PC AND THE CLOUD ECOSYSTEM SOLUTIONS FROM LENOVO

Lenovo™

EFFECTIVE DEVICE MANAGEMENT AND SECURITY SOLUTION DATASHEET Ver. 1.0

Businesses win half the battle by choosing the right endpoint devices and Cloud solution. It is also essential to have a good device management system to ensure complete visibility and control of networks and devices for higher uptime and better security.

Lenovo's PC and the Cloud Ecosystem solutions enable you to kick-start your future growth by addressing every aspect of IT.

SOLUTION SETS

EFFECTIVE ENDPOINT DEVICES

EFFECTIVE DEVICE MANAGEMENT AND SECURITY

ENDPOINT DEVICE MANAGEMENT

Effective Device Management and Security

DATA SECURITY AND USER AUTHENTICATION

5 reasons
why Lenovo is a difference maker
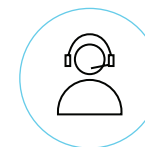
Trusted around the world

Expertise across categories

Confidence in our products

Business-boosting technology

Flexible support network

(intel)

Powered by Intel®.
Intel Inside®.
Powerful Productivity Outside.

ENDPOINT DEVICE MANAGEMENT

Designed to meet every stage of need in a PC and the Cloud Ecosystem, Lenovo's endpoint device management solutions range from preloaded and built-in technology to powerful, partnership enabled solutions for Think devices.

PRELOADED TOOLS

Lenovo Vantage unclutters the PC experience and makes it easier for users to get the most out of their Lenovo devices. It reduces the cost incurred in procuring resources for system updates and upgrades to prevent any cost due to human error or unwanted attacks. It is the only Lenovo-branded preloaded application on systems running Windows 10.

- Personalize your settings
- Improve your WiFi security
- Update drivers
- Run device diagnostics
- Identify the system serial number and product number
- Request support

HARDWARE ENABLED MANAGEMENT

In the event of an attack, new **8th Generation Intel® Core™ vPro™ Processor**-based computers with **Intel® Active Management Technology (Intel® AMT)** help you stay prepared for recovery. By installing **Intel® Manageability Commander (Intel® MC)** into your Microsoft SCCM* console (System Center Configuration Manager), you can use **Intel® AMT** to remotely take a compromised device off the network so a virus doesn't spread. Even if the operating system is down, or the device is without power, the PC can be reimaged and brought back to a good state without costly deskside visits.
*Sold separately

OS ENABLED MDM

Windows 10 Pro provides a consistent set of configurations across device form factors through a common MDM layer. Manage Active Directory Domain-joined devices through MDM, and migrate easily to a Cloud-based management service.

Windows MDM shows users what policies, settings, and apps are managed by their organization and what their status is, so end users know when their devices are ready for productive use. This lowers help desk calls and allows administrators to easily troubleshoot issues. Users get fewer, shorter interruptions if they run into problems with mobile access to corporate resources. MDM can implement policies on devices even when users are not active. And, if a device is offline or asleep, Windows Notification Services will deliver policy updates when it is back online.

INDUSTRY LEADING EMM WITH MOBILEIRON

The global strategic partnership of Lenovo and MobileIron EMM ensures secure provisioning and simplifies endpoint device management. It incorporates identity, context, and privacy enforcement to set the appropriate level of access to business data and services. MobileIron secures data-at-rest on the mobile device, in mobile apps, desktop and in Cloud storage. Additionally, the MobileIron EMM platform secures data-in-motion as it moves between the corporate network, devices, and various on-premise and Cloud storage repositories.

COMPLETE DEVICE MANAGEMENT SOLUTIONS

- Lenovo Vantage warns users against nearby real-time threats, letting them work in a secure environment

- **Intel® Active Management Technology** is an advanced toolset that allows IT pros to manage computers remotely and out-of-band

- Access consistent set of configurations across device form factors through a common MDM layer with Windows 10 Pro

- MobileIron enables security for endpoints, networks, apps and Cloud — all in one platform

DATA SECURITY AND USER AUTHENTICATION

Endpoint devices are the gateways to data stored in the Cloud. For this reason, they must be adequately secured from unauthorized access, unsafe networks, and data theft/corruption. Lenovo's data security and user authentication solutions range from built-in technology to simple and effective protection services for Think devices.

FAST IDENTITY ONLINE (FIDO) FOR CUTTING EDGE USER AUTHENTICATION

Many ThinkPads are FIDO enabled. FIDO authentication pertains to online credentials when users sign into internal and external websites or make payments online. This global solution creates better security for online services, reduces costs for organizations, and is simpler and safer for users. It ensures hardened authentication and wraps access information into three layers of security.

