Managing Business Technology for the Distributed Workforce

Stable, secure, scalable IT platforms support employee satisfaction and productivity

IT affects the employee experience

It's a work-from-anywhere world now.

During the COVID-19 pandemic, companies worldwide were forced to adapt quickly to the needs of a remote workforce under lockdown conditions. The burden fell on information technology (IT) managers and decision-makers as they rushed to equip homebound employees.

While the pandemic wanes, remote work is here to stay. Employees prefer the flexibility of combining remote and on-premises work in a new hybrid model, and employers are prioritizing the needs of their skilled workers.

Now the demand to hire and retain talent is expected to grow and intensify as the global economy recovers. That means employee satisfaction is rapidly becoming a competitive necessity.

Employee satisfaction, in turn, depends to a great extent on the performance of each employee's device and the supporting technology. Access to advanced technology has become a key contributor to employee satisfaction and productivity, and to the overall success of the organization. It's mission is clear, but implementation may be a challenge.

The IT-specific takeaway is that any organization's technology infrastructure must be secure, powerful, and capable of handling future workloads, both centrally and at every endpoint. That means all networked devices must have the power and business-class features needed to run advanced software today and tomorrow.

The challenge of supporting remote manageability is heightened due to an increase in unauthorized intrusions and cybercrime. Security is a paramount consideration that extends to the entire network and every endpoint, whether employees operate within the organization's intranet, in the public cloud, or at the edge.

Powerful technology boosts employee satisfaction

Recent research by Forrester Consulting[1] found that employees' satisfaction and productivity are tied directly to their daily experience with technology at work. When the company provides appropriate resources, its employees are effective, productive, and engaged.

A focus on employee experience is not just good management, it's good business. Forrester found that "a five percent improvement in employee engagement leads to a three percent increase in bottom-line revenue." Not coincidentally, among the companies that Forrester surveyed, "nearly 60 percent ... have seen a more than ten percent increase in their employee experience scores by improving employees' satisfaction with technology."[1]

According to IDC, "72 percent of enterprise IT decision-makers recognize that device choice is very important to their ability to recruit and retain talent. Employee satisfaction must be a critical consideration for IT, but it can't come at the expense of security and manageability."[2]

60%

"Nearly 60 percent ... have seen a more than ten percent increase in their employee experience scores by improving employees' satisfaction with technology."[1]

IT holds keys to employee productivity

However, it isn't easy to manage remote users—or their behavior. Too many users are doing too much at once. They run advanced software, manipulate large data sets, and shuffle among dozens of open browser windows while checking email, chatting on Slack, and attending back-to-back video calls, or similar concurrent activities.

Three-year-old laptops cannot manage those workloads. They crash or fail, requiring tech support or a restart that frustrates the employee, hampers productivity, and wastes valuable time.

IT and employee assessments don’t match up

While IT managers and employees “agree that PCs need to be fast, reliable, and highly connected … employees are largely not experiencing these benefits,” says Forrester.[1]

Among employees surveyed by Forrester:

- **50%** **agree that their PC devices are out of date or insufficient**
- **44%** **report that their PC devices break often**
- **46%** **say their software malfunctions frequently and disrupts their work**
- **33%** **are extremely satisfied with their company-provided laptop**

Meanwhile, the same survey revealed that 79 percent of IT decision-makers allow employees to upgrade to a more powerful device, but only 49 percent of employees thought that option was available to them. The other 51 percent may feel both dissatisfied and powerless to improve the work environment and tools that they rely on all day, every day.

Key takeaways

01 Positive employee experience hones an organization’s competitive advantage

02 Satisfaction with technology improves the employee experience

03 Only 33% of employees are happy with devices provided by their companies[1]

04 Half of employees don’t think they can upgrade

Hybrid workforce: The next "new normal"

