Dell Technologies recommends the Intel vPro® platform: It's built for business

Employees are choosing how they work

And with the right secure digital strategy, this could be a great thing for your business: today and far into the future

DELL Technologies

Innovation Built-In intel.

Contents

1

Work has changed, and it will again

Employees are redefining the workplace like never before, and smart businesses are cashing in

> “The measure of intelligence is the ability to change.”

This quote, attributed to Albert Einstein, is particularly apt for the seismic shift happening in our workplaces today. Few would disagree that the way we work now is vastly different to the way it was just a few short years ago. Whether excited by the possibilities of change, or feeling disrupted by it, organizations have had to enhance their technology strategies to enable people to work from anywhere and interact with customers in new digital ways.

To remain connected, productive and secure in a world where many forms of work can now be done remotely, employees need confidence that the digital environment won’t hinder their ability to deliver their best work. Global research from Statista shows that 80% of employees working at least partially remotely would recommend it to a friend. But, as the study notes, “attitudes on telework are positive if employees are given the appropriate tools and technology to work remotely. These include digital collaboration and productivity management tools, as well as necessary hardware.”[1]

Such attitudes are profoundly changing the role of the IT function within organizations worldwide. Now, more than ever, the role of IT leaders in delivering a modern digital employee experience – providing secure access to all of the tools and resources needed for diverse roles – is bringing a distinct productivity advantage to the most forward-thinking businesses.

Research conducted in 2021, for example, found that those with access to remote work increased innovation by 63%, work engagement by 75% and organizational commitment by 68%.[2]

Prioritizing employee experience

IT teams are very aware of this growing responsibility. Analysis by Gartner predicts that, “by 2025, more than 50% of IT organizations will use digital employee experience to prioritize and measure digital initiative success, which is a significant increase from fewer than 5% in 2021.”[3] There is a clear shift toward placing the distinct digital needs of employees at the heart of digital strategy, with IT as the engine for creating new business opportunity as the workplace evolves today and will continue to do so tomorrow.

In this paper, Dell Technologies and our partners from Intel look at the key challenges and opportunities emerging from the changing workplace. Together, we define best IT leadership practices that will ensure employees can work, collaborate and innovate securely and productively from anywhere and, most importantly, accelerate the business toward its goals.

63% ↑

increase in innovation through access to remote work

2

Past lessons, new opportunities

What historic technology shifts can tell us about the future, and how to take full business advantage

Let's address a challenging and at times divisive issue. For many business leaders, it can seem counter intuitive that the remote working technology needs of employees might dictate the way an organization should operate and innovate. But the workplace shift is happening all the same.

At the release of LinkedIn's 2022 Global Talent Trends report, Jennifer Shappley, global head of talent acquisition, said: "The contract between employees and employers is being rewritten. What employees used to accept is no longer acceptable to them. When they aren't feeling care and love from their employers, they are leaving."[4]

Adapting to change

Amid this climate, executives have a vital decision to make: retain current strategy or adapt with the forces of workplace change. In the fight for skilled talent, fast-moving organizations are choosing to adapt – career site Ladders is predicting that 25% of high-paying jobs will be available remotely by the end of 2022.[5]

For those still hesitant about supporting remote working capabilities over the long-term, particularly because they blend the line between personal/consumer life and working/employee life, it may help to consider other times in the recent past when consumer and workplace technologies have converged, creating vast business opportunities in the process...

1. The consumerization of IT: In 2005, the migration of software and hardware designed for personal use into the workplace was described by Gartner as "the most significant trend affecting IT in the next 10 years." Today, it's hard to imagine a business functioning without mobile technologies, accessible broadband and the ability to utilize personal devices in a work context.

2. The internet of things (IoT): Creating a network of physical objects, embedded with software and sensors, and given the ability to exchange data with other devices and systems, has created a new world of possibilities for consumers, such as home energy management. At the same time, it has presented vast opportunities for businesses, such as predictive maintenance to drive efficiency in factories.

