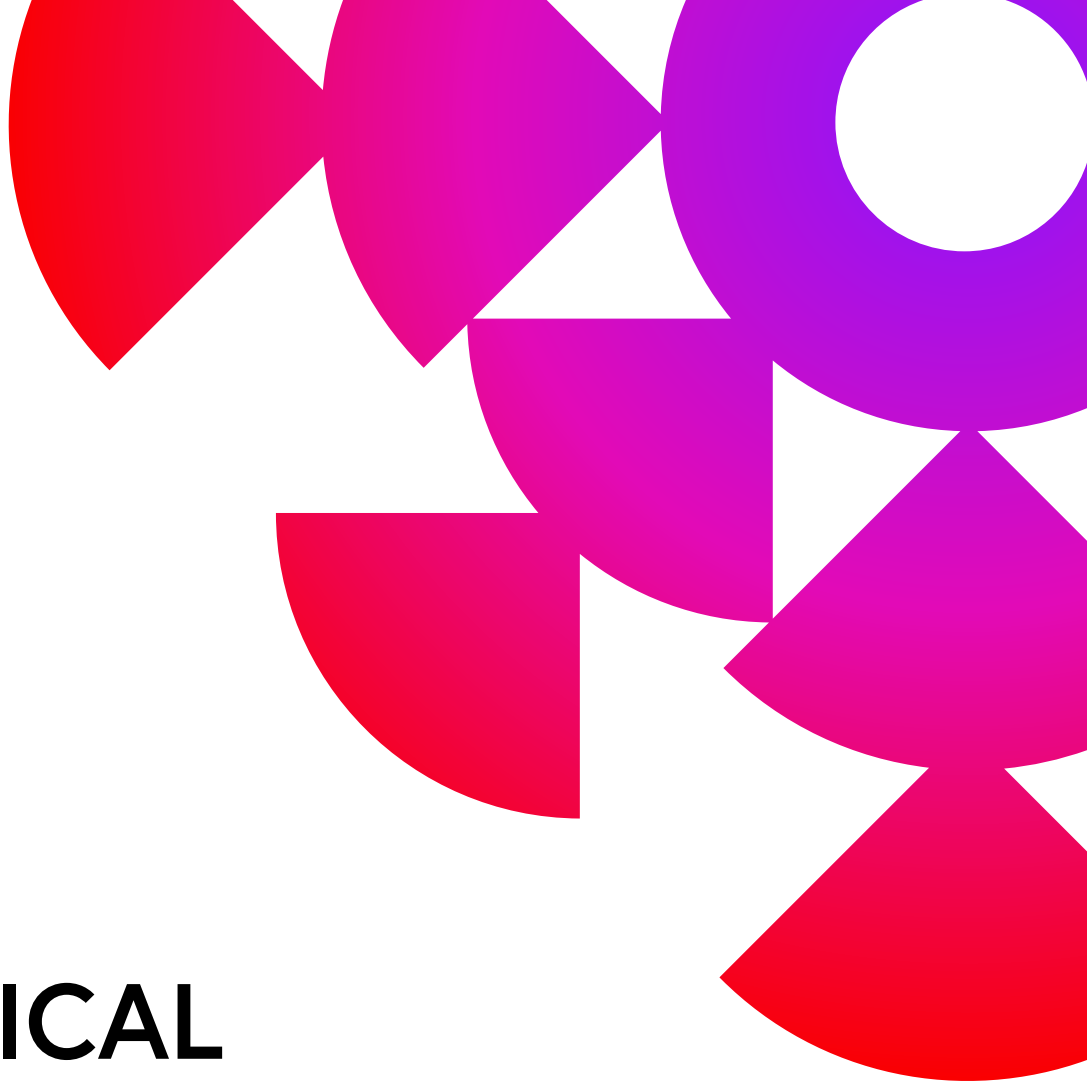


THE CRITICAL CONVERGENCE OF IT AND OT SECURITY IN A GLOBAL CRISIS

Weathering a Perfect Storm and Preparing for a Post-Pandemic Future

CLAROTY

EXECUTIVE SUMMARY

This independent, global survey of information technology (IT) and operational technology (OT) security professionals who own, operate, or otherwise support components of critical infrastructure within large enterprises, explores how their concerns, experiences, and attitudes have shifted since the COVID-19 pandemic began. Key findings include:

