SentinelOne

RANSOMWARE RESEARCH DATA SUMMARY

Ransomware Attacks

SentinelOne

Almost half (48%) of those surveyed state that their organization has suffered a ransomware attack in the last 12 months. Those who have been affected have had to defend against six attacks on average, 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%).

Just under two thirds (65%) of respondents agree that traditional cyber security techniques cannot protect them from the next generation of malware like ransomware attacks. While it is under four in ten (36%) respondents who agree that their organization feels helpless to defend itself, over seven in ten (71%) agree that they need a new solution to protect organizations from ransomware.

Of those respondents whose organization has suffered a ransomware attack in the last 12 months, just over eight in ten (81%) report that the ransomware attacker gained access to their organization's network through phishing via email or social media network. Half (50%) report that the attacker gained access through a drive-by-download caused by clicking on a compromised website, and four in ten (40%) state that it was through an infection via a computer that was part of a botnet.

Fewer than half (45%) of respondents whose organization has suffered a ransomware attack in the last 12 months report that the attacker was able to encrypt some files/data, but their organization was able to decrypt them. Moreover, around a quarter state that the attacker was unable to successfully encrypt any files/data (27%), or that the attacker was able to encrypt some files/data, but a back-up was held and respondents' organizations were able to replace the encrypted files (25%). On average, this replacement process took 33 employee hours. Only a minority of respondents (3%) report that the attacker was able to encrypt some files/data, which their organization was unable to decrypt.

Ransomware Attacks

SentinelOne

Of the respondents whose organization has suffered a ransomware attack in the last 12 months, employee information (42%), financial data (41%) and customer information (40%) were types of data most likely to have been affected by these attacks.

Just over six in ten (61%) respondents state that upon suffering a ransomware attack, they did or would notify the CEO/board. Around half of respondents did/would notify law enforcement (54%) and lawyers (50%), but only 38% did/would notify customers.

Just under half (48%) of those surveyed whose organization has suffered a ransomware attack in the last 12 months, report that the ransomware attacker was an opportunistic hacker and a similar number (45%) state that it was an organised cyber-criminal. In fact, over eight in ten (85%) report that their organization was able to identify the ransomware attacker. Similarly, the majority (95%) say that they have an insight into the motivation of the cyber-attackers targeting their organization. The most common motives are financial gain (54%), simple disruption to a successful business (47%) and cyber espionage (42%). Of those respondents whose organization has been able to identify the ransomware attacker, 47% report that the source of the breach was Eastern Europe and 45% state that it was within their own country.

Antivirus

Over five in ten (54%) of those surveyed agree that their organization has lost faith in traditional cyber security and over four in ten (44%) also agree that antivirus is dead. Despite this, the majority (85%) of respondents' organizations install antivirus on all company owned static devices.

Data Summary – October 14th, 2016

SentinelOne

1	Has your organisation suffered a ransomware attack in the last 12 months?
2	How did the ransomware attacker gain access to your organisation's network?
3	In the past 12 months, how many ransomware attacks has your organisation had to defend against?
4	How far did the most successful ransomware attack get when targeting your organisation's data?
5	Please estimate the number of employee hours dedicated to replacing encrypted data with back-up data.
6	Considering all the ransomware attacks your organisation has experienced in the last 12 months, has your organisation paid the ransom demanded by ransomware attackers?
7	What was the total value of the ransoms paid by your organisation?
8	What was the value of the largest ransom your organisation has paid?
9	What results have your organisation experienced from paying the ransom ?
10	What has been the impact of ransomware attacks on your organisation in the past 12 months?
11	What type of data has been affected by ransomware attackers in the past 12 months in your organisation?
12	Upon suffering a ransomware attack, which of the following did/would your IT security department do?
13	Has your organisation been able to identify the attacker in any of the ransomware attacks on your organisation, and if so who was the attacker?
14	What do you believe to be the main motive for cyber-attackers when using ransomware against your organisation?
15	Was your organisation able to locate the source of the breach (the location of the attacker/s)?
16a	To what extent do you agree with the following statements? Country
16b	To what extent do you agree with the following statements? Size
16c	To what extent do you agree with the following statements? Sector
	Demographics
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 organisation?