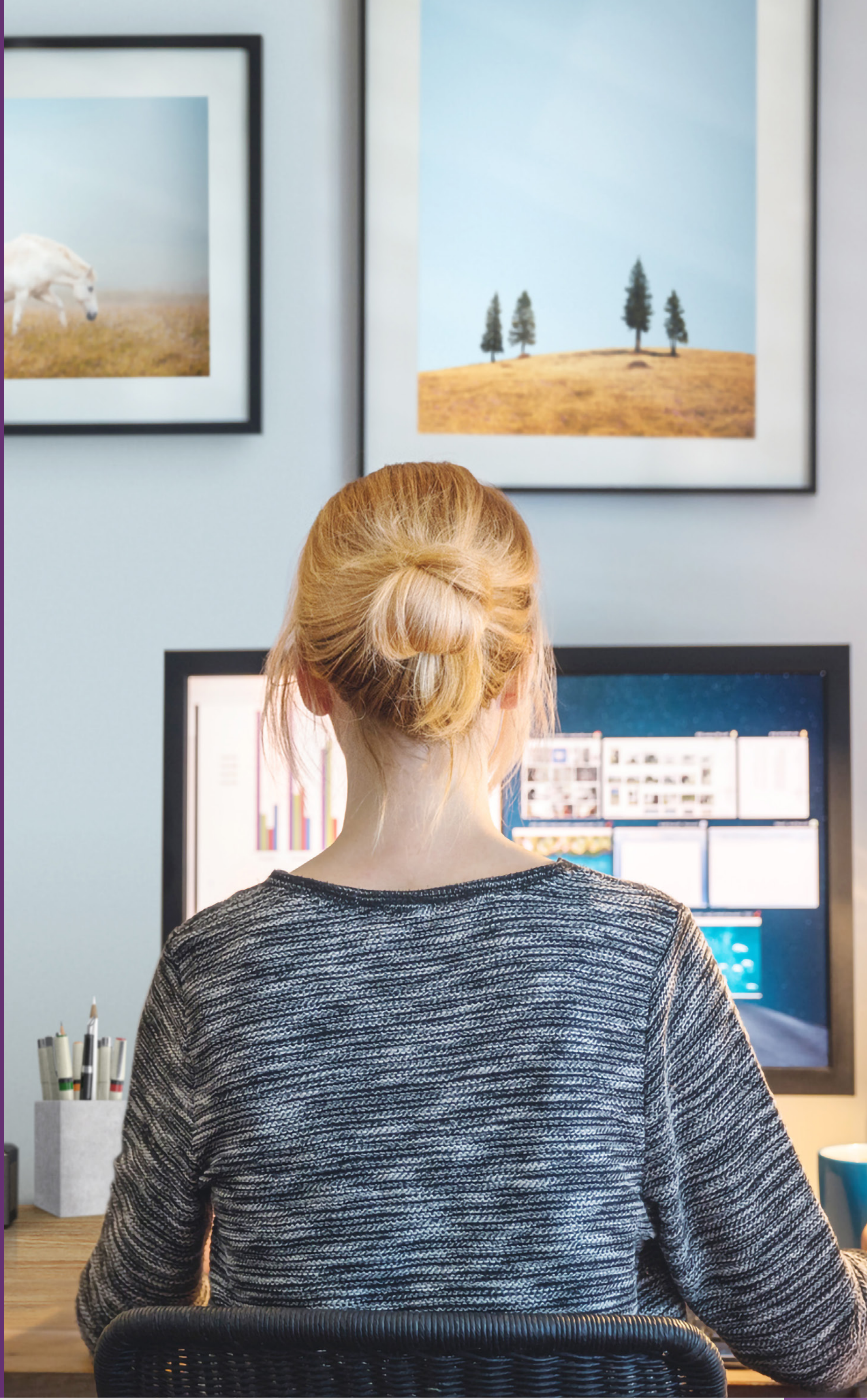
The remote or hybrid workforce is here to stay, as "ninety-seven percent of employees and entrepreneurs said they prefer some degree of flexibility between working remotely and working in an office," according to a survey reported in *Forbes*.[3]

Likewise, corporate leaders expect that most employees will continue to work remotely for at least a few days per week, long after the pandemic ends. The "new normal" will be a hybrid style of work, with some days—and/or employees—on-premises and some remote, according to 82 percent of company leaders surveyed by Gartner in 2020.[4]

The pandemic-driven global experiment in remote work did yield some positive results. Companies that were quick to acquire and deploy adequate technologies and devices found that their employees largely remained productive. Many of the employees even reported improvements in job satisfaction while working at home.

Hybrid work can cause rifts within the workforce, as some employees interact in the office when others do not. Corporate leaders must establish and maintain clear lines of communication to ensure fairness and accountability.

IT staff will be responsible for setting up the infrastructure that supports and connects employees and management in such a dynamic, flexible environment.



Key takeaways

01 Organizations are adopting a hybrid model of remote and on-premises work

02 Hybrid work models can add to stress among employees

03 IT staff and technologies must support productivity and interactivity for the hybrid workforce

Management of a remote user base

IT will continue to face the challenges associated with a distributed workforce. It's the IT staff's responsibility to manage and support hundreds or thousands of client devices while employees are off-premises and away from their desks, in the cloud or at the edge, with or without the organization's intranet and its firewall protections.

