Quad9 public domain name service moves to Switzerland for maximum internet privacy protection

Q&A

1 About Quad9

1.1 Who is Quad9?

Quad9 is a DNS-based system that provides to users a basic, easily implemented security service at no cost and with high privacy. Quad9 is a not-for-profit service with no other products and has no motivation to upsell or create value from personal user data.

1.2 Why did Quad9 move its headquarters to Switzerland?

The Quad9 operators have stated consistently that data privacy is one of the core components of the service. However, being based in the United States means that only the promise of the organisation shields the user from misuse of data – there are no consistent national legal protections for personal data in the US. It was the intention from creation of Quad9 to secure this promise with a more legally binding action, and moving under the protection of Swiss data and privacy laws proves the dedication to that integrity. Other DNS services based in the US may change their data policies with little or no notice and with no legally binding implications. This lack of constraint incentivises commercial organisations to change their behavior for profit, if not for other reasons. The Quad9 providers have removed doubt as to the treatment of private data under their control by placing the legal base of operations in a nation with strong privacy laws. Specifically, Switzerland was chosen as the most appropriate choice because it is the country with the longest standing reputation for neutrality and stable jurisprudence regarding data and procedural constraints on corporate actions. Quad9's continued non-profit status creates no motives for capitalizing user data, so there is no conflict between the goals of the user and the goals of the organisation.

1.3 What advantages does Quad9 offer (compared to other DNS server operators)?

Quad9 provides several distinct advantages compared to other "over-the-top" DNS providers: First, Quad9 has embedded in its mission the task of providing privacy as a primary component of the service. There are no secondary revenue streams being generated from personal data and no incentive or technological possibility to do so. Quad9 performs a single task: privacy and security services via the DNS, with no logging of personal data. Secondly, Quad9 is an aggregator of security services for those users who choose to utilize the anti-malware/anti-phishing options Quad9 offers. This means that Quad9 can offer a broad protection suite instead of just guarding against a limited set of internally generated indicators of compromise, as some other services do. Thirdly, Quad9 has deployed its services worldwide, in 90 countries, including emerging markets with typically lower security service coverage yet high risks—higher risks, if one uses monetary impact versus income per event as a measurement. The Quad9 coverage area attempts to support the whole internet, not just the most profitable parts. Lastly, Quad9 is a no-cost option, with no contractual requirements for end users or organizations of any size.

1.4 How extensive is Quad9's DNS infrastructure and how does it compare with Google or others?

Quad9 is deployed worldwide, in 90 nations and more than 150 locations. This means that Quad9 has the ability to answer queries from locations that are typically quite close to end users, leading to lower latency and fewer opportunities for interception or observation of query traffic. Other anycast DNS networks have broad scope in densely populated regions, but they are often located in datacenters that are geographically distant from major interconnection exchange (IX) locations. Quad9 has focused initially on deploying service as close as possible to these carrier-neutral facilities (typically inside the same building as the IX) and is expanding to larger datacenter footprints in 2021 and onwards. Additionally, Quad9 is deploying services to nations and regions that lag significantly in service delivery by commercially oriented organisations because of the latters' profitability concerns. Quad9 covers the same geographic and political regions as other large recursive operators and operates its services using infrastructure partners that are among the top 1% of interconnected networks as measured by peering and traffic exchange relationships.

1.5 Why did Quad9 team up with SWITCH?

There have been long-standing and very good cooperative efforts between SWITCH and Quad9 co-founding member organisation Packet Clearing House (PCH), including hosting resources for the .ch country code top level domain. The internet is still to a large degree based on mutual trust and long-term relationships that create a basis for the legal and contractual frameworks supporting those trust relationships. SWITCH and Quad9 have proven that they are dedicated to the same goals of privacy, security, and internet stability.

1.6 What were the reasons for setting up a foundation in Switzerland? Why not in Germany, a larger nation?

The decision to establish the foundation in Switzerland is based upon several factors:

Switzerland was the most appropriate choice, for it is the country with a long-standing reputation for neutrality and stable jurisprudence regarding data and procedural constraints on corporate actions.

Swiss regulatory authorities were able to provide assurances that Quad9 would not be considered as falling into any regulatory framework that would require Quad9 to track users or keep records about user data interactions under Swiss law.

An additional key factor in this collaboration is the match of Quad9 and SWITCH missions: providing security and stable services to users worldwide. SWITCH being based in Switzerland and having a long history of positive interactions with PCH provided the final incentive for the decision to create the Swiss entity in which the Quad9 service would be re-established.

1.7 Why is Quad9 a non-commercial organisation?

The primary answer is “trust”. An organisation that is not permitted to seek profit has a clearer alignment with end users. If there was an incentive to gain profit from the service, then the natural behavior would be to treat end users as a resource to be exploited instead of a community to be protected. By rejecting the motive for profit, Quad9 creates an alignment of goals between the end user and the mission.

