

Smarter technology for all

Lenovo + IGEL Securing Devices at the Edge

**Joe Cleary - EMEA Cloud Connected Solutions Lead
Lenovo Cloud and Software Business Group**

Lenovo

COMMON TYPES OF CYBER ATTACK

01

MALWARE

Software programs designed to damage or do unwanted actions on a computer. Common examples include: viruses, worms, trojan horses, spyware, and ransomware.

02

PHISHING

Attacks sent via email and ask users to click on a link and enter their personal data. They include a link that directs the user to a dummy site that will steal a user's information.

03

PASSWORD ATTACKS

Involves a third party trying to gain access to your systems by solving a user's password.

04

DENIAL OF SERVICE ATTACKS

Attackers send high volumes of data or traffic through the network until the network becomes overloaded and can no longer function.

05

MAN IN THE MIDDLE (MITM)

Information is obtained from the end user and the entity the user is communicating with by impersonating the endpoints in an online information exchange (i.e. connection from smartphone to website).

06

DRIVE-BY DOWNLOADS

A program is downloaded to a user's system just by visiting the site. It doesn't require any type of action by the user to download.


888.698.0763 | totalprosource.com

Look Familiar?




Is this what you thought it was?

Data Storage > External Data Storage > USB Flash Drives




Roll over image to zoom in

[Visit the MILI Store](#)



3.6  5 ratings

-20% £3⁹⁹
Was: £4.99

 **prime** One-Day
FREE Returns

Brand	MILI
Connector type	USB
Cable type	USB
Compatible devices	iPhone, iPad, Computer
Special feature	Lightweight

About this item

-  **[FREE UP YOUR STORAGE]** Use MiLi iData Pro APP to transfer photos, videos and any files such as PPT, compressed files, PDF to MiLi USB flash drive to free up space on iphone and ipad and computer.
-  **[BACKUP IMPORTANT DOCUMENTS]** Back up, sync, store and share all your digital content; automatically or manually back up your contacts and other important digital content or pictures and videos anytime, anywhere with MiLi USB flash drive.

Did you know....

Device HW ID Spoofing is a thing?

It is possible to spoof HW vendor and Device ID's?

“Other USB Devices” CAN BE recognised as HID devices!

- USB Charger Cables Firmware Logic Spoofing

RISK - Silent installers/apps could auto launch in the background and start collecting data or instal malicious SW.

Hardware emerges as the new frontier of cyber attacks!



63%

Of companies have experienced a breach due to a hardware manipulation



75%

Of organizations plan to implement a hybrid work model

Existing security tools do not verify whether the hardware (HW) and USB controls are an all-or-nothing decision.

IGEL OS – USB POLICIES

Device Configurator - ITC000C29DD0870

Accessories | User Interface | Network | **Devices** | Security | System

Hardware Info

- Storage Devices
- Bluetooth
- USB Access Control**
- Audio
- Webcam Information

Enable

Default rule: Allow

Default permission: Read/Write

Class rules

Rule	Class ID	Name
Allow	HID (Human Interface Device)	Allow HID

Device Rules

Rule	Vendor ID	Product ID	Device uuid	Permission	Name
No entries found					

Close Save Save and Close

Class rules

Rule: Deny

Class ID: [Dropdown menu open]

- Audio
- Communications and CDC Control
- HID (Human Interface Device)
- Physical Interface
- Imaging
- Printers

Close Confirm

Device Rules

Rule: Deny

Vendor ID: [Input field]

Product ID: [Input field]

Device uuid: [Input field]

Permission: Global setting

Name: Policy Rule

Close Confirm

Lenovo ThinkShield Hardware Defense



Sepio Platform



Physical Fingerprinting, Machine Learning & Big Data

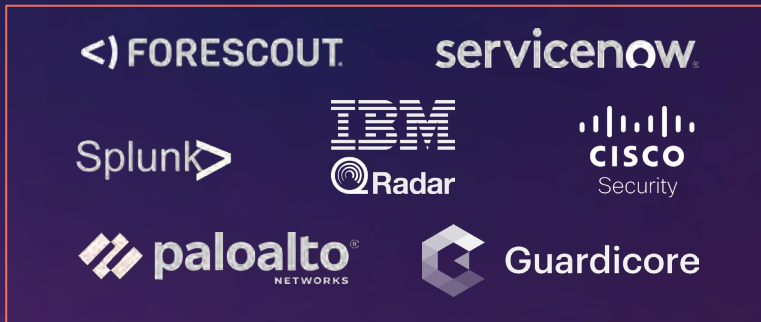
RAW Meta Data



Endpoints



REST API



Agents



Challenges of Physical HW Protection

Cybersecurity Challenge

How can I proactively tackle emerging hardware threats?

