# Fleet Management Handbook

## Four Essentials for the Hybrid Workplace

# Your PC selection is more business critical than ever

Today, employees want the freedom and flexibility to work from wherever suits them best. To meet this demand, hybrid workplaces that operate both in person and remotely are quickly becoming the new standard for businesses worldwide.

This rapid rise should be a crucial factor in fleet management and investment strategy. With the hybrid workplace comes new challenges across mobility, security, and performance. Business PCs need to deliver what end users expect while providing the security and manageability that your IT department requires, even when workers are on the go.

At the same time, business is also more digital than ever. Your users' PC devices are their essential tools for making great things happen. To maximize productivity and innovation, they need a device that works for them. And your business needs stability and assurance that once you've selected a device, it will be readily available and easy to support.

To help you address these challenges and make the right PC investment, this buyer's guide outlines the **four essentials** you need to look for as you select business devices.

**Four hybrid-workplace essentials** for modern business PCs

1. **Hardware-level features for remote manageability and access**
2. **Foundational security**
3. **Platform stability**
4. **A standout user experience**

# The Intel vPro® platform advantage

Along the way, we'll highlight some of the benefits of the Intel vPro platform: an integrated, validated platform for business PCs with built-in features for performance, security, manageability, and stability.

Essential 1

# Hardware-level features for remote manageability and access

Hybrid workplace's biggest IT challenge is an obvious one: how can your team manage devices without being anywhere near them? Find out how the right features ensure your staff can access and repair devices from anywhere—even if the device is experiencing significant technical issues.

**Visibility and asset management are critical for distributed organizations**

Nearly 40 percent of companies surveyed anticipate most of their employees being hybrid workers in the future.[1] But with a high number of remote employees, proactively managing your fleet and recovering damaged assets becomes even more complex. When your IT department finds itself in a black hole, unable to assess or repair remote devices, your business can suffer. Work-from-anywhere employees require your IT team to be able to see and manage devices anywhere, even if the devices are experiencing major technical problems.

Solving this problem requires hardware-level access and control features for your IT team. Relying solely on management software can leave IT staff unable to access devices that are experiencing major system failures. Likewise, not having access to keyboard, video, and mouse (KVM) functions when trying to remediate a downed machine can severely limit IT's ability to solve problems.

# The benefits of out-of-band management

## Better access and functionality to remote machines

Administrators can set levels on the BIOS and UEFI firmware interfaces or make elevated task changes. They can also perform routine tasks, like PC setup and configuration and OS or security updates.

## Help lower IT management costs

Businesses that have hundreds or thousands of PC-based devices in many locations can reduce their operational costs related to travel, truck rolls, and IT staff hours.

## Faster fixes

With remote out-of-band management and KVM controls, technicians have more tools to get PCs up and running faster. And without the need to be in front of the device, IT can reduce downtime and boost productivity.

### TIP: Out-of-band management is a hybrid-workplace necessity

Hardware-based out-of-band-management allows IT staff to manage any device that has a network connection and a power source—even if they're turned off or unresponsive. As workers become more remote and mobile, it's a critical feature for enabling the access your team needs. Without it, remote employees can find themselves without a working device for days, weeks, or even months as they wait for a usable machine to be delivered. Out-of-band management also enables cloud manageability features and USB-R functionality for remote image installation.

# Additional management capabilities to look for in the hybrid workplace

In addition to out-of-band management, you need to ensure that your business PC delivers some additional management features that help boost IT productivity through quicker processes and less required travel time.

As you assess devices, be sure to look for other critical capabilities including:

- Achieving faster patch saturation with direct power-on and command
- Automatically controlling sleep/wake cycles to avoid costly power spikes
- Easily and efficiently deploying OS images
- Detecting and monitoring the status of all endpoints on a network, independent of their power state, OS status, or connectivity type

## The Intel vPro® platform advantage: Ideal manageability for the hybrid workplace

Hardware-based Intel® Active Management Technology (Intel® AMT), part of the Intel vPro platform, provides persistent out-of-band connectivity that empowers your IT staff to remotely discover, monitor, repair, restore, and help protect networked PCs and other devices, even when they're powered off or unresponsive.* Intel® Endpoint Management Assistant, another part of the Intel vPro platform, enables Intel AMT to manage devices inside and outside your corporate firewall.

*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.

