Maintain Security Visibility In The TLS 1.3 Era

You Have Two Years To Prepare Your Security Tools For TLS 1.3 And DNS-Over-HTTPS

by David Holmes

July 30, 2020 | Updated: August 12, 2020

Why Read This Report

New encryption standards TLS 1.3 and DNS-over-HTTPS (DoH) are sweeping the last crumbs of visible user activity off the enterprise network table. Soon, security controls, already starved for unencrypted traffic to analyze, will be completely famished. This report looks at the actions that security professionals must take now to get their visibility programs back to the feast. Fail to take any action, and within two years, you'll lose the ability to analyze network traffic and detect the cyberthreats that will endanger your organization.

Key Takeaways

Prepare For The Impact Of TLS 1.3 On Visibility And Threat Detection

The new encryption protocol foils mass surveillance and encrypts metadata but also blinds enterprise security tools. You have two years to put a program in place to fix it.

Turn The Lights Back On With New Techniques

Enterprise security teams and security vendors are pioneering new approaches and techniques, from session key forwarding to encrypted traffic analysis (ETA) to side-band checking. To regain visibility, security pros will have to experiment with and adopt many of these emerging techniques as part of their programs.

Prepare Today, Even Though Adoption Isn't Widespread Just Yet

While the evolutions of TLS 1.3, encrypted domain name system (DNS), and encrypted server name indicator (SNI) are recent and the adoption rates are currently modest, security pros shouldn't delay their preparations. You can take a number of steps today, from prioritizing key upgrades to blocking what you can, until new approaches and techniques are ready.

Maintain Security Visibility In The TLS 1.3 Era

You Have Two Years To Prepare Your Security Tools For TLS 1.3 And DNS-Over-HTTPS

by David Holmes
with Joseph Blankenship, Stephanie Balaouras, Heidi Shey, Josh Zelonis, Chase Cunningham, Alexis Bouffard, and Peggy Dostie

July 30, 2020 | Updated: August 12, 2020

Your Current Network Monitoring Practices Won't Work Anymore

Two of the foundational protocols of the internet, transport layer security (TLS) and DNS, have recently undergone radical changes to protect browser user privacy. Both changes have created controversy in the security community because, while they hide user activity from the searching eyes of nation-states and ISPs, they also hide valuable metadata from enterprise network inspection tools. As these changes gain momentum, security monitoring tools will be blinded to the contents and destination of traffic and unable to detect threats. The network will be darker than it's ever been. Both the security practitioner and vendor communities are actively creating solutions that can bring visibility back to the network.

Security Teams Are Innocent Bystanders Between Privacy Activists And State Surveillance

The current conflict between privacy activists and surveillance advocates resembles the famed Star Wars conflict of the Rebel Alliance versus the Empire. The rebels in this war are privacy activists within Internet Engineering Task Force (IETF) working groups and the browsers (namely, Google Chrome and Mozilla's Firefox) and open source crypto libraries that follow their blueprints. The Empire is, well, actual empires — nation-states and their enablers, such as ISPs, who surveil citizenry on the internet. "Forrester's Global Map Of Privacy Rights And Regulations, 2019" cites alarming levels of government surveillance in 14 of 54 countries, including Austria, Columbia, India, Hungary, Kuwait, and the UK.

To counter mass government surveillance, privacy activists have been advocating for encryption everywhere and have been working within the IETF groups to provide countermeasures against eavesdropping and data collection.[1] The latest version, TLS 1.3, and encryption of the venerable domain name system are the results of their most recent efforts. These changes have stirred controversy because:

- **Conventional decryption architectures go blind.** The financial services community has invested heavily in passive decryption, as regulation prohibits unencrypted data, even on their internal networks. The privacy activists engineered TLS 1.3 to require "forward secrecy," making it incompatible with the security inspection architectures of large financial services with heavy

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

regulatory burdens.[2] A vice president of one such organization told Forrester, "It would cost us $1 million per connection to terminate TLS 1.3 inline, because we can't tolerate the risk of downtime. Out-of-band has no downtime risk."

