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:

ExtraHop

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

TABLE OF CONTENTS

Executive Summary

This research project 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. In its newest form, the transport layer encryption standard departs in significant ways from the longstanding TLS 1.2 version that a majority of enterprises have been using for years.

Some industry groups have expressed serious reservations over the ability to decrypt and inspect traffic for troubleshooting and possible malware using TLS 1.3, but the good news 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. Although it's common for IT practitioners to be unaware of the details of new standard specifications as they are hashed out by IETF insiders, a very clear majority of the respondents in the survey indicated great familiarity with it on a technical level.

Multiple factors drive the surprisingly quick adoption plans for the new standard. The fact that major web server and browser vendors have already implemented TLS 1.3 within their products is one factor. Another is the perceived benefits in improved privacy and end-to-end data security that come with the enhancements made to the standard. Still, serious concerns around application security monitoring are tempering enthusiasm for the standard.

The fast rise in the use of encryption across the Internet is mirrored within large and small enterprises alike. While the use of encryption for the data center and enterprise networks increased the most over the last 18 months, enterprises will turn their attention to internally developed applications and web services over the next 18 months.

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 the use of out-of-band decryption is not as pervasive as inline decryption, 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

Methodology and Demographics

This research project draws from an online survey of 249 respondents in a range of IT-related roles in enterprises primarily serving North American markets and secondarily other regions across the globe. IT or IT-related roles represented among respondents fell across 12 different areas of responsibility, with the heaviest representation among IT-related Directors and Managers at 40 percent, followed by CIO/CTO/IT-VP at 15 percent. It should also be noted that 67 percent of all respondents reported that IT security was their primary role in the organization.

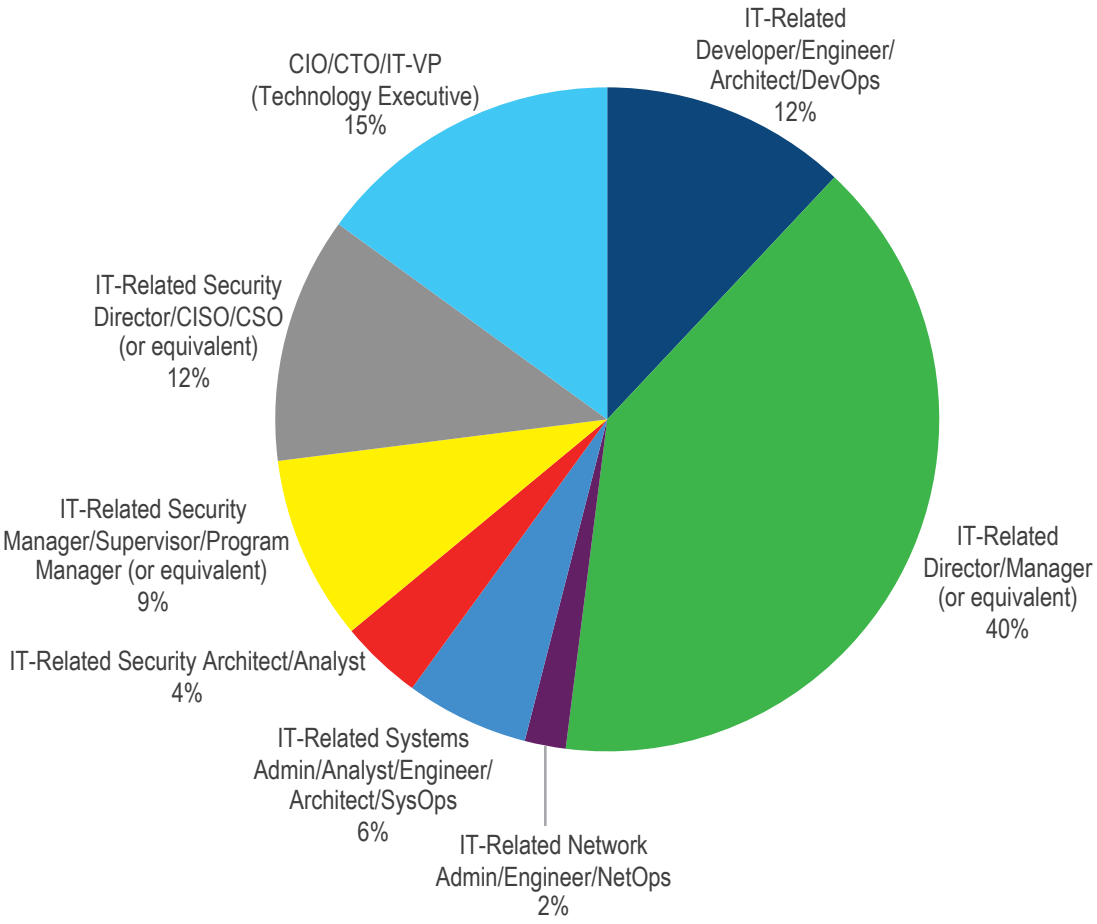

Figure 1: Organizational Roles

Key Findings

Given the implications of the TLS 1.3 specification, it's not surprising that a clear majority of respondents expressed both operational and security concerns over implementing TLS 1.3 within their organizations. Fifty-six percent of all respondents expressed either some or significant operational concerns, while 61 percent expressed either some or significant security concerns.

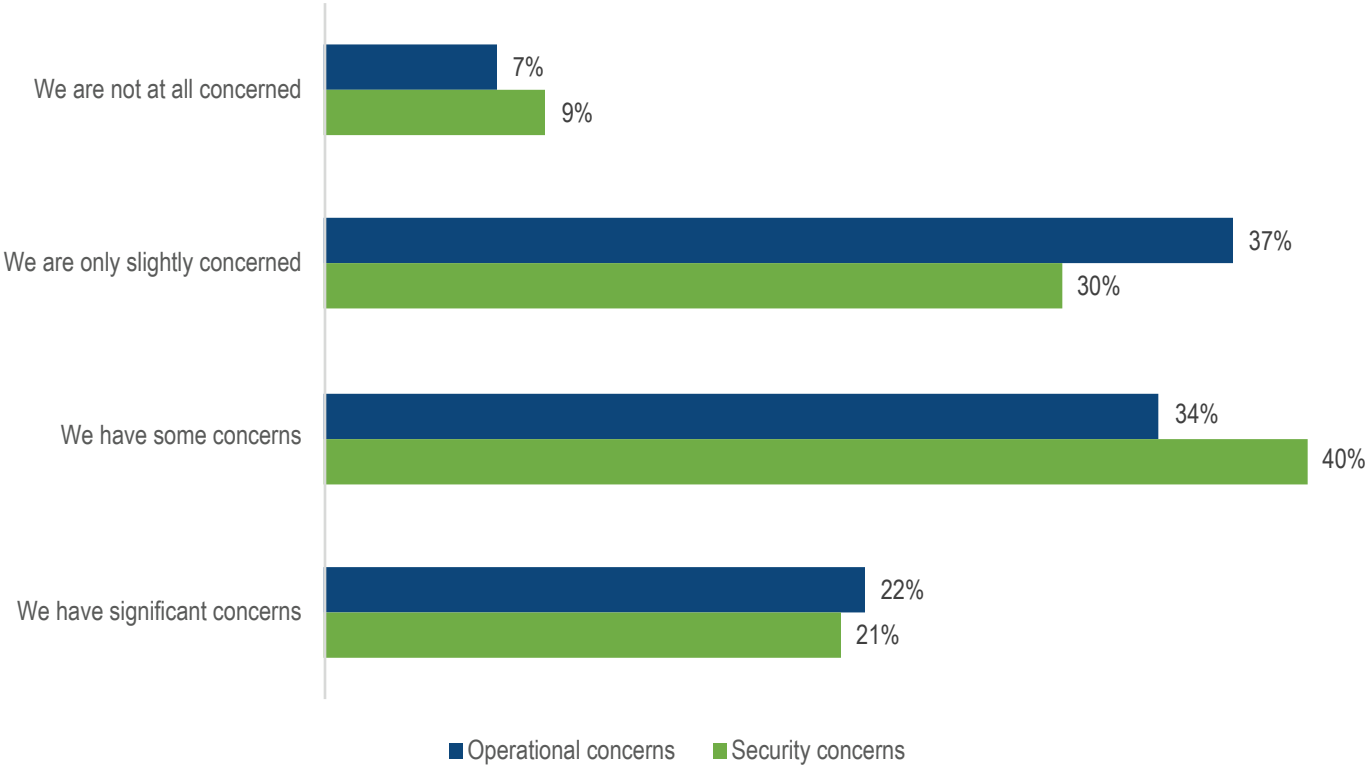

Figure 2: Level of Operational and Security Concerns for Implementing TLS 1.3

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.