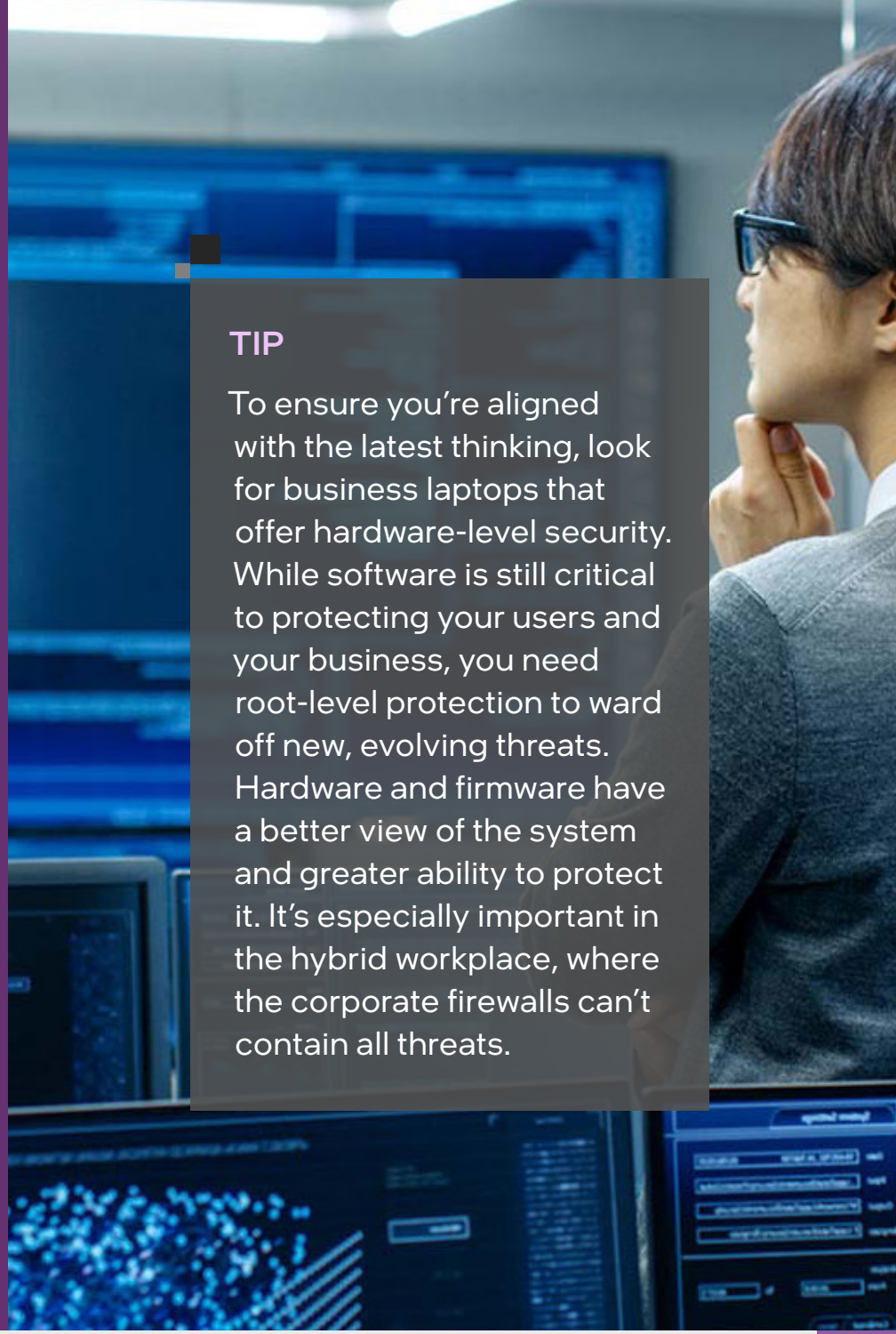
Essential 2

# Foundational security

Modern business PCs face an ever-evolving landscape of cybersecurity threats. And the hybrid workplace shift introduces even more new complexities and challenges. Read on to learn what you need to keep your users—and your business—safe.

63%

A survey of enterprises in the United States, Canada, the United Kingdom, France, and Germany revealed that 63 percent of companies have been compromised due to a vulnerability in hardware or silicon.[2]



**TIP**

To ensure you're aligned with the latest thinking, look for business laptops that offer hardware-level security. While software is still critical to protecting your users and your business, you need root-level protection to ward off new, evolving threats. Hardware and firmware have a better view of the system and greater ability to protect it. It's especially important in the hybrid workplace, where the corporate firewalls can't contain all threats.

## Why a deeper approach to cybersecurity is needed

New reports of costly cyber breaches appear almost daily. Attackers are becoming more sophisticated and employing new approaches to get what they want. Businesses need to look for ways to mitigate risks and ward off attackers. To do so, they're finding it necessary to rely on foundational protections running at the hardware level.

