Future of Secure Remote Work Report

cisco SECURE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The COVID-19 pandemic has caused businesses across the globe to transition to a remote work environment at unprecedented speed and scale. What was once "nice to have" for employees and companies became a "must have" almost overnight, with organisations all over the world shifting their entire workforce to remote working arrangements. As the transition happened, organisations had to adapt and evolve their cybersecurity approach, solutions, and policies to enable their employees to work remotely, access company resources securely, and ensure business continuity.

In what has been a year fraught with uncertainty, a significant trend has emerged – that of a flexible and hybrid future of work. Having worked remotely for an extended period of time, employees are now expecting that they will continue to have the flexibility and ability to work from anywhere, at any time and on any device, in a post-COVID era, even as they return to the office.

This has accelerated the need for businesses to reassess their cybersecurity posture, especially at this time when business leaders are looking to build resilient enterprises. Security can be the bridge to business resiliency as it can enable businesses to operate with flexibility by securely adapting to protect what's now and what's next. To achieve this, it is key to ensure that networking and collaborative solutions are flexible, simple to use, effective, and secure, whether delivered via on-premises data centers or in the cloud, and across all user devices – work or personal.

We wanted to understand how prepared organisations were, globally, in securing their businesses as they were forced to take their entire workforce remote due to the pandemic. More importantly, we wanted to get insights into where organisations are today in terms of the rising cybersecurity threats and alerts, the challenges they faced in this sudden transition, and how they are adapting their cybersecurity approaches to better prepare for the hybrid and flexible work environment that is here to stay. To do this, we commissioned a global research survey across 21 markets in the Americas (AMER), Asia Pacific, Japan and China (APJC), and Europe, surveying over 3000 IT decision makers from small businesses to large enterprises.

The study, titled Future of Secure Remote Work, aims to better understand the challenges that organisations faced in transitioning to remote work, while uncovering the state of their cybersecurity readiness, as well as the shifts in their priorities, policies, and investments as they prepare for a hybrid work environment that is likely here to stay.

The results are telling.

EUROPE HIGHLIGHTS

EUROPE HIGHLIGHTS

Regional Summary

The study surveyed over 600 respondents from four countries in Europe – France, Germany, Italy, and the United Kingdom. Based on data gleaned from the respondents, COVID-19 has had a similar impact across Europe where remote work will earn, in some capacity, a permanent place in the employment mix. Thirty-four percent of organisations believe that ***more than half*** of their employees will continue working remotely post-pandemic

Contrary to their regional counterparts, organisations in Europe appear to be better prepared in supporting the sudden transition to a remote workforce. While 45% stated that they were ***very prepared*** (compared to 40% globally and 39% in APJC and AMER, respectively), 50% said they were ***somewhat prepared*** (compared to 53% globally), and 6% said they were ***not prepared*** (tied with AMER and the global averages).

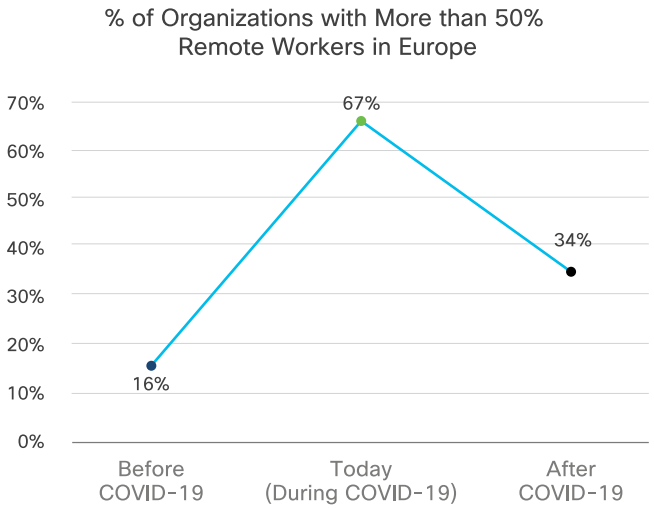
While only 37% of European respondents experienced a jump of ***25% or more*** in cyber threats or alerts, lower than the 61% global average, a worrying 17% of European respondents did not know if there was an increase or decrease in cyber threats or alerts at all. This is significantly higher than the AMER (5%) and APJC (6%) averages.

	Global	APJC	AMER	Europe
Increase in cyber alerts or attacks (25% or more)	61%	69%	64%	37%
Don't know	8%	6%	5%	17%

Just over half (52%) of organisations in Europe indicated that the COVID-19 situation will result in an increase in future cybersecurity investments. This makes Europe the region with the ***smallest proportion of organisations expecting an increase in cybersecurity investments among the three regions,*** compared to the global average of 66%. Thirty-seven percent said there will be no change to their organisation's investment, the highest when compared to the AMER (23%) and APJC (17%) averages.