What are my employees attaching to their PCs?

Is procurement purchasing devices from reputable vendors?

IGEL OS + Lenovo ThinkShield

Strengthen security ecosystem and view risk scores

Full visibility and control of PCs and peripherals

Supply chain verification and BOM level visibility

ThinkShield

Below The Operating System



- Firmware Security & Bios Self-Healing



- Hardware Inventory



- Track, Map, Lock, Wipe Device



- Disk Encryption

At The Operating System



- Data Wipe



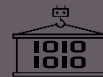
- Software Inventory & Monitoring



- Patch Management



- Passwordless Authentication



- Data Containment

In The Cloud



- AI Endpoint Protection, Detection & Response



- Ransomware Protection & Rollback



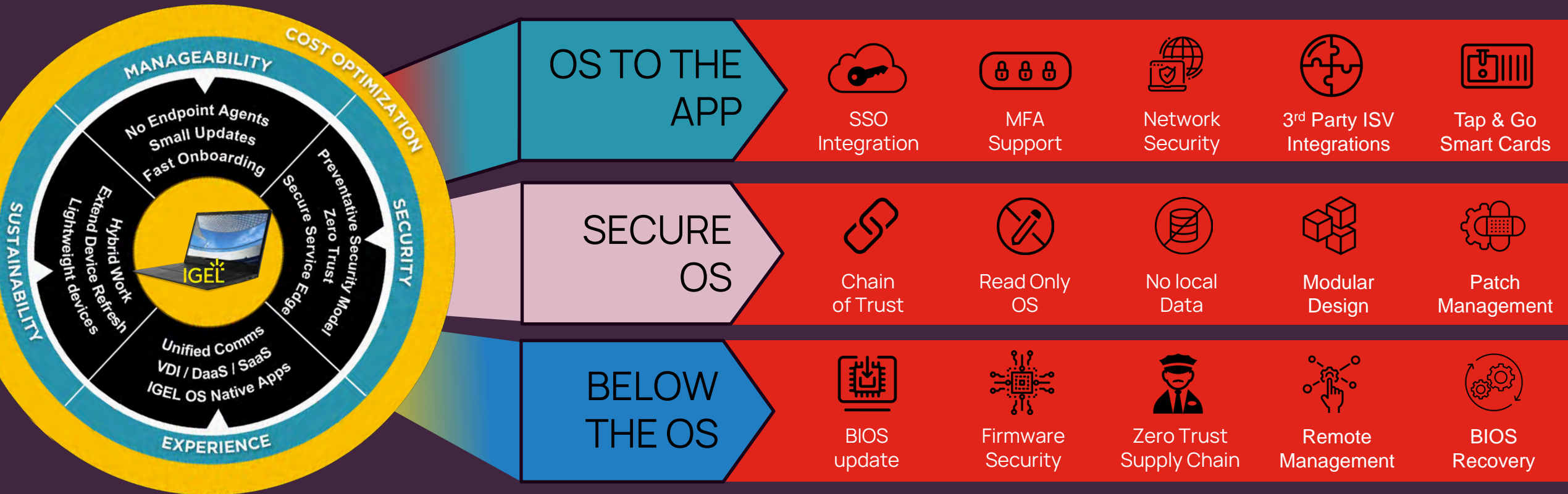
- Browser Protection



- Phishing & Malware Protection

Preventative, Multilayer Security to Help Keep You Safe

Proactive, resilient, and fully equipped to face the cybersecurity challenges of now and next. Together, we form an end-to-end defense strategy, providing unparalleled protection for your organization's endpoints.





IGEL Ready ThinkEdge Clients

Lenovo ThinkEdge clients are purpose built for streamlined edge computing, fostering efficiency, security, and seamless innovation in business operations.

Data-ready and secure: Businesses can rely on the security and reliability of the NIST-compliant ThinkShield offered on the SE10. With in-band manageability using the Lenovo XClarity Orchestrator, Edge Client and Server devices are secure and easy to manage no matter the challenge.

SE10 Series

Powerful performance with reliable ease and adaptability



SE30

For enterprise automation, smart retail, and smart buildings



SE50

Power and reliability at the edge



IGEL OS + Lenovo Think Edge

IGEL OS on Lenovo Think Edge products ensures the highest levels of security and operational resilience at the edge!

- Secure Digital Signage
- PoS Devices
- Warehousing
- Manufacturing/Productions lines
- Registration Web Kiosks
- Patient Kiosks



Smarter
technology
for all

Lenovo

thanks.

Visit Lenovo in the
vendor village to learn
more about our IGEL
Ready range!