SWK
NETWORK SERVICES

White Paper

Lenovo

Global Security Compliance and Its Technological Implications

Windows 10 Pro

Lenovo recommends Windows 10 Pro.

www.lenovo.com

Aligning with Global Security Regulations

Sophisticated security threats have created the need for a holistic approach to building a strategy to keep users, business devices, networks, and data protected.

This paper will help you understand how Lenovo's 360° security strategy can assist you to align with global governance regulations by adopting a holistic approach to security leveraging Lenovo's security philosophy.

Windows 10 Pro

Lenovo recommends Windows 10 Pro.

The Need for Cyber Security Norms

Digitization has led to data proliferation. Organizations are struggling to handle the sheer volumes of data. Meanwhile, the abundance of valuable information has also captured the attention of subversive elements. Cyber criminals have breached networks and compromised billions of data records, not only causing revenue losses but also impacting brand equities.

Windows 10 Pro

Lenovo recommends Windows 10 Pro.

Breaches in Recent Years

18 Hyatt properties in China were affected when a hacker got access to credit card details

Cybercrime steals 15-20% of the value created by the Internet[1]

28 million users of Reddit in Latin America had their login credentials compromised

Benesse Holdings, a Japanese education service provider compromised the personally identifiable information of up to 20.7 million people

In 2011, the personal data of 35 million South Koreans was stolen from a social networking site

Over a billion data records breached in 2013[4]

81% of large and 60% smaller UK-based companies reported cyber breaches in 2014[3]

Losses caused by security compromises increased by 34% in 2014[2]

In 2014, 500 million Yahoo user accounts were tampered with

In 2016, Uber suffered a data breach that affected 57 million customers and drivers worldwide. Uber in return paid $100,000 to the hackers to delete the data

Footnotes:

1 Intel/McAfee, “Net Losses: Estimating the Global Cost of Cybercrime,” June 2014. http://aka.ms/mcafee-cybercrime-report
2 PWC, “Global State of Information Security Survey: 2015.” http://aka.ms/pwc-cybercrime
3 UK Dept. for Business, Innovation and Skills, “2014 Information Security Breaches Survey.” http://aka.ms/uk-gov_breach-survey
4 Gemalto, 2014 Breach Level Index Report

Setting Global Governance Standards

Combating cyber threats is no longer the exclusive domain of IT service providers. Governments and cyber law enforcement agencies across the world have also been coming together to help overcome this challenge. Companies and governments are working together to evolve newer, higher standards of cyber security that would not only help save billions of dollars in losses, but also create a safer environment in which they can manage their confidential information efficiently and effectively. Strict legislation is being enacted, and mandatory industry standards are in place to protect massive volumes of business-sensitive information and facilitate complete customer privacy.

Laws which existed since 2003 (Japan's Act on the Protection of Personal Information) to laws which will be effective in 2018 (EU's General Data Regulation and Protection) all have a single point focus – PROTECT PERSONAL INFORMATION. These laws are expected to make a huge global impact.

Windows 10 Pro

Lenovo recommends Windows 10 Pro.

USA

The United States has a system of federal and state laws which are considered as best practices. The self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators. The objective of the laws is to improve cybersecurity in the United States. At least 42 states have introduced more than 240 bills to deal with cybersecurity. The Acts enforced influence the IT infrastructure of various industries.

EUROPE

The General Data Protection and Regulation (GDPR) Act is a regulation policy that will likely make significant changes in how organizations gather, use and manage data regardless of where it is sent, processed, or stored. The key elements of GDPR are:

- Increased personal privacy rights
- Augmented accountability for protecting data
- Mandatory data breach reporting
- Significant penalties for non-compliance

According to the Financial Times, the maximum fine for failing to comply with the regulation is 4% of the previous year's annual global turnover, or €20m, whichever is the higher.

LATIN AMERICA

There is no single document for the whole region. Most of the laws are based on the EU Data Protection Directive 95/46 EC (the EU Directive). The categories into which the data protection frameworks fall into are:

- Constitutional rights-based model, i.e. **Habeas Data** which is the right to have access to information and comprehensive data protection laws.

