Windows 10 and the Anti-malware Ecosystem

Dennis Batchelder
Director, Antimalware strategy

Microsoft

We shipped Windows 10!

Recap: The Windows 10 upgrades process for AVs

- Our AV upgrade plan
  - If the AV product is Windows 10-compatible, auto-upgrade
  - Else, if the AV product has passed MS certification tests, offer for upgrade after 3 hours, and again on every reboot
  - We presented this plan in Docs, MVI meetings, and at MSRA in July

- When we presented, AVs had the following concerns
  - No time to upgrade products to Windows 10-compatible versions
  - Customers would never see/click on the pop-up
  - Customers would never reboot, see the pop-up, etc.

- We said we'd measure and report the results

What we measured

Data used: MSRT and Windows Defender telemetry

Caveats:
- data only through September 13
- not all machines run MSRT each month
- this is early in the Windows 10 upgrade process
- some issues mapping machines across OS installs
- imperfect mapping of AV vendors

Region	UpgradeShare	Unprotected	Infected
Africa	1.0%	17%	13%
Asia	15.3%	19%	6%
Australia	2.7%	12%	4%
Central America	0.5%	15%	9%
Europe	39.1%	13%	6%
Middle East	1.6%	18%	12%
North America	32.2%	13%	4%
Pacific	0.4%	16%	11%
South America	7.3%	14%	9%
Grand Total	100%	14%	6%

First: MSRT saw as Win 7/8	Then: Windows Defender saw as Win10	Finally: MSRT saw as Win 10	We called this	How many we measured	What else we measured:	Then we calculated:
Yes	No	Yes	Auto-upgrades	10 million	• Country • Vendor	
Yes	Yes	Yes	Offer-upgrades	46 million	• Country • Offered vendor • Eventual vendor • AV protection state • Windows Defender infections found • Days Windows Defender was active	• OfferRetention • OfferBonus • FirstDayRetention
No	n/a	Yes	Fresh installs	24 million	• Country • Vendor	

So how did AV vendors fare?

--- *the biggest affecting factor:*

1) Net change: AV vendors retained most customers who upgraded Windows 10
2) 77% of machines did not have on-box Windows 10-compatible AVs for auto-upgrades, causing us to offer upgrades

--- *then when we had to offer AV after the upgrade:*

3) The majority of machines were retained by AV vendor
4) The majority of retained machines occurred on the first day
5) Many customers chose to switch 3rd party AV vendors after the offered upgrade
6) Very few machines with out-of-date or disabled AVs were retained by AV vendor
7) Few machines where Windows Defender found infections were retained by AV vendor
8) No machines with missing Windows-10 compatible AVs were retained by AV vendor

Suggestions to increase AV retentions on Windows 10 upgrades

1) Avoid offer-upgrades
   - Get your AV ready for auto-upgrades by making it Windows 10-compatible

2) If that fails, make sure you have a Windows 10 AV for us to offer
   - Otherwise customers won't have a fast path to install your product after upgrade

3) And, encourage your customers to enable your product
   - Unprotected customers aren't staying with their original AV vendor

4) Also, reduce your infection rates
   - Infected customers aren't staying with their original AV vendor

5) Promote your product/brand as Windows 10-ready
   - Ride the wave of upgrades and maybe pick up some new customers ☺

Antimalware Platform on Windows 10

Antimalware Platform

- The Antimalware Platform (AMP) is a Windows-based effort to ensure that all Windows 10 users are protected from malware by an antimalware app that provides synchronous protection using updated signatures.

- Microsoft invests in platform features that help protect our common customers. Many AMs take advantage of: ELAM, Secure Events Channel, AM-PPL, etc.

- Guidelines are required to keep the platform healthy and growing.

Antimalware Platform Whitepaper: Requirements for Windows 10

The AMPW requirements focus on three primary areas :

1. **Performance** requirements detail the metrics that will be used to ensure that antimalware software does not unnecessarily degrade the user experience. The metrics being used revolve around boot, browser launch, browser page display, and Windows Store app time.

