

# Discover the Synergistic Value of Dell Technologies, Intel vPro and VMware Workspace ONE

## Unlock the Combined Power of Dell, Intel and VMware to Modernize Security and Endpoint Management

As more and more organizations adopt hybrid work, employee productivity and workspace security have grown in importance. Today's distributed workers require flexibility in where they work and streamlined access to the corporate network. Similarly, IT teams have the challenge to ensure critical security needs aren't just met, they are executed seamlessly without interruption or delay.

That's where unified endpoint management (UEM) comes into play.

Although there are both hardware and software solutions to address the above challenges, each has its limitations – e.g., you trade a bit of security for performance and user experience or lose performance in favor of greater security. The best approach combines both hardware and software – and this is something that Dell, Intel and VMware have diligently worked to deliver to customers.

In our upcoming webinar, learn about the powerful integration across Dell business PCs, Intel vPro technology and VMware Workspace ONE. Rooted in the principles of Zero Trust, Dell commercial devices are built securely, with strict supply chain controls, and feature unique protections to help verify user identity and integrity of the BIOS and firmware. Dell PCs enabled with Intel vPro technology further safeguard the workspace, with an added layer of hardware-based security such as Intel Hardware Shield

which provides protection against foundational attacks "below-the-operating-system". This added layer also extends application protection with dedicated hardware-accelerated encryption.

The unique Intel vPro integration with VMware Workspace ONE UEM gives organizations the ability to unlock new security, management, and support capabilities for their IT teams and end users, including out-of-band management, from a single tool. IT teams can streamline endpoint security and management across any device and application with analytics and automation. Additionally, this exclusive integration provides IT admins key tools for remote security, support, access management, device configuration and maintenance. These capabilities offered via this cloud-native platform give IT admins the ability to support end users en masse with minimal disruption to performance or productivity.

With the additional integration of these solutions into Dell devices, IT groups are able to use Workspace ONE to utilize Intel vPro technologies to easily access and configure a system's BIOS with Dell Command Suite and remotely execute bare metal OS recoveries and restores, to quickly get employees back up and running.

Learn more about this combination of modern endpoint management combined with hardware-assisted security abilities during our upcoming expert panel discussion and demo. Unlock the value of modern security and cloud-native device management and help your organization move into the future of hybrid work.

## Read More

Interested in learning more? See these resources:

**Paper** [Endpoint Management Point of View Part 1 | Part 2](#)

**Blog** [Five Ways to Improve Security Through Modern Endpoint Management](#)

**Blog** [Scale Security with a Frictionless User Experience](#)

## Follow Us

Stay tuned for exciting new updates on this integration!

**Website** [dell.com/endpoint-security](https://dell.com/endpoint-security)

**LinkedIn** [/delltechnologies](https://www.linkedin.com/company/delltechnologies)

**Twitter** [@delltech](https://twitter.com/delltech)

## Contact Us

We're here to help!

Reach out to your Dell sales representative or complete [this contact form](#).