Secondarily, the extensive resources that are made available to Quad9 from infrastructure and threat intelligence advisors are extremely valuable and difficult to develop. These resources are made available to Quad9 because of our mission to make the internet a safer place, and our partners appreciate that mission and are willing to assist Quad9 towards that end. If Quad9 was charging for services, our partners and sponsors would in turn wish to be paid instead of providing these resources at no cost.

By committing to goals that help end users and help the internet, Quad9 is able to obtain resources that would otherwise be extremely expensive or impossible to acquire. The internet, despite being a vehicle for commercial gain, is still operated by people who desire to see positive results achieved by efforts that do not have a profit motive. Quad9 helps make end users and the internet safe, with no hidden agenda of revenue generation, which benefits end users, network operators, and organisations who rely on a trusted and stable internet.

1.8 How does Quad9 make money?

Quad9 does not make money or charge for its services. The organisation is funded by a variety of sources: corporate sponsorship and partnerships, non-profit donations from organisations with like-minded goals, partnerships with network providers who want dedicated instances or support, and end user donations.

The partnership with SWITCH has allowed Quad9 to move to a new jurisdiction in Switzerland, and the SWITCH contributions to this transition in the form of advisorship, local sponsorship and contributions for administrative costs, and provision of a headquarters for the organisation have been absolutely vital to the process.

The most significant operational sponsorship of Quad9 comes from PCH (also a non-profit) with the donation of network infrastructure, co-location, transit, and support services that deliver connectivity to the majority of Quad9’s service locations.

The primary source of capital funds is from corporate partnerships and sponsorships. IBM was one of Quad9’s founding organisations and continues to be a significant partner and sponsor in cooperation with its XForce threat intelligence group. Organisations such as IBM contribute funds and resources (often in the form of threat intelligence) that assist Quad9 in daily operations and in service delivery.

With this announcement of European re-homing, companies and NGOs in the European region may be more likely to partner with Quad9 to promote an EU-oriented solution that

is consistent with the regulatory norms and social goals of the European internet community.

1.9 When do these changes to Quad9's status come into effect?

The announcement on February 17 declares the establishment of the Quad9 Foundation, which is the entity that has responsibility for the Quad9 service and systems. Over the coming weeks, there will be the transition of various registrations and responsibilities such as domain names and internet registrar data that will reflect the new name and address for the Quad9 Foundation on existing Quad9 components.

2 About SWITCH

2.1 Why did SWITCH team up with Quad9?

By participating in Quad9's foundation as a Swiss entity, SWITCH can help to shape a secure and high-performance global DNS infrastructure with a European focus and strengthen both organisations' expertise and innovative capacity. The education, research, and innovation community in Switzerland will also benefit from this cooperation.

The matching mission between SWITCH and Quad9 was a key factor in this collaboration: providing security and stable services to users worldwide.

2.2 How did SWITCH contribute to Quad9's move to Switzerland?

The partnership with SWITCH has allowed Quad9 to move to a new jurisdiction in Switzerland, and the SWITCH contributions to this transition in the form of advisorship, local sponsorship and contributions for administrative costs, and provision of headquarters for the organisation have been absolutely vital to the process.

2.3 How does SWITCH's participation benefit the beneficiaries of the foundation, i.e., the Swiss universities?

As part of Quad9's governance, SWITCH is further expanding its security contacts and sources of information. The foundation is thus in an even better position to protect the Swiss universities and internet users from cyber threats.

2.4 What is SWITCH's role in the Swiss Quad9 Foundation?

Initially:
- Assist with legal and financial aspects of setting up the foundation in Switzerland
- Begin financing of the foundation

At present:
- Being a member of the board of trustees and thus part of Quad9's governance
- Provide business support and legal advice regarding local canton business matters
- Promote and assist Quad9 in Swiss press, industry forums, and professional forums of relevance

2.5 How is SWITCH represented on Quad9's foundation council?

Quad9's foundation council consists of five members. SWITCH is entitled to appoint one member from its own ranks. At present, this is Martin Leuthold, Head of the Security and Network Division and a member of SWITCH's Executive Board. SWITCH also has the right to nominate a further member, which must be approved by PCH. At present, this member is Florian Schuetz, Federal Cybersecurity Delegate and Head of the National Cybersecurity Centre (NCSC) in Switzerland.

PCH is entitled to nominate two members. At present, these are Bill Woodcock (PCH), and Dorian Kim (NTT.). In addition, PCH has the right to nominate one further member, which currently is Benno Overeinder, Managing Director at NLNet Labs.

2.6 Are other SWITCH employees strategically or operationally active for Quad9?

No, apart from the person who represents SWITCH in Quad9's foundation council, no one from SWITCH works for Quad9.

