ACCELERATED DIGITAL TRANSFORMATION

In the post-pandemic era:
a catalyst for security transformation

SKYBOX SECURITY

See the bigger picture

CONTENTS

Digital transformation marks a radical rethinking of how an organization uses technology, people and processes to fundamentally change business.[1]

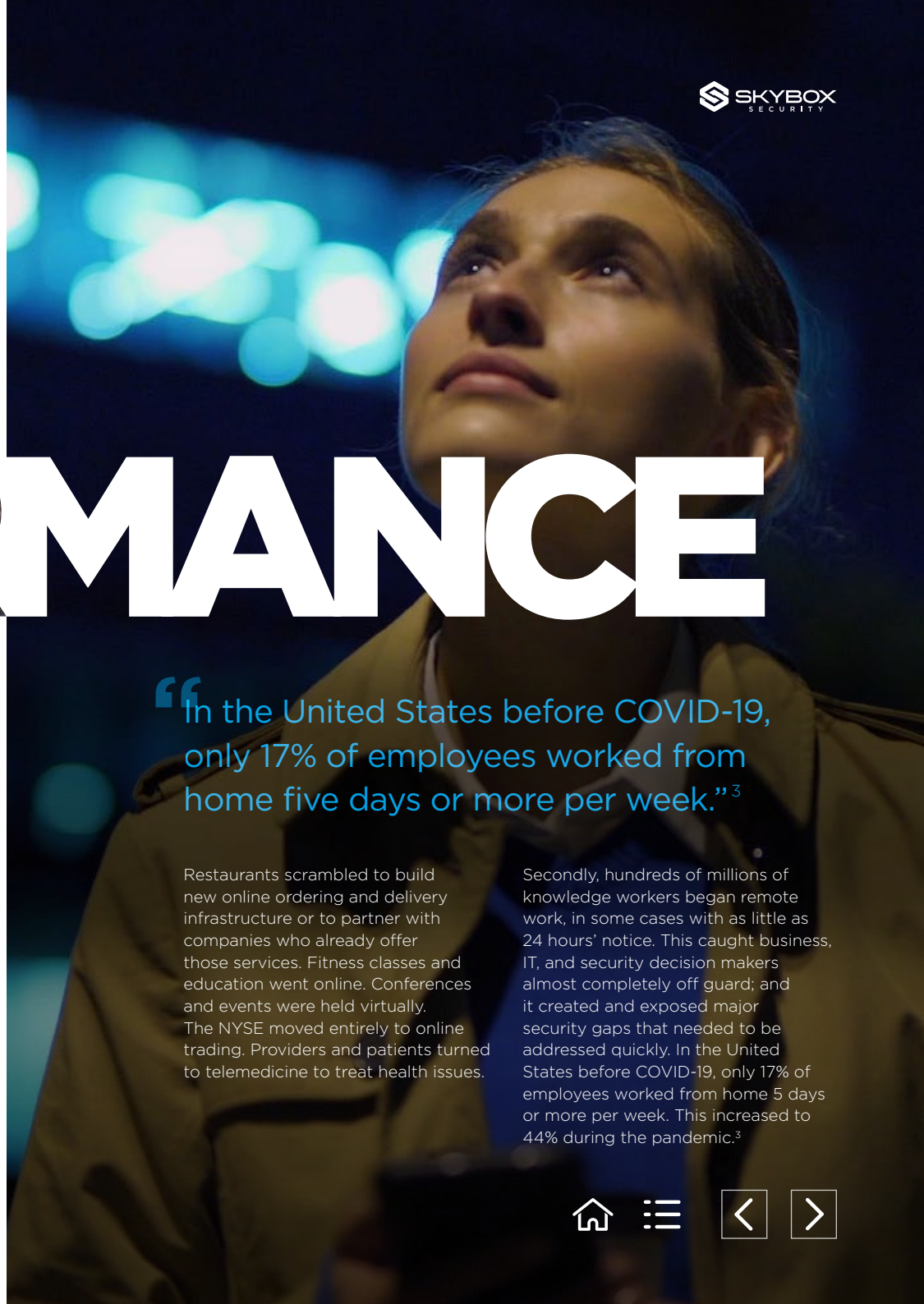
PERFORMANCE

It has been a leading priority for the C-suite for many years, but the trend toward digital transformation has accelerated as a result of two fundamental changes wrought by the COVID-19 pandemic.

Firstly, the lockdowns rapidly accelerated the need for businesses to find new ways to engage with customers and supply chains. While digital transformation has been important for years, many decision-makers now view it as essential to the survival of their businesses and maintenance of their revenue streams.

In an effort to survive and get back to business safely, companies have rapidly adopted services such as contactless payment, click-and-collect applications, and enhanced customer relationship management.

