REPORT SUMMARY: TLS 1.3 ADOPTION IN THE ENTERPRISE

Growing Encryption Use Extends to New Standard

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research
Written by Paula Musich

January 2019

SPONSORED BY:

ixia
A Keysight Business

EMA™ IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

TABLE OF CONTENTS

Introduction

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. Inline interception is still possible, but it increases latency to the point that, in most networks, it becomes impractical. At the same time, TLS 1.3 encrypts the certificate itself, which makes it harder for enterprises to gather critical metadata. Out-of-band network traffic analysis with decryption is also still possible given the ability for the analysis product to access the relevant session keys, but its use is more limited than inline decryption in all enterprises, and especially among small- to medium-sized businesses.

Given these changes and the need to adapt in order to continue monitoring and troubleshooting networks, industry groups like the Enterprise Data Center Consortium became involved in the later stages of the TLS 1.3 specification's development to try to achieve reduced latency and improved privacy benefits while preserving existing management practices. Although it did not succeed, the Consortium continues to look for fixes or workarounds. In the meantime, enterprises are beginning to start on the path toward adoption. This study is designed in two parts to examine:

1. IT practitioners' concerns about TLS 1.3, their adoption plans, approaches to dealing with visibility issues, expected costs, etc.
2. Overall encryption adoption, practices, concerns, and trends within enterprise networks

Top Security Worries: Visibility into Application Security and the Data Center

In ranking four potential issues caused by lost visibility on a scale of one to four, with one being the most concerned and four being the least concerned, 57 percent of respondents indicated the inability to monitor application security was their top concern.

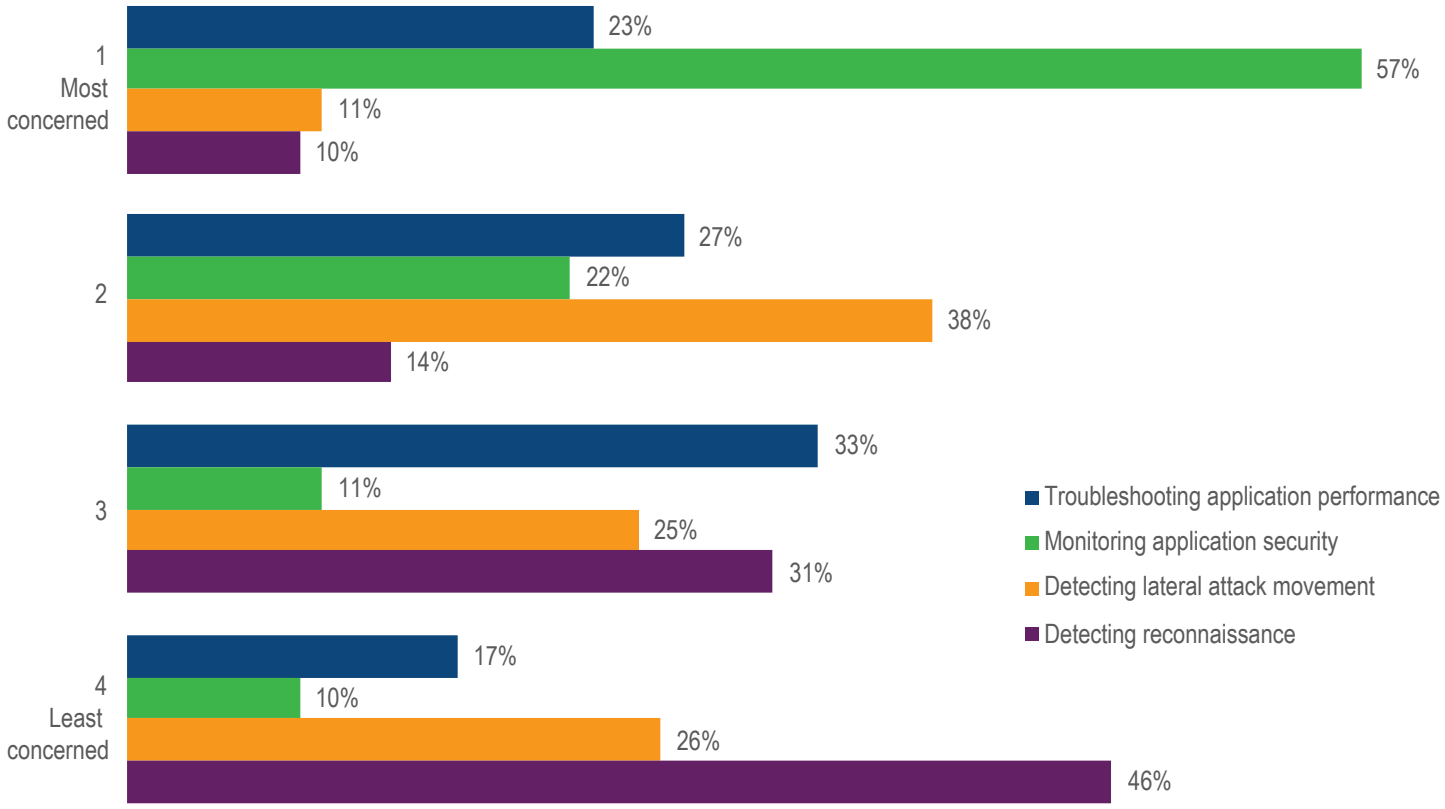

Figure 1: Lost Visibility into Application Security is the Biggest Concern

As in real estate, it's all about location, and when it comes to location and lost visibility, it wasn't surprising that the biggest concern for lost visibility was concentrated first in the data center, and second in the core of the enterprise network. When asked to rank eight different locations in the order that lost visibility concerned them, with one being the most concerned and eight being the least concerned, 27 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. It was a bit surprising that with the rapid adoption of cloud services, respondents seemed least concerned about losing visibility into east-west traffic in private and public cloud locations.