- **Encrypted certificates hide unsafe sites.** TLS 1.3 encrypts the server certificate, hiding its contents from passive network monitoring tools. With TLS 1.3, security teams can no longer apply network policies that prevent users from visiting sites with unsafe certificates, including those that are expired, revoked, or self-signed.[3] Because TLS 1.3 hides server certificates, some network monitoring systems are already blocking TLS 1.3 connections.[4] Two different security architects we interviewed for this report likened the enhanced privacy of TLS 1.3 to a Pyrrhic victory in which enterprises will now have to decrypt everything.
- **DNS-over-HTTPS removes IT control.** Privacy activists see the current domain name system as a significant privacy leak and have proposed encrypting DNS-over-HTTPS to fix it.[5] Browsers and content delivery networks (CDNs) adopted it as quickly as they could, even over the protests of many detractors. Paul Vixie, the godfather of DNS, has been particularly vocal in his disdain for DNS-over-HTTPS: "DoH is an over the top bypass of enterprise and other private networks. DNS is part of the control plane, and network operators must be able to monitor and filter it."[6] Indeed, researchers have already found a strain of malware that hides its DNS queries over DNS-over-HTTPS to evade detection.[7] Vixie's opinion of DNS-over-HTTPS is clear: "RFC 8484 is a cluster duck for internet security. Sorry to rain on your parade. The inmates have taken over the asylum."

Build A Strategy Now For The Capabilities You Can't Live Without

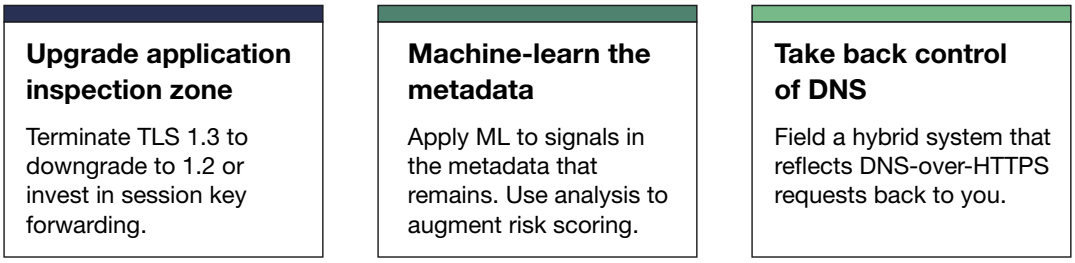
Security and risk professionals can't control browsers or the internet, but they're still responsible for securing the environment. As TLS 1.3 and DNS-over-HTTPS gain momentum, teams need to plan now to augment their inspection programs. Explicitly lay out a visibility upgrade program, or piggyback it onto a larger effort like network modernization or digital transformation. Within the larger effort, incorporate tactical approaches to recapture network metadata and lost decryption capabilities.

You Have Two Years To Put Key Capabilities In Place

Both TLS 1.3 and DNS-over-HTTPS represent a minority of user-generated traffic today. According to Qualys Labs SSL Pulse data, only about one in four internet web properties currently offers TLS 1.3.[8] However, security pros should expect TLS 1.3 adoption outside of the megasites to increase by 10% per year.[9] DNS-over-HTTPS is already supported by all major browsers and Microsoft's Active Directory.[10] Today, only Firefox enables it by default, and within two years, most modern browsers will as well. As TLS 1.3 and DNS-over-HTTPS become prevalent in the enterprise network and within public and private clouds, security professionals will have to (see Figure 1):

