

A large, abstract graphic on the left side of the slide, consisting of numerous overlapping, thin, light blue lines that form a circular, textured shape resembling a globe or a complex network. The background is a solid blue gradient, darker on the left and lighter on the right.

SentinelOne

ETUDE SUR LES RANSOMWARE
RÉSUMÉ

Près de la moitié (48 %) des personnes interrogées affirment que leur organisation a subi une attaque par ransomware au cours des 12 derniers mois. Celles qui ont été touchées ont dû se défendre contre six attaques en moyenne et la majorité (94 %) a déclaré que ces attaques par ransomware ont eu des conséquences. Les conséquences les plus courantes sont l'augmentation des dépenses en sécurité informatique (67 %), le changement de la stratégie de sécurité informatique pour se concentrer sur la diminution des impacts d'une attaque (52 %) et la perte de confiance dans les solutions de cybersécurité existantes (45 %).

Un peu moins des deux tiers (65 %) des répondants conviennent que les solutions traditionnelles de cybersécurité ne sont pas en mesure de les protéger contre la prochaine génération de logiciels malveillants tels que les ransomware. Bien que moins de quatre répondants sur dix (36 %) qui conviennent que leur organisation se sent impuissante à se défendre, et plus de sept sur dix (71 %) pensent qu'ils ont besoin d'une nouvelle solution pour protéger leur organisation contre les ransomwares.

Parmi les répondants dont l'organisation a été victime d'une attaque par ransomware au cours des 12 derniers mois, un peu plus de huit sur dix (81 %) affirment que le cybercriminel a accédé au réseau de l'organisation par le biais d'un phishing via un email ou les réseaux sociaux. La moitié (50 %) affirme que le cybercriminel a obtenu l'accès grâce à la technique du drive-by-download causé par un clic sur un site web compromis et quatre personnes sur dix (40 %) déclarent avoir été infectées par un ordinateur faisant partie d'un botnet.

Moins de la moitié (45 %) des répondants dont l'organisation a été touchée par une attaque par ransomware au cours des 12 derniers mois indiquent que le cybercriminel a pu crypter une partie des fichiers/données, mais que leur organisation a été capable de les décrypter. Environ un quart indique que le cybercriminel n'a pas réussi à crypter les fichiers/données (27 %) ou que celui-ci a pu crypter une partie des fichiers/données, mais qu'une sauvegarde était en place et que les organisations ont pu remplacer les fichiers cryptés (25 %). En moyenne, ce processus de remplacement a pris 33 heures "homme". Seule une minorité de répondants (3 %) signale que le cybercriminel a pu crypter des fichiers/données que leur organisation n'a pas pu décrypter.

Parmi les répondants dont l'organisation a été victime d'une attaque par ransomware au cours des 12 derniers mois, les types de données les plus touchées étaient les informations sur les employés (42 %), les données financières (41 %) et les données clients (40 %).

Un peu plus de six répondants sur dix (61 %) déclarent que, lorsqu'ils ont subi une attaque de type ransomware, ils ont/auraient avisé le PDG / le comité de direction. Environ la moitié des répondants a/aurait notifié les autorités (54 %) et la justice (50 %), mais seuls 38 % ont informé/informerait les clients.

Un peu moins de la moitié (48 %) des sondés dont l'organisation a subi une attaque par ransomware dans les 12 derniers mois, rapportent que le cybercriminel était un pirate opportuniste et un nombre similaire (45 %) déclarent qu'il s'agissait d'une organisation criminelle organisée. En fait, plus de huit répondants sur dix (85 %) déclarent que leur organisation a été en mesure d'identifier le cybercriminel. De même, la majorité (95 %) affirme avoir une idée de la motivation des cybercriminels ciblant leur organisation. Les motifs les plus courants sont le gain financier (54 %), la perturbation de l'activité de l'entreprise (47 %) et le cyberespionnage (42 %). Parmi les répondants dont l'organisation a été en mesure d'identifier le cybercriminel à l'origine du ransomware, 47 % déclarent que l'origine de l'attaque provenait de l'Europe de l'Est et 45 % déclarent qu'elle provenait de leur propre pays.

Antivirus

Plus de cinq répondants sur dix (54 %) estiment que leur organisation a perdu confiance dans les technologies de cybersécurité traditionnelles et plus de quatre sur dix (44 %) conviennent également que l'antivirus est dépassé. Malgré cela, la majorité (85 %) des organisations de répondants installent un antivirus sur tous les appareils statiques appartenant à l'entreprise.

