

The background is a solid blue gradient. On the left side, there is a large, abstract, circular graphic composed of many thin, overlapping, light blue lines that swirl around, resembling a stylized globe or a network. The SentinelOne logo is positioned on the left, with the word "Sentinel" in a bold, sans-serif font and "One" in a lighter, sans-serif font.

SentinelOne

RANSOMWARE RESEARCH
CYBER INSURANCE & CYBER GUARANTEES

Almost half (48%) of those surveyed state that their organization has suffered a ransomware attack in the last 12 months (sheet 6). Those who have been affected have had to defend against six attacks on average (sheet 8), with the majority (94%) stating that there was an impact on their organization as a result of these ransomware attacks. The most common impacts are increased spending on IT security (67%), change of IT security strategy to focus on mitigation (52%) and loss of confidence in existing cyber security solutions (45%) (sheet 15). Of those respondents whose organization has suffered a ransomware attack in the last 12 months, over one in ten (15%) report that an impact of this attack was that their organization invested in cyber insurance. However, just over seven in ten (72%) report that their organization has a cyber insurance policy in place. Under two in ten (17%) do not have a policy in place but are planning on implementing one in the future and under one in ten (7%) are not planning to do this at all.

Of those respondents whose organization does not have a cyber insurance policy in place, just over six in ten (61%) report that their organization chose to invest the money in preventing the breach in the first place. Furthermore, around two in ten (24%) state that cost is too prohibited and the same proportion (24%) report that their organization does not feel that they are at great enough risk. Almost two in ten (18%) also report that their organization did not know that they could buy cyber insurance.

Just under half of those interviewed (49%) agree that cybercriminals are constantly ahead and their organization is now focused on mitigation rather than cyber protection. Similarly, around half (52%) agree that their organization may look to get cyber insurance now that the possibility of fines is higher with the GDPR.

Of those respondents whose organization does have a cyber insurance policy in place, 91% have some level of coverage for ransomware attacks, but only 55% are fully covered. Of those respondents whose organization has cover for at least one cyber-attack, 78% have made an insurance claim against at least one attack and 17% of respondents with coverage for ransomware in particular have made a claim against ransomware attacks.

Of those whose organization has made an insurance claim against a ransomware attack in the last 12 months, 70% of respondents state that their cyber insurance provider paid the costs of notifying relevant parties of the breach. Furthermore, just under seven in ten (68%) paid the cost of investigating the source of the breach and a similar proportion (51%) paid the costs of recriminating lawsuits or legal proceedings. Only a quarter (25%) of respondents cite that their cyber insurance provider paid the ransom cost demanded by the attacker.

Nine in ten (90%) respondents would like to see all IT security vendors/managed security providers offer a guarantee on their products/services. Of those respondents, just under six in ten (59%) believe that if IT security vendors are confident their product works, then they should guarantee it. Moreover, half (50%) of respondents believe that if the product has a fault the vendor should be responsible and a further 43% report that the cost of failure is too high for only the vendor's clients to shoulder the burden alone.

'Out of the minority (7%) of respondents who do not agree that all IT security vendors/managed security providers should offer a guarantee on their products/services, over half (53%) believe that IT security vendors would likely increase their prices to cover the cost of a guarantee. Furthermore, nearly four in ten (38%) cite that cyber-attacks are evolving too quickly for IT security vendors to be expected to keep up.

'Under half (47%) of respondents' organizations' primary IT security vendor/managed security providers will cover the cost of detecting the source of the breach. In addition, 46% believe that their organization's primary IT security vendor will ensure that the relevant parties of the breach are notified and just over four in ten (42%) state that their organization's primary IT security vendor will offer business remuneration, covering for business losses associated with a security breach. However, one in ten (10%) of respondents' organizations' primary IT security vendors offer no cyber guarantee.

Of those respondents whose organization does have a cyber insurance policy in place, 91% have some level of coverage for ransomware attacks, but only 55% are fully covered. Of those respondents whose organization has cover for at least one cyber-attack, 78% have made an insurance claim against at least one attack and 17% of respondents with coverage for ransomware in particular have made a claim against ransomware attacks.

The majority (85%) report that they would change provider to an IT security vendor who offers a guarantee should their products fail and leave their organization exposed to cyber-attackers. Nearly eight in ten (79%) respondents agree that if security vendors were confident in their products they would guarantee them and the same proportion (79%) agree that if other products (like cars etc.) come with warranties or guarantees, then IT security products should too. Around half (53%) of respondents also believe that hackers are winning the battle against IT security vendors.