- **Upgrade the application inspection zone.** Organizations will have to create full-proxy inspection zones for inbound traffic, be it on-premises or in the cloud. Terminate TLS 1.3, inspect the content, and then re-encrypt to the final destination using TLS 1.2. Alternately, organizations with multiple passive decryption tiers will invest in session key forwarding to restore visibility to their existing security inspection zones. Everyone needs to upgrade next-generation firewalls to inspect outbound TLS 1.3.
- **Machine-learn the metadata.** Where decryption inspection zones aren't feasible, security and risk pros must augment their networking monitoring with machine learning (ML) applied to the network metadata that remains. Don't believe vendor hype about their models divining evil within the ciphertext; they're actually getting their signals from destination addresses, packet size, packet distribution, and protocol attributes. One of the common signals is the cleartext SNI, which the privacy activists are also trying to encrypt.[11]
- **Take back control of DNS.** DNS is the redheaded stepchild of IT: Operations hates running it, security doesn't want it, and the one person who understands it is probably retiring any day now. Most organizations have already outsourced external DNS management to companies like Oracle (through Dyn) or their telco providers. The anticipated headaches caused by DNS-over-HTTPS will spur more to do the same. Organizations will have to field a hybrid system that captures domain requests over DNS-over-HTTPS with on-premises solutions like Infoblox for internal views and a trusted third party in the cloud. These systems will mirror the organization's DNS requests back to them, to be fed to logging, monitoring, and other security technologies.

FIGURE 1 Key Steps To Prepare For TLS 1.3 During The Next Two Years

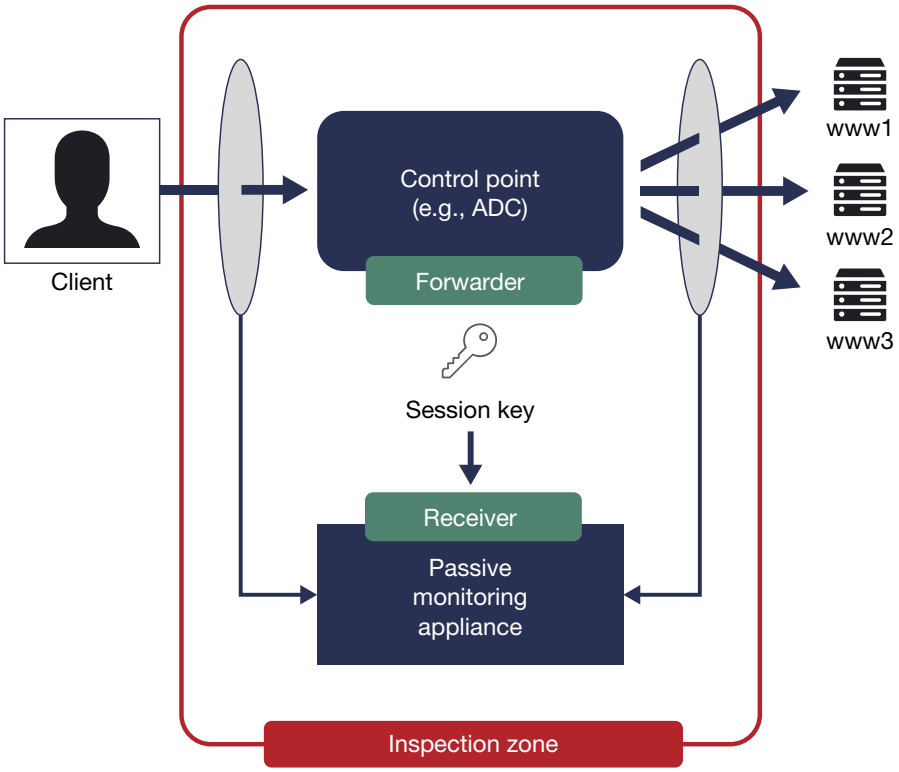


Turn The Lights Back On With New Techniques

Top minds around the world are working on solving these visibility problems. Forrester interviewed security architects from clients at financial services as well as a mix of network security vendors to uncover these new tactics. To build a program that can maximize inspection capabilities across networks that are almost entirely encrypted, security and risk professionals will have to:

