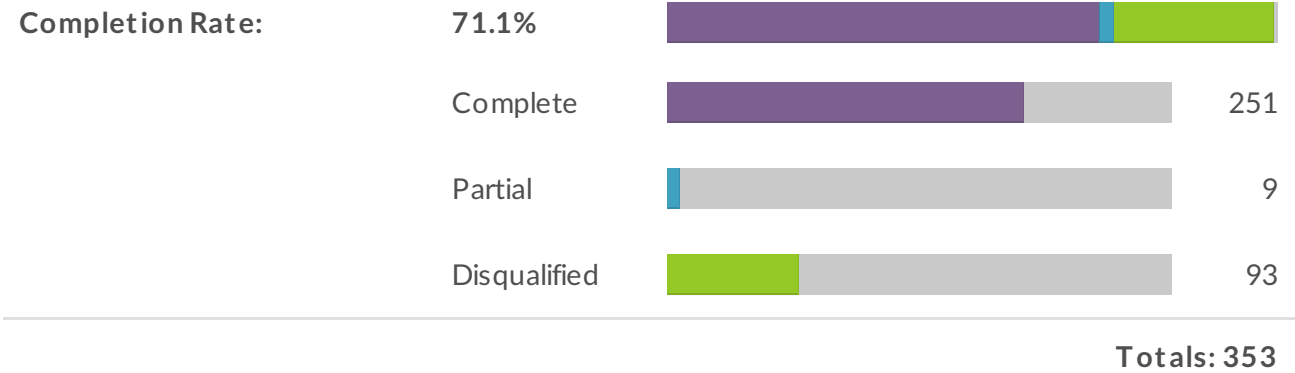
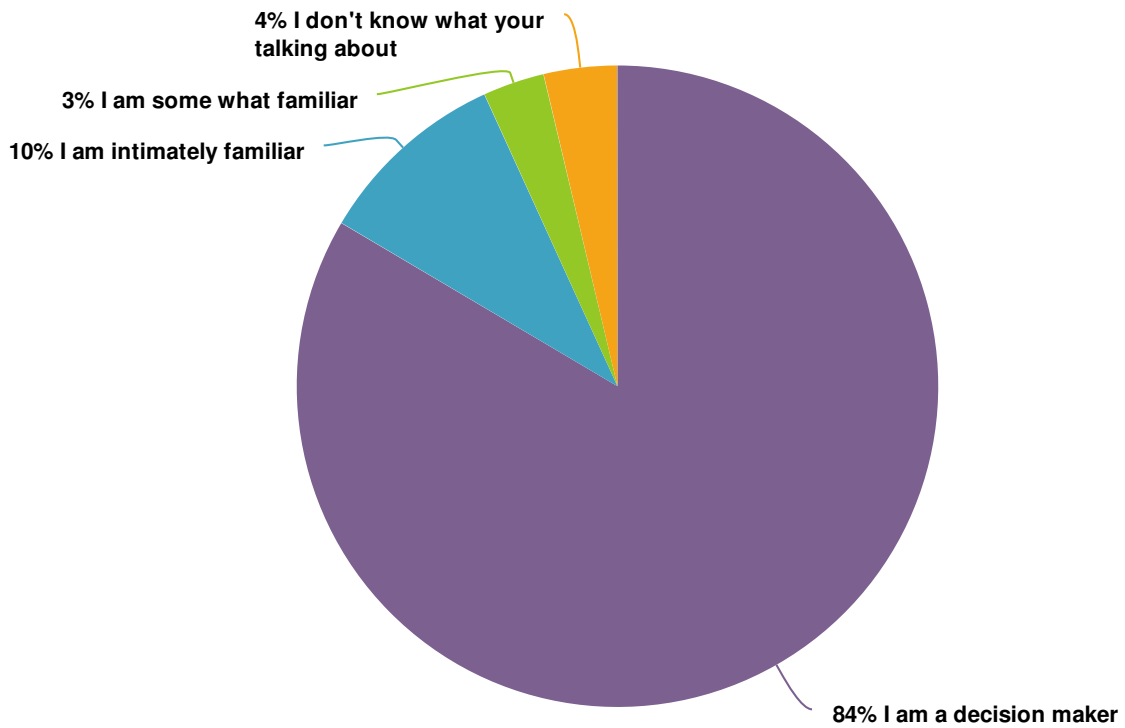