Overall threat level on the rise; Pharmaceutical most vulnerable sector

- Respondents said the overall threat level during COVID-19 has increased. 56% have experienced more threats and 70% have seen cybercriminals using new tactics to target their organization since the pandemic began.
- Respondents rated five industrial sectors as the most vulnerable to a cyberattack: pharmaceutical (14.09%), oil & gas (13.45%), electric utilities (13.45%), manufacturing (12.55%), and building management systems (12%).

IT/OT convergence accelerates, yet gaps remain

- COVID-19 has accelerated the convergence of IT and OT networks. 67% say their IT and OT networks have become more interconnected since the pandemic began, and more than 75% expect they will become even more so as a result.
- However, disparities between IT and OT remain. 66% find collaboration between IT and OT teams more challenging during the pandemic, while 62% believe their organization's IT and OT networks are not equally secure.

Ability to adapt enhanced by secure remote access, cybersecurity response plans

- Fortunately, 68% reported a seamless shift to remote work. A contributing factor may be that 80% already had a secure remote access solution (aside from a VPN, which is not secure enough for OT) in place prior to the pandemic.
- However, there are commonalities among the share of respondents who did not experience a seamless transition (25%): the lack of a pre-existing secure remote access solution aside from a VPN (20%), and the lack of a pre-existing cybersecurity plan to manage a disruptive scenario such as COVID-19 (25%). This suggests both factors are essential for organizations to adapt quickly and safely.

Organizations building resilience with cybersecurity leaders, technology at the helm

- Organizations have learned from the experience and are prioritizing cybersecurity. 86% are confident their organization is prepared, from a security standpoint, for another major disruption in the future. 88% said their crisis-response plan has been updated to reflect a more dispersed workforce.
- CISOs and cybersecurity executives are leading the way in building resiliency and enabling newly distributed teams. 83% report their head of cybersecurity has provided new training or encouraged the development of new skills related to working in a more dispersed organization.
- The role of technology is paramount. By far, organizations' top cybersecurity priority during the pandemic has been implementing new technology solutions (54%).

INTRODUCTION

Since the World Health Organization characterized COVID-19 as a global pandemic in March 2020, digital transformation has accelerated dramatically, driving a surge in the convergence of information technology (IT) and operational technology (OT) networks. More employees began working remotely and companies were forced to move extremely fast on everything from online collaboration tools to secure remote access. This has created a perfect storm situation: Legacy OT devices – never designed for Internet connectivity – are now connected, the attack surface has expanded, and opportunistic adversaries are stepping up attacks. It's become extremely clear that security is a foundational component of digital transformation. To reduce exposure, IT and OT teams must collaborate to create a new normal and prepare for a post-pandemic future.

Even though less than a year has passed since we conducted our last survey, the world has changed significantly. So, we decided it was time to update our report released in March, "The Global State of Industrial Cybersecurity." This time around, we surveyed both IT and OT security professionals at large enterprises who own, operate, or otherwise support components of critical infrastructure, with a focus on how their concerns, experiences, and attitudes have shifted since the pandemic began.

Questions centered on:

- Overall threat level during the COVID-19 pandemic
- The convergence of IT and OT networks
- How respondents have adapted to the disruption
- Building resilience and moving forward

While we asked many new questions in this latest survey, one question we started with again was:

Q1. What do you think has the potential to inflict more damage (during the COVID-19 pandemic) – a cyberattack on critical infrastructure or an enterprise data breach?

A cyberattack on critical infrastructure					
68.82%	GLOBAL 2020		75.50%	GLOBAL 2019	
An enterprise data breach					
31.18%	GLOBAL 2020		24.50%	GLOBAL 2019	

A majority of respondents are still more concerned about cyberattacks on critical infrastructure versus an enterprise data breach. While survey results point to an increased focus on OT security and preparedness as IT and OT networks become more interconnected during the COVID-19 pandemic, they also reveal an increase in targeted attacks and challenges in collaboration between IT and OT teams as organizations shift to working remotely. In this report we explore this perfect storm situation and strategies to weather it.