2. **Reliability** requirements have been added in order to make sure customers are able to receive and install timely security and operating system updates. This boils down to not using undocumented APIs and data structures.

3. **User notifications**:

    a) AM apps must make exclusive use of User Protection Always On (UPAO) notifications that WSC provides to notify users that the app may expire soon, and enable users to proactively take action to renew their subscription.

    b) We have revised the other notification requirements in Chapter 9 to be objective and measurable, and these requirements will be included in the next version of the Whitepaper.

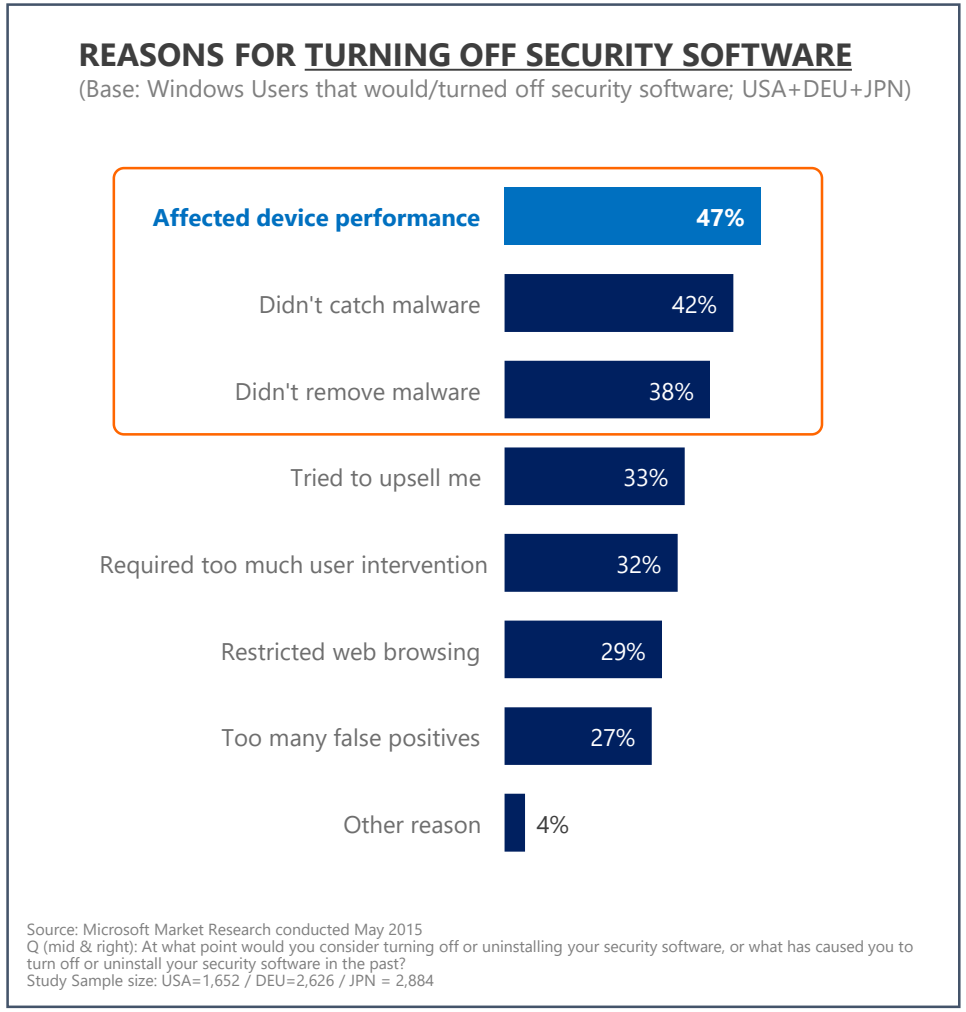
MVI members received this whitepaper (v2) on 2 July 2015

Motivation for AMPW Requirements

1. Current RTP software has a **dramatic impact on performance**, leading to a poor user experience. Performance impact is also a significant contributor to users turning RTP off, and thus making it less secure.

2. Necessary system updates and **upgrades are sometimes blocked** by RTP software's use of undocumented APIs and data structures, resulting in customer frustration, as well as customers being left in a less secure state.

