DPX

Data protection after/during eXchange

Intro - Digitalization

“How do we trust something which cannot be seen?”

Before digitalization, information was written on pieces of paper. The integrity of information can be ensured through naked eyes. The mechanism remained workable until digital bits swept the world. Information was then transformed into zero or one stored in the memory. As we open or transfer files, integrity is questioned since what is displayed may not be what it is. Malicious bits may hide under the cloak of legitimacy. In this regard, a question is raised: how do we trust something which cannot be seen?

Whether data are stored or transferred, we should be suspicious. Malware may be injected; someone may hack into the system and steal the data in disguise of legitimate users; eavesdroppers may intercept and relay messages between two parties who believe they are directly communicating with each other. These are just some of the examples.

Risk of data breaches

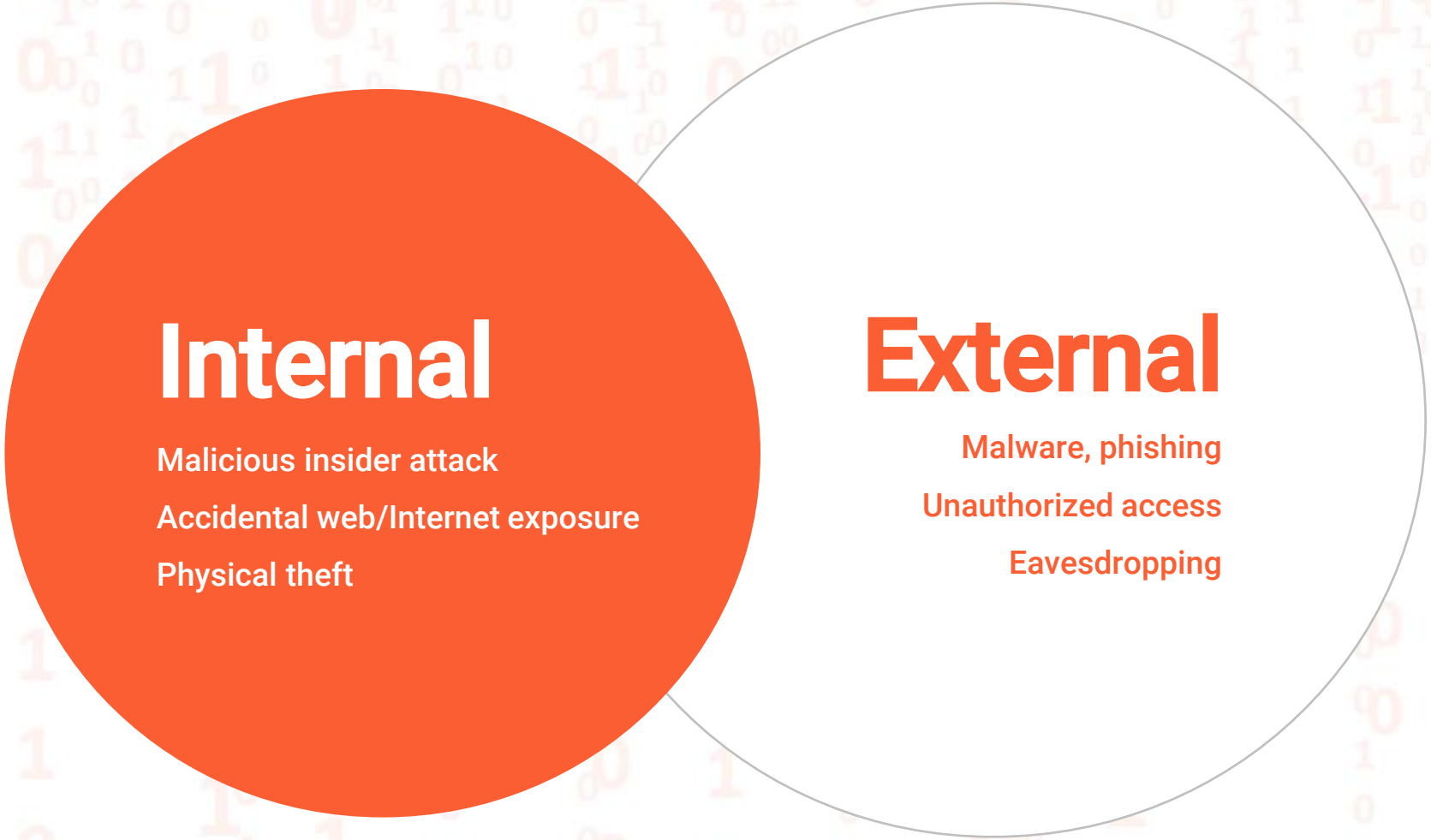
Data at rest

Malware
Unauthorized Access

Data in transit

Eavesdropping
Man In The Middle