- **Invest in session key forwarding for inbound applications.** TLS 1.3 requires forward secrecy, which foils passive monitoring via public key sharing used by many security inspection architectures. Two network monitoring vendors, ExtraHop and Nubeva, have pioneered a bold — some say radical — solution: cracking the servers (or clients) that terminate the TLS sessions and exporting the session keys from process memory. The keys are then forwarded to the vendor's monitoring solution (ExtraHop) or a centralized repository (Nubeva), where they can be fed to the existing passive monitoring infrastructure, thereby re-enabling full visibility (see Figure 2). Note that the centralized key repository must be protected and the session keys must be aged out responsibly.
- **Augment data collection with encrypted traffic analysis.** ETA feeds multiple signals from the encrypted transmissions into AI/ML models to determine the maliciousness of any connection. ETA can detect interactive SSH shells due to the small size and periodicity of each packet, which might not sound like a revelation, but what if some are terminating in Iran, or North Korea, or some other unexpected region? Barac (a London-based startup), Cisco, and Juniper Networks have ETA solutions. NAV vendor Corelight can use ETA to spot the difference between a typical encrypted user Remote Desktop Protocol (RDP) session and malicious automated RDP Metasploit module.
- **Target suspicious sites with side-band checking.** In a TLS 1.3 and DoH environment, where one can't pull session keys from an endpoint or see DNS requests, outbound connections will be completely opaque. There will be no domain name or server certificate to test against reputation databases. Stall connections to questionable internet destinations, retrieve their server certificates, and make some rudimentary security policy decisions; look for certificates that are self-signed, expired, revoked, or otherwise out of policy. Cisco currently uses this approach to inform its StealthWatch NAV, but your security tools can be scripted to do this as well.
- **Deploy DIY enterprise DoH.** Security professionals will deploy DNS-over-HTTPS solutions, ideally one on-premises and another that's integrated with endpoints for mobile users (though technology is only now emerging). F5 Networks is upgrading its on-premises DNS solution to support DoH. Webroot (acquired by OpenText) will host a cloud DoH server to process requests from Webroot client endpoints. The DNS queries will be reflected back to the enterprise's logging infrastructure.
- **Fingerprint TLS.** TLS handshakes are complicated affairs, with dozens of protocol extensions and packet sizes, making it possible to identify specific encryption stacks and clients. Ivan Ristić conducted research into fingerprinting via TLS cipher suites in 2009.[12] More recently, the JA3 project has made a good-faith effort to be able to fingerprint TLS endpoints by the characteristics each session.[13] The JA3 project is already in use in many networking inspections tools, but multiple NAV vendors have told Forrester that JA3 is too imprecise and is actively being sidestepped by malware attackers, so it will be replaced by other (proprietary) solutions.[14] One vendor used TLS fingerprinting to identify strange behavior from three VoIP phones in a farm of 100. Upon investigation, the VoIP phones had been hacked and were uploading conference room recordings to Dropbox.

FIGURE 2 A Session Key Forwarding Architectural Diagram For Inspection Zones



Recommendations

Prepare Today For A Future Where All Network Traffic Is Opaque

While the evolutions of TLS 1.3, encrypted DNS, and encrypted SNI are recent, and the adoption rates are currently modest, security pros shouldn't delay their preparations for the time when most traffic will become opaque. The network monitoring community is developing countermeasures for the blind spots, but right now, until the toolset is complete, you should:

› **Embrace DoH, but only if you see it.** If your local DNS solution supports DoH, push policy out to your browsers to enable it, but only if that solution can mirror your DNS requests and responses to your monitoring platforms. Otherwise, push policy that blocks it, or disable it at the network.[15]

› **Raise the risk score on encrypted SNI.** Support for encrypted SNI is embryonic. As tools become available, either block encrypted SNI transiting the corporate network or raise the risk score of endpoints using it.

