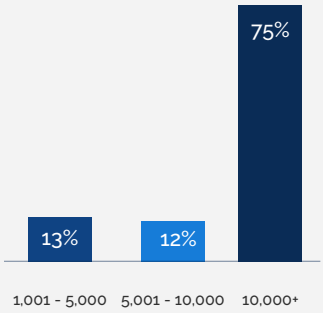
ARCHIVE360

SECURITY REQUIREMENTS FOR SAAS VENDORS

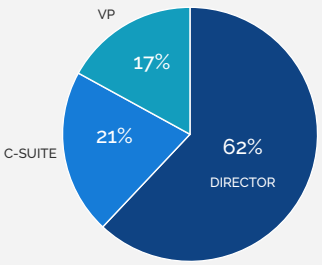
Research by **Pulse Q&A**

Breakdown

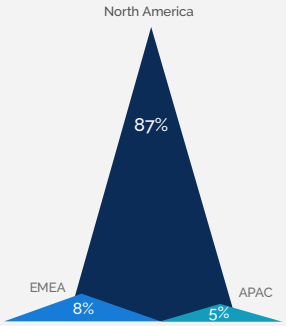
75%
RESPONDENTS FROM COMPANY SIZE 10K AND UP



62%
DIRECTOR RESPONDENTS



87%
RESPONDENTS FROM NORTH AMERICA

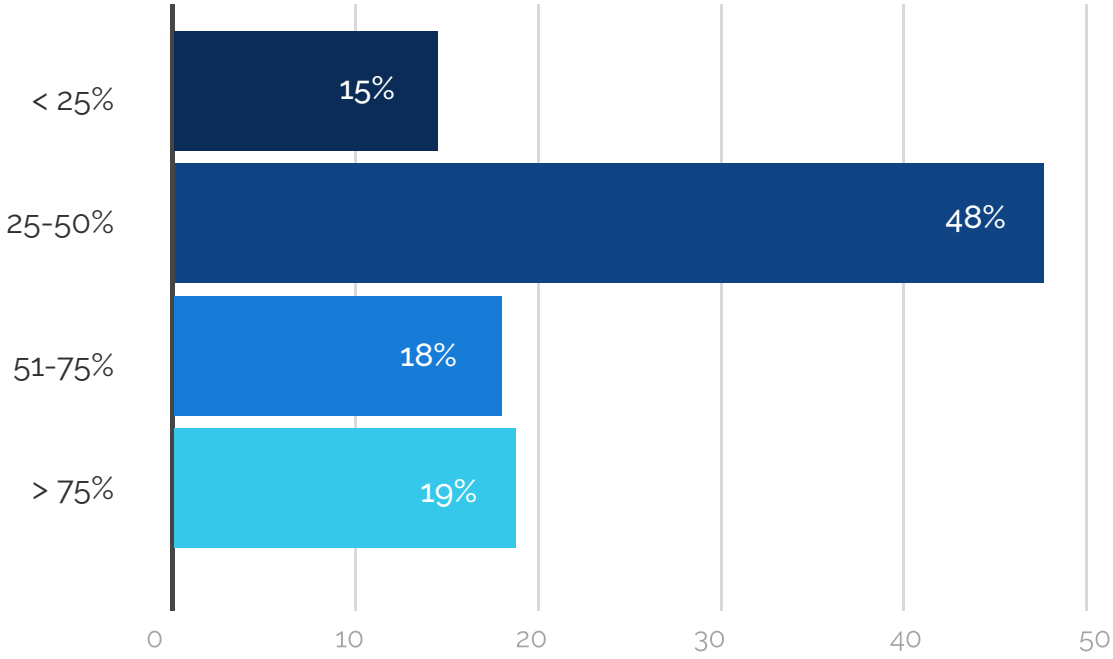


Methodology

Pulse Q&A partnered with Archive360 to conduct a study on security protocols for SaaS vendors. In this study, we surveyed **100 IT executives** in enterprise companies that were based in North America, EMEA and APAC. All survey respondents are verified IT executives on the Pulse Q&A platform