METHODOLOGY

Claroty contracted with Pollfish to conduct a survey of IT and OT security professionals in countries including the United States, the United Kingdom, France, Belgium, Germany, Austria, Switzerland, Australia, New Zealand, and Singapore. Only individuals who work full time in cybersecurity or information security completed the survey, for a total of 1,100 respondents. The survey was completed in August 2020.

KEY FINDINGS

I. Overall threat level during the COVID-19 pandemic

Not surprisingly, respondents believe that the overall threat level during the COVID-19 pandemic has increased.

Q2. Is your organization more or less of a target for cybercriminals since the COVID-19 pandemic began?

More of a target

55.00% GLOBAL | 51.40% U.S.

Less of a target

20.45% GLOBAL | 23.60% U.S.

There hasn't been a change

24.55% GLOBAL | 25.00% U.S.

Further substantiating this finding, organizations also report they have experienced more cyber threats since the pandemic began, with new tactics being used.

Q3. Has your organization experienced more cybersecurity threats, compared to the months before the COVID-19 pandemic began?

Yes, we've seen more threats

56.36% GLOBAL | 52.80% U.S.

No, we've seen fewer threats

17.55% GLOBAL | 18.80% U.S.

We've seen the same level of threats

26.09% GLOBAL | 28.40% U.S.

Q4. Have you seen cybercriminals carrying out new tactics to target your organization since the start of the COVID-19 pandemic?

Yes, we've seen new tactics

69.82% GLOBAL | 67.00% U.S.

No, we have not seen new tactics

30.18% GLOBAL | 33.00% U.S.

Notably, when compared to other regions, threat levels for Australia and New Zealand (ANZ) and Germany, Austria, and Switzerland (the DACH region) appear to be much higher. A greater percentage of respondents from the two regions report being more targeted (68% and 64% respectively), experiencing more threats (70% and 75%), and seeing new tactics (74% and 80%) since the pandemic started.

Finally, in terms of the threat landscape, survey results show that the old adage "attackers don't discriminate" continues to hold true.

Q5. Which sector has been the most vulnerable to a cyberattack since the start of the COVID-19 pandemic?

Pharmaceutical		
14.09% GLOBAL	12.40% U.S.	
Oil & gas		
13.45% GLOBAL	8.80% U.S.	
Electric utilities		
13.45% GLOBAL	12.60% U.S.	
Manufacturing		
12.55% GLOBAL	15.40% U.S.	
Building management systems		
12.00% GLOBAL	12.80% U.S.	
Consumer goods		
10.73% GLOBAL	12.00% U.S.	
Food and beverage		
8.82% GLOBAL	10.00% U.S.	
Air transportation		
8.64% GLOBAL	8.80% U.S.	
Rail transportation		
3.18% GLOBAL	4.00% U.S.	
Water		
1.91% GLOBAL	1.80% U.S.	
Other		
1.18% GLOBAL	1.40% U.S.	

On a global basis, five industrial sectors are quite close together at the top of the list – pharmaceutical, oil & gas, electric utilities, manufacturing, and building management systems. With no consensus regarding which industrial sector has been the most vulnerable since the start of the pandemic, this could indicate that they are all equally at elevated risk. This assertion is supported by the July 23, 2020 alert issued by the U.S. National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), which includes broad warnings of an imminent and serious threat across all 16 critical infrastructure sectors, and lengthy, detailed sets of recommendations for how to protect OT environments.

Most regions followed similar patterns, identifying three to five industries clustered closely toward the top of the list. The exceptions are the DACH region, where oil & gas clearly holds the top spot at 36%, and Singapore, where pharmaceutical is at 22%. Both results likely reflect industry sectors of particularly elevated interest in those regions; the much publicized Nord Stream II pipeline from Russia to Germany is nearing completion and eight of the world's top 10 pharmaceutical companies have facilities in Singapore.

Q6. Has your job become more or less challenging during the COVID-19 pandemic?