3. Mobile apps and cloud services: For many, the first app they encountered was the game "Snake" on the Nokia 6110. But apps truly came to widespread use with the launch of Apple's App Store in July 2008. Today, mobile apps and the cloud services that support them are the lifeblood of everyday workforce productivity for organizations worldwide.

4. Gamification: First coined by UK-born computer programmer Nick Pelling in 2002, "gamification" refers to utilizing the mechanics of games to increase the engagement, happiness and loyalty of an audience. Today, it's a vital part of business engagement with employees and customers alike, from training to marketing.

5. Artificial intelligence and machine learning: Now behind a vast number of the interactions we have online and via mobile apps, AI and ML have seemingly limitless capacity to entertain and engage while simultaneously transforming almost every industry and organizational function – making life easier, more efficient and potentially more meaningful, both in and out of the workplace.

6. 5G: The more embedded in our lives that mobile devices have become, the more wireless networks have evolved in their coverage and speed, creating new opportunities for business. With the roll-out of 5G, fast, always-on internet connectivity is providing the infrastructure for the technologies that businesses rely on and those they are yet to create.

So, in the same way that the intersection of consumer and business technology has created new opportunities for business in the past, the shifting working preferences and digital needs of employees can create new possibilities for businesses today – enabling them to unlock new value, remain competitive and outpace disruption.

Overcoming the challenges

But to maximize their advantage from these opportunities, organizations must overcome key challenges – and principal among them is addressing new cybersecurity risks. Because, as workforces, apps and data are increasingly distributed across central and remote locations, and employees utilize both work-issued devices and their own personal devices, data security threats are growing.

As a result, IT teams are finding it increasingly difficult to maintain secure control of their environments and keep them optimally operating to meet business needs. In a recent survey of IT decision makers by Vanson Bourne, 50% expressed concerns about keeping their organization secure against growing cybersecurity threats, while 49% are worried about their ability to provide proactive and remote IT support to an increasingly distributed workforce.[6]

It's therefore clear that the organizations to take greatest competitive advantage from this new working reality will be those who build future-ready cyber resilience; deliver an enhanced, modern and secure employee experience to support productivity; and address the cultural considerations that ensure everyone sees security as part of their role: today and in the future.

25%

of high-paying jobs will be available remotely by the end of 2022

Contents

3

Step securely into the future

Research shows that maximizing the business opportunity from hybrid working demands a focus on cyber resilience

Contents

Everyone at work needs help from their IT team from time to time, but where does the IT team turn for help? As they strive to deliver enhanced digital experiences wherever employees may be working, IT functions are deeply aware that they need support.

In the Vanson Bourne study, when IT leaders were asked in which area they required assistance in order to transition to a hybrid working environment, the top answer was "keeping remote workers secure" (48%), ahead of factors including "improving productivity" (45%) and "improving efficiency" (40%). Only 5% of leaders said they didn't need help at all.[7]

It's little wonder that the shifting needs of increasingly distributed workforces have created a security headache for IT leaders at organizations worldwide. Due to the evolving work environment, endpoint security has grown ever more complex, with an extended risk perimeter, apps and data being delivered from a multitude of traditional and cloud data centers, and a rapid increase in edge devices that need protection from proliferating cyber threats.

Viewing security differently

As news headlines from across the world have repeatedly shown us over the past few years, cyberattack tactics such as ransomware are cutting through time and again, across industries, and having severe impacts on both balance sheets and business reputations.

Indeed, in VMware's Global Security Insights Report 2021, 78% of security professionals surveyed confirmed that attacks had increased as a result of employees working from home. And 61% acknowledged the need to view security differently due to the expanded threat surface.[8] The State of Ransomware 2022 Report found that such attacks impacted 66% of organizations in 2021, up from 37% in 2020.[9]

Enhancing cyber resilience across the hybrid working landscape is therefore now a mission-critical imperative. The latest 2022 research from ESG shows a direct correlation between cyber resilience investment, the development of enhanced cost-efficiency and a better, more positive environment for productivity and innovation.[10] In the study, IT decision makers were surveyed and segmented by the maturity of cyber resilience at their organizations. They were asked four key questions:

- How would you describe the level of staffing in your cybersecurity team?
- How would you describe the level of skills in your cybersecurity team?
- How would you characterize your organization's investment in products and services to secure its systems, applications, and data?
- Does your organization audit or inspect the security of its partners/IT vendors?