1	In case of a successful cyber-attack, does your organisation have cyber insurance?
2	Why does your organisation not have a cyber insurance policy in place currently?
3a	Which of the following types of cyber-attack or risks does your organisation's cyber insurance cover? Country
3b	Which of the following types of cyber-attack or risks does your organisation's cyber insurance cover? Size
3c	Which of the following types of cyber-attack or risks does your organisation's cyber insurance cover? Sector
4	And against which of these cyber-attacks or risks have you had to make an insurance claim against in the past 12 months?
5	Which of the following costs did your cyber insurance provider pay out for on your organisation's claim for this ransomware attack?
6	Does your organisation install anti-virus on endpoints?
7a	To what extent do you agree with the following statements? Country
7b	To what extent do you agree with the following statements? Size
7c	To what extent do you agree with the following statements? Sector
8	Do you agree that IT security vendors/managed security providers should be offering a guarantee on the competence of their products?
9	When thinking about your organisation's primary IT security vendor/managed security provider, do they offer a cyber guarantee should their security fail and your organisation fall victim to a successful cyber-attack?
10	Why do you think IT security vendors/managed security providers should offer a guarantee to their clients on the competence of their products?
11	Why do you think IT security vendors/managed security providers do not need to offer a guarantee to their clients on the competence of their products?
	<u>Demographics</u>
D1	How many employees does your organisation have globally?
D2	Within which sector is your organisation?
D3	In which one of these functional areas are you primarily employed within your organisation?
D4	What is your level of involvement in IT security within your organization?

In case of a successful cyber-attack, does your organization have cyber insurance?

SentinelOne

						Employees		
	Total	UK	US	France	Germany	1k-3k	3k-5k	5k+
Yes, we have a policy in place	72%	49%	83%	69%	77%	67%	73%	76%
No, but we are planning on implementing a policy in the future	17%	20%	14%	17%	20%	22%	15%	13%
No, and we are not planning on implementing a cyber insurance policy	7%	20%	3%	7%	2%	5%	9%	8%
Don't know	4%	11%	1%	7%	1%	6%	3%	3%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
Yes, we have a policy in place	72%	73%	93%	71%	75%	70%	71%	66%	64%	76%
No, but we are planning on implementing a policy in the future	17%	16%	7%	17%	18%	18%	6%	18%	20%	17%
No, and we are not planning on implementing a cyber insurance policy	7%	4%	0%	9%	3%	9%	12%	11%	10%	5%
Don't know	4%	7%	0%	3%	4%	3%	12%	5%	6%	2%

Why does your organization not have a cyber insurance policy in place currently?

	Total	UK	US	France	Germany	Employees		
						1k-3k	3k-5k	5k+
We choose to invest the money in preventing the breach in the first place	61%	65%	70%	38%	68%	58%	65%	63%
We have an existing insurance policy (not a specific cyber insurance policy) that covers losses incurred from a cyber-attack	28%	30%	21%	38%	23%	28%	30%	25%
Cost is too prohibitive	24%	23%	30%	21%	23%	32%	30%	6%
My organisation does not feel we are at great enough risk	24%	23%	21%	25%	27%	16%	35%	22%
We did not know that we could buy cyber insurance	18%	20%	18%	21%	9%	18%	14%	22%
We tried to buy cyber insurance but were denied coverage	2%	0%	3%	4%	0%	0%	3%	3%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	2%	5%	0%	0%	0%	0%	0%	6%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
We choose to invest the money in preventing the breach in the first place	61%	45%	50%	61%	57%	56%	33%	67%	67%	79%
We have an existing insurance policy (not a specific cyber insurance policy) that covers losses incurred from a cyber-attack	28%	55%	50%	39%	14%	22%	0%	11%	24%	43%
Cost is too prohibitive	24%	18%	100%	11%	36%	33%	33%	28%	14%	21%
My organisation does not feel we are at great enough risk	24%	36%	0%	28%	14%	28%	0%	17%	24%	29%
We did not know that we could buy cyber insurance	18%	18%	50%	22%	36%	11%	33%	11%	5%	21%
We tried to buy cyber insurance but were denied coverage	2%	0%	0%	0%	0%	0%	0%	6%	5%	0%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	2%	0%	0%	0%	0%	0%	0%	6%	5%	0%

Country - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	Total			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	75%	21%	2%	2%
Phishing	62%	34%	3%	1%
DDoS	62%	32%	4%	3%
Ransomware	55%	36%	7%	3%
Advance persistent threats (APTs)	59%	35%	4%	2%
Lost devices (employee negligence)	58%	33%	9%	1%
Privileged account breach	60%	33%	5%	2%
Blastware	51%	36%	8%	5%
Zero-day attacks	52%	33%	11%	5%
Malicious insider	48%	41%	9%	2%

	UK			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	49%	37%	4%	10%
Phishing	51%	33%	8%	8%
DDoS	49%	37%	8%	6%
Ransomware	43%	41%	6%	10%
Advance persistent threats (APTs)	47%	37%	6%	10%
Lost devices (employee negligence)	45%	39%	12%	4%
Privileged account breach	49%	31%	10%	10%
Blastware	37%	37%	12%	14%
Zero-day attacks	39%	39%	8%	14%
Malicious insider	31%	49%	12%	8%

Country - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	US			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	82%	16%	2%	1%
Phishing	69%	28%	2%	1%
DDoS	62%	33%	1%	4%
Ransomware	52%	39%	6%	2%
Advance persistent threats (APTs)	67%	30%	2%	1%
Lost devices (employee negligence)	63%	27%	8%	1%
Privileged account breach	72%	22%	4%	2%
Blastware	52%	34%	8%	7%
Zero-day attacks	50%	32%	12%	6%
Malicious insider	55%	38%	6%	1%