2.7 SWITCH provides Quad9 with lists of websites that are known to include malware or other threats. Where do the malware threat feeds from SWITCH originate?

SWITCH has been part of a global network of leading cyber security companies for decades. Activity within this network is based on the highest level of mutual trust, thus enabling the exchange of relevant information on cyber security.

2.8 Will SWITCH also receive malware feeds from Quad9?

SWITCH will receive Quad9 DNS services as well as specific volumetric telemetry about threats provided by SWITCH data feeds in order to improve the results for Quad9, SWITCH, and SWITCH’s other threat feed consumers.

3 Internet privacy protection

3.1 How does Quad9 provide privacy and more security to internet users?

Whenever consumers use DNS services to surf the internet, click on a link, open an app, or send an email, they are leaving behind digital footprints and data. Recursive DNS providers see a broader set of personal data than any other organisations on the internet. Unlike many DNS providers that operate in jurisdictions without centralized privacy legislation, Quad9 is required to comply with the strong legal mandates on privacy (GDPR-harmonized) as defined by Swiss law.

Quad9 is a not-for-profit organisation dedicated only to the operation of DNS services. There are no secondary revenue streams for personally identifiable data. In addition to privacy protection, Quad9 also offers protection against cyber crime by blocking access to websites known to contain malware, phishing, and other threats. The core charter of Quad9 is to provide secure, fast, private DNS service. Those who prefer to entrust their surfing behaviour to a non-commercial DNS service provider that is also subject to the Swiss Data Protection Act make the right choice with Quad9.

3.2 How does Quad9 ensure that it does not collect/market private user data?

Quad9's specific mission is to provide security and privacy services in order to help end users experience a more stable and trustworthy internet. The board of the organisation is tasked with ensuring that the organisation's actions are consistent with the mission goals as chartered by the Swiss cantonal authorities who recognize Quad9 as a foundation. As part of its core DNS service, Quad9 discards IP addresses that are associated with queries, which is the personal data that would permit association of a specific DNS event with a natural person. The fact that Quad9 does not store or transmit any of these IP addresses associated with queries prevents Quad9 from creating any database of private user data as defined by the GDPR.

4 Protection from cyber crime

4.1 How does Quad9's protection from cyber crime differ from that of Google or other DNS providers?

Most DNS recursive systems do not include a blocking list to prevent access to malicious sites. Typically, an internet service provider offers no threat mitigation via its DNS systems, or if there is a blocking system in place it is from a single provider of threat data. Quad9 has roughly twenty different threat intelligence sources at any time, giving a broad cross-section of threat coverage. There are paid services that provide DNS blocking capabilities, but they require contracts and may not treat personal data in the same way that Quad9 does, or they may have sources of threat data that are not as comprehensive as those Quad9 utilizes. Quad9 discards all personal information associated with DNS transactions, such as IP address data, and never stores or retransmits that data.

4.2 How does Quad9 block websites with malicious content?

Quad9 obtains lists of malicious sites from Threat Intelligence (TI) partners. These lists are installed into the DNS recursive resolvers Quad9 operates. End users then utilize those recursive DNS resolvers. From that point, each internet transaction the user engages in is sent to the Quad9 systems for DNS resolution. Sites that are without risk are resolved, and the Quad9 system provides the name-to-IP address to the client's computer or device. On the other hand, sites that are on the blocking list are not resolved, and the user is prevented from connecting to the remote server because the IP address remains unresolved, and therefore the user is prevented from connecting to the threat source.

4.3 How do blocking and exceptions work?

Quad9 receives lists of malicious domains from Threat Intelligence (TI) partners. These lists are updated many times per day or even per hour and are generated by the TI provider's specific threat discovery process. Each TI provider may utilise unique threat types, market segments, or techniques to tag domains as housing malicious content. Rarely, a domain may be tagged as housing malicious content when it does not. This often happens when a website is "cleaned" after infection, or if a host contains content that triggers phishing detection algorithms but is not actually a phishing site, or if some other faulty algorithm or human examination misinterprets properties of a site or timing of an entry. In these cases, Quad9 supports a reporting model (email and web form) that allows end users to report a domain as being incorrectly blocked. If the site passes a validation check, then it is excepted from the block list, meaning that the domain is again allowed to resolve for end users. Quad9 reports exception events to the TI provider who delivered the domain, so that the provider may examine their methodology or refute the exception with evidence of malicious intent. TI providers who contribute higher-than-normal exception volumes may be temporarily removed from the blocking list inventory until an investigation into the high rates is completed, but Quad9 works closely with providers to ensure this happens rarely.