More challenging	
72.27% GLOBAL	68.80% U.S.

Less challenging	
11.00% GLOBAL	11.60% U.S.

No change	
16.73% GLOBAL	19.60% U.S.

Given the threat levels and observations during the pandemic, it is not too surprising that a large majority of IT and OT security professionals report their jobs have become more challenging, with even more respondents from ANZ (85%) and the DACH region (80%) finding their jobs more challenging during this period.

II. The convergence of IT and OT networks

While IT and OT convergence unlocks business value in terms of operations efficiency, performance, and quality of services, it can also be detrimental because threats – both targeted and non-targeted – now have the freedom to move from IT to OT environments. The potential risk is high, as nearly every respondent reports their IT and OT networks are interconnected at least partially.

Q7. To what degree are your IT and OT networks interconnected?

Completely	
51.27% GLOBAL	48.20% U.S.

Partially	
46.18% GLOBAL	49.60% U.S.

Not at all/siloed	
2.55% GLOBAL	2.20% U.S.

Of note, a particularly large concentration of respondents from ANZ (64%) and the DACH region (66%) report complete connectivity.

COVID-19 has clearly had an impact on IT/OT convergence, as a majority say that their IT and OT networks have become more interconnected since the pandemic began and more than 75% expect they will become even more interconnected as a result of the pandemic. Clearly this indicates the need to remain ever vigilant to the increased risk of threats to OT networks and secure them.

Q8. Have your IT and OT networks become more interconnected since the COVID-19 pandemic began?

Yes, more connected	
67.36% GLOBAL	65.00% U.S.

No, less connected	
10.00% GLOBAL	11.40% U.S.

No change	
22.64% GLOBAL	23.60% U.S.

Q9. Looking ahead, do you feel that your IT and OT networks will become more interconnected as a result of the COVID-19 pandemic?

Yes, more connected	
77.09% GLOBAL	72.60% U.S.
No, less connected	
8.55% GLOBAL	11.00% U.S.
No change	
14.36% GLOBAL	16.40% U.S.

The impact of COVID-19 on interconnectedness is even higher in ANZ (80%), the DACH region (79%) and Singapore (71%), and expected to grow to 91% in ANZ, 85% in the DACH region, and 82% in Singapore.

Finally, as IT/OT convergence accelerates, collaboration between IT and OT teams is critical to bridge the IT/OT security gap, yet a majority of respondents are finding collaboration more challenging right now.

Q10. Have the IT and OT teams within your organization found it more or less challenging to collaborate during the COVID-19 pandemic?

More challenging	
65.55% GLOBAL	62.80% U.S.
Less challenging	
13.73% GLOBAL	14.60% U.S.
No change	
20.73% GLOBAL	22.60% U.S.

Q11. How would you compare the security of your organization's IT and OT networks?

IT networks more secure than OT	
47.18% GLOBAL	44.80% U.S.
OT networks more secure than IT	
14.91% GLOBAL	14.20% U.S.
IT and OT networks equally secure	
37.91% GLOBAL	41.00% U.S.

It is worth highlighting that more than 78% of respondents in ANZ and the DACH region are finding collaboration more challenging. This is especially problematic given that more respondents from ANZ (60%) and the DACH region (62%) report an IT/OT security gap in their organizations. Such disparity points to even greater need for IT/OT collaboration in these regions.

III. Adapting to disruption

Within days of COVID-19 being labeled a global pandemic, organizations began to shift to a remote workforce. The study reveals that for the majority of organizations the shift was seamless, but roughly a quarter experienced some sort of difficulties. This can be attributed partially to the lack of a secure remote access solution (aside from a VPN) at the start of the pandemic, as well as a lack of a plan to manage such a scenario.

Q12. Did your organization seamlessly shift to remote work?

Yes, the transition was seamless	
67.91% GLOBAL	66.60% U.S.
No, the transition was not seamless	
25.45% GLOBAL	26.00% U.S.
My organization didn't experience a shift to remote work	
6.64% GLOBAL	7.40% U.S.

Q13. Aside from VPN, did your organization have a solution in place before the COVID-19 pandemic began that allowed employees to securely work from a remote location?

