Ponemon INSTITUTE

The State of SD-WAN, SASE and Zero Trust Security Architectures

Sponsored by Aruba

Independently conducted by Ponemon Institute LLC

Publication Date: April 2021

The State of SD-WAN, SASE and Zero Trust Security Architectures

Presented by Ponemon Institute, April 2021

Part 1. Introduction

The purpose of this research is to learn important information about the use of Software-defined Networking in a Wide Area Network (SD-WAN), Secure Access Service Edge (SASE) and Zero Trust Architectures. Sponsored by Aruba, Ponemon Institute surveyed 1,826 security and networking practitioners in North America, EMEA, Asia-Pacific and LATAM. In the context of this research, these technologies are defined as follows.

- **SD-WAN** simplifies the management and operation of a Wide Area Network (WAN) by decoupling the networking hardware from its control mechanism and virtualizing transport services.

- **SASE and Zero Trust** are security architectures used to implement security controls.

Following are findings that reveal the state of adoption and implementation.

- **Selection of a best-in-class for a SASE architecture is preferred.** Seventy-one percent of respondents would select a best-in-breed vendor when deploying both SD-WAN and cloud-delivered security for a SASE architecture.

- **Organizations highly confident that their security architecture and implementation is effective are leading in the deployment of Zero Trust, SASE and SD-WAN.** Almost half of high performing organizations (48 percent of respondents) have deployed or will deploy Zero Trust vs. 35 percent of respondents in the overall sample. Forty-three percent of respondents in the high performing organizations have or will deploy SASE vs. 24 percent of respondents in the overall sample.

- **North America leads in the deployment of Zero Trust, SD-WAN and SASE.** Forty-three percent of North American respondents have deployed Zero Trust vs. respondents in EMEA, APAC and LATAM, 33 percent, 31 percent and 26 percent of respondents. This is similar to the deployment of SD-WAN and SASE, as shown in the report.

- **There is more familiarity with Zero Trust security architecture than with SD-WAN and SASE.** Sixty-two percent of respondents are familiar or very familiar with Zero Trust. This is followed by familiarity with SASE security architecture (45 percent of respondents).

- **Adoption of Zero Trust and SASE architectures is expected to grow.** Fifty-seven percent of respondents say their organizations have either deployed or will deploy Zero Trust and 49 percent of respondents say their organizations have either deployed or will deploy SASE architectures.

- **The network team is most influential in the deployment of SD-WAN.** Forty-six percent of respondents say the network team has the most influence in the deployment of SD-WAN solutions with advice from the security team. Thirty-seven percent of respondents say the security team leads the deployment with advice from the network team.

- **How would organizations engage a vendor when implementing cloud-delivered security services such as a cloud-based firewall as a service or a CASB?** Forty-four percent of respondents say their organizations would use leading vendors who focus on cloud-delivered security services.

Part 2. Key findings

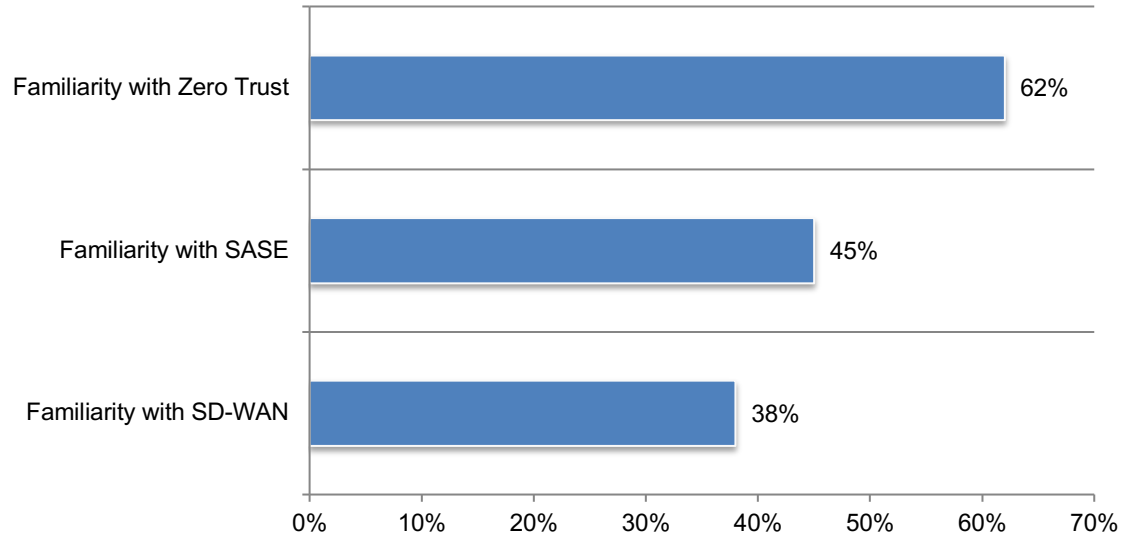
In this section, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. The following topics are covered in this report.

- The familiarity and deployment of SD-WAN, cloud-delivered security, SASE Architecture and Zero Trust Security Architecture
- Regional differences
- The practices of organizations with highly effective security architecture and implementation

The familiarity and deployment of SD-WAN, cloud-delivered security, SASE Architecture and Zero Trust Security Architecture