Businesses have had to adapt rapidly to maintain continuity. Many industries fast-tracked their digital initiatives, and organizations of all types turned to digital platforms to provide goods and services. In particular, omnichannel commerce exploded during COVID-19 lockdown with e-commerce spending surging by78% in May 2020 over May 2019.[2]



"In the United States before COVID-19, only 17% of employees worked from home five days or more per week."[3]

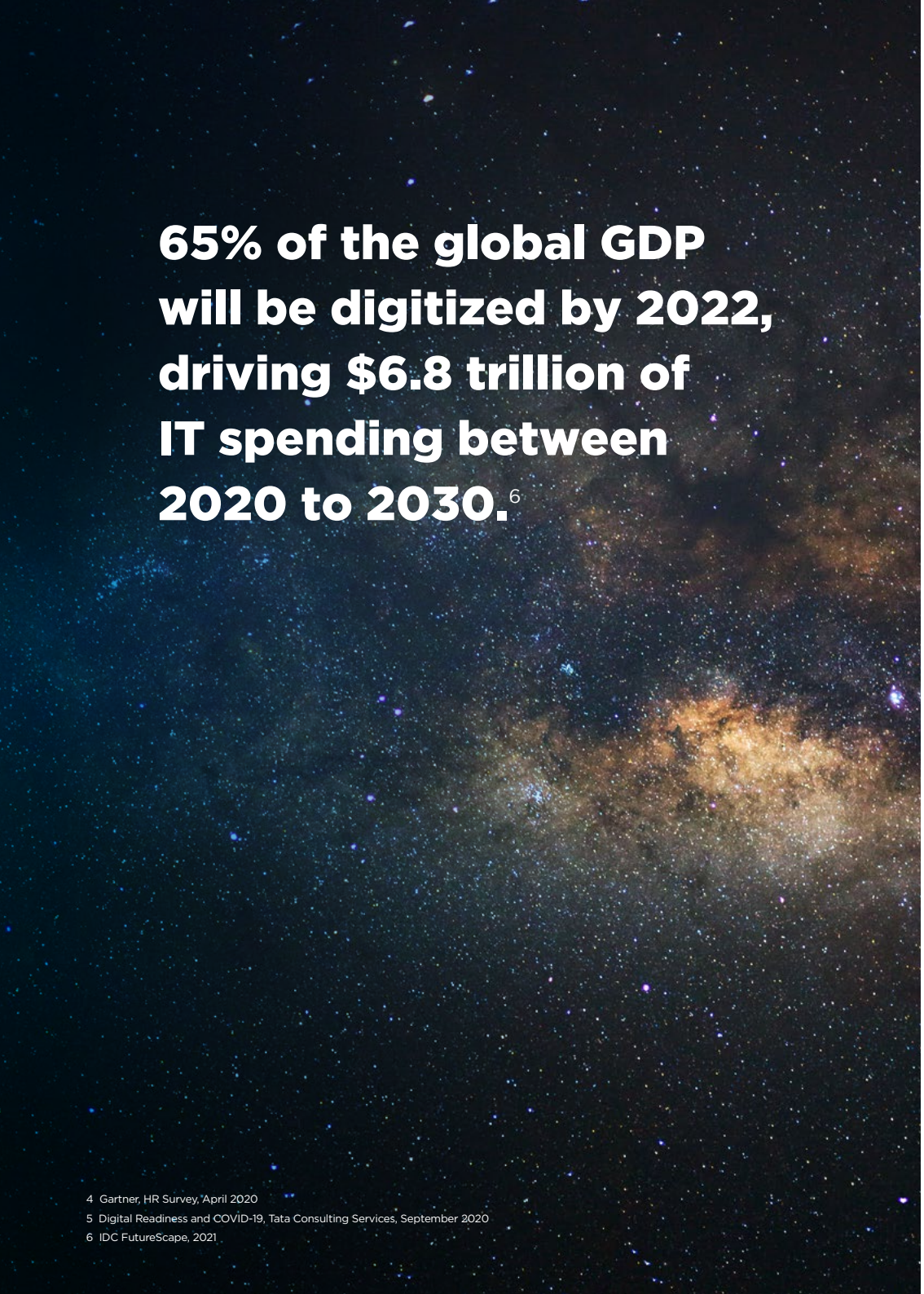
Restaurants scrambled to build new online ordering and delivery infrastructure or to partner with companies who already offer those services. Fitness classes and education went online. Conferences and events were held virtually. The NYSE moved entirely to online trading. Providers and patients turned to telemedicine to treat health issues.