1	Votre organisation a-t-elle subi une attaque par ransomware au cours des 12 derniers mois ?
2	Comment le cybercriminel à l'origine du ransomware a-t-il pu accéder au réseau de votre organisation ?
3	Au cours des 12 derniers mois, contre combien d'attaques par ransomware votre organisation a-t-elle dû se défendre ?
4	Quel résultat l'attaque par ransomware la plus réussie a-t-elle obtenu lors du ciblage des données de votre organisation ?
5	Pouvez-vous estimer le nombre d'heures consacrées au remplacement des données cryptées par des données de sauvegarde ?
6	Compte tenu des attaques par ransomware auxquelles votre organisation a dû faire face au cours des 12 derniers mois, celle-ci a-t-elle payé la rançon demandée par les cybercriminels ?
7	Quel a été le montant total des rançons payées par votre organisation ?
8	Quel a été le montant de la rançon la plus importante payée par votre organisation ?
9	Quels résultats a obtenu votre organisation en payant la rançon ?
10	Quel a été l'impact des attaques par ransomware sur votre organisation au cours des 12 derniers mois ?
11	Quel type de données a-t-il été affecté par les attaques par ransomware au cours des 12 derniers mois dans votre organisation ?
12	Après avoir subi une attaque par ransomware, qu'a fait/aurait fait votre département de sécurité informatique parmi les choix suivants ?
13	Votre organisation a-t-elle été en mesure d'identifier le cybercriminel dans l'une des attaques par ransomware qui a ciblé votre organisation et, si oui, qui était t'il ?
14	Quelles sont, selon vous, les principales motivations des cybercriminels lorsqu'ils ont ciblé votre organisation avec une attaque par ransomware ?
15	Votre organisation a-t-elle pu localiser l'origine de la fuite (la localisation du ou des cybercriminels) ?
16a	Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? Pays
16b	Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? Taille
16c	Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? Secteur d'activité
	<u>Données démographiques</u>
D1	Combien d'employés compte votre organisation à l'échelle mondiale ?
D2	Dans quel secteur évolue votre organisation ?
D3	Dans quels domaines fonctionnels êtes-vous principalement employé au sein de votre organisation ?
D4	Quel est votre niveau d'implication dans la sécurité informatique au sein de votre organisation ?

Votre organisation a-t-elle subi une attaque par ransomware au cours des 12 derniers mois ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Oui	48%	39%	50%	52%	51%	45%	52%	49%
Non	49%	55%	48%	46%	49%	53%	47%	47%
Ne sais pas	2%	6%	2%	2%	0%	3%	1%	4%

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Oui	48%	51%	57%	45%	52%	49%	24%	42%	47%	56%
Non	49%	47%	43%	49%	46%	48%	76%	56%	53%	40%
Ne sais pas	2%	2%	0%	6%	1%	3%	0%	2%	0%	5%

Comment le cybercriminel à l'origine du ransomware a-t-il pu accéder au réseau de votre organisation ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Phishing via email ou réseaux sociaux	81%	72%	83%	69%	94%	80%	79%	83%
Drive-by-download résultant du clic sur lien vers un site compromis	50%	38%	59%	35%	57%	48%	56%	45%
Infection par un ordinateur faisant partie d'un botnet	40%	18%	47%	46%	37%	39%	41%	40%
*Autre (merci de préciser)	0%	0%	0%	2%	0%	1%	0%	0%
Ne sais pas	1%	3%	0%	2%	0%	1%	0%	1%

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Phishing via email ou réseaux sociaux	81%	79%	94%	84%	74%	64%	100%	81%	82%	91%
Drive-by-download résultant du clic sur lien vers un site compromis	50%	46%	88%	39%	60%	58%	25%	35%	48%	43%
Infection par un ordinateur faisant partie d'un botnet	40%	32%	53%	32%	63%	30%	50%	27%	39%	43%
*Autre (merci de préciser)	0%	0%	0%	3%	0%	0%	0%	0%	0%	0%
Ne sais pas	1%	0%	0%	0%	0%	3%	0%	4%	0%	0%

Au cours des 12 derniers mois, contre combien d'attaques par ransomware votre organisation a-t-elle dû se défendre ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
1-2 attaques	19%	36%	15%	29%	2%	22%	18%	15%
3-4 attaques	26%	23%	27%	31%	22%	26%	28%	24%
5-6 attaques	22%	8%	19%	23%	37%	12%	23%	32%
7-8 attaques	12%	3%	12%	10%	24%	19%	10%	8%
9-10 attaques	12%	21%	15%	4%	6%	14%	13%	7%
11-15 attaques	6%	3%	9%	0%	8%	6%	6%	5%
15-20 attaques	2%	0%	3%	4%	2%	0%	1%	7%
Plus de 20 attaques (merci de préciser)	0%	0%	0%	0%	0%	0%	0%	0%
Ne sais pas	1%	8%	0%	0%	0%	1%	0%	3%
Nombre moyen d'attaques par ransomware auxquelles les organisations interrogées ont dû se défendre au cours des 12 derniers mois	6	5	6	5	7	5	6	6

