TRACTION Guest.

Creating opportunity from crisis.

As the world begins to re-open and workplaces start calling employees back, security leaders are faced with the challenge of re-integrating their workforce and essential workers safely and securely into their facilities. With the traditional workplace posing many risks in the time of COVID-19, organizations will be faced with many questions about the future of workplace safety and how to create an environment that balances the demands of occupant safety and wellness with organizational productivity.

What lessons have been learned over the past year, and what current security trends can be applied by security professionals as they think through the next stage in their strategic plans?

Read this eBook to discover how operations, facilities, HR, and security staff are implementing solutions to support a more inclusive security approach and preparing for unknown and unforeseen threats beyond the pandemic.

In this ebook we explore:

- Current and future measures for advancing duty of care measures for employees and contingent workforces
- New safety and compliance considerations to help organizations prepare and support their workforces for the future
- Recommendations for working with the right solution partners to build organizational resilience

Table of contents.

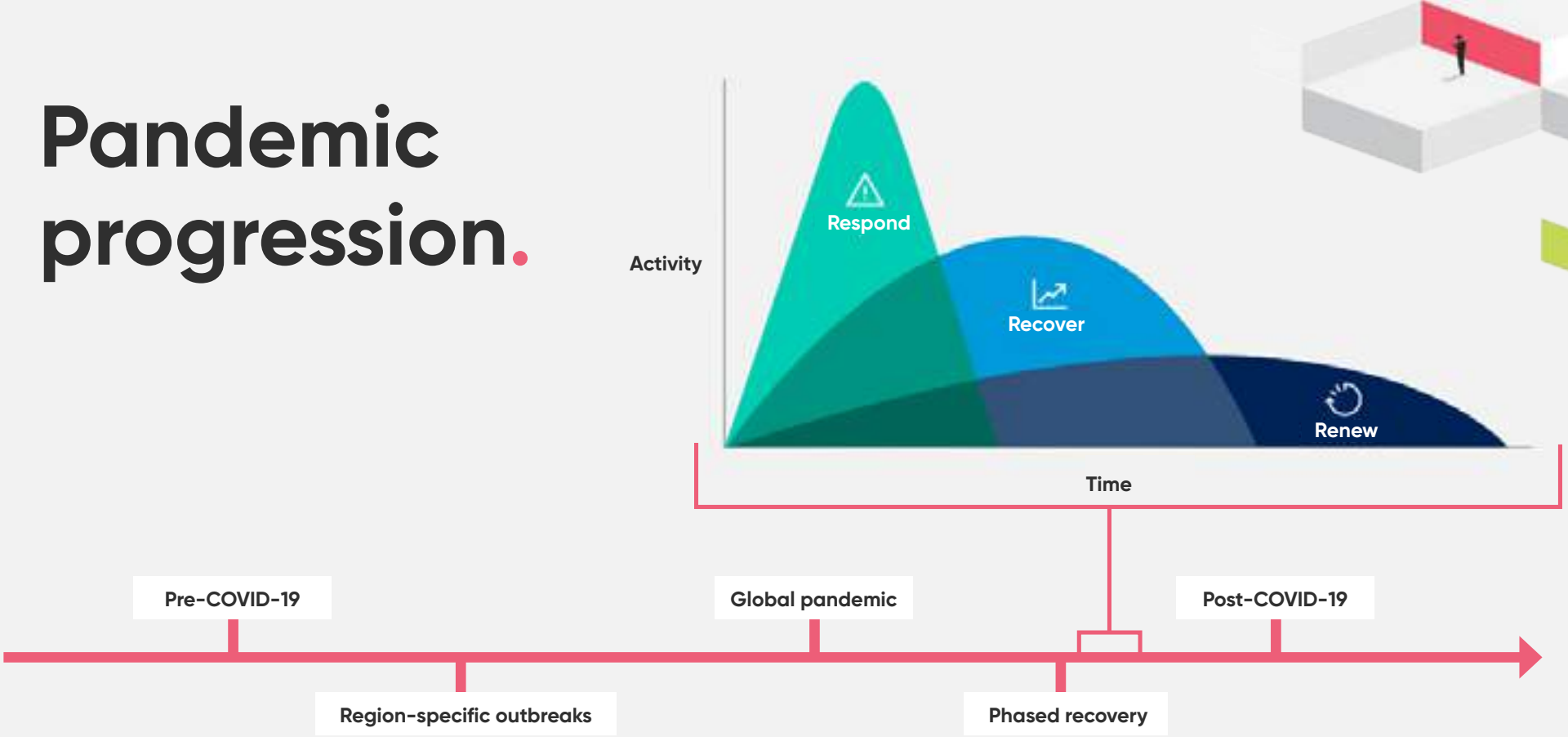
COVID-19 and the future of the workplace security.