	France			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	72%	26%	0%	1%
Phishing	58%	42%	0%	0%
DDoS	64%	32%	4%	0%
Ransomware	71%	23%	6%	0%
Advance persistent threats (APTs)	62%	30%	7%	0%
Lost devices (employee negligence)	58%	30%	12%	0%
Privileged account breach	54%	42%	4%	0%
Blastware	58%	35%	7%	0%
Zero-day attacks	57%	33%	10%	0%
Malicious insider	33%	49%	17%	0%

Country - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	Germany			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	79%	19%	1%	0%
Phishing	58%	39%	3%	0%
DDoS	70%	25%	5%	0%
Ransomware	56%	35%	9%	0%
Advance persistent threats (APTs)	47%	47%	6%	0%
Lost devices (employee negligence)	53%	42%	5%	0%
Privileged account breach	45%	48%	6%	0%
Blastware	53%	39%	8%	0%
Zero-day attacks	60%	31%	9%	0%
Malicious insider	57%	34%	8%	1%

Size - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	Total			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	75%	21%	2%	2%
Phishing	62%	34%	3%	1%
DDoS	62%	32%	4%	3%
Ransomware	55%	36%	7%	3%
Advance persistent threats (APTs)	59%	35%	4%	2%
Lost devices (employee negligence)	58%	33%	9%	1%
Privileged account breach	60%	33%	5%	2%
Blastware	51%	36%	8%	5%
Zero-day attacks	52%	33%	11%	5%
Malicious insider	48%	41%	9%	2%

	1,001-3,000 employees			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	79%	19%	1%	2%
Phishing	72%	26%	2%	1%
DDoS	63%	29%	5%	2%
Ransomware	55%	36%	5%	3%
Advance persistent threats (APTs)	59%	34%	5%	2%
Lost devices (employee negligence)	55%	38%	7%	1%
Privileged account breach	61%	34%	3%	2%
Blastware	58%	27%	9%	5%
Zero-day attacks	55%	28%	10%	7%
Malicious insider	51%	39%	8%	2%

Size - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	3,001-5,000 employees			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	77%	20%	1%	3%
Phishing	55%	41%	3%	2%
DDoS	60%	36%	3%	2%
Ransomware	56%	36%	7%	2%
Advance persistent threats (APTs)	59%	37%	3%	2%
Lost devices (employee negligence)	60%	30%	9%	1%
Privileged account breach	52%	39%	7%	2%
Blastware	48%	41%	8%	3%
Zero-day attacks	50%	36%	11%	3%
Malicious insider	41%	43%	15%	2%

	More than 5,000 employees			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	69%	26%	3%	2%
Phishing	59%	36%	3%	2%
DDoS	63%	31%	3%	3%
Ransomware	55%	35%	8%	3%
Advance persistent threats (APTs)	59%	34%	5%	2%
Lost devices (employee negligence)	58%	29%	11%	2%
Privileged account breach	66%	26%	6%	3%
Blastware	47%	39%	8%	6%
Zero-day attacks	50%	36%	10%	4%
Malicious insider	52%	40%	6%	2%

Sector - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	Total			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	75%	21%	2%	2%
Phishing	62%	34%	3%	1%
DDoS	62%	32%	4%	3%
Ransomware	55%	36%	7%	3%
Advance persistent threats (APTs)	59%	35%	4%	2%
Lost devices (employee negligence)	58%	33%	9%	1%
Privileged account breach	60%	33%	5%	2%
Blastware	51%	36%	8%	5%
Zero-day attacks	52%	33%	11%	5%
Malicious insider	48%	41%	9%	2%

	Business and professional services			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	68%	20%	5%	8%
Phishing	55%	35%	3%	8%
DDoS	60%	33%	3%	5%
Ransomware	53%	28%	13%	8%
Advance persistent threats (APTs)	40%	48%	5%	8%
Lost devices (employee negligence)	58%	33%	8%	3%
Privileged account breach	40%	43%	10%	8%
Blastware	38%	43%	13%	8%
Zero-day attacks	48%	28%	15%	10%
Malicious insider	48%	33%	15%	5%

Sector - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	Construction and property			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	79%	18%	0%	4%
Phishing	79%	21%	0%	0%
DDoS	75%	18%	7%	0%
Ransomware	46%	50%	4%	0%
Advance persistent threats (APTs)	71%	25%	4%	0%
Lost devices (employee negligence)	75%	14%	11%	0%
Privileged account breach	57%	43%	0%	0%
Blastware	57%	25%	11%	7%
Zero-day attacks	54%	36%	11%	0%
Malicious insider	46%	54%	0%	0%

	Financial services			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	76%	20%	4%	0%
Phishing	59%	39%	2%	0%
DDoS	65%	29%	6%	0%
Ransomware	55%	37%	6%	2%
Advance persistent threats (APTs)	65%	31%	2%	2%
Lost devices (employee negligence)	51%	37%	12%	0%
Privileged account breach	73%	20%	6%	0%
Blastware	43%	45%	6%	6%
Zero-day attacks	57%	33%	6%	4%
Malicious insider	55%	41%	4%	0%