Au cours des 12 derniers mois, contre combien d'attaques par ransomware votre organisation a-t-elle dû se défendre ?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
1-2 attaques	19%	18%	0%	19%	23%	21%	25%	23%	18%	17%
3-4 attaques	26%	29%	12%	42%	20%	33%	50%	27%	15%	23%
5-6 attaques	22%	39%	6%	26%	26%	18%	25%	15%	18%	20%
7-8 attaques	12%	0%	12%	10%	14%	3%	0%	23%	15%	23%
9-10 attaques	12%	7%	59%	3%	6%	15%	0%	4%	12%	9%
11-15 attaques	6%	0%	12%	0%	6%	6%	0%	4%	12%	9%
15-20 attaques	2%	4%	0%	0%	6%	0%	0%	0%	9%	0%
Plus de 20 attaques (merci de préciser)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Ne sais pas	1%	4%	0%	0%	0%	3%	0%	4%	0%	0%
Nombre moyen d'attaques par ransomware auxquelles les organisations interrogées ont dû se défendre au cours des 12 derniers mois	6	5	9	4	6	5	4	5	7	6

Quel résultat l'attaque par ransomware la plus réussie a-t-elle obtenu lors du ciblage des données de votre organisation ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Le cybercriminel a pu crypter des fichiers / données, mais nous avons pu les décrypter nous-mêmes	45%	44%	46%	52%	35%	48%	41%	44%
Le cybercriminel n'a pas réussi à crypter de fichiers/données	27%	8%	36%	19%	31%	22%	32%	27%
Le cybercriminel a pu crypter des fichiers/données, mais nous avions une sauvegarde et avons été en mesure de remplacer les fichiers chiffrés	25%	46%	14%	27%	27%	29%	23%	21%
Le cybercriminel a pu crypter des fichiers/données, que nous n'avons pas pu déchiffrer	3%	0%	4%	2%	6%	0%	4%	7%
Ne sais pas	0%	3%	0%	0%	0%	0%	0%	1%

Quel résultat l'attaque par ransomware la plus réussie a-t-elle obtenu lors du ciblage des données de votre organisation ?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Le cybercriminel a pu crypter des fichiers / données, mais nous avons pu les décrypter nous-mêmes	45%	57%	12%	48%	31%	55%	75%	23%	67%	43%
Le cybercriminel n'a pas réussi à crypter de fichiers/données	27%	25%	76%	26%	43%	18%	0%	23%	6%	23%
Le cybercriminel a pu crypter des fichiers/données, mais nous avons une sauvegarde et avons été en mesure de remplacer les fichiers chiffrés	25%	14%	6%	26%	17%	24%	25%	50%	21%	34%
Le cybercriminel a pu crypter des fichiers/données, que nous n'avons pas pu déchiffrer	3%	0%	6%	0%	9%	3%	0%	4%	6%	0%
Ne sais pas	0%	4%	0%	0%	0%	0%	0%	0%	0%	0%

Pouvez-vous estimer le nombre d'heures consacrées au remplacement des données cryptées par des données de sauvegarde ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
*Moins de 8 heures de travail (merci de préciser)	10%	11%	7%	21%	0%	12%	5%	13%
8-16 heures de travail	18%	33%	14%	21%	0%	12%	26%	19%
16-24 heures de travail	20%	39%	7%	7%	21%	20%	21%	19%
24-32 heures de travail	8%	11%	14%	0%	7%	12%	0%	13%
32-40 heures de travail	7%	0%	14%	0%	14%	12%	0%	6%
40-48 heures de travail	23%	0%	21%	36%	43%	28%	32%	6%
48-56 heures de travail	3%	0%	0%	7%	7%	0%	5%	6%
56-64 heures de travail	5%	0%	14%	0%	7%	4%	5%	6%
64-72 heures de travail	0%	0%	0%	0%	0%	0%	0%	0%
72-80 heures de travail	5%	6%	7%	7%	0%	0%	5%	13%
Plus de 80 heures de travail (merci de préciser)	0%	0%	0%	0%	0%	0%	0%	0%
Nombre moyen d'heures de travail consacrées au remplacement des données cryptées par des données de sauvegarde	33	22	38	37	38	32	33	35

Pouvez-vous estimer le nombre d'heures consacrées au remplacement des données cryptées par des données de sauvegarde ?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport
*Moins de 8 heures de travail (merci de préciser)	0%	0%	38%	0%	13%	0%	8%	0%	8%
8-16 heures de travail	0%	0%	13%	17%	25%	100%	31%	29%	0%
16-24 heures de travail	25%	0%	0%	17%	38%	0%	31%	0%	25%
24-32 heures de travail	0%	0%	13%	17%	13%	0%	8%	0%	8%
32-40 heures de travail	25%	0%	0%	0%	0%	0%	8%	14%	8%
40-48 heures de travail	0%	100%	25%	33%	13%	0%	8%	29%	42%
48-56 heures de travail	0%	0%	0%	0%	0%	0%	8%	14%	0%
56-64 heures de travail	25%	0%	0%	17%	0%	0%	0%	0%	8%
64-72 heures de travail	0%	0%	0%	0%	0%	0%	0%	0%	0%
72-80 heures de travail	25%	0%	13%	0%	0%	0%	0%	14%	0%
Plus de 80 heures de travail (merci de préciser)	0%	0%	0%	0%	0%	0%	0%	0%	0%
Nombre moyen d'heures de travail consacrées au remplacement des données cryptées par des données de sauvegarde	48	44	41	35	22	12	24	39	37