Key Findings

The shift to a hybrid work environment continues in Europe but at varying levels



Europe had the lowest proportion of remote workers prior to the pandemic with just 16% of organisations reporting having more than half of their workforce remote – slightly below the global average (19%). Once the pandemic hit, the proportion of organisations with ***more than half*** of their workforce remote surged to 67%, higher than the global average of 62%. Looking ahead post-COVID-19, 34% of European organisations are expecting more than half of their employees to continue working remotely, double the proportion before the outbreak.

- While respondents in France and Italy saw a four-fold increase in the proportion of organisations with ***more than half*** of their workforce being remote pre-pandemic (15% respectively) versus at the height of the pandemic (64% in France and 65% in Italy), the United Kingdom experienced the highest increase in remote workers in the world, with 85% of organisations with ***more than half*** of their workforce remote during the pandemic (up from 18% pre-pandemic). This is likely due to the country's stringent lockdown measures at the height of the outbreak.
- According to the data, more organisations in the United Kingdom (50%) are expecting ***more than half*** of their employees to continue working remotely post-COVID-19, the highest increase in remote workers of those countries surveyed in the world (ahead of the global average of 37%).
- Organisations in France (32%), Germany (24%), and Italy (33%) are also expecting to have more remote workers post-pandemic, compared to their pre-COVID-19 levels, though these numbers are lower than the global average.

32%
France

24%
Germany

33%
Italy

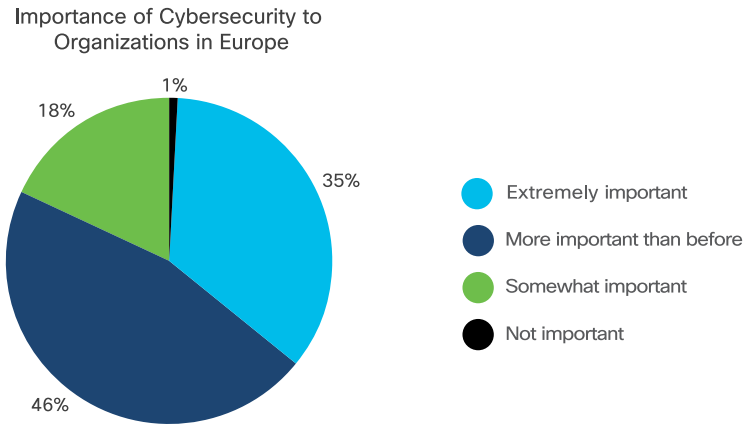
The United Kingdom had the second highest proportion of organisations that reported to be ***very prepared*** (59%) to make the accelerated transition to a remote work environment at the outset of COVID-19, in the world, after Vietnam (67%). Meanwhile, France and Italy saw the highest proportion of organisations ***not prepared*** for the transition in Europe, with a higher than global average of 9% and 8%, respectively.

Cybersecurity preparedness to transition to remote working	France	Germany	Italy	UK
Very prepared	43%	41%	35%	59%
Somewhat prepared	47%	55%	57%	39%
Not prepared	9%	4%	8%	2%

Cybersecurity Preparedness to Transition to Remote Working by Country

Cybersecurity is important but not important enough

At a time when businesses are facing an onslaught of challenges from the sudden and massive transition to remote work, Europe had the most organisations attesting to cybersecurity being ***more important than before*** at 46%, which is higher than global and APJC (41%) as well as AMER (38%) averages. Yet it still had the smallest proportion of organisations recognising that cybersecurity is ***extremely important*** at 35%.



Importance of cybersecurity	Global	APJC	AMER	Europe
Extremely important	44%	44%	50%	35%
More important than before	41%	41%	38%	46%
Somewhat important	15%	15%	11%	18%
Not important	1%	1%	1%	1%

Importance of Cybersecurity to the Organisation Regional vs. Global Average

- Delving deeper, the level of cybersecurity importance also varies within Europe itself. Forty-six percent of organisations in the United Kingdom said cybersecurity is ***extremely important***, 2% higher than the global average (44%), whereas the rest of the European countries surveyed (France, Germany, and Italy) had a higher proportion of organisations indicating that cybersecurity is ***more important than it was before***.

- Europe is also the region with the most organisations saying cybersecurity is only ***somewhat important***, at 18%, higher than the global average of 15%.

Importance of cybersecurity	France	Germany	Italy	U.K.
Extremely important	34%	32%	28%	46%
More important than before	44%	47%	57%	35%
Somewhat important	20%	19%	15%	17%
Not important	2%	1%	-	1%

Importance of Cybersecurity to the Organisation by Country

Organisations in Europe experienced the smallest increase in cyber threats or alerts since the pandemic but many are not completely certain

As highlighted earlier, most European organisations reported a lower level of increase in cyber threats or alerts compared to their regional counterparts in AMER and APJC. However, they also recorded the largest proportion of organisations that are uncertain about the increase or decrease in cyber threats or alerts.

Breaking this down further, close to half of organisations in France (48%) experienced an increase of ***25% or more*** in cyber threats or alerts during the pandemic, the highest observed among the four European countries surveyed, and also higher than the regional average (37%).