COVID-19 brought unprecedented change to the workplace. Almost overnight, offices everywhere closed, forcing millions of workers to rapidly shift to work from home environments. Now, as vaccination rates increase globally, the promise of office re-entry is becoming an exciting reality for many. However, it's also a challenging reality for most enterprise security leaders who are now tasked with creating a new workplace environment that's responsive to the social distancing and health regulations of the COVID-19 era, while also continuing to foster productivity, collaboration, and culture.

Evolution of the pandemic response in the workplace

Before we can talk about where the workplace is headed, we need to first take a quick look at where we have been since COVID-19 first struck in 2020.

Pandemic progression.



According to Gartner, the pandemic has and will continue to progress through three major phases: respond, recover, renew. When the pandemic first hit, organizations reacted as they would to any crisis — by going into immediate 'response' mode. Incident management teams were quickly mobilized to help 'put out the fire' while, simultaneously, heavy government regulation forced rapid office and workplace closures around the world. All attention and energy were placed on squashing COVID-19 and as a result, everything, everywhere, was shut down almost overnight.

Following this initial response phase, we then moved into the second pandemic progression phase or the 'recovery' phase (most of the world is currently in this phase). In the recovery phase, we've begun to see a gradual easement of restrictions in many areas, while other areas continue to oscillate between escalation and de-escalation of restrictions depending on current virus caseloads.

So, what's next in this recovery phase and beyond into the 'renewal' phase? While no one can answer the question with 100% certainty, it is likely that new and permanent regulations will be implemented, but for the most part, heavy government mandates will begin to fade out of the picture during the renewal phase. Beyond that, it will ultimately come down to individuals and organizations to rethink everything about the future of work — from where we work, to how we work, and who is coming into work

Rebuilding the workplace: Creating opportunity from crisis.

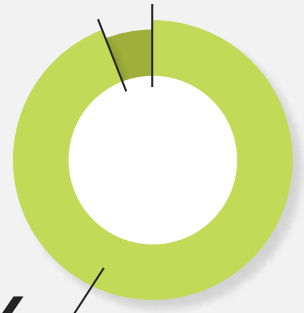
As most security professionals know, from every crisis comes opportunity. In the case of COVID-19, organizations can become more proactive in their security efforts to foster a more agile, productive, and ultimately more resilient workplace.

> **The COVID-19 crisis has created an imperative for companies to reconfigure their operations — and an opportunity to transform them. To the extent that they do so, greater productivity will follow.**

Further underscoring the importance of security in the future of the workplace, let's turn quickly to findings from our recent employee survey. After surveying some 300 employee stakeholders we found that over 90% say that physical security is of greater importance than before the pandemic. Further, this importance is also being embraced by the C-suite with over 60% of respondents saying that there is heightened participation from executives with the organization's security function and nearly 90% of respondents report a planned increase in physical security spending.

(Re)newed imperative.

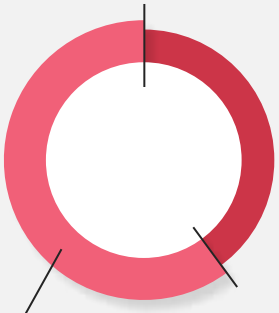
Physical security is a strategic imperative.



92%

of professionals say physical security is of greater strategic importance now than it was before the pandemic

And with opportunity, comes attention.

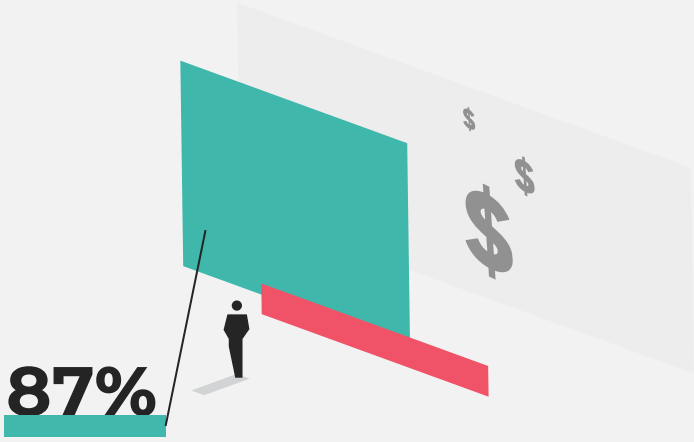


62%

of respondents cited the frequency of interaction between C-level executives and the physical security function is higher than before COVID-19

And funding/staffing.