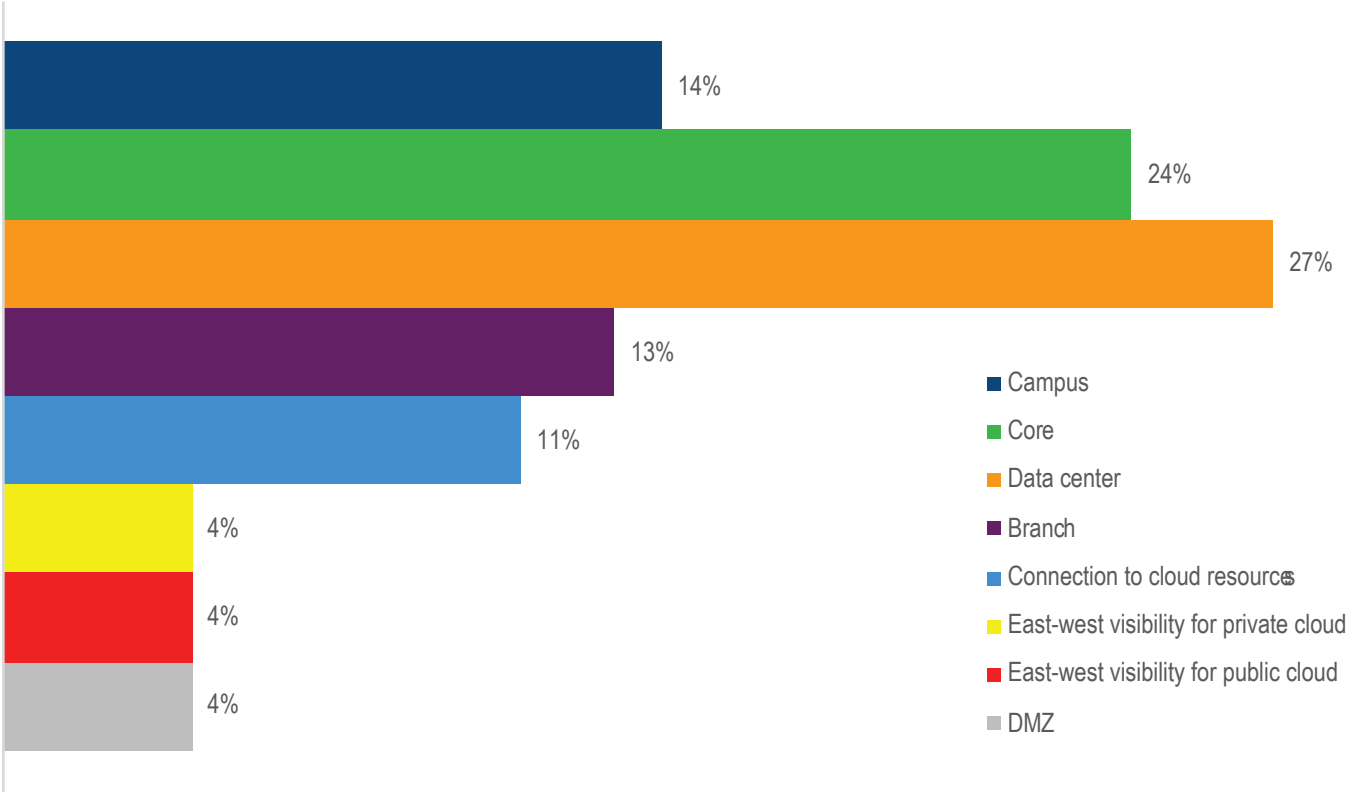

Figure 2: Lost Visibility Concerns According to Location

Operational Issues in Enabling TLS 1.3

There are multiple operational concerns surrounding the enablement of TLS 1.3 within the enterprise, not only for IT operations and security, but also for internal web applications and web services development. With major web server and browser vendor adoption pushing enterprises ahead in their enablement plans, respondents expressed concerns over the increased cost and amount of time it takes to develop web applications. In fact, 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, and another 21 percent indicated they were most concerned about the increased development training time and costs. Another 21 percent expressed the increase in operations lifecycle time and cost as one of their top three concerns.

