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

Solution

In a powerful new integration across Dell business PCs, Intel vPro technology and VMware Workspace ONE, IT teams can now leverage an improved cloud-native approach to monitor, restore, upgrade and protect their Dell PC fleet, both in- and out-of-band, from any location.

Key Benefits

- Configure, update, patch or restore Dell PCs, including on devices that are asleep, powered off or not functioning

- Perform remote maintenance with full keyboard, video, and mouse access on Dell PCs, even without a working operating system, minimizing the need to return PCs for maintenance

- Execute remote secure erase functions on Dell PCs from your Workspace One console

- Access and respond to PC wi-fi performance & battery health

- Remotely wake devices to push patches, removing user action to implement

- Easily access Dell Client Command Suite, enabling configuration of Dell BIOS and updates to firmware, drivers and applications

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 you 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 a powerful new integration across Dell business PCs, Intel vPro technology and VMware Workspace ONE, IT teams can now leverage an improved cloud-native approach to monitor, restore, upgrade and protect their Dell PC fleet, both in- and out of band, from any location. 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. *(cont'd on next page)*

D&LL Technologies

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 pane of glass. 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 can use Workspace ONE and Intel vPro technologies to easily access and configure a system's BIOS with Dell Client Command Suite and remotely execute bare metal OS recoveries and restores, minimizing user downtime. It also removes critical barriers for an IT team to maintain a secure PC fleet by enabling updating, monitoring and patching – regardless if a PC is asleep, powered off or without a functional operating system.

Unlock the value of modern security and cloud-native device management and move into the future of hybrid work with Dell commercial PCs, Intel vPro technology and VMware Workspace ONE.

Key Capabilities

Streamlined Manageability
- Centralization of device management via one pane of glass, the VMware Workspace ONE console, creating efficiency when working across complex and large IT environments
- Seamless remote management, enabling IT teams to manage any task from anywhere
- Integration with Dell Command Suite enables easier BIOS configurations and restores
- Ability to remotely wake a Dell PC, deploy required OS and application patches and profiles, and put the PC back to sleep mode
- Manage devices while in- or-out-of-band

Improved Security
- Minimize blind spots in the IT environment with out-of-band device management
- Out-of-band updating and patching enables optimal security compliance of all devices
- Grant access by device efficiently, defining strict rules around permissioning and contextual behavior
- Ease in accessing key security features of Intel vPro technology, such as Intel Hardware Shield
- Easily execute secure erase functions to protect against threats

Increased Productivity
- Enabling out-of-band PC management saves time for IT teams, enabling updating, patching and restoring when a PC is asleep, powered off or without a functioning operating system
- Ability to execute bare metol OS recoveries and restores, improves productivity for employees and IT teams
- Increased ease in identifying and predicting employee experience issues for faster remediation
- Extends remote support capabilities to keyboards, video and mouse access via VMware Workspace ONE

D≪LL Technologies

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

Overview of Integrated Technologies

Intel® Active Management Technology (Intel® AMT), Available Exclusively on the Intel vPro Platform
Modern cyber threats have grown more complex, and devices are not always powered on and available to push patches to. Intel AMT enables a persistent out-of-band connection to devices below the OS and allow a hardware-based keyboard, video, and mouse (KVM) session for accessing a device, regardless of OS functional state. With the Intel vPro platform, IT can regain control of systems from anywhere, even devices without a functioning OS.

VMware Workspace ONE
A cloud-native, modern solution enables organizations to improve security, automate IT operations, and improve employee experiences across every PC, whether on or off the company network. With Workspace ONE, devices can be provisioned and deployed to employees directly from the factory, configured and patched over-the-air and in real-time, and supported remotely and proactively. IT can orchestrate and automate processes as well as collect actionable insights to address user issues proactively. As users and IT work remotely and must do more with less, Workspace ONE enables modern approaches to unified endpoint management that includes Windows PC management.

Dell Client Command Suite
Dell Client Command Suite is a comprehensive collection of system management tools that automate and streamline client device image setup, configuration, monitoring and updates. IT can ensure systems stay secure and up-to-date over the course of the PC lifecycle with less time, effort and resources using Dell Client Command Suite. By automating and streamlining endpoint management, Dell Client Command Suite helps IT minimize tedious, time-consuming and error-prone tasks. Included with commercial client systems, Dell Client Command Suite allows you to do more with less so you can optimize time spent managing your fleet.

Read More

Interested in learning more? See these resources:

Dell Client Command Suite
Intel vPro Platform and Workspace ONE UEM Integration
VMware | Intel

Follow Us

Stay tuned for exciting new updates on this integration!

Website dell.com/endpoint-security
LinkedIn /delltechnologies
Twitter @delltech

Contact Us

We're here to help!

Reach out to your Dell sales representative or complete this contact form.

DELLTechnologies