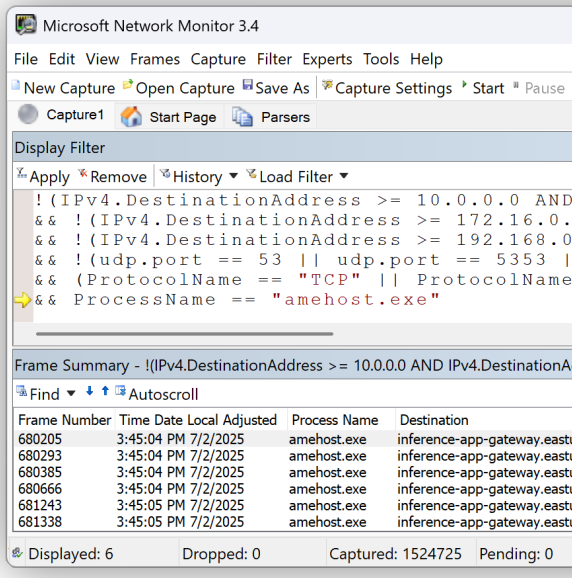
Privacy+ overcomes this by directly modifying the APPX database, deleting any unwanted sub-components, such as `Globals.IrisService` and `WebExperienceHost`, from the `Client.CBS` package. This custom approach ensures effective telemetry reduction without destabilizing the system by leaving the rest of the package intact.

With Privacy+, all APPX packages—system and non-system—are handled using this specialized method, replacing traditional commands for a more thorough, powerful, and non-destructive uninstallation process.

Firewall Rules

When removal isn't feasible, Privacy+ uses Windows Firewall to block outbound traffic from specific executables, stopping suspect traffic while preserving functionality. For instance, the Windows Settings app, which sends telemetry during navigation, is restricted via firewall rules to maintain functionality without successful outbout transmissions.

Services hosted by svchost.exe, which supports multiple system services, are more difficult. Blocking svchost.exe entirely would disrupt critical operations. Privacy+ creates a renamed duplicate (`amehost.exe`), reconfigures the target service to use it, and applies a tailored firewall rule to block it. This isolates telemetry from specific services without affecting others, showcasing Privacy+'s adaptive privacy approach.



Screenshot of Microsoft Network Monitor 3.4 displaying outbound network **packets isolated by amehost.exe**. This allows for the traffic to be entirely blocked with a firewall rule, without hampering the functionality of other services that may need internet for legitimate purposes.

Potential Improvements

Privacy+ has made substantial strides in minimizing telemetry, achieving levels significantly lower than those observed in a standard Windows installation. This results in a system with exceptionally low network activity. Nevertheless, the pursuit of excellence is ongoing, and several opportunities for further enhancement have been identified. These improvements focus on both reducing residual telemetry and refining the methodologies employed in Privacy+ development.

Replacing OS Components

With Privacy+ v0.8, ISO-injection was introduced, replacing the default OOBE with an Amelabs-designed version that applies the playbook at boot. Further improvements to this OOBE could reduce background traffic during this phase. Open-Shell, enhanced with a custom theme, eliminates start menu-related network activity. However, the default start menu, if used, generates traffic blocked by our extensive firewall rules. A fully custom-designed start menu could eliminate this entirely, offering peace of mind, resistance to any Microsoft alternations, and a smoother user experience. Copilot is stripped out to halt network-dependent operations; exploring local AI solutions could provide a functional, privacy-respecting alternative.

Traffic Remnants

Privacy+ successfully eliminates the vast majority of telemetry; however, a small number of exceptions persist. Efforts are underway to address these remaining instances. The following list highlights key areas under investigation, though it is not exhaustive due to the evolving nature of this work:

- **Windows Push Notifications:** The WpnService, which facilitates app notifications from servers, intermittently connects to `wns.notify.trafficmanager.net`. This traffic appears benign, as it is required for notification functionality. Nonetheless, an option to disable this service is being considered for users who prefer to eliminate all such network activity entirely.
- **Sign-In Assistant Service:** The `wlidsvc` service, necessary for launching newly installed APPX/UWP applications, occasionally establishes connections to Microsoft domains. Potential solutions are being explored, though traditional firewall rules are ineffective here, as the service requires network access to operate correctly.

Conclusion

Testing demonstrates Privacy+'s effectiveness in minimizing telemetry and enhancing system stability in Windows environments.

For users seeking a balance of privacy and usability, Privacy+ offers a compelling solution. Its minimal telemetry footprint reduces exposure to data collection, while its focus on stability ensures reliable performance for everyday computing tasks. In a landscape of privacy tools, Privacy+ distinguishes itself through these measurable outcomes, providing a practical, evidence-based approach for privacy-conscious Windows users.

Threat Model Considerations

Privacy+ is designed for users who prioritize privacy and stability in typical computing scenarios, such as personal or professional use where data collection is a concern but extreme anonymity is not required. It is not intended for high-risk users—such as journalists who travel to conflict areas, or other individuals requiring absolute anonymity—who may face advanced surveillance or targeted attacks. In such cases, specialized operating systems like TailsOS or QubesOS, which prioritize security and anonymity over usability, are more appropriate. Privacy+ is optimized for everyday privacy needs, not for countering sophisticated threats.