HARDWARE ENHANCED MULTIFACTOR AUTHENTICATION

ThinkPad laptops are integrated with **Intel® Authenticate** solution that gives IT the flexibility to create and deploy customized hardened multifactor authentication policies to enforce user identity protection for access to the corporate domain, network, and VPN. **Intel® Authenticate** solution provides a simple self-service enrollment tool for end users to quickly get started, eliminating calls to IT.

LENOVO VANTAGE FOR IN-BUILT WIFI PROTECTION

Using Cloud based services and applications means being connected always, anywhere. This presents a great risk as malicious WiFi networks can compromise employee and business data.
Designed to monitor WiFi security in real-time, Lenovo Vantage can distinguish between legitimate networks and risky, possibly malicious networks. It can also detect threats or attacks that are present near the laptop and alert the IT to it, for further action.

*Now a standard preload on all Lenovo systems running Windows 10

ABSOLUTE WITH PERSISTENCE TECHNOLOGY

ThinkPads have the Persistence agent from Absolute embedded into the firmware. Persistence is the only technology that keeps you in complete command with a self-healing, two-way connection to any endpoint or application — even if they are off the network. With Absolute Persistence:

• Guarantee the connection with every endpoint — on or off the network

• Remotely invoke adaptive security commands to limit damage and protect data

• Reach any device, anywhere and execute custom scripts to remediate threats

• Scan for sensitive data on an endpoint that's no longer in your control

• Be notified if encryption, SCCM, or anti-virus, or any other security or IT management applications are removed or corrupt

SAFE AND SECURE USER EXPERIENCE

Lenovo Vantage

OLDB

FIDO

ABSOLUTE

Hardware Enhanced Multifactor Authentication
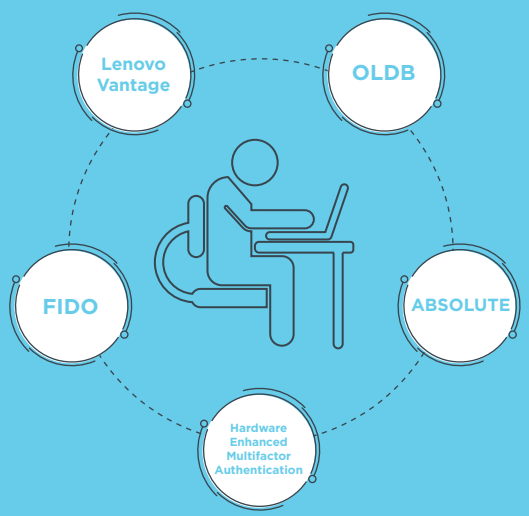
PREVENT DATA LOSS EASILY

- OLDB is compatible even with non-Lenovo hardware

- Data centers are SAS-70, ISO 27001 certified, where applicable and adhere to European Safe Harbor Privacy Policies

- OLDB allows up to 90-days of version control for files

- Private encryption key ensures no one but the user has access to the data, including Lenovo

ONLINE DATA BACKUP (OLDB)

Lenovo's Online Data Backup is an easy-to-use, automatic online backup and recovery software solution. With this tool, organizations and user groups can share a pool of storage without the administrator assigning storage to specific users.

Requires no capital expenditures for hardware; low upfront investment with minimal maintenance overhead

Relative to tape-based approaches, OLDB is more efficient, less intensive for the operator, and not as prone to human error

Reliable Data Protection

- Safeguards business data from accidents, operating system and application errors, hard drive failures, and other unexpected risks

- Sync functionality allows users to access data from any device

- Compatible with all Think and Lenovo-branded systems, as well as with non-Lenovo branded hardware

Secure Storage and Access

- Data is encrypted using 256-bit AES enterprise-grade encryption for private encryption key and data storage. It is then transmitted to secure data centres using 128-bit SSL encryption – same as online banking

- The optional single sign-on automatically triggers user creation from a federated identity provider (like Active Directory)

- Users can access their data from anywhere in the world with the option of owning a personal encryption key for an added layer of security

Simple Management

- No need to manage user licenses

- The web-based administrative console provides easy account management, allowing users to either select preconfigured backup and recovery settings or customize them

Easy Deployment

- No additional hardware is required. The Lenovo OLDB software is downloadable from the web.

- Professional service options available with OLDB include:

  - Basic setup and test
  - Activation and testing
  - Eight or four-hour administrative training

  - Level 1 support training
  - Federated ID
  - Single sign-on