Yes, we already had a solution in place	
80.09% GLOBAL	77.20% U.S.
No, we did not have a solution in place	
19.91% GLOBAL	22.80% U.S.

Q14. Did your Chief Information Security Officer (CISO) or top cybersecurity executive have a pre-existing plan in place to manage a scenario like the one we've experienced with the COVID-19 pandemic?

Yes, there was a plan	
67.00% GLOBAL	66.20% U.S.
No, there was no plan	
24.09% GLOBAL	25.40% U.S.
I'm not sure	
8.91% GLOBAL	8.40% U.S.

No one could have predicted the global and long-term disruption of the pandemic on nearly every aspect of life. But a greater share of respondents from France (48%) and the U.K. (39%) report there was no pre-existing plan in place, or they were not aware of one. The good news is that organizations have learned from the experience – respondents overwhelmingly report that they have updated their plans and will be ready for a similar event in the future.

Q15. Do you believe that your organization is prepared, from a cybersecurity standpoint, for the possibility of another major disruption?

Yes, we are prepared	
86.45% GLOBAL	84.40% U.S.
No, we are not prepared	
13.55% GLOBAL	15.60% U.S.

Notably, respondents from ANZ and the DACH region share an even higher level of confidence in their ability to handle a similar disruption in the future – at 94%. This likely corresponds to the fact that both regions reported higher levels of preparedness from the start. However, even in France and the U.K, where fewer respondents report having a plan from the beginning, 83% of respondents from each region now say they are prepared for another major disruption. Many organizations are using this period as an opportunity to emerge stronger – a silver lining amidst the pandemic, for which we see additional evidence in the next section.

IV. Building resilience

CISOs and their teams have been in the spotlight since the COVID-19 pandemic, and their work has never been more important. The majority of respondents around the globe laud their organization's cybersecurity leadership and feel they are prioritizing the right things. From encouraging training and skills development to prioritizing the implementation of new technologies and updating crisis response plans, cybersecurity leaders are helping their companies to build resilience as changes, such as a more dispersed workforce, will remain for the foreseeable future.

Q16. How would you grade your CISO or top cybersecurity executive's leadership throughout the COVID-19 pandemic?

Good leadership		
61.55% GLOBAL	60.40% U.S.
Average leadership		
35.00% GLOBAL	34.60% U.S.
Below-average leadership		
3.45% GLOBAL	5.00% U.S.

Digging deeper, more respondents from ANZ (74%) and the DACH region (73%) gave their CISOs good marks for leadership than any other region. Also demonstrating strong support for CISOs, in the UK only 2.5% of respondents said they felt there had been below-average leadership during the pandemic. ANZ was the only region where not a single respondent gave a "below average" score.

Based on the answers to the next four questions, CISOs and organizations are prioritizing security and preparedness.

Q17. Has your organization updated its cybersecurity crisis response plan to reflect a more dispersed workforce?

Yes, we've updated our crisis response plan		
88.36% GLOBAL	88.80% U.S.
No, we have not updated our crisis response plan		
11.64% GLOBAL	11.20% U.S.

Q18. Has your organization's leadership made cybersecurity enough of a priority during the COVID-19 pandemic?

Yes, it has		
85.91% GLOBAL	86.40% U.S.
No, it has not		
14.09% GLOBAL	13.60% U.S.

It is interesting to note that at opposite ends of the spectrum, only 5% of respondents from ANZ say their leadership has not made cybersecurity enough of a priority, whereas 20% of respondents from the U.K. said their leadership has not. While respondents in the U.K. gave their CISOs high marks, as noted in Q16, they still feel their organizations can do more. This is reflected in their responses to Q14 where 39% said there was no pre-existing plan in place or they were not aware of one, and to Q19, where 22% would like more training and skills development.

Q19. Has your CISO or top cybersecurity executive provided new trainings or encouraged the development of new skills related to working in a more dispersed organization?

Yes, they have	
83.45% GLOBAL	83.80% U.S.
No, they have not	
16.55% GLOBAL	16.20% U.S.

Q20. What has been your organization's leadership's highest cybersecurity priority during the COVID-19 pandemic?