Has your organization suffered a ransomware attack in the last 12 months?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Yes	48%	39%	50%	52%	51%	45%	52%	49%
No	49%	55%	48%	46%	49%	53%	47%	47%
Don't know	2%	6%	2%	2%	0%	3%	1%	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	48%	51%	57%	45%	52%	49%	24%	42%	47%	56%
No	49%	47%	43%	49%	46%	48%	76%	56%	53%	40%
Don't know	2%	2%	0%	6%	1%	3%	0%	2%	0%	5%

How did the ransomware attacker gain access to your organization's network?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Phishing via email or social media network	81%	72%	83%	69%	94%	80%	79%	83%
Drive-by-download caused by clicking on a compromised website	50%	38%	59%	35%	57%	48%	56%	45%
Infection via a computer that was part of a botnet	40%	18%	47%	46%	37%	39%	41%	40%
*Other (please specify)	0%	0%	0%	2%	0%	1%	0%	0%
Don't know	1%	3%	0%	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
Phishing via email or social media network	81%	79%	94%	84%	74%	64%	100%	81%	82%	91%
Drive-by-download caused by clicking on a compromised website	50%	46%	88%	39%	60%	58%	25%	35%	48%	43%
Infection via a computer that was part of a botnet	40%	32%	53%	32%	63%	30%	50%	27%	39%	43%
*Other (please specify)	0%	0%	0%	3%	0%	0%	0%	0%	0%	0%
Don't know	1%	0%	0%	0%	0%	3%	0%	4%	0%	0%

In the past 12 months, how many ransomware attacks has your organization had to defend against?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
1-2 attacks	19%	36%	15%	29%	2%	22%	18%	15%
3-4 attacks	26%	23%	27%	31%	22%	26%	28%	24%
5-6 attacks	22%	8%	19%	23%	37%	12%	23%	32%
7-8 attacks	12%	3%	12%	10%	24%	19%	10%	8%
9-10 attacks	12%	21%	15%	4%	6%	14%	13%	7%
11-15 attacks	6%	3%	9%	0%	8%	6%	6%	5%
15-20 attacks	2%	0%	3%	4%	2%	0%	1%	7%
More than 20 attacks	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	1%	8%	0%	0%	0%	1%	0%	3%
Average number of ransomware attacks that respondents' organizations have had to defend against in the past 12 months	6	5	6	5	7	5	6	6

In the past 12 months, how many ransomware attacks has your organization had to defend against?

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
1-2 attacks	19%	18%	0%	19%	23%	21%	25%	23%	18%	17%
3-4 attacks	26%	29%	12%	42%	20%	33%	50%	27%	15%	23%
5-6 attacks	22%	39%	6%	26%	26%	18%	25%	15%	18%	20%
7-8 attacks	12%	0%	12%	10%	14%	3%	0%	23%	15%	23%
9-10 attacks	12%	7%	59%	3%	6%	15%	0%	4%	12%	9%
11-15 attacks	6%	0%	12%	0%	6%	6%	0%	4%	12%	9%
15-20 attacks	2%	4%	0%	0%	6%	0%	0%	0%	9%	0%
More than 20 attacks	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Don’t know	1%	4%	0%	0%	0%	3%	0%	4%	0%	0%
Average number of ransomware attacks that respondents' organizations have had to defend against in the past 12 months	6	5	9	4	6	5	4	5	7	6

How far did the most successful ransomware attack get when targeting your organization's data?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
The attacker was able to encrypt some files/data, but we were able to decrypt them ourselves	45%	44%	46%	52%	35%	48%	41%	44%
The attacker was unable to successfully encrypt any files/data	27%	8%	36%	19%	31%	22%	32%	27%
The attacker was able to encrypt some files/data, but we had a back-up and were able to replace the encrypted files	25%	46%	14%	27%	27%	29%	23%	21%
The attacker was able to encrypt some files/data, which we were unable to decrypt	3%	0%	4%	2%	6%	0%	4%	7%
Don't know	0%	3%	0%	0%	0%	0%	0%	1%

How far did the most successful ransomware attack get when targeting your organization's data?