4.4 What types of things does Quad9 block?

Quad9 blocks only hosts or domains that contain malicious content; it does not implement any other type of content filtering. Malicious content is broadly described as content that delivers a result that a reasonable end user would not expect to obtain by visiting that site and which is designed to defraud, deceive, misdirect, or cause some action considered harmful to the end user or the end user's computer or network. Sites that deliver malware, phishing sites, spyware, botnet command and control servers, and coin mining are examples of malicious hosts or sites that Quad9 includes in the blocking data set.

4.5 Where do the malware threat feeds from Quad9 originate?

Quad9 has partnerships with many different Threat Intelligence (TI) partners, who provide rapidly updating lists of domains that present risks. These are both public sources as well as private, commercial providers whose data is used in single-source settings. Each TI provider has specific areas of focus. Some may provide deep-link malware analysis, others may focus on look-alike phishing domains, still others target COVID-specific risks, and some are even focused on specific sectors such as financial or cryptocurrency fraud. Each TI provider has expertise and data analysis that is far beyond what any one organisation might be able to provide. By combining these feeds, Quad9 is able to give end users broad-based DNS-based threat mitigation.

4.6 Why do threat intelligence sources share data with Quad9?

The partnerships with Threat Intelligence (TI) providers are based on improvement of security for Quad9, the TI provider, and the end users of both Quad9 and the TI provider's data. When Quad9 receives threat data from a TI provider (in the form of domain lists), they are inserted into the blocking database. When a client of Quad9 attempts to reach one of these malicious sites, Quad9 blocks the attempt and then also sends the TI provider a brief set of telemetry data about the block: timestamp, the domain, and a rough geography of the client (no private data about the end user is transmitted or stored.) This allows the TI provider to understand the scope of the risk, answering such questions as these: Is a malicious campaign growing in scale? Falling? Are the targets of the campaign coming from one particular continent? What is the velocity of growth? This data is extremely valuable to TI providers, who can then determine the accuracy of their threat models and thus refine their algorithms to provide faster, more reliable data as part of a feedback loop. As a result of this feedback loop, Quad9 receives better blocking data, and the TI provider improves their own data set for their consumers, including those who may not be using Quad9. Security for end users, no matter whose end users, benefits from the relationship.

5 Using Quad9

5.1 How can the Internet user choose to have their DNS queries run through Quad9's resolvers?

Quad9 is free and available throughout the world. Users may configure their computer's DNS resolvers to 9.9.9.9, 149.112.112.112 and 2620:FE::FE. For a step-by-step guide or for more advanced options, please visit https://quad9.net.

Converting to Quad9 services is relatively simple, though still a technical task. The Quad9 website has instructional videos for Windows and Macintosh operating systems and has available an Android application in the Google Play store for free download (search for “Quad9 Connect”). Home routers, WiFi access points, and firewalls can also be configured so that Quad9 is automatically used by all devices in the home or office network without the need to configure each system individually. The brief description of configuration in its most simple form is that the “DNS Servers” for the device are changed from the defaults provided by the local network operator (typically, the ISP provides DNS Servers) and modified so that these three IP addresses appear in the configuration: 9.9.9.9 and 149.112.112.112, and 2620:FE::FE. Different variations of the service are available on slightly different IP addresses; see the Quad9 website for more details and configuration notes. There is no sign-up, contract, or other interaction with Quad9 – simply changing those IP addresses is sufficient to receive security and privacy coverage in its most basic form.

5.2 When I surf the Internet with Google's Chrome Browser, do I automatically use Google's DNS resolvers?

Chrome uses the DNS resolver configured by the operating system. This means that, if your device is configured to use Quad9, Chrome will utilize the Quad9 systems and have blocking enabled. Additionally, Chrome has the ability to provide “DoH upgrade,” which will, if enabled, cause communication with Quad9 systems for DNS queries to be performed over an encrypted channel.

5.3 What reasons are there for Swiss internet users to change or not change to Quad9?

DNS servers from Swiss internet service providers (ISPs) are a good choice for internet users in Switzerland, since they fall under the same legal constraints as Quad9 in regard to the use of end-user data.

However, mobile device users may find Quad9 a suitable replacement for roaming services, since Quad9’s data policy is consistent with Swiss data privacy laws even outside Swiss borders.

The malware and phishing security provided by Quad9 is a combination of many different commercial and non-commercial sources, and so it may be suitable as a replacement for local ISP resolvers to provide higher security to devices on the network. Because of the GDPR harmonization that all Swiss network providers must offer, the privacy assurances must be publicly stated and therefore are equivalent to the requirements placed on Quad9, though the privacy guidelines may not be the same as Quad9's policy of not collecting any personal data as part of the DNS transactions.

If a user is in a commercial network where there are local security policies that regulate access to sites via non-Quad9 DNS filters, then we do not recommend using Quad9, which could contradict local security policy.