On the flip side, while only 24% of U.K. organisations experienced an increase of ***25% or more*** in cyber threats or alerts, the United Kingdom recorded the largest proportion of organisations in the region that ***do not know*** whether there has been an increase or decrease (27%). This is significantly higher than the global average (8%) and regional average (17%).

Increase in cyber threats or alerts	France	Germany	Italy	U.K.
25% or more	48%	31%	43%	24%
Don't know	12%	14%	14%	27%

Increase in Cyber Threats or Alerts According to Country

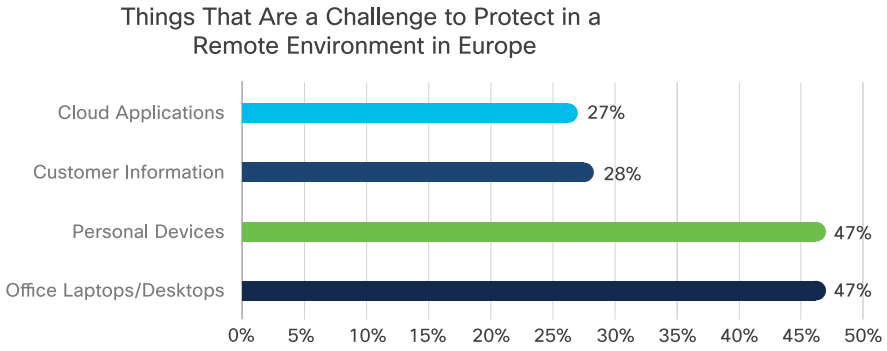
Cybersecurity challenges continue to be relentless

As more users continue to connect remotely, EU companies have seen surges in cybersecurity-related challenges. Secure access was named as the **top cybersecurity challenge** faced by the largest proportion of organisations at 57%. Other concerns include data privacy (41%), which has implications for the overall security posture, and maintaining control and enforcement policies (39%).

Endpoint security is a critical measure

Workers taking corporate devices home became the Achilles' heel to nearly half (47%) of European businesses with endpoint security threats circumventing traditional cybersecurity defenses that were not set up for remote work. This is in alignment with the global trend where 1 in 2 respondents stated that office laptops/desktops (56%) and personal devices (54%) are a top challenge in protecting a remote environment.

European organisations also found customer information (28%) and cloud applications (27%) a challenge to protect in a remote work environment. However, these figures were both significantly less than the global average (46% respectively).



- The United Kingdom is the only country in the region that had a larger proportion of organisations that found it a challenge to protect office devices (46%) than personal devices (39%).

- The same proportion (55%) of German organisations found personal devices and office laptops/desktops in a remote working environment a challenge to protect – the only market in the region with a tie. This was also 8% percent higher than the tied regional average (47%).

Supporting remote workers with the right technology priorities

As businesses went from having the majority of their meetings face-to-face to virtualising all their communications almost overnight, Europe is on par with its global counterparts at keeping workers connected remotely yet securely. Consistent with global trends, over half (55%) of organisations that adopted these solutions ranked cybersecurity measures as its #1 priority, ahead of collaboration tools (48% ranked it first) and professional services (25% ranked it first).

- Within Europe itself, all but Germany ranked cybersecurity measures as their top priority.

Most Widely Adopted	vs	Number 1 Priority
Collaboration Tools 76%	1	Cybersecurity Measures 55%
Cybersecurity Measures 65%	2	Collaboration Tools 48%
Cloud-Based Document Sharing 56%	3	Professional Services 25%

Top IT Solutions Adoption vs. Priority Among European Organisations to Support Remote Working

- While the region ranked professional services third overall, three of the EU-surveyed countries bumped cloud sharing up into third place, except for France.

France	Germany	Italy	U.K.
Cybersecurity measures (51%)	Collaboration tools (54%)	Cybersecurity measures (58%)	Cybersecurity measures (63%)
Collaboration tools (50%)	Cybersecurity measures (46%)	Collaboration tools (44%)	Collaboration tools (43%)
Professional services (31%)	Cloud-based document sharing (31%)	Cloud-based document sharing (21%)	Cloud-based document sharing (23%)

IT Solutions Ranked #1 by Organisations in Europe

Renewing commitment to cybersecurity policies

As organisations continue to secure remote workers, the majority found it absolutely necessary to update their cybersecurity policies immediately in an effort to support this massive shift. Ninety-three percent of organisations in Europe reported changes to their cybersecurity policies – despite this being the lowest proportion among all three regions and against the global average (96%). The top policy-related change made was **increased VPN capacity** (64%), higher than the global average of 59%. Other top policy-related changes made were **implementing multi-factor authentication** (38% in Europe vs. 53% globally), **increasing web controls and acceptable use policy** (34% in Europe vs. 55% globally), and **endpoint protection** (34% in Europe vs. 48% globally).

- Interestingly, a higher proportion of organisations in France and Germany cited endpoint protection as their third cybersecurity policy change at 37% and 40%, respectively.