Report for Cavin Cyber Security Posture Survey

Response Counts



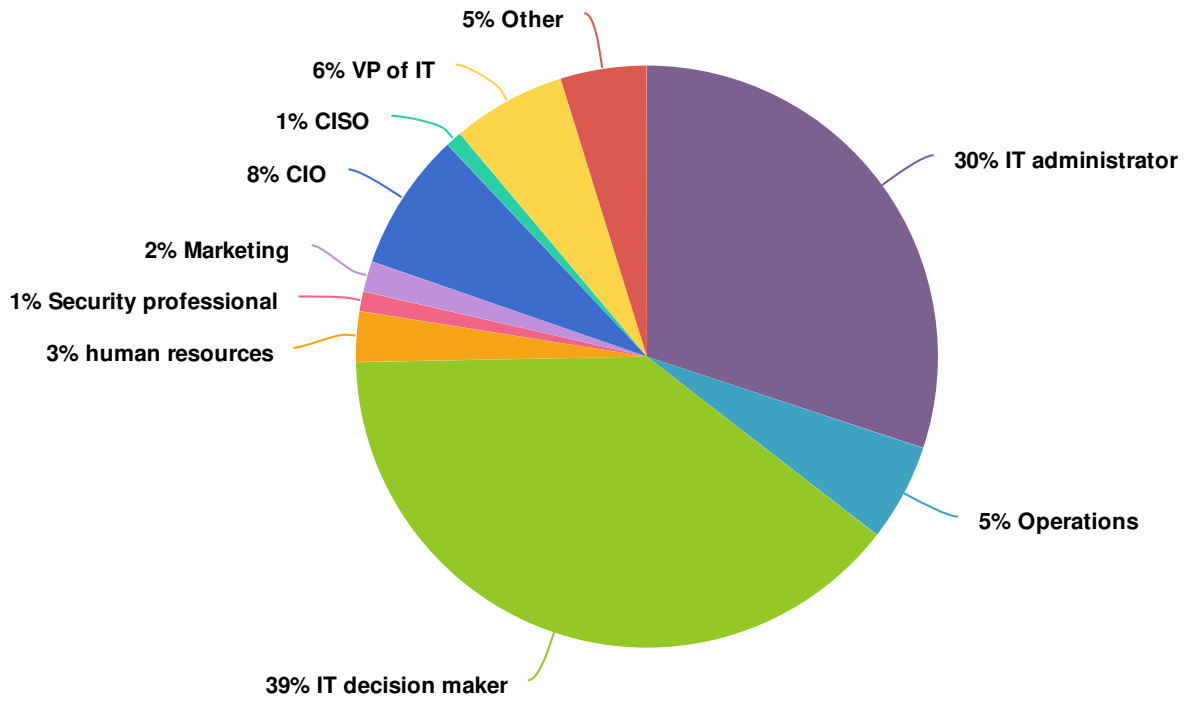
1. How familiar are you with how your organization assesses and maintains its cybersecurity/risk posture?



Value	Percent	Responses
I am a decision maker	83.5%	294
I am intimately familiar	9.7%	34
I am some what familiar	3.1%	11
I don't know what your talking about	3.7%	13

Totals: 352

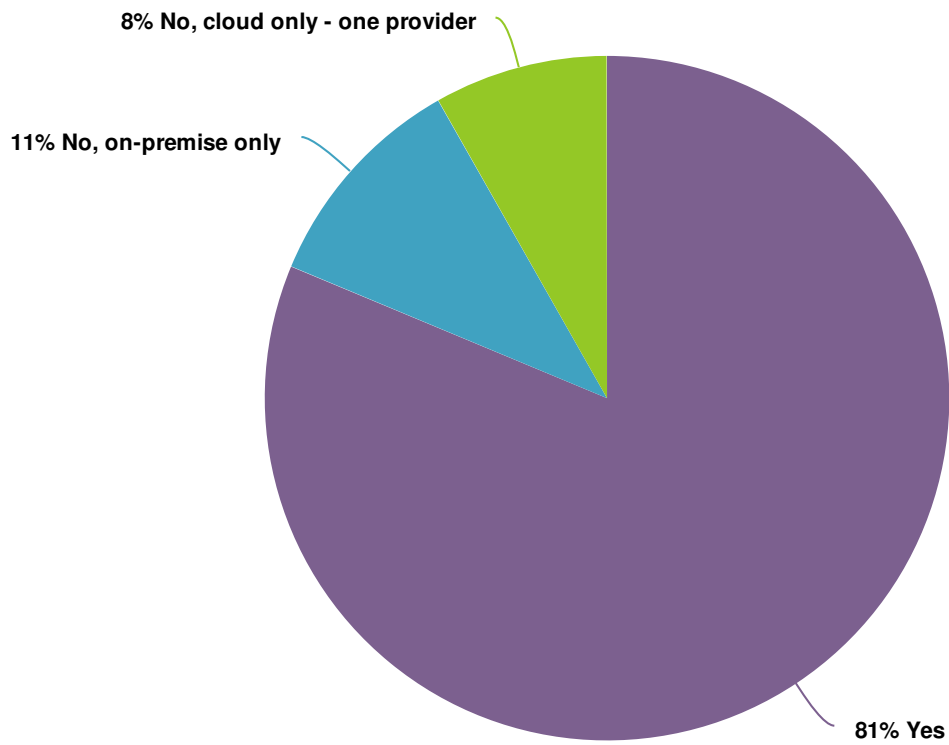
2. What is your role within your organization?



Value	Percent	Responses
IT administrator	30.1%	106
Operations	5.4%	19
IT decision maker	39.2%	138
human resources	2.8%	10
Security professional	1.1%	4
Marketing	1.7%	6
CIO	7.7%	27
CISO	0.9%	3
VP of IT	6.3%	22
Other	4.8%	17