Software-only security doesn't provide the root-layer protection that's required to detect and prevent advanced cyberthreats. It can be more easily bypassed by an attacker who has obtained higher privileges through a system vulnerability. Plus, hardware-based security helps protect your device against hardware-level attacks that would otherwise go unguarded against and unnoticed.

## What makes hardware-based security so effective

Attackers typically live in the software space, where the intrinsic openness and freedom can be exploited for their gain. The hardware level is more tightly controlled and less susceptible to attack. Working at the hardware level, security tools are better positioned to spot anomalies—and the hardware-based controls will remain effective even if the system's software or operating system is compromised.

Hardware-based security can also help prevent firmware attacks or supply-line tampering. On each start-up, security technologies verify the loaders that boot the code and execute the boot sequence of the firmware and operating system. This added layer of security helps mitigate the risk of tampering or the injection of malware under the operating system.

# Intel vPro® platform advantage: Enable a deeper approach to PC security

Devices that are part of the Intel vPro platform provide powerful, integrated features to help protect your business, data, and users:

**01**

**Use Intel® Hardware Shield technologies to provide full-stack protections, including features to minimize the risk of malware injection and help enable secure OS boots**

**02**

**Run virtual machines for security-based isolation with application compatibility across different operating sytems running on the same PC**

**03**

**Accelerate virtualized security software like Windows Defender Credential Guard and Application Guard with Intel virtualization capabilities to help protect against OS kernel-level malware and browser-based attacks**

**04**

**Complement virtualization with hardware-based encryption to help protect data at every layer**

**05**

**Defend against ransomware and malicious crypto mining with Intel® Threat Detection Technology**

Essential 3

# Platform stability

Developing and verifying a PC imaging strategy is critical to efficient fleet management. But what happens when components become unavailable or configurations change after you purchase? What happens when you introduce various and diverse standards into the fleet and need to maintain a number of complex corporate images? Building and scaling your PC fleet on a stable platform is critical for your IT investments—especially when you're dealing with a dispersed or global workforce.

**How to manage your fleet without surprises**

You need assurance that once you've selected a device, it will be available and supportable for an extended period of time. A stable laptop platform means your team won't experience issues as you source laptops after your initial selection. Because verifying images takes a significant amount of time, changes to your investment's specifications can create additional verification processes that bog down IT operations and ultimately inflate TCO.

## The Intel vPro® platform advantage: The Intel® Stable IT Platform Program (Intel® SIPP)

The Intel Stable IT Platform Program (Intel SIPP) features an extensive validation program that aims for no hardware changes throughout the buying cycle, for at least 15 months or until the next generational release. You can scale and grow more simply by getting the same level of validation and compatibility no matter where the device is purchased. Rest easy when adding new PCs to the fleet, knowing custom images and drivers will be compatible across Intel vPro platform-based devices.

Intel also works hand in hand with OEMs for a full year—every year—conducting thousands of tests and feedback loops to certify that devices are built to give IT and end users the stability and reliability of a true business-class device.