Sector - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

SentinelOne

	IT, technology and telecoms			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	84%	16%	0%	0%
Phishing	70%	28%	2%	0%
DDoS	56%	40%	4%	0%
Ransomware	60%	32%	8%	0%
Advance persistent threats (APTs)	64%	30%	6%	0%
Lost devices (employee negligence)	60%	38%	2%	0%
Privileged account breach	76%	22%	2%	0%
Blastware	58%	36%	6%	0%
Zero-day attacks	58%	34%	6%	2%
Malicious insider	62%	30%	8%	0%

	Manufacturing and production			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	72%	26%	0%	2%
Phishing	45%	53%	2%	0%
DDoS	68%	28%	4%	0%
Ransomware	60%	38%	2%	0%
Advance persistent threats (APTs)	55%	38%	6%	0%
Lost devices (employee negligence)	57%	28%	15%	0%
Privileged account breach	62%	23%	15%	0%
Blastware	60%	34%	6%	0%
Zero-day attacks	49%	40%	11%	0%
Malicious insider	47%	45%	9%	0%

Sector - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

	Media, leisure and entertainment			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	67%	17%	8%	8%
Phishing	58%	25%	8%	8%
DDoS	67%	25%	0%	8%
Ransomware	50%	25%	8%	17%
Advance persistent threats (APTs)	50%	42%	0%	8%
Lost devices (employee negligence)	33%	33%	25%	8%
Privileged account breach	58%	25%	8%	8%
Blastware	42%	25%	17%	17%
Zero-day attacks	58%	17%	8%	17%
Malicious insider	50%	42%	0%	8%

	Public sector			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	80%	17%	0%	2%
Phishing	66%	29%	2%	2%
DDoS	61%	22%	5%	12%
Ransomware	54%	27%	12%	7%
Advance persistent threats (APTs)	54%	39%	2%	5%
Lost devices (employee negligence)	59%	27%	10%	5%
Privileged account breach	61%	32%	0%	7%
Blastware	46%	27%	7%	20%
Zero-day attacks	34%	41%	10%	15%
Malicious insider	32%	39%	22%	7%

Sector - Which of the following types of cyber-attack or risks does your organization's cyber insurance cover?

	Retail, distribution and transport			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	67%	33%	0%	0%
Phishing	71%	27%	2%	0%
DDoS	56%	42%	2%	0%
Ransomware	58%	36%	7%	0%
Advance persistent threats (APTs)	58%	33%	9%	0%
Lost devices (employee negligence)	51%	44%	4%	0%
Privileged account breach	42%	56%	2%	0%
Blastware	53%	33%	13%	0%
Zero-day attacks	51%	29%	18%	2%
Malicious insider	29%	62%	7%	2%

	Other commercial sectors			
	We are fully covered for this	We are partially covered up to a certain value	We are not covered for this	Don't know
Trojans	77%	21%	2%	0%
Phishing	60%	35%	4%	0%
DDoS	60%	38%	0%	2%
Ransomware	54%	44%	2%	0%
Advance persistent threats (APTs)	67%	31%	2%	0%
Lost devices (employee negligence)	63%	31%	6%	0%
Privileged account breach	60%	33%	4%	2%
Blastware	56%	40%	4%	0%
Zero-day attacks	58%	29%	10%	2%
Malicious insider	60%	27%	13%	0%

And against which of these cyber-attacks or risks have you had to make an insurance claim against in the past 12 months? **SentinelOne**

	Total	UK	US	France	Germany	1-3k employees	3-5k employees	5k employees
Trojans	39%	21%	39%	38%	47%	39%	39%	38%
Phishing	39%	24%	37%	46%	47%	41%	39%	38%
DDoS	34%	21%	31%	35%	48%	35%	39%	28%
Ransomware	17%	17%	19%	20%	11%	18%	19%	15%
Advance persistent threats (APTs)	26%	10%	27%	36%	26%	20%	33%	27%
Lost devices (employee negligence)	31%	15%	40%	28%	25%	26%	36%	32%
Privileged account breach	20%	10%	21%	24%	19%	17%	22%	21%
Blastware	18%	8%	20%	20%	15%	17%	20%	16%
Zero-day attacks	18%	5%	20%	11%	29%	18%	21%	16%
Malicious insider	14%	3%	20%	16%	9%	11%	17%	16%
None of the above	22%	48%	25%	6%	14%	24%	15%	26%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
Trojans	39%	20%	48%	38%	60%	35%	40%	13%	40%	49%
Phishing	39%	44%	50%	27%	39%	41%	50%	31%	43%	41%
DDoS	34%	24%	31%	30%	33%	31%	18%	35%	41%	47%
Ransomware	17%	13%	22%	11%	35%	20%	0%	18%	14%	11%
Advance persistent threats (APTs)	26%	29%	37%	23%	34%	14%	18%	18%	27%	34%
Lost devices (employee negligence)	31%	28%	36%	37%	37%	45%	0%	14%	26%	31%
Privileged account breach	20%	18%	32%	17%	22%	15%	10%	24%	18%	18%
Blastware	18%	19%	26%	19%	26%	18%	13%	7%	8%	20%
Zero-day attacks	18%	10%	32%	11%	30%	12%	0%	10%	22%	24%
Malicious insider	14%	9%	18%	11%	24%	9%	0%	21%	20%	10%
None of the above	22%	36%	18%	31%	8%	17%	55%	33%	13%	15%

Which of the following costs did your cyber insurance provider pay out for on your organization's claim for this ransomware attack?