Secondly, hundreds of millions of knowledge workers began remote work, in some cases with as little as 24 hours' notice. This caught business, IT, and security decision makers almost completely off guard; and it created and exposed major security gaps that needed to be addressed quickly. In the United States before COVID-19, only 17% of employees worked from home 5 days or more per week. This increased to 44% during the pandemic.[3]

1 Leading Digital, Turning Technology Into Business Transformation, 2014

2 2020 Digital Economy Index, Adobe, 2020

3 Change in remote work trends due to COVID-19 in the United States in 2020, Statistica 2020



65% of the global GDP will be digitized by 2022, driving $6.8 trillion of IT spending between 2020 to 2030.[6]

A Gartner survey of HR leaders revealed that nearly half of organizations reported 81% or more of their employees are working remotely during the coronavirus pandemic. Gartner analysis reveals that post-pandemic, 41% of employees are likely to continue working remotely at least some of the time.[4]

These two factors, working together, have led to a boom in digital transformation spend, with Tata Consultancy pointing to 90% of organizations either maintaining or increasing their transformation budgets despite 68% of companies experiencing revenue declines amid COVID-19.[5] Further, IDC predicts that 65% of the global GDP will be digitized by 2022, driving $6.8 trillion of IT spending between 2020 and 2030.[6]

For the Chief Information Security Officer (CISO) and their security team this means they now have a lot more to protect – more access points to configure, more technologies to secure, and more changes to properly validate. As the deployment of new digital transformation initiatives continues to gather pace, it is critical to consider the security implications. Are security teams able to provide the support needed for ongoing transformation projects? How should the CISO evolve the security function to effectively enable the business? And what does theirshifting responsibilities and influence mean for the future of security within their organization?

4 Gartner, HR Survey, April 2020
5 Digital Readiness and COVID-19, Tata Consulting Services, September 2020
6 IDC FutureScape, 2021

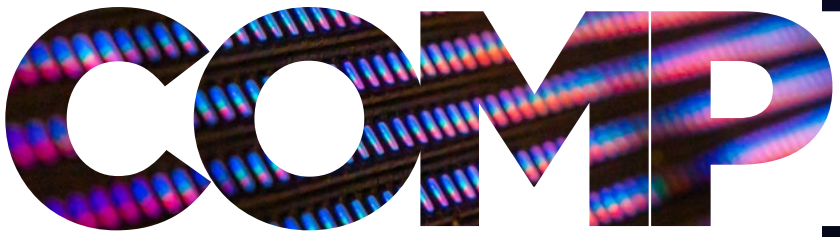
70%

of cybersecurity professionals claim their organization has been impacted by the skills shortage.[8]

Digital transformation impacts many aspects of a business: how their employees work, how they acquire and serve customers, how they manage supply chains, and how they address competitive challenges. According to KPMG's CEO Outlook study, 75% of CEOs say the pandemic has accelerated the creation of a seamless digital customer experience, with over 1 in 5 of those saying progress "has sharply accelerated, putting us years in advance of where we expected to be".[7] Considering the rapid pace of change, it should not be a surprise that, in the same report, CEOs also ranked cybersecurity in the top three areas that pose a risk to growth.

This risk should not be underestimated. Even prior to global lockdowns, the complexity of enterprise security was becoming increasingly unmanageable. Sprawling, fragmented networks were growing ever larger with new cloud services and third-party networks introduced to the corporate environment with a regular cadence. The cybersecurity skills crisis has deepened, with 70% of cybersecurity professionals claiming their organization has been impacted by the skills shortage.[8] And the threats they face have been diversifying and increasing in sophistication at a speed that outpaces capability.

Accelerated digitalization increases security



COMPLEXITY

The distributed workforce expands the attack surface even further, rapidly increasing digital transformation needs. It equates to new and significant challenges adding to an already complex cybersecurity landscape. These issues are unlikely to abate any time soon – new technologies and services bring their own unique technical demands, and the need for the business to innovate and evolve to maintain competitive advantage is only going to gather pace. Security practitioners are under immense pressure to support new business initiatives while still working to improve overall security posture and limit opportunities for breaches. They have become the first port of call for help – but they are also the first to be blamed when something goes wrong.

> "The events of 2020 have brought about a new imperative: security by design."[7]

7 KPMG 2020 CEO Outlook: COVID-10 Special Edition, September 2020
8 ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2020

Security's role in supporting digital transformation has not always been so prominent. Prior to COVID-19, security teams were either a late inclusion in transformation projects or, in many cases, excluded from the process. This lack of inclusion has left the teams and their companies underprepared and unequipped for the massive operational shift that came with COVID-19. Where security was once considered to be a solution to deploy on top of existing infrastructure, recent events have made large organizations reconsider the role security needs to play across the business. The events of the past year have brought about a new imperative: security by design.

Race to the Cloud

Central to the increase in complexity is the unprecedented and sizeable expansion of the attack surface. Most organizations went from having on-premise networks, whether in one central hub or spread over multiple locations, to a distributed workforce introducing new ingress and egress points to corporate entities from their home networks.

Employees now access corporate networks and data stores from the same home networks that also support employees' internet-connected doorbells, home automation systems, refrigerators and gaming devices. The rapid expansion in the use of videoconferencing tools, unauthorized cloud applications, and mobile apps means malicious actors now find it much easier to exploit vulnerabilities in mainstream business tools. This is exacerbated by the fact that consumer-focused tools are not designed with an underlying foundation of security, yet they are now used for business purposes that were never designed with an underlying foundation of security.