Just 5%

of IT leaders say they don't need help in transitioning to a hybrid working environment

Contents

ESG classified only the top 10% as "prepared" organizations with the highest level of cyber resilience maturity. These companies are defined as having "an optimal level of security technology investment, staffing level, and rigorous third-party risk inspection." The next 26% were classed as "vulnerable" and the remaining 64% as "exposed."

Several key differences were identified between prepared organizations and those with lower levels of cyber resilience maturity, specific to the business value arising from their utilization of end-user device security across the hybrid workforce.

For instance, prepared organizations are 2.5 times more likely to deliver 99.99% uptime or better for their business-critical apps, equating to an estimated $33.3 million cost-of-downtime advantage. They are also far more agile when it comes to incident detection and response, with a 20% faster mean time to detect and 35% faster mean time to recover. On average, these businesses have been able to shrink their unprotected device footprint by 33%.[11]

Return on investment

As organizations pursue a new hybrid working future, keeping up with the most prepared 10% of businesses will, of course, require investment in skills, resilience technologies, and the rigorous inspection of third-party risk. But the research clearly shows that this cost component comes with a significant return on investment.

And, as we turn now to look at the benefits that resilience can bring to employee engagement and productivity, that return could take an organization to areas of opportunity far beyond those currently accessible by its less mature, more vulnerable rivals.

$33.3 million advantage

prepared organizations are 2.5 x more likely to deliver 99.99% uptime or better, equating to an estimated $33.3million cost-of-downtime advantage.

Contents

4

Supercharge employee productivity

Businesses that provide secure and seamless digital experiences for employees everywhere are proving more productive than those that don't

Let's cut to the chase here – if there was no business benefit to upholding and enhancing hybrid work practices, most organizations probably wouldn't pursue this transformation, in an undisrupted world.

But in a global survey of executives and HR-focused leaders by PwC, published at the end of 2021, 57% said remote and hybrid working had led to their organization performing better against workforce performance and productivity targets over the past 12 months – compared to just 4% saying their company performed significantly worse in that time.[12]

Business advantages

Business productivity, and therefore profit and growth, is a key motivator for advancing hybrid working. So it's a natural progression that enabling people to work securely and compliantly, where and how they prefer, on the devices of their choice, is a major goal of organizations that are embracing the hybrid working future.

Because when workers have the freedom to confidently work where and how they choose without friction, they can stay focused on core organizational objectives, while strengthening their commitment to the business.

For example, ESG's 2022 research into cyber resilience and end-user performance shows that employees at "prepared" organizations give their IT teams a satisfaction score five times higher that those at "exposed" organizations.[13]

Most crucially for business leaders, this is translating into business advantage – those same organizations are 7.7 times more likely than exposed organizations to get new offerings to market ahead of the competition, and they are now forecasting that their revenue will grow at twice the rate of their peers.[14]

These insights build on research conducted by ESG in mid-2021, which explored whether modern device technology adoption is correlated to broader business success and resilience. The study found organizations that can be classed as "Digital Workplace Accelerators" experience 18% fewer critical events tied to device compromise on average.

The same proactive organizations are also 2.1 times more likely to exceed customer satisfaction goals than their more reactive counterparts and, on average, 40% more of their annual revenue is derived from newly developed, innovative offerings.[15]

Public places, private data

But while the creation of friction-free, secure digital environments for remote and hybrid workers has clear business benefits, what about the times when those workers are unable to find a completely private space in which to operate?

Many employees are rightly concerned, and therefore at times distracted, about working with sensitive information which could be seen by others in public spaces. This is a highly valid concern, given that a 2022 study found 62% of commuters in the UK admit to having peered at the smartphone screens of fellow passengers.[16]

When working in a completely private space simply isn't an option, organizations must still ensure that their employees can be confident, and seamlessly and securely productive, via devices built to deliver intelligent privacy.