Totals: 352

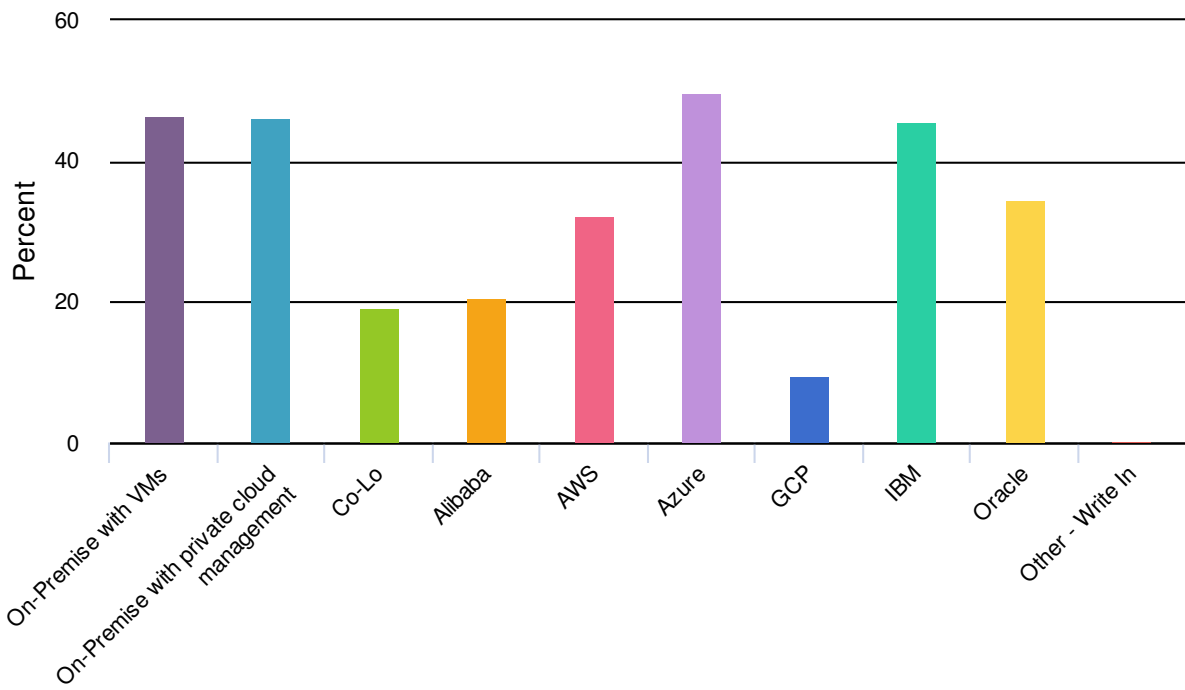
3. Does your organization currently deploy a hybrid or multi cloud strategy?













Value	Percent	Responses
Yes	81.3%	286
No, on-premise only	10.5%	37
No, cloud only - one provider	8.2%	29