Quel a été l'impact des attaques par ransomware sur votre organisation au cours des 12 derniers mois ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Augmentation des dépenses en matière de sécurité informatique	67%	54%	70%	63%	76%	62%	63%	77%
Changement de la stratégie de sécurité informatique pour limiter les impacts d'une attaque	52%	31%	65%	56%	39%	53%	55%	48%
Perte de confiance dans les solutions de cybersécurité existantes	45%	54%	35%	44%	57%	51%	41%	41%
Atteinte à la réputation de l'entreprise	37%	33%	41%	23%	47%	35%	43%	33%
Des cadres du personnel informatique (DSI, RSSI) ont perdu leur emploi	22%	10%	30%	13%	25%	15%	24%	28%
Mauvaise presse/publicité	22%	13%	20%	33%	22%	15%	28%	23%
Mon organisation a investi dans une cyber-assurance	15%	8%	22%	12%	12%	14%	18%	13%
*Autre (merci de préciser)	1%	3%	0%	4%	0%	1%	1%	1%
Il n'y a eu aucun impact sur mon organisation du à des attaques de ransomware au cours des 12 derniers mois	6%	15%	5%	8%	0%	6%	5%	8%

Quel a été l'impact des attaques par ransomware sur votre organisation au cours des 12 derniers mois ?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Augmentation des dépenses en matière de sécurité informatique	67%	68%	59%	65%	74%	64%	75%	50%	73%	77%
Changement de la stratégie de sécurité informatique pour limiter les impacts d'une attaque	52%	46%	65%	39%	60%	61%	25%	42%	48%	60%
Perte de confiance dans les solutions de cybersécurité existantes	45%	39%	41%	55%	37%	42%	0%	46%	52%	49%
Atteinte à la réputation de l'entreprise	37%	39%	76%	35%	43%	18%	75%	42%	36%	23%
Des cadres du personnel informatique (DSI, RSSI) ont perdu leur emploi	22%	14%	47%	16%	31%	9%	25%	31%	24%	17%
Mauvaise presse/publicité	22%	18%	18%	23%	34%	24%	25%	15%	18%	20%
Mon organisation a investi dans une cyber-assurance	15%	14%	12%	16%	23%	15%	0%	12%	15%	14%
*Autre (merci de préciser)	1%	0%	0%	0%	3%	0%	0%	4%	0%	3%
Il n'y a eu aucun impact sur mon organisation du à des attaques de ransomware au cours des 12 derniers mois	6%	4%	6%	10%	0%	6%	0%	12%	12%	3%

Quel type de données a-t-il été affecté par les cybercriminels à l'origine des ransomware au cours des 12 derniers mois dans votre organisation ?

SentinelOne

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Informations employés	42%	26%	46%	31%	57%	49%	40%	35%
Données financières	41%	15%	52%	38%	43%	38%	46%	40%
Données clients	40%	31%	37%	42%	51%	45%	39%	36%
Données produits	34%	23%	35%	35%	41%	36%	39%	27%
Salaires/RH	28%	21%	25%	33%	35%	28%	26%	31%
Recherche et développement	24%	15%	22%	35%	25%	13%	33%	28%
Propriété intellectuelle de l'entreprise	19%	10%	18%	21%	25%	15%	20%	23%
L'attaque semblait aléatoire	12%	31%	7%	13%	4%	13%	11%	11%
Toutes les données étaient ciblées	7%	8%	13%	4%	0%	6%	4%	13%
Ne sais pas	0%	3%	0%	0%	0%	1%	0%	0%

Quel type de données a-t-il été affecté par les cybercriminels à l'origine des ransomware au cours des 12 derniers mois dans votre organisation ?

SentinelOne

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Informations employés	42%	39%	88%	35%	49%	15%	25%	31%	52%	46%
Données financières	41%	46%	65%	35%	46%	33%	0%	27%	36%	54%
Données clients	40%	43%	24%	35%	37%	30%	25%	46%	48%	51%
Données produits	34%	18%	41%	23%	43%	45%	0%	31%	42%	34%
Salaires/RH	28%	39%	47%	26%	31%	21%	25%	19%	30%	20%
Recherche et développement	24%	32%	41%	13%	29%	30%	0%	31%	15%	17%
Propriété intellectuelle de l'entreprise	19%	14%	12%	16%	17%	21%	25%	23%	27%	17%
L'attaque semblait aléatoire	12%	7%	6%	10%	3%	18%	25%	27%	9%	11%
Toutes les données étaient ciblées	7%	4%	0%	13%	14%	9%	25%	4%	6%	3%
Ne sais pas	0%	4%	0%	0%	0%	0%	0%	0%	0%	0%