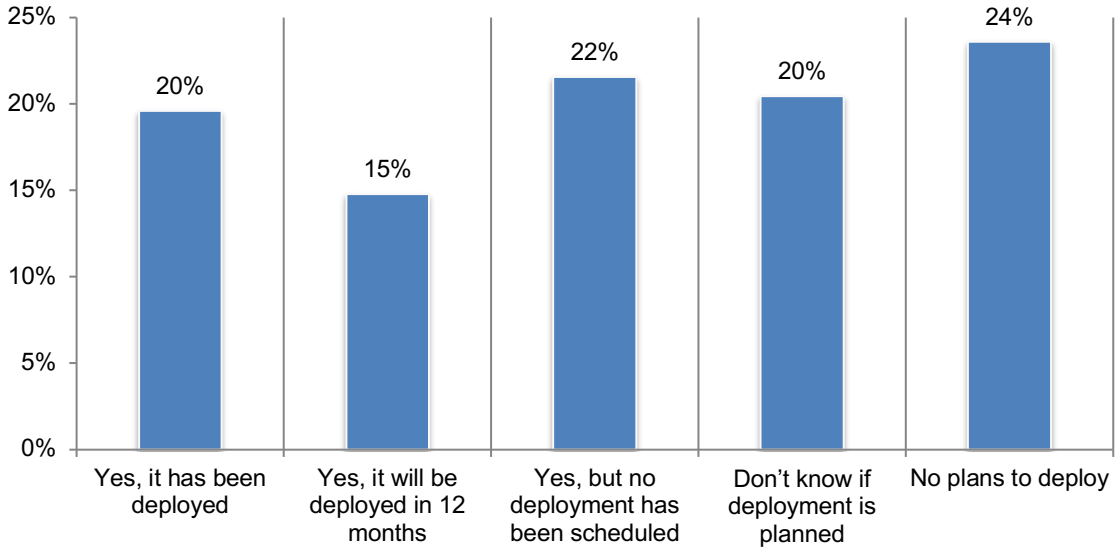
There is more familiarity with Zero Trust security architecture than with SD-WAN and SASE. As shown in Figure 1, 62 percent of respondents are familiar or very familiar with Zero Trust. This is followed by familiarity with SASE security architecture (45 percent of respondents). Only 38 percent of respondents say they are familiar or very familiar with SD-WAN solutions.

Figure 1. Familiarity with Zero Trust, SD-WAN and SASE
Very familiar and Familiar responses combined



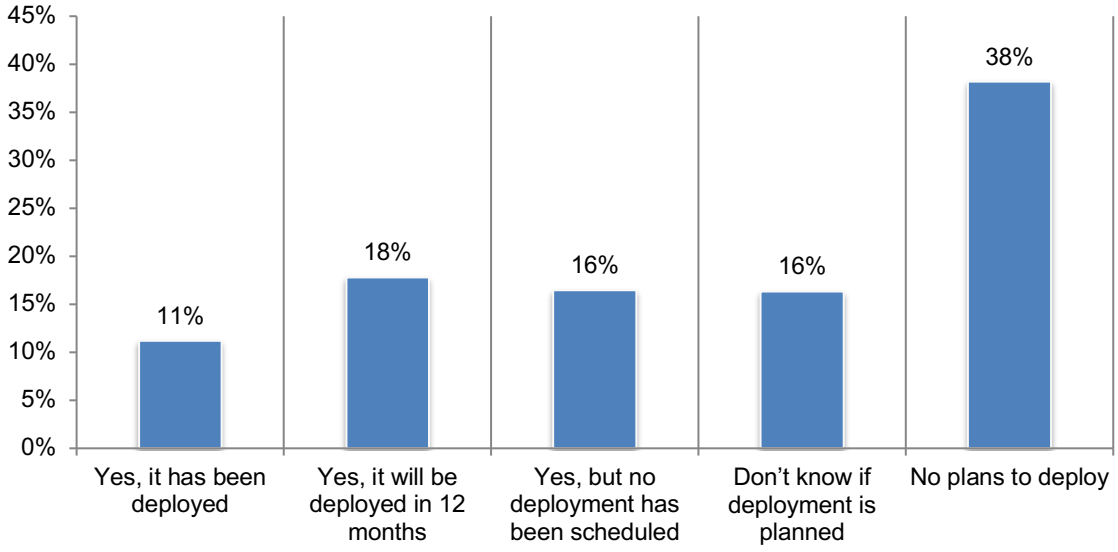
The majority of organizations have deployed or plan to deploy Zero Trust security architecture. According to Figure 2, 57 percent of respondents say Zero Trust has been deployed (20 percent), it will be deployed in the next 12 months (15 percent) or will be deployed sometime in the future (22 percent).

Figure 2. Has your organization deployed or plan to deploy the Zero Trust security architecture?



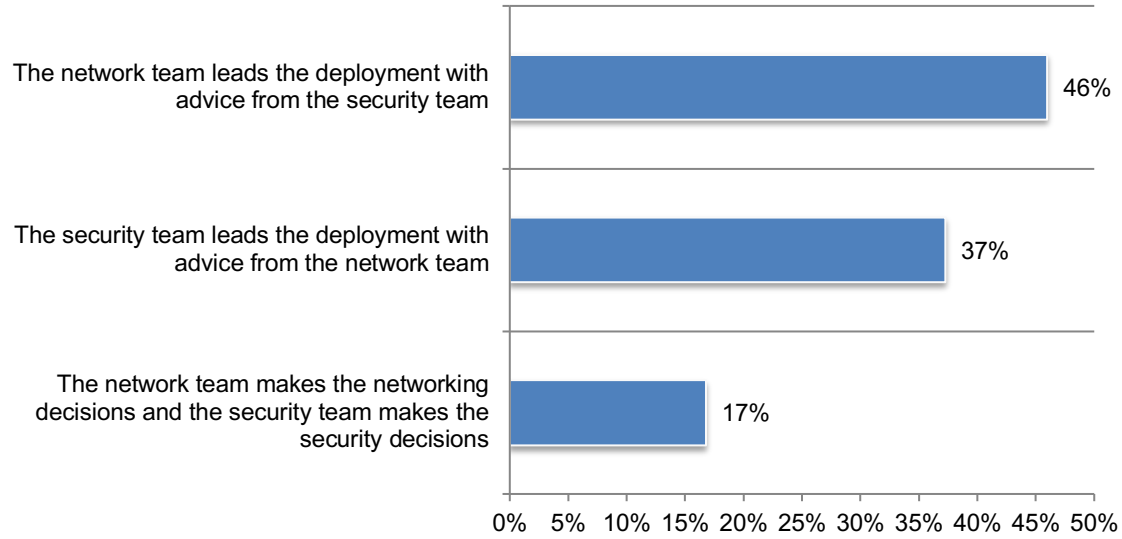
Forty-five percent of respondents say their organizations have deployed or plan to deploy SD-WAN solutions. According to Figure 3, 11 percent of respondents say it has been deployed, 18 percent of respondents say it will be deployed in 12 months and 16 percent of respondents say it will be deployed in the future.