ASIA PACIFIC

Countries like China, Japan and Singapore have implemented personal data protection acts which forbid people from using:

- Information networks to violate the privacy of others
- Illegal methods to acquire personal information
- Their positions of access to acquire, leak, sell or share personal information

Technological Implications

The security regulations for data privacy has changed the way organizations process data. The regulations ensure that technology failure is negligible in the case of an external or internal attack. Any case of mismanagement on the enterprise or employee part opens a line of enquiry to reconsider the IT infrastructure of the organization.

How Do You Collect Data?

With the government regulations being enforced, it is essential to keep the process of data collection and processing transparent. Organizations that collect personal data without user consent will be subject to high penalties – increasing their responsibility in collecting and analyzing data.

How Do You Store Data?

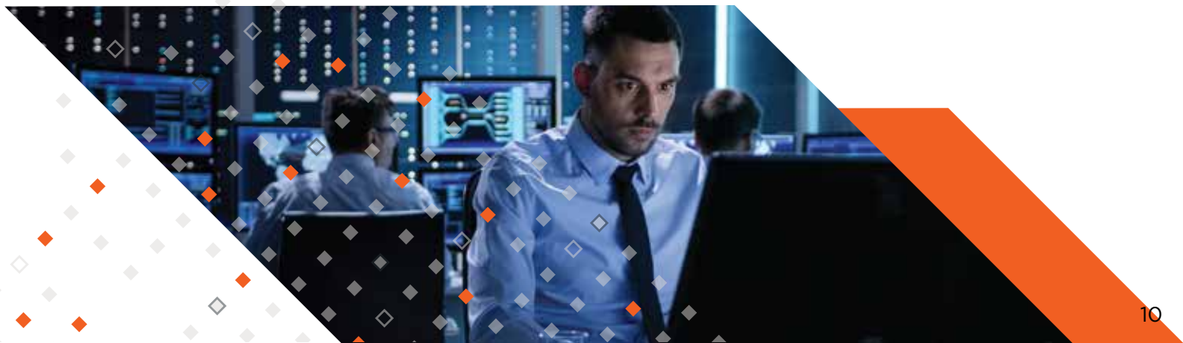
Once all the data is collected, the next big challenge is to store it safely – in silos or in the cloud. Therefore, organizations are moving towards setting up the right IT infrastructure which helps them store data securely without compromising on accessibility.

Is Your Data Protected at All Times?

Keeping in mind the huge amount of penalty organizations have to pay in case of a data breach, protection of data at a hardware as well as software level is essential. This is done by prevention of unauthorized access, disclosure or damage to your data. Securing data through passwords is not enough. Encryption and access control at all points help mitigate and manage risks. If governments sense any potential threat to an organization's big data, they're likely to penalize these organizations heavily.

How Do You Comply With User's Rights?

Due to the 'right to erasure' given to users, they can ask to delete or demand a physical copy of their data anytime they want. Conforming to such requests is compulsory. The right IT framework helps organizations comply with such requests efficiently.