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 attacker was able to encrypt some files/data, but we were able to decrypt them ourselves	45%	57%	12%	48%	31%	55%	75%	23%	67%	43%
The attacker was unable to successfully encrypt any files/data	27%	25%	76%	26%	43%	18%	0%	23%	6%	23%
The attacker was able to encrypt some files/data, but we had a back-up and were able to replace the encrypted files	25%	14%	6%	26%	17%	24%	25%	50%	21%	34%
The attacker was able to encrypt some files/data, which we were unable to decrypt	3%	0%	6%	0%	9%	3%	0%	4%	6%	0%
Don't know	0%	4%	0%	0%	0%	0%	0%	0%	0%	0%

Please estimate the number of employee hours dedicated to replacing encrypted data with back-up data.

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
*Less than 8 employee hours	10%	11%	7%	21%	0%	12%	5%	13%
8-16 employee hours	18%	33%	14%	21%	0%	12%	26%	19%
16-24 employee hours	20%	39%	7%	7%	21%	20%	21%	19%
24-32 employee hours	8%	11%	14%	0%	7%	12%	0%	13%
32-40 employee hours	7%	0%	14%	0%	14%	12%	0%	6%
40-48 employee hours	23%	0%	21%	36%	43%	28%	32%	6%
48-56 employee hours	3%	0%	0%	7%	7%	0%	5%	6%
56-64 employee hours	5%	0%	14%	0%	7%	4%	5%	6%
64-72 employee hours	0%	0%	0%	0%	0%	0%	0%	0%
72-80 employee hours	5%	6%	7%	7%	0%	0%	5%	13%
More than 80 employee hours	0%	0%	0%	0%	0%	0%	0%	0%
Average number of employee hours dedicated to replacing encrypted data with back-up data	33	22	38	37	38	32	33	35

Please estimate the number of employee hours dedicated to replacing encrypted data with back-up data.

SentinelOne

	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
*Less than 8 employee hours	0%	0%	38%	0%	13%	0%	8%	0%	8%
8-16 employee hours	0%	0%	13%	17%	25%	100%	31%	29%	0%
16-24 employee hours	25%	0%	0%	17%	38%	0%	31%	0%	25%
24-32 employee hours	0%	0%	13%	17%	13%	0%	8%	0%	8%
32-40 employee hours	25%	0%	0%	0%	0%	0%	8%	14%	8%
40-48 employee hours	0%	100%	25%	33%	13%	0%	8%	29%	42%
48-56 employee hours	0%	0%	0%	0%	0%	0%	8%	14%	0%
56-64 employee hours	25%	0%	0%	17%	0%	0%	0%	0%	8%
64-72 employee hours	0%	0%	0%	0%	0%	0%	0%	0%	0%
72-80 employee hours	25%	0%	13%	0%	0%	0%	0%	14%	0%
More than 80 employee hours	0%	0%	0%	0%	0%	0%	0%	0%	0%
Average number of employee hours dedicated to replacing encrypted data with back-up data	48	44	41	35	22	12	24	39	37

What has been the impact of ransomware attacks on your organization in the past 12 months?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Increased spending on IT security	67%	54%	70%	63%	76%	62%	63%	77%
Change of IT security strategy, to focus on mitigation	52%	31%	65%	56%	39%	53%	55%	48%
Loss of confidence in existing cybersecurity solutions	45%	54%	35%	44%	57%	51%	41%	41%
Damage to company reputation	37%	33%	41%	23%	47%	35%	43%	33%
Senior IT staff (CIO, CISO) lost their jobs	22%	10%	30%	13%	25%	15%	24%	28%
Negative press/bad publicity	22%	13%	20%	33%	22%	15%	28%	23%
My organization invested in cyber insurance	15%	8%	22%	12%	12%	14%	18%	13%
*Other (please specify)	1%	3%	0%	4%	0%	1%	1%	1%
There was no impact on my organization because of ransomware attacks in the past 12 months	6%	15%	5%	8%	0%	6%	5%	8%

What has been the impact of ransomware attacks on your organization in the past 12 months?