Physical security spending on the rise.



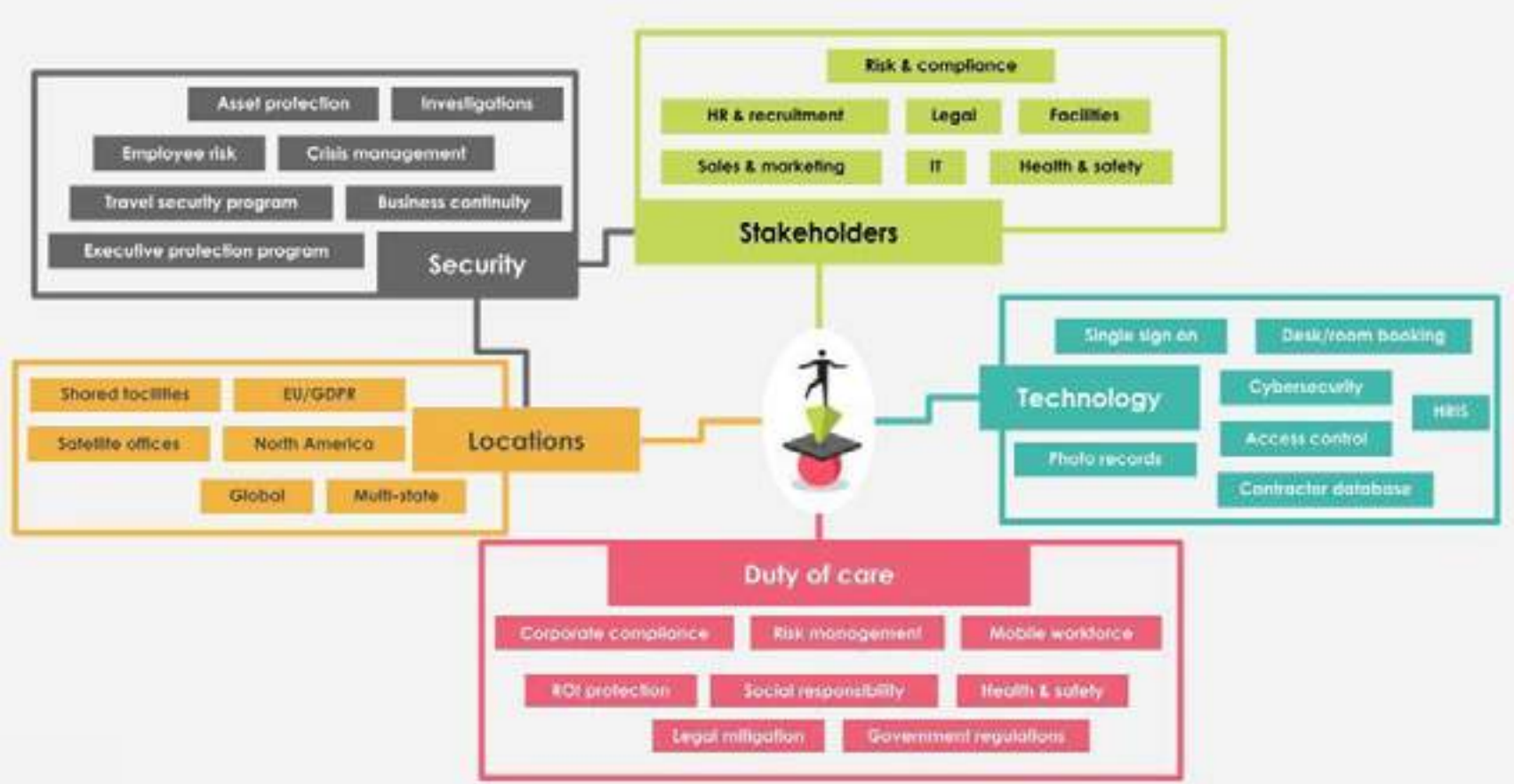
87%

of companies plan to increase spending on physical security

The expanding role of security leaders

Let's now explore how we as organizations can collectively transition from crisis mode into opportunity mode. Moving ahead, security professionals will play a central role in not only the day-to-day operations but also the high-level and future planning strategic efforts of an organization.

As the graphic below illustrates, security leaders will now take a central role in most organizations and will likely begin working regularly with a larger group of internal stakeholders. Within this expanded role, the security leader will play a central role in facilitating cross-departmental collaboration, safety technology implementation, and ensuring the new standards of duty of care are upheld.



Rise of the enterprise security risk management model.

