Fact: Chrome rules the world.

Now with 69.2% of the world's browser user share – a measure of browser activity calculated by California-based analytics company Net Applications – Google's Chrome has no equal, at least in popularity. Rivals like Microsoft's Edge, Mozilla's Firefox and Apple's Safari eke out single digits, while niche browsers under them fight over the smallest scraps.

It's no surprise, then, that when Chrome speaks, everyone listens, whether about each browser upgrade – something Computerworld tracks in the What's in the latest Chrome update? series – or about Google's plans for the future.

Every Chrome upgrade is accompanied by enterprise-centric release notes that highlight some of the planned additions, substitutions, enhancements and modifications. We've collected the most important for this what's-coming round-up.

Just remember, nothing is guaranteed. As Google says: "They might be changed, delayed, or canceled before launching to the Stable channel."

Chrome 84: Full-page TLS 1.0, 1.1 warnings

Last year, Google spelled out the stages of warnings it would put in front of Chrome users about obsolete TLS (Transport Layer Security) 1.0 or 1.1 encryption. A first step – a "Not Secure" alert in the address bar – was taken in January 2020.

With Chrome 81, the browser was to display a full-page interstitial alert that interrupted attempts to reach the destinations secured with TLS 1.0 or 1.1. That schedule, however, was abandoned in early April.

[Become a Microsoft Office 365 administrator in record time with this quick start course from PluralSight.]

Now, it's Chrome 84, slated for release July 14, that is to contain the page-sized warning.

IT administrators can disable both warnings with the SSLVersionMin policy. Setting that policy to "tls1" allows Chrome to connect to TLS 1.0- and 1.1-encrypted sites sans alerts. The SSLVersionMin policy will work until January 2021, when it will be deprecated.

Chrome 84: Risky downloads, rescheduled

Starting with Chrome 84, the browser will warn users when executable files begin their downloading from a secure page (one marked as HTTPS) but actually transfer their bits over an insecure HTTP connection. "These cases are especially concerning because Chrome currently gives no indication to the user that their privacy and security are at risk," Joe DeBlasio, a software engineer on the Chrome security team, wrote in a Feb. 6 post announcing the scheme.

At the time, Chrome 81 was pegged to begin the warnings. But as with the TLS 1.0 and 1.1 alerts, these were rescheduled in early April, pushed back to later versions of the browser. Google did not say aloud what prompted the change, but it likely was related to the March decision to pause Chrome's release cadence and when distribution was restored, abandon Chrome 82, skipping from 81 to May's 83.

With Chrome 85, set to ship Aug.25, Google will drop the hammer, barring those executable files from downloading.

Over several more versions, Google will warn, then block, additional file types, including (in order)

archives such as .zip; "all other non-safe types, like .pdf and .docx; then finally image files, such as .png. For example, Chrome 85 will institute warnings for archives (and Chrome 86 will block them).

By Chrome 88 (a Jan. 19, 2021, appearance), the browser will be blocking "all mixed-content downloads."

Organizations managing Chrome can disable this future blocking on a per-site basis with the InsecureContentAllowedForUrls policy.