Today's IT leaders should therefore demand modern devices from their trusted technology partners that deliver an intuitively productive experience to employees while helping protect digital assets and keep sensitive data private at all times.

Advanced privacy technologies

For example, this means insisting on a comprehensive suite of intelligent privacy features such as "onlooker detection," which can notify a user when a snooper is nearby and instantly texturize the display or turn on a safe screen mode.

Today's most advanced PCs can also now darken the screen at the moment a user looks away, to give the employee ongoing confidence that their data will remain protected if they suddenly need to turn their attention elsewhere.

The productivity and bottom-line benefits of enabling secure, optimal remote and hybrid working are now well documented and the evidence is continuing to grow. With the right digital strategy and devices, organizations across sectors can deliver the secure and seamless employee working experiences that will start increasing their advantage in this area from today. But, as we'll now go on to discuss, to make the benefits lasting there is a key cultural element to consider...

40% ↑

more revenue derived from newly developed, innovative offerings at organizations considered "Digital Workplace Accelerators"

5

Why security is everyone's business

If businesses are to gain lasting benefits from hybrid working, security can't be left to the IT team

Like the three little pigs in the classic children's fable, remote and hybrid working employees must face up to both coercive ("let me come in") and forceful ("I'll blow your house down") attempts to breach their security. Unfortunately, today's cyber criminals have much more subtle and sophisticated ways of getting in than those employed by an ill-tempered fictional wolf.

Take the recently emerged "browser-in-the-browser," or "BitB," phishing attack – which convincingly fakes secure sign-on (SSO) windows in order to steal log-in credentials, such as for Google and Microsoft accounts. It's the latest example from the rapidly evolving world of malicious "social engineering," which was summarized neatly in a recent MIT Technology Review podcast by John Scimone, President and Chief Security Officer at Dell Technologies:

"Social engineering, in particular, continues to be a top concern," he said. "For those unfamiliar with social engineering, it's essentially when criminals try to trick employees into handing over information or opening up the door to let criminals into their system, such as through phishing emails, which we continue to see as one of the most popular methods used by hackers to get their first foot in the door of corporate networks."

Everyone's duty

It is for this reason that, to continually reap the benefits of hybrid working for the long-term, organizations must make upholding security the ongoing duty of everyone in the entire business, rather than simply the role of the IT function. Scimone explains how Dell Technologies has established this philosophy within its own business: "We've been building, over many years, a culture of security where we arm our employees with the right knowledge and training so that they can make the right decisions.

"One particular training program that's been very successful has been our phishing training program. In this, we are continuously testing and training our employees by sending them simulated phishing emails, getting them more familiar with what to look for. Even just in this last quarter, we saw more employees spot and report the phishing simulation test than ever before. These training activities are working, and they're making a difference."[17]

Of course, it was much easier to remind employees of their security responsibilities when they were predominantly based on-site, so, as Scimone adds, it's vital to ramp up awareness with specific advice related to remote working situations: "…we're amplifying our efforts and promoting security awareness and the responsibilities that team members have, whether it be how to securely use the VPN, securing their home network, or even how to travel securely," he says.

Contents

Back up education with technology

Of course, while providing ongoing training, organizations must ensure employees are always supported with future-ready solutions and devices that safeguard against ever-evolving threats unique to hybrid work. When considering how to protect distributed data and devices over the long-term, it is important to take a holistic view.

Key considerations for protection above the operating system include: How are we encrypting sensitive information and protecting our data? How are we preventing, detecting and remediating attacks? And can our end users securely access apps and devices from anywhere? While key considerations for protection below the operating system include: Are we securing end-user credentials? Is our BIOS protected? And do we also protect digital privacy?

In response, organizations should ensure they are equipping their people with trusted devices that create a secure foundation: with resilient layers of protection above and below the operating system that harden the endpoint attack surface and protect, detect and respond to evolving threats.