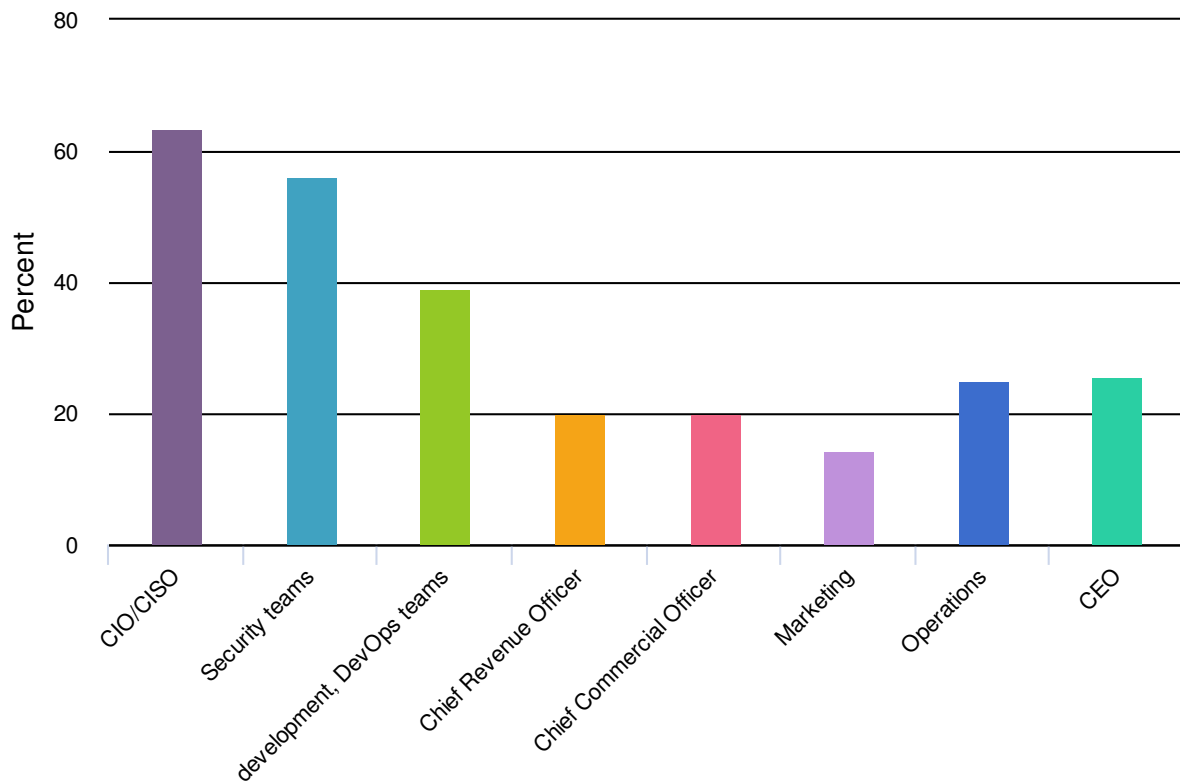
Totals: 352

4. What is your multi-cloud / hybrid-cloud deployment architecture? Two or more.



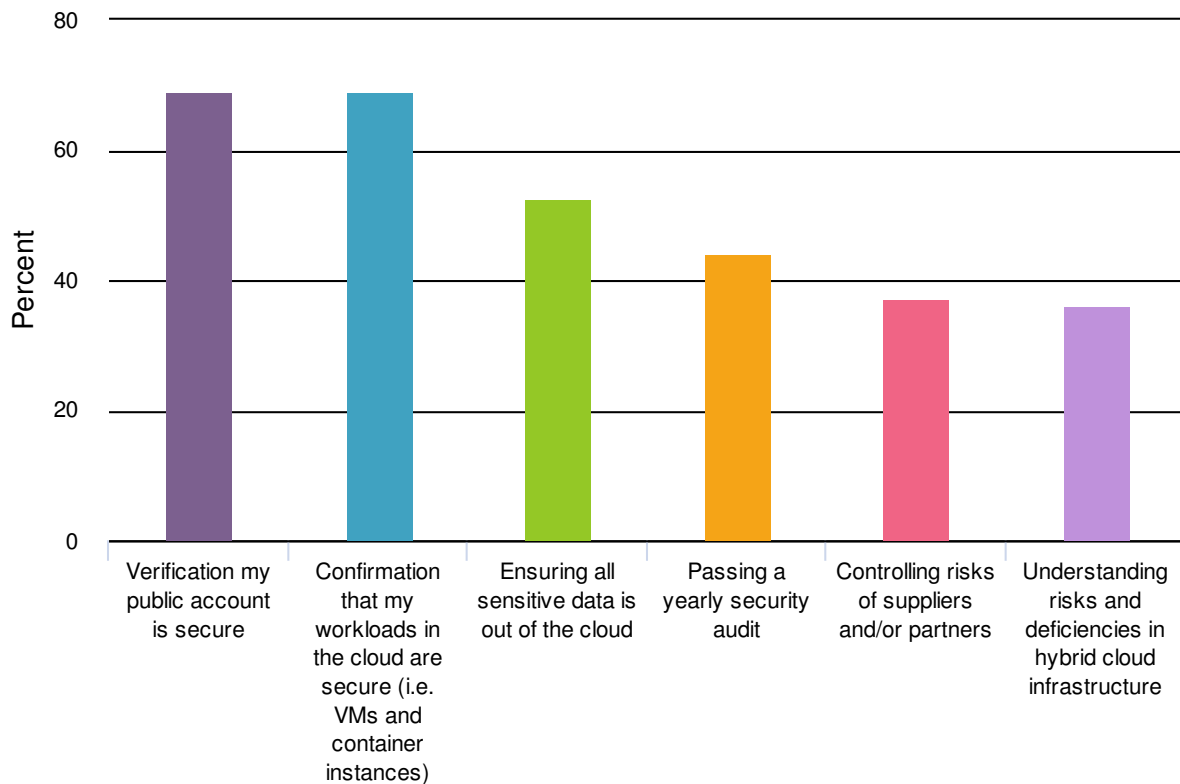
Value		Percent	Responses
On-Premise with VMs		46.6%	117
On-Premise with private cloud management		46.2%	116
Co-Lo		19.1%	48
Alibaba		20.7%	52
AWS		32.3%	81
Azure		49.8%	125
GCP		9.6%	24
IBM		45.8%	115
Oracle		34.7%	87
Other - Write In		0.4%	1

5. Who within your organization cares about the cyber security posture? One or more.



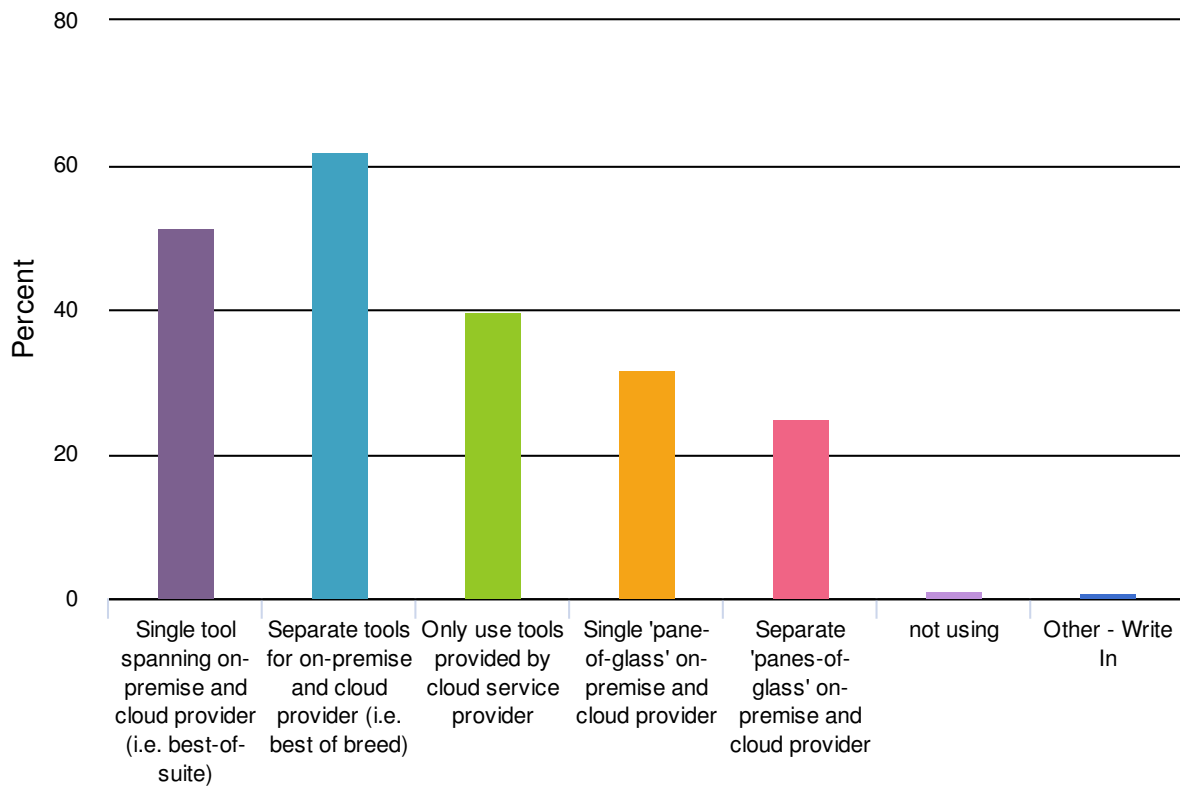
Value	Percent	Responses
CIO/CISO	63.3%	159
Security teams	56.2%	141
development, DevOps teams	39.0%	98
Chief Revenue Officer	19.9%	50
Chief Commercial Officer	19.9%	50
Marketing	14.3%	36
Operations	25.1%	63
CEO	25.5%	64