SentinelOne

	Total	UK	US	France	Germany	1-3k employees	3-5k employees	5k employees
The costs of notifying the relevant parties of the breach and ensuring compliance with the laws of the relevant countries regarding data protection	70%	86%	72%	46%	88%	76%	70%	63%
The cost of investigating the source of the breach, liaising with law enforcement agencies or third party security agencies to track down the responsible party	68%	14%	76%	85%	63%	43%	90%	75%
The costs of business losses associated with a security breach (loss of income, reputation damage, organisation downtime)	67%	86%	76%	62%	25%	76%	55%	69%
Legal costs of recriminating lawsuits or legal proceedings (civil and criminal) and also in the case of extortion due to ransomware breaches	51%	14%	59%	46%	63%	57%	45%	50%
The cost of paying the ransom demanded by the ransomware attacker	25%	0%	31%	23%	25%	19%	40%	13%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
My organisation's cyber insurance provider did not pay out at all for this ransomware attack	0%	0%	0%	0%	0%	0%	0%	0%
Don't know	0%	0%	0%	0%	0%	0%	0%	0%

Which of the following costs did your cyber insurance provider pay out for on your organization's claim for this ransomware attack?

SentinelOne

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
The costs of notifying the relevant parties of the breach and ensuring compliance with the laws of the relevant countries regarding data protection	70%	100%	50%	80%	75%	56%	-	50%	67%	100%
The cost of investigating the source of the breach, liaising with law enforcement agencies or third party security agencies to track down the responsible party	68%	50%	83%	100%	69%	78%	-	33%	83%	40%
The costs of business losses associated with a security breach (loss of income, reputation damage, organisation downtime)	67%	75%	67%	60%	75%	78%	-	33%	50%	80%
Legal costs of recriminating lawsuits or legal proceedings (civil and criminal) and also in the case of extortion due to ransomware breaches	51%	25%	50%	60%	38%	78%	-	67%	33%	60%
The cost of paying the ransom demanded by the ransomware attacker	25%	25%	33%	60%	25%	11%	-	17%	17%	20%
Other (please specify)	0%	0%	0%	0%	0%	0%	-	0%	0%	0%
My organisation's cyber insurance provider did not pay out at all for this ransomware attack	0%	0%	0%	0%	0%	0%	-	0%	0%	0%
Don't know	0%	0%	0%	0%	0%	0%	-	0%	0%	0%

Does your organization install anti-virus on endpoints?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
We install anti-virus on all <u>company owned</u> static devices (PCs, printers)	85%	83%	92%	79%	80%	83%	89%	84%
We install anti-virus on all <u>company owned</u> mobile devices (company laptops, phones)	73%	71%	74%	72%	72%	80%	71%	65%
We install anti-virus on all <u>employee owned</u> devices used by employees for work (employees own laptop, tablet, phone)	47%	33%	49%	39%	64%	49%	44%	47%
We do not install anti-virus on any endpoints	0%	0%	0%	0%	1%	0%	0%	1%
Don't know	0%	1%	0%	1%	0%	1%	0%	1%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
We install anti-virus on all <u>company owned</u> static devices (PCs, printers)	45%	57%	12%	48%	31%	55%	75%	23%	67%	43%
We install anti-virus on all <u>company owned</u> mobile devices (company laptops, phones)	27%	25%	76%	26%	43%	18%	0%	23%	6%	23%
We install anti-virus on all <u>employee owned</u> devices used by employees for work (employees own laptop, tablet, phone)	25%	14%	6%	26%	17%	24%	25%	50%	21%	34%
We do not install anti-virus on any endpoints	3%	0%	6%	0%	9%	3%	0%	4%	6%	0%
Don't know	0%	4%	0%	0%	0%	0%	0%	0%	0%	0%

Country - To what extent do you agree with the following statements?

	Total				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	38%	47%	12%	2%	1%
If security vendors were confident in their products they would guarantee them	41%	38%	18%	3%	1%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	38%	41%	16%	4%	1%
Hackers are currently winning the battle against IT security vendors	17%	36%	28%	15%	4%

	UK				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	33%	46%	18%	1%	2%
If security vendors were confident in their products they would guarantee them	35%	38%	23%	3%	1%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	33%	41%	20%	6%	0%
Hackers are currently winning the battle against IT security vendors	12%	40%	35%	12%	1%

Country - To what extent do you agree with the following statements?

	US				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	49%	39%	10%	2%	1%
If security vendors were confident in their products they would guarantee them	46%	39%	12%	2%	2%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	47%	41%	10%	3%	0%
Hackers are currently winning the battle against IT security vendors	21%	37%	26%	13%	4%

	France				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	37%	47%	13%	2%	1%
If security vendors were confident in their products they would guarantee them	38%	38%	22%	2%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	32%	41%	21%	4%	2%
Hackers are currently winning the battle against IT security vendors	17%	36%	19%	20%	8%

Country - To what extent do you agree with the following statements?

