

# WORKPLACE EFFICIENCY SOLUTIONS

Lenovo's downtime reduction solutions focus on aligning IT with user's needs for maximum efficiency.

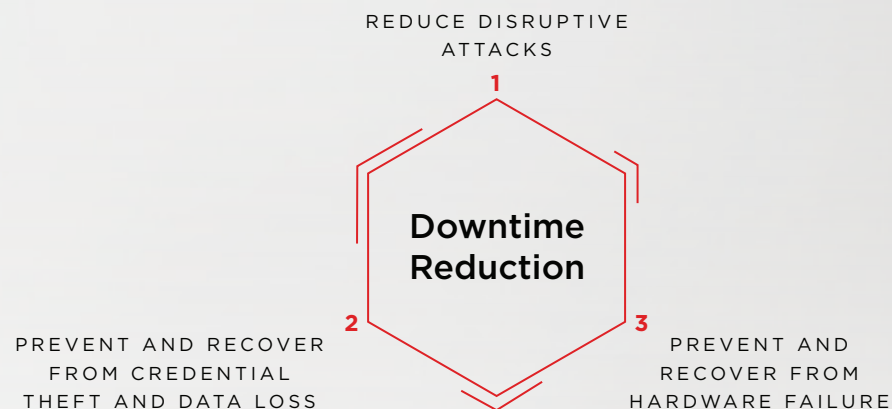
## SOLUTION SETS:

- | WORKPLACE OPTIMIZATION
- | DOWNTIME REDUCTION
- | IT AUTOMATION

# DOWNTIME REDUCTION SOLUTION DATASHEET

Ver. 1.0

Downtime can harm your business in many ways: decreased work efficiency, IT costs, data loss, and negative publicity. Cutting the risk of downtime improves workplace efficiency.



## 5 reasons why Lenovo is a difference maker



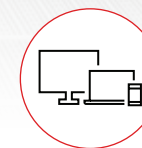
Trusted around the world



Expertise across categories



Confidence in our products



Business-boosting technology



Flexible support network



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

## ENSURE A SAFE AND SECURE WORKPLACE

- BUFFERZONE helps shield user data from malicious attacks to help users stay efficient
- Enable easy and secure collaboration with Secure Bridge
- Identify potential threats and reduce IT dependency

## CORONET MINIMIZES THE RISK OF EVERYTHING BEING CONNECTED

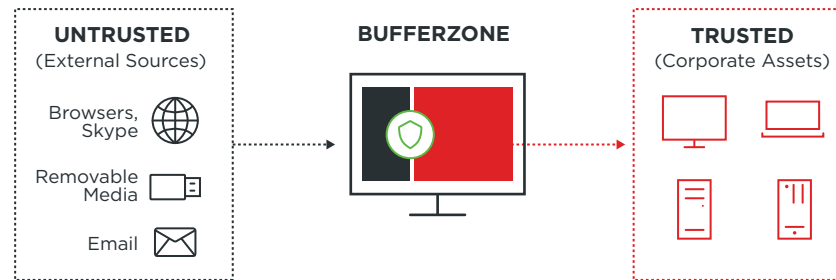
- Forbid connections to risky networks
- Block access by rooted mobile phones
- Allow connection OS updated devices only
- Get notified of users who are in proximity to risks
- Implement geo-fencing of corporate box accounts

## REDUCE DISRUPTIVE ATTACKS

It is essential to have the right protection to prevent cyber-attacks that can disrupt the business and result in loss of reputation.

### BUFFERZONE® – Sophisticated and supreme malware protection

Without restricting or inconveniencing employees, BUFFERZONE protects endpoints and trusted organizational resources from any kind of malware. It isolates browsers and applications that come into contact with the internet and other untrusted sources, in their own, virtual environment.



### BUFFERZONE'S advanced endpoint security solution features:

- **Virtual Container:** a secure, isolated environment for accessing content from any potentially risky source.
- **Secure Bridge:** a configurable process for extracting data from the container to enable collaboration between people and systems.
- **Endpoint Intelligence:** detailed reporting and integration with SIEM and Big Data analytics to identify targeted attacks.

### Coronet – Intelligent and secure WiFi experiences on Think devices

Productivity can only be achieved when there is confidence in the wireless networks surrounding the device. Coronet can detect and evade unsafe wireless connections over both WiFi and Cellular networks. It requires no installation and ensures that only trusted devices, networks and Cloud services can access your data.

### FULLY FUNCTIONAL PROTECTION FROM DAY ONE

Management credentials for sanctioned services	Fully functional system	5 min. per service
Corporate email domain association	Client activation by email	5 min.
IDP access settings	Device authentication	5 min.
AD access settings	Import AD user groups Transparent client activation via MDM	5 min.
SIEM access settings	Incidents export to SIEM	5 min.