France	Germany	Italy	U.K.
Increased VPN capacity (63%)	Increased VPN capacity (64%)	Increased VPN capacity (66%)	Increased VPN capacity (65%)
Increasing web controls and acceptable use policy (40%)	Implementing multi-factor authentication (44%)	Implementing multi-factor authentication (40%)	Implementing multi-factor authentication (35%)
Endpoint protection (37%)	Endpoint protection (40%)	Increasing web controls and acceptable use policy (39%)	Increasing web controls and acceptable use policy (29%)

The Top Policy-Related Changes Made by Country

Simplicity and education are key to reinforcing protocols

While the pandemic forced businesses to accelerate their digital transformation and remote work plans, many employees were also learning and evolving their work habits in real time, with many working remotely for the first time. Security awareness training became more important than ever, as malicious actors recognised this potential learning gap and have continued to find new ways to capitalise on the unsuspecting.

Fifty-four percent of European organisations (vs. 59% globally) reported that the lack of employee awareness and education was the ***top challenge faced in reinforcing cybersecurity protocols*** for remote working, followed by having too many tools and solutions to manage and toggle (43% vs. 50% globally). Only 22% of European organisations reported struggling with the deployment of inconsistent interfaces (vs. 35% globally). While Europe's average is the lowest among global and regional averages, the findings show that there is an opportunity for further education and better security measures that are simple and easy to use and work well together.

Global	APJC	AMER	Europe
Lack of employee awareness/employee education (59%)	Lack of employee awareness/employee education (61%)	Lack of employee awareness/employee education (58%)	Lack of employee awareness/employee education (54%)
Too many tools/ solutions to manage and toggle (50%)	Too many tools/ solutions to manage and toggle (53%)	Too many tools/ solutions to manage and toggle (49%)	Too many tools/ solutions to manage and toggle (43%)
Inconsistent interfaces (35%)	Inconsistent interfaces (40%)	Inconsistent interfaces (33%)	Inconsistent interfaces (22%)

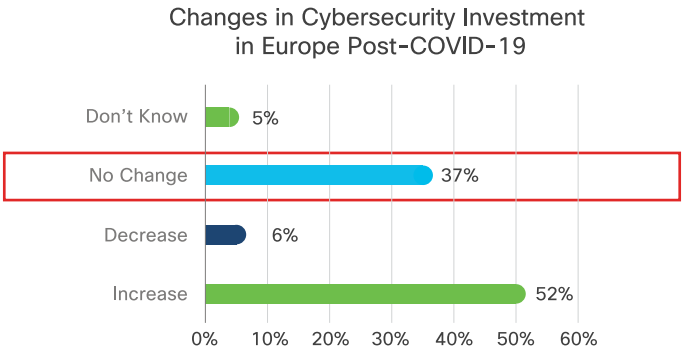
Top 3 Challenges in Reinforcing Cybersecurity Protocols by Region

- Germany bucked the trend with more organisations listing having too many tools and solutions to manage and toggle as its top challenge at 55%, higher than the regional average (43%).

Taking a measured yet proactive approach to increasing cybersecurity investments

More than half (52%) of European organisations indicated that the COVID-19 situation will result in an increase in their future cybersecurity investments. This is a step in the right direction despite it being the region recording the lowest proportion of organisations looking to boost such investments. Consequently, 37% of European organisations indicated that there will be ***no change*** to their organisation's cybersecurity investment, the highest across all regions.

- France (56%), Italy (52%), and Germany (56%) had over half of organisations claiming that they will increase their cybersecurity spending following the pandemic.
- The United Kingdom, on the other hand, recorded the largest proportion of respondents indicating no change to their future investment in cybersecurity (49%) in the world. They also recorded the lowest proportion of organisations indicating an increase to their cybersecurity investment in the world at 44%.



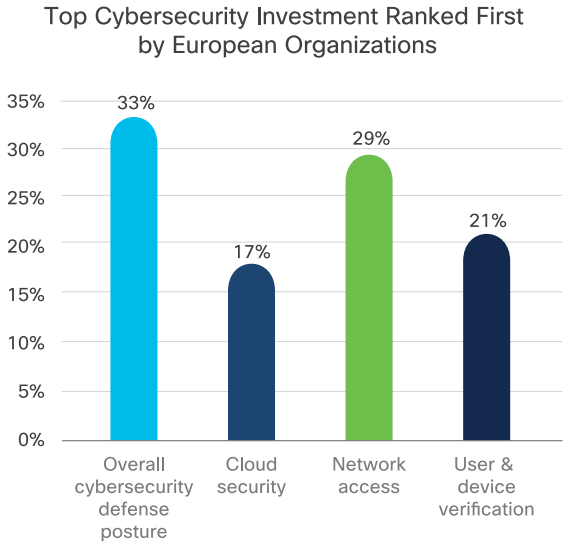
Changes in cybersecurity investments due to COVID-19	Global	APJC	AMER	Europe
Increase	66%	70%	68%	52%
Decrease	9%	11%	7%	6%
No change	22%	17%	23%	37%
Don't know	3%	2%	2%	5%

Changes in Cybersecurity Investments Regional vs. Global Averages

Pandemic spurs organisations in Europe to rethink their cybersecurity strategy

When asked to rank their cybersecurity investments in terms of importance, overall cybersecurity defense posture is the top-ranked investment priority (33% ranked it first).