	Germany				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	24%	63%	10%	2%	1%
If security vendors were confident in their products they would guarantee them	39%	38%	19%	4%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	30%	43%	21%	5%	1%
Hackers are currently winning the battle against IT security vendors	12%	33%	35%	16%	4%

Size - To what extent do you agree with the following statements?

	Total				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	38%	47%	12%	2%	1%
If security vendors were confident in their products they would guarantee them	41%	38%	18%	3%	1%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	38%	41%	16%	4%	1%
Hackers are currently winning the battle against IT security vendors	17%	36%	28%	15%	4%

	1001-3,000 Employees				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	38%	48%	13%	1%	1%
If security vendors were confident in their products they would guarantee them	42%	43%	14%	2%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	38%	46%	13%	3%	1%
Hackers are currently winning the battle against IT security vendors	16%	34%	33%	16%	1%

Size - To what extent do you agree with the following statements?

	3,001-5000 Employees				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	43%	43%	11%	2%	1%
If security vendors were confident in their products they would guarantee them	36%	40%	22%	3%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	42%	37%	14%	6%	1%
Hackers are currently winning the battle against IT security vendors	17%	42%	18%	15%	8%

	More than 5,000 employees				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	35%	48%	12%	2%	3%
If security vendors were confident in their products they would guarantee them	44%	31%	18%	4%	3%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	33%	40%	24%	3%	1%
Hackers are currently winning the battle against IT security vendors	17%	33%	32%	13%	5%

Sector - To what extent do you agree with the following statements?

	Total				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	38%	47%	12%	2%	1%
If security vendors were confident in their products they would guarantee them	41%	38%	18%	3%	1%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	38%	41%	16%	4%	1%
Hackers are currently winning the battle against IT security vendors	17%	36%	28%	15%	4%

	Business and professional services				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	33%	51%	9%	4%	4%
If security vendors were confident in their products they would guarantee them	33%	42%	22%	4%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	33%	51%	15%	0%	2%
Hackers are currently winning the battle against IT security vendors	13%	36%	35%	13%	4%

Sector - To what extent do you agree with the following statements?

	Construction and property				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	40%	47%	10%	3%	0%
If security vendors were confident in their products they would guarantee them	40%	33%	27%	0%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	43%	43%	10%	3%	0%
Hackers are currently winning the battle against IT security vendors	17%	50%	17%	13%	3%

	Financial services				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	39%	46%	14%	0%	0%
If security vendors were confident in their products they would guarantee them	38%	36%	25%	1%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	33%	32%	30%	4%	0%
Hackers are currently winning the battle against IT security vendors	9%	35%	33%	20%	3%

Sector - To what extent do you agree with the following statements?

	IT, technology and telecoms				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	48%	46%	4%	1%	0%
If security vendors were confident in their products they would guarantee them	37%	45%	15%	3%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	48%	31%	16%	4%	0%
Hackers are currently winning the battle against IT security vendors	19%	40%	22%	10%	7%

	Manufacturing and production				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	34%	51%	13%	0%	1%
If security vendors were confident in their products they would guarantee them	51%	27%	18%	1%	3%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	46%	36%	10%	6%	1%
Hackers are currently winning the battle against IT security vendors	15%	39%	30%	13%	3%

Sector - To what extent do you agree with the following statements?

	Media, leisure and entertainment				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	35%	41%	18%	0%	6%
If security vendors were confident in their products they would guarantee them	35%	41%	12%	6%	6%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	24%	41%	18%	18%	0%
Hackers are currently winning the battle against IT security vendors	12%	24%	47%	18%	0%

	Public sector				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	29%	48%	21%	2%	0%
If security vendors were confident in their products they would guarantee them	50%	34%	15%	2%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	32%	47%	18%	3%	0%
Hackers are currently winning the battle against IT security vendors	16%	32%	31%	19%	2%

Sector - To what extent do you agree with the following statements?

	Retail, distribution and transport				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	44%	41%	9%	3%	3%
If security vendors were confident in their products they would guarantee them	37%	44%	13%	4%	1%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	36%	41%	17%	4%	1%
Hackers are currently winning the battle against IT security vendors	24%	34%	21%	14%	6%

	Other commercial sectors				
	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
I would change provider to an IT security vendor who offers a guarantee should their products fail and leave my organisation exposed to cyber-attackers	40%	44%	14%	2%	0%
If security vendors were confident in their products they would guarantee them	40%	43%	14%	3%	0%
If other products (like cars etc.) come with warranties or guarantees, then IT security products should, too	35%	52%	10%	3%	0%
Hackers are currently winning the battle against IT security vendors	21%	35%	25%	13%	6%

Do you agree that IT security vendors/managed security providers should be offering a guarantee on the competence of their products?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Yes, I would like to see all IT security vendors/managed security providers offer a guarantee on their products/services	90%	75%	95%	93%	95%	93%	90%	87%
No, I do not feel that this is necessary	7%	18%	3%	6%	4%	5%	7%	9%
No opinion	3%	7%	3%	1%	1%	2%	3%	4%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
Yes, I would like to see all IT security vendors/managed security providers offer a guarantee on their products/services	90%	96%	100%	83%	97%	91%	82%	84%	89%	92%
No, I do not feel that this is necessary	7%	2%	0%	12%	1%	4%	18%	13%	10%	5%
No opinion	3%	2%	0%	6%	1%	4%	0%	3%	1%	3%

