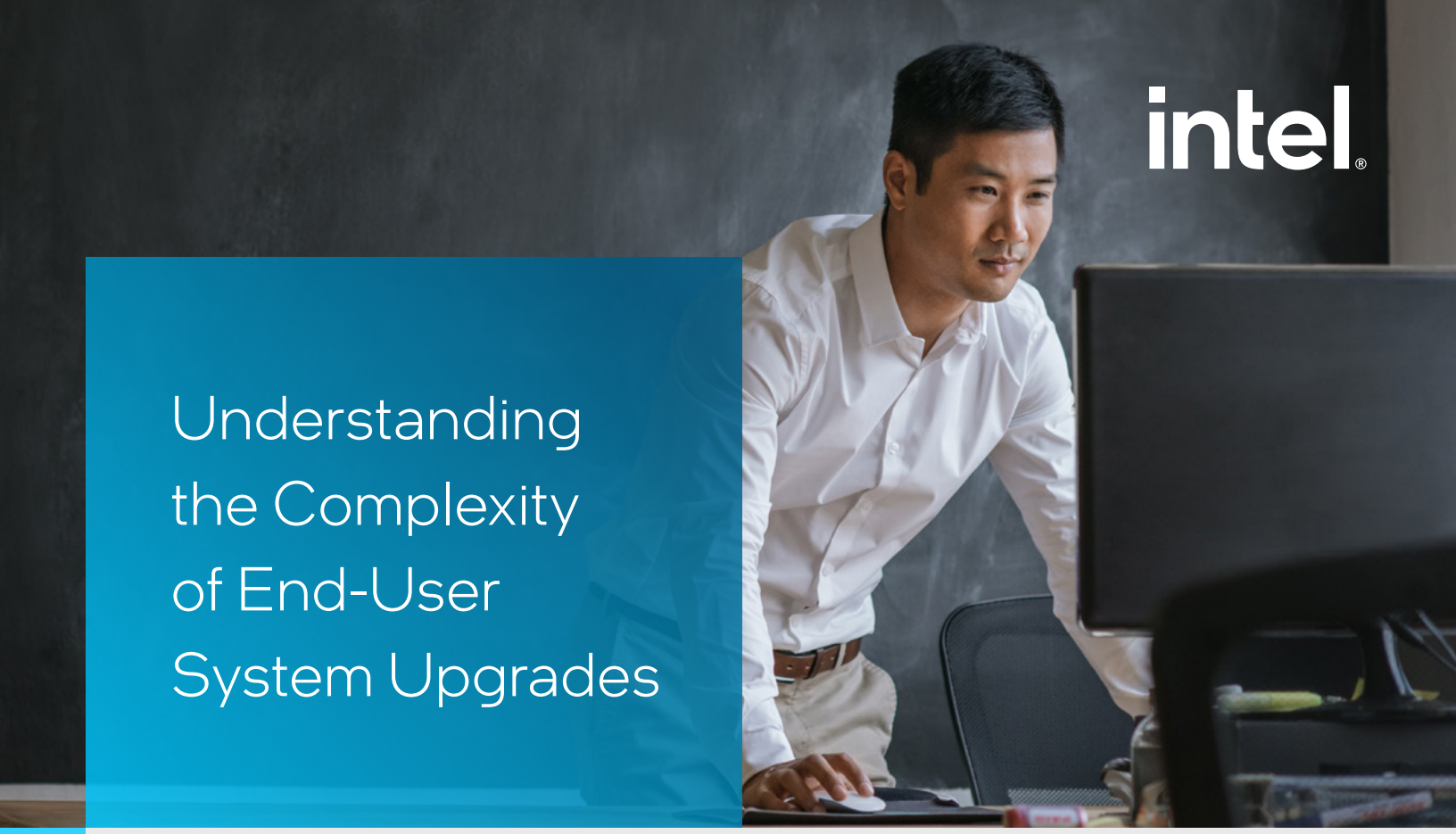

Understanding the Complexity of End-User System Upgrades

One of the most important roles that IT ops plays is verifying that employees across the organization have access to modern devices.

This helps deliver top productivity and the ability to leverage new applications and services. It also ensures the business can stay up to date with security measures and patches. An aging PC simply doesn't have the performance, flexibility, or ability to guard against the latest threats to make it viable for the business environment.

As a result, the PC refresh process is one place where IT ops can deliver outsized value to the organization. But if managed incorrectly, it can also introduce everything you're working so hard to prevent: lower productivity, higher costs, and increased security risks. In other words, complexity.

When sourcing new PCs, one of the critical factors to evaluate is the original equipment manufacturer's (OEM's) ability to guarantee build stability over the generation of the device. When IT ops decides to upgrade end-user PCs, it has to test the PC to confirm all its critical business applications work as expected.

Once a PC is validated, IT ops can then order more like it in batches as it replaces older PCs across the organization. However, if the OEM can't guarantee stability in terms of components and software across the generation of devices, the PC you buy for Employee A might not be the same one you buy for Employee Z.

Let's evaluate the challenges this lack of a stability guarantee can generate.

Validation complexity

Taking the scenario described above, you functionally have two different devices. The first is the one you validated, and the second is the one you didn't. To ensure security, you'll have to revalidate the second device, which costs time, money, and resources.

Now multiply this process with dozens of PC models representing the many different workstyles of your business users. You can see how simply testing and validating PCs could be a full-time job.

In addition, every time there's an operating system upgrade like the new Windows 11, you'll have to test the new OS against every device configuration. You'll also have to test the operating system's compatibility with all the business applications, drivers, and components found on each configuration.

This cascading complexity means it'll take longer to validate and install the upgrade. This can leave your business unable to access its latest and greatest features and functionality.

Security complexity

Every business relies on dozens or hundreds of applications to enable employees to do their best work. However, cybercriminals are working just as hard to find exploits in each of these programs and the underlying operating system they run on. They want to hack into your business, steal valuable data, conduct ransomware attacks, or just cause mischief.

While software developers work hard to create patches once a dangerous exploit is identified, that's only the first step. You must still deploy the patch to the end-user device.

However, as with device validation, IT ops must validate each patch against each device build to ensure compatibility. The more configurations, the longer it takes to protect the entire organization.

Management complexity

In addition to managing and updating software, you must manage hardware components. These components require frequent patching and driver upgrades. In addition, if they break, you need to be able to fix or replace them quickly so employees can get back to work.

The more device configurations to manage, the more components you have to track and maintain. This work can increase IT ops costs and time resources as you source and learn the nuances of the multiple component versions.

Component variability can also prevent you from being able to integrate new technologies and capabilities. It can lead some employees to have a poor experience compared to others who have PCs capable of fully leveraging the technology.

Reducing complexity through stability guarantees

As you can see, a little uncertainty can go a long way in increasing the complexity of end-user system upgrades. By leveraging a program like the Intel® Stable IT Platform Program, you help ensure consistent quality and performance throughout the generation of a device. How? By guaranteeing no hardware changes across the buying cycle for at least 15 months or until the next generational cycle.

It also helps remove the complexity of the refresh process by eliminating the risk of upgrade incompatibility. The benefits include:

- Shorter qualification cycles
- Consistent roll-out of validated devices across time
- Fewer platforms to manage over your workforce
- Consistent security and patching requirements
- Unified ability to integrate new technology
- Less complexity in the PC fleet upgrade process

Learn more about **Intel Stable IT Platform Program.**

intel