› **Isolate and proxy your TLS 1.0 servers.** 1999's venerable version, TLS 1.0, is not only old enough to drink — it's about to move into your basement and hang out there playing Call of Duty. All major browsers have announced they'll be withdrawing support for TLS 1.0 in the first half of 2020 (though there have already been some COVID-19-related delays), but, of course, you're still going to have legacy servers (somewhere!) that still speak only that protocol.[16] Isolate these servers on their own segments, and install reverse proxies to them.

› **Deploy the inevitable upgrades.** Many existing TLS inspection tools, such as secure web gateways (SWGs), have lagged in their support of TLS 1.3, though this is slowly changing. Forrester recently interviewed 18 security tool vendors, and the majority of them still can't parse TLS 1.3 today.[17] Fortinet, Gigamon, and McAfee are notable exceptions. For the rest, TLS 1.3 is on their roadmaps; get their account managers on a video call so they can start making promises.

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Akamai
Awake Security
Barac
Cisco
Cloudflare
Corelight
Extrahop
Gigamon
Nubeva
Palo Alto Networks
ShieldX
Venafi
Webroot

Endnotes

[1] The internet has seen a dramatic increase in encrypted traffic due to projects like Let's Encrypt. In 2016, only about half of all web traffic was encrypted; today, that figure is 86%. Source: David Warburton, "2019 TLS Telemetry Report Summary," F5 Labs; February 27, 2020 (https://www.f5.com/labs/articles/threat-intelligence/2019-tls-telemetry-report-summary).

[2] Asymmetric cryptographic algorithms like RSA, DSA, and Diffie-Helman pinned the security of their connections on the security of a private key. An attacker could record all encrypted traffic between two parties, and then, if they ever recovered the private data in the future (forward in time), they could go back and decrypt the stored transmissions. Forward secrecy solves this problem by computing an additional key that is specific to each connection.

[3] Infrastructure outages caused by expired certificates occur frequently. Recent outages include Microsoft Teams, on February 4, 2020, impacting 20 million users. On May 23, 2019, LinkedIn suffered from its second major outage related to an expired certificate. On December 6, 2018, 30 million mobile users and businesses in the UK were impacted when a certificate expired on the O2 mobile network. In 2017, attackers were able to hide their presence due for 76 days to an expired certificate in the Equifax network. Source: "The Equifax Data Breach," US House of Representatives Committee on Oversight and Government Reform, December 2018 (https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf); "Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," US Government Accountability Office, September 7, 2018 (https://www.gao.gov/products/GAO-18-559); "CIO Study: Certificate-Related Outages Continue to Plague Organizations," Venafi (https://www.venafi.com/resource/CIO-Study-Certificate-Related-Outages-Continue-to-Plague-Organizations); and "810 Million Users Impacted by Major Outages in the Past 4 Years," Venafi, February 2020 (https://www.venafi.com/sites/default/files/2020-02/Venafi_Infographic_MicrosoftTeamsOutage_2002_1.pdf).

[4] In August 2020, a joint report by three long-time observers of censorship in mainland China — iYouPort, the Great Firewall Report, and the University of Maryland — indicated that outbound TLS 1.3 connections showing the encrypted SNI extension are being blocked at the national perimeter. Source: Kevin Bock, Louis-Henri Merino, David Fifield, Amir Houmansadr, and Dave Levin, "Exposing and Circumventing China's Censorship of ESNI," Great Firewall Report, August 7, 2020 (https://gfw.report/blog/gfw_esni_blocking/en/).

[5] DNS queries have always been "public" in the sense that they're not encrypted, but should they be? In 2015, in RFC8484, DNS-over-HTTPS, Stéphane Bortzmeyer eloquently wrote, "The web site of Alcoholics Anonymous is public; the fact that you visit it should not be." Source: S. Bortzmeyer, "DNS Privacy Considerations," IETF, August 2015 (https://ietf.org/rfc/rfc7626.html).