80% of enterprises will shift to cloud-centric infrastructure and applications twice as fast as before the pandemic.[9]

The pandemic has illuminated new use cases for cloud computing by necessity, and those use cases are becoming increasingly strategic to key business objectives. However, as companies pivoted overnight to support employees and customers, they moved mission-critical applications and data stores to the cloud. The decision-making process for doing so was compressed, often without adequate consideration of the security and compliance implications that these changes would have. This also has implications for vendors and the full supply chain. As companies are more rapidly migrating to the cloud, often incumbent vendors are unable to support the migration and changes that need to be made. And the velocity of cloud migrations will only increase. IDC predicts that by the end of 2021, 80% of enterprises will shift to cloud-centric infrastructure and applications twice as fast as before the pandemic[9].

9 IDC FutureScape 2021

An exponential increase in risk

Many cloud applications, including those authorized and approved for use by corporate security departments, are not properly configured or managed by cloud providers. This by itself presents major security issues. But considering the wider threat landscape and the volume of new vulnerabilities that already stretched security teams must manage, the lack of confidence in the security surrounding cloud services, and the limited visibility into the vulnerabilities they introduce to the corporate network, it's a serious cause of concern for security practitioners. Underscoring these flaws in need of monitoring, Skybox Security analysis reports the discovery of 9,799 vulnerabilities during the first half of 2020, a 34% increase from the same period in 2019.[10] As growth in vulnerabilities is a leading indicator for future attacks, this sharp increase should not be ignored.

While rapid migration to the cloud can cause disruption, it can also force important items on the security agenda forward. For example, migration to the cloud necessitates coordination and cooperation across multiple stakeholder groups within the organization. It requires internal organizations to align towards a holistic security agenda and ensure all elements of the infrastructure are secure. This was often a struggle prior to the pandemic when other pressing business priorities, or a resistance towards transparency, caused roadblocks. Another element is the opportunity to evaluate the current tech stack and discontinue underutilized assets and components that no longer serve a critical business purpose. This streamlines business processes and resources, as well as reduces the company's footprint, to limit the amount of alerting and investigations. With fewer endpoints to manage, more valuable resources can be focused on priority and critical items.

As growth in vulnerabilities is a leading indicator for future attacks, this sharp increase should not be ignored.

10 Vulnerability and Threat Trends Report Mid-Year Update, Skybox Security, 2020

SKYBOX SECURITY

"Enterprises cannot stop the greatest organizational risks. New ransomware samples are up 72% in 1H 2020 and are exploiting multiple vulnerabilities." [10]

Flying blind

The diversity of cloud services and public, private, and hybrid cloud architectures makes visibility across cloud and physical environments a major challenge. When rushing to implement policy and rule changes during the initial stages of the pandemic, many security teams lacked the necessary network topology and configuration visibility to accurately determine and implement essential changes across on-premise and multi-cloud environments. In their efforts to enable a distributed workforce and secure their perimeter, they could have unknowingly introduced new risk. If security practitioners blindly apply changes without proper impact assessments on cyber exposure, they could increase the exposure of new vulnerabilities and further introduce systemic risk across the organization.

Financial ramifications of non-compliance are significant

Despite the macroeconomic landscape, regulatory bodies have not reduced pressure. The CISO is still responsible for preventing breaches and maintaining compliance to avoid incurring heavy fines. During the lockdown, organizations faced difficulties unifying compliance and policy effectively across both on-premises and multi-cloud networks. New technology and service deployment speed meant proper care might not have been taken to ensure full compliance. Now, the CISO needs to be concerned with ensuring the validity of all changes made during the rush to enable their distributed workforce while developing capacity and capabilities that allow them to build confidence in the compliance of any new transformation initiative.

CISOs chart

THE COURSE

Organizations that commit to robust and integrated cybersecurity capabilities will gain competitive differentiation.

COVID-19 lockdowns have raised the visibility of security as a business issue. CISOs, at the helm of security strategy, now have an unprecedented seat at the boardroom table. According to PwC research, "a majority of CISOs have interacted more frequently with their CEOs (65%) and the boards (50%) during the crisis. In 2019, only 33% of all business and IT executives said that their cyber team communicates effectively with the board and senior executives about cyber risks and adjacent risks."[11] The opportunity has arrived for CISOs to champion 'security by design,' embedding security best practices into the fabric of the organization's business strategy.