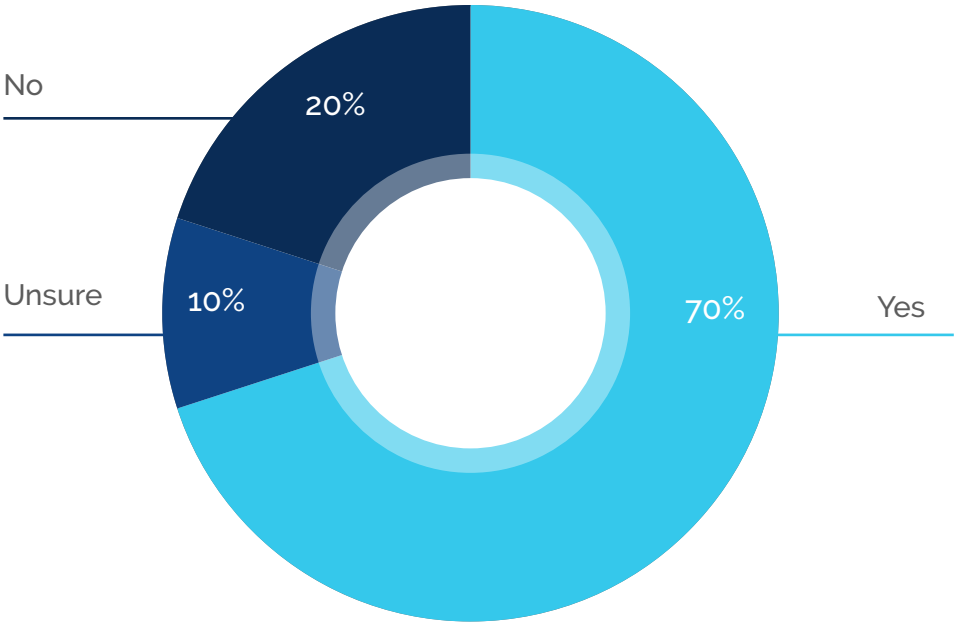
1. How many of your SaaS vendors meet 100% of your company's security requirements?

Only 19% of executives said 75% or more of their SaaS vendors meet all of their security requirements.



2. To your knowledge, have you ever had to make a security policy exception for one or more existing SaaS solution providers?

70% of companies have made at least one security exception for a SaaS vendor.

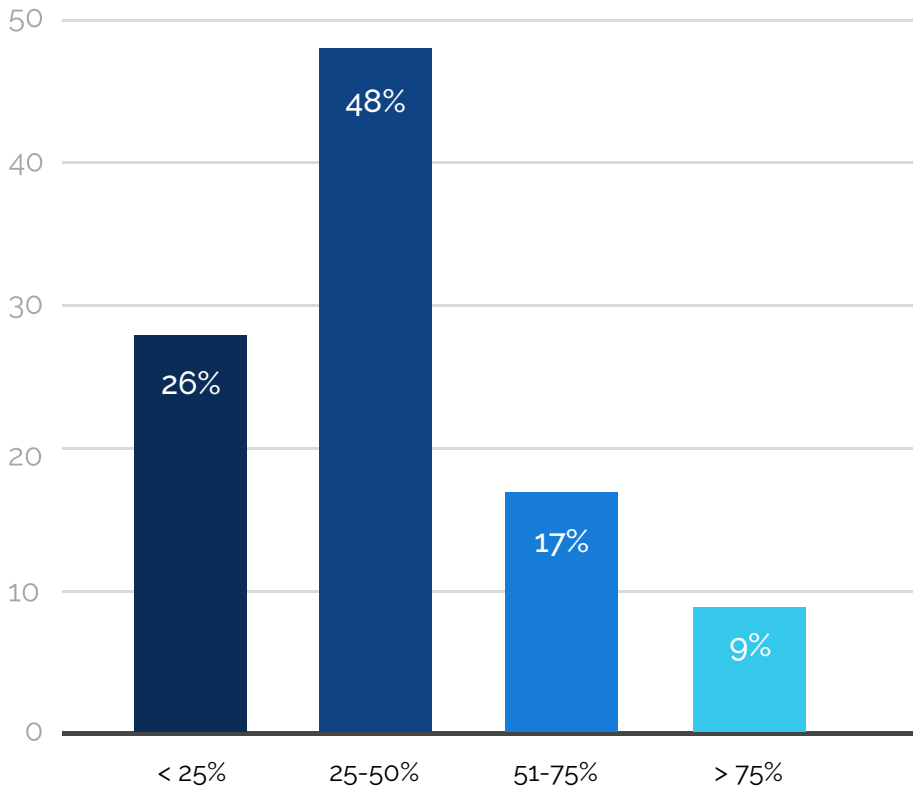


3. When sensitive data is stored in an application outside of your Data Center, is it important that you control the encryption keys protecting that data?

