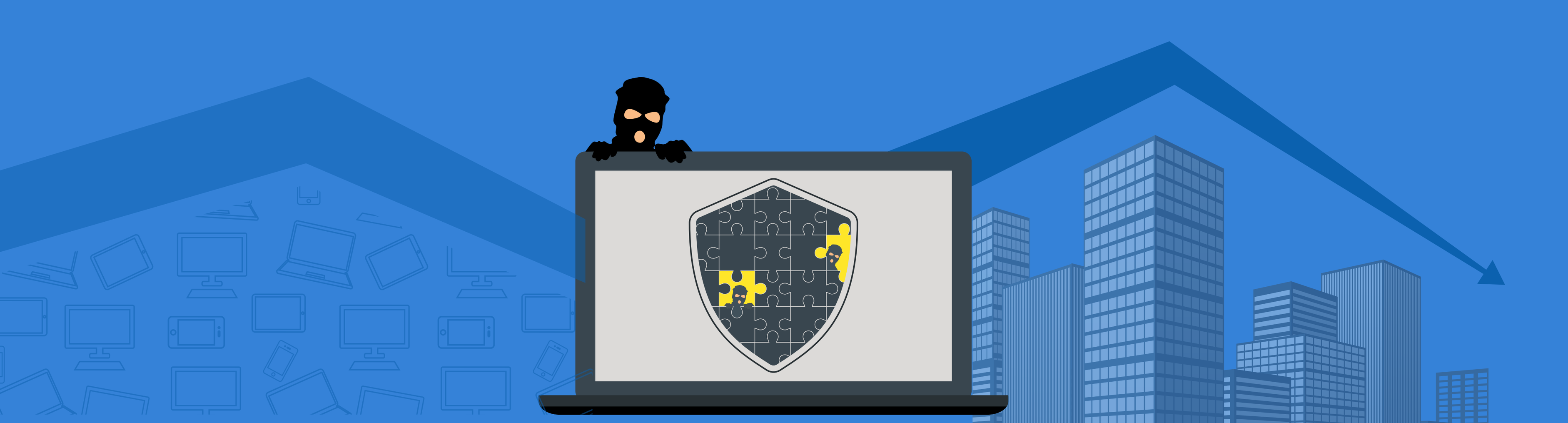


Unsafe Devices Can Be Detrimental to Your Business

Digitization is making data generation and accessibility easy for everyone. Including hackers. With strict regulatory policies around the globe, securing organizational data is more than just another technology investment.

Regulatory Policies around the Globe

USA

- The Federal Trade Commission Act prohibits deceptive practices on private data
- The Financial Services Modernization Act regulates the collection and disclosure of financial information
- Computer Fraud and Abuse Act regulates the interception of computer tampering

EUROPE

GDPR: effective May 2018

- Protects and increases personal privacy rights
- Governs the way data is managed and protected
- Penalizes heavily in case of non-compliance

LATIN AMERICA

- Implements constitutional rights-based model (Habeas Data)
- Executes comprehensive data protection laws
- Combines Habeas Data and comprehensive data protection laws

ASIA PACIFIC

- China's Cyber Security Law forbids using any information network to violate privacy
- Singapore's Personal Data Protection Act provides guidance for businesses and consumers
- Hong Kong's Privacy Ordinance regulates collection, use and handling of personal data

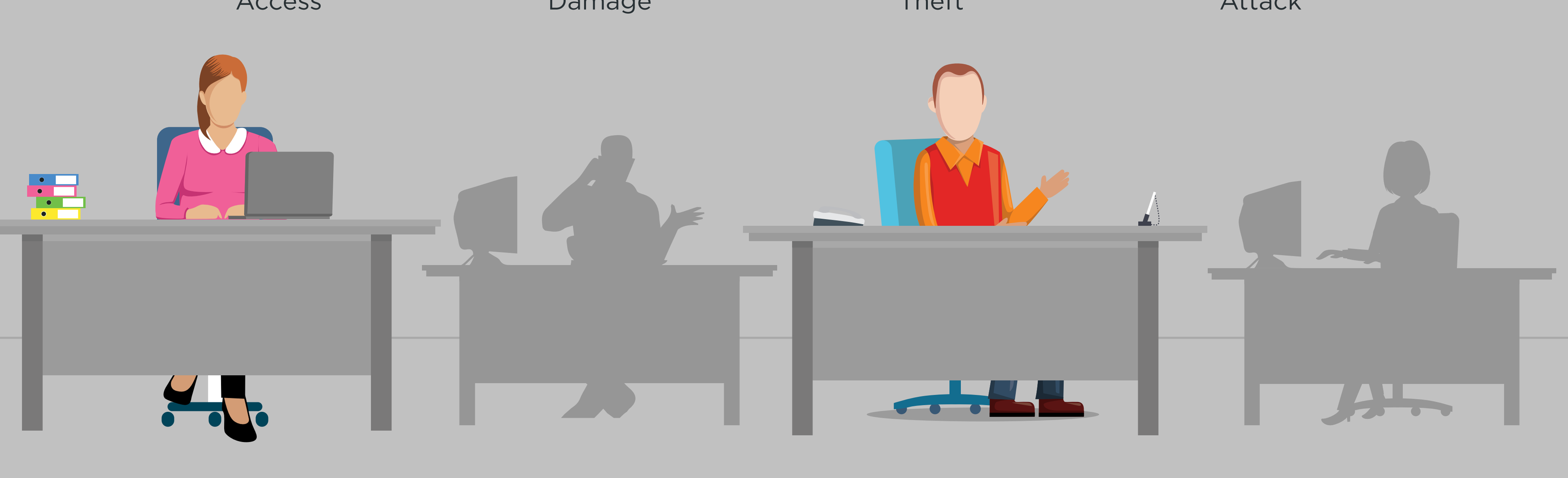
Network authentication and infrastructure security would be in vain if endpoint devices are not secure. Loss through endpoint devices can cost any organization a fortune:

Unauthorized Access

Device Damage

Device Theft

Ransomware Attack



So What Should You Do?

Choose Lenovo End Computing Devices Which Imbibe Lenovo's 360° Security Policy

User Access Control

Grant PC Access to Authorized Personnel Only

Multi Factor Authentication

Biometric security feature using fingerprint recognition

Smart Card Access

No passwords needed. Secure login credentials in a tamper-proof card

Near Field Communication

Security based on radio communication and user proximity

Match On Chip Fingerprint Reader (MoC FPR):

Technology in which biometric credentials are stored on a separate chip, making it almost impossible to hack into a PC. It also strengthens identity and data protection with the support of **Intel® Authenticate Technology**.

Port and Physical Protection

Prevent Data Theft from a Corporate Device

Smart USB Protection

Blocks data transfer capability of the USB port but keeps the port functional for input devices

Camera Shutter

Ensures user privacy and security by closing the built-in camera shutter

Chassis Lock

A lock and key mechanism to restrict access and prevent theft of components like graphics card and hard drives

Data Protection

Protect and Secure Data

Full Drive Encryption

Encrypts hard drive to avoid unauthorized access to data and sophisticated attacks

Data Backup

Backs up business data online or in server stacks where it is accessible and secure

Hard Drive Retention

Allows the company to retain the original hard drive and data when it is replaced under warranty

Lenovo Is Your First Choice for Security

Lenovo's 360° approach to security ensures best-in-class end point devices

Lenovo Security Philosophy

Best-in-class Hardware Security

Securely Developed Software

Complete Component Verification

Secure Supply Chain

Adoption and Extension of Security Technology

Think Security. Think Lenovo.

Lenovo™

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