Lenovo's Approach to Compliance with Global Norms

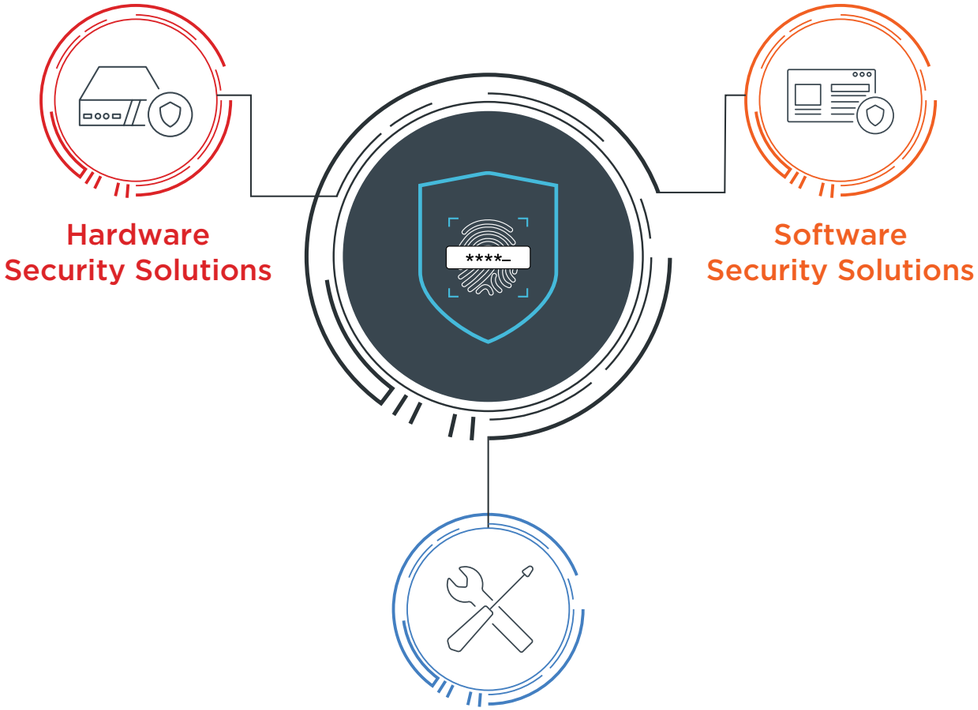
Lenovo is the only vendor to offer a 360° approach to security. It can be easily leveraged to protect your business and your users, because it is strongly implemented across all Lenovo business products and software.

We look at security in terms of solutions and have come with DIOD – an acronym to describe the four different areas that we focus on around security solutions. DIOD stands for Data, Identity, Online and Device. The focus is on how you protect data that is on your device and provide strong security and identity.

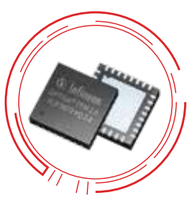
Lenovo believes in keeping customers and their data safely protected, no matter where they are located. Specially designed Lenovo security features comply with local government mandates and can easily be leveraged to protect businesses, networks, and users against theft or loss resulting from onsite or remote cyber-attacks.

Windows 10 Pro

Lenovo recommends Windows 10 Pro.



Hardware Security Solutions



Data Encyrtption: encrypt your data with dTPM 2.0 chip which is a built-in feature of ThinkPads, ThinkCentres, and ThinkStations. Lenovo's Discrete Trusted Platform Module (dTPM) encrypts all of your data, including passwords, automatically to the PC. You don't have to worry about securing your data afterwards.

Secure Hard Drives: safeguard your essential data on-the-go with ThinkPad Secure Hard drives which offer high-level 256-bit Advanced Encryption Standard (AES) security, in real-time.

Windows Hello: Windows Hello uses biometrics sensors to recognize you, so when you unlock your device with your face you get a superior level of enterprise-grade protection.

ThinkPad Glance: allows automatic locking using the Infrared camera when you are away from your device. ThinkPad Glance can be controlled by the local IT Department to lock at a certain level ensuring that the device is secure.

Privacy Filters: the requirement to protect sensitive data is even more critical in light of the security regulations. Lenovo privacy filters come with patented 3M microlouver privacy technology so only people directly in front of the display can clearly see the image ensuring no one else can peep into your screen.

Windows 10 Pro

Lenovo recommends Windows 10 Pro.

Port Protection: by keeping your port accessible for input devices like mouse and keyboard only, Lenovo's Smart USB protection disables ports to help prevent data theft and network security risks against unauthorized use of storage devices.

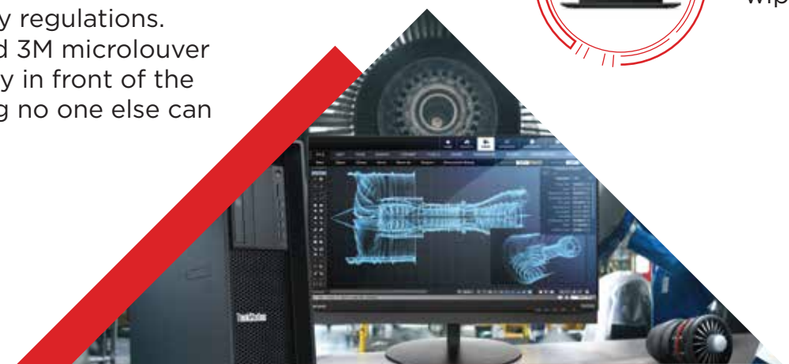
Match on Chip Fingerprint Reader (MoC FPR): back in 2004, the ThinkPad T42 became the first notebook PC to include a built-in fingerprint reader. Since then, we have continued to upgrade and improve fingerprint technology and the user experience.