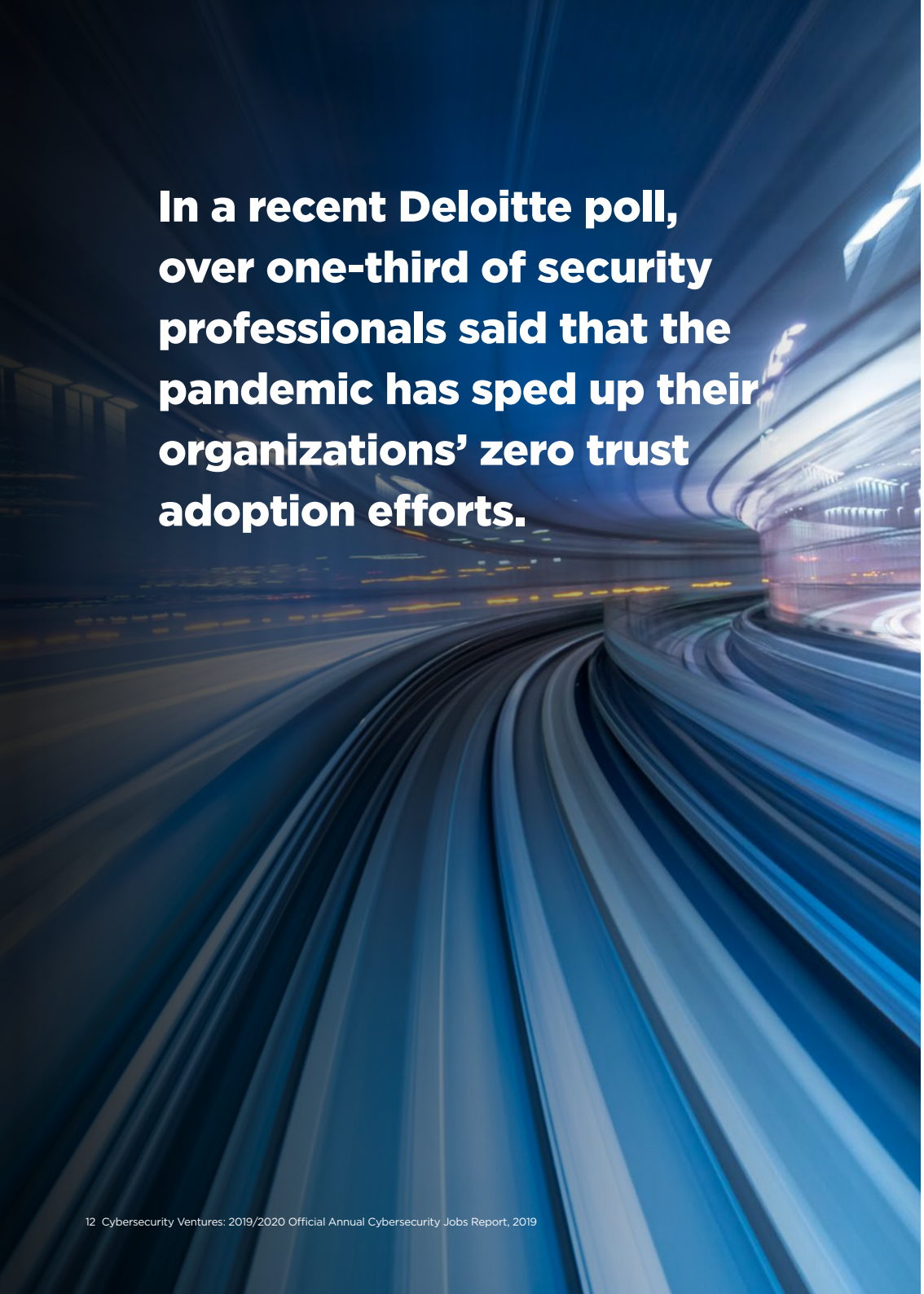
The research further emphasizes that the role of the CISO is at the precipice of significant change. "In the past, CISOs were often not included in strategic business decisions, even those with significant security and privacy implications. The pandemic may have changed all that. CISOs were significantly involved in decision-making around pandemic responses that were both operational and transformational."

> "A majority of CISOs have interacted more frequently with their CEOs (65%) and the boards (50%) during the crisis."[12]

As companies look to innovate new digital-first customer experiences and beyond, CISOs have demonstrated the importance of being in those conversations at the onset. Organizations that are ambitious about the speed and scale of their digitalization plans will be more successful if they collaborate with their security chiefs from the start.

Moreover, organizations that commit to robust and integrated cybersecurity capabilities will gain competitive differentiation, as they will be perceived as safer and more trustworthy than their competitors. Importantly, this commitment to cybersecurity will enable companies to emerge stronger and better prepared to handle future large-scale disruptions.

11 Digital Trust Insights Pulse Survey, PwC, May 2020



In a recent Deloitte poll, over one-third of security professionals said that the pandemic has sped up their organizations' zero trust adoption efforts.

12 Cybersecurity Ventures: 2019/2020 Official Annual Cybersecurity Jobs Report, 2019

Using their newfound seat at the table, CISOs must proactively address the new normal by advocating for the changes necessary to address the situation at hand:

- There is an increasingly energized and sophisticated network of bad actors
- Employees use a growing number of authorized and unauthorized cloud applications
- Organizations migrating to the cloud must also maintain mission-critical legacy applications
- Organizations must satisfy a growing set of compliance requirements
- Security professionals must deal with incomplete data sets for vulnerability management and policy management

All of the above causes a greater potential for security breaches that needs recognition at the highest levels of the company and the board. In order to accelerate digital transformation in light of the above factors, CISOs are prioritizing the following areas:

Retain talent

Digital transformation requires an organization to attract and retain the security industry's best and brightest talent. With current predictions stating that there are likely to be 3.5 million unfilled cybersecurity positions globally by 2021[12], the competition for top talent is incredibly fierce and the challenges associated with retaining staff are pronounced.