This new normal offers few opportunities to administer hands-on support, or even deliver services via VPN. Everything from routine updates and password resets to data breaches and emergency troubleshooting must be accomplished remotely.

97%

Ninety-seven percent of employees and entrepreneurs said they prefer some degree of flexibility between working remotely and working in an office.[5]

Intel vPro® platform supports remote manageability

Well before the pandemic focused the world's attention on remote manageability, the forward-looking engineers at Intel had already developed a solution: the Intel vPro® platform.

The Intel vPro platform supports IT departments:

- **Cuts costs through remote diagnostics and remediation**
- **Enables IT to isolate and wipe infected devices**
- **Streamlines remote patch management, inside and outside the firewall**
- **Simplifies large-scale deployments**

A laptop or desktop PC built on the Intel vPro platform delivers effective, hardware-enhanced security features and PC fleet stability. Devices based on the Intel vPro platform are available with a selection of Intel® Core™ vPro® processors, in a variety of form factors. IT teams can offer a range of Intel vPro platform options to satisfy their most-demanding users, while maintaining the highest level of manageability across the entire fleet of devices.

IT departments are advised to activate Intel® Active Management Technology (Intel® AMT) for added control. Intel AMT interacts with each endpoint through the hardware layer below the operating system. Available exclusively on the Intel vPro platform, Intel AMT enables the IT professional to support remote devices, even when they are unresponsive, turned off, or infected by malware.

What's in the Intel vPro® platform?

The Intel vPro® platform integrates a suite of transformative technologies that have been tuned and tested rigorously for demanding business workloads. IT teams can be confident that every Intel vPro platform-based device is designed for productivity, security, manageability, and reliability.

intel vPRO® PLATFORM BUILT FOR BUSINESS

Business-class performance

with the Intel vPro platform that includes the Intel® Core™ vPro® processor or Intel® Xeon® processor, and **Intel® Optane™ memory H10** with solid-state storage and other advanced components

Remote management

capabilities, inside or outside the firewall, with **Intel® Active Management Technology and Intel® Endpoint Management Assistant**

Fast, reliable connectivity

with built-in Wi-Fi 6 and Thunderbolt™ 4 technology

Hardware-enhanced security

features, with **Intel® Hardware Shield**, for built-in protection against intrusions and cyberattacks

Stability, compatibility,

and long-term reliability, in an integrated, validated platform

Available in many device types

including desktops, laptops, 2-in-1s, and workstations, from a wide variety of providers worldwide

Key takeaways

01

Tech support must be able to be administered remotely, even when devices are turned off or disconnected from the organization's intranet

02

The Intel vPro® platform provides business-class performance, security, manageability, and stability

03

A variety of devices are built on the Intel vPro platform, available from many providers worldwide

Remote work and security risks

Remote work poses unique risks to the security of an organization's users and its data. A report from Deloitte[5] noted that "47 percent of individuals fall for a phishing scam while working at home," exposing their companies and networks to intrusions. Such data breaches cost an average of USD 137,000 per incident, according to the report.[5]

Working from home amplifies other risks as well. Workers are more prone to human error and subject to more frequent distractions. They may share devices with family members, and their home Wi-Fi or personal devices may not meet the organization's security needs.

Meanwhile, "CIOs face continued pressures to scale infrastructure that supports moving complex workloads to the cloud and the demands of a hybrid workforce," according to a research report published by Gartner.[6] That trend is expected to boost annual spending on cloud services by another 23 percent in 2021 to USD 332 billion worldwide, the report said.[6]

With the increased acceptance of remote and hybrid work modes, it is imperative for IT to strengthen security measures throughout the network and at every endpoint.

Software-based security measures, including antivirus programs, do not provide sufficient protection against today's cybercriminals, however. Some of the latest ransomware attackers and hackers have begun injecting malware directly into a device's UEFI/BIOS firmware, where it is often undetected by antivirus software.

Fleet-level security on the Intel vPro® platform

The Intel vPro® platform's hardware-based security features enable profiling and detection of BIOS-level ransomware and other threats that can compromise data security and degrade CPU performance. The Intel vPro platform helps to protect the entire fleet of devices in an organization, with a multilevel approach that includes:

- **Protection from firmware-level attacks on the BIOS**
- **Threat detection that harnesses hardware telemetry and acceleration capabilities to identify threats and anomalous activities in real time**
- **Endpoint management support, so IT staff can monitor, restore, and patch devices remotely, to protect the fleet and reach devices that are not physically accessible**

Intel's commitment to security is relentless and pervasive, with innovative solutions and support to protect your business today and in the future.