6. What does your hybrid cloud cyber posture and security mean to you? One or more



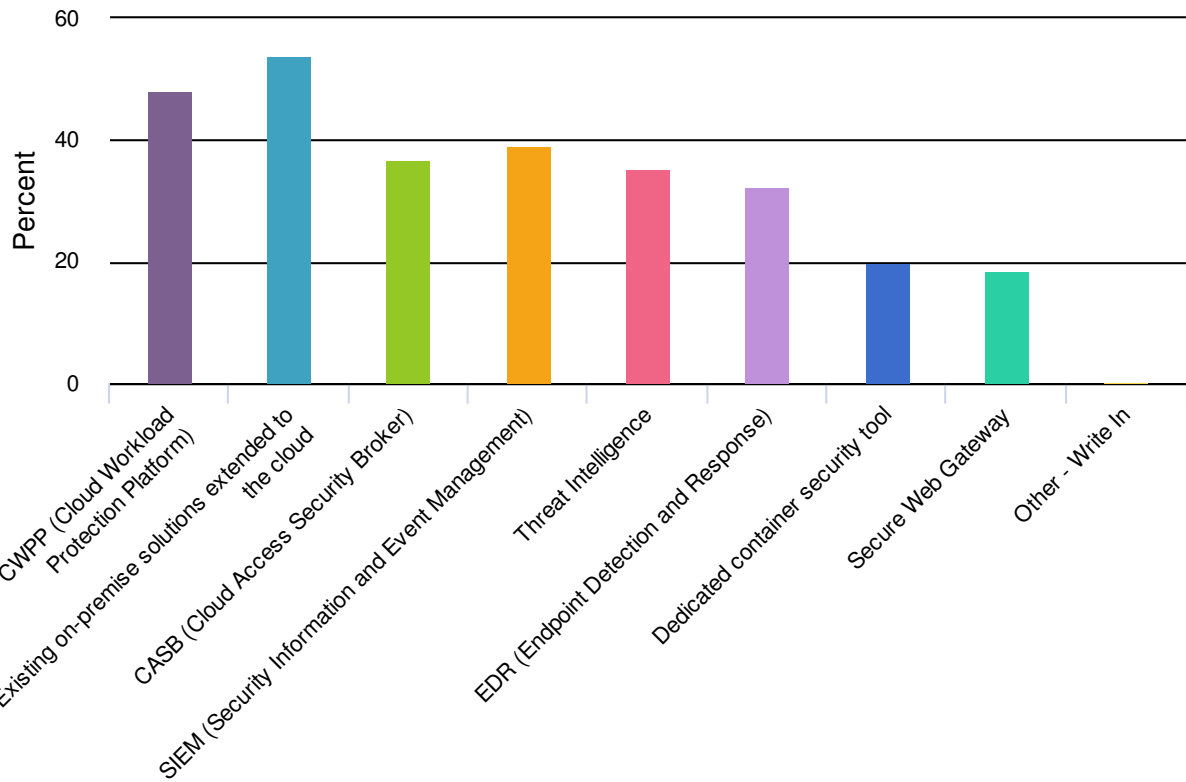
Value	Percent	Responses
Verification my public account is secure	68.9%	173
Confirmation that my workloads in the cloud are secure (i.e. VMs and container instances)	68.9%	173
Ensuring all sensitive data is out of the cloud	52.6%	132
Passing a yearly security audit	44.2%	111
Controlling risks of suppliers and/or partners	37.1%	93
Understanding risks and deficiencies in hybrid cloud infrastructure	36.3%	91










7. What is your hybrid cloud security management architecture? One or more



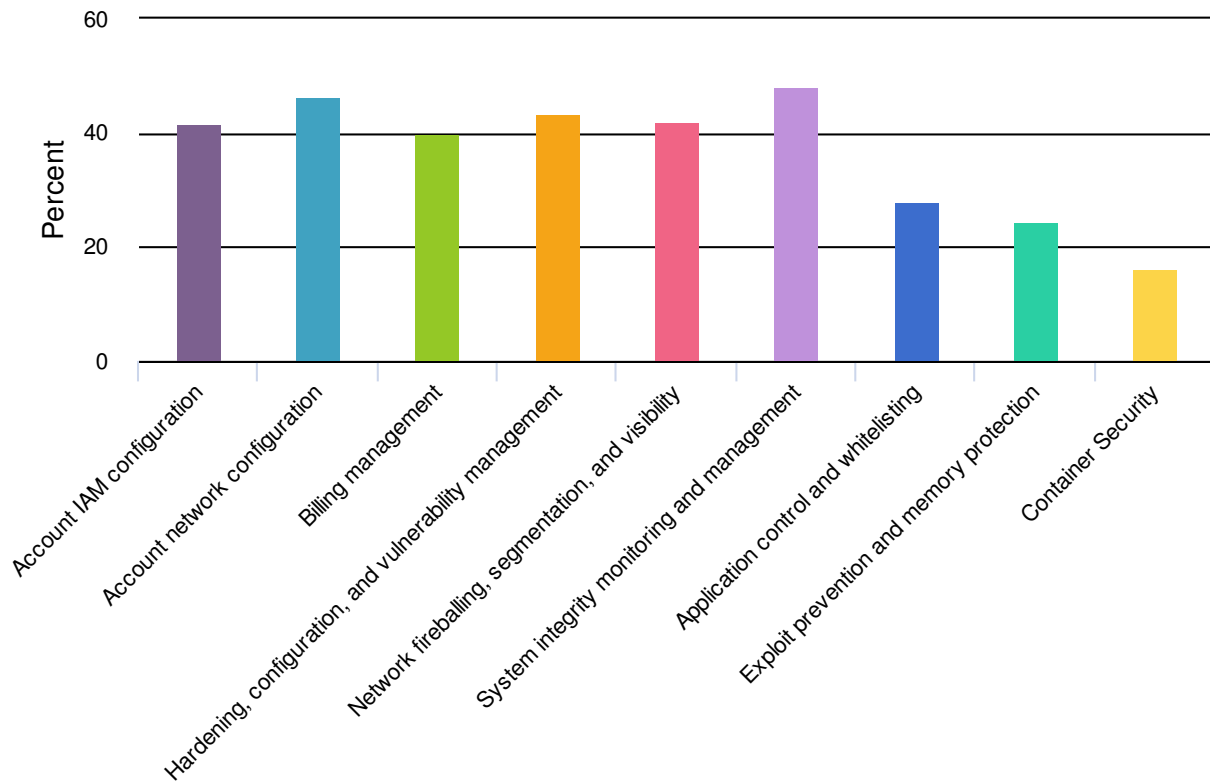
Value	Percent	Responses
Single tool spanning on-premise and cloud provider (i.e. best-of-suite)	51.4%	129
Separate tools for on-premise and cloud provider (i.e. best of breed)	61.8%	155
Only use tools provided by cloud service provider	39.8%	100
Single 'pane-of-glass' on-premise and cloud provider	31.9%	80
Separate 'panes-of-glass' on-premise and cloud provider	25.1%	63
not using	1.2%	3
Other - Write In	0.8%	2