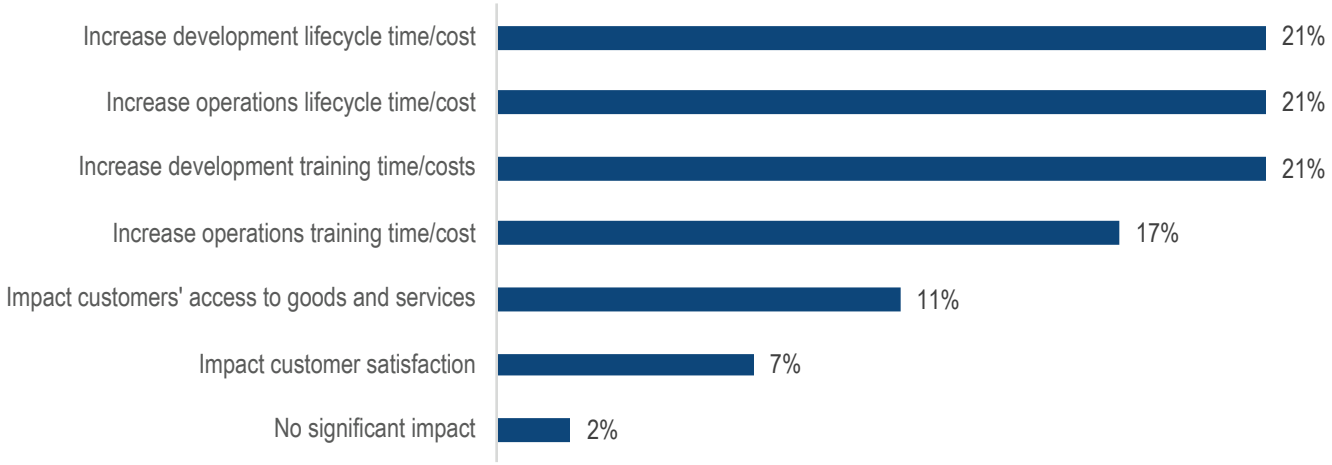

Figure 3: Top Three Concerns on Internal Web Application Development Driven by Web Server Vendor Adoption of TLS 1.3

While moving along with their TLS 1.3 enablement efforts, respondents demonstrated that they have no illusions that it will be business as usual when it comes to their security architectures and the changes in the TLS 1.3 standard. Ninety-five percent of respondents indicated that those security architectures will need to change in order to accommodate TLS 1.3 and its perfect forward secrecy mandate. They differed on exactly how significant that change is, however. Half of the respondents who believe a change is required think that change will be slight, while 45 percent view it as requiring a significant change. It's interesting to note that a larger majority of respondents in very large enterprises (62%) view the required change as slight.

TLS 1.3 Enablement Forging Ahead

Those concerns, however, have not stopped organizations from forging ahead with their efforts to enable the use of TLS 1.3 within the enterprise. A full 73 percent of respondents have either already begun enabling TLS 1.3 for inbound connections, or are planning to enable it for those inbound connections 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. Only two percent of respondents indicated that their organizations did not intend to enable TLS 1.3. This is surprising for a few reasons. The specification was only published in August of 2018, just a few months before the survey was released. At the same time, common wisdom suggests that when faced with significant changes, IT organizations (especially larger IT shops) tend to move more slowly and cautiously to adapt to such changes. Perhaps the best example of that is the long adoption period for IP V6. Respondents turned that thinking around, demonstrating that very large enterprises are leading the adoption charge. Fifty-nine percent of VLEs reported TLS 1.3 enablement was already underway for inbound connections, and 55 percent for internal connections. Enterprises followed next with 40 percent and 45 percent, respectively, already underway for inbound and internal traffic. It's also interesting to note that 40 percent all respondents are in the process of implementing TLS 1.3 for internal traffic, and 41 percent of all respondents anticipate enabling it for inbound connections within six months.

