CIO FROM IDG

WHITE PAPER
SPONSORED CONTENT

Optimizing User Experience in the Hybrid Workplace with Intel® Evo™ vPro® Platform

65%

Executives who believe employees must be in the office 3 days a week or less.

SOURCE: PRECEWATERHOUSECOOPERS US REMOTE WORK SURVEY 2021

Empower your on-the-move workforce while giving IT peace of mind that they can manage and secure devices from any location.

Remote work has created new challenges for the enterprise as people went from using their devices intermittently to centering their workday around them. The COVID-19 pandemic has cast a harsh light on the difficulty of managing these complex remote workforce environments, particularly when people aren't always connected to the corporate network.

Ensuring a clean and consistent personal computing experience was simpler when everyone was in the office. IT owned the hardware, maintained the software, and ensured that protections, updates, and patches were applied. But extending those controls to a work environment in which employees are effectively their own IT managers has presented unprecedented challenges.

And they are challenges that are likely to persist for some time. Nearly one-third of the 9,000 knowledge workers surveyed by Slack **don't want to go back to working in the office full-time**. PricewaterhouseCoopers reported in January 2021 that 65% of executives believe employees need to be in the office **three days a week or less**.

Despite people's preference for remote work arrangements, there is evidence that maintaining high levels of morale is more challenging in a distributed workforce than in an office. Numerous studies conducted during the pandemic found that home-based employees work longer hours. Isolation can cause burnout, a syndrome that afflicted **40% of homebound workers in 2020**, according to a study by FlexJobs and Mental Health America.

For people who are already stressed, the need to maintain and troubleshoot the computers that have become lifelines to their employers only adds to their anxiety. Home-based workers must assume the bulk of the responsibility for ensuring that devices are in good working order, free of malware, and up-to-date. They must install patches, configure peripheral devices, troubleshoot performance problems, and arrange for repairs to be made when necessary.

Home environments also introduce new risks such as kids using their parents' computers, vulnerability to Wi-Fi hacks, and the risk of damage from household hazards. For the majority of office workers who would classify themselves as non-technical, these tasks can be intimidating and time-consuming. Mistakes that damage equipment or expose data only increase their frustration.

PRESENTED BY

intel®

Processor speed equates directly to employee productivity. Optimum performance is needed to handle the volume and variety of applications that home-based PCs must manage without frustrating slowdowns.

Employees are customers, too

Improving customer experience is a top-of-the-agenda item for many businesses, but employees are also customers when it comes to the IT organization. Businesses need to be aware of the value of delivering user experiences that minimize worry and frustration. PCs should work the way people expect them to.

This need is particularly acute as PCs are being called upon to do more than ever. Employees routinely multitask between several applications and maintain dozens of open browser windows. As enterprise applications have overwhelmingly shifted to a software-as-a-service model, networks have become a critical chokepoint. Processor speed equates directly to employee productivity. Optimum performance is needed to handle the volume and variety of applications that home-based PCs must manage without frustrating slowdowns.

The PC has also recently become an essential collaboration and communication device. Video conference calls are now an integral part of the remote work environment—and will continue to be central for years to come. Everyone has experienced the delays caused by dropped video calls, background noise, and garbled audio. Video meetings must evolve to become just as seamless as in-person.

Redefining mobility

The laptop was the mobile office for many people before 2020. Now it's likely to be the home office as well.

As employees increasingly depend on their laptops for everything from email to presentations and collaboration, the importance of responsive and available equipment has grown. Part of delivering a great user experience is giving employees the technology they know they can rely on, even when they can't always plug in.

As the workplace returns to a new normal with a hybrid on-site and remote workforce, employees will increasingly take their work computers with them to customer sites and meetings with suppliers and business partners. Mobile performance and battery life will assume greater importance than before the pandemic. Whether meeting with customers offsite, running between conference rooms in the office, or working at home, not everyone will have the luxury of being plugged in all day.

The Intel® Evo™ vPro® platform enables a new class of laptops to incorporate features designed specifically for highly mobile workers. The Intel Evo platform specification has been widely adopted by PC makers and will support more than 60 new laptop products in 2021.

Intel Evo platform certification requirements

To achieve Intel Evo certification, candidate mobile PCs must provide:

- At least nine hours of battery life on an FHD display[1]
- Wake from sleep in less than one second
- Consistent responsiveness
- A minimum of four hours of battery life from a 30-minute charge[1]
- Best-in-class Wi-Fi technologies with Wi-Fi 6 and Thunderbolt™ 4 connectivity.[2]

SOURCE: DEEP INSTINCT 2020 CYBER THREAT LANDSCAPE REPORT

Threats at home

Home-based work has also presented a host of new security challenges beginning with the simple fact that home networks are more vulnerable to attack than corporate ones. Weak or nonexistent passwords, unpatched routers, and outdated encryption protocols are just some of the gaps that are common in home Wi-Fi networks.

Even virtual private networks, which are widely used to create secure tunnels inside the corporate firewall over public networks, are proving to be a vulnerability. Malware introduced when an employee's computer is not connected to the VPN can spread when the employee logs back onto the corporate network. That threat is unlikely to disappear any time soon given that 45% of enterprises intend to continue using them **until at least the end of 2023**, according to a survey by network security firm NetMotion Software.