8. What hybrid cloud security management tools do you currently use? One or more



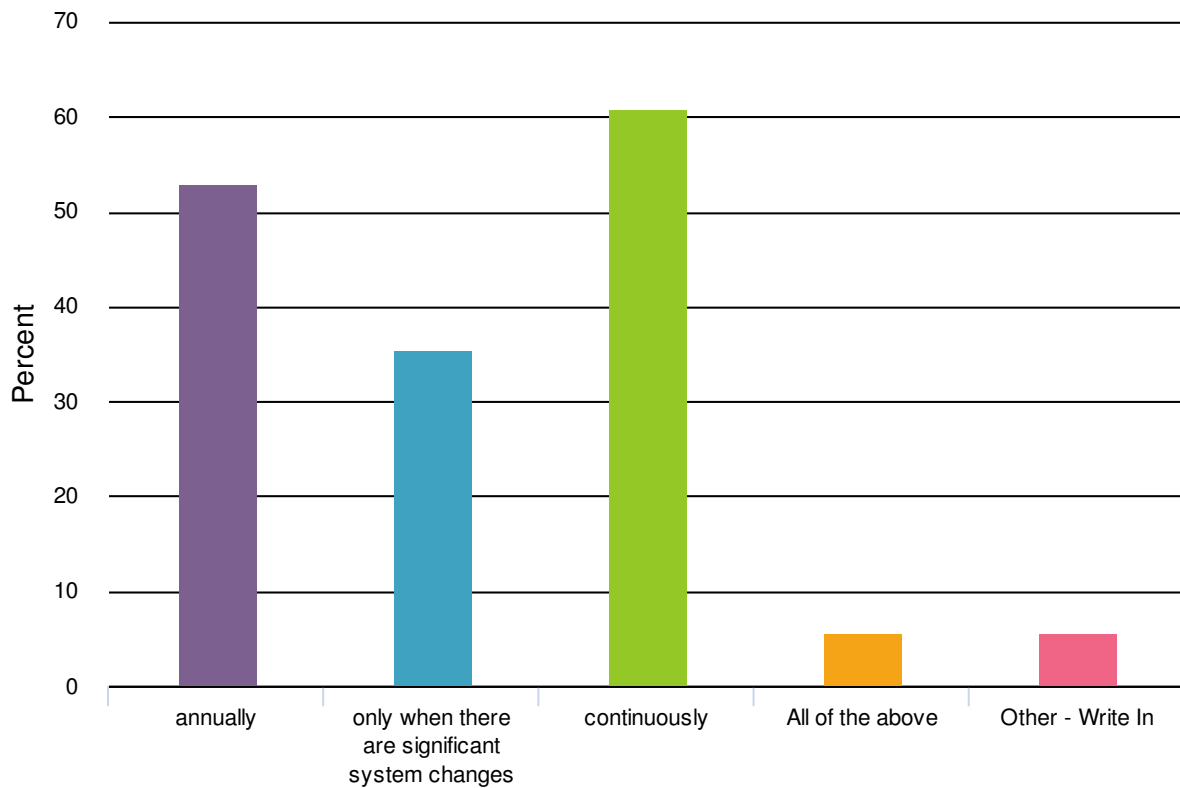
Value		Percent	Responses
CWPP (Cloud Workload Protection Platform)		48.2%	121
Existing on-premise solutions extended to the cloud		53.8%	135
CASB (Cloud Access Security Broker)		36.7%	92
SIEM (Security Information and Event Management)		39.0%	98
Threat Intelligence		35.5%	89
EDR (Endpoint Detection and Response)		32.3%	81
Dedicated container security tool		19.9%	50
Secure Web Gateway		18.7%	47
Other - Write In		0.4%	1