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
Increased spending on IT security	67%	68%	59%	65%	74%	64%	75%	50%	73%	77%
Change of IT security strategy, to focus on mitigation	52%	46%	65%	39%	60%	61%	25%	42%	48%	60%
Loss of confidence in existing cybersecurity solutions	45%	39%	41%	55%	37%	42%	0%	46%	52%	49%
Damage to company reputation	37%	39%	76%	35%	43%	18%	75%	42%	36%	23%
Senior IT staff (CIO, CISO) lost their jobs	22%	14%	47%	16%	31%	9%	25%	31%	24%	17%
Negative press/bad publicity	22%	18%	18%	23%	34%	24%	25%	15%	18%	20%
My organization invested in cyber insurance	15%	14%	12%	16%	23%	15%	0%	12%	15%	14%
*Other (please specify)	1%	0%	0%	0%	3%	0%	0%	4%	0%	3%
There was no impact on my organization because of ransomware attacks in the past 12 months	6%	4%	6%	10%	0%	6%	0%	12%	12%	3%

What type of data has been affected by ransomware attackers in the past 12 months in your organization?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Employee information	42%	26%	46%	31%	57%	49%	40%	35%
Financial data	41%	15%	52%	38%	43%	38%	46%	40%
Customer information	40%	31%	37%	42%	51%	45%	39%	36%
Product information	34%	23%	35%	35%	41%	36%	39%	27%
Payroll/HR	28%	21%	25%	33%	35%	28%	26%	31%
Research and design	24%	15%	22%	35%	25%	13%	33%	28%
Company IP	19%	10%	18%	21%	25%	15%	20%	23%
The attack appeared to be random	12%	31%	7%	13%	4%	13%	11%	11%
All data was targeted	7%	8%	13%	4%	0%	6%	4%	13%
Don't know	0%	3%	0%	0%	0%	1%	0%	0%

What type of data has been affected by ransomware attackers in the past 12 months in your organization?

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
Employee information	42%	39%	88%	35%	49%	15%	25%	31%	52%	46%
Financial data	41%	46%	65%	35%	46%	33%	0%	27%	36%	54%
Customer information	40%	43%	24%	35%	37%	30%	25%	46%	48%	51%
Product information	34%	18%	41%	23%	43%	45%	0%	31%	42%	34%
Payroll/HR	28%	39%	47%	26%	31%	21%	25%	19%	30%	20%
Research and design	24%	32%	41%	13%	29%	30%	0%	31%	15%	17%
Company IP	19%	14%	12%	16%	17%	21%	25%	23%	27%	17%
The attack appeared to be random	12%	7%	6%	10%	3%	18%	25%	27%	9%	11%
All data was targeted	7%	4%	0%	13%	14%	9%	25%	4%	6%	3%
Don't know	0%	4%	0%	0%	0%	0%	0%	0%	0%	0%

Upon suffering a ransomware attack, which of the following did/would your IT security department do?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Notify the CEO/board	61%	69%	68%	46%	56%	65%	64%	55%
Inform law enforcement	54%	50%	57%	49%	59%	54%	54%	55%
Notify our lawyers	50%	46%	60%	40%	43%	48%	43%	58%
Notifying data protection regulators	48%	35%	49%	52%	53%	46%	51%	46%
Attempt to decrypt the files ourselves	42%	36%	45%	45%	38%	45%	38%	41%
Notify customers	38%	27%	39%	39%	47%	43%	39%	31%
Demand answers from IT security vendor	38%	30%	42%	39%	39%	38%	39%	38%
Contact our cyber insurance provider	23%	13%	32%	20%	17%	25%	20%	22%
Change IT security vendor	18%	10%	22%	18%	17%	13%	21%	20%
*Other	1%	2%	0%	1%	0%	1%	1%	1%
None of the above	3%	5%	3%	3%	0%	4%	1%	3%

Upon suffering a ransomware attack, which of the following did/would your IT security department do?