Key takeaways

01

Enhanced security is an urgent requirement for the remote or hybrid workforce

02

Virus-detection software does not provide sufficient protection against today's cybercrime

03

The Intel vPro® platform includes hardware-based security and threat detection that help protect networks and all endpoints

Endpoint stability in an unstable time

Managing a business PC fleet has become more complex due to a growing volume of software updates and driver incompatibilities. Validation and testing of a system image can take weeks or months to complete. By that time, a new set of software or driver updates could delay the image rollout even more or trigger an additional deployment, accompanied by more testing and greater disruption.

Plus, the transition to a remote or hybrid workforce removes the option for hands-on management and may introduce personal devices that were never in the plan to begin with, further complicating the update process.

Stability in the Intel vPro® platform

Devices on the Intel vPro® platform are covered by the Intel® Stable IT Platform Program (Intel® SIPP), designed to ensure long-term IT reliability and compatibility for business-class systems. Intel SIPP aims to keep hardware components consistent for 15 months from product launch, empowering IT teams to manage and scale their PC fleets without the need to revalidate new devices.

As part of this stability initiative, the Intel vPro platform delivers the latest technologies in an integrated, validated platform that scales easily to accommodate future growth. Individual devices based on the Intel vPro platform are available for at least 12 months from most manufacturers, who also provide extended support.

Regardless, all devices built on the Intel vPro platform are compatible with each other, so IT can maintain a stable system image across an entire fleet of PCs throughout their lifecycle, or as part of a global rollout.

The improved quality, reliability, and compatibility are built into the Intel vPro platform and validated rigorously, saving time and aggravation for IT teams and their end users.

Key takeaways

01

Maintaining a fleet of business devices is more complicated with a remote workforce

02

Frequent updates to software and drivers can disrupt or delay system image rollouts

03

Intel® SIPP minimizes updates, enabling IT teams to control the PC lifecycle and maintain a stable system image

Managing the hybrid future

During this unprecedented time, IT leaders have heroically kept businesses running, enabling a distributed workforce to remain employed and productive. As the global economy recovers, organizations have a renewed opportunity to design strategic solutions for the new hybrid environment.

Careful planning and execution are required as IT teams choose the devices and technologies that will support the needs of their organizations and their users, now and in the future. Employee satisfaction has become a high priority for the business world, and technology has a big impact on the employee experience. As a result, IT must focus its efforts on improving user experience, while tackling the manageability and security challenges posed by the remote and hybrid workforce.

IT leaders rely on the Intel vPro® platform to support their organizations' goals. The comprehensive, business-ready platform reflects Intel's commitment to the management, security, and reliability capabilities that have proven their real-world value—before, during, and after the pandemic.

As the workplace continues to evolve, so will the Intel vPro platform, incorporating innovative technologies into a stable, compatible platform that provides the best-managed business experience for organizations, their IT teams, and end users.

Empower productivity with business-class technology

Learn more about the built-for-business Intel vPro® platform

intel.com/vpro

Performance. Security. Manageability. Stability.

Sources

1. Forrester, "Invest in Employee Experience, Drive Your Bottom-Line Growth," October 2020.
   https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/lenovo-ex-whitepaper.pdf
2. IDC, "The Importance of the PC in a Data-Centric World," April 2030. (Study commissioned by Intel).
   https://plan.seek.intel.com/vProIDC_WhitepaperLPCD.
3. *Forbes*, "5 Statistics Employers Need To Know About The Remote Workforce," February 10, 2021.
   https://www.forbes.com/sites/ashiraprossack1/2021/02/10/5-statistics-employers-need-to-know-about-the-remote-workforce/
4. *Forbes*, "Four Hidden Traps of Managing A Hybrid Workforce," May 12, 2021.
   https://www.forbes.com/sites/forbescommunicationscouncil/2021/05/12/four-hidden-traps-of-managing-a-hybrid-workforce/
5. Deloitte, "Impact of COVID-19 on Cybersecurity," 2020.
   https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html
6. Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021," April 21, 2021.
   https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021

Notices and disclaimers

Intel® technologies may require enabled hardware, software, or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

US/07/2021/PDF/JH/CMD