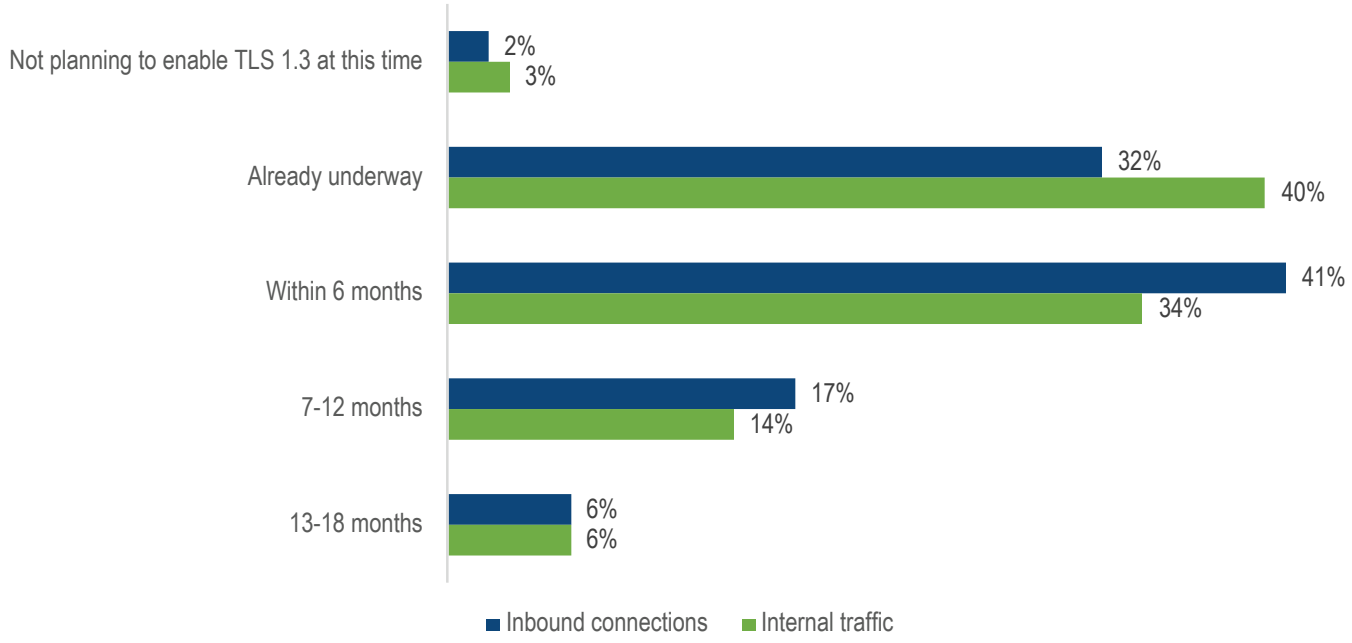

Figure 4: Timeframes for TLS 1.3 Enablement for Inbound and Internal Connections

Drivers Behind Quick Adoption

Perhaps one of the biggest drivers behind such 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 impact that adoption had on their plans for TLS 1.3 enablement, respondents (by a clear majority) indicated that it forced them to accelerate their plan. Sixty-three percent indicated they felt forced to accelerate their plan, while only 33 percent said it had no impact. It's interesting to note that while a majority of SMBs and very large enterprise groups indicated that they were forced to accelerate their enablement plans due to early browser vendor adoption, VLEs as a group felt the least pressure (52%) to enable TLS 1.3 and more of them said it had no impact. However, since that group is further along the adoption curve, that would suggest that more VLEs had planned adoption all along. At the same time, it appears that even those who believe they have a strong understanding of TLS 1.3 and are highly motivated to upgrade their current systems to remain compatible with cloud and web services, may not be as informed as they think. Though TLS 1.3 impacts aspects of security, network, and application performance monitoring, there should be little impact on day-to-day use and web operations. Thus, the greatest need for work comes not from impacting business, but from maintaining the ability to provide visibility into the traffic for security and operations troubleshooting.

Figure 5: Impact of Early Adoption by Major Browser Vendors on Enterprise TLS 1.3 Enablement Plans

It's possible there are additional business drivers for using a more advanced encryption standard on internal traffic. For example, enterprises have grown to recognize that their networks are compromised and they see the new transport encryption standard as a way to better secure their more sensitive and valuable data. That explanation is proven in the study findings when looking at the benefits respondents see in enabling TLS 1.3. Respondents were given a list of seven possible motivations for enabling TLS 1.3 and asked to rate each one according to its relevance to their organization on a five-point scale, from very important to not at all important. The advantages rated most important to all respondents were improved data security (73%) and improved privacy for end-to-end security (67%). Decreased latency through faster session setup time took a backseat to the security benefits of TLS 1.3 in respondents' eyes, with only 44 percent indicating that was a very important driver for adoption.