3. Many antimalware applications generate an **excessive number of alerts**. This not only leads to a poor user experience, but could also habituate the user to dismissing alerts if out of hand, thus missing out on truly urgent notifications.



AMP Engagement Calendar

- **Windows *is* a Service (WaaS)**
  - 75 million devices in 1st month.
  - We'll deliver new features when they're ready, not waiting for the next major release.
  - *You should too!*

- **White Paper & Requirements updates to match Windows releases**
  - We'll update the white paper up to three times a year, aligned with Windows releases.*
  - Your timely feedback on draft requirements is very important.

- **Continue regular engagement with our AM partners**
  - Today at Virus Bulletin
  - December in Da Nang, Vietnam (AVAR)
  - February in San Diego (AMTSO)
  - May in Bucharest (CARO)
  - July in Redmond (MSRA)

* Microsoft reserves the right to change this schedule as required to keep our customers safe.

Platform Updates

Windows 10 AMP Improvements

- **AM-PPL: Antimalware Protected Process Light**
  - AM processes can run critical user-mode service components as AM-PPL which is at a higher level than an Admin thus can help shield itself from admin level malware
  - White paper on MSDN
- **Secure Event Channel**
  - Extensible channel that provides critical insight into process activities
  - AMs can listen to selected TCB/kernel/win32 level events without kernel level hooks
  - TCB/kernel events are trusted, they cannot be tampered with by malware
  - Whitepaper published via Connect in Feb 2015.
- **Inbox support for Offline Cleaning**
  - WSC provides API to AM apps to make use of inbox WinRE (Windows Recovery Environment) to provide seamless frictionless offline cleaning experience.
  - AM applications can remove rootkits and kernel malware difficult to clean online using this feature, without a need to carry their own offline environment.

We will be encouraging you to use these as undocumented API replacements

Upcoming API Deprecations

- **Anti Spyware component in Windows Security Center (WSC) will be deprecated**
  - WSC will support only Anti-Virus but not Anti-Spyware
  - Converging will simplify AM management through WSC
  - All the existing APIs will continue to work, and will gracefully ignore Anti-Spyware registration/status

- **WDEnable API will be deprecated (MSDN link)**
  - Windows Defender status that the calling application wants to set. **TRUE** enables Windows Defender. **FALSE** disables Windows Defender.
  - This API will be deprecated.
  - WSC is the only supported way to disable Windows Defender

- **Timeline for Change**
  - Anti Spyware component deprecated: July 2016*
  - WDEnable API deprecated no later than July 2016*

* Microsoft reserves the right to change this schedule as required to keep our customers safe.

Reliability

Real World Problems with Current Reliability

Example 1

Internal testing showed that Windows would suffer BSOD when receiving a security update if the user had AM software from a particular vendor. The update was delayed for the entire world for a month. When it did ship, Windows Update detected if that vendor's software was present and didn't install the update, leaving those customers insecure until the vendor issued their own update.

Root cause: relying on undocumented data structures.

Example 2

Another vendor's AM software blocked upgrades to Windows 10.

Root cause: the software was parsing signature information directly, rather than using the publicly documented crypto APIs.

Windows 10 AMP Reliability Requirements

- Antimalware apps for Windows 10 **must not** use any undocumented, unsupported or private Windows APIs or data structures.

- Antimalware apps for Windows 10 should use Microsoft-documented APIs and data structures for which documentation is:
  - Publically available via the Microsoft Developer Network, and/or
  - Privately shared with antimalware ISVs via the Microsoft Virus Initiative or Virus Information Alliance.

Our goal is to improve reliability, not limit your ability to detect block or remove malware.

Update on API lists sent to Microsoft

- **Since July:**
  - Received more than 1000 requests from 12 ISVs → 700+ unique APIs and data structures.
  - Volume much higher than expected.
  - We've triaged many of them, sent some back to you via Sysdev for more info.