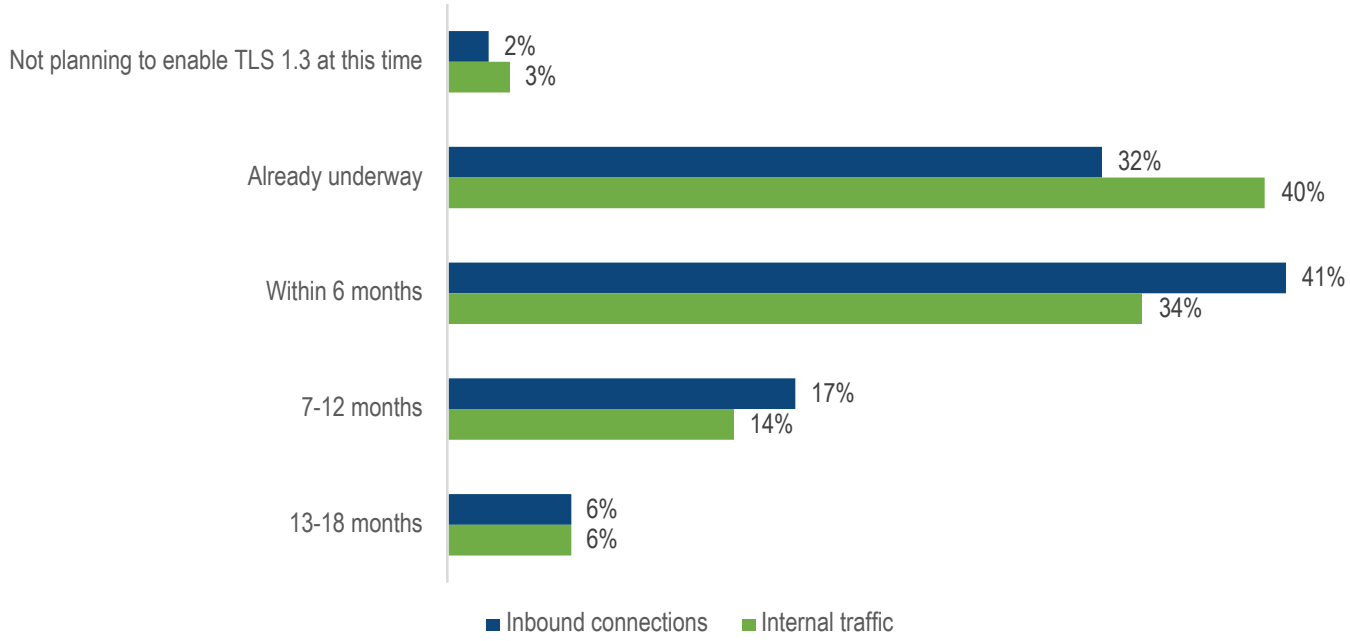

Figure 3: Timeframes for TLS 1.3 Enablement for Inbound and Internal Connections

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 4: 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.

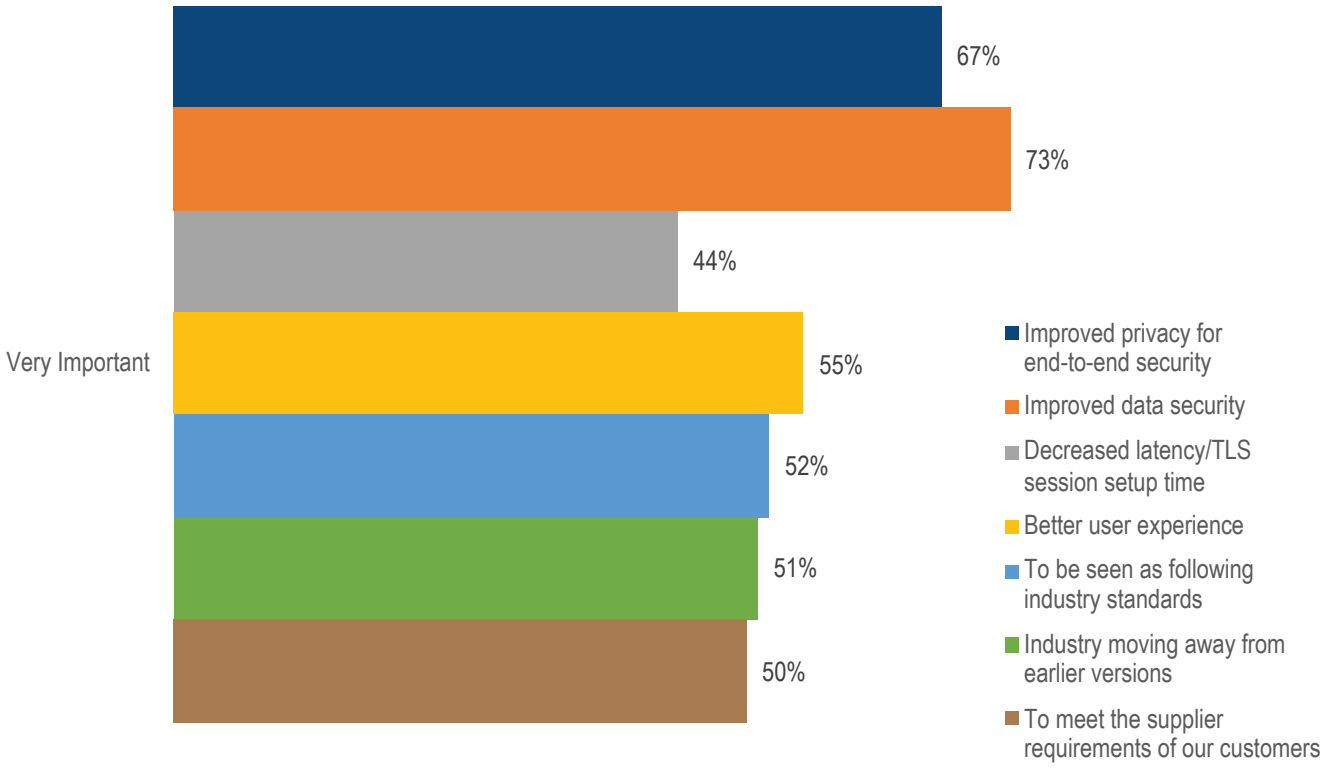

Figure 5: Top Motivations for Enabling TLS 1.3

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.