Essential 4

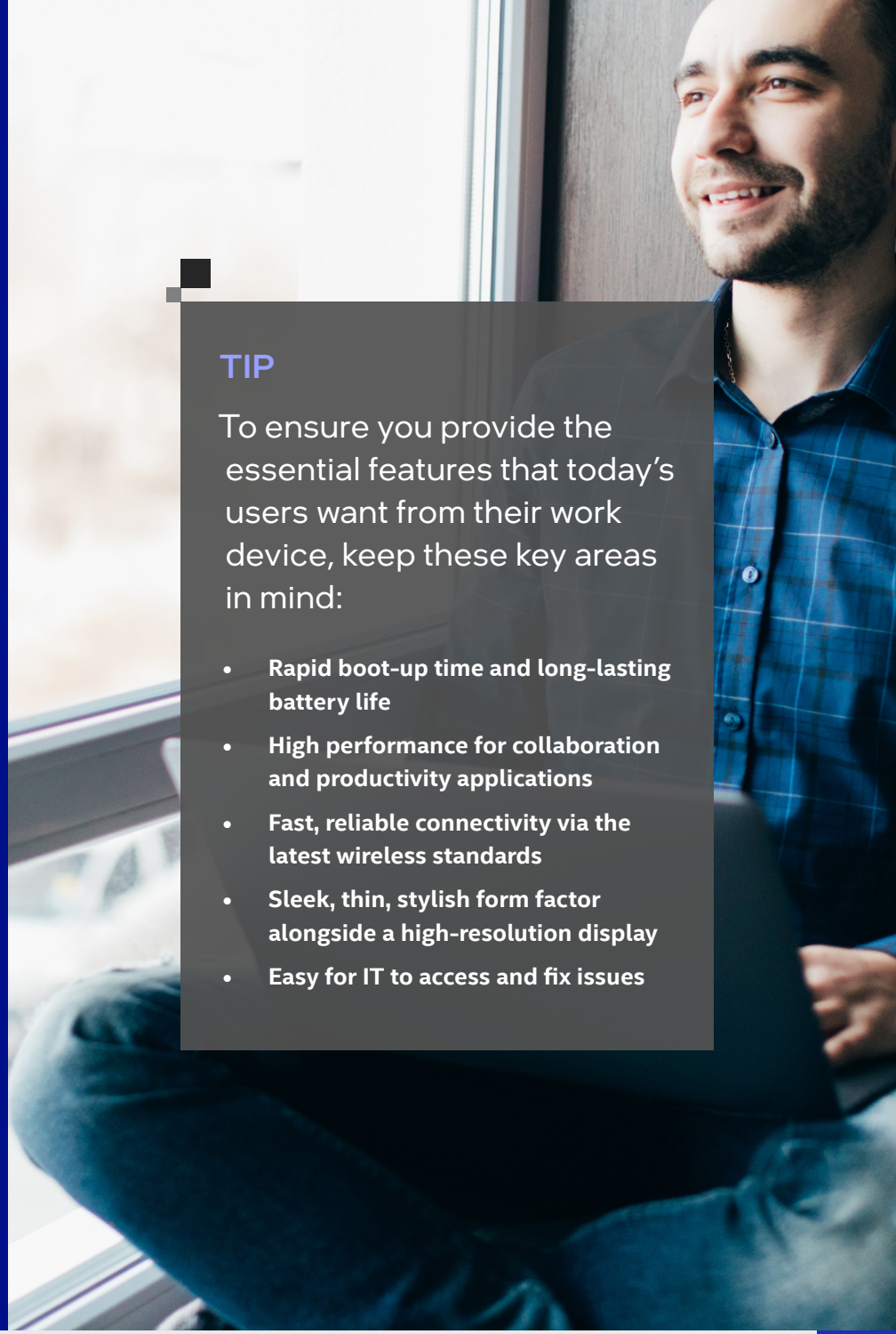
# A standout user experience

As workers become more mobile and business becomes even more digital centric, their laptops become even more important. Understanding what today's top talent want from their work devices can help you make a smarter investment. Find out what to look for in this section.

**Your employee's device is central to their work experience**

A recent survey of full-time employees illustrates just how essential PC devices are to team engagement and daily work. Sixty-two percent of respondents agreed that PC devices are critical for revenue growth—and 55 percent cited them as critical to employee retention, too.[1] But only 33 percent of respondents said that they are extremely satisfied with their company-provided device.[1]

IT decision-makers are tasked with investing in the right PCs and devices to drive a better experience for their employees—delivering benefits for current team members while helping to attract the most talented recruits too.



**TIP**

To ensure you provide the essential features that today's users want from their work device, keep these key areas in mind:

- **Rapid boot-up time and long-lasting battery life**
- **High performance for collaboration and productivity applications**
- **Fast, reliable connectivity via the latest wireless standards**
- **Sleek, thin, stylish form factor alongside a high-resolution display**
- **Easy for IT to access and fix issues**

## The vPro® advantage: Built for what modern users need

vPro platform devices deliver validated performance alongside the key capabilities and features that today's hybrid workplace employees need, including rapid performance, accelerated start-up times, integrated remote management, beautiful displays, and attractive form factors.

### Many employees report frustration with their current technology.[1]

**50%**

of employees believe their computer is insufficient or out of date

**44%**

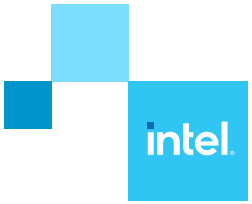
report frequent breaks

**46%**

report frequent software malfunctions and work disruptions

**30%**

believe their device works well across teams




# Ensure your next business PC investment is a sound one

Use the insights and tips in this guide to assess and evaluate your prospective device investments. Finding and selecting the right device among the many available options is critical to your business.

To learn more about the Intel vPro platform and browse our latest world-class business computing devices, visit:

**intel.com/vPro**

**References**

1. *Invest in Employee Experience (EX), Drive Your Bottom Line Growth*, a Forrester Consulting thought leadership paper commissioned by Lenovo and INTEL, October 2020. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/lenovo-ex-whitepaper.pdf
2. *Match Present-Day Security Threats with BIOS-Level Control*, a Forrester Consulting thought leadership paper commissioned by Dell, June 2019. https://www.intel.com/content/www/us/en/business/enterprise-computers/hardware-security.html

**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/08/2021/PDF/JH/CMD