'Après avoir subi une attaque par ransomware, qu'a fait/aurait fait votre département de sécurité informatique parmi les choix suivants ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Notifier le PDG / Comité de direction	61%	69%	68%	46%	56%	65%	64%	55%
Informers les autorités	54%	50%	57%	49%	59%	54%	54%	55%
Informers nos avocats	50%	46%	60%	40%	43%	48%	43%	58%
Notification des régulateurs de protection des données	48%	35%	49%	52%	53%	46%	51%	46%
Essayer de décrypter les fichiers nous-mêmes	42%	36%	45%	45%	38%	45%	38%	41%
Informers les clients	38%	27%	39%	39%	47%	43%	39%	31%
Demander des réponses aux fournisseurs de solutions de sécurité informatique	38%	30%	42%	39%	39%	38%	39%	38%
Contacters le prestataire de notre cyberassurance	23%	13%	32%	20%	17%	25%	20%	22%
Changer de fournisseurs de solutions de sécurité informatique	18%	10%	22%	18%	17%	13%	21%	20%
*Autre (merci de préciser)	1%	2%	0%	1%	0%	1%	1%	1%
Aucun des choix ci-dessus	3%	5%	3%	3%	0%	4%	1%	3%

'Après avoir subi une attaque par ransomware, qu'a fait/aurait fait votre département de sécurité informatique parmi les choix suivants ?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport
Notifier le PDG / Comité de direction	61%	64%	53%	55%	67%	67%	59%	65%	61%
Informers les autorités	54%	51%	53%	57%	58%	52%	53%	58%	54%
Informers nos avocats	50%	60%	43%	51%	34%	52%	71%	55%	51%
Notification des régulateurs de protection des données	48%	49%	60%	46%	55%	40%	47%	50%	46%
Essayer de décrypter les fichiers nous-mêmes	42%	51%	47%	42%	43%	36%	41%	31%	46%
Informers les clients	38%	35%	30%	26%	39%	45%	29%	39%	39%
Demander des réponses aux fournisseurs de solutions de sécurité informatique	38%	35%	43%	41%	45%	37%	35%	37%	40%
Contacters le prestataire de notre cyberassurance	23%	24%	27%	23%	24%	28%	35%	23%	19%
Changer de fournisseurs de solutions de sécurité informatique	18%	15%	30%	12%	25%	22%	6%	18%	19%
*Autre (merci de préciser)	1%	0%	0%	1%	0%	1%	0%	0%	0%
Aucun des choix ci-dessus	3%	0%	7%	3%	3%	3%	0%	3%	3%

Votre organisation a-t-elle été en mesure d'identifier le cybercriminel dans l'une des attaques par ransomware qui a ciblé votre organisation et, si oui, qui était-t'il ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Pirate opportuniste (non organisé)	48%	41%	46%	50%	53%	49%	45%	48%
Cybercriminels organisés	45%	23%	48%	37%	67%	40%	49%	48%
Manifestants anticapitalistes	31%	18%	33%	38%	27%	24%	33%	36%
Hacktivistes politiques	24%	15%	23%	21%	37%	24%	28%	21%
Employés mécontents/Anciens employés	24%	15%	23%	27%	29%	12%	34%	27%
Concurrents	19%	3%	26%	15%	22%	14%	17%	27%
Clients mécontents	18%	10%	20%	19%	20%	13%	22%	20%
Pirates travaillant pour un Etat	6%	0%	11%	2%	4%	2%	10%	5%
Autre (merci de préciser)	0%	0%	0%	0%	0%	0%	0%	0%
Mon organisation n'a pas été en mesure de déterminer l'identité des attaquants dans aucune des attaques de ransomware que nous avons subi	15%	38%	15%	12%	0%	19%	12%	13%

Votre organisation a-t-elle été en mesure d'identifier le cybercriminel dans l'une des attaques par ransomware qui a ciblé votre organisation et, si oui, qui était-t'il ?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Pirate opportuniste (non organisé)	48%	50%	65%	42%	51%	39%	25%	31%	64%	46%
Cybercriminels organisés	45%	36%	82%	32%	57%	33%	0%	35%	48%	57%
Manifestants anticapitalistes	31%	36%	47%	42%	26%	27%	25%	23%	30%	23%
Hacktivistes politiques	24%	21%	35%	26%	37%	21%	25%	15%	30%	11%
Employés mécontents/Anciens employés	24%	25%	41%	16%	37%	24%	0%	31%	15%	14%
Concurrents	19%	18%	12%	16%	37%	24%	0%	15%	18%	9%
Clients mécontents	18%	11%	29%	16%	31%	15%	0%	12%	21%	14%
Pirates travaillant pour un Etat	6%	4%	12%	6%	9%	9%	0%	8%	3%	0%
Autre (merci de préciser)	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Mon organisation n'a pas été en mesure de déterminer l'identité des attaquants dans aucune des attaques de ransomware que nous avons subi	15%	7%	6%	13%	6%	21%	25%	27%	15%	20%