Implementing new technology solutions	
53.97% GLOBAL	55.09% U.S.
Created or updated its crisis response plan	
26.56% GLOBAL	26.62% U.S.
Hiring more staff	
10.37% GLOBAL	8.56% U.S.
Increasing team budget	
8.68% GLOBAL	9.03% U.S.
Other	
0.42% GLOBAL	0.69% U.S.

RECOMMENDATIONS FOR EMERGING STRONGER

As companies embrace distributed models and the convergence of IT and OT networks to maintain productivity and drive competitive advantage, OT security becomes foundational to success. But a combination of legacy devices connected to the internet, many more attack vectors, and opportunistic adversaries creates a perfect storm situation. The following recommendations can help CISOs securely accelerate IT/OT convergence to propel their organizations forward now and after the crisis fades.

1. Focus on OT security to enable business

The more important OT networks are to a business, the more essential effective OT security is to the success of operations. Revenue is generated and customers' lives are improved when those systems are up and running. But there is a 25+ year gap between IT security and OT security, and attempts to close that gap can be hampered by trying to apply trusted IT security best practices and technologies – many of which introduce unnecessary complexity and are ineffective or even downright harmful – in OT environments. Because most OT networks lack suitable security controls, security leaders should use the opportunity to focus on what can be executed immediately to reduce risk the most. Start by prioritizing the most important use cases and gaining full visibility into the OT environment. Granular details of all assets, sessions, processes, and corresponding risk levels help to identify threats in the network to mitigate risk and assure operational continuity and process integrity.

2. Understand the threats

Among an extensive list of specific recommendations in the aforementioned NSA and CISA alert is the deployment of threat monitoring technology. One of the biggest challenges in securing OT environments is zero telemetry and thus no visibility into OT networks. However, these networks communicate and share much more information than is typically available from IT components – the software version they are running, firmware, serial numbers, and more. OT network traffic can typically provide all the security information required to monitor for threats, so consider an asset visibility and continuous threat monitoring solution that can be implemented quickly and integrated into IT systems and workflows to increase preparedness and mitigate risk.

3. Improve collaboration

World circumstances have exposed security gaps and pushed IT and OT teams to work together to drive resolution, but good intentions only go so far. One of the longstanding barriers is that IT and OT teams have different – and in many cases, competing – priorities. Specifically, IT teams typically prioritize the CIA triad, which encompasses the three principles of confidentiality, integrity, and availability in the context of data or information and corresponding IT systems. OT teams, meanwhile, typically prioritize the principles of availability, reliability, and safety in the context of physical processes and corresponding OT systems. Yet both teams share the same desired outcome: risk reduction.