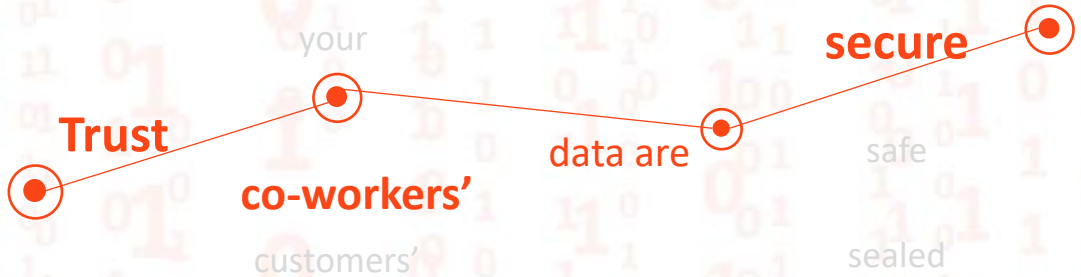
Basically, attacks can be categorized into the internal and the external ones.



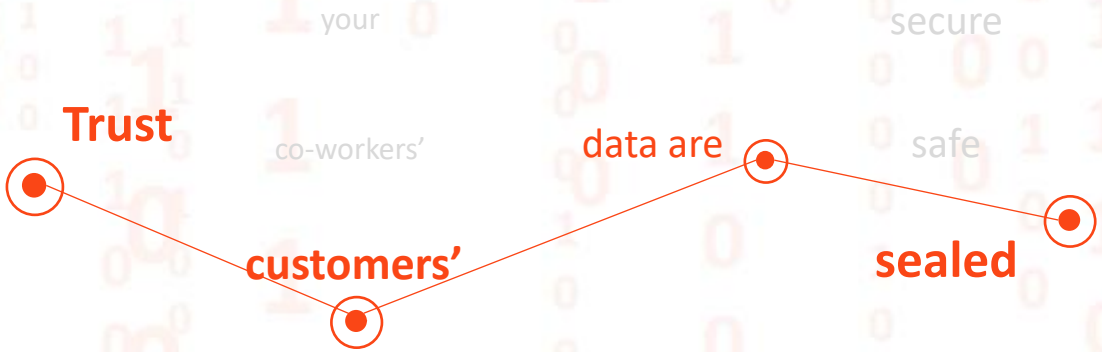
WiSECURE DPX Solution assures you that

1. You can trust your data are secure – data on premises are encrypted in case of internal and external attacks or human errors.

2 You can trust co-workers' data are safe – FIDO2 authentication cracks unauthorized access and enforces audit logging of action. Additional signing mechanisms can also be supplemented.



3 You can trust customers' data are sealed – leakage of customers' personal information may bring about massive legal fines.



“Where there is data…there is **WiSECURE**.”

DPX Security Concept

The end-point security has the four parts below:

Endpoint threat detection and response

Data protection
(at rest/in transit)

Multi-factor
authentication

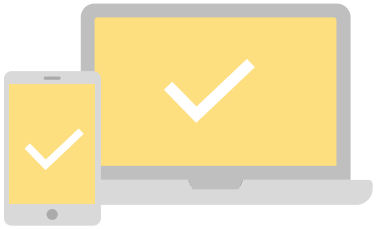
Least privilege
management

From another perspective, DPX's capacity and limitation in endpoint security are as follows.

Endpoint threat detection and response

DPX end-point security capacity

Data protection
(at rest/in transit)