While the Enterprise Security Risk Management Model (ESRM) has been a common practice for many organizations already, many have yet to implement it. The challenges brought on by COVID-19 have certainly highlighted the value of the ESRM, and for those who have yet to use it, now is the perfect time to formally integrate it.

Enterprise security risk management.

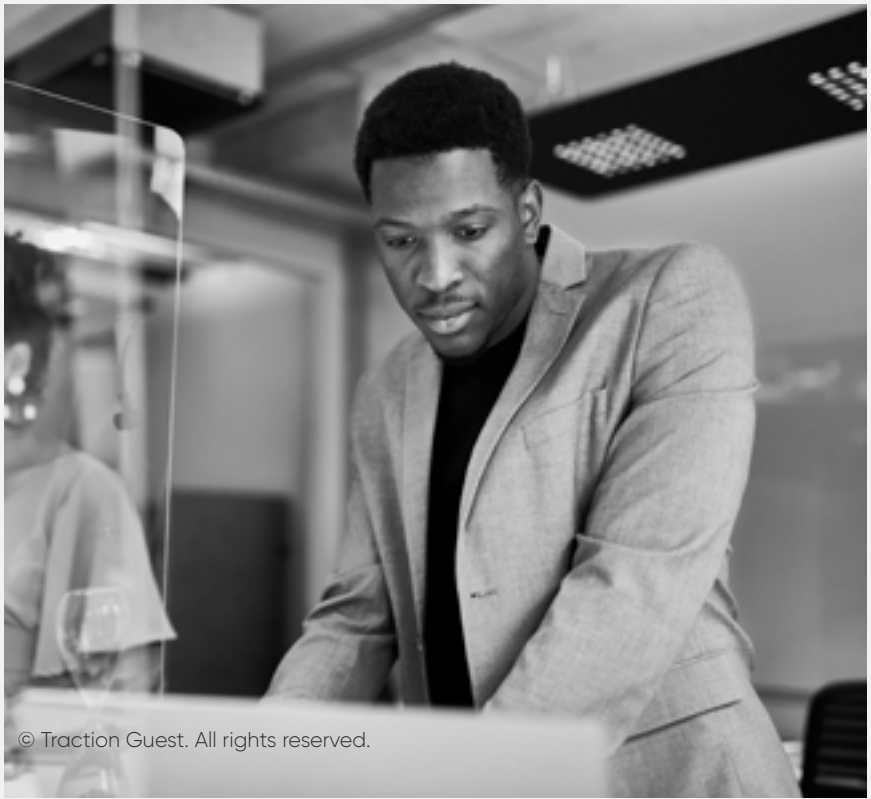
What is ESRM?

For those of you not familiar with ESRM, it's considered a strategic approach to security management that connects a business' security practices to its mission, vision, and goals using established and accepted risk management principles.

According to ASIS International, the ESRM aligns organizational responsibilities, risks, and mitigation efforts and provides a consistent practice of risk-based security management that benefits organizations and their security functions.

Getting started with ESRM

Typically, when organizations utilize the ESRM framework, it's standard practice to start at the top of the cycle (in the 'Identify & prioritize assets' phase) and move through in a clockwise motion. However, given how heavily COVID-19 impacted all organizational practices, we suggest starting at the far-left phase at 'Continuous improvement.'



Continuous improvement phase

For organizations just getting started with ESRM, continuous improvement is a great place to start as it will basically serve as one large post-incident review. Here, you'll take into account everything that happened since the pandemic struck until now. The findings you document will then serve as a baseline that will reflect the challenges and realities of pandemic times and provide a basis from which to move forward and improve.

While working through the continuous improvement phase (and all ESRM phases), two key components should be kept in the foreground: stakeholder partnerships and transparency. Be sure to work closely with all of your stakeholders, both old and new, throughout the process. Be sure to also share your data with each other and remember that this is new territory for most of us. To successfully move forward, we must be transparent about our risks, what we did about those risks, and leverage the data we have in order to construct an analysis that will help us with our renewal strategies.

Identify and prioritize assets

Moving ahead in the ESRM cycle, you will next enter the identify & prioritize assets phase. The pandemic has changed our assets and risks in many ways. Take assets, for example, and specifically an organization's employees. Before the pandemic hit, many organizations utilized their Visitor Management Systems (VMS) solely to vet visitors and contractors. Since the pandemic, organizations have now broadened the use of their VMS to focus on vetting and bringing employees back into the workplace with the emphasis now on maintaining employee health and protection, while also largely blocking the entrance of visitors and contractors.