[6] Source: Richard Chirgwin, "'The inmates have taken over the asylum': DNS godfather blasts DNS over HTTPS adoption," The Register, October 23, 2018 (https://www.theregister.com/2018/10/23/paul_vixie_slaps_doh_as_dns_privacy_feature_becomes_a_standard/).

Source: @paulvixie Twitter account, October 20, 2018.

[7] Source: Alex Turing and Genshen Ye, "An Analysis of Godlua Backdoor," 360 Netlab Blog, July 1, 2019 (https://blog.netlab.360.com/an-analysis-of-godlua-backdoor-en/).

Source: @paulvixie Twitter account, October 21, 2018.

[8] Three groups have already adopted TLS 1.3: megasites like Facebook, Google, and Netflix; content delivery networks like Akamai and Cloudflare; and enthusiastic early adopters with isolated web properties.

[9] Adoption of the previous version of TLS, 1.2, proceeded at about 10% per year after it was introduced. TLS 1.3 will do the same, barring a TLS 1.2 security vulnerability. After the 2014 POODLE vulnerability, the internet at large was very quick to leave SSLv3 behind, with all browsers and most web properties upgrading within a year, writes Ivan Ristić in the Qualys SSL Labs Blog. Source: Ivan Ristic, "SSL 3 is dead, killed by the POODLE attack," Qualys Security Blog, October 15, 2014 (https://blog.qualys.com/ssllabs/2014/10/15/ssl-3-is-dead-killed-by-the-poodle-attack).

[10] Source: Tommy Jensen, Ivan Pashov, and Gabriel Montenegro, "Windows will improve user privacy with DNS over HTTPS," Microsoft Networking Blog, November 17, 2019 (https://techcommunity.microsoft.com/t5/networking-blog/windows-will-improve-user-privacy-with-dns-over-https/ba-p/1014229).

[11] One of the very last bits of plain-text data to disappear is the ancient "server name indicator" field of the TLS handshake, which helps CDNs direct HTTPS requests to the correct website. NAV tools use the SNI to determine the destination of the connection without having to even look at DNS. Encrypted SNI (currently in draft status in the IETF working group) addresses that leak. CDN vendor Cloudflare (one of its designers) has already rolled it out in the US. Multiple vendors have told Forrester that they're not yet seeing encrypted SNI traffic with their customers, and its adoption isn't yet a foregone conclusion. Both Chrome and Firefox can be instructed not to use DoH, though there's no single way to disable both.

[12] Source: "HTTP Client Fingerprinting Using SSL Handshake Analysis," Qualys SSL Labs (https://www.ssllabs.com/projects/client-fingerprinting/).

[13] Source: John Althouse, "TLS Fingerprinting with JA3 and JA3S," Salesforce Engineering, January 16, 2019 (https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967).

[14] Source: "Bots Tampering with TLS to Avoid Detection," The Akamai Blog, May 15, 2019 (https://blogs.akamai.com/sitr/2019/05/bots-tampering-with-tls-to-avoid-detection.html).

[15] Source: Troy Kent, "TLS Fingerprinting: Rethinking Encrypted Traffic Analysis Strategies," Security Boulevard, July 24, 2019 (https://securityboulevard.com/2019/07/tls-fingerprinting-rethinking-encrypted-traffic-analysis-strategies/).

[16] Mozilla (or was it Firefox?) just pulled back its TLS 1.0 EOL due to some government COVID-19-related sites still being TLS 1.0.

[17] The McAfee secure web gateway supports TLS 1.3. Fortinet's FortiGate firewall has supported for TLS 1.3 for over two years. Gigamon recently debuted a TLS-proxy in April 2020. For most other vendors, TLS 1.3 is on their 2020 roadmap, which means general availability on a case-by-case basis in 2021.

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.