95% of executives said it was important to control their own encryption keys.

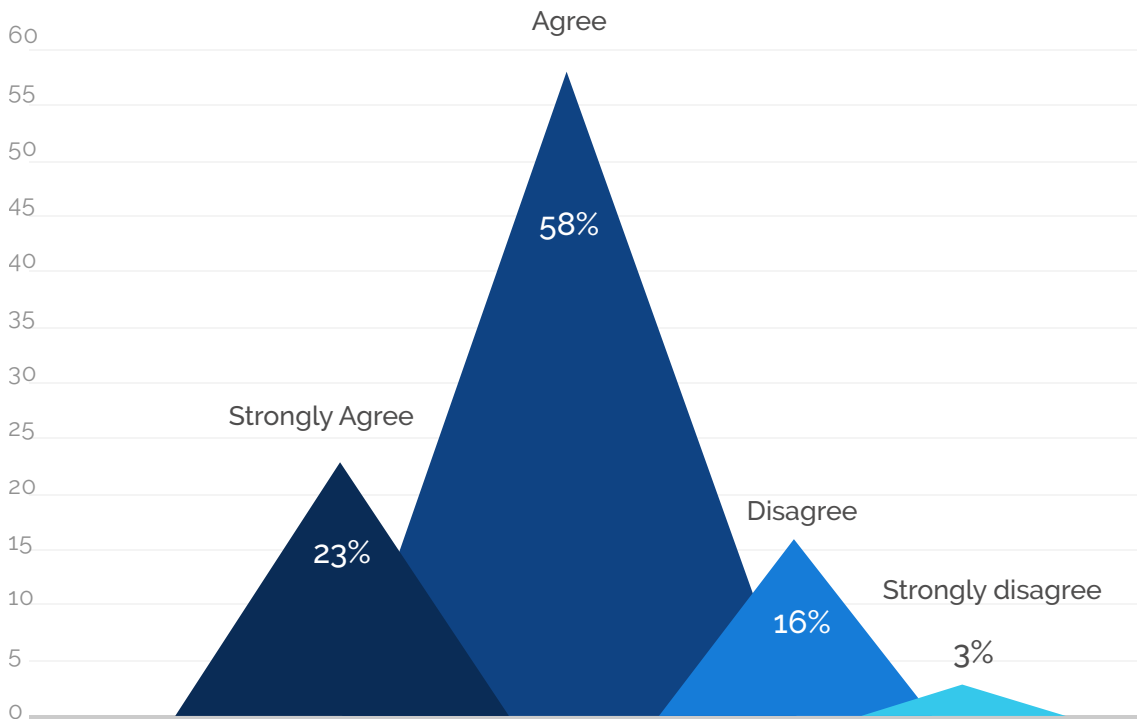
4. In your best estimation, what portion of your SaaS solution providers give your team control over your encryption keys?

74% of companies do not have control of their encryption keys with a majority of SaaS vendors.



5. To what extent do you agree with this statement - “I am uncomfortable that my SaaS solution providers maintain access and control of my encryption keys.”

81% of executives are uncomfortable with their SaaS vendors controlling their encryption keys.



6. Why are you uncomfortable with your SaaS solution providers maintaining access and control of your encryption keys?

1	**"Loss of independent control of data security"** - VP of IT, UK based Software company
2	**"Uncontrolled access, raises concerns for audit and compliance, data privacy integrity"** - VP of Security, US based Software company
3	**"Past history of compromises"** - Director of IT, Mid-sized Professional Services company
4	**"I've seen too many strong companies go out of business, and have also audited our vendors and seen great vendors fall out of compliance. Having them control the keys is just one more additive risk"** - Director of IT, Large US Manufacturing Company
5	**"Trust for Data Breach and confidentiality of Data"** - CIO, Large Asian Software Company
6	**" As a government entity we would want full control"** - Director of IT, US based Hardware company
7	**"Because you are trusting the service provider properly securing your data without much view the process. Over reliance on service providers can be a big risk to the organization"** - Director of IT, US based Software company

8 " Concern of my privacy"
- Director of IT, US based Software company

9 "Creates an opportunity for exploitation by subcontracted vendors"
- VP of IT, US based Arts, Entertainment and Recreation company

10 "My data, my keys"
- C-Suite, UK based Software company

11 "Potential conflict with my company's standards"
- Director of IT, US based Software company

12 "Security and privacy and regulatory"
- Director of IT, US based Retail company

13 "Security reasons as we have no control when there is a breach at the providers end"
- Director of IT, US based Educational Services Company

