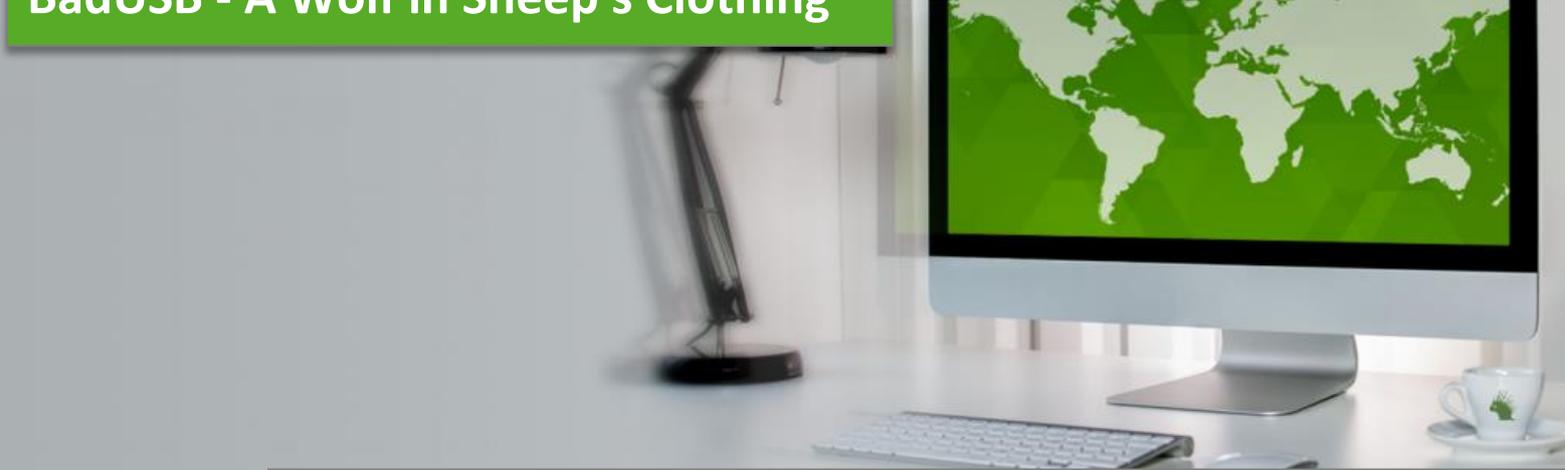


BadUSB - A Wolf in Sheep's Clothing



Protection against BadUSB Malware with EGOSECURE

The security challenge

For some years, the so-called BadUSB has been doing the rounds; it's a common and powerful attack vector that can put any organisation at risk. A BadUSB is a USB stick loaded with malware, or malicious code. It is camouflaged and, because it acts as a keyboard, it is hidden from any anti-virus programmes, or other protective mechanisms. In this guise as a supposedly authentic keyