# Security Now! #638 - 11-21-17

## Quad Nine

### This week on Security Now!

This week we discuss, Windows having a birthday, Net Neutrality about to succumb to big business despite a valiant battle, Intel's response to the horrifying JTAG over USB discovery, another surprising AWS public bucket discovery, Android phones caught sending position data when all permissions are denied, many websites found to be watching their visitors' actions, more Infineon ID card upset, the return of BlueBorne, a new arrival to our "Well... THAT didn't take long" department, speedy news for Firefox 57, some miscellany, listener feedback, and a look at the very appealing and speedy new "Quad9" alternative DNS service.

### Our Picture of the Week

HUMAN RESOU
klossner

" WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US. HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

## Security News

**Yesterday, November 20th, Microsoft Windows turned 32.**

- November 20th, 1985 was RTM for Windows 1.0
- December 9th, 1987 was RTM for Windows 2.0
- May 22, 1990 was RTM for Windows 3.0

**Bye Bye Net Neutrality**

Today, FCC’s chairman, Ajit Pai, who has made the reversal of the previous administration's net neutrality protections one of his top priorities unveiled the FCC's plan to give Internet providers broad powers to determine what websites and online services their customers can see and use, and at what cost. In other words, the end of federal government enforced Net Neutrality. The final decision, to be put to a vote next month on Thursday, December 14th -- in just over three weeks -- is expected to pass if the votes falls along political party lines since the Ajit Pai's Republican party holds three of the co

**Intel responds quickly to the horrific "JTAG over USB" research:**

Intel's disclosure reveals that 9 years of their chips are affected.

Intel Management Engine Critical Firmware Update (Intel SA-00086)
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr

Corporate Speak:

> Intel: "In response to issues identified by external researchers, Intel has performed an in-depth comprehensive security review of our Intel® Management Engine (ME), Intel® Server Platform Services (SPS), and Intel® Trusted Execution Engine (TXE) with the objective of enhancing firmware resilience. As a result, Intel has identified security vulnerabilities that could potentially place impacted platforms at risk."

Systems using ME Firmware versions 11.0/11.5/11.6/11.7/11.10/11.20, SPS Firmware version 4.0, and TXE version 3.0 are impacted.

Based on the items identified through the comprehensive security review, an attacker could gain unauthorized access to platform, Intel® ME feature, and 3rd party secrets protected by the Intel® Management Engine (ME), Intel® Server Platform Service (SPS), or Intel® Trusted Execution Engine (TXE).

This includes scenarios where a successful attacker could:

- Impersonate the ME/SPS/TXE, thereby impacting local security feature attestation validity.
- Load and execute arbitrary code outside the visibility of the user and operating system.
- Cause a system crash or system instability.
- For more information, please see this Intel Support article

Intel® Management Engine Critical Firmware Update (Intel SA-00086)
https://www.intel.com/content/www/us/en/support/articles/000025619/software.html

Affected products:

6th, 7th & 8th Generation Intel® Core™ Processor Family
Intel® Xeon® Processor E3-1200 v5 & v6 Product Family
Intel® Xeon® Processor Scalable Family
Intel® Xeon® Processor W Family
Intel® Atom® C3000 Processor Family
Apollo Lake Intel® Atom Processor E3900 series
Apollo Lake Intel® Pentium™
Celeron™ N and J series Processors

Intel-SA-00086 Detection Tool (Windows & Linux)
https://downloadcenter.intel.com/download/27150

Lenovo IME Updates:
https://support.lenovo.com/us/en/product_security/len-17297

**Another case of an exposed AWS Bucket (okay... three, actually)**
Chris Vickery of UpGuard, who has recently been discovering open and publicly accessible AWS shares has found three buckets belonging to the U.S. Department of Defense intelligence-gathering operations CENTCOM and PACOM.

https://www.upguard.com/breaches/cloud-leak-centcom

Three S3 buckets were configured to allow anyone with an Amazon Web Services account to access them and were labeled "centcom-backup," "centcom-archive" and "pacom-archive."

Centcom responded in typical bureau-speak:

"We determined that the data was accessed via unauthorized means by employing methods to circumvent security protocols," said Maj. Josh Jacques, a spokesperson for U.S. Central Command. "Once alerted to the unauthorized access, Centcom implemented additional security measures to prevent unauthorized access."

(Translation: we decided not to leave the password field blank.)

The UpGuard post noted:

The data exposed in one of the three buckets is estimated to contain at least 1.8 billion posts of scraped internet content over the past 8 years, including content captured from news sites, comment sections, web forums, and social media sites like Facebook, featuring multiple languages and originating from countries around the world. Among those are many apparently benign public internet and social media posts by Americans, collected in an apparent Pentagon intelligence-gathering operation, raising serious questions of privacy and civil liberties.

While a cursory examination of the data reveals loose correlations of some of the scraped data to regional US security concerns, such as with posts concerning Iraqi and Pakistani politics, the apparently benign nature of the vast number of captured global posts, as well as the origination of many of them from within the US, raises serious concerns about the extent and legality of known Pentagon surveillance against US citizens. In addition, it remains unclear why and for what reasons the data was accumulated, presenting the overwhelming likelihood that the majority of posts captured originate from law-abiding civilians across the world.

**Android: Found to be sending tracking info to Google without permission**

Throughout all of 2017, Android devices with all location tracking permissions disabled and even without a carrier SIM card install, have been sending the IDs of all cell towers within range back to Google for analysis... which Google acknowledge after the guys at Quartz observed the behavior and asked Google why this was occurring when all location tracking had been disabled?

https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

In their reporting, Quartz wrote: "The cell tower addresses have been included in information sent to the system Google uses to manage push notifications and messages on Android phones for the past 11 months, according to a Google spokesperson.

They were never used or stored, the spokesperson said, and the company is now taking steps to end the practice after being contacted by Quartz. By the end of November, the company said, Android phones will no longer send cell-tower location data to Google, at least as part of this particular service, which consumers cannot disable.

Google explained to Quartz via eMail: “In January of this year, we began looking into using Cell ID codes as an additional signal to further improve the speed and performance of message delivery. However, we never incorporated Cell ID into our network sync system, so that data was immediately discarded, and we updated it to no longer request Cell ID.”

There's some worthwhile debate about the "reasonable expectation of privacy." My own feeling is that anyone carrying a cellphone should have a very low expectation of privacy. By its very nature it is a heavily Internet- connected computer that its user did not design and build. So it COULD be doing anything. And we keep finding that, indeed, it is doing anything. If you don't wish to be tracked and monitored, leave the phone at home. It's not realistic to imagine that it's possible to have it both ways.

**Websites are monitoring our actions:**

Websites log keystrokes and mouse movements in real time, before their users click submit.

“Session Replay Scripts”
https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/

Researchers at Princeton's Center for Information Technology Policy, on Princeton's "Freedom to Tinker", last week posted the result of their analysis of websites that are using JavaScript to monitors their visitors' actions and activities while present on the site.

We've talked about this sort of behavior in the past: How once upon a time and the quaint old days before website could run powerful code in the web browsers of everyone who visited, a static page was delivered and it was only if we went to another page, or explicitly and deliberately filled out and submitted a form that the site "saw" anything further from us.

But the position of the user's mouse can be monitored (we've talked about how Google's latest "I'm not a robot" Captcha uses this as another "I'm moving my mouse around like a human" signal) and sites can monitor scroll position, and intercept every click and keystroke BEFORE it is sent. (I use this handy and powerful feature on GRC's Password Haystacks page to dynamically recalculate the user's password AS it is being entered... making the system far more interactive.)

But..."WebSockets" is a technology that allows code running on web pages to silently initiate connections back to the mothership (or to the 3rd-party provider of the JavaScript) and dynamically send -- in real time -- everything that the page's user is doing without their explicit knowledge or permission.

The Princeton researchers have named these "session reply scripts" since the stream can be "replayed" at the hosting end to recreate the user's actions on the page.

The researchers wrote: "The stated purpose of this data collection includes gathering insights into how users interact with websites and discovering broken or confusing pages. However the extent of data collected by these services far exceeds user expectations; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can’t reasonably be expected to be kept anonymous. In fact, some companies allow publishers to explicitly link recordings to a user’s real identity.

For this study [they write] we analyzed seven of the top session replay companies (based on their relative popularity in our measurements). The services studied are Yandex, FullStory, Hotjar, UserReplay, Smartlook, Clicktale, and SessionCam. We found these services in use on 482 of the Alexa top 50,000 sites.

https://webtransparency.cs.princeton.edu/no_boundaries/session_replay_sites.html

- wordpress.com
- microsoft.com
- adobe.com
- godaddy.com
- outbrain.com
- spotify.com
- skype.com
- rt.com

As a result of this work, Easylist has been updated to include all of these domains... and Gorgill's uBlock Origin is already pulling from Easylist... so userss of our recommended uBlock Origin are protected from any concerns over this intrusion.

**ID card security: Spain is facing chaos over chip crypto flaws**
With the security of its 60 million national ID smartcards in question, Spain faces some tough choices.
http://www.zdnet.com/article/id-card-security-spain-is-facing-chaos-over-chip-crypto-flaws/

The trouble presented by even little-used security cards: Once they cannot be trusted, none can be used.

Estonia had "only" issued 760,000 Infineon cards which are now known to be generating insecure private key. By comparison, Spain has issued 60 MILLION similar -- and similarly insecure -- identity smartcards. And even though they are in very low common usage, now that ANY OF THEM can be attacked, none of the security assertions made by ANY card can be trusted. Thus they are all useless for their intended purpose.

**The return of BlueBorne**
https://thehackernews.com/2017/11/amazon-alexa-hacking-bluetooth.html

About ten episodes/weeks ago, in early September, we covered the "BlueBorne" attacks; a series of 8 new zero-day vulnerabilities affecting Bluetooth-equipped devices such as smartphones, laptops, smart TVs, many IoT devices, etc. And the attacks were significant since just have the Bluetooth radio ON allowed for remote (within radio range) compromise and takeover of Bluetooth-equipped devices without requiring any user interaction.

Well... it turns out that both Amazon's Echo and Google's Home device are, or were, similarly exposed and vulnerable.

The IoT security firm Armis that discovered this issue, has disclosed that an estimated 20 million Amazon Echo and Google Home devices are also vulnerable to attacks leveraging the BlueBorne vulnerabilities. That's likely about 15 million Amazon Echoes and 5 million Google Home devices.

The Amazon Echo is affected by two of the eight vulnerabilities:

> A remote code execution vulnerability in the Linux kernel (CVE-2017-1000251)
> An information disclosure flaw in the SDP server (CVE-2017-1000250)

Whereas the Google Home devices are affected by one vulnerability:

> Information disclosure vulnerability in Android's Bluetooth stack (CVE-2017-0785)

This Android flaw can also be exploited to cause a denial-of-service (DoS) condition.

These devices' Bluetooth radios cannot be disabled, so attackers within radio range of the affected devices can launch an attack. The vulnerability's discovers at Armis have published a proof-of-concept (PoC) video showing how they were able to hack and manipulate an Amazon Echo device.

Being responsible, Armin privately notified both Amazon and Google about its findings, and both companies have since released patches and issued automatic updates for the Amazon Echo and Google Home that fixes the BlueBorne attacks.

So... problem dodged.  But this also further reinforces the absolute necessity of all Internet-connected devices -- whether they be $1000 Smartphones or $15 lightbulbs -- being remotely updated.

**From the "Well... that didn't take long" department...**
A worrisome shortcoming has been uncovered in Amazon's Key
https://arstechnica.com/gadgets/2017/11/amazon-key-flaw-makes-entering-your-home-undetected-a-possibility/
http://www.theregister.co.uk/2017/11/16/amazon_key_wi_fi_vulnerability/

<<Amazon Key Recap>>

Rhino Labs discovered that a courier equipped with a simple program can use their laptop to fake a command from the house's Wi-Fi router to disconnect the Cloud Cam from its network. This causes the camera to stop functioning by freezing the image at the last frame.

At that point, the courier could re-enter the house, do whatever they wish -- without any monitoring surveillance -- then exit, reactivate the camera, and lock the door as usual. This re-entry would be undetectable by the resident, and it would appear like a normal delivery in Amazon's data.

Since camera-monitoring functionality is a critical part of Amazon's security pitch for Key, Amazon quickly issued the following statement in response to reports about this issue:

<quote> We currently notify customers if the camera is offline for an extended period... Later this week, we will deploy an update to more quickly provide notifications if the camera goes offline during delivery.</quote>

However, while this could help Amazon Key customers know when something is amiss, it doesn't prevent the event from happening. Ben Caudill, Rhino Labs founder, told Wired Magazine for their reporting of this that the only way to fully close the loophole would be to cache video locally even when the camera is disconnected from the network. However, the Cloud Cam doesn't currently cache video locally... and this would require significantly more local storage than for pure streaming.

**Firefox 57 Screams!**
Firefox 57 "Quantum" Released – promising a 2x Faster Web Browser

The Hacker News writes:

It is time to give Firefox another chance.

The Mozilla Foundation today announced the release of its much awaited Firefox 57, aka Quantum web browser for Windows, Mac, and Linux, which claims to defeat Google's Chrome.

It is fast. Really fast. Firefox 57 is based on an entirely revamped design and overhauled core that includes a brand new next-generation CSS engine written in Mozilla's Rust programming language, called Stylo.

Firefox 57 "Quantum" is the first web browser to utilize the power of multicore processors and offers 2x times faster browsing experience while consuming 30 percent less memory than Google Chrome.

Besides fast performance, Firefox Quantum, which Mozilla calls "by far the biggest update since Firefox 1.0 in 2004," also brings massive performance improvements with tab prioritization, and significant visual changes with a completely redesigned user interface (UI), called Photon.

This new version also adds in support for AMD VP9 hardware video decoding during playback to reduce power consumption, and thus helping to prevent systems from draining their batteries.

Firefox 57 also includes built-in screenshot functionality, improved tracker blocking and support for WebVR to enable websites to take full advantage of VR headsets.

Firefox has plans to speed things even further by leveraging modern GPUs in the near future.

Firefox Quantum for the desktop version is available for download now on Firefox's official website, and all existing Firefox users should be able to upgrade to the new version automatically.

The Android version of Firefox 57 is rolling out on Google Play in coming days, and its iOS version should eventually arrive on Apple's official App Store.

## Miscellany

- @SGgrc is approaching 60K followers
- ShieldsUP! is approaching 100 Million uses!
- ~4500 / day so... in 10 days we'll cross the 100 Million served mark. :)

**RT Simon Zerafa: Stephen Cole @sthenc**

- "The US dollar plummets to a new low of 0.00013 $BTC #bitcoin"
- BTC == $8,203.

## SpinRite

**Benjamin Rose / @BenjaminJRose91**

@SGgrc Steve! Could hard drive ECC be disabled on a hard disk? If so could that be in the next SpinRite release? I'd rather let Dynastat do the work instead of the controller's ECC. SpinRite does a better job.

**Naruto Uzumaki (@Razor512)**

@SGgrc While more for fun, on a clearly failing 1GB Sony microvault flash drive, a level 4 scan using SpinRite is able to temporarily fix it.

## Closing The Loop

**Simon Zerafa / @SimonZerafa**

@SGgrc Any thoughts in the Intel JTAG bug being deliberate? How useful would such a working attack be on any Intel platform to a Three Letter Agency? ????

**Adam van Kuik / @avankuik**

@SGgrc What was the 19 book series you were talking about earlier this year? You mentioned it a few times on Security now and I believe you said you read it twice.

**Ove Karlsson / @KarlssonOve**

Thank you @SGgrc, got bored on friday, went scrolling through Netflix and The Expanse was on one of the cards. Remembering you raving about it on SN, so I gave it a go, now a 2 day and 2 season binch later I can't wait for season 3. #TheExpanse #SN #GreatTip #ThankYou

**Simon Zerafa / @SimonZerafa**

@SGgrc PingFS. Stores data as a endless series of ICMP packets ??

- John Arundel @bitfield
- Mind. Blown. "Pingfs is a filesystem that stores data in the Internet itself, as ICMP packets going to remote servers and back" github.com/yarrick/pingfs
- (Several years old... but a fun idea reminiscent of mercury delay lines.)

**jmwhitty / @jmwhitty**

@SGgrc @leolaporte when you talk about Apple vs FBI re: golden keys, you often do not mention the impact to the non Apple's of the world.

**Michael Synan / @mike_synan**

@SGgrc any suggestion for network firewall hardware not containing IME? Or how to build an uncompromised network firewall without the hardware hack discussed two episodes ago?

**Kyle / @craigconsulting**

@SGgrc @leolaporte Hey Steve if you think watching disc defragmentation is mesmerizing, you should try watching a 3D printer at work! #soothing

**Will Springer / @W_L_Springer**

@SGgrc On Security Now, you and Leo were discussing the trend and importance of "pushing" updates to IoT devices to patch firmware vulnerabilities. Would that functionality create a new vector for a party to push malicious firmware to these devices? Thank you!

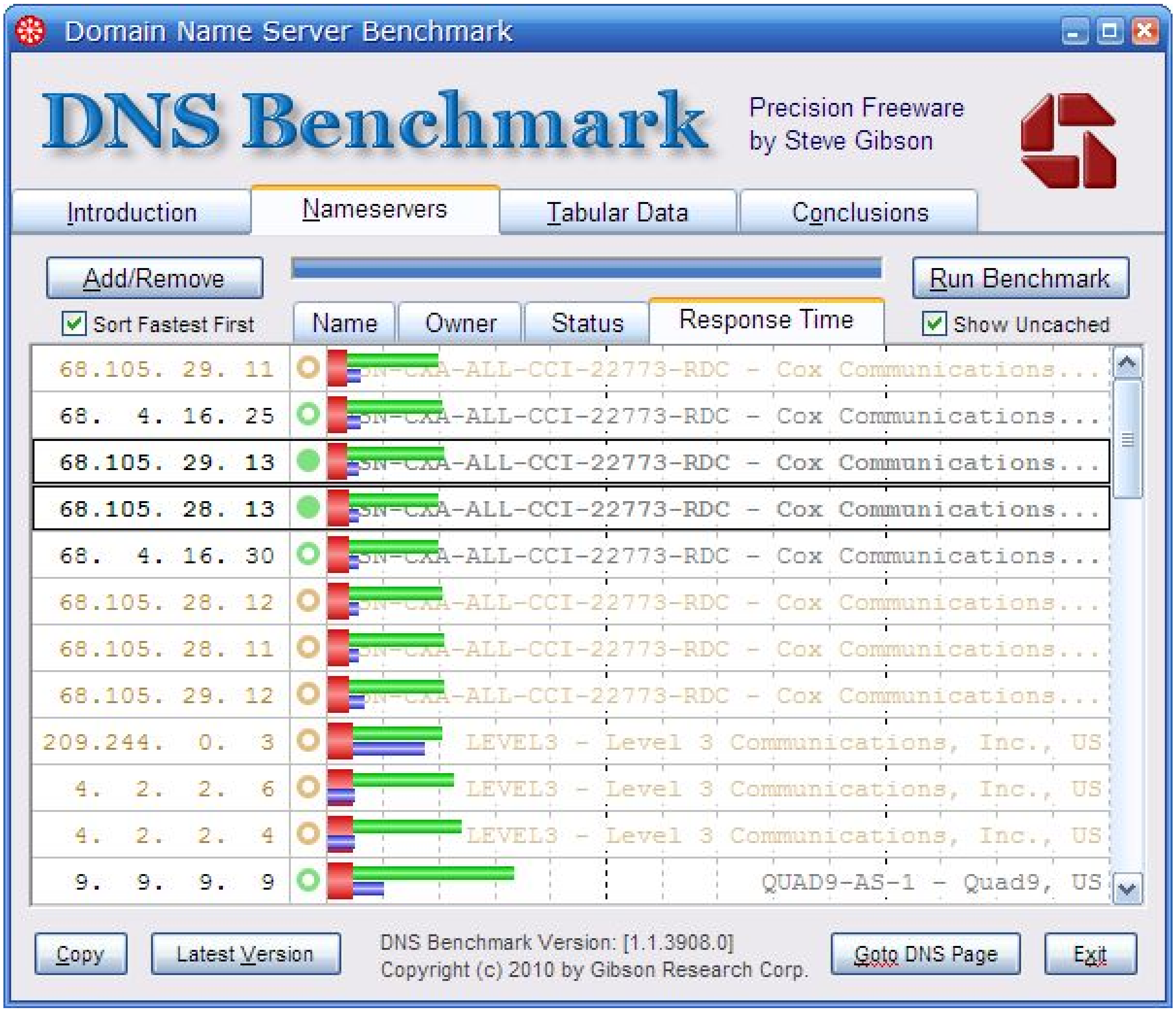
# Quad 9

https://quad9.net/#/

https://www.globalcyberalliance.org/ibm-packet-clearing-house-global-cyber-alliance-collaborate-protect-businesses-consumers-internet-threats.html

https://securityintelligence.com/new-quad9-dns-service-makes-the-internet-safer-and-more-private/

A newly unveiled DNS service which has emerged from it quiet beta phase under the name of “Quad9” -- for 9.9.9.9. It is a nonprofit jointly founded by IBM Security, Packet Clearing House (PCH), and The Global Cyber Alliance. It is a privacy- and security-enhancing DNS service which is completely free to use. And thanks to the Packet Clearing House (PCH) which maintains a globe-spanning infrastructure, the service is screamingly fast:



| | | |
|---|---|---|
| 68.105. 29. 11 | ○ | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 68. 4. 16. 25 | ○ | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 68.105. 29. 13 | ● | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 68.105. 28. 13 | ● | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 68. 4. 16. 30 | ○ | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 68.105. 28. 12 | ○ | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 68.105. 28. 11 | ○ | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 68.105. 29. 12 | ○ | SN-CXA-ALL-CCI-22773-RDC - Cox Communications... |
| 209.244. 0. 3 | ○ | LEVEL3 - Level 3 Communications, Inc., US |
| 4. 2. 2. 6 | ○ | LEVEL3 - Level 3 Communications, Inc., US |
| 4. 2. 2. 4 | ○ | LEVEL3 - Level 3 Communications, Inc., US |
| 9. 9. 9. 9 | ○ | QUAD9-AS-1 - Quad9, US |

DNS Benchmark Version: [1.1.3908.0]
Copyright (c) 2010 by Gibson Research Corp.

Using “Anycast” routing to automatically use the nearest DNS server, at this launch the service offers 70 points of presence in 40 countries… growing to 160 during 2018.

Quad9 is a free, recursive, anycast DNS platform that provides end users robust security protections, high-performance, and privacy.

**Security:** Quad9 blocks against known malicious domains, preventing your computers and IoT devices from connecting malware or phishing sites. Whenever a Quad9 user clicks on a website link or types in an address into a web browser, Quad9 will check the site against the IBM X-Force threat intelligence database of over 40 billion analyzed web pages and images. Quad9 also taps feeds from 18 additional threat intelligence partners to block a large portion of the threats that present risk to end users and businesses alike.

**Performance:** Quad9 systems are distributed worldwide in more than 70 locations at launch, with more than 160 locations in total on schedule for 2018. These servers are located primarily at Internet Exchange points, meaning that the distance and time required to get answers is lower than almost any other solution. These systems are distributed worldwide, not just in high-population areas, meaning users in less well-served areas can see significant improvements in speed on DNS lookups. The systems are "anycast" meaning that queries will automatically be routed to the closest operational system.

**Privacy:** No personally-identifiable information is collected by the system. IP addresses of end users are not stored to disk or distributed outside of the equipment answering the query in the local data center. Quad9 is a nonprofit organization dedicated only to the operation of DNS services. There are no other secondary revenue streams for personally-identifiable data, and the core charter of the organization is to provide secure, fast, private DNS.

**Ease of use**: Administrators can easily configure endpoint devices to point to the Quad9 DNS server at address 9.9.9.9.

Quad9 also maintains a whitelist of the top one million sites to prevent inadvertent blacklisting. So the "known safe" list overrides the "known bad" list.

The primary IP address for Quad9 is 9.9.9.9, which includes the blocklist, DNSSEC, and other security features. However, there are alternate IP addresses that the service operates which do not have these security features. These might be useful for testing validation, or to determine if there are false positives in the Quad9 system.

Secure IP: 9.9.9.9 Blocklist, DNSSEC, No EDNS Client-Subnet

Unsecure IP: 9.9.9.10 No blocklist, no DNSSEC, send EDNS Client-Subnet

***Does Quad9 share the DNS data that is generated with marketers?***
*Quad9 does not and never will share any of its data with marketers, nor will it use this data for demographic analysis. Our purpose is fighting cyber crime on the Internet and to enable individuals and entities to be more secure. We do this by increasing visibility into the threat landscape by providing generic telemetry to our security industry partners who contribute data for threat blocking.*