It is the top-ranked choice for Italy (32% ranked it first) and United Kingdom (48% ranked it first). Other priority investments reported by European organisations include network access (29% ranked first) and user and device verification (21% ranked first). This indicates that organisations in Europe are tailoring their cybersecurity strategy toward a holistic, zero-trust approach to securely support a hybrid future of work as a result of the pandemic.



France	Germany	Italy	U.K.
Network access (33%)	Network access (32%)	Overall cybersecurity defense posture (32%)	Overall cybersecurity defense posture (48%)
Overall cybersecurity defense posture (25%)	Overall cybersecurity defense posture (28%)	Network access (32%)	User and device verification (20%)
User and device verification (22%)	User and device verification (22%)	User and device verification (21%)	Network access (17%)
Cloud security (20%)	Cloud security (18%)	Cloud security (15%)	Cloud security (15%)

Cybersecurity Investments Priorities (Ranked #1) by Country

COUNTRY DEEP DIVE: EUROPE

France

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organisations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 15% • During COVID-19: 64% • After COVID-19: 32%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organisations	• Extremely important: 34% • More important than before: 44% • Somewhat important: 20%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 48% • Don't know: 12%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 52% • Data privacy: 40% • Protection against malware: 36%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 49% • Office laptops/desktops: 44% • Cloud applications: 26% • Customer information: 25%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46%
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 43% • Somewhat prepared: 47% • Not prepared: 9%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritising Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 73% • Cybersecurity measures: 66% • Cloud-based document sharing: 53%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organisations that ranked it first)	• Cybersecurity measures: 51% • Collaboration tools: 50% • Professional services: 31%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional services: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 63% • Increasing web controls and acceptable use policy: 40% • Endpoint protection: 37%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 53% • More than 30%: 45%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 50% • Too many tools/solutions to manage and toggle: 46% • Inconsistent interfaces: 27%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organisation's future investment in cybersecurity due to COVID-19	• Increase: 56% • Decrease: 9% • No change: 29%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 63% • More than 30%: 27%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organisations that ranked it first)	• Network access: 33% • Overall cybersecurity defense posture: 25% • User and device verification: 22% • Cloud security: 20%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Germany

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organisations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 15% • During COVID-19: 53% • After COVID-19: 24%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organisations	• Extremely important: 32% • More important than before: 47% • Somewhat important: 19%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 31% • Don't know: 14%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 64% • Data privacy: 54% • Maintaining control and enforcement policies: 43%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices AND Office laptops/desktops: 55% (TIED) • Cloud applications: 42% • Customer information: 31%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 41% • Somewhat prepared: 55% • Not prepared: 4%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritising Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 72% • Cybersecurity measures: 62% • Cloud-based document sharing: 53%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organisations that ranked it first)	• Collaboration tools: 54% • Cybersecurity measures: 46% • Cloud-based document sharing: 31%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional services: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 44% • Endpoint protection: 40%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 57% • More than 30%: 38%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Too many tools/solutions to manage and toggle: 55% • Lack of employee awareness/employee education: 49% • Inconsistent interfaces: 23%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organisation's future investment in cybersecurity due to COVID-19	• Increase: 56% • Decrease: 6% • No change: 34%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 77% • More than 30%: 16%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organisations that ranked it first)	• Network access: 32% • Overall cybersecurity defense posture: 28% • User and device verification: 22% • Cloud security: 18%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Italy

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organisations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 15% • During COVID-19: 65% • After COVID-19: 33%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organisations	• Extremely important: 28% • More important than before: 57% • Somewhat important: 15%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 43% • Don't know: 14%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 68% • Maintaining control and enforcement policies: 49% • Data privacy: 47%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Personal devices: 46% • Office laptops/desktops: 42% • Customer information: 30% • Cloud applications: 21%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 35% • Somewhat prepared: 57% • Not prepared: 8%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%

Research Parameters	Country %	Regional Average	Global Average
Prioritising Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 79% • Cybersecurity measures: 68% • Cloud-based document sharing: 62%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document Sharing: 63%
Adopted IT solutions ranked in order of importance (% of organisations that ranked it first)	• Cybersecurity measures: 58% • Collaboration tools: 44% • Cloud-based document sharing: 21%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional service: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 66% • Implementing multi-factor authentication: 40% • Increasing web controls and acceptable use policy: 39%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 39% • More than 30%: 46%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 63% • Too many tools/solutions to manage and toggle: 41% • Lack of visibility / Inconsistent interfaces: 15%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%

Research Parameters	Country %	Regional Average	Global Average
Investments in Cybersecurity on the Rise			
Change in organisation's future investment in cybersecurity due to COVID-19	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 52% • Decrease: 6% • No change: 37	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 63% • More than 30%: 26%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organisations that ranked it first)	• Overall cybersecurity defense posture: 32% • Network access: 32% • User and device verification: 21% • Cloud security: 15%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