MoC FPR is the most secure fingerprint technology on a PC. Your biometric credentials are stored on a separate chip, making it almost impossible to hack into.

- Further strengthen your authentication with **Intel® Authenticate** which 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, protecting identity and securing data. **Intel® Authenticate** provides a simple self-service enrollment tool for end users to quickly get started, eliminating calls to IT.

Security Cable Lock: the Lenovo Security Cable Lock allows you to manage endpoint device safety within the enterprise. Cable lock helps reduce theft and increase endpoint device security protection for notebooks, docking stations, desktops and flat panel monitors.

Remote Data Wipe: don't waste time by manually wiping drives. **Intel® Remote Secure Erase** for **Intel® Solid State Drives** are managed by **Intel® Active Management Technology,** and help you wipe SSD media and delete encryption keys faster and efficiently.



Software Security Solutions

Lenovo XClarity™: organizations suffer when they don't report a data breach to the Government. According to the regulations, it is obligatory to report a data breach within 72 hours of its occurrence. And if you have no record of who had access, then you are in trouble.

Lenovo XClarity™ Administrator is a centralized resource management solution that is aimed at reducing complexity, speeding up response, and enhancing the availability of Lenovo server systems and solutions. Lenovo XClarity includes features like firmware management, configuration management, OS provisioning, hardware monitoring and management.

Documentation is key to ensuring compliance here. Lenovo XClarity includes an audit log that provides a historical record of user actions, such as logging on, creating users, or changing user passwords.

Lenovo Absolute: losing your company device makes the organization prone to data attacks.

The Lost & Found service of Lenovo Absolute combines software from Absolute and security tools from Lenovo with additional alerts that make it easy to return missing PCs to their registered owners. Absolute's software traces the stolen device and makes it easier for the authorities to get it back.

Windows 10 Pro

Lenovo recommends Windows 10 Pro.

Security Services & Support

Keep Your Drive (KYD): the Keep Your Drive (KYD) service from Lenovo allows you to keep your Lenovo drive and data within your custody, improving security and potentially alleviating civil liability risks. It lets you dispose off business data on your terms and helps your organization avoid the legal and monetary consequences associated with a breach of data security.

Online Data Backup (OLDB): the crucial task of backing up data can be an exigent and expensive endeavor, especially for larger businesses. And only backing up the data isn't enough – having the flexibility to access it whenever you want is also an essential factor.

Lenovo OLDB is a powerful solution for endpoint data backup. Backed by Mozy by EMC, OLDB can give you the confidence that your company data is safe, secure, and available when you need it.

Product End-of-Life Management (PELM): PELM is the reuse, refurbishing, demanufacturing, dismantling, reclamation, shredding, recycling, treatment and disposal of products, parts, and options when they are taken out of service, reach end of life, and/or scrapped. This ensures that your personal data or corporate data never falls into the wrong hands.

Encryption Services: hard drive encryption is essential to avoid unauthorized access to data and sophisticated attacks. Lenovo's data encryption services encrypt all your data to the PC automatically.

Conclusion

Data protection regulations all over the globe have technological implications. As governments and organizations are coming together to build a secure network, we at Lenovo are doing our part by giving you the right IT infrastructure. Lenovo's 360° security strategy is the preferred way to protect your network, your devices, and your data from cyber threats. When you think security, think Lenovo.

5 reasons why Lenovo is a difference maker

- Trusted around the world
- Expertise across categories
- Choose Lenovo with confidence
- Business-boosting technology
- Flexible support network

To learn more contact us:

SWK Network Services
nwsinfo@swktech.com
www.swknetworkservices.com

SWK NETWORK SERVICES

Windows 10 Pro

Lenovo recommends Windows 10 Pro.

www.lenovo.com