In a world of growing data compliance regulations across industries and geographies, this holistic approach to hybrid working security is highly significant. For example, ESG research in 2022 found that prepared organizations are 44% more likely to report no data loss due to device compromise in the last 12 months – delivering clear compliance and financial benefits.[18]

Only through education, backed by action, can organizations step into the hybrid working future with true confidence and gain a clear competitive advantage over rivals who have yet to do the same.

> "We are continuously testing and training our employees by sending them simulated phishing emails, getting them more familiar with what to look for."
>
> **John Scimone**, President and Chief Security Officer, Dell Technologies

Contents

6

Advice and support

Contents

Work is no longer tied to a location. Seamless, secure hybrid working experiences are a pre-requisite for employee productivity and optimum business growth. With our groundbreaking solutions, deep experience and global scale, Dell Technologies and Intel are the trusted digital partners to support organizations in taking maximum business advantage from this fundamental shift in the workplace.

Future-ready

Our secure future-ready digital infrastructure, modern devices and supportive expertise keep sensitive data private while delivering the modern user experience essential for innovation and collaboration.

For example, Dell Technologies modern devices, powered by Intel, help protect digital assets and keep sensitive data private with the world's most comprehensive suite of intelligent privacy features. Resilient layers of protection – above and below the operating system – harden the endpoint attack surface and help ensure you can protect from, and detect and respond to, rapidly evolving cyber threats.

Intel Hardware Shield, for instance, is included with every Dell commercial device running on the Intel vPro® platform and delivers hardware-enhanced security features that help protect all layers in the computing stack right out of the box.

Employees across the world are reshaping the future of work and, together with Dell Technologies and Intel, you can ensure that this new era of hybrid working is also one of exciting new growth opportunities for your business.

References

1 https://www.statista.com/statistics/1111394/attitudes-on-remote-work-for-employees/#:~:text=In%20general%2C%20employees%20consider%20remote,company%20for%20a%20remote%20role.

2 https://blogs.lse.ac.uk/businessreview/2021/09/29/remote-work-can-boost-productivity-and-curb-burnout/#:~:text=Overall%2C%20compared%20to%20those%20without,likely%20to%20report%20feeling%20included.

3 https://www.1e.com/resources/report/gartner-innovation-insight-for-the-digital-employee-experience-dex/thank-you/?submissionGuid=ZwbrOIKg21dUNdg2ONjZ

4 https://www.cnbc.com/2022/02/04/companies-are-reinventing-rules-as-employees-seek-remote-work-and-flexible-hours.html

5 https://www.cnbc.com/2022/02/04/companies-are-reinventing-rules-as-employees-seek-remote-work-and-flexible-hours.html

6 https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/vb-hybrid-work-productivity-and-collaboration-research.pdf

7 https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/dell-empowering-the-future-of-work.pdf

8 https://www.vmware.com/resources/security/global-security-insights-report-2021-index.html

9 https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/

10 ESG eBook commissioned by Dell Technologies, "How to Build a Cyber-resilient Business Ready to Innovate and Thrive," March 2022

11 ESG Research Summary commissioned by Dell Technologies, "Cyber Resiliency and End-user Performance," March 2022

12 https://www.pwc.com/gx/en/news-room/press-releases/2021/pwc-future-of-work-survey-2021.html

13 ESG Research Summary commissioned by Dell Technologies, "Cyber Resiliency and End-user Performance," March 2022

14 ESG eBook commissioned by Dell Technologies, "How to Build a Cyber-resilient Business Ready to Innovate and Thrive," March 2022