Figure 3. Has your organization deployed or plan to deploy SD-WAN solutions?



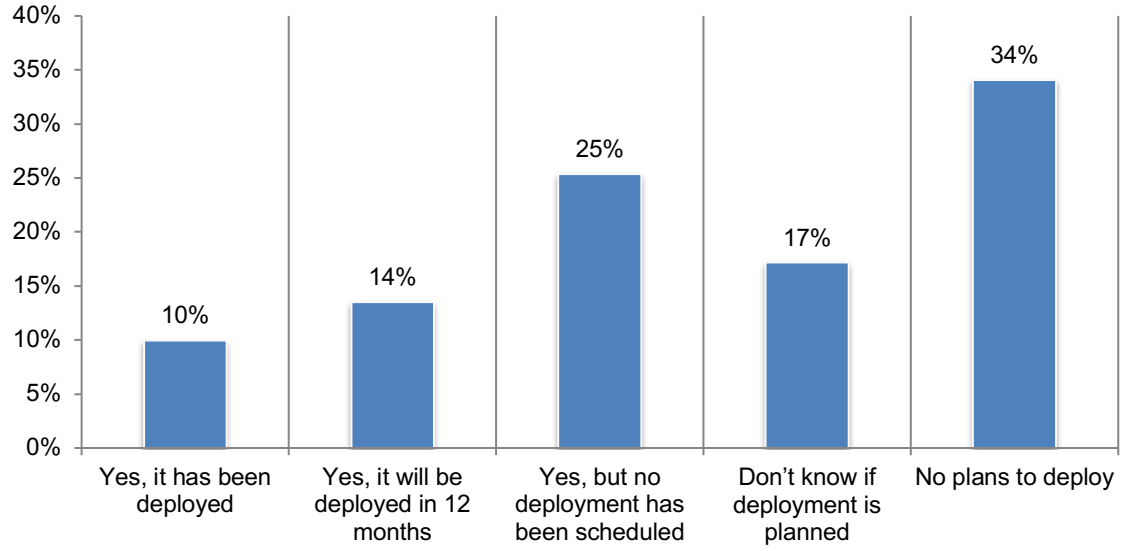
The network team is most influential in the deployment of SD-WAN solutions. As shown in Figure 4, 46 percent of respondents say the network team has the most influence with advice from the security team. Only 17 percent of respondents say the network team makes the networking decisions and the security team makes the security decisions.

Figure 4. Who will have the greatest influence in the deployment of SD-WAN?



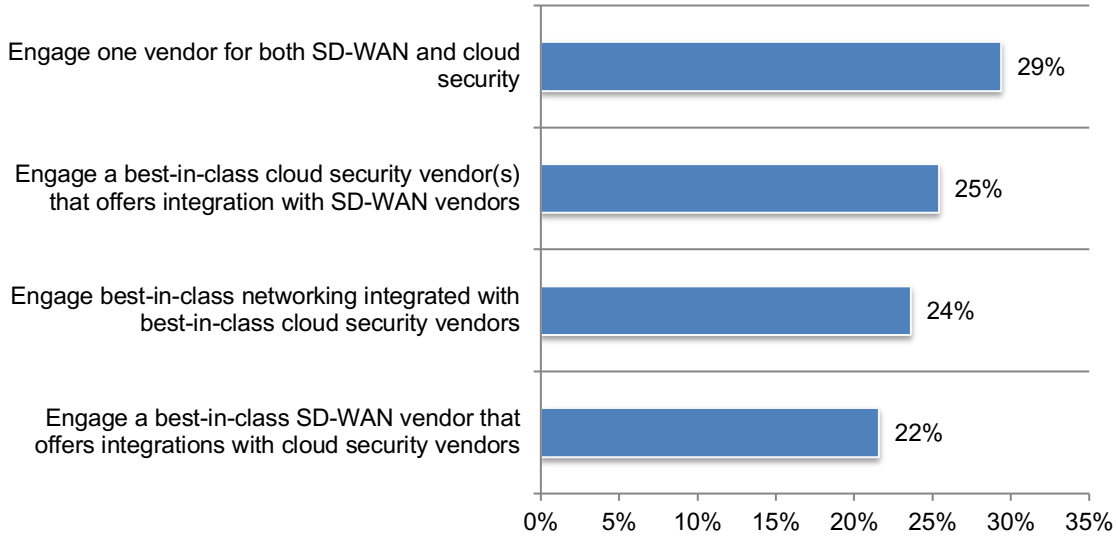
Almost half of respondents say their organizations have deployed or will deploy SASE security architecture. According to Figure 5, 49 percent of respondents say they have deployed (10 percent), will deploy in 12 months (14 percent) or will deploy in the future (25 percent).

Figure 5. Has your organization deployed or plan to deploy the SASE security architecture?



Selection of a best-in-breed vendor for the deployment of both SD-WAN and cloud-delivered security for a SASE architecture is preferred. As shown, 71 percent of respondents say their organizations would engage a best-in-class cloud security vendor(s) that offers integration with SD-WAN vendors (25 percent), engage best-in-class networking integrated with best-in-class cloud security vendors (24 percent) and engage a best-in-class SD-WAN vendor that offers integrations with cloud security vendors (22 percent).