# PREVENT AND RECOVER FROM CREDENTIAL THEFT AND DATA LOSS

A data breach can cost organizations time and money. IT teams need to monitor and protect their users against credential theft and data loss.

## DATA PROTECTION SOLUTIONS

- Automatic online data backup (OLDB) recovery solution for software reduces IT dependency
- Lenovo Vantage warns users against nearby real-time threats, letting them work in a secure environment
- Unbreakable encryption to keep your data safe without any third-party encryption solutions, eliminating hassles

### Fast Identity Online (FIDO)

Fast Identity Online (FIDO) authenticates and wraps your online credentials by three layers of security while working on a ThinkPad. This global solution creates better security for online services, reduces costs for organizations, and is simpler and safer for users.

### Hardware enhanced multifactor authentication

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

### Lenovo Vantage

Enables Lenovo WiFi Security that detects and analyzes in real-time any nearby threats or attacks and distinguishes between legitimate networks and possibly risky and malicious networks. This keeps your network free from uninvited elements.

\*Now a standard preload on all Lenovo systems running Windows 10; existing systems received Lenovo Vantage as an automatic update in December.

### Absolute with Persistence technology

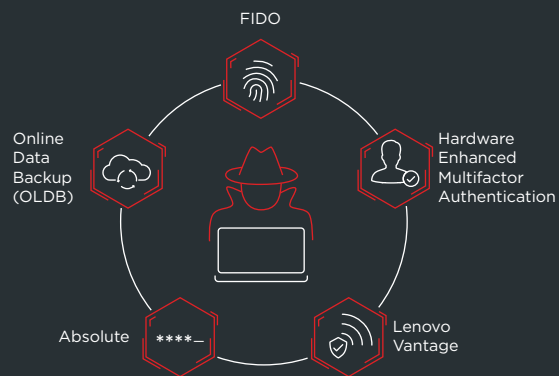
ThinkPads have the Persistence agent from Absolute embedded into the firmware. Persistence is the only technology that keeps you in complete command with a self-healing, two-way connection to any endpoint or application — even if they are off the network. With Absolute Persistence,

- 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

### Online Data Backup (OLDB)

Lenovo's Online Data Backup is easy-to-use, includes automatic online backup and recovery solution for software. 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
- Allows users to retrieve personal data from the secure OLDB Cloud without assistance from IT



# PREVENT AND RECOVER FROM HARDWARE FAILURE

To prevent or quickly recover from a hardware failure it is essential to have a device that can withstand everyday bumps and drops and survive the vagaries of remote locations, such as temperature and surroundings.

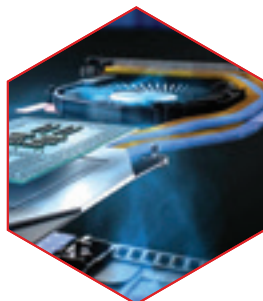
## NO MORE SYSTEM FAILURES

- Lower failure rate with Intelligent Cooling Technology in ThinkPads and Intelligent Cooling Engine in ThinkCentres
- Protection of devices due to unintentional damage to keep users worry-free at work
- **Intel® Active Management Technology (AMT)** helps devices recover faster



### MIL-STD testing leadership

Since 2007, Lenovo has used the US Department of Defense's MIL-STD 810G standards to strike the perfect balance of value and durability. ThinkPad products are currently tested for 12 total methods and 23 procedures. ThinkCentre Tiny models are tested in extreme environments including temperature, pressure, dust, humidity and vibration.



### Cooling technology

The Intelligent Cooling Technology of ThinkPads and the Intelligent Cooling Engine (ICE) in ThinkCentres maintain temperatures at an optimal level for high-performance computing. It allows ThinkPads to be up to 15% cooler and 10% quieter.



### Accidental Damage Protection (ADP)

Accidental Damage Protection (ADP) is a Lenovo Protection Service that minimizes the repair costs associated with non-warranted damage, such as LCD breakage.

© 2018 Lenovo. All rights reserved. These products are available while supplies last. Prices shown are subject to change without notice. For any questions concerning price, please contact your Lenovo Account Executive. Lenovo is not responsible for photographic or typographic errors. Warranty: For a copy of applicable warranties, write to: Warranty Information, 500 Park Offices Drive, RTP, NC 27709, Attn: Dept. ZPYA/B600. Lenovo makes no representation or warranty regarding third-party products or services. Trademarks: Lenovo, the Lenovo logo, Rescue and Recovery, ThinkPad, ThinkCentre, ThinkStation, ThinkVantage, and ThinkVision are trademarks or registered trademarks of Lenovo. Microsoft, Windows, and Vista are registered trademarks of Microsoft Corporation. Intel, the Intel logo, Intel Inside, Intel Core, and Core Inside are trademarks of Intel Corporation in the U.S. and/or other countries. Other company, product, and service names may be trademarks or service marks of others.