9. What hybrid cloud security features are most important to you? One or more



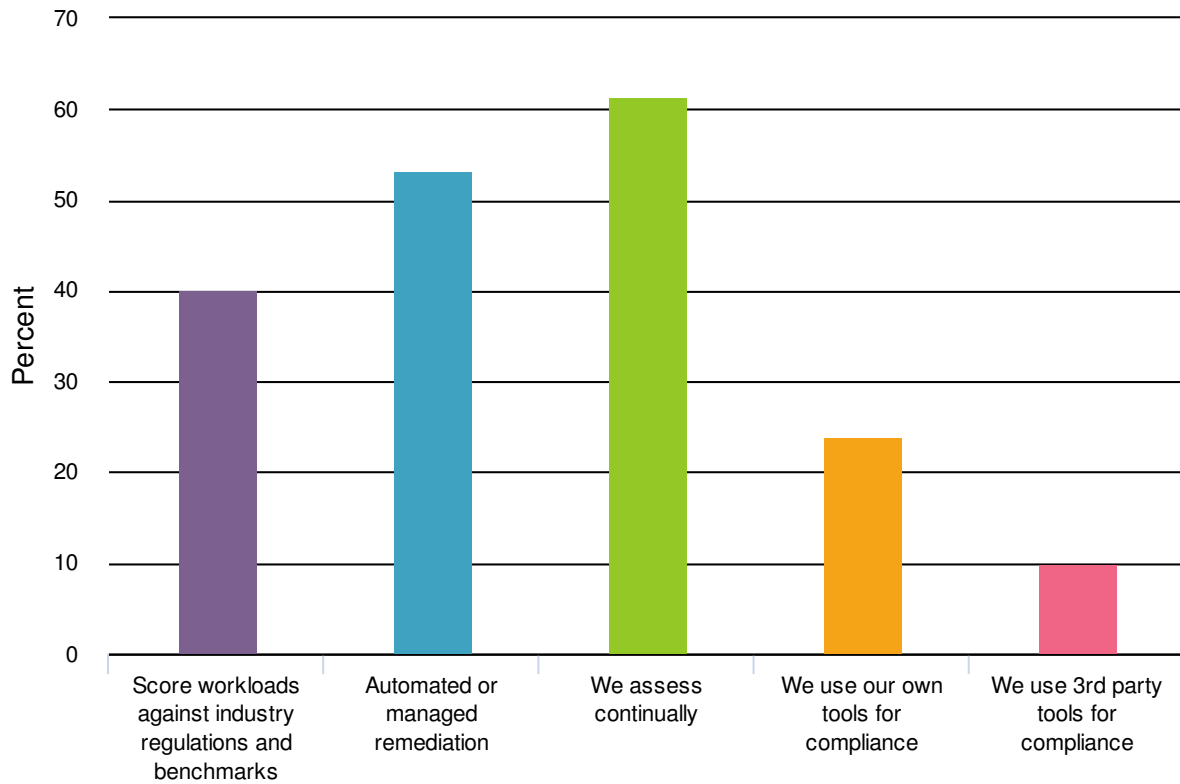
Value	Percent	Responses
Account IAM configuration	41.8%	105
Account network configuration	46.2%	116
Billing management	39.8%	100
Hardening, configuration, and vulnerability management	43.4%	109
Network fireballing, segmentation, and visibility	42.2%	106
System integrity monitoring and management	48.2%	121
Application control and whitelisting	27.9%	70
Exploit prevention and memory protection	24.3%	61
Container Security	16.3%	41

10. how often do you determine the state or health of your organization's cyber security posture? One or more.



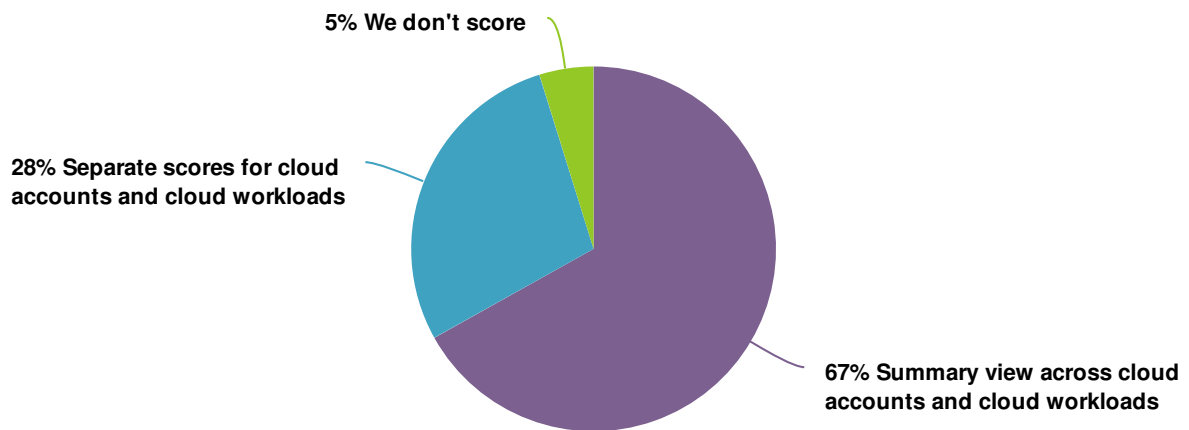
Value	Percent	Responses
annually	53.0%	133
only when there are significant system changes	35.5%	89
continuously	61.0%	153
All of the above	5.6%	14
Other - Write In	5.6%	14




11. How do you enable continuous compliance across your hybrid cloud? One or more



Value	Percent	Responses
Score workloads against industry regulations and benchmarks	40.2%	101
Automated or managed remediation	53.4%	134
We assess continually	61.4%	154
We use our own tools for compliance	23.9%	60
We use 3rd party tools for compliance	10.0%	25