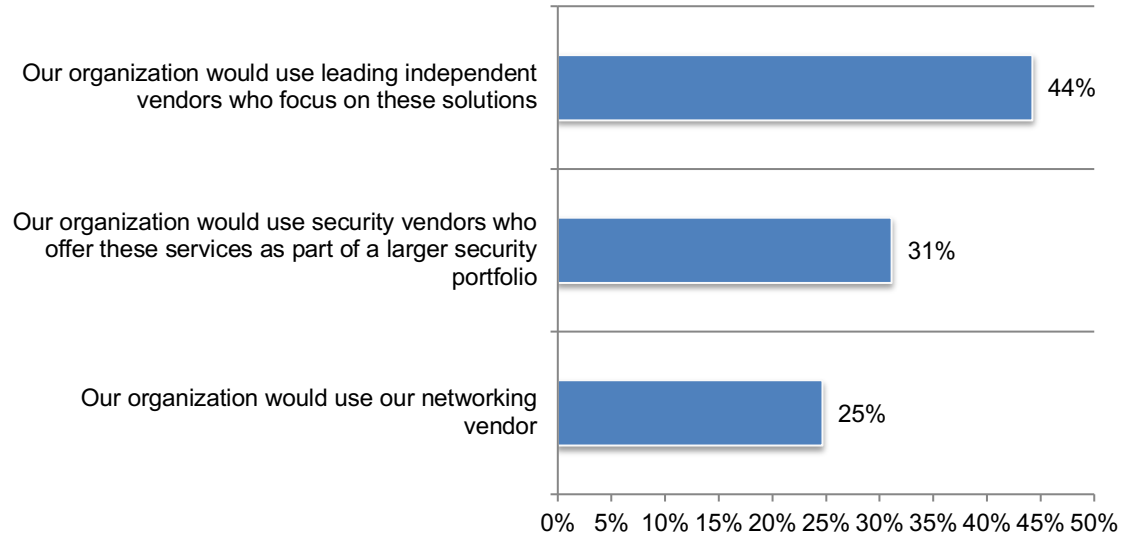
Figure 6. If your organization is deploying both SD-WAN and cloud-delivered security for a SASE architecture, how would vendors be selected?
Only one choice permitted



The network team is most likely to make security solution architecture product decisions. Forty-two percent of respondents say in their organizations the network team makes these decisions followed by 31 percent of respondents who say it is the security and 27 percent of respondents say it was both the network and security team that makes security solution architecture/product decisions.

According to Figure 7, engaging a vendor when implementing cloud-delivered security services (e.g., cloud-based firewall as-a-service, CASB, etc.) is based on the desire to use leading independent vendors who focus on these solutions (44 percent of respondents), security vendors who offer these services as part of a larger security portfolio (31 percent of respondents) or they would use their networking vendor (25 percent of respondents).

Figure 7. How are vendor decisions made when implementing cloud-delivered security services?

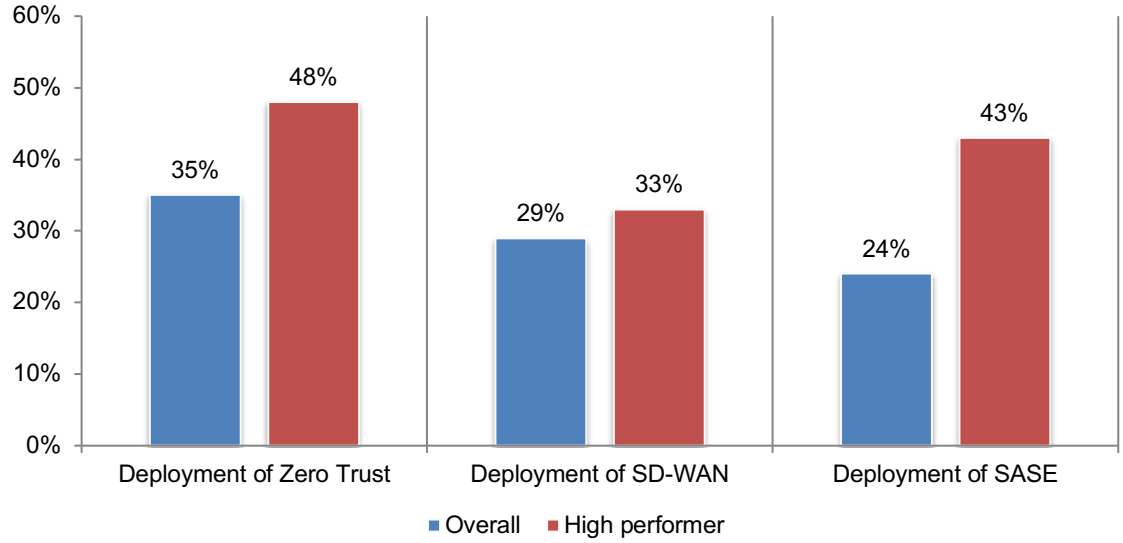


The practices of organizations with highly effective security architecture and implementation

In this section, we provide an analysis of findings from respondents that self-reported their organizations are highly confident that their security architecture and implementation is effective (22 percent of respondents). We refer to these respondents as high performers.

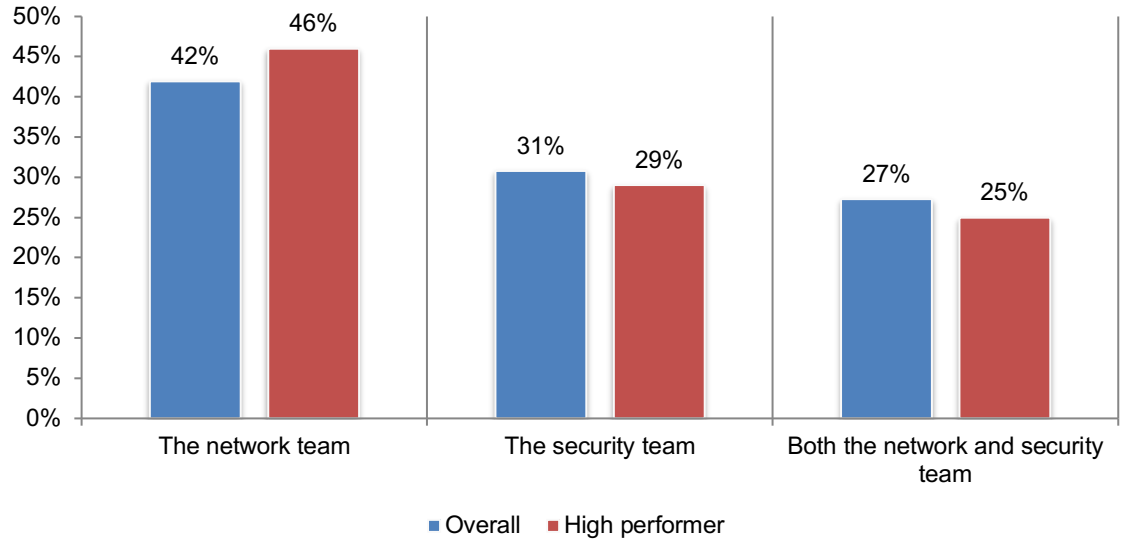
High performing organizations are far more likely to deploy Zero Trust, SD-WAN and SASE. According to Figure 8, almost half of high performer respondents (48 percent) have deployed Zero Trust vs. 35 percent in the overall sample of respondents. Forty-three percent of high performers have deployed SASE vs. 24 percent of respondents in the overall sample.