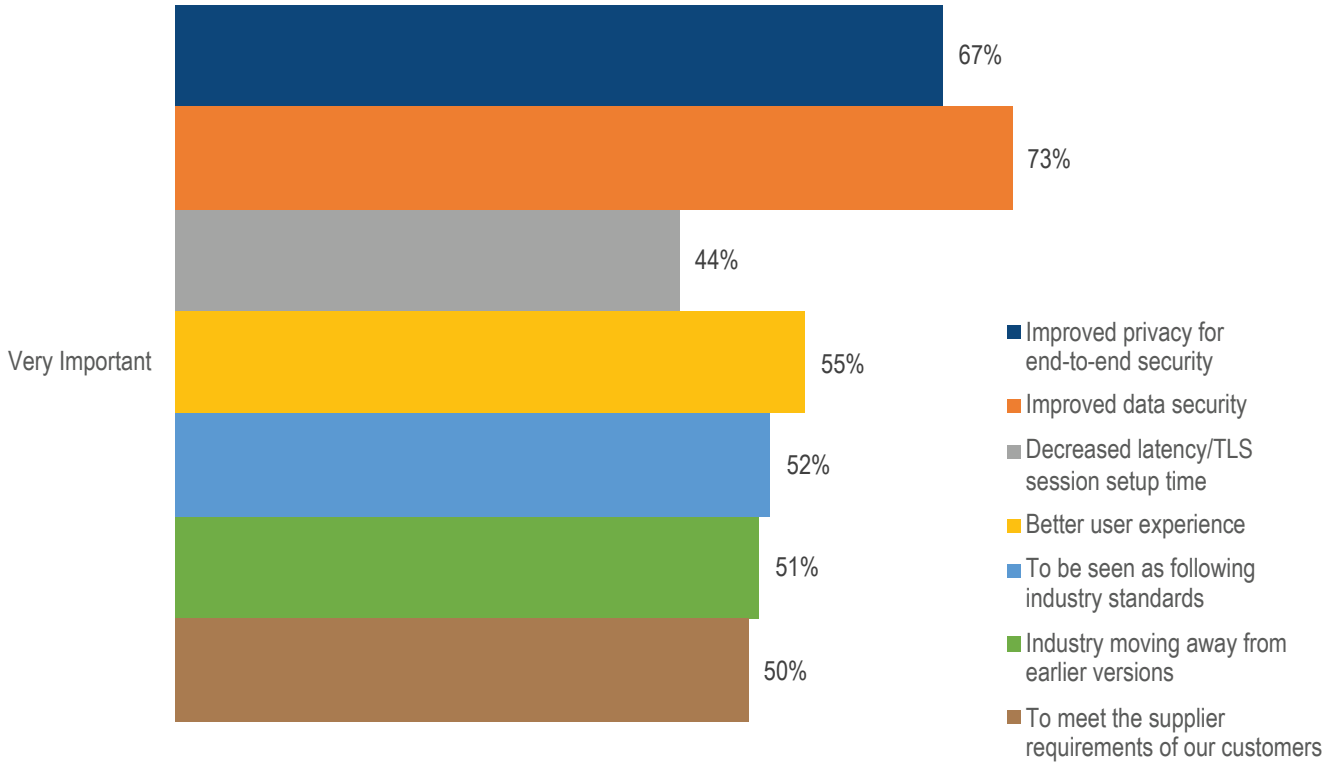

Figure 6: Top Motivations for Enabling TLS 1.3

Nearly 30 percent of very large enterprises still view the architectural change as requiring over $1 million in investment. Of course, that's a drop in the bucket for enterprises with IT budgets exceeding $100 million annually. When looked at through the lens of the annual IT budget, 54 percent of respondents reporting an IT budget of $50 to $100 million expect the security architecture change will cost between $251,000 to $500,000. Fifty-one percent of respondents reporting an annual IT budget of between $10 million to less than $25 million expect the cost to adapt their organization's security architecture will range between $101,000 to $250,000. On the other end of the size spectrum, none of the respondents representing SMBs expect the cost to adapt to be under $50,000—although the sample size of SMB respondents was small.

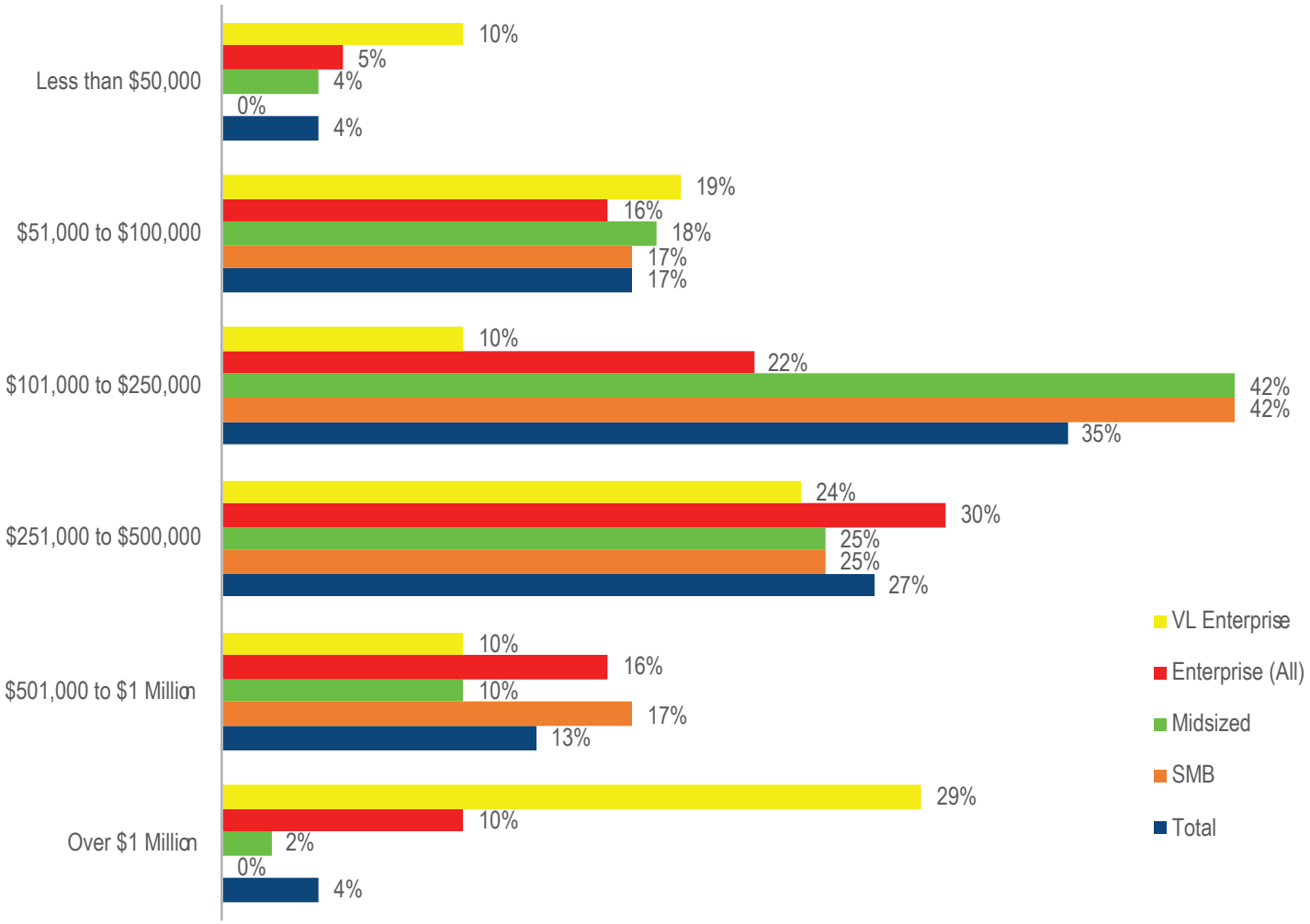

Figure 7: Estimated Costs to Adapt Security Architectures to TLS 1.3 by Company Size