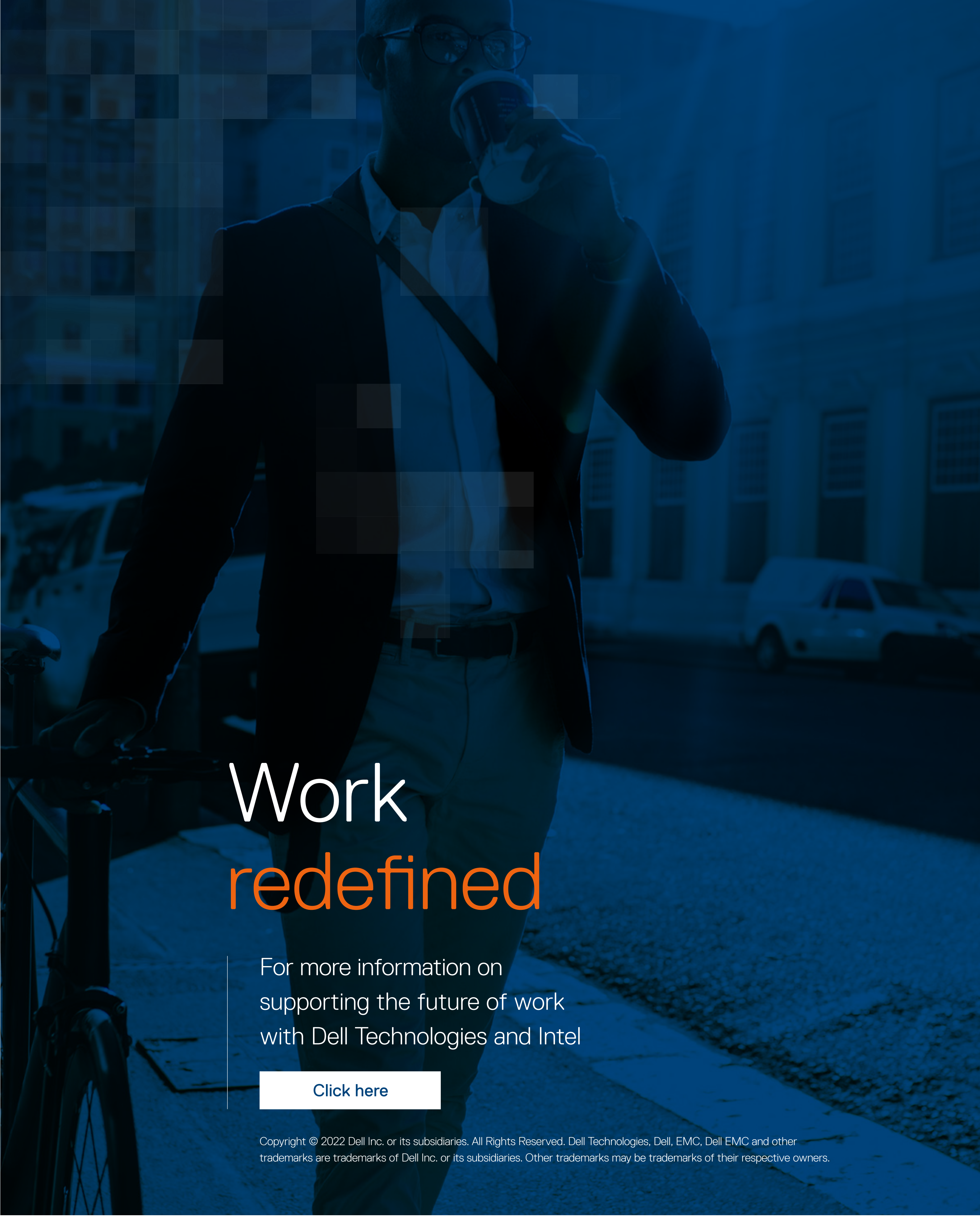
15 ESG eBook commissioned by Dell Technologies, "Organizations Accelerating Their Digital Workplace Achieve Improvements," April 2021

16 https://www.walesonline.co.uk/news/uk-news/brits-admit-spying-what-fellow-23734428

17 https://www.technologyreview.com/2021/11/22/1040358/security-is-everyones-job-in-the-workplace/

18 ESG Research Summary commissioned by Dell Technologies, "Cyber Resiliency and End-user Performance," March 2022

Contents



Work redefined

For more information on supporting the future of work with Dell Technologies and Intel

Click here

DELL Technologies

Innovation Built-In intel.