- **Themes have emerged:**

General Use case	How it is done	Supported Mechanism to Consider
System observation for detection purposes	Hooking/interception of undocumented APIs for parameter inspection. Writing signatures to match calling patterns associated with known malicious behavior.	Secure Event Channel Filter Drivers
System observation for self-preservation purposes	Hooking/interception of undocumented APIs for parameter inspection. Looking to match calling patterns associated with known malicious behavior with their own processes/resources as the target.	AM-PPL
Direct modification of APIs/Data Structures for remediation purposes	Invocation of undocumented APIs or changes made to in-memory data structures as part of cleaning a detected threat.	WinRE Offline Cleaning

Performance

Why is Performance Important?

- According to Microsoft research, 19% of consumers who pay for security software rate performance as one of their top three criteria for purchasing.

- According to the same study, 47% of users who turned their security software off did so because of how they perceived it affected device performance. This was the number one reason cited for disabling security software.

- A Forester Research study concluded that performance was the second most important criteria (behind reliability) for purchasing a new PC.

The AM ecosystem has noted the importance of performance

Performance Requirements

For a given metric, a system falls into one of three categories, based on measured performance: *exceptional*, *on target*, or *strong concerns.*

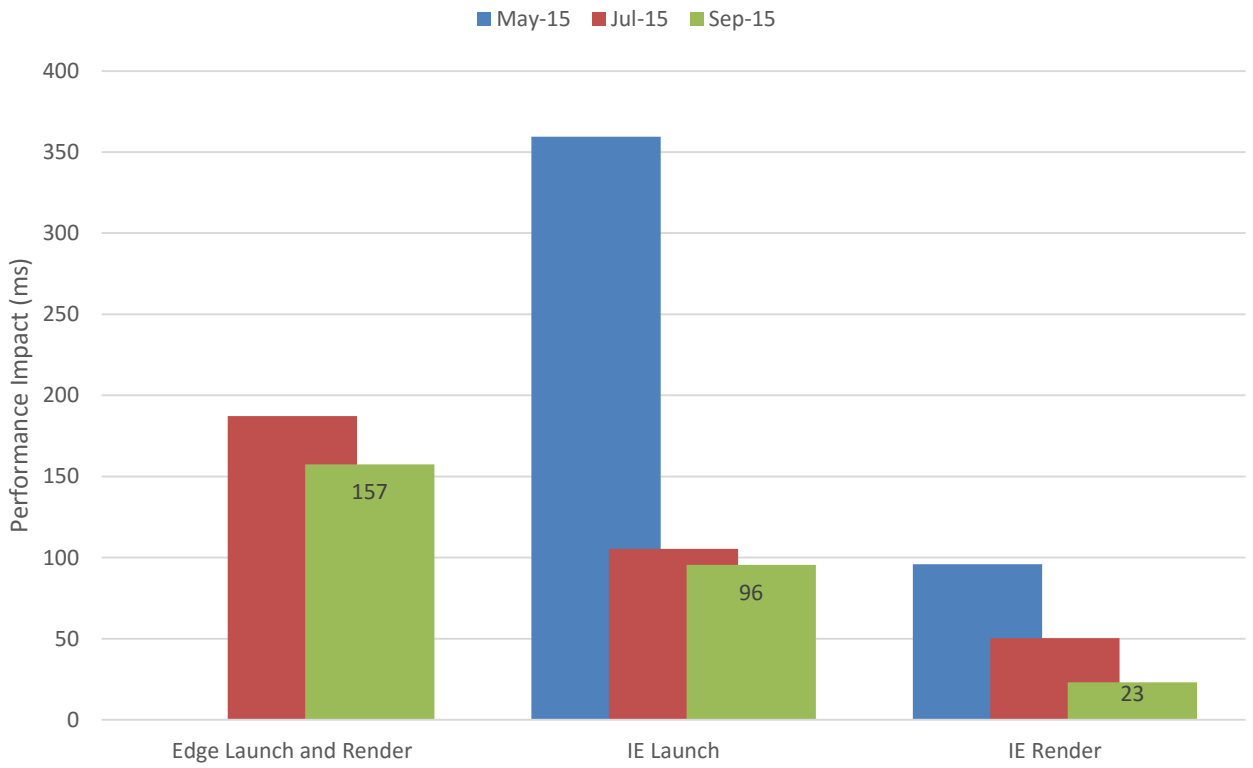
For each of the four metrics, we run the test twice, once without the 3rd party AM software and once with it.