Strategies for Enabling TLS 1.3

When it comes to dealing with the visibility issues caused by TLS 1.3, respondents appear to be mulling over several strategies. Overall, 60 percent are looking to maintain existing firewalls at earlier versions of TLS for as long as possible, and a majority of respondents at medium-sized enterprises indicated that is their top strategy. Respondents in large or very large enterprises appeared to be split in their top choice, between maintaining existing firewalls at earlier versions of TLS for as long as possible and enabling decryption and re-encryption on existing inline security devices and hoping that it doesn't add too much latency, complexity, or security vulnerability. The TLS 1.3 PFS mandate puts IT security and operations practitioners in large enterprises between a rock and a hard place. The former choice suggests a disconnect between apparent plans to move ahead with TLS 1.3 enablement while at the same time maintaining existing firewalls at earlier versions of TLS for as long as possible. The latter is akin to a Hail Mary pass – suggesting some level of desperation or optimism. In addition, half of all respondents reported that they would look for inline alternatives that enable decryption and inspection by existing security controls without exacting a significant performance penalty—also a clear second choice for medium-sized enterprises. Only respondents representing SMBs indicated that their clear top choice was to replace existing stateful inspection firewalls with proxy-based firewalls, with 69 percent indicating that option. That being said, it's important to keep in mind that the sample of SMB respondents was small.

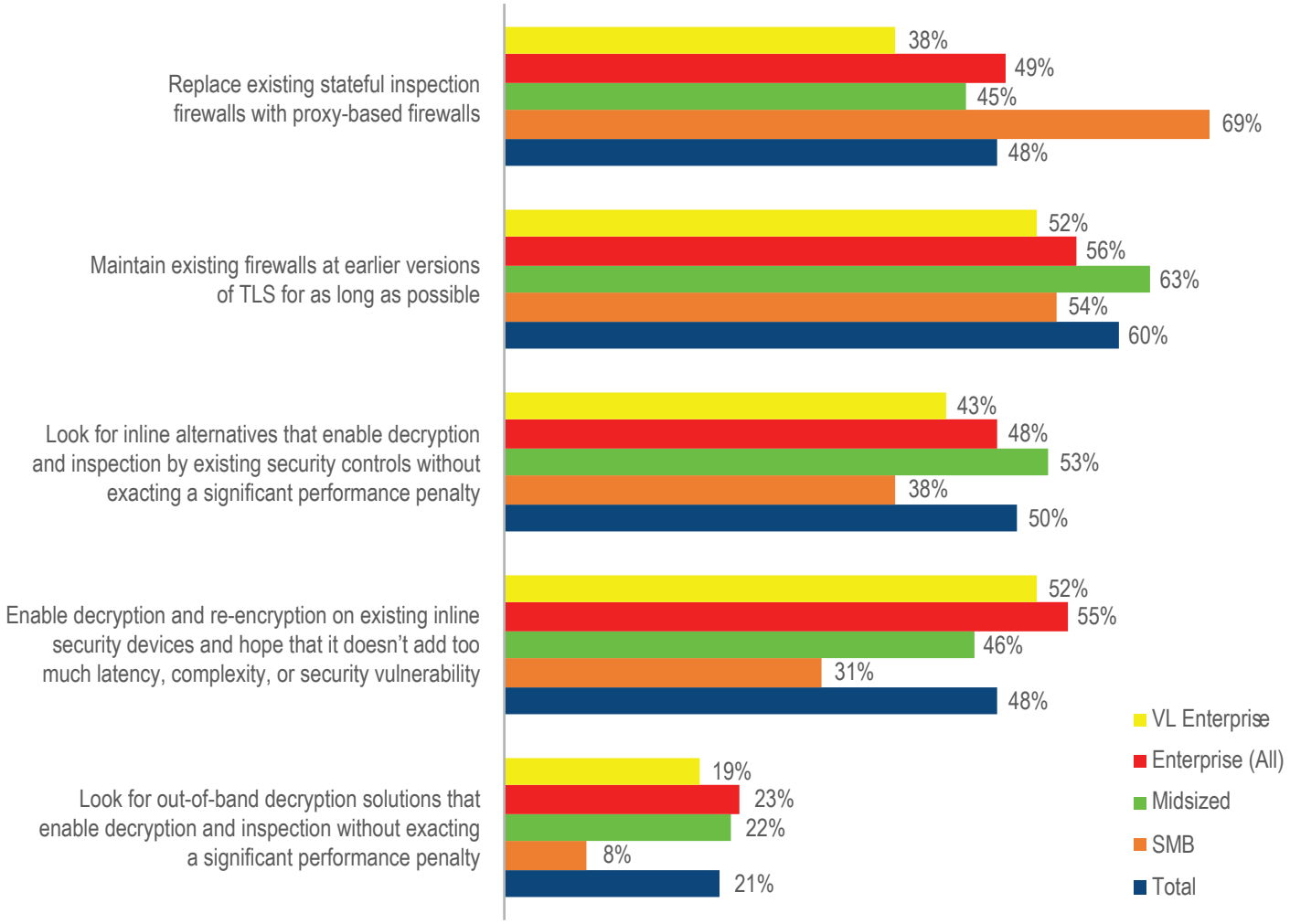

Figure 8: Options Considered for Addressing TLS 1.3 Visibility Issues

Where to Begin?