When thinking about your organization's primary IT security vendor/managed security provider, do they offer a cyber guarantee should their security fail and your organization fall victim to a successful cyber-attack?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
My organisation's primary IT security vendor/managed security provider will cover the cost of detecting the source of the breach, and liaising with law enforcement agencies or third party security agencies to track down the responsible party	47%	24%	55%	44%	59%	55%	44%	59%
My organisation's primary IT security vendor/primary security provider will ensure that the relevant parties of the breach are notified and ensure that we are compliant with the laws of the relevant countries regarding data protection	46%	27%	50%	47%	56%	50%	47%	56%
My organisation's primary IT security vendor/managed security provider will offer business remuneration, covering for business losses associated with a security breach (loss of income, reputation damage, organisation downtime)	42%	28%	47%	47%	39%	47%	47%	39%
My organisation's primary IT security vendor/managed security provider will cover legal costs of recriminating lawsuits or legal proceedings (civil and criminal) and also in the case of extortion due to ransomware breaches	19%	10%	25%	17%	17%	25%	17%	17%
My organisation's primary IT security vendor/managed security provider offers no cyber guarantee should their security fail and my organisation fall victim to a cyber-attack as a result	10%	23%	7%	6%	8%	7%	6%	8%
Don't know	7%	20%	4%	5%	1%	4%	5%	1%

When thinking about your organization's primary IT security vendor/managed security provider, do they offer a cyber guarantee should their security fail and your organization fall victim to a successful cyber-attack?

SentinelOne

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
My organisation's primary IT security vendor/managed security provider will cover the cost of detecting the source of the breach, and liaising with law enforcement agencies or third party security agencies to track down the responsible party	47%	44%	73%	39%	64%	42%	41%	31%	50%	51%
My organisation's primary IT security vendor/primary security provider will ensure that the relevant parties of the breach are notified and ensure that we are compliant with the laws of the relevant countries regarding data protection	46%	38%	47%	51%	51%	49%	41%	32%	44%	56%
My organisation's primary IT security vendor/managed security provider will offer business remuneration, covering for business losses associated with a security breach (loss of income, reputation damage, organisation downtime)	42%	40%	63%	42%	55%	48%	24%	35%	33%	32%
My organisation's primary IT security vendor/managed security provider will cover legal costs of recriminating lawsuits or legal proceedings (civil and criminal) and also in the case of extortion due to ransomware breaches	19%	16%	33%	19%	25%	13%	6%	21%	16%	16%
My organisation's primary IT security vendor/managed security provider offers no cyber guarantee should their security fail and my organisation fall victim to a cyber-attack as a result	10%	9%	7%	12%	1%	12%	6%	18%	13%	10%
Don't know	7%	11%	3%	3%	6%	6%	18%	6%	4%	10%

Why do you think IT security vendors/managed security providers should offer a guarantee to their clients on the competence of their products? **SentinelOne**

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
If they are confident their product works, then they should guarantee it	59%	72%	59%	54%	53%	64%	54%	58%
If the product has a fault the vendor should be responsible	50%	51%	49%	54%	45%	50%	52%	46%
The cost of failure is too high for only the vendor's clients to shoulder the burden	43%	35%	45%	40%	47%	44%	40%	44%
I would expect a guarantee for other products that I buy (new car, TV etc.) so why not this	42%	40%	45%	31%	49%	40%	49%	38%
They owe a duty of care to their customers	38%	39%	40%	33%	39%	33%	42%	41%
It will force vendors to adapt to protect against emerging threats	29%	29%	34%	19%	27%	26%	27%	35%
It is not the client's fault the security failed	27%	27%	26%	28%	29%	24%	27%	32%
Vendors can no longer completely protect my organisation from attackers so it is right that they offer a fall back	9%	4%	11%	3%	13%	7%	8%	12%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%

Why do you think IT security vendors/managed security providers should offer a guarantee to their clients on the competence of their products? **SentinelOne**

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
If they are confident their product works, then they should guarantee it	59%	75%	40%	63%	78%	61%	43%	46%	53%	47%
If the product has a fault the vendor should be responsible	50%	47%	53%	53%	48%	48%	57%	46%	48%	53%
The cost of failure is too high for only the vendor's clients to shoulder the burden	43%	32%	57%	40%	42%	26%	43%	46%	56%	48%
I would expect a guarantee for other products that I buy (new car, TV etc.) so why not this	42%	40%	43%	44%	35%	52%	36%	37%	42%	47%
They owe a duty of care to their customers	38%	30%	20%	44%	42%	41%	36%	38%	44%	36%
It will force vendors to adapt to protect against emerging threats	29%	21%	17%	33%	25%	33%	21%	31%	39%	28%
It is not the client's fault the security failed	27%	28%	27%	26%	32%	23%	7%	23%	35%	28%
Vendors can no longer completely protect my organisation from attackers so it is right that they offer a fall back	9%	13%	7%	7%	6%	10%	0%	8%	13%	7%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

Why do you think IT security vendors/managed security providers do not need to offer a guarantee to their clients on the competence of their products?