Figure 8. Deployment of Zero Trust, SD-WAN and SASE
Deployed and Will be deployed in 12 months responses combined



High performing organizations are slightly more likely to say the network team makes security solution architecture product decisions, as shown in Figure 9.

Figure 9. Who makes security solution architecture product decisions?

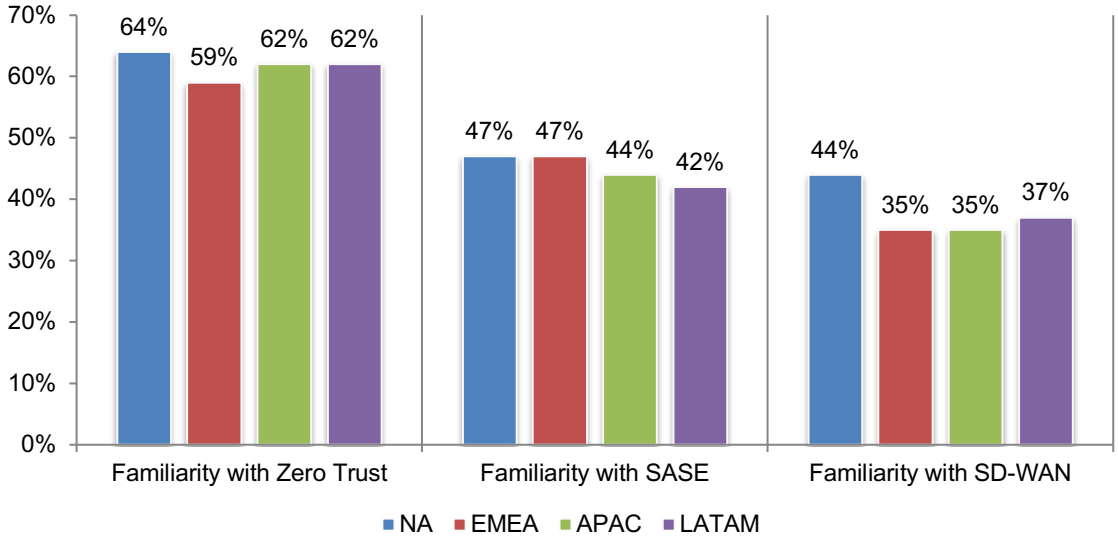


Regional differences

In this section, we present a comparison among the four regions represented in this research: North America (598 respondents), EMEA (454 respondents), Asia-Pacific (402 respondents) and LATAM (372 respondents).

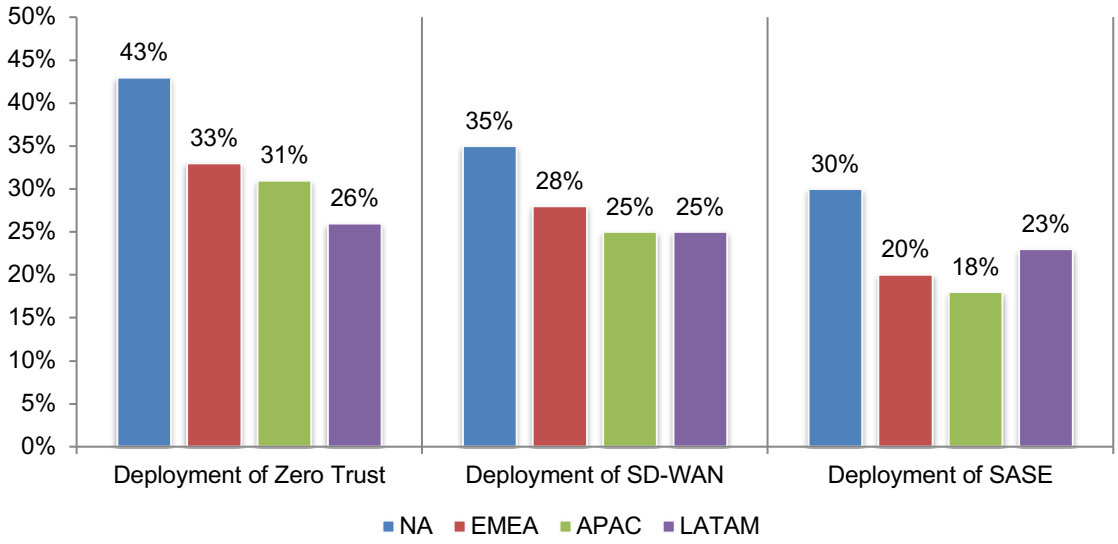
Among the regions, there is more familiarity with Zero Trust security architecture than with SD-WAN and SASE. As shown in Figure 10, in all regions most respondents are familiar or very familiar with Zero Trust. Respondents in North America and EMEA are slightly more familiar with SASE than Asia-Pacific or LATAM. North American respondents are most familiar with SD-WAN (44 percent of respondents).

Figure 10. Familiarity with Zero Trust, SD-WAN and SASE
Very familiar and Familiar responses combined



Deployment of Zero Trust, SD-WAN and SASE is highest in North America, as shown in Figure 11.