As organizations grapple with architectural issues associated with enabling TLS 1.3, they are not likely to enable it carte blanche across all applications and network traffic at once. There are several approaches enterprises can take in enabling TLS 1.3 across the enterprise network. The survey revealed that different-sized organizations are likely to take different approaches. For example, over half of respondents representing large enterprises indicated they intend to enable TLS 1.3 for critical traffic first, then other traffic if convenient. Conversely, 46 percent of respondents representing SMBs indicated that their organizations intend to enable TLS 1.3 for all traffic at once. For medium-sized enterprises, the top choice appeared to be enabling TLS 1.3 for critical traffic only, with 40 percent of those respondents identifying that as their top approach. These differences suggest that the varying levels of network complexity, security operations sophistication, and available talent all play a role in how different-sized organizations intend to approach enablement. Curiously, despite the increasingly stringent privacy regulations being enacted in both the U.S. and Europe, regulatory compliance was not a factor for many respondents. Only seven percent of respondents overall indicated that their organizations would enable TLS 1.3 only where it was required for compliance.

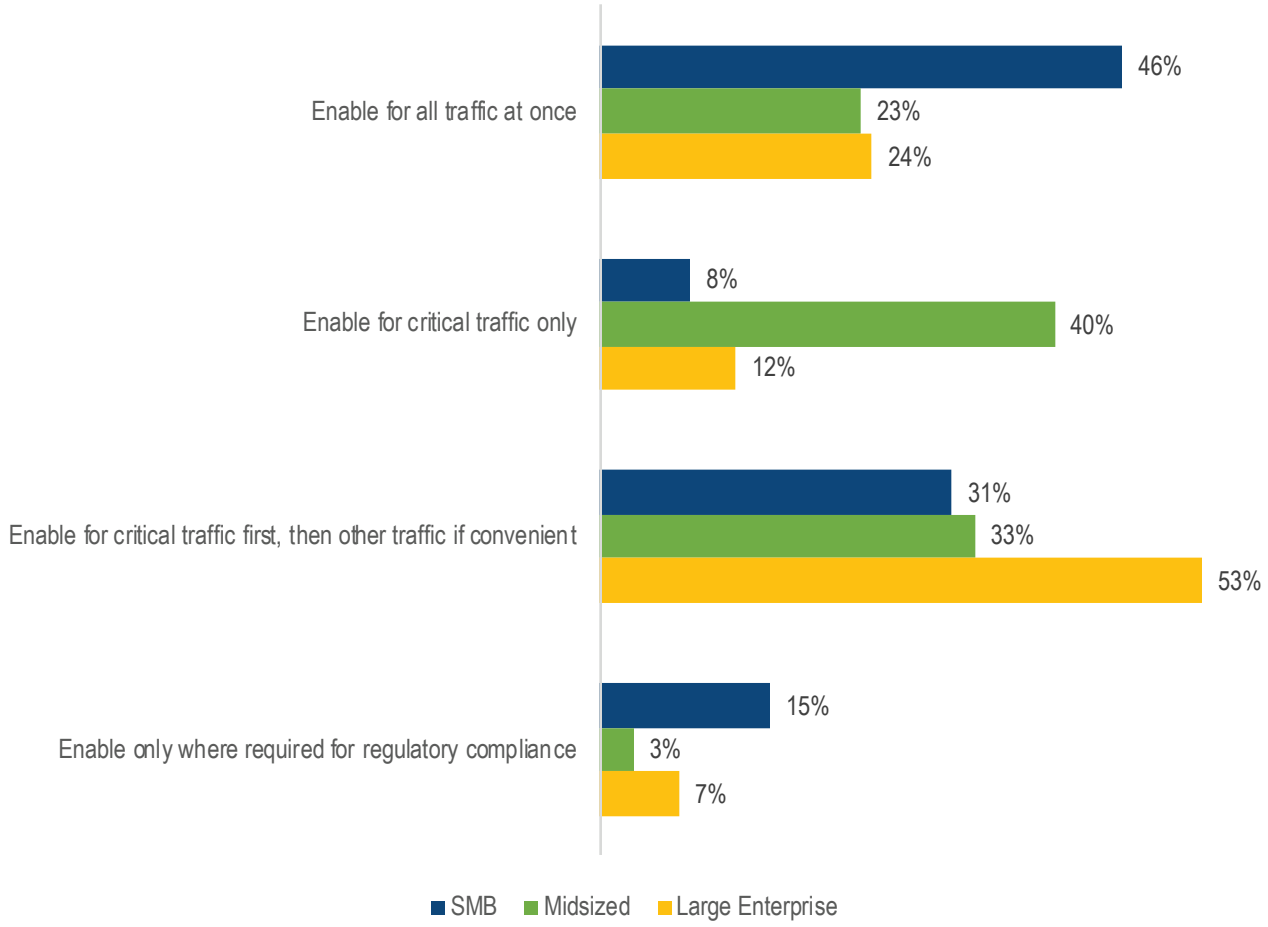

Figure 9: How Different-Sized Organizations Intend to Approach TLS 1.3 Enablement

Decryption Policies and Practices

IT has a range of options at its disposal to decrypt network traffic for troubleshooting performance and availability issues, as well as monitoring for malware and potentially malicious behavior. Such options generally fall into two types: inline or man-in-the-middle decryption and re-encryption, and passive or out-of-band decryption and re-encryption. Inline options generally exact a performance penalty and so are used sparingly within the enterprise network. Passive or out-of-band deployments are relatively common across large enterprises, especially those governed by regulatory compliance mandates. EMA asked survey participants which of five common methods they used and whether they performed decryption at all. Of those five methods, the top choice for all categories of organization sizes was to use a web proxy for decryption, followed closely by using an inline security device. However, for both SMBs and VLEs, the top choice was to use an inline security device. Less popular options include decrypting using an out-of-band security device, an inline load balancer, and an inline dedicated decryption device. Curiously, 12 percent of VLE respondents indicated their organization does not decrypt any of their enterprise's traffic—the largest percentage of all the organization sizes.