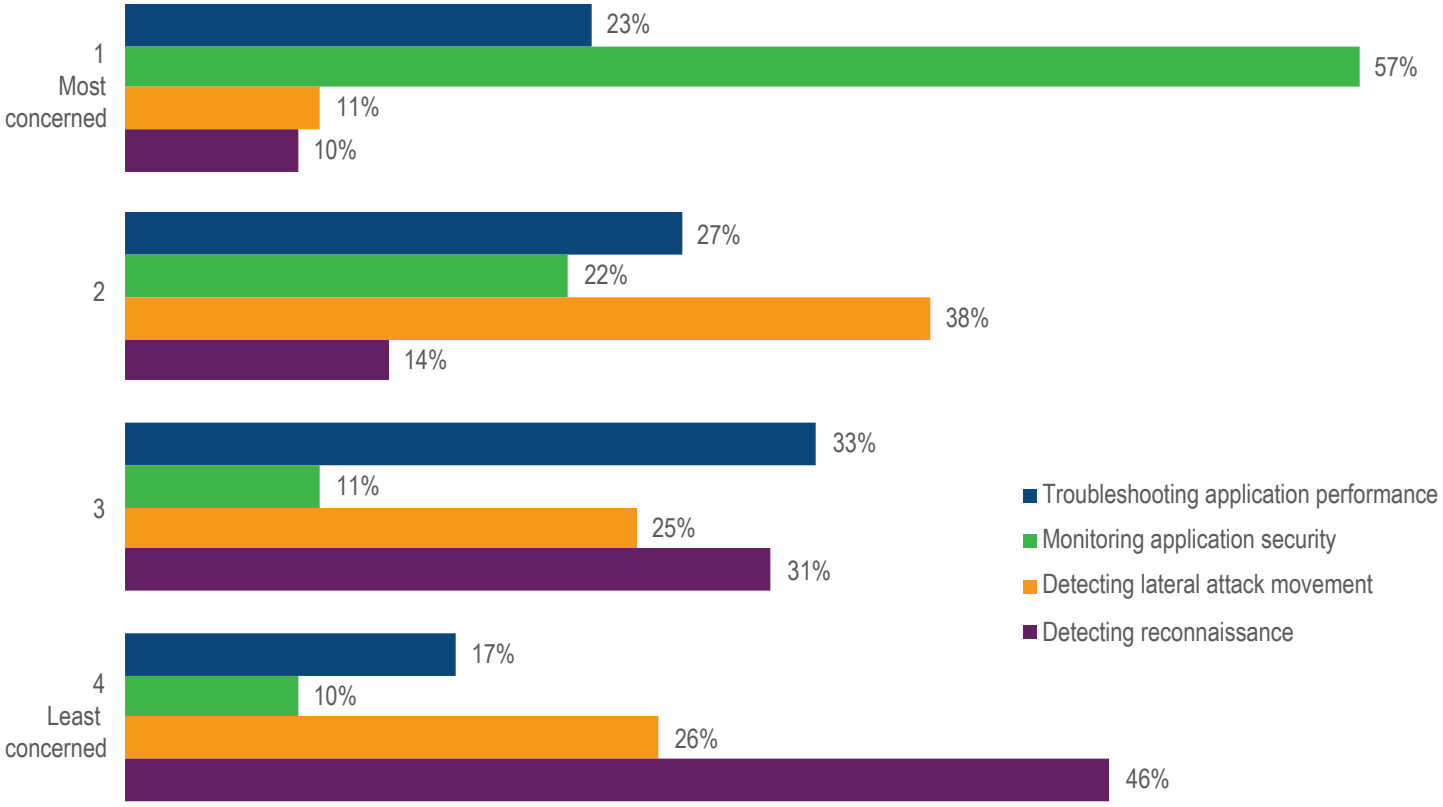

Figure 6: Lost Visibility into Application Security is the Biggest Concern

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.

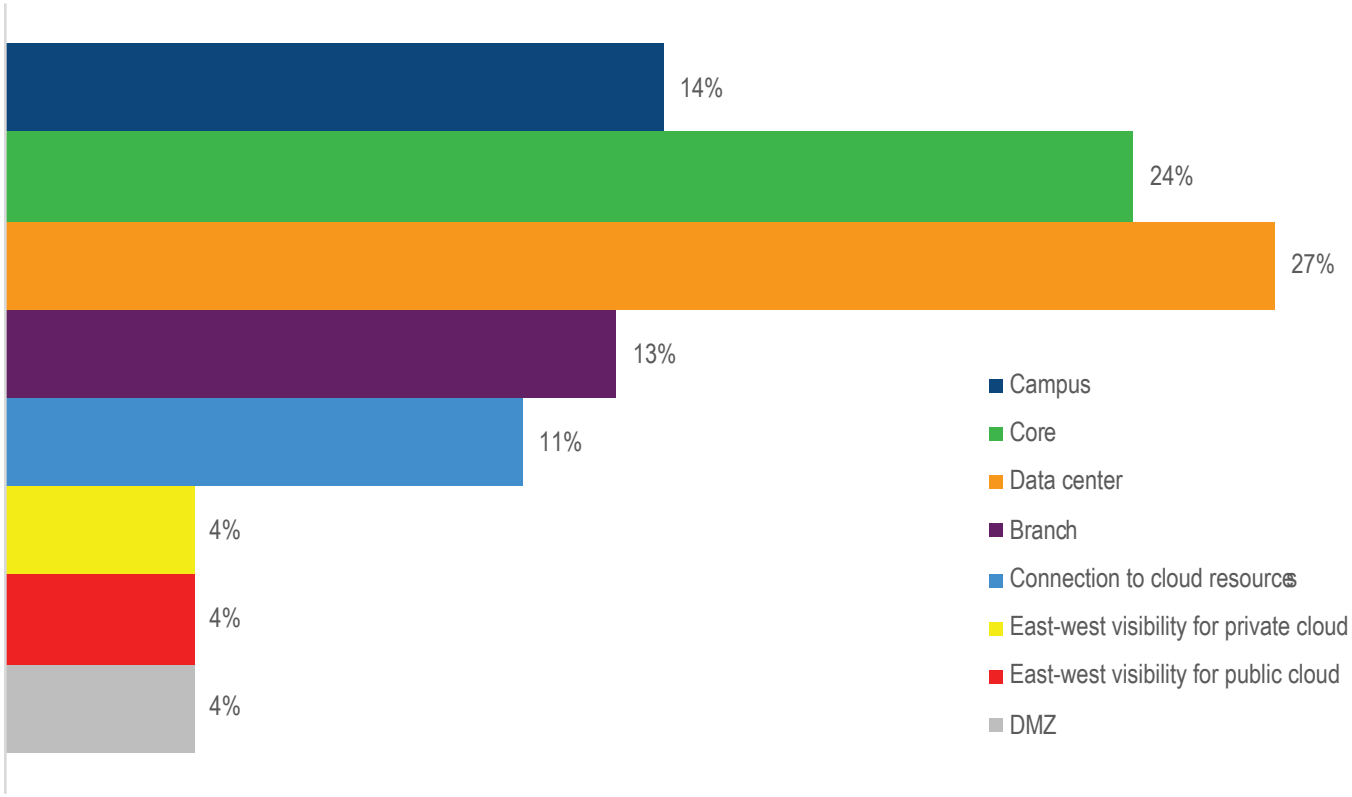

Figure 7: Lost Visibility Concerns According to Location

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.