Multi-factor authentication

Least privilege
management

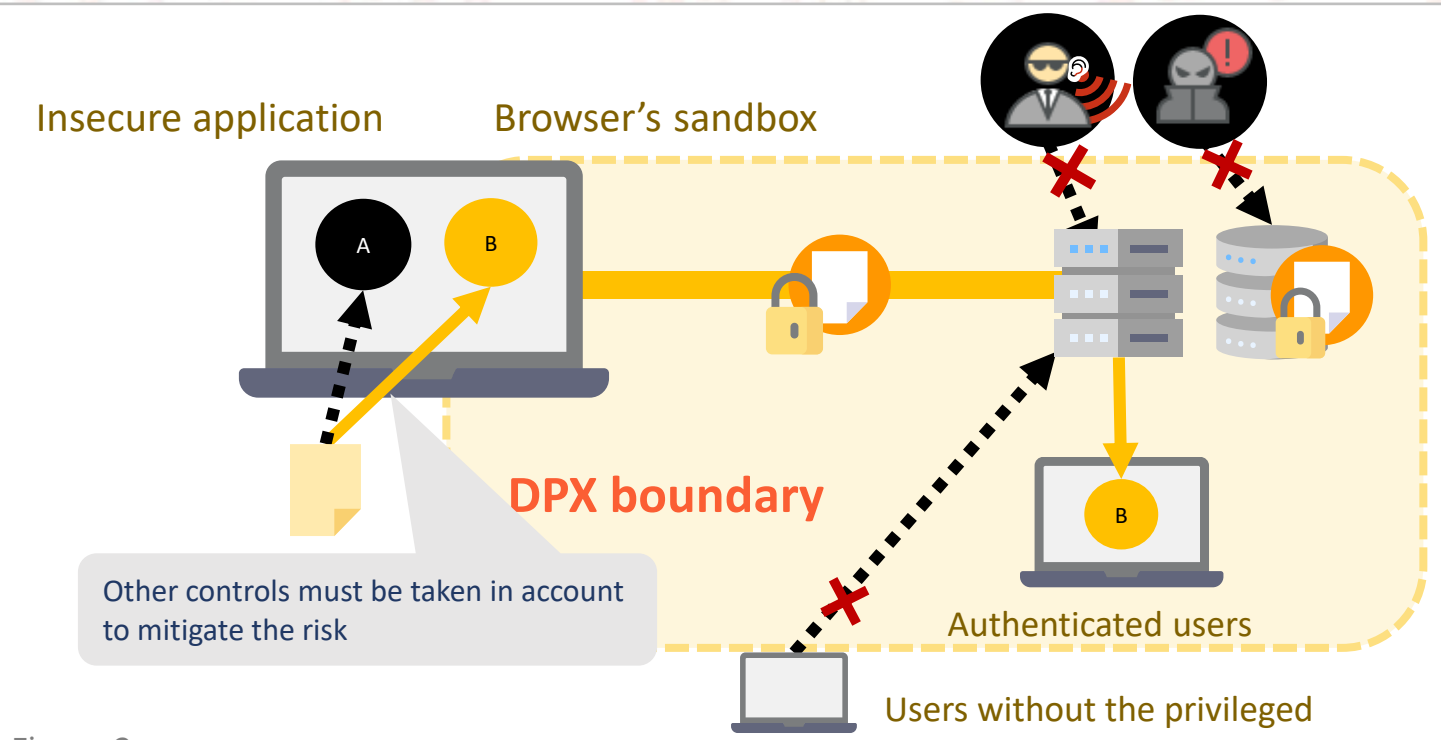


Figure 2

Figure 2 is a simplified use case scenario of file sharing. Risks of data breaches and appropriation lie in the area outside the DPX boundary. The insecure application may be vulnerable and likely to expose data uploaded. As files are transferred, eavesdroppers may intercept and relay data, which eventually causes files to be replaced with malicious contents. Regarding data at rest, internal physical thefts may steal hard drives or network attached storages. Last, external attackers may gain privilege and log into the server, doing whatever they want.

DPX enable your solution with security capabilities below:

1. **Data in transit**

   files are encrypted before transferring

2. **Key protection**

   the key establishment mechanism does not require encryption key to be transferred.

3. **FIDO USB Key and Role**

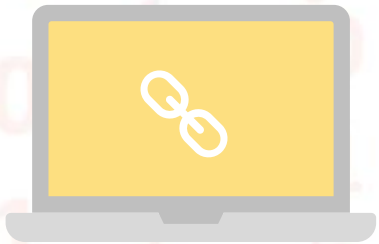
   strong authentication enforces least privilege management and audit logging of user actions.

4. **Advanced key management**

   files are encrypted through hardware security modules on the intranet.

Other Scenarios

Code Signing



Email Attachment Protection

Contact us:
rose@wisecure-tech.com

WiSECURE Technologies (WiSECURE) was founded in 2019, aiming to design standardized hardware security modules in various form factors, including PCIe cards, microSD cards, USB tokens, etc. WiSECURE specializes in cryptographic implementation and key management, which are fundamental in storage encryption, authentication, emerging digital assets, industrial control, IoT, WFH (Working from home), digital rights managements (DRM) and other innovative services and applications.