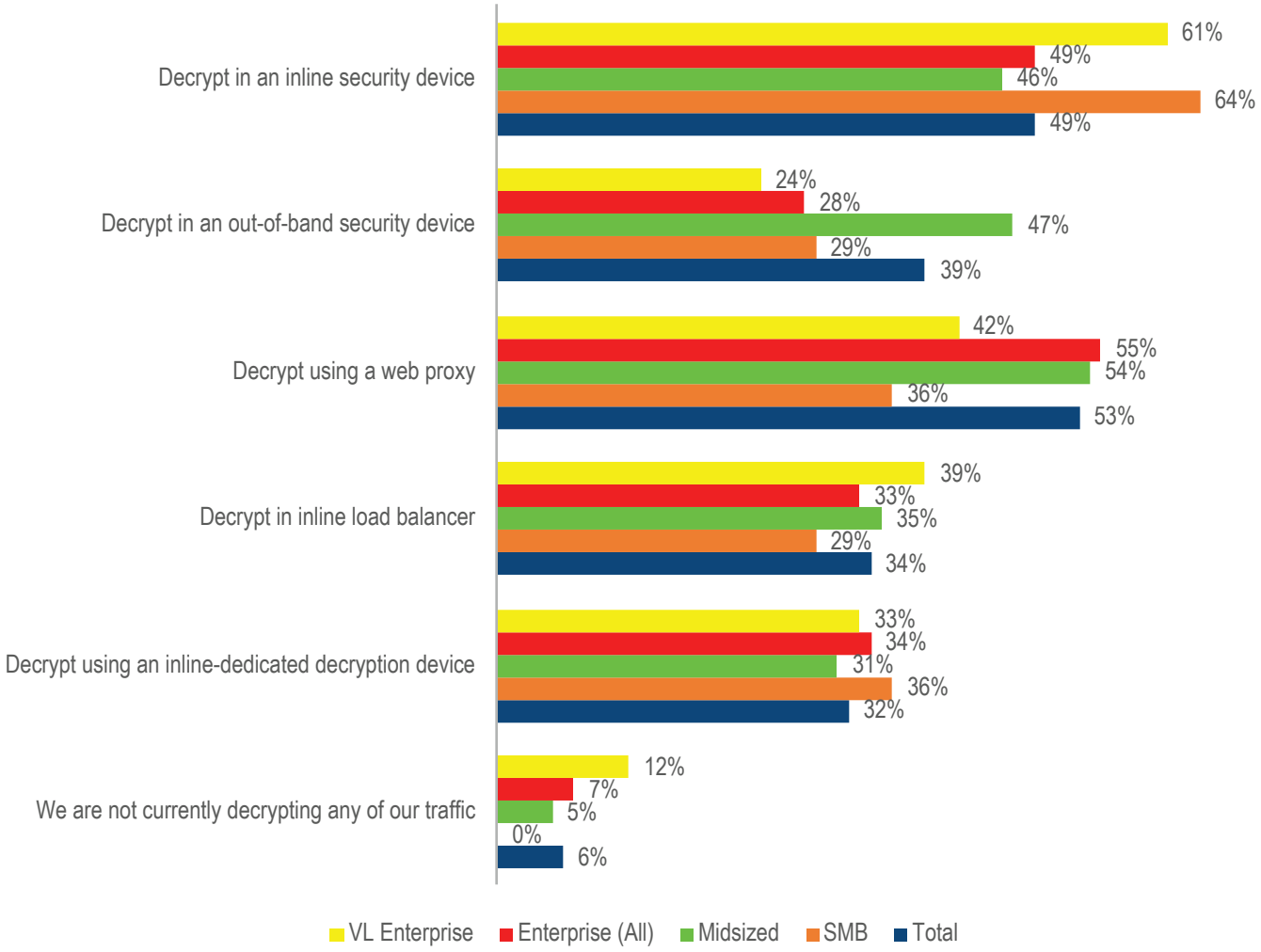

Figure 10: Current Decryption Methods

Conclusion

The use of encryption across enterprise networks of all sizes is widespread and growing quickly. It is not just limited to the data center, and its use is spreading out across multiple locations and to applications at a rapid clip. Although concerns exist around the ability to detect malicious activity or malware hidden in encrypted files, those concerns do not appear to slow encryption's momentum across the network.

At the same time, security practitioners appear to be ready to embrace the new TLS 1.3 standard, despite publicized concerns about its implications for existing security architectures and the operational constraints it puts on troubleshooting problems on the network. Security practitioners are clearly aware that the new standard will require a change in existing security architectures and anticipate the need to spend additional budget to enable TLS 1.3.

As they prepare to enable TLS 1.3, there is a caveat in survey participants' rollout plans. Some of the approaches to enabling the new standard indicated by respondents appear to be more wishful thinking than well-planned deployments. Some participants' organizations may find they have to go back to the drawing board and come up with a Plan B to enable TLS 1.3 without losing visibility, introducing unacceptable performance bottlenecks and greatly increasing operational overhead.

Whether they feel they have no choice but to enable TLS 1.3 because major web server and browser vendors have already pushed ahead with it, or because they need to keep pace with the industry as it embraces the new standard, is unclear. What is clear is that security practitioners see the new standard as offering greater privacy and end-to-end data security for their organizations, and that the long wait for its advancement is over.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (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 EMA's 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 or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3802-Keysight.012919