There are opportunities to turn the tide. COVID-19 is an opportunity for organizations to use the new normal 'work-from-anywhere' policies to provide the flexibility that many employees want to compete for finite talent resources.

3.5 million unfilled cybersecurity positions globally by 2021.[13]

Additionally, for those organizations that continue to have a flexible work-from-anywhere model, recruiting can become easier. Rather than bound to a location-based search, recruiters can look globally for top talent.

Build resilience

No cybersecurity solution can protect against every conceivable cyber threat. Therefore security programs must effectively mitigate damage to systems, processes, and reputation, and continue operating once those systems or data have been compromised. They need to address both adversarial threats as well as simple human error.

This includes determining who gains access to the network and how, pinpointing the most important assets and services, and ensuring all critical data is protected. It also involves identifying what controls must be updated to function in a predominately remote workforce.

Accelerate cloud adoption

Cloud services are now a prerequisite for operational agility and business continuity. While the CISO must continue to accelerate cloud adoption to support an ecosystem approach to business operations, they must also ensure that connections are safe, secure, compliant, and aligned with data governance policies. Connecting suppliers, customers, shippers and employees is more important than ever to allow all parties to work collaboratively and improve decisions. Now is the time to make hard decisions around replacing legacy technologies, expanding cloud infrastructure, and assessing new technologies.

Adopt a zero-trust framework

Accelerated digital transformation has also paved the way for more rapid adoption of zero-trust frameworks. In a recent Deloitte poll, over one-third of security professionals said the pandemic has sped up their organizations' zero trust adoption efforts.[13] Prior to the pandemic, interest in zero-trust architectures was primarily driven by a recognition that traditional perimeter-centric security models are incompatible with the way businesses work today. Zero trust has come to the forefront due to a massive volume of remote workers and the stress that this places on infrastructure, particularly VPNs.

13 Zero Trust cybersecurity: Never trust, always verify, July 2020

SKYBOX SECURITY

Using their newfound seat at the table, CISOs must proactively address the new normal.

Increase operational efficiencies

Digital initiatives provide prime ways to improve operational efficiencies. Chief among these is automation, which is fast becoming a hallmark of the smartest and most visionary organizations' approaches to cybersecurity. Companies that can automate routine tasks can free up time for other, more valuable work. CISOs at organizations that use outsourced services can offset increased workloads by adding services such as automated security orchestration and automation response tooling without needing to heavily increase staffing or budgets.

Build effective governance

The most resilient organizations have frameworks for consistent prioritization and mitigation of risk. It means security teams can stay focused on what matters most. They model and validate compliance requirements across hybrid networks, including those in a business supply chain, where data that is subject to compliance requirements is stored and processed in multiple environments. If improperly managed, the interchange of data between these networks can create additional opportunity for compliance failure.

Five steps to securing

DIGITAL TRANSFORMATION

> “Current security practices are not keeping up with the changing security landscape.”

With further acceleration of digital transformation now inevitable, security teams have some tough areas to navigate to enable all new technologies and services while concurrently reducing systemic risk across their entire organization. They need to develop a mature and tightly connected security management framework that empowers planning, implementation, and business continuity teams to collectively attain the best overall security posture.

The reality is that current security practices are not keeping up with the changing security landscape. In a post-pandemic era, what was once ‘good enough’ will no longer work.

Security teams are scrambling to determine which new rules and policies are required with the expansion of the business, but they are failing to adequately model and analyze new deployments and changes relative to network paths and configurations. Without gaining a full understanding of their attack surfaces, organizations are unable to identify and remediate potential threat vectors. Additionally, they cannot safely automate policy changes and are likely to expose their businesses to vulnerabilities and unintended risk.

This, combined with siloed vulnerability and policy management processes, contributes to systemic risk introduction across the organization. Security leaders must rethink current practices and move to adopt a secure posture-management approach. This in turn begins the journey toward transforming the way their departments function.

Key steps include:

1. Assess the environment

To transform security and be better positioned to support digitalization efforts, it is first important to assess exactly how the security environment has changed. It is likely that most organizations will find themselves with a profoundly expanded attack surface and a large volume of new, potentially insecure, network elements. Before any security practice improvements can be made and to build posture, the CISO must achieve holistic network visibility to regain control of their environment.

This can only happen if they are able to analyze and validate all network, cloud, and security configurations that sit within their environment. Such analysis should involve the aggregation and normalization of data sets, giving security leaders insight and visibility into their biggest security issues. Without first knowing what needs to be fixed, it is incredibly difficult to build the strong foundations needed to drive change within the organization.