SentinelOne

	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
Notify the CEO/board	64%	53%	55%	67%	67%	59%	65%	61%	56%
Inform law enforcement	51%	53%	57%	58%	52%	53%	58%	54%	49%
Notify our lawyers	60%	43%	51%	34%	52%	71%	55%	51%	43%
Notifying data protection regulators	49%	60%	46%	55%	40%	47%	50%	46%	41%
Attempt to decrypt the files ourselves	51%	47%	42%	43%	36%	41%	31%	46%	41%
Notify customers	35%	30%	26%	39%	45%	29%	39%	39%	52%
Demand answers from IT security vendor	35%	43%	41%	45%	37%	35%	37%	40%	30%
Contact our cyber insurance provider	24%	27%	23%	24%	28%	35%	23%	19%	14%
Change IT security vendor	15%	30%	12%	25%	22%	6%	18%	19%	10%
*Other	0%	0%	1%	0%	1%	0%	0%	0%	2%
None of the above	0%	7%	3%	3%	3%	0%	3%	3%	2%

Has your organization been able to identify the attacker in any of the ransomware attacks on your organization, and if so who was the attacker?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Opportunistic hackers (non-organised)	48%	41%	46%	50%	53%	49%	45%	48%
Organised cyber-criminals	45%	23%	48%	37%	67%	40%	49%	48%
Anti-capitalist protesters	31%	18%	33%	38%	27%	24%	33%	36%
Political hacktivists	24%	15%	23%	21%	37%	24%	28%	21%
Disgruntled employees/former employees	24%	15%	23%	27%	29%	12%	34%	27%
Rival organizations	19%	3%	26%	15%	22%	14%	17%	27%
Dissatisfied customers	18%	10%	20%	19%	20%	13%	22%	20%
State sponsored hackers	6%	0%	11%	2%	4%	2%	10%	5%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
My organization has not been able to determine the identity of the attacker in any of the ransomware attacks we have suffered	15%	38%	15%	12%	0%	19%	12%	13%

Has your organization been able to identify the attacker in any of the ransomware attacks on your organization, and if so who was the attacker?

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
Opportunistic hackers (non-organised)	48%	50%	65%	42%	51%	39%	25%	31%	64%	46%
Organised cyber-criminals	45%	36%	82%	32%	57%	33%	0%	35%	48%	57%
Anti-capitalist protesters	31%	36%	47%	42%	26%	27%	25%	23%	30%	23%
Political hacktivists	24%	21%	35%	26%	37%	21%	25%	15%	30%	11%
Disgruntled employees/former employees	24%	25%	41%	16%	37%	24%	0%	31%	15%	14%
Rival organizations	19%	18%	12%	16%	37%	24%	0%	15%	18%	9%
Dissatisfied customers	18%	11%	29%	16%	31%	15%	0%	12%	21%	14%
State sponsored hackers	6%	4%	12%	6%	9%	9%	0%	8%	3%	0%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
My organization has not been able to determine the identity of the attacker in any of the ransomware attacks we have suffered	15%	7%	6%	13%	6%	21%	25%	27%	15%	20%

What do you believe to be the main motive for cyber-attackers when using ransomware against your organization?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Financial gain	54%	64%	60%	44%	43%	54%	54%	53%
Simple disruption to a successful business	47%	33%	53%	38%	53%	44%	54%	43%
Cyber espionage	42%	21%	39%	56%	51%	38%	46%	43%
Political motivation	30%	8%	27%	33%	49%	28%	27%	35%
'Revenge' for a bad experience with my organization	27%	8%	27%	37%	33%	21%	33%	28%
State sponsored international attack	20%	5%	23%	17%	29%	11%	29%	21%
Entertainment (hacking just for fun)	16%	13%	21%	12%	14%	12%	17%	20%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%
We have no insight into the motivation of the cyber-attackers targeting my organization	5%	13%	6%	4%	0%	11%	1%	4%

What do you believe to be the main motive for cyber-attackers when using ransomware against your organization?