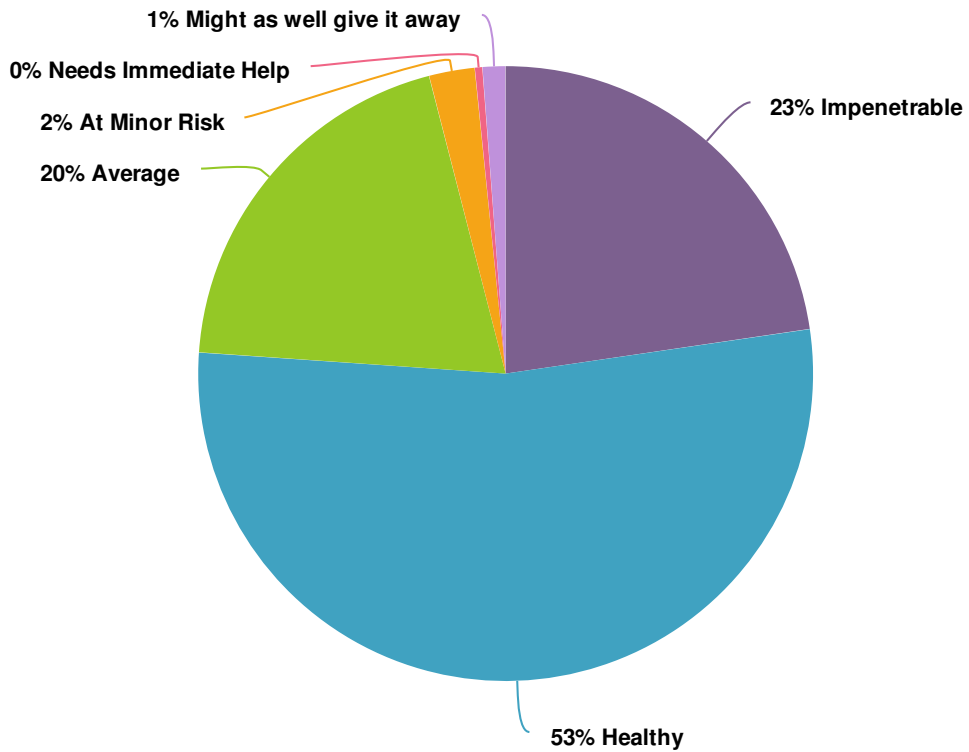
12. How do you score overall risk posture?



Value		Percent	Responses
Summary view across cloud accounts and cloud workloads		66.9%	168
Separate scores for cloud accounts and cloud workloads		28.3%	71
We don't score		4.8%	12

Totals: 251

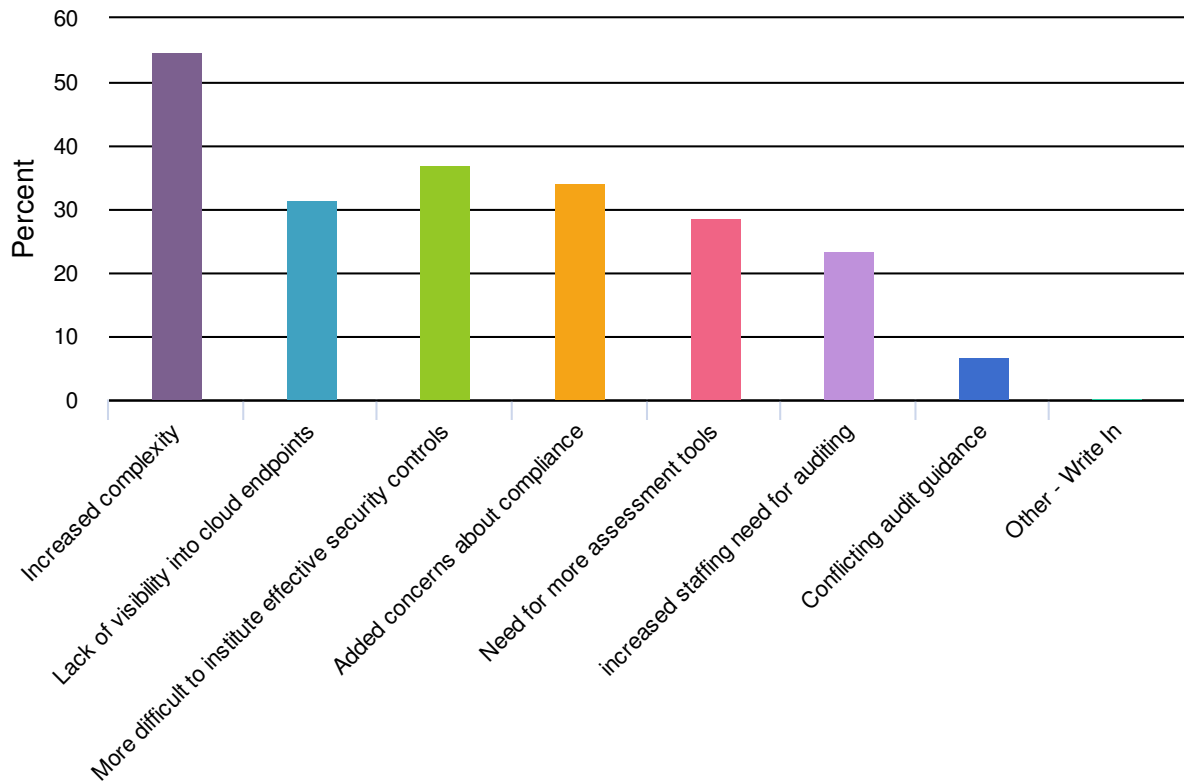
13. If you were to honestly rate the health of your organization's cybersecurity posture, what would it be?











Value	Percent	Responses
Impenetrable	22.7%	57
Healthy	53.4%	134
Average	19.9%	50
At Minor Risk	2.4%	6
Needs Immediate Help	0.4%	1
Might as well give it away	1.2%	3

Totals: 251

14. In what ways have the deployment of hybrid cloud architectures changed your organization's cybersecurity posture?



Value		Percent	Responses
Increased complexity		55.0%	138
Lack of visibility into cloud endpoints		31.5%	79
More difficult to institute effective security controls		37.1%	93
Added concerns about compliance		34.3%	86
Need for more assessment tools		28.7%	72
increased staffing need for auditing		23.5%	59
Conflicting audit guidance		6.8%	17
Other - Write In		0.4%	1