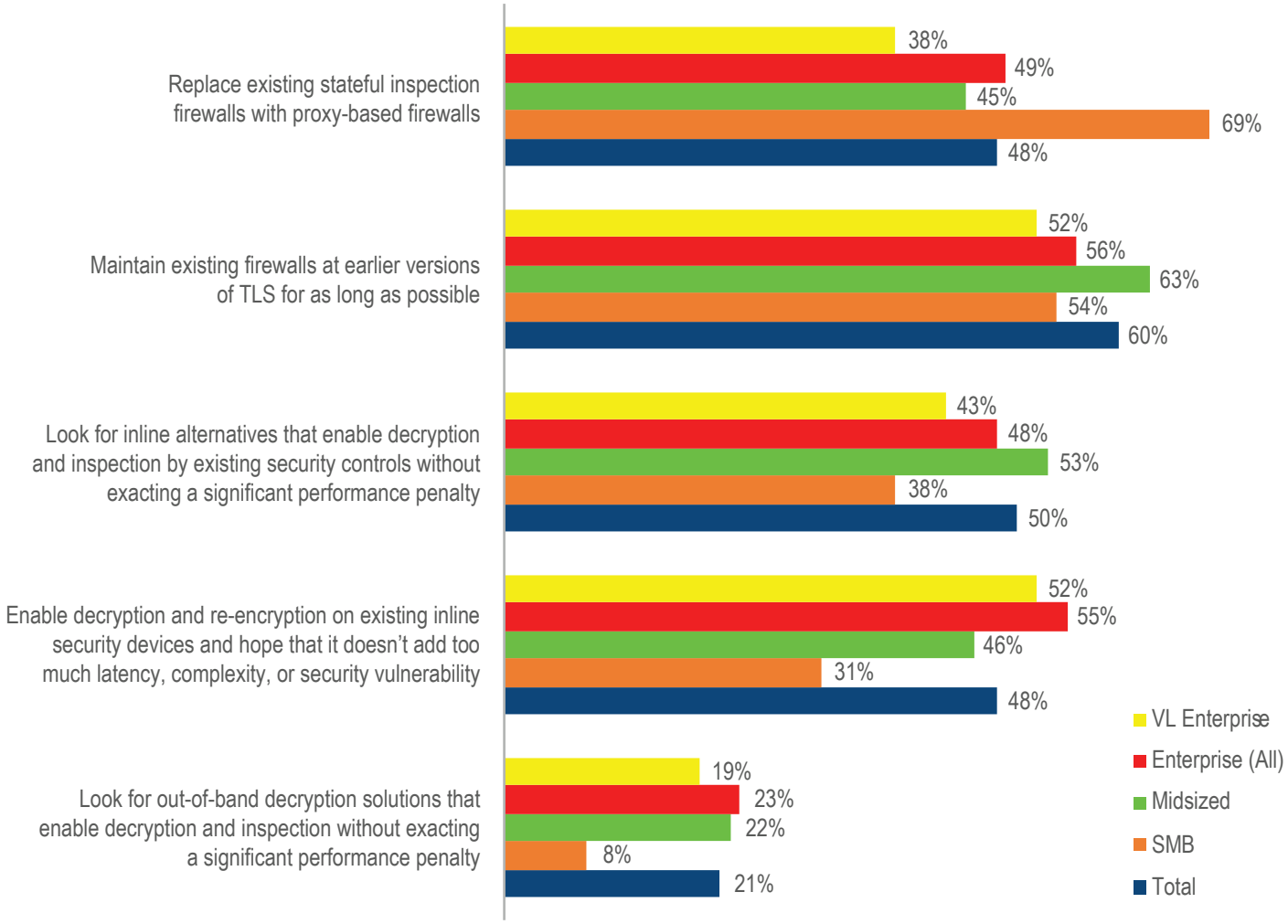

Figure 8: Options Considered for Addressing TLS 1.3 Visibility Issues

Despite the visibility issues caused by the perfect forward secrecy function, which exists within the longstanding TLS 1.2 standard as an option rather than a mandate, a clear majority of respondents reported that their organizations had already enabled that option, with 70 percent of all respondents indicating its usage. That suggests that organizations of all sizes view the increased privacy and end-to-end data security advantages of PFS as critical. At the same time, 76 percent of all respondents foresee enabling and setting preference for TLS 1.3 connections to their organization's applications, even though PFS is already enabled with TLS 1.2. There are several potential explanations for what could be driving that planned migration to the new standard. It could be that respondents believe the additional privacy and data security benefits in TLS 1.3 outweigh the concerns and costs associated with upgrading to the new standard. Other motivations selected as very important by at least half of all respondents include a better user experience, to be seen as following industry standards, and to meet supplier requirements of customers. Alternatively, it could be that they feel they are forced to move to the standard because the top web server and web browser vendors have already adopted TLS 1.3. Indeed, 51 percent of all respondents indicated that they are motivated by the fact that the industry is moving away from earlier versions.

Figure 9: Do you foresee enabling and setting preference for TLS 1.3 connections to your applications, even if PFS is already enabled within TLS 1.2?

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.

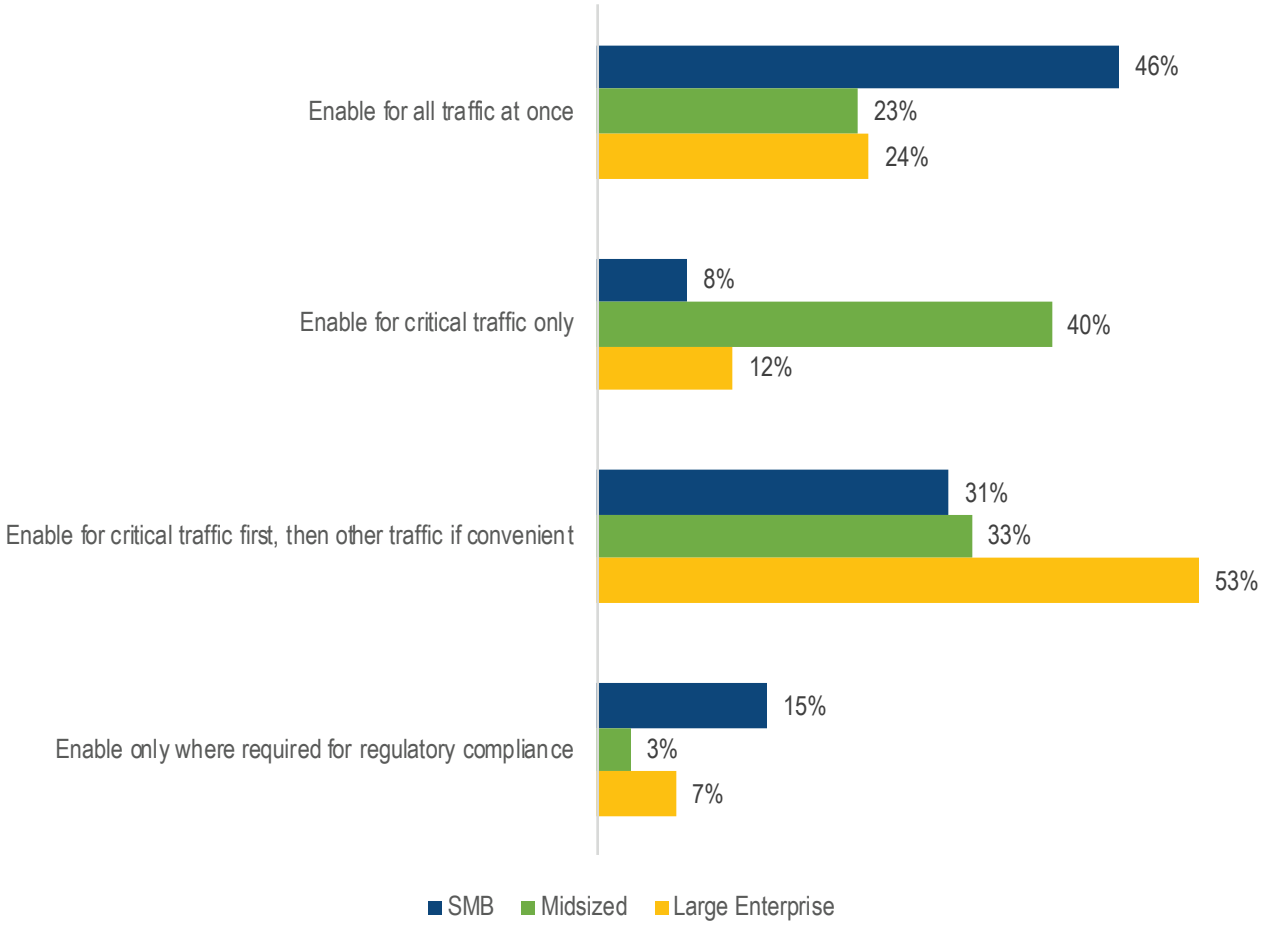

Figure 10: How Different-Sized Organizations Intend to Approach TLS 1.3 Enablement

Encryption Practices and Concerns Within the Enterprise

The increasing use of encryption both across the public Internet and within private enterprise networks is well documented. Estimates range from 50 percent of Internet traffic, to 72 percent of all network traffic, to 80 percent of U.S. network traffic. Also fairly well documented is the growing use of encryption by bad actors to hide their attacks, whether those are stealthy advanced attacks aimed at exfiltrating sensitive data, phishing attacks, or ransomware. At the intersection of both trends is the increasing worry that existing methods used to monitor for malware and malicious activity are no longer effective. To gauge the level of anxiety among respondents about such issues, 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. Only six percent said they were not at all concerned. Nearly the same percentages were reported in expressing the level of concern that existing security monitoring practices/technologies would miss malicious behavior hidden in legitimate traffic.