2. Obtain visibility of cloud networks to understand overall business risk

One of the most effective ways organizations can build resilience is through increased visibility and understanding context. This allows for more informed decision making and governance. In the face of regular and inevitable changes to cloud infrastructure, organizations need to test their security and make sure it is properly safeguarded. Nothing is static. This is especially true when it comes to dynamic cloud environments. This is why it is vital for organizations to continuously monitor their environments and engage in thorough reporting. To manage exposure to risks in the cloud, they need to have visibility of their entire hybrid security environments.

Organizations should start all monitoring activities by creating an attack surface model which shows all the ways in which they are susceptible to attacks. By modeling a network infrastructure that is inclusive of vulnerabilities and threat intelligence, enterprises will have an accurate view of how susceptible they are. Other information, such as app usage, and the type of data being uploaded and shared, should also be incorporated into reports.

With this context-driven insight and visibility, actions can be accurately prioritized, moving security programs away from constant firefighting and towards developing more strategic and mature processes.

3. Secure end-to-end change management

Businesses should implement a lifecycle-focused, vulnerability management process that is tied to policy change validation. Because implementing any sort of change in a system that has already been validated can be risky, a well-considered approach to change management is essential to enabling robust security and to demonstrating compliance with data protection regulations. The policy change validation process should include discovery of vulnerabilities assessment and prioritization of these vulnerabilities, their remediation, and verification that the changes have been successful.

Prior to deploying any additional infrastructure in a network, it is critical to model and validate any and all security policy and network changes. For many businesses this would not have been possible, nor would it have been realistic during the rapid period of change during the lockdowns. They will know there are inherent problems with validating changes after the fact, and are now dealing with the reality that unwanted traffic could be introduced to the network, or that legitimate traffic from employees or customers could be blocked.

However, it is now critically important that security practitioners retroactively model and validate any changes that have been made so they are able to apply fixes where necessary.

Going forward, this needs to be built into their ongoing change management processes to greatly limit opportunities for threat actors and to protect sensitive data.

4. Focus on automation

Automation needs to focus where it can deliver the greatest value. Applied correctly, and used with contextual insight into the wider security environment, automation can alleviate pressures placed on security teams and prevent burn-out while increasing efficiency and freeing up resource for more value-adding business initiatives.

Context-aware change management has a variety of use cases. However, automating change provisioning carries the highest risk. Because this is when automation can directly impact network security. Where context is useful for other automation workflows, it is critical for change management – without this context it is possible for errors to quickly compound over a large environment, which could lead to rollbacks and could end up worsening security and compliance posture rather than improving it.

5. Supercharge process orchestration

Processes and workflows must be thoughtfully organized to ensure the security framework operates on all cylinders. Orchestration must be backed up by visibility, context, and some human interaction to prevent inadvertent security or performance issues. Orchestrating firewall change processes with analytics-driven automation, as an example, reduces the time to carry out changes by up to 80%, and avoids wasting time on rollbacks due to human error.

As the CISO tentatively considers evolving their function within the new security normal, they must prioritize the development of a program that can join together disparate elements within their environment. The sum of their technologies needs to be more than their parts – process orchestration can help integrate data from a diverse range of sources to improve overall levels of security and eliminate silos. Forward-thinking CISOs with a 'bigger picture' mentality were developing this ecosystem-led approach to cybersecurity management before the onset of the pandemic. Those that have already done the groundwork have seen how improved process orchestration can help during times of crisis.

Radical change requires
a radically new approach to

SECURITY

2020 has been a year defined by radical change. Driven by economic uncertainty and a newly distributed workforce, the corporate security function is now saddled with increased expectations and new responsibilities. However, now is not the time to bury one's head in the sand and wait for things to get better. The exponential increase in vulnerabilities, ransomware, and chained attacks indicates that 2021 will see this trend continue. Traditional approaches to managing cybersecurity based on reactive detect-and-response tactics are simply not good enough in the new security normal. To securely drive digital transformation and support new business initiatives, the CISO should seize on this moment to fundamentally change the way their department works.

Previous roadblocks have been dismantled. The CEO and company board are keenly aware of the criticality with which cybersecurity considerations be embedded into business decisions, and the communication channels are open. Security and IT teams are now working closer together than ever before due to accelerated initiatives such as cloud migration. Business continuity practices have been pushed to the brink, and many stakeholder groups have heightened sensitivity towards the importance of building business resiliency.

> "Digital transformation, accelerated by the pandemic, has now sparked a new era of security transformation."