United Kingdom

Research Parameters	Country %	Regional Average	Global Average
The Importance of Cybersecurity in a Hybrid Future of Work			
Percentage of organisations with ***more than half*** of their workforce working remotely	• Pre-COVID-19: 18% • During COVID-19: 85% • After COVID-19: 50%	• Pre-COVID-19: 16% • During COVID-19: 67% • After COVID-19: 34%	• Pre-COVID-19: 19% • During COVID-19: 62% • After COVID-19: 37%
Importance of cybersecurity to organisations	• Extremely important: 46% • More important than before: 35% • Somewhat important: 17%	• Extremely important: 35% • More important than before: 46% • Somewhat important: 18%	• Extremely important: 44% • More important than before: 41% • Somewhat important: 15%

Research Parameters	Country %	Regional Average	Global Average
A Resilient Rebound: Tackling Cybersecurity Threats and Challenges			
Level of increase in cyber threats and alerts	• Increase of 25% or more: 24% • Don't know: 27%	• Increase of 25% or more: 37% • Don't know: 17%	• Increase of 25% or more: 61% • Don't know: 8%
Top 3 cybersecurity challenges faced	• Secure access: 43% • Maintaining control and enforcement policies: 31% • Protection against malware: 27%	• Secure access: 57% • Data privacy: 41% • Maintaining control and enforcement policies: 39%	• Secure access: 62% • Data privacy: 55% • Maintaining control and enforcement policies: 50%
Challenge to protect in a remote environment	• Office laptops/desktops: 46% • Personal devices: 39% • Customer information: 27% • Cloud applications: 20%	• Personal devices: 47% • Office laptops/desktops: 47% • Customer information: 28% • Cloud applications: 27%	• Office laptops/desktops: 56% • Personal devices: 54% • Customer information AND cloud applications: 46% (TIED)
Preparedness to transition to a remote work environment at the outset of COVID-19	• Very prepared: 59% • Somewhat prepared: 39% • Not prepared: 2%	• Very prepared: 45% • Somewhat prepared: 50% • Not prepared: 6%	• Very prepared: 40% • Somewhat prepared: 53% • Not prepared: 6%
Prioritising Cybersecurity for What's Now and What's Next			
Top 3 IT solutions adopted to enable remote work	• Collaboration tools: 79% • Cybersecurity measures: 65% • Cloud-based document sharing: 57%	• Collaboration tools: 76% • Cybersecurity measures: 65% • Cloud-based document sharing: 56%	• Collaboration tools: 73% • Cybersecurity measures: 68% • Cloud-based document sharing: 63%
Adopted IT solutions ranked in order of importance (% of organisations that ranked it first)	• Cybersecurity measures: 63% • Collaboration tools: 43% • Cloud-based document sharing: 23%	• Cybersecurity measures: 55% • Collaboration tools: 48% • Professional services: 25%	• Cybersecurity measures: 52% • Collaboration tools: 41% • Professional services: 27%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 65% • Implementing multi-factor authentication: 35% • Increasing web controls and acceptable use policy: 29%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 30% • More than 30%: 64%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 57% • Too many tools/solutions to manage and toggle: 29% • Inconsistent interfaces: 21%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organisation's future investment in cybersecurity due to COVID-19	• Increase: 44% • Decrease: 1% • No change: 49%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 57% • More than 30%: 21%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organisations that ranked it first)	• Overall cybersecurity defense posture: 48% • User and device verification: 20% • Network access: 17% • Cloud security: 15%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

Research Parameters	Country %	Regional Average	Global Average
Top 3 cybersecurity policy changes made to support remote working	• Increased VPN capacity: 65% • Implementing multi-factor authentication: 35% • Increasing web controls and acceptable use policy: 29%	• Increased VPN capacity: 64% • Implementing multi-factor authentication: 38% • Increasing web controls and acceptable use policy: 34%	• Increased VPN capacity: 59% • Increasing web controls and acceptable use policy: 55% • Implementing multi-factor authentication: 53%
Proportion of permanent changes to cybersecurity policies	• 30% or less: 30% • More than 30%: 64%	• 30% or less: 45% • More than 30%: 48%	• 30% or less: 50% • More than 30%: 45%
Top 3 challenges in enforcing cybersecurity protocols	• Lack of employee awareness/employee education: 57% • Too many tools/solutions to manage and toggle: 29% • Inconsistent interfaces: 21%	• Lack of employee awareness/employee education: 54% • Too many tools/solutions to manage and toggle: 43% • Inconsistent interfaces: 22%	• Lack of employee awareness/employee education: 59% • Too many tools/solutions to manage and toggle: 50% • Inconsistent interfaces: 35%
Investments in Cybersecurity on the Rise			
Change in organisation's future investment in cybersecurity due to COVID-19	• Increase: 44% • Decrease: 1% • No change: 49%	• Increase: 52% • Decrease: 6% • No change: 37%	• Increase: 66% • Decrease: 9% • No change: 22%
Proportion of increase in future cybersecurity investment	• 30% or less: 57% • More than 30%: 21%	• 30% or less: 65% More than 30%: 23%	• 30% or less: 59% • More than 30%: 36%
Cybersecurity investments ranked in order of importance (% of organisations that ranked it first)	• Overall cybersecurity defense posture: 48% • User and device verification: 20% • Network access: 17% • Cloud security: 15%	• Overall cybersecurity defense posture: 33% • Network access: 29% • User and device verification: 21% • Cloud security: 17%	• Overall cybersecurity defense posture: 34% • Network access: 24% • Cloud security: 22% • User and device verification: 20%