Figure 11. Deployment of Zero Trust, SD-WAN and SASE
Deployed and Will be deployed in 12 months responses combined



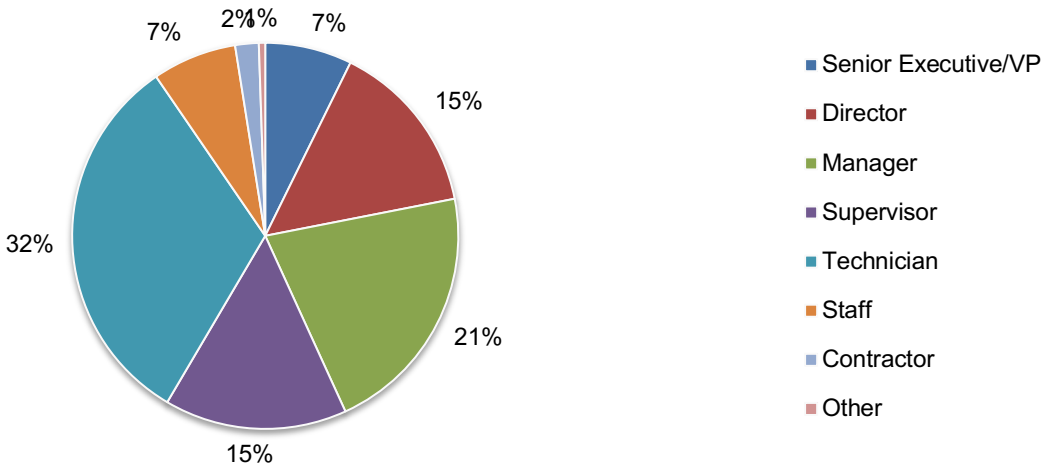
Part 3. Methods

The sampling frame is composed of 51,248 IT and IT security practitioners in the following regions: Asia-Pacific, EMEA, North America, and LATAM. As shown in Table 1, 2,040 respondents completed the survey. Screening removed 214 surveys. The final sample was 1,826 surveys (or a 3.6 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	51,248	100.0%
Total returns	2,040	3.9%
Rejected or screened surveys	214	0.4%
Final sample	1,826	3.6%

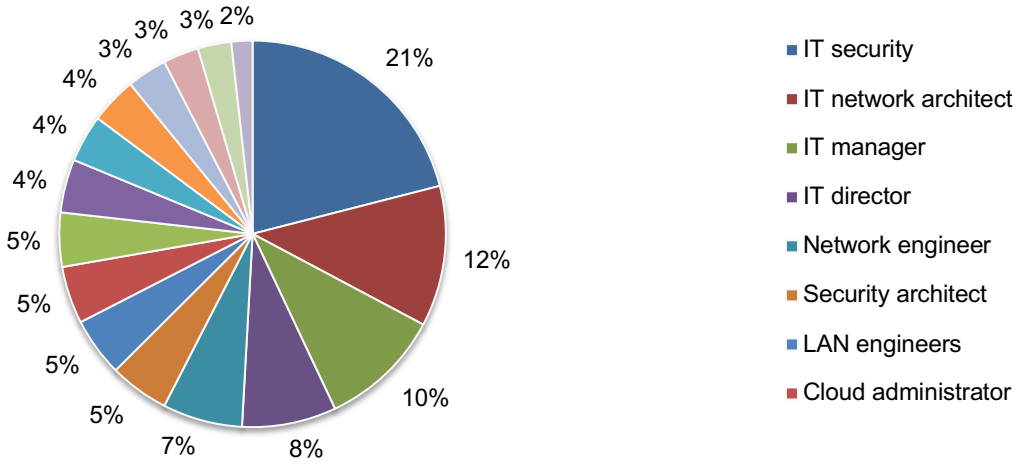
Pie Chart 1 reports the current position or organizational level of the respondents. Fifty-eight percent of respondents reported their current position as supervisory or above and 32 percent of respondents reported their position as technician.

Pie Chart 1. Distribution of respondents according to position level



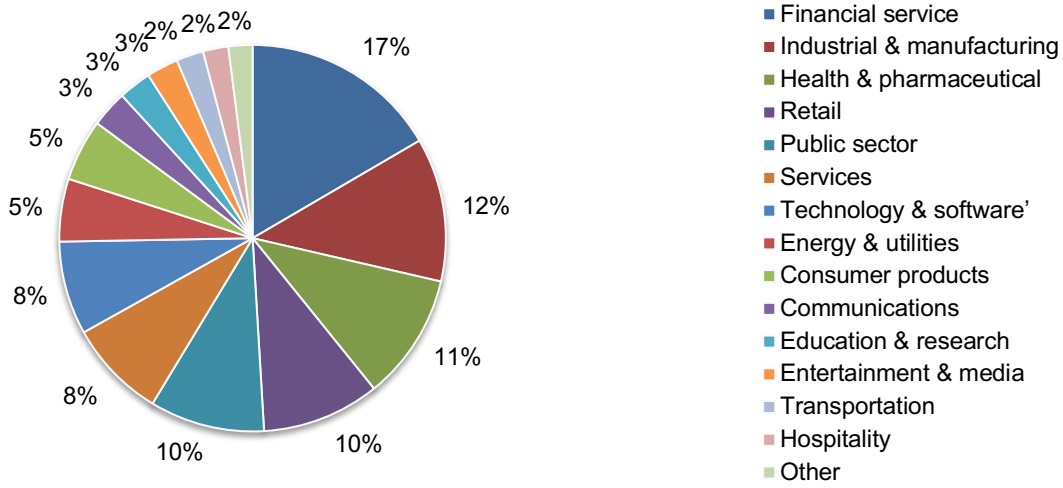
Pie Chart 2 identifies the primary role of the respondent. Twenty-one percent of respondents identified their role as IT security, 12 percent of respondents identified IT network architect, 10 percent of respondents identified IT manager and 8 percent of respondents identified their role as IT director.