SentinelOne

	Total	UK	US	France	Germany	1k -3k employees	3k-5k employees	5k employees
They cannot be held responsible for every successful cyber-attack	53%	56%	67%	33%	50%	33%	64%	57%
IT security vendors would likely increase their prices to cover the cost of a guarantee	53%	50%	67%	50%	50%	78%	55%	36%
The breach could be caused by client's failings, not the security vendor's	53%	61%	33%	50%	50%	78%	45%	43%
Cyber-attacks are evolving too quickly for IT security vendors to be expected to keep up	38%	33%	50%	33%	50%	33%	45%	36%
I would prefer for IT security vendors to concentrate on preventing an attack	29%	39%	17%	17%	25%	56%	27%	14%
It is just a marketing ploy and adds no real value	9%	11%	0%	17%	0%	0%	18%	7%
My IT security vendor's products speak for themselves and we do not require a fall back guarantee	6%	6%	0%	17%	0%	0%	9%	7%
Other (please specify)	3%	6%	0%	0%	0%	0%	9%	0%

Why do you think IT security vendors/managed security providers do not need to offer a guarantee to their clients on the competence of their products?

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
They cannot be held responsible for every successful cyber-attack	53%	100%	-	50%	100%	67%	100%	63%	29%	0%
IT security vendors would likely increase their prices to cover the cost of a guarantee	53%	100%	-	63%	0%	67%	67%	63%	0%	100%
The breach could be caused by client's failings, not the security vendor's	53%	100%	-	50%	0%	33%	33%	63%	71%	33%
Cyber-attacks are evolving too quickly for IT security vendors to be expected to keep up	38%	0%	-	38%	0%	33%	67%	50%	43%	0%
I would prefer for IT security vendors to concentrate on preventing an attack	29%	0%	-	38%	0%	33%	33%	50%	0%	33%
It is just a marketing ploy and adds no real value	9%	0%	-	13%	0%	0%	33%	13%	0%	0%
My IT security vendor's products speak for themselves and we do not require a fall back guarantee	6%	0%	-	0%	0%	33%	0%	0%	14%	0%
Other (please specify)	3%	0%	-	0%	0%	0%	0%	13%	0%	0+L47

How many employees does your organization have globally?

SentinelOne

	Total	UK	US	France	Germany
1,001-3,000 employees	38%	45%	38%	28%	41%
3,001-5,000 employees	31%	28%	31%	40%	28%
More than 5,000 employees	31%	27%	32%	32%	31%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
1,001-3,000 employees	38%	40%	53%	29%	42%	42%	24%	39%	33%	40%
3,001-5,000 employees	31%	36%	43%	32%	33%	27%	29%	24%	33%	30%
More than 5,000 employees	31%	24%	3%	39%	25%	31%	47%	37%	34%	30%

Within which sector is your organization?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Retail, distribution and transport	14%	14%	12%	18%	14%	12%	15%	16%
Financial services	14%	14%	13%	17%	13%	11%	14%	18%
IT, technology and telecoms	13%	10%	14%	20%	10%	15%	14%	11%
Manufacturing and production	13%	15%	12%	13%	15%	15%	11%	14%
Public sector	12%	10%	12%	13%	15%	13%	10%	15%
Business and professional services	11%	19%	9%	5%	14%	12%	13%	8%
Construction and property	6%	5%	11%	0%	3%	8%	8%	1%
Media, leisure and entertainment	3%	6%	4%	4%	0%	2%	3%	5%
*Other commercial sectors	13%	7%	15%	10%	16%	13%	12%	12%

In which one of these functional areas are you primarily employed within your organization?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Information technology	99%	100%	99%	98%	100%	99%	100%	99%
Risk/fraud/compliance/governance	1%	0%	1%	2%	0%	1%	0%	1%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
Information technology	99%	98%	100%	99%	100%	100%	100%	98%	100%	98%
Risk/fraud/compliance/governance	1%	2%	0%	1%	0%	0%	0%	2%	0%	2%

What is your level of involvement in IT security within your organization?

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
I work exclusively in IT security	41%	20%	42%	47%	57%	38%	46%	41%
The majority of my work involves IT security	33%	25%	39%	30%	33%	36%	32%	29%
Some of my work involves IT security but I have other responsibilities	26%	55%	20%	23%	10%	25%	22%	30%

	Total	Business and professional services	Construction and property	Financial services	IT, technology and telecoms	Manufacturing and production	Media, leisure and entertainment	Public sector	Retail, distribution and transport	Other commercial sectors
I work exclusively in IT security	41%	44%	70%	32%	48%	39%	29%	32%	41%	44%
The majority of my work involves IT security	33%	31%	23%	43%	40%	30%	18%	24%	31%	38%
Some of my work involves IT security but I have other responsibilities	26%	25%	7%	25%	12%	31%	53%	44%	27%	17%

SentinelOne