Quelles sont, selon vous, les principales motivations des cybercriminels lorsqu'ils ont ciblé votre organisation avec une attaque par ransomware ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Gains financiers	54%	64%	60%	44%	43%	54%	54%	53%
Perturbation de l'activité de l'entreprise	47%	33%	53%	38%	53%	44%	54%	43%
Cyber espionnage	42%	21%	39%	56%	51%	38%	46%	43%
Motivations politiques	30%	8%	27%	33%	49%	28%	27%	35%
Vengeance suite à une mauvaise expérience avec mon organisation	27%	8%	27%	37%	33%	21%	33%	28%
Attaque internationale parrainée par un État	20%	5%	23%	17%	29%	11%	29%	21%
Divertissement (piratage pour s'amuser)	16%	13%	21%	12%	14%	12%	17%	20%
Autre (merci de préciser)	0%	0%	0%	0%	0%	0%	0%	0%
Nous n'avons aucune idée de la motivation des cyber-attaquants ayant ciblés notre organisation	5%	13%	6%	4%	0%	11%	1%	4%

Was glauben Sie war das Hauptmotiv der Ransomware-Angreifer, als Sie Ihr Unternehmen attackiert haben?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Gains financiers	48%	50%	65%	42%	51%	39%	25%	31%	64%	46%
Perturbation de l'activité de l'entreprise	45%	36%	82%	32%	57%	33%	0%	35%	48%	57%
Cyber espionnage	31%	36%	47%	42%	26%	27%	25%	23%	30%	23%
Motivations politiques	24%	21%	35%	26%	37%	21%	25%	15%	30%	11%
Vengeance' suite à une mauvaise expérience avec mon organisation	24%	25%	41%	16%	37%	24%	0%	31%	15%	14%
Attaque internationale parrainée par un État	19%	18%	12%	16%	37%	24%	0%	15%	18%	9%
Divertissement (piratage pour s'amuser)	18%	11%	29%	16%	31%	15%	0%	12%	21%	14%
Autre (merci de préciser)	6%	4%	12%	6%	9%	9%	0%	8%	3%	0%
Nous n'avons aucune idée de la motivation des cyber-attaquants ayant ciblés notre organisation	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Gains financiers	15%	7%	6%	13%	6%	21%	25%	27%	15%	20%

Votre organisation a-t-elle pu localiser l'origine de la fuite (la localisation du ou des cybercriminels) ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Europe de l'Est	47%	54%	35%	48%	61%	52%	44%	43%
Depuis mon propre pays	45%	21%	66%	33%	31%	45%	49%	40%
Europe de l'Ouest	34%	21%	25%	30%	59%	35%	32%	35%
Amérique du Nord	19%	8%	32%	11%	12%	12%	22%	25%
Moyen-Orient	19%	8%	8%	33%	29%	13%	19%	25%
Extrême-Orient	17%	29%	9%	20%	20%	12%	19%	18%
Afrique	13%	13%	5%	22%	18%	7%	14%	17%
Amérique du Nord	4%	0%	9%	2%	0%	3%	6%	5%
Mon organisation n'a pas été en mesure de déterminer l'emplacement source de l'attaque	4%	8%	2%	7%	2%	3%	3%	6%

Votre organisation a-t-elle pu localiser l'origine de la fuite (la localisation du ou des cybercriminels) ?

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Europe de l'Est	47%	31%	75%	37%	39%	50%	33%	47%	50%	57%
Depuis mon propre pays	45%	35%	75%	33%	64%	42%	33%	37%	43%	36%
Europe de l'Ouest	34%	46%	50%	30%	18%	27%	0%	32%	43%	39%
Amérique du Nord	19%	23%	38%	11%	21%	15%	0%	11%	25%	18%
Moyen-Orient	19%	23%	13%	22%	3%	38%	33%	21%	25%	7%
Extrême-Orient	17%	12%	13%	26%	12%	19%	0%	32%	18%	7%
Afrique	13%	19%	6%	15%	12%	12%	33%	5%	14%	11%
Amérique du Nord	4%	0%	25%	4%	6%	4%	0%	0%	4%	0%
Mon organisation n'a pas été en mesure de déterminer l'emplacement source de l'attaque	4%	0%	0%	4%	3%	4%	0%	16%	4%	4%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Pays

Total

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	19%	35%	19%	18%	9%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	28%	37%	20%	12%	3%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	13%	23%	25%	27%	12%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	30%	41%	20%	7%	2%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	19%	30%	22%	18%	10%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	14%	38%	32%	11%	5%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	15%	29%	24%	23%	9%