Pie Chart 2. Distribution of respondents according primary role in the organization



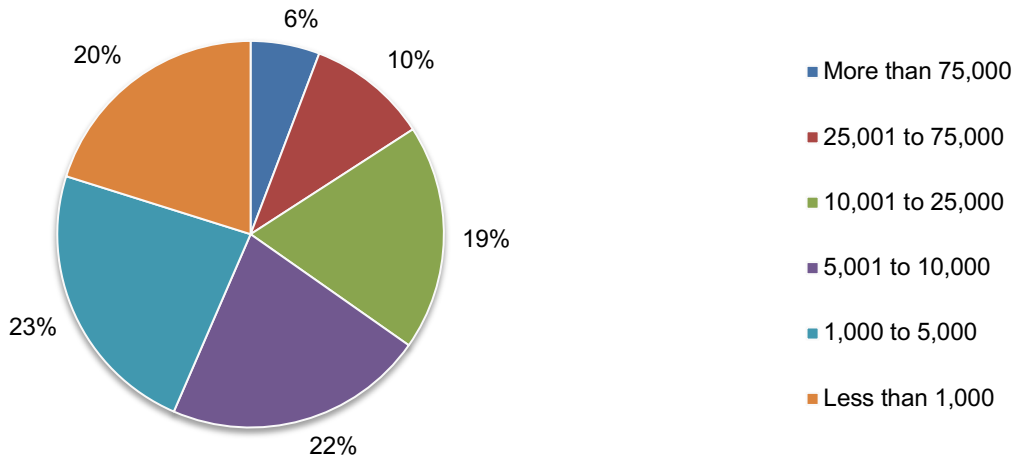
Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, which includes banking, insurance, brokerage, investment management and payment processing. This is followed by industrial/manufacturing (12 percent of respondents), health and pharmaceutical (11 percent of respondents), retail and public sector (each at 10 percent of respondents).

Pie chart 3. Distribution of respondents according to primary industry classification



According to Pie Chart 4, more than half (57 percent) of respondents are from organizations with a global headcount of more than 5,000 employees.

Pie Chart 4. Distribution of respondents according to the number of employees within the organization



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT security or networking practitioners in various organizations in Asia-Pacific, EMEA, North America, and LATAM. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in February 2021.

Survey response	NA	EMEA	APAC	LATAM	Total
Total sampling frame	16,248	12,445	11,891	10,664	51,248
Total returns	663	501	456	420	2,040
Rejected surveys	65	47	54	48	214
Final sample	598	454	402	372	1,826
Response rate	3.7%	3.6%	3.4%	3.5%	3.6%
Sample weights	32.7%	24.9%	22.0%	20.4%	100.0%

Part 1. Screening

S1. What best describes your role within your organization?	NA	EMEA	APAC	LATAM	Total
I am mostly a security practitioner	41%	35%	36%	30%	36%
I am mostly a networking practitioner	27%	37%	39%	42%	35%
I am both a security and networking practitioner	32%	28%	25%	28%	29%
None of the above (stop)	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%

Part 2. The use of SD-WAN, Cloud-delivered Security, SASE architecture and Zero Trust security architecture

Q1. How familiar are you with the Zero Trust security architecture?	NA	EMEA	APAC	LATAM	Total
Very familiar	34%	30%	28%	27%	30%
Familiar	30%	29%	34%	35%	32%
Somewhat familiar	27%	30%	28%	17%	26%
Not familiar	9%	11%	10%	21%	12%
Total	100%	100%	100%	100%	100%

Q2. Has your organization deployed or plan to deploy the Zero Trust security architecture?	NA	EMEA	APAC	LATAM	Total
Yes, it has been deployed	24%	19%	18%	15%	20%
Yes, it will be deployed in 12 months	19%	14%	13%	11%	15%
Yes, but no deployment has been scheduled	23%	19%	20%	24%	22%
Don't know if deployment is planned	16%	25%	27%	15%	20%
No plans to deploy	18%	23%	22%	35%	24%
Total	100%	100%	100%	100%	100%

Q3. How familiar are you with SD-WAN solutions?	NA	EMEA	APAC	LATAM	Total
Very familiar	21%	16%	13%	17%	17%
Familiar	23%	19%	22%	20%	21%
Somewhat familiar	32%	23%	30%	33%	30%
Not familiar	24%	42%	35%	30%	32%
Total	100%	100%	100%	100%	100%

Q4. Has your organization deployed or plan to deploy SD-WAN solutions?	NA	EMEA	APAC	LATAM	Total
Yes, it has been deployed	15%	9%	11%	8%	11%
Yes, it will be deployed in 12 months	20%	19%	14%	17%	18%
Yes, but no deployment has been scheduled	11%	20%	23%	14%	16%
Don't know if deployment is planned	18%	12%	19%	16%	16%
No plans to deploy	36%	40%	33%	45%	38%
Total	100%	100%	100%	100%	100%

Q5. Who has or will have the greatest influence in the deployment of SD-WAN solutions?	NA	EMEA	APAC	LATAM	Total
The security team leads the deployment with advice from the network team	40%	34%	38%	36%	37%
The network team leads the deployment with advice from the security team	45%	47%	50%	42%	46%
The network team makes the networking decisions and the security team makes the security decisions	15%	19%	12%	22%	17%
Total	100%	100%	100%	100%	100%

Q6. How familiar are you with the SASE security architecture?	NA	EMEA	APAC	LATAM	Total
Very familiar	24%	18%	17%	19%	20%
Familiar	23%	29%	27%	23%	25%
Somewhat familiar	30%	28%	25%	28%	28%
Not familiar	23%	25%	31%	30%	27%
Total	100%	100%	100%	100%	100%

Q7. Has your organization deployed or plan to deploy the SASE security architecture?	NA	EMEA	APAC	LATAM	Total
Yes, it has been deployed	12%	8%	9%	10%	10%
Yes, it will be deployed in 12 months	18%	12%	9%	13%	14%
Yes, but no deployment has been scheduled	23%	28%	27%	24%	25%
Don't know if deployment is planned	15%	21%	18%	15%	17%
No plans to deploy	32%	31%	37%	38%	34%
Total	100%	100%	100%	100%	100%