For each of the four metrics, a system must be in the same measured performance category with the 3rd party AM software as it was without it. If it does, it passes for that metric. If it doesn't, but the performance degradation was less than 20% or less than 200ms, then it still passes.

There are eight predefined off-the-shelf systems with varying characteristics that are used for testing. The antimalware must pass for all 4 metrics on all 8 systems in order to be compliant

ADK Assessment	Metric and units
Boot Performance (Fast Startup)	Total Boot [Excluding BIOS] Duration in seconds
Internet Explorer Startup Performance	IE Startup Duration (User Perceived) in seconds
Internet Explorer Security Software Impact	Page Display Time in seconds
Windows Store App Performance	Launch time in seconds The evaluated metric will be an average of the launch time of all Bing apps on the system.
Microsoft Edge Performance	Navigation time in seconds

Performance Progress



"The ADK enabled us to make double digit improvements for many perf metrics across low/mid/high end platforms. For some metrics we observed 30% ~50% improvements."

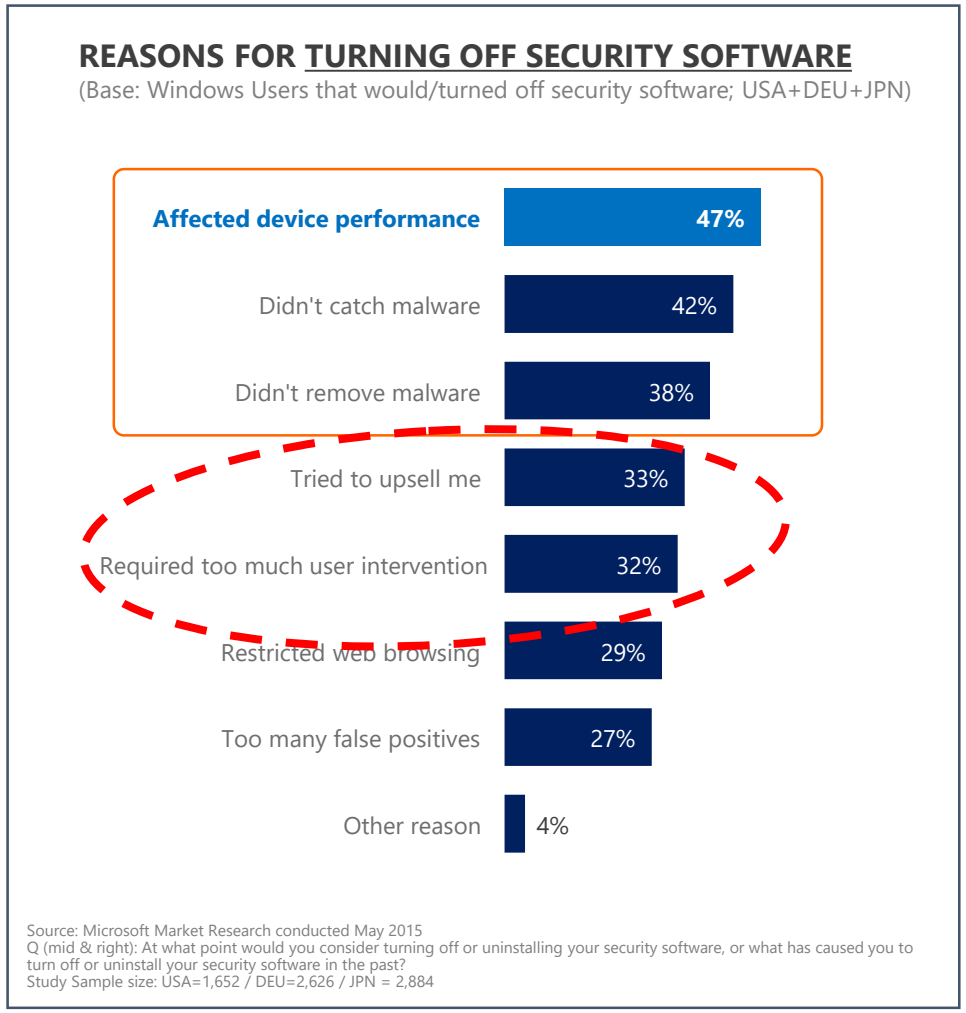
--AM vendor performance engineer

Do not delay in submitting your app for performance testing. See submission details in the white paper.