KEY TAKEAWAYS AND RECOMMENDATION

KEY TAKEAWAYS AND RECOMMENDATIONS

#1 The future of work is dynamic: Cybersecurity must meet the needs of a distributed workforce.

The world now sees that it is possible for employees to stay connected and productive while working away from the office for prolonged periods. It is likely that many businesses will move toward a hybrid work environment that caters to both in-office and remote employees. This will offer employer and employees greater choice and flexibility from business and human capital perspectives, as well as bring more diversity into the workforce. The abrupt shift also created a series of cybersecurity challenges – keeping your business running in a very different environment or securing access at a greater scale than ever before.

Employees are connecting their office devices to their home Wi-Fi or external networks or using their personal devices to connect to corporate applications in the cloud. This is putting a sudden strain on both security and IT teams who are being tasked with quickly providing support for an unprecedented number of offsite workers and their devices – without compromising security. Policies and controls that once resided in headquarters must now follow the worker wherever and whenever they choose to require access. In addition, the opportunity for remote work comes with a sinister shadow: modern threat actors have launched more phishing attacks to trick users and steal information from them, compromise the newly remote workforce systems with malware, or exploit gaps in a company's evolving cybersecurity posture.

Businesses need to create a flexible, safe, and secure hybrid work environment with employees moving on and off network with similar levels of protection. As business and IT leaders deliver significant changes to their technology and business priorities, cybersecurity should be the bridge that enables organisations to reach their full potential.

#2 The success of a flexible hybrid workforce hinges upon preparation, collaboration, and empowerment.

One of the key issues that has emerged from the overnight shift to remote work of the last eight months is how well organisations transitioned into it. Businesses that have made incremental and continuous investments in pre-pandemic technology, such as cloud security solutions and zero-trust frameworks, have been the best prepared to support remote work. Likewise, enhancing cybersecurity measures that support such arrangements has placed organisations in a better position to face the potential increase in the number and variety of cybersecurity attacks.

In order to reap the full benefits of a flexible and hybrid workplace, however, such investments cannot be made in a vacuum. With the shift to a distributed workforce, network and security teams need to provide seamless and secure access to applications and services, anywhere and anytime. Security, networking, and collaboration can no longer be seen in silos. They must work hand in hand. Alongside these functions, leaders must put in place additional enforcement protocols and enhanced cybersecurity policies. This should also be complemented by a solid employee education program, given the fact that investment in a healthy security culture is absolutely critical.

#3 Simpler and more effective cybersecurity is critical to building business resilience.

The experience of prolonged remote working has propelled the value of cybersecurity up corporate agendas, with long-term changes in corporate cybersecurity policies likely. Additionally, many have stated that they intend to increase their cybersecurity spending in the future.

With many competing priorities for IT leaders, security cannot be an afterthought – it should be the foundation behind the success of any digitalisation effort. This will ensure the security, scalability, and adaptability of these efforts. To reduce the likelihood and impact of a cybersecurity breach, organisations also need to look for ways to reduce the complexity of their cybersecurity measures. Taking a simplified approach toward more effective security ensures that it will be a business enabler, not a hinderance to what's needed now and what comes next.

Recommendations:

For businesses to enable people to work securely from anywhere, anytime, and on any device, cybersecurity should be the foundation of every IT investment. This requires a platform approach to deliver highly effective security from the network to the endpoint to the cloud. Best-of-breed point products simply do not measure up. When security must deliver less complexity, solutions must work together and offer ease of use.

To securely enable a distributed workforce and ensure the flexibility to adapt to what the future of work brings, organisations should ensure the following conditions are met:

- Verify the user's identity to establish trust: are you who you say you are?
- Enable work on any kind of device, any kind of connection, securely
- Give access to the company apps and data that workers need
- Protect users from threats once they're on the network