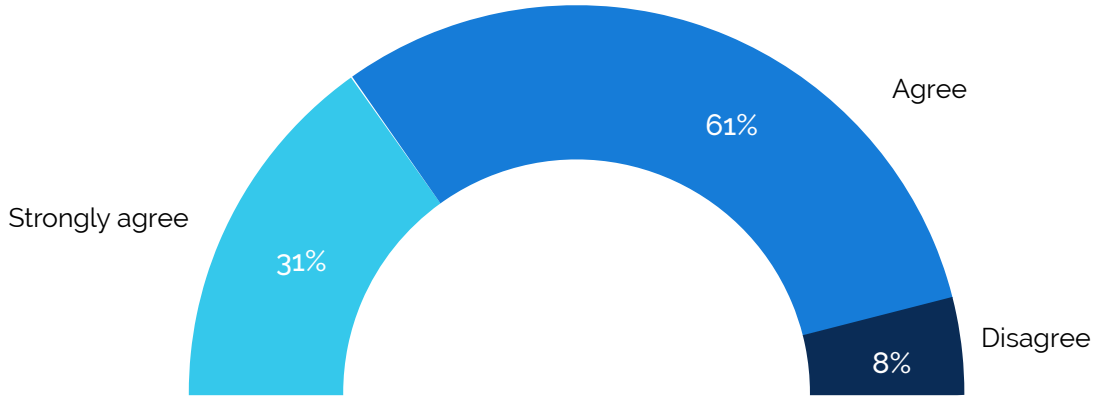
14 "The maturity of the vendors aren't there yet. In a few years maybe"
- Director of IT, Educational Services Company

15 "Without internal controls, you do not know where the information goes"
- C-Suite, US based Manufacturing company

16 "Would like to understand how they are managed and changed and also the access matrix"
- C-Suite, US based Health Care and Social Assistance company

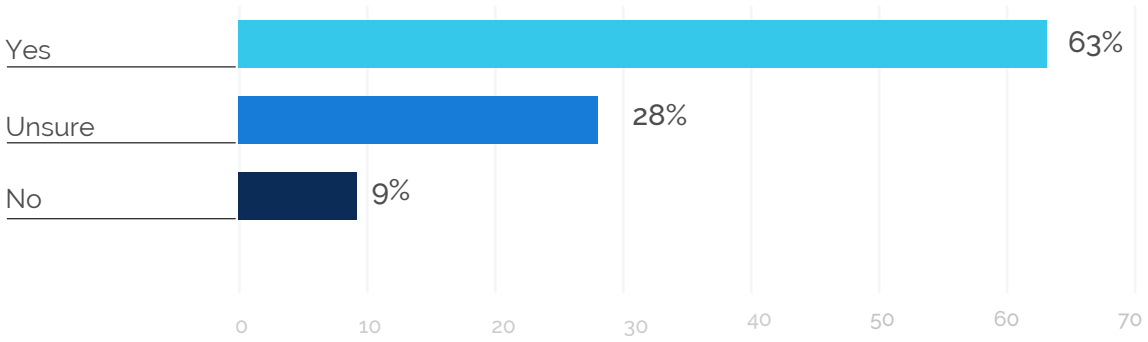
7. SaaS vendors offer one-size-fits-all security, but there is a movement towards “security customization”. To what extent do you believe that in the future your team will require more customization of security for applications running outside your Data Centre?

92% of executives believe they will need more customization of security in the future.



8. In the future, do you believe that you will retire SaaS applications/vendors who maintain control over your encryption keys and/or use one encryption key for multiple customers?

63% of executives believe they will retire SaaS applications that do not give them control of encryption keys.



About Archive360

Archive360 provides the world's most secure archive. Unlike SaaS archives, Archive360 retains your emails, files and videos inside of your public cloud tenant giving you unparalled control of your data. You control your encryption keys ensuring only you have access to your data. You control the countries where your data is stored ensuring compliance with data sovereignty and privacy laws. You control the people, process and technology protecting your data ensuring your archive meets 100% of your security policies. And your security team isn't the only one that will love Archive360. Legal, Compliance and End-Users have access to blazing fast search and next-generation features making it easy for them to find what they need.

About Pulse Q&A

Pulse Q&A is a trusted community of thousands of IT executives. Members use the community to share knowledge, ask questions on IT trends, and engage in peer-based research for rapid access to insights to drive business decisions.
Visit https://home.pulse.qa/ to learn more.