Notifications

Problems with Current Notifications

- Alerts that are modal and display on top of whatever other applications the customer has open
- Alerts that do not leverage Windows Notification Services (WNS)
- Alerts that are not always clear or actionable to the customer (Ex: “Unknown device or PC detected”)
- Alerts that are shown to the customer by default, with no option within the desktop app to turn off alerts.
- Frequent pop-ups for marketing or sales purposes



User Protection Always On (UPAO) Requirement

User Protection Always On:

- Antimalware apps must use UPAO notifications that WSC provides to notify users that the app may expire soon, and enable users to proactively take action to renew their subscription.
- This requirement has been published since March 31st 2015 in the AMPW, and it will be enforced by February 1st 2016. This enforcement date will not be extended.

Notifying Users Before Expiration

- WSC provides an API for antimalware apps to notify users 5 days prior to the app's expiration date. AM apps must:
  - Register with WSC to report their apps correct status as expired.
  - Notify the user through the provided API. (They cannot notify the user outside of the API.)
- Requirements to prompt users before the antimalware app expires. AM apps must:
  - Be active, enabled, and not out of date.
  - Be close to its expiration date.
  - Invoke the UPAO scenario, but no more than 2x's in a 30 day period.

Windows 10 Notification Requirements – **Updated**

Windows 10 Notification Requirements:

1. Non-critical information, no user action required
   - Use a toast message with Suppress-Popup = TRUE.
   - Notification will show up directly in the Action Center
2. Non-critical issue, may or may not be due to malware issues
   - Use a toast notification.
   - No more than once per 24 hours
3. User action or decision needed, not a malware threat
   - Use a toast notification
   - No more than once per 72 hours

Windows 10 Notification Recommendations:

- Critical malware issues
  - Use current notification service via AM
  - Can use toast notifications, is desired.

Please send any feedback you have on WNS to: ECOAV@microsoft.com by 10/16.


We heard your
Feedback

Upgrade.exe
UX Changes

Post-upgrade notifications: antimalware

- Feedback is consistent
  - Users want to be informed about their protection state
  - Toast notification is not prominent enough
- Adjust messaging to ensure users are informed of state and choices
  - Notify users as soon as possible, rather than 3 hours after OOBE
  - Ensure users know that they have protection (Windows Defender)
  - Users can quickly fetch a compatible version of their third party antimalware if upgrade.exe is present
  - Better way to notify users (e.g., system modal dialog, persistent toast, etc) upgrade.exe isn’t present, offer users options on landing page

Summary

√	Newly enforced in February 2016
√	Newly enforced in July 2016

Summary

- Ship a Windows 10 compatible app before your customers upgrade.
- Feb 2016 enforcements include Perf, UPAO and notifications.
- Please send us feedback on revised notifications requirements by 10/16.
- Start preparing now for the No undocumented API requirement in July.

Scenario	Detailed Scenario	By July 2015	By February 2016	By July 2016
Fast Startup	Total boot duration	-	√	√
App Launch	Internet Explorer startup performance	-	√	√
Responsiveness	Internet Explorer Security Software impact	-	√	√
	Windows Store apps performance	-	√	√
Browsing	Microsoft Edge performance	-	√	√
Energy Efficiency	Streaming video playback	-	-	√
File Operations	File Copy	-	-	√
OOBE	OOBE duration	-	-	√
User Experience	Upgrade.exe	√	√	√
	No additional apps promoted through Upgrade.exe	√	√	√
	Using Notifications In Windows 10	-	√	√
	No undocumented APIs	-	-	√
	User Protection Always On	-	√	√

Q&A