New EMA Research Examines the Adoption of TLS 1.3 in the Enterprise

73 percent of survey respondents have either already begun enabling TLS 1.3 for inbound connections or are planning to enable it within the next six months, while 74 percent have either begun TLS 1.3 enablement for internal connections or plan to enable it for internal traffic within the next six months.

BOULDER, Colo. (PRWEB) January 30, 2019 -- Enterprise Management Associates (EMA™), a leading IT and data management research and consulting firm, has released a new research report titled “TLS 1.3 Adoption In the Enterprise: Growing Encryption Use Extends to New Standard,” based on criteria defined by Paula Musich, research director of security and risk management at EMA. This report sought to gauge awareness of and adoption plans for the new TLS 1.3 specification published by the IETF in August, 2018 as RFC 8446, and to better understand how enterprises are adapting to the growing use of encryption overall.

The TLS 1.3 specification was published in August 2018, ten years after its predecessor 1.2 became an IETF standard. The new standard lowers latency and improves the privacy of end-to-end communication, but it comes at a cost for enterprises. This is because it replaces the existing static RSA key exchange with the Diffie-Helman Ephemeral (DHE) perfect forward secrecy key exchange, which requires that a monitoring solution has access to the ephemeral key for each session, rather than a static key per server. Although perfect forward secrecy existed in TLS 1.2, it was optional. In TLS 1.3, it is required. This makes it much harder for enterprises to passively monitor traffic to inspect for malware, data breaches, and malicious activity, as well as troubleshoot availability or performance issues on the network.

Some industry groups have expressed serious reservations over the ability to decrypt and inspect traffic for troubleshooting and possible malware using TLS 1.3. The good news, however, is that a healthy percentage of respondents in the survey are either already in the throes of enabling TLS 1.3 or plan to enable it in the near future, with 73 percent of respondents indicating that they have already begun enabling TLS 1.3 for inbound connections or are planning to enable it within the next six months. At the same time, 74 percent of respondents have either begun TLS 1.3 enablement for internal connections or plan to enable it for internal traffic within the next six months.

“There’s no question that security practitioners are concerned about the security implications of TLS 1.3 and the potential to miss malware and attackers hidden in encrypted traffic, but that’s not stopping enterprises from enabling TLS 1.3 in the near term,” said Musich.

Some other key data points this research sheds light on includes:

- One of the biggest drivers behind the quick enablement of the new TLS 1.3 standard is the early adoption of TLS 1.3 by major web services, web server, and browser vendors, including Apple, CloudFlare, Google, and Microsoft.
- When asked what their top three concerns were over the adoption of TLS 1.3 by major web server and browser vendors with respect to their effect on internal web application and services development, 21 percent indicated they were most concerned about the increased development lifecycle time and cost.
- In terms of top security worries, twenty-seven percent of respondents indicated they were most concerned about losing visibility into the data center, while 24 percent were most concerned about losing visibility into the core of the network.

PRWeb ebooks - Another online visibility tool from PRWeb
- Ninety-five percent of respondents indicated that their security architectures will need to change in order to accommodate TLS 1.3 and its perfect forward secrecy mandate.
- The survey asked respondents how concerned their organizations were that their existing security monitoring practices/technologies will miss malware hidden in encrypted files. Thirty-five percent of all respondents said they were either very or extremely concerned, while 36 percent said they were somewhat concerned.

Despite publicized concerns about its implications for existing security architectures and the operational constraints it puts on troubleshooting problems on the network, however, security practitioners appear to be ready to embrace the new TLS 1.3 standard. The report delves into the strategies enterprises are implementing or plan to implement to enable this new standard.

A detailed analysis of the research findings are available in the report, “TLS 1.3 Adoption In the Enterprise: Growing Encryption Use Extends to New Standard.”

Highlights from the report will be revealed during the February 28 Webinar, TLS 1.3 Adoption in the Enterprise: Growing Encryption Use Extends to New Standard.

About Enterprise Management Associates (EMA)
Founded in 1996, EMA is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com.
Contact Information
Raleigh Gould
Enterprise Management Associates
http://www.enterprisemanagement.com
303-543-9500

Online Web 2.0 Version
You can read the online version of this press release here.