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
Opportunistic hackers (non-organised)	48%	50%	65%	42%	51%	39%	25%	31%	64%	46%
Organised cyber-criminals	45%	36%	82%	32%	57%	33%	0%	35%	48%	57%
Anti-capitalist protesters	31%	36%	47%	42%	26%	27%	25%	23%	30%	23%
Political hacktivists	24%	21%	35%	26%	37%	21%	25%	15%	30%	11%
Disgruntled employees/former employees	24%	25%	41%	16%	37%	24%	0%	31%	15%	14%
Rival organizations	19%	18%	12%	16%	37%	24%	0%	15%	18%	9%
Dissatisfied customers	18%	11%	29%	16%	31%	15%	0%	12%	21%	14%
State sponsored hackers	6%	4%	12%	6%	9%	9%	0%	8%	3%	0%
Other (please specify)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
My organization has not been able to determine the identity of the attacker in any of the ransomware attacks we have suffered	15%	7%	6%	13%	6%	21%	25%	27%	15%	20%

Was your organization able to locate the source of the breach (the location of the attacker/s)?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employees	3k-5k employees	5k+ employees
Eastern Europe	47%	54%	35%	48%	61%	52%	44%	43%
Within my own country	45%	21%	66%	33%	31%	45%	49%	40%
Western Europe	34%	21%	25%	30%	59%	35%	32%	35%
North America	19%	8%	32%	11%	12%	12%	22%	25%
Middle East	19%	8%	8%	33%	29%	13%	19%	25%
Far East	17%	29%	9%	20%	20%	12%	19%	18%
Africa	13%	13%	5%	22%	18%	7%	14%	17%
South America	4%	0%	9%	2%	0%	3%	6%	5%
My organization was unable to determine the source location of the breach	4%	8%	2%	7%	2%	3%	3%	6%

Was your organization able to locate the source of the breach (the location of the attacker/s)?

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
Eastern Europe	47%	31%	75%	37%	39%	50%	33%	47%	50%	57%
Within my own country	45%	35%	75%	33%	64%	42%	33%	37%	43%	36%
Western Europe	34%	46%	50%	30%	18%	27%	0%	32%	43%	39%
North America	19%	23%	38%	11%	21%	15%	0%	11%	25%	18%
Middle East	19%	23%	13%	22%	3%	38%	33%	21%	25%	7%
Far East	17%	12%	13%	26%	12%	19%	0%	32%	18%	7%
Africa	13%	19%	6%	15%	12%	12%	33%	5%	14%	11%
South America	4%	0%	25%	4%	6%	4%	0%	0%	4%	0%
My organization was unable to determine the source location of the breach	4%	0%	0%	4%	3%	4%	0%	16%	4%	4%

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

SentinelOne

Total

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	19%	35%	19%	18%	9%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	28%	37%	20%	12%	3%
My organization feels helpless to defend itself from new forms of ransomware	13%	23%	25%	27%	12%
We need a new solution to protect organizations from ransomware	30%	41%	20%	7%	2%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	19%	30%	22%	18%	10%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	14%	38%	32%	11%	5%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	15%	29%	24%	23%	9%

United Kingdom

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	10%	37%	22%	23%	8%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	19%	44%	26%	11%	0%
My organization feels helpless to defend itself from new forms of ransomware	5%	19%	31%	36%	9%
We need a new solution to protect organizations from ransomware	25%	38%	25%	12%	0%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	10%	33%	30%	18%	9%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	8%	35%	35%	16%	6%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	7%	25%	27%	34%	7%

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

SentinelOne

United States

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	23%	29%	20%	16%	13%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	31%	37%	16%	11%	6%
My organization feels helpless to defend itself from new forms of ransomware	15%	23%	19%	28%	16%
We need a new solution to protect organizations from ransomware	35%	42%	13%	7%	4%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	24%	26%	20%	19%	13%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	23%	37%	29%	6%	6%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	15%	32%	22%	20%	12%