And the risk isn't confined to networks. Children using a shared PC can inadvertently install malware or accept incoming chats from malicious characters. Even printers and voice-enabled assistants can introduce vulnerabilities in some circumstances. Mobile phones are vulnerable to attacks that can turn them into surreptitious listening devices.

All these factors challenge employees to maintain something approaching the rigor of enterprise IT security professionals. And cybercriminals have turned up the volume since the pandemic began.

The incidence of ransomware attacks jumped more than 400% in 2020, according to a **Deep Instinct study**. There has also been a surge of attacks on the BIOS, which contains more than 300 settings that include instructions about the basic hardware functions of the computer. Changes at the BIOS level can't be detected by software; they must be monitored by other hardware components. Even blanket protections like virtualization are ineffective at that level. IT organizations need solutions that enable them to manage critical functions remotely while ensuring that security and performance are in peak condition.

Planning for the new workplace

The **Intel vPro platform** was created to meet the unique needs of enterprise IT organizations supporting knowledge workers. It has evolved over 15 years to encompass a wide range of productivity enhancements and security innovations aimed at providing the optimal user experience.

Intel vPro platform is a validated and integrated platform built for business and available in a wide variety of form factors that include all types of laptops, desktops, workstations, and all-in-one devices. It is designed to meet the needs of all types of corporate users while giving IT an extensive and consistent pallet of tools to secure and manage them. The new Intel Evo platform extends enterprise-focused features to mobile platforms.

Consistency is core to the Intel® Core™ i5 vPro® processor user experience. All Intel vPro platform-certified devices require an i5 or higher CPU as well as a corporate-grade chipset and firmware. Dynamic voltage and frequency scaling match power to the workload for maximum efficiency. An onboard graphics processing unit delivers significant gains in power efficiency as well as massive performance improvements. Built-in Wi-Fi 6 and 6E support can be up to six times faster than previous Wi-Fi versions.[2]

For video calls, a **built-in AV1 codec** provides the highest levels of video encoding at half the bandwidth of its predecessor. The result is a more natural collaboration experience and reduced video conferencing fatigue, which can be a major factor in employee experience.

Intel vPro® platform gives IT organizations the tools to monitor, restore, upgrade, and protect devices both inside and outside the corporate firewall, even if the devices are plugged in but turned off.

How Intel vPro Platform addresses management challenges

The best PC user experience relieves users of the task of tuning parameters and installing updates. **Intel® Active Management Technology** (Intel® AMT) and **Intel® Endpoint Management Assistant** (Intel® EMA) give IT organizations the tools to monitor, restore, upgrade, and protect devices both inside and outside the corporate firewall, even if the devices are plugged in but turned off.[3]

Administrators can remotely access and control unattended devices to perform important functions such as applying patches and remediating problems. Intel EMA provides a secure remote connection to Intel vPro platform-enabled devices outside the corporate firewall. The combination means that systems can be reached virtually anywhere in the field, regardless of whether they're connected to the corporate network.

How Intel vPro Platform addresses security challenges

Nothing is more disruptive to the user experience than a devastating cyberattack. With ransomware dominating the headlines since the onset of COVID-19, employees are understandably on edge about the risk to them and the organization as a whole if they become a victim.

Software-only protections are not enough now that attackers are targeting underlying hardware. The Intel vPro platform incorporates **Intel® Hardware Shield** to provide multi-level security that complements software-based protections. It features Intel® Threat Detection Technology (Intel® TDT) for silicon-level telemetry to help identify threats and detect abnormal activity. Intel Hardware Shield augments existing antivirus protections to help quickly detect and remediate the latest ransomware and crypto-mining attacks.

Each Intel vPro platform-based system also ships with an image of the factory BIOS in a location where it can't be reached by the operating system. This enables Intel Hardware Shield to detect and halt a boot sequence if an attacker has made low-level changes to the hardware. Virtualization helps prevents memory corruption and malware injection to keep workloads secure and running.

[1] Time taken to drain from 100% to critical battery level while performing workflows under a typical-use environment comprising multiple cloud-based and local apps and web pages including Google Chrome*, Google G-Suite*, Microsoft Office 365*, YouTube* and Zoom*, including limited periods of non-use. Testing conducted on laptops connected to 802.11 wireless, and with shipped hardware configurations including Windows* 10 and 250-nit LCD screen brightness. Testing results as of August 2020, and do not guarantee individual laptop performance. Power and performance vary by use, configuration and other factors. Learn more at intel.com/evo.

[2] Intel® Wi-Fi 6 (Gig+) products enable the fastest possible maximum speed for typical laptop Wi-Fi products. Thunderbolt™ 4 is the fastest port available on a laptop, at 40 Gb/s, as compared to other laptop I/O connection technologies including eSATA, USB, and IEEE 1394 Firewire*. Performance varies by use, configuration and other factors.

[3] Intel AMT requires a network connection; must be a known network for Wi-Fi out-of-band management. Learn more at intel.com/11thgenvpro. Results may vary.

Intel technologies may require enabled hardware, software, or service activation. No product or component can be absolutely secure. Your costs and results may vary.

intel.

© Intel Corporation.

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

PCs built for business

PCs based on the Intel vPro and Intel Evo vPro platforms are built for business to optimize performance, manageability, security, and stability. At a time when IT organizations are dealing with unprecedented workloads, this is one less stress factor they have to contend with.

Learn more **here**.

intel vPRO PLATFORM
BUILT FOR BUSINESS