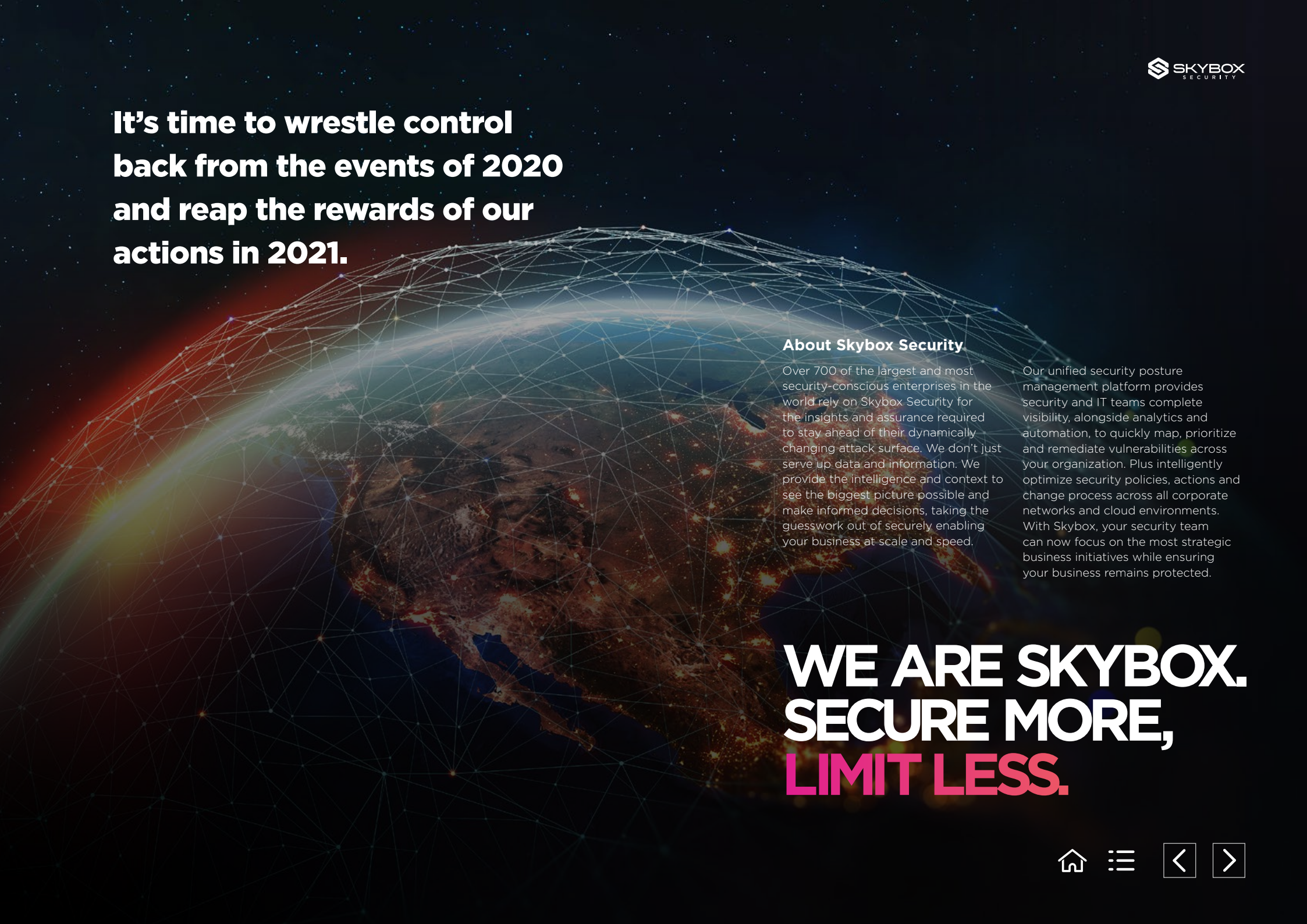
Security and IT teams are now working closer together than ever before due to accelerated initiatives like cloud migration.

The macroeconomic conditions have made it paramount that all organizations – including IT and security – look to do things better, faster, and in less-resource intensive ways than before.

Digital transformation, accelerated by the pandemic, has now sparked a new era of security transformation. Forward-thinking CISOs – those able to see the bigger picture – will capitalize on this opportunity to design a new approach to their security programs.

This will be underpinned by holistic network visibility, context -rich security environment insight, and key process automation. Winning security organizations will benefit from increased efficiencies, more time to focus on strategic initiatives, improved decision-making capabilities, and a healthier security posture.

It's time to wrestle control back from the events of 2020 and reap the rewards of our actions in 2021.



About Skybox Security

Over 700 of the largest and most security-conscious enterprises in the world rely on Skybox Security for the insights and assurance required to stay ahead of their dynamically changing attack surface. We don't just serve up data and information. We provide the intelligence and context to see the biggest picture possible and make informed decisions, taking the guesswork out of securely enabling your business at scale and speed.

Our unified security posture management platform provides security and IT teams complete visibility, alongside analytics and automation, to quickly map, prioritize and remediate vulnerabilities across your organization. Plus intelligently optimize security policies, actions and change process across all corporate networks and cloud environments. With Skybox, your security team can now focus on the most strategic business initiatives while ensuring your business remains protected.

WE ARE SKYBOX. SECURE MORE, LIMIT LESS.