France

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	21%	40%	15%	17%	7%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	25%	38%	18%	17%	2%
My organization feels helpless to defend itself from new forms of ransomware	16%	29%	22%	26%	7%
We need a new solution to protect organizations from ransomware	34%	39%	18%	5%	4%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	22%	38%	18%	14%	8%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	13%	35%	32%	13%	6%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	21%	31%	23%	15%	10%

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

SentinelOne

Germany

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	17%	43%	16%	20%	4%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	33%	28%	25%	13%	1%
My organization feels helpless to defend itself from new forms of ransomware	13%	21%	34%	19%	13%
We need a new solution to protect organizations from ransomware	21%	43%	29%	6%	1%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	18%	26%	25%	23%	8%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	17%	48%	30%	4%	0%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	19%	24%	24%	28%	5%

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

SentinelOne

Total

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	19%	35%	19%	18%	9%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	28%	37%	20%	12%	3%
My organization feels helpless to defend itself from new forms of ransomware	13%	23%	25%	27%	12%
We need a new solution to protect organizations from ransomware	30%	41%	20%	7%	2%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	19%	30%	22%	18%	10%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	14%	38%	32%	11%	5%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	15%	29%	24%	23%	9%

1,001-3,000 Employees

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	18%	38%	21%	16%	6%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	29%	38%	18%	14%	2%
My organization feels helpless to defend itself from new forms of ransomware	9%	25%	29%	26%	11%
We need a new solution to protect organizations from ransomware	31%	37%	23%	7%	3%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	20%	33%	23%	16%	8%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	10%	47%	34%	8%	2%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	13%	30%	24%	27%	7%

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

SentinelOne

3,001-5,000 Employees

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	23%	29%	20%	16%	13%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	31%	37%	16%	11%	6%
My organization feels helpless to defend itself from new forms of ransomware	15%	23%	19%	28%	16%
We need a new solution to protect organizations from ransomware	35%	42%	13%	7%	4%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	24%	26%	20%	19%	13%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	23%	37%	29%	6%	6%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	15%	32%	22%	20%	12%

5,000+ Employees

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	21%	40%	15%	17%	7%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	25%	38%	18%	17%	2%
My organization feels helpless to defend itself from new forms of ransomware	16%	29%	22%	26%	7%
We need a new solution to protect organizations from ransomware	34%	39%	18%	5%	4%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	22%	38%	18%	14%	8%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	13%	35%	32%	13%	6%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	21%	31%	23%	15%	10%

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

SentinelOne

Total

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	19%	35%	19%	18%	9%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	28%	37%	20%	12%	3%
My organization feels helpless to defend itself from new forms of ransomware	13%	23%	25%	27%	12%
We need a new solution to protect organizations from ransomware	30%	41%	20%	7%	2%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	19%	30%	22%	18%	10%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	14%	38%	32%	11%	5%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	15%	29%	24%	23%	9%

Business & Professional Services

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	7%	47%	20%	20%	5%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	16%	45%	24%	13%	2%
My organization feels helpless to defend itself from new forms of ransomware	11%	18%	31%	29%	11%
We need a new solution to protect organizations from ransomware	31%	42%	18%	4%	5%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	11%	25%	31%	24%	9%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	0%	60%	33%	0%	7%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	15%	31%	20%	27%	7%

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

SentinelOne

Financial Services

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	20%	28%	25%	17%	10%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	25%	38%	22%	13%	3%
My organization feels helpless to defend itself from new forms of ransomware	13%	23%	23%	30%	10%
We need a new solution to protect organizations from ransomware	22%	39%	32%	4%	3%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	17%	29%	26%	20%	7%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	15%	20%	45%	15%	5%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	12%	30%	26%	26%	6%