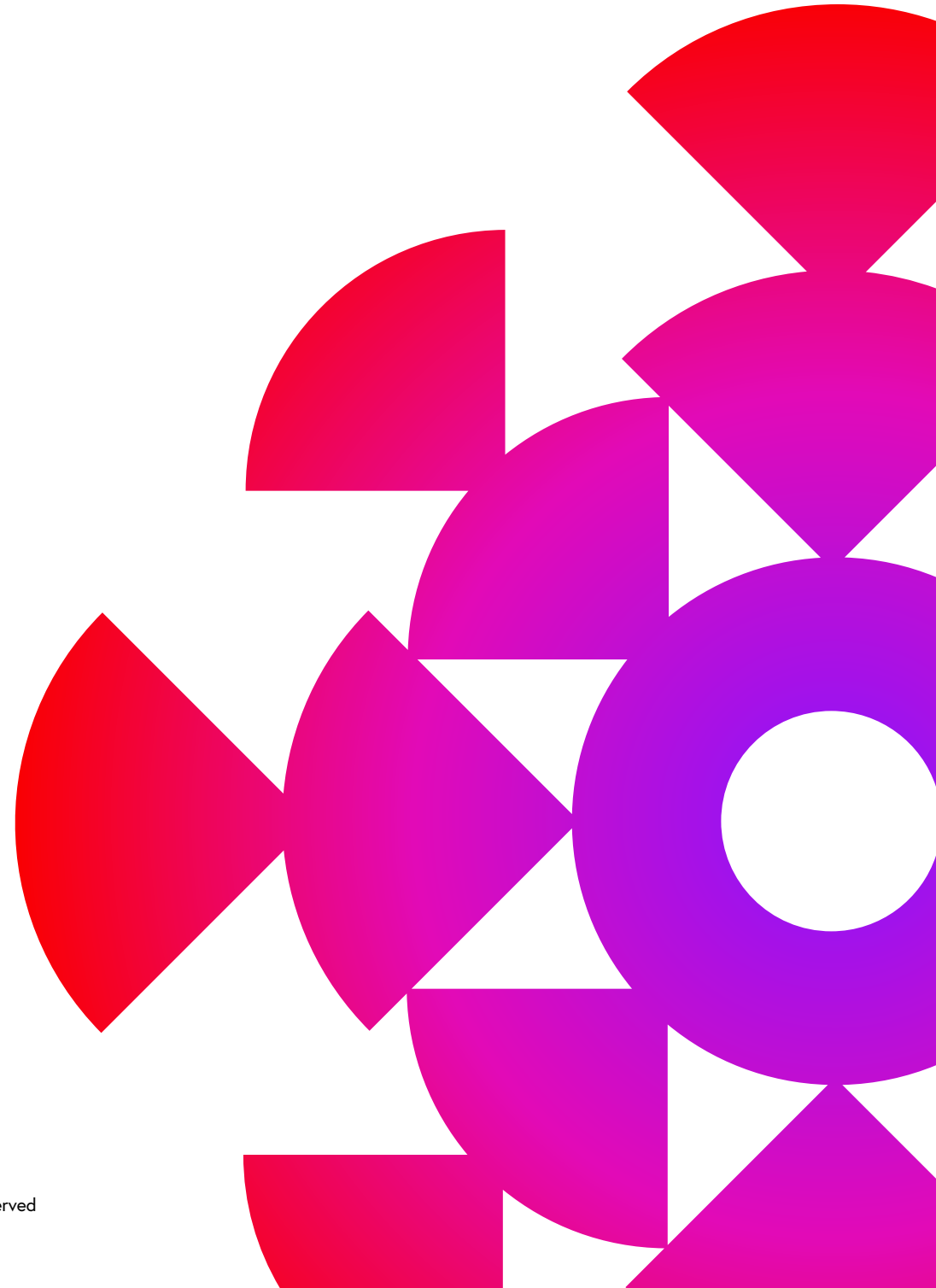
Another area that presents a challenge is the different way in which organizations and adversaries view IT and OT networks. Organizations often think of them as separate networks; but to adversaries, a network is a network, so attacks are intertwined. Solutions that enable IT and OT teams to look at OT environments together and start to identify deviations from established behavioral baselines, unauthorized connections, and the presence of adversary techniques bring the full power of the organization's resources to bear on risk mitigation. Working together toward a common goal while respecting differences enables collaboration to become concrete — not just philosophical — and organizations to become more resilient, faster.

4. Build coalitions

Don't slow down the rapid progress made during the last few months. There is no better time than now for cybersecurity leaders to garner support from the rest of the executive team for the work the security teams are doing. Many board members have been very hands-on and involved at an operational level. They have seen how being prepared and having the right technologies and processes in place are essential to enabling IT/OT convergence and creating a more resilient business, so CISOs and other security leaders should be in a strong position to garner their support.
As security teams reassess what risk looks like now and develop plans for how to focus on resiliency within the new structure in place, strong coalitions are essential to moving forward quickly.

CONCLUSION

We are living in a completely different world since March 2020 – a world that continues to evolve and will never return to its previous state. On the plus side, as organizations pivoted to a more remote workforce and IT and OT networks converged, they increased their focus on OT security and those that didn't have a plan to deal with a similar crisis have quickly put one in place. Still, IT and OT security professionals report challenges collaborating as they face higher threat levels. Fortunately, by leveraging this time to focus on OT security, understand the threats, improve collaboration, and build coalitions, organizations can accelerate IT/OT convergence with greater confidence and unlock new business value.



CLAROTY