United Kingdom

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	10%	37%	22%	23%	8%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	19%	44%	26%	11%	0%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	5%	19%	31%	36%	9%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	25%	38%	25%	12%	0%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	10%	33%	30%	18%	9%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	8%	35%	35%	16%	6%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	7%	25%	27%	34%	7%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Pays

United States

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	23%	29%	20%	16%	13%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	31%	37%	16%	11%	6%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	15%	23%	19%	28%	16%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	35%	42%	13%	7%	4%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	24%	26%	20%	19%	13%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	23%	37%	29%	6%	6%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	15%	32%	22%	20%	12%

France

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	21%	40%	15%	17%	7%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	25%	38%	18%	17%	2%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	16%	29%	22%	26%	7%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	34%	39%	18%	5%	4%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	22%	38%	18%	14%	8%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	13%	35%	32%	13%	6%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	21%	31%	23%	15%	10%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Pays

Germany

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	17%	43%	16%	20%	4%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	33%	28%	25%	13%	1%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	13%	21%	34%	19%	13%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	21%	43%	29%	6%	1%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	18%	26%	25%	23%	8%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	17%	48%	30%	4%	0%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	19%	24%	24%	28%	5%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Taille

Total

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	19%	35%	19%	18%	9%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	28%	37%	20%	12%	3%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	13%	23%	25%	27%	12%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	30%	41%	20%	7%	2%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	19%	30%	22%	18%	10%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	14%	38%	32%	11%	5%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	15%	29%	24%	23%	9%

1,001-3,000 Employees

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	18%	38%	21%	16%	6%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	29%	38%	18%	14%	2%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	9%	25%	29%	26%	11%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	31%	37%	23%	7%	3%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	20%	33%	23%	16%	8%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	10%	47%	34%	8%	2%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	13%	30%	24%	27%	7%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Taille

3,001-5,000 Employees

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	23%	29%	20%	16%	13%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	31%	37%	16%	11%	6%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	15%	23%	19%	28%	16%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	35%	42%	13%	7%	4%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	24%	26%	20%	19%	13%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	23%	37%	29%	6%	6%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	15%	32%	22%	20%	12%

5,000+ Employees

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	21%	40%	15%	17%	7%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	25%	38%	18%	17%	2%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	16%	29%	22%	26%	7%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	34%	39%	18%	5%	4%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	22%	38%	18%	14%	8%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	13%	35%	32%	13%	6%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	21%	31%	23%	15%	10%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Secteur

Total

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	19%	35%	19%	18%	9%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	28%	37%	20%	12%	3%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	13%	23%	25%	27%	12%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	30%	41%	20%	7%	2%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	19%	30%	22%	18%	10%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	14%	38%	32%	11%	5%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	15%	29%	24%	23%	9%

Business & Professional Services

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	7%	47%	20%	20%	5%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	16%	45%	24%	13%	2%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	11%	18%	31%	29%	11%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	31%	42%	18%	4%	5%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	11%	25%	31%	24%	9%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	0%	60%	33%	0%	7%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	15%	31%	20%	27%	7%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Secteur

Financial Services

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	20%	28%	25%	17%	10%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	25%	38%	22%	13%	3%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	13%	23%	23%	30%	10%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	22%	39%	32%	4%	3%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	17%	29%	26%	20%	7%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	15%	20%	45%	15%	5%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	12%	30%	26%	26%	6%

Construction & Property

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	33%	33%	3%	27%	3%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	30%	23%	30%	13%	3%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	23%	37%	3%	27%	10%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	20%	40%	30%	7%	3%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	33%	23%	27%	13%	3%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	50%	50%	0%	0%	0%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	30%	23%	23%	17%	7%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Secteur

IT, Tech & Telecom

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	30%	33%	18%	9%	10%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	31%	36%	13%	16%	3%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	16%	28%	25%	19%	10%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	37%	45%	13%	4%	0%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	24%	40%	18%	12%	6%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	18%	59%	18%	0%	6%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	18%	36%	24%	18%	4%

Manufacturing & Production

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	18%	27%	22%	22%	10%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	28%	42%	16%	7%	6%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	7%	27%	21%	31%	13%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	34%	37%	18%	7%	3%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	27%	30%	15%	15%	13%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	20%	20%	45%	5%	10%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	13%	19%	31%	22%	13%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Secteur

Media, Leisure & Entertainment

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	18%	24%	24%	18%	18%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	18%	35%	24%	18%	6%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	6%	18%	12%	47%	18%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	18%	29%	29%	18%	6%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	12%	35%	18%	29%	6%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	20%	40%	20%	20%	0%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	18%	29%	12%	18%	24%

Public Sector

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	16%	35%	13%	27%	8%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	35%	31%	21%	13%	0%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	6%	21%	29%	16%	27%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	34%	32%	21%	11%	2%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	21%	21%	18%	27%	13%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	14%	24%	33%	19%	10%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	11%	31%	26%	24%	8%