Construction & Property

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	33%	33%	3%	27%	3%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	30%	23%	30%	13%	3%
My organization feels helpless to defend itself from new forms of ransomware	23%	37%	3%	27%	10%
We need a new solution to protect organizations from ransomware	20%	40%	30%	7%	3%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	33%	23%	27%	13%	3%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	50%	50%	0%	0%	0%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	30%	23%	23%	17%	7%

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

SentinelOne

IT, Tech & Telecom

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	30%	33%	18%	9%	10%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	31%	36%	13%	16%	3%
My organization feels helpless to defend itself from new forms of ransomware	16%	28%	25%	19%	10%
We need a new solution to protect organizations from ransomware	37%	45%	13%	4%	0%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	24%	40%	18%	12%	6%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	18%	59%	18%	0%	6%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	18%	36%	24%	18%	4%

Manufacturing & Production

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	18%	27%	22%	22%	10%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	28%	42%	16%	7%	6%
My organization feels helpless to defend itself from new forms of ransomware	7%	27%	21%	31%	13%
We need a new solution to protect organizations from ransomware	34%	37%	18%	7%	3%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	27%	30%	15%	15%	13%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	20%	20%	45%	5%	10%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	13%	19%	31%	22%	13%

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

SentinelOne

Media, Leisure & Entertainment

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	18%	24%	24%	18%	18%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	18%	35%	24%	18%	6%
My organization feels helpless to defend itself from new forms of ransomware	6%	18%	12%	47%	18%
We need a new solution to protect organizations from ransomware	18%	29%	29%	18%	6%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	12%	35%	18%	29%	6%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	20%	40%	20%	20%	0%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	18%	29%	12%	18%	24%

Public Sector

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	16%	35%	13%	27%	8%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	35%	31%	21%	13%	0%
My organization feels helpless to defend itself from new forms of ransomware	6%	21%	29%	16%	27%
We need a new solution to protect organizations from ransomware	34%	32%	21%	11%	2%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	21%	21%	18%	27%	13%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	14%	24%	33%	19%	10%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	11%	31%	26%	24%	8%

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

SentinelOne

Retail, Distribution & Transport

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	11%	47%	17%	17%	7%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	24%	41%	23%	11%	0%
My organization feels helpless to defend itself from new forms of ransomware	16%	11%	27%	40%	6%
We need a new solution to protect organizations from ransomware	31%	49%	14%	6%	0%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	14%	30%	21%	20%	14%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	12%	44%	28%	16%	0%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	13%	29%	17%	30%	11%

Other Commercial Sectors

	Completely agree	Somewhat agree	Neither agree or disagree	Somewhat disagree	Completely disagree
My organization has lost faith in traditional cyber security, such as anti-virus	21%	37%	21%	13%	10%
Traditional cyber security techniques cannot protect us from the next generation of malware like ransomware attacks	35%	32%	16%	11%	6%
My organization feels helpless to defend itself from new forms of ransomware	14%	27%	33%	17%	8%
We need a new solution to protect organizations from ransomware	29%	43%	13%	13%	3%
We've accepted that cybercriminals are constantly ahead and we are now focused on mitigation rather than cyber protection	16%	33%	29%	11%	11%
We may look to get cyber insurance now that the possibility of fines is higher with the GDPR	13%	47%	27%	13%	0%
Antivirus is dead – it will soon be useless in the fight against cyber-attacks	19%	29%	24%	19%	10%

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%	14%	12%	15%
Financial services	14%	14%	13%	17%	13%	14%	11%	14%
IT, technology and telecoms	13%	10%	14%	20%	10%	13%	15%	14%
Manufacturing and production	13%	15%	12%	13%	15%	13%	15%	11%
Public sector	12%	10%	12%	13%	15%	12%	13%	10%
Business and professional services	11%	19%	9%	5%	14%	11%	12%	13%
Construction and property	6%	5%	11%	0%	3%	6%	8%	8%
Media, leisure and entertainment	3%	6%	4%	4%	0%	3%	2%	3%
*Other commercial sectors	13%	7%	15%	10%	16%	13%	13%	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?

SentinelOne

	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