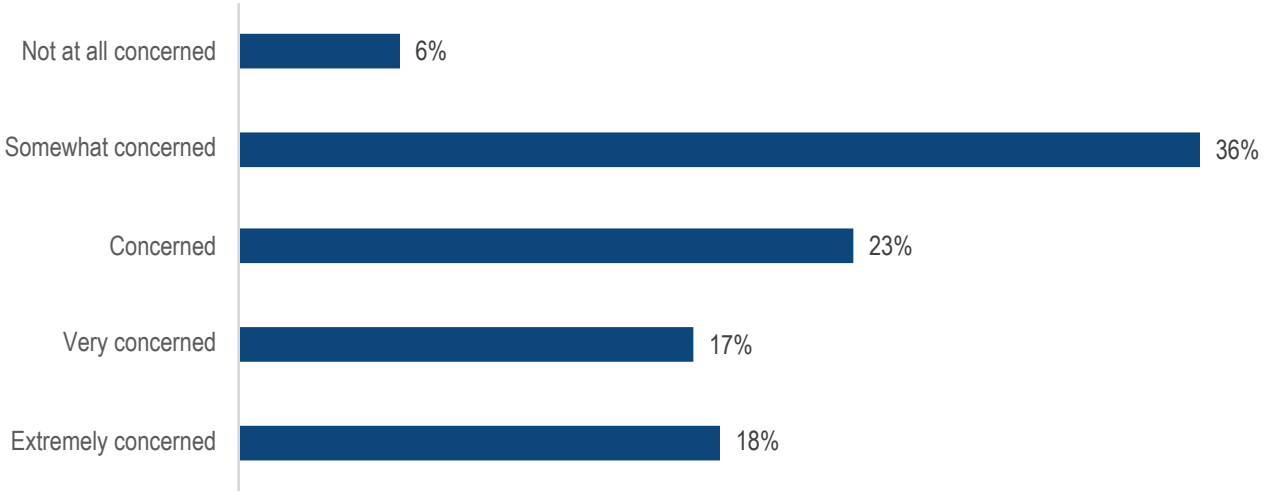

Figure 11: As more network traffic is encrypted, how concerned is your organization that your existing security monitoring practices/technologies will miss malware hidden in encrypted files and malicious behavior hidden within legitimate traffic?

Current Practices

Despite those concerns, there is no going back. From a policy perspective, enterprises are clearly mandating the use of transport encryption to protect data, and TLS is the protocol of choice. Eighty-one percent of all respondents mandate the use of TLS to encrypt at least some data, although which version of the standard varies. Not surprisingly, the majority of respondents mandate the longstanding TLS 1.2 version, although TLS 1.3 appears to be gaining ground. Very large enterprises are driving adoption of the new standard. While 17 percent of all respondents say their organizations mandate the use of TLS 1.3 to encrypt data, that percentage rose to 33 percent for very large enterprises.

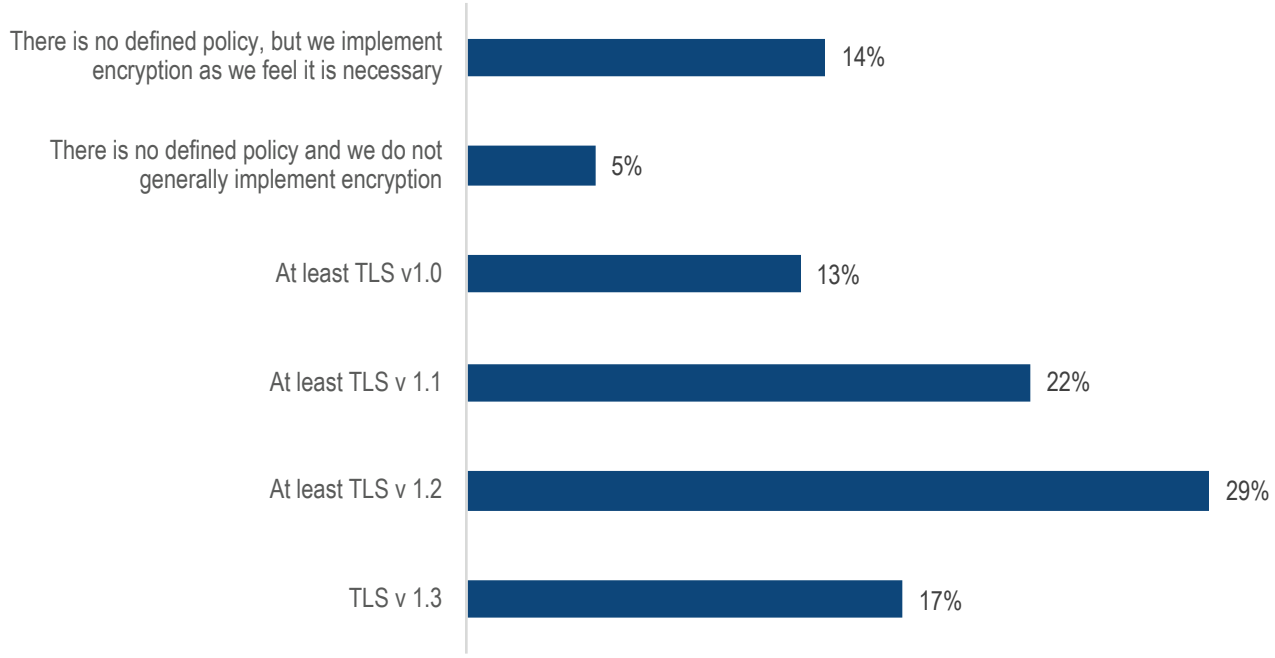

Figure 12: Does your organization mandate any transport encryption standards for any of its data?

When it comes to specific locations within the enterprise network where encryption is being used and for what types of applications and services, it's not surprising that a clear majority of respondents use encryption first within the enterprise network, then within the data center at 76 percent and 71 percent, respectively. However, among SMB, mid-sized, large, and very large enterprises, VLEs are leading the way with 91 percent using encryption in their enterprise network, and another 67 percent using it in their data centers. VLEs are also leading the way among groups in encrypting web services traffic at 67 percent, which is also not surprising since those very large enterprises are further along the adoption curve in web applications development and in the use of web services. The same is true for internally developed applications, where 48 percent of VLEs are using encryption.