Dans quelle mesure êtes-vous d'accord avec les énoncés suivants ? - Secteur

Retail, Distribution & Transport

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	11%	47%	17%	17%	7%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	24%	41%	23%	11%	0%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	16%	11%	27%	40%	6%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	31%	49%	14%	6%	0%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	14%	30%	21%	20%	14%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	12%	44%	28%	16%	0%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	13%	29%	17%	30%	11%

Other Commercial Sectors

	Complètement d'accord	Plutôt d'accord	Ni d'accord, ni en désaccord	Plutôt en désaccord	Complètement en désaccord
Mon organisation a perdu confiance dans les solutions de cybersécurité traditionnelles, comme les antivirus	21%	37%	21%	13%	10%
Les techniques traditionnelles de cybersécurité ne peuvent pas nous protéger contre la nouvelles génération de logiciels malveillants telles que les attaques par ransomware	35%	32%	16%	11%	6%
Mon organisation se sent impuissante à se défendre contre les nouvelles formes de ransomware	14%	27%	33%	17%	8%
Nous avons besoin d'une nouvelle génération de solutions pour se protéger contre les ransomware	29%	43%	13%	13%	3%
Nous avons accepté que les cybercriminels sont constamment en avance et nous nous concentrons maintenant sur l'atténuation plutôt que sur la cyberprotection	16%	33%	29%	11%	11%
Nous allons probablement chercher à nous doter d'une cyber-assurance maintenant que la possibilité d'amendes est plus élevée avec le GDPR	13%	47%	27%	13%	0%
L'antivirus est dépassé - il sera bientôt inutile dans la lutte contre les cyber-attaques	19%	29%	24%	19%	10%

Combien d'employés compte votre organisation à l'échelle mondiale ?

	Total	UK	US	France	Germany
1,001-3,000 employés	38%	45%	38%	28%	41%
3,001-5,000 employés	31%	28%	31%	40%	28%
Plus de 5000 employés	31%	27%	32%	32%	31%

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
1,001-3,000 employés	38%	40%	53%	29%	42%	42%	24%	39%	33%	40%
3,001-5,000 employés	31%	36%	43%	32%	33%	27%	29%	24%	33%	30%
Plus de 5000 employés	31%	24%	3%	39%	25%	31%	47%	37%	34%	30%

Dans quel secteur évolue votre organisation ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Grande distribution, commerces et transport	14%	14%	12%	18%	14%	12%	15%	16%
Services financiers	14%	14%	13%	17%	13%	11%	14%	18%
IT, technologie et télécoms	13%	10%	14%	20%	10%	15%	14%	11%
Fabrication et production	13%	15%	12%	13%	15%	15%	11%	14%
Secteur public	12%	10%	12%	13%	15%	13%	10%	15%
Services aux entreprises et aux professionnels	11%	19%	9%	5%	14%	12%	13%	8%
Construction et immobilier	6%	5%	11%	0%	3%	8%	8%	1%
Médias, loisirs et divertissements	3%	6%	4%	4%	0%	2%	3%	5%
*Autres secteurs commerciaux (merci de préciser)	13%	7%	15%	10%	16%	13%	12%	12%

Dans quels domaines fonctionnels êtes-vous principalement employé au sein de votre organisation ?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Technologie de l'information	99%	100%	99%	98%	100%	99%	100%	99%
Risque/fraude/conformité/gouvernance	1%	0%	1%	2%	0%	1%	0%	1%

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Technologie de l'information	99%	98%	100%	99%	100%	100%	100%	98%	100%	98%
Risque/fraude/conformité/gouvernance	1%	2%	0%	1%	0%	0%	0%	2%	0%	2%

Wie stark sind Sie in Ihrem Unternehmen in den Bereich IT-Security eingebunden?

	Total	UK	US	France	Germany	1k-3k employés	3k-5k employés	5k+ employés
Je travaille exclusivement pour la sécurité informatique de mon organisation	41%	20%	42%	47%	57%	38%	46%	41%
La majorité de mon travail concerne la sécurité informatique de mon organisation	33%	25%	39%	30%	33%	36%	32%	29%
Certains de mes travaux impliquent la sécurité informatique mais j'ai d'autres responsabilités	26%	55%	20%	23%	10%	25%	22%	30%

	Total	Services aux entreprises et aux professionnels	Construction et immobilier	Services financiers	IT, technologie et télécoms	Fabrication et production	Médias, loisirs et divertissements	Secteur public	Grande distribution, commerces et transport	Autres secteurs commerciaux
Ich arbeite ausschließlich im Bereich IT-Security	41%	44%	70%	32%	48%	39%	29%	32%	41%	44%
Meine Arbeit betrifft überwiegende den Bereich IT-Security	33%	31%	23%	43%	40%	30%	18%	24%	31%	38%
Meine Arbeit betrifft gelegentlich den Bereich IT-Security, ich habe jedoch eigentlich andere Verantwortlichkeiten	26%	25%	7%	25%	12%	31%	53%	44%	27%	17%

SentinelOne