Future of Work: 10 Takeaways

1. Adopt a zero-trust strategy to verify the identity of all users before granting access to company-approved applications: protect the workforce, workload, and workplace.
2. Multi-factor authentication (MFA) is a natural first step in securing a distributed workforce, allowing you to verify the identities of employees attempting to access corporate assets.
3. Implement a VPN, providing a safe tunnel between users and applications so workers can stay productive and connected when they are on the road or working from home. It helps ensure only approved users get in by providing the right level of security without compromising the user experience.
4. Use DNS. Most security breaches target endpoint users, requiring a first line of defense at the DNS layer. This crucial first layer blocks domains associated with malicious behaviour before they get into your network or contains malware if it is already inside.
5. Secure Office 365 email against advanced threats. With email being the #1 attack vector, protection from email threats like phishing, ransomware, business email compromise, and others is needed using an integrated, cloud-native security solution for Microsoft 365 that stops threats to Office 365 from both internal and external senders.
6. Maintain the last line of defense with secure endpoint solutions. Not only does endpoint security prevent cyber attacks, but it also rapidly detects, contains, and remediates malicious files if they evade defenses and infiltrate endpoints – before damage can be done.
7. Accelerate the strategic adoption of cloud-based security solutions to protect your workforce by delivering a seamless connection to applications in any environment from any location. Secure access service edge (SASE) is a network architecture that combines SD-WAN capabilities with cloud-native security functions such as secure web gateways, cloud access security brokers, and firewalls, all delivered from the cloud.
8. Realise greater benefits from existing products through a platform approach. This provides visibility across multiple security solutions in a unified dashboard while integrating with third-party security solutions.
9. Automate Security Operation Center (SOC) workflows such as threat investigation, hunting, and remediation to strengthen efficiency and precision, lowering operational costs. This helps security teams better support evolving business and technology needs while staying ahead of an ever-changing threat landscape.
10. Remember: People can be the strongest link in any defense. Encourage greater employee cybersecurity awareness and empowerment. Organisations need to also look at improving employee awareness on the importance of adopting security-centric practices such as learning to identify phishing attacks, practicing good password policy, and keeping software up to date. Cybersecurity training cannot be a once-a-year, compliance-based training that most employees dislike. It must be a part of the culture.

Cisco SecureX™ is a cloud-native, platform experience that connects Cisco's security and networking portfolio and your existing infrastructure. It is integrated and open for simplicity, unified in one location for visibility, and maximises operational efficiency with automated workflows.

ABOUT THE FUTURE OF SECURE REMOTE WORK REPORT

In February to March 2020, organisations sought to protect their workforce by mandating and enabling their employees to work from home. While necessary for protecting people and communities, this experience physically separated security professionals from their own teams, from the employees who depended on them, and from the critical systems they were responsible for. The remote work arrangement also placed greater strain on existing digital policies and business continuity planning during an already stressful time.

That's not to say that we couldn't find ways to adapt to this new way of working. In the spirit of this reality, more than 3000 IT decision makers from small to large organisations were surveyed from June 16 to September 4, 2020, across a spectrum of 30 industries, including financial services, healthcare, architecture, transportation, etc., to understand how they have been impacted by the COVID-19 crisis from a cybersecurity perspective.

3196 respondents in **21** markets

AMER:
- Brazil
- Canada
- Mexico
- United States

EUROPE:
- France
- Germany
- Italy
- United Kingdom

APJC:
- Australia
- China
- Hong Kong
- India
- Indonesia
- Japan
- Korea
- Malaysia
- Philippines
- Singapore
- Taiwan
- Thailand
- Vietnam

Industries:
- Accounting
- Architecture
- Business Consulting
- Chemical Engineering or Manufacturing
- Construction
- Education
- Financial Services
- Government
- Healthcare
- Manufacturing:
- Non-computer Related
- Retail
- Software Development
- Telecommunications
- Transportation
- Wholesale and Distribution
- Non-Profit/ Charitable

Audience:
Professionals responsible for their company's IT

These organisations include:
- small (between 1 and 249 employees),
- medium (between 250 and 999 employees), and
- large businesses (1000 employees or more).

Objectives:

- To explore the **challenges** of moving some or all of an organisation's workforce to a **remote environment** almost overnight and the **readiness** of organisations around the world in securing their businesses in a remote work arrangement

- To understand how businesses adapted to this sudden transition including the shifts in their cybersecurity priorities, policies and investments

- To enable businesses to understand and prepare for a hybrid work environment by securely adapting to protect what's now and what's next.

Research Parameters

#1 The rise of remote workers during COVID-19 and the importance of cybersecurity to support them

1) Number of people working remotely before, during and after COVID-19
2) Importance of cybersecurity in today's COVID-19 and remote working landscape

#2 Addressing cybersecurity preparedness, threats, and challenges

1) How prepared are organisations with their cybersecurity features/solutions when (suddenly) transitioning to remote working
2) Types of cybersecurity challenges encountered during mass remote working and their gravity in order of importance
3) Most challenging things to protect during remote working

#3 Technology priorities and adoption to support remote working

1) Type of technologies adopted
2) Rank and order of importance of technologies adopted

#4 Movements in cybersecurity policies and enforcement protocols to support remote workers

1) Type of changes made
2) Proportion of changes in cybersecurity policies
3) Challenges in enforcing cybersecurity protocols

#5 Cybersecurity investments, today and beyond

1) Whether COVID-19 will change organisation's future cybersecurity investment
2) Percentage of increase, decrease, or no change in investment
3) Rank of future cybersecurity investment in order of importance

Future of Secure Remote Work Report

cisco SECURE