Q8. If your organization is deploying both SD-WAN and cloud-delivered security for a SASE architecture, how would vendors be selected? Please select only one choice.	NA	EMEA	APAC	LATAM	Total
Engage one vendor for both SD-WAN and cloud security	29%	28%	31%	30%	29%
Engage best-in-class networking integrated with best-in-class cloud security vendors	23%	27%	25%	19%	24%
Engage a best-in-class SD-WAN vendor that offers integrations with cloud security vendors	25%	24%	18%	17%	22%
Engage a best-in-class cloud security vendor(s) that offers integration with SD-WAN vendors	23%	21%	26%	34%	25%
Total	100%	100%	100%	100%	100%

Q9. Who makes security solution architecture/product decisions?	NA	EMEA	APAC	LATAM	Total
The network team	40%	48%	38%	42%	42%
The security team	33%	29%	33%	27%	31%
Both the network and security team	27%	23%	29%	31%	27%
Total	100%	100%	100%	100%	100%

Q10. How are vendor decisions made when implementing cloud-delivered security services (e.g. cloud-based firewall as-a-service, cloud access security broker, etc.)? Please select the **one** best choice.	NA	EMEA	APAC	LATAM	Total
Our organization would use leading independent vendors who focus on these solutions	47%	41%	43%	45%	44%
Our organization would use our networking vendor	23%	26%	28%	22%	25%
Our organization would use security vendors who offer these services as part of a larger security portfolio	30%	33%	29%	33%	31%
Total	100%	100%	100%	100%	100%

Q11. How confident is your organization in the effectiveness of its security architecture and implementation from 1 = not confident to 10 = highly confident?	NA	EMEA	APAC	LATAM	Total
1 or 2	5%	8%	11%	9%	8%
3 or 4	15%	6%	8%	13%	11%
5 or 6	25%	15%	8%	25%	19%
7 or 8	33%	36%	35%	34%	34%
9 or 10	22%	35%	38%	19%	28%
Total	100%	100%	100%	100%	100%
Extrapolated value	6.54	7.18	7.12	6.32	6.78

Q12. Do you think it is possible to have all your **security needs** met exclusively by one vendor?	NA	EMEA	APAC	LATAM	Total
Yes	68%	64%	59%	57%	63%
No	27%	30%	37%	36%	32%
Unsure	5%	6%	4%	7%	5%
Total	100%	100%	100%	100%	100%

Q13. Do you think it is possible to have all your **networking needs** met exclusively by one vendor?	NA	EMEA	APAC	LATAM	Total
Yes	48%	45%	41%	39%	44%
No	45%	47%	53%	55%	49%
Unsure	7%	8%	6%	6%	7%
Total	100%	100%	100%	100%	100%

Q14. Do you think it is possible to have all your **security and networking needs** met exclusively by one vendor?	NA	EMEA	APAC	LATAM	Total
Yes	57%	52%	50%	47%	52%
No	35%	42%	43%	45%	41%
Unsure	8%	6%	7%	8%	7%
Total	100%	100%	100%	100%	100%

Part 3. Your Role & Organizational Characteristics

D1. What organizational level best describes your current position?	NA	EMEA	APAC	LATAM	Total
Senior Executive/VP	8%	6%	7%	8%	7%
Director	16%	14%	13%	15%	15%
Manager	21%	23%	19%	22%	21%
Supervisor	15%	17%	15%	14%	15%
Technician	30%	31%	35%	33%	32%
Staff	7%	8%	8%	5%	7%
Contractor	2%	1%	3%	2%	2%
Other	1%	0%	0%	1%	1%
Total	100%	100%	100%	100%	100%

D2. What best describes your primary role in the organization?	NA	EMEA	APAC	LATAM	Total
Cloud administrator	5%	6%	3%	5%	5%
Data protection officer	0%	0%	0%	0%	0%
IT director	7%	8%	9%	8%	8%
IT manager	11%	8%	9%	13%	10%
IT network architect	12%	10%	13%	12%	12%
IT security	20%	19%	23%	23%	21%
LAN engineers	5%	3%	6%	6%	5%
Network administrator	3%	3%	2%	4%	3%
Network engineer	6%	7%	8%	6%	7%
Network operations manager	4%	3%	4%	2%	3%
Network specialist	3%	6%	4%	3%	4%
Security administrator	5%	3%	5%	2%	4%
Security analysts	6%	5%	2%	4%	4%
Security architect	4%	8%	3%	5%	5%
Security specialist	3%	3%	3%	2%	3%
WAN engineers	4%	7%	3%	4%	5%
Other (please specify)	2%	1%	3%	1%	2%
Total	100%	100%	100%	100%	100%

D3. What industry best describes your organization's industry focus?	NA	EMEA	APAC	LATAM	Total
Agriculture & food service	1%	1%	1%	1%	1%
Communications	3%	2%	4%	3%	3%
Consumer products	5%	5%	5%	6%	5%
Defense & aerospace	1%	1%	2%	1%	1%
Education & research	2%	2%	4%	3%	3%
Energy & utilities	5%	5%	6%	5%	5%
Entertainment & media	2%	2%	3%	4%	3%
Financial service	18%	15%	17%	15%	17%
Health & pharmaceutical	11%	12%	9%	10%	11%
Hospitality	2%	2%	2%	3%	2%
Industrial & manufacturing	12%	15%	11%	10%	12%
Public sector	9%	10%	9%	11%	10%
Retail	10%	10%	9%	10%	10%
Services	9%	9%	8%	7%	8%
Technology & software'	8%	8%	8%	7%	8%
Transportation	2%	2%	2%	3%	2%
Other	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%

D4. What range best describes the full-time headcount of your global organization?	NA	EMEA	APAC	LATAM	Total
Less than 1,000	18%	24%	21%	18%	20%
1,000 to 5,000	20%	25%	24%	26%	23%
5,001 to 10,000	19%	20%	23%	27%	22%
10,001 to 25,000	22%	17%	19%	16%	19%
25,001 to 75,000	13%	9%	8%	9%	10%
More than 75,000	8%	5%	5%	4%	6%
Total	100%	100%	100%	100%	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Insights Association,** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.