The approach to physical and environmental assets has also changed, with many organizations now undergoing radical changes to their real estate portfolios. With varying degrees of work from home scenarios now an option for many organizations, the traditional central workplace is being replaced by a number of smaller satellite offices and facilities. This shift is happening rapidly and has resulted in the increased need for these smaller facilities in a short time. In response, organizations are finding themselves pressured to quickly reorganize and reprioritize their budgets in order to meet this shift in physical and environmental asset needs.

Identity & prioritize assets.

Tangible

- Humans
  - New health risk - personal time comes into play
- Physical assets
  - Smaller satellite offices vs large HQ building
- Environmental
  - Working from home
  - Working from anywhere

New risk considerations

With many employees now working from home, organizations need to calculate the off-site equipment and risks required to enable this sort of work scenario. In the near future, as restrictions ease, many work from home employees will want opportunities to work outside their homes. This could include co-workspaces with other companies, local coffee shops, and other public areas.

These new work scenarios will of course create a new range of risks. Cyber crime, for example, is now a heightened risk with employees fragmented across a mix of private residential and public spaces. As such, new strategies will need to be deployed that educate employees about these risks while also proactively preventing such cyber crimes from occurring, regardless of where an employee may be working from.

Insider threats are another big concern that must be mitigated. With employees potentially working in co-work and public spaces in the near future, strategies will need to be developed to ensure employees don't inadvertently disclose sensitive materials to outsiders (through verbal communication or simply leaving sensitive information on an unsupervised computer screen).

Workplace violence is another major consideration moving into the future. As many disheartening news headlines have revealed, the pandemic has exposed many employees to volatile situations at home. From isolation-related depression to the outcomes of increased substance abuse, many employees are facing difficult scenarios due to the blurred work-home setting.

As such, employers must develop strategies to mitigate this risk in a way that supports the well-being of their employees in these new environments. That said, employees have a reasonable expectation of privacy in their own homes, even if they are working in them.

Because of this, immediate countermeasures will not be available for all of these risks, however, organizations still have the duty of care to now evaluate them.

New risk considerations.

The evolving duty of care model.

Let's now take a look at the concept of 'duty of care' and how it applies to the evolving workplace context.

By definition, duty of care is the obligation of an organization to assume responsibility for protecting its employees from risks and threats while working and is widely protected within the legislation of many countries.

Many items are covered under the duty of care umbrella and include health and safety, corporate compliance, adherence to government regulations, and social responsibility to name a few. As a result of COVID-19, there will likely be some gaps between acceptable pre-pandemic levels of duty of care and the levels that will be necessary upon return to the workplace. Traditionally, many organizations have looked at duty of care programs as too great an expense to fully implement. But in the wake of COVID-19, perspectives are greatly shifting as organizations are now realizing the risk of avoiding duty of care strategies is far too great to carry on any longer.

In the pandemic and post-pandemic eras, effective duty of care programs will not only be essential in terms of keeping production running, but they will also be an essential part of the overall employee retention strategy.

Duty of care in the new norm.

The obligation of organization to assume responsibility for protecting their employees from risks and threats when working.

The responsibility of organizations to look after their employees is widely protected within the legislation of many countries.

Security is now the strategy.

Looking ahead, security will become a critical and central business strategy for most organizations and will see greater interest and participation from the C-suite. Teams will need to get deeply collaborative with the entire organization in order to build agile and holistic security strategies that adapt to new and shifting external challenges. As part of that strategy building, teams should start by answering the following five questions:

1. **Arenas:** What function and scope will each area of business take on to ensure organizational security?
2. **Vehicles:** What tools will be used to achieve our security goals? And how will we use them?
3. **Differentiators:** How are we going to measure our success? (This is where you'll show the ROI of the tools you're using).
4. **Staging:** What are our priorities and sequence of events?
5. **Logic:** What is our risk vs. reward tolerance? This risk may call for a prison-style security program but the organization's operability may require the program to be much more flexible.

Summary.

The COVID-19 pandemic dramatically altered the workplace as we know it for the foreseeable future. For some organizations, the impact has resulted in a complete and permanent shift to remote work. Meanwhile, others are considering a hybrid model that blends remote and on-site work or a complete return of staff to the on-site workplace.

As a result, security leaders will be required to engage like never before and will become a central business figure in an organization's strategic forward movement.

About Traction Guest.

Traction Guest, the leading Visitor Management platform for addressing complex people entry requirements, empowers businesses to reimagine how they provide safe and secure workplaces for employees, contractors, and essential visitors.

Global brands across five continents and dozens of industries trust Traction Guest's highly customizable platform to mitigate risk and deliver unparalleled security through an intuitive, touchless, highly-branded experience that supports compliance, employee engagement, and duty of care requirements.

TRACTION Guest.