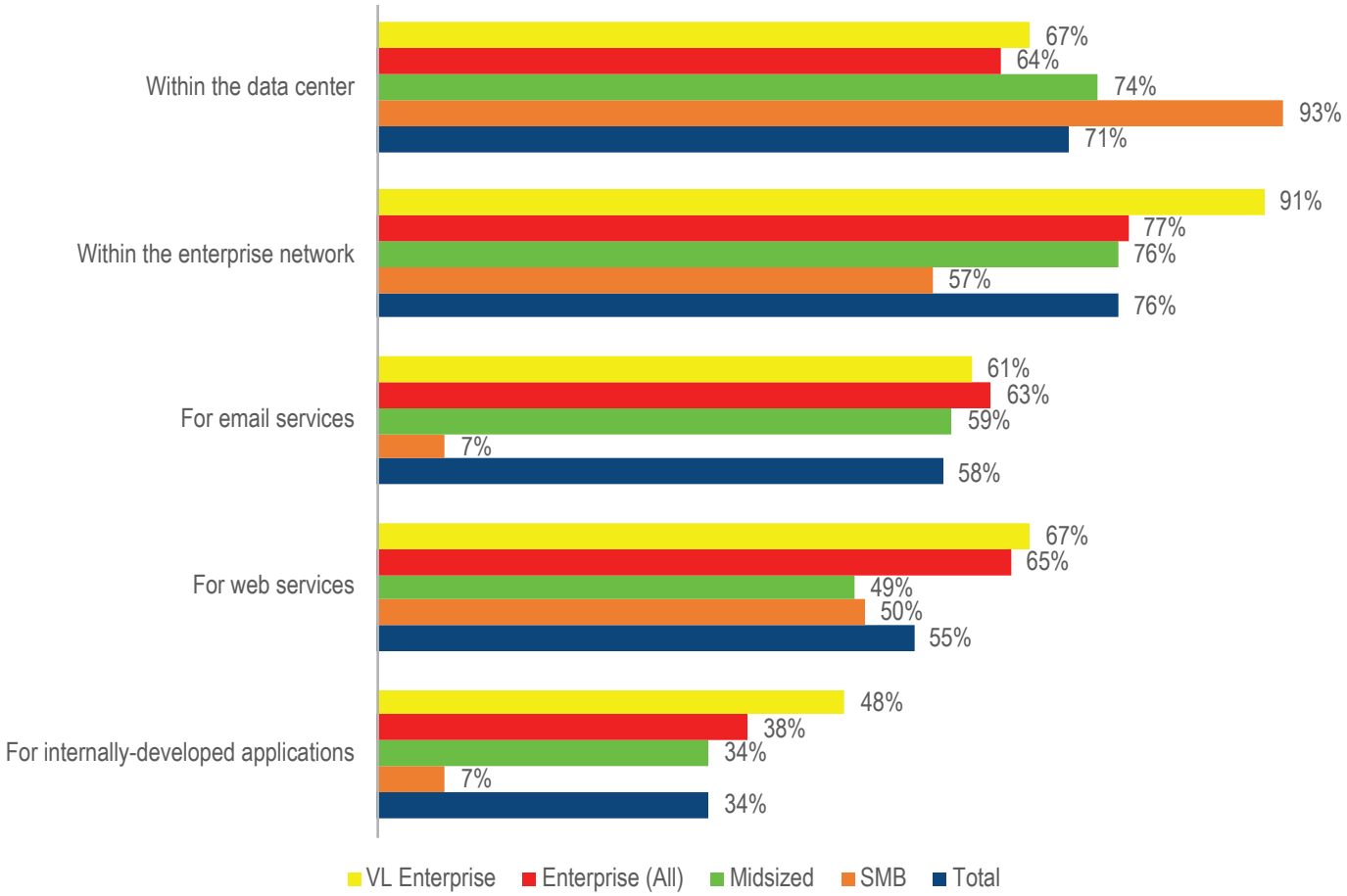

Figure 13: Where Encryption is Enabled

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. 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.

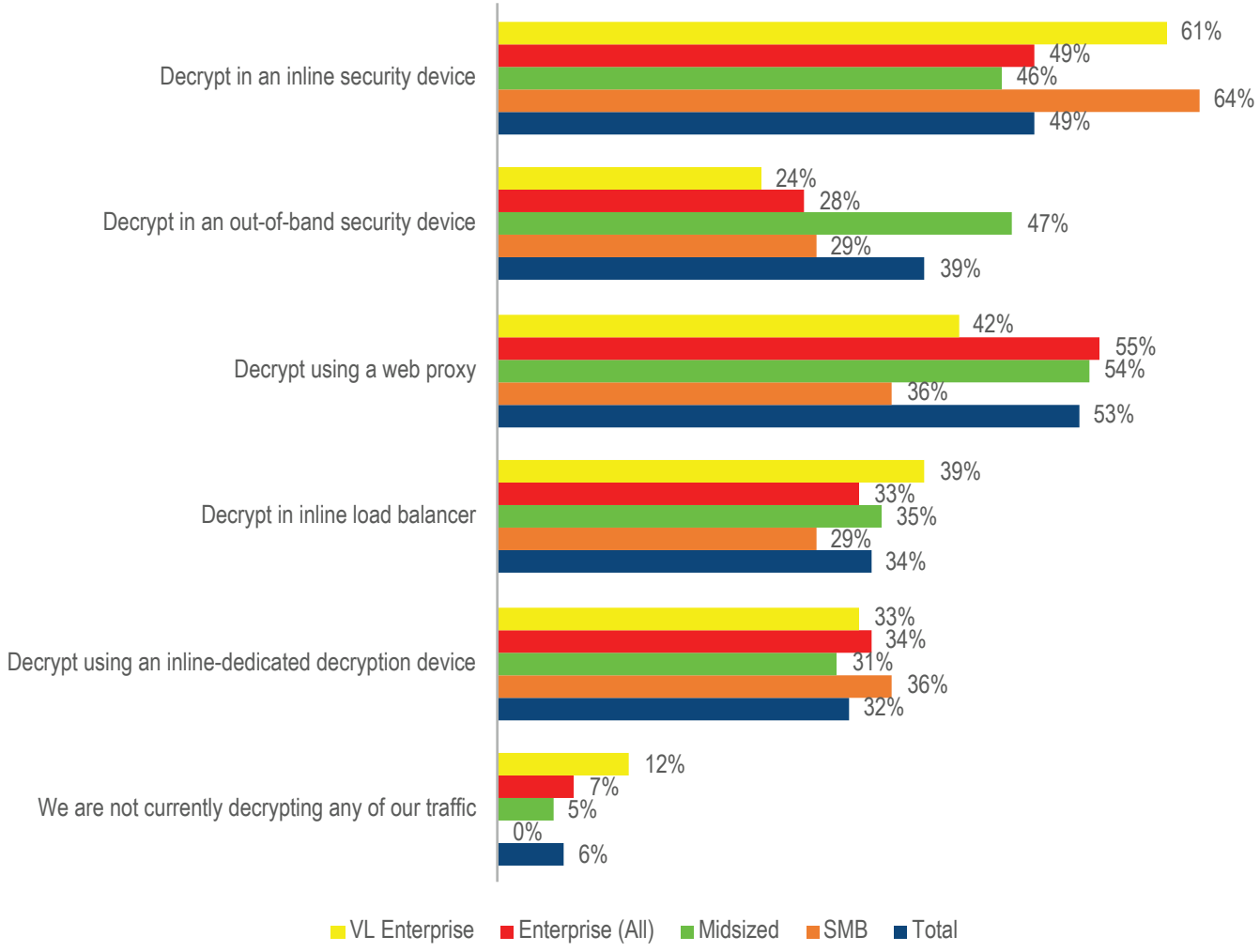

Figure 14: Current Decryption Methods

Organizations subject to regulatory mandates, such as the Health Insurance Portability and Accountability Act (HIPAA), PCI DSS payment card information, and a range of privacy regulations, are especially sensitive to the types of traffic they choose to decrypt for troubleshooting and monitoring. Respondents were asked which, if any, of four different decryption policies were used to determine what network traffic types are not decrypted for analysis. Those policies included no HIPAA traffic, no PCI payment card traffic, no personally identifiable information traffic, and no user credentials. As expected, a solid majority of large and very large enterprises choose not to decrypt personally identifiable information, more so than the other three types of traffic at 66 and 67 percent, respectively. For mid-sized enterprises, the clear choice on what not to decrypt landed on PCI payment card data at 70 percent. For SMBs, the clear choice on what not to decrypt was HIPAA-governed data, although that sample size was small.

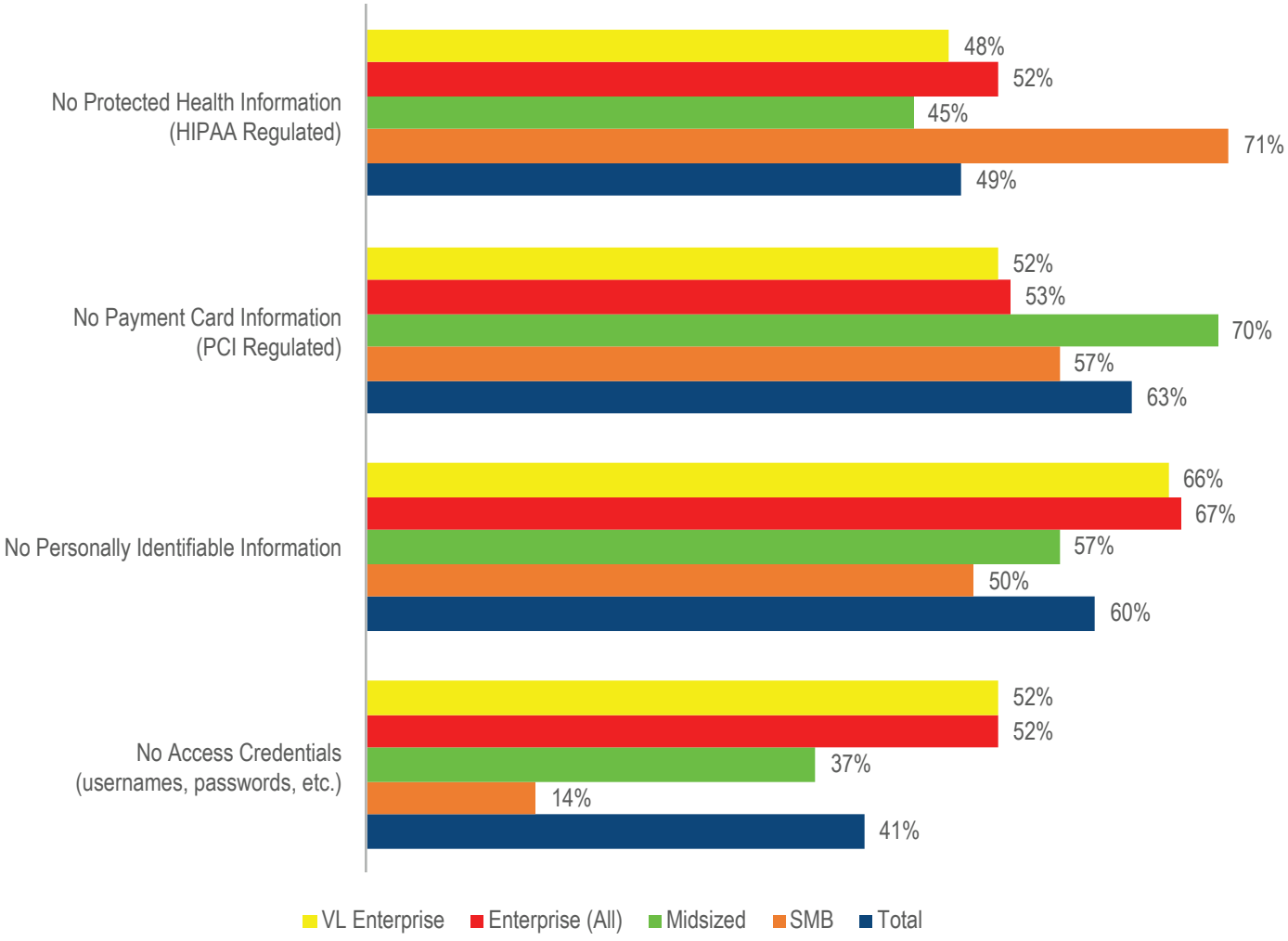

Figure 15: Which, if any, of the following policies does your organization follow in determining the types of traffic you decrypt for inspection?

Respondents were also asked what percentage of all network traffic their organizations currently decrypt for analysis. For SMB, mid-sized, and large enterprises, the top percentage range is between 26 to 50 percent, with a split at 50 percent SMB, 35 percent mid-sized, and 33 percent large enterprises reporting that range. For those groups, the next most often cited range was between 51 to 75 percent of traffic decrypted for analysis, with the split at 43/44/28 percent, respectively. The responses provided by participants at very large enterprises were interesting. That group was evenly split between 28 percent estimating 26 to 50 percent, and 28 percent who didn't know what percentage range of traffic their organizations decrypt for analysis. Given the great complexity of largescale networks and the decentralized nature of very large IT organizations, this lack of awareness is not unusual. What also stood out is that a significantly larger percentage of those very large enterprises reported that their organizations decrypted between 0 to 25 percent of traffic compared to the other three groups.

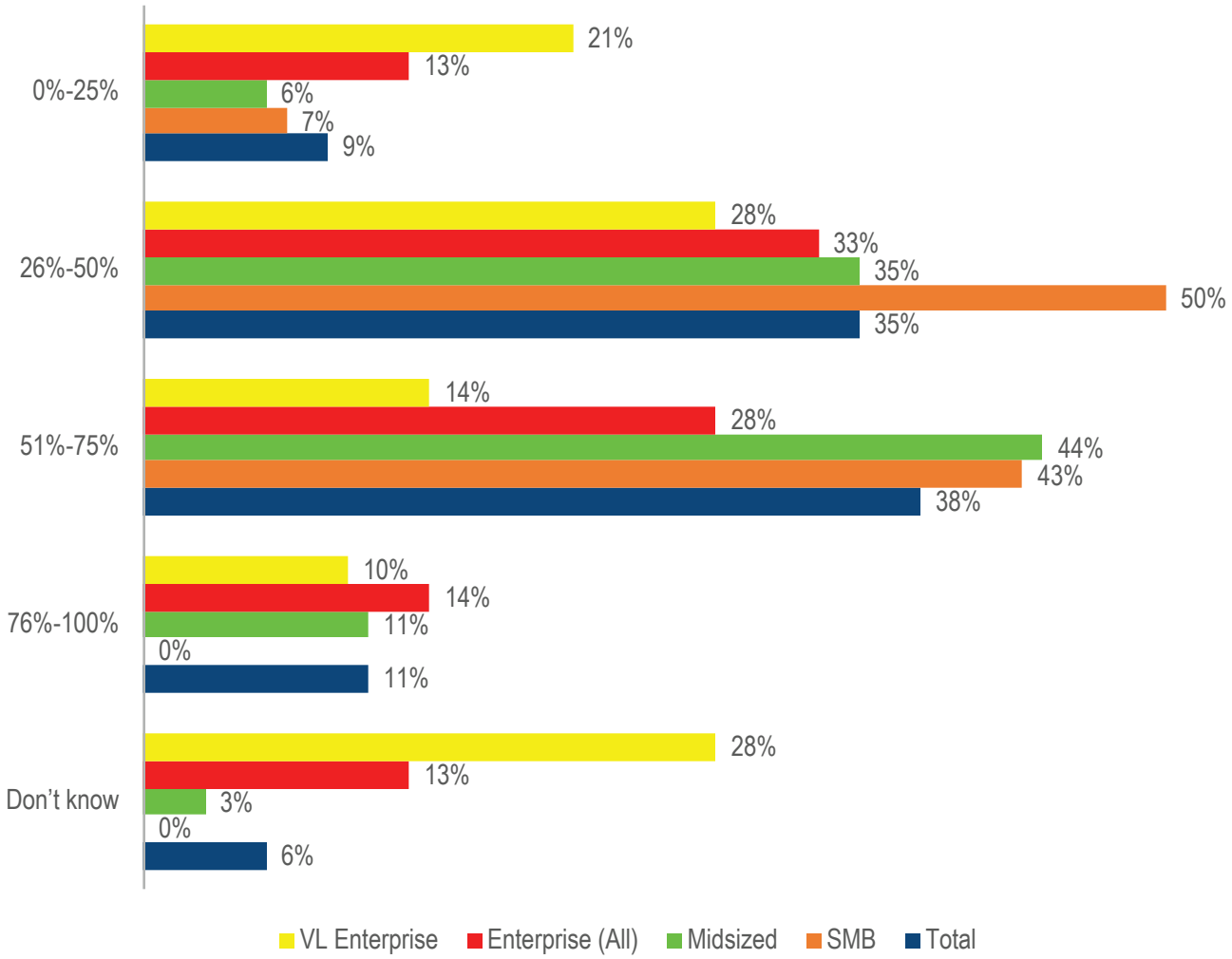

Figure 16: What percentage of the encrypted traffic do you decrypt for analysis?

Changing Encryption Practices

Encryption will continue to be a big push for survey participants over the next year, and their attention will turn to applications and web services. Over the next six months, respondents overall will emphasize encrypting a greater percentage of internally developed applications and web services, with 50 percent indicating they expect their organizations to encrypt internally developed applications, and 49 percent indicating they would encrypt web services. For that timeframe, the data center and enterprise network follow at 44 and 45 percent, respectively. Over the next seven to 12 months, respondents expect to continue to expand encryption in the data center, with 34 percent indicating additional encryption there, and 29 percent will expand it across all other locations and traffic types in that timeframe.

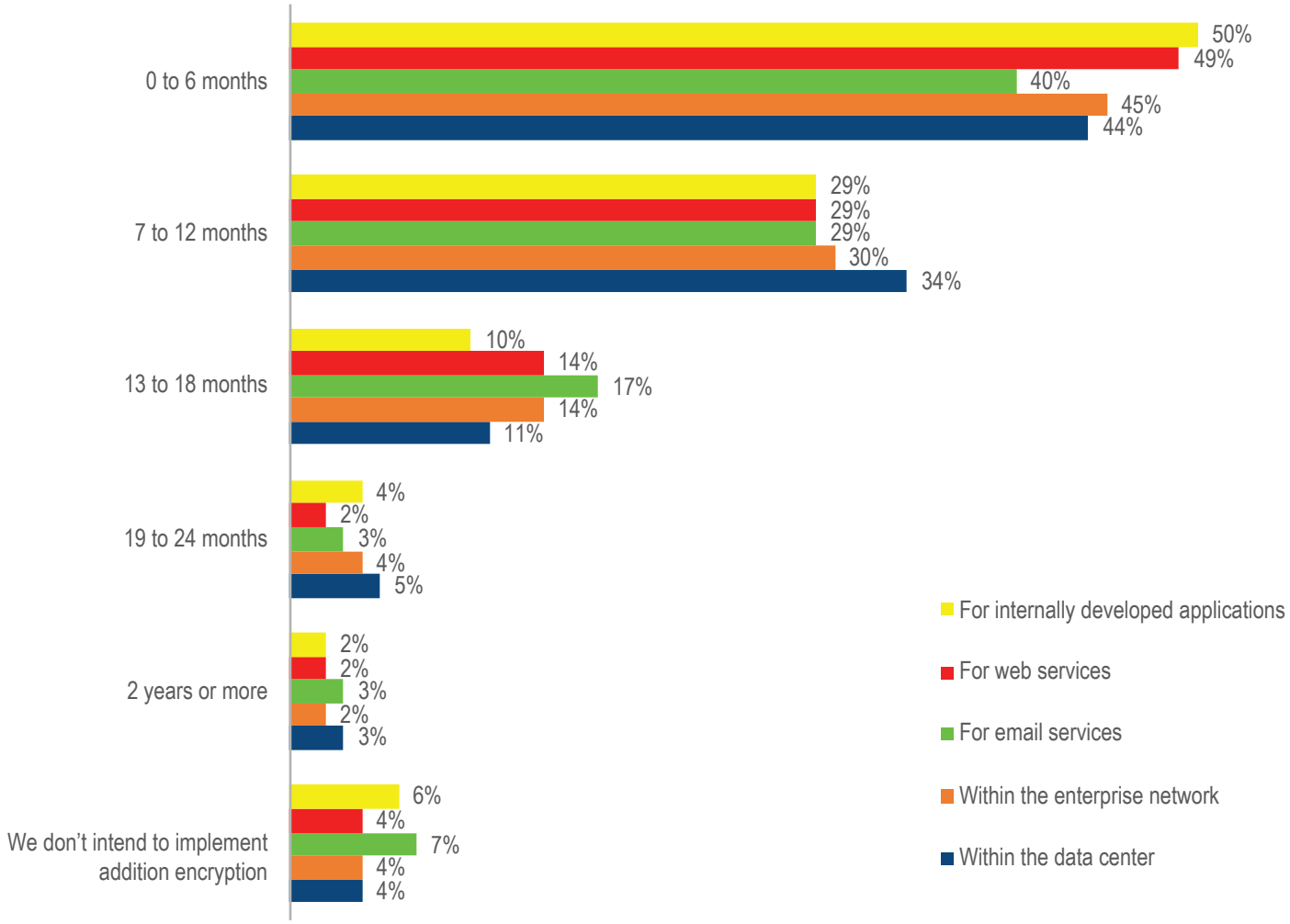

Figure 17: Where, if at all, does your organization intend to implement encryption over the following timeframes?

Looking back over the last 18 months, the use of encryption across organizations of all sizes has increased dramatically. Thirty percent of all respondents indicated that the use of encryption over that timeframe rose from between 1 to 25 percent, and 31 percent indicated that it rose between 26 to 50 percent, mirroring the rapid rise across the Internet. Mid-sized enterprises increased their use of encryption the most over that timeframe, with 45 percent estimating that it increased between 26 to 50 percent. For 17 percent of all respondents, the percentage of encrypted traffic on their organization's network grew by 51 to 75 percent over the last 18 months.

Over the next 18 months, the greatest percentage increase of encrypted traffic for all organization sizes will be between one to 25, according to 35 percent of all respondents. However, mid-sized enterprises will be more aggressive in their increased use of encryption. Forty-eight percent of respondents representing mid-sized enterprises indicated that their percentage of encrypted traffic is expected to increase between 26 to 50 percent.

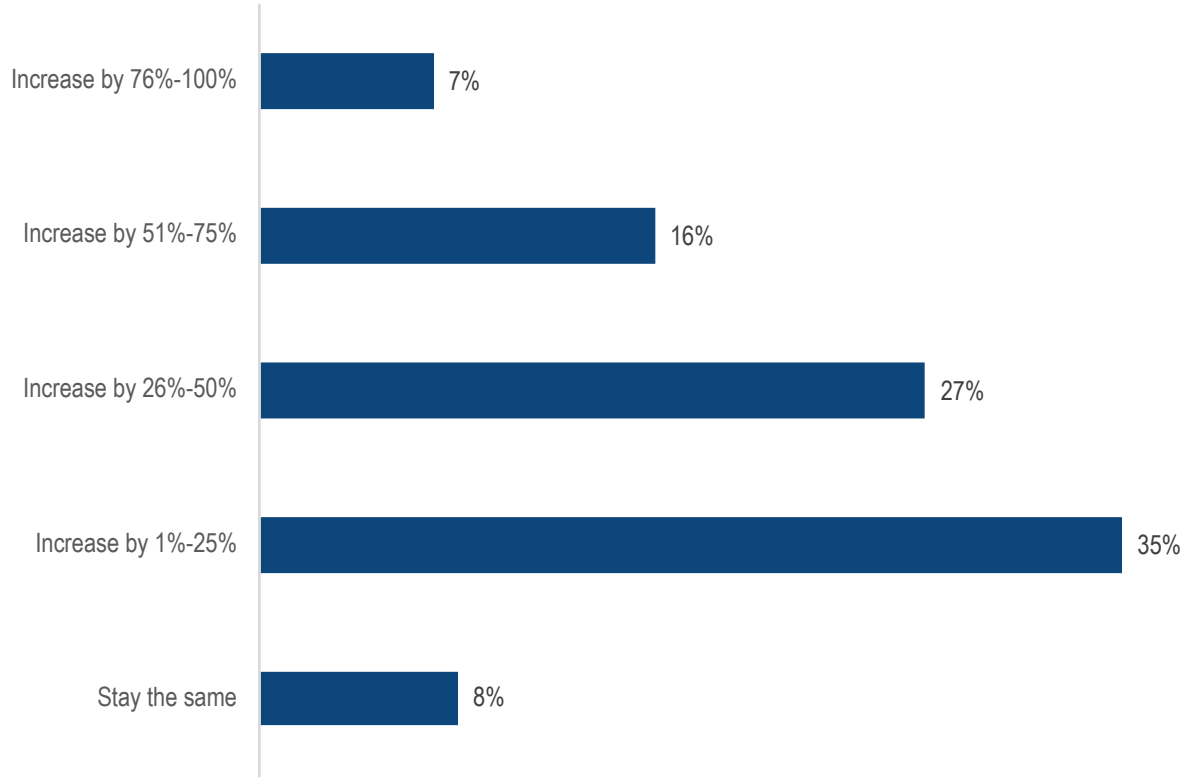

Figure 18: Overall, how do you expect the percentage of encrypted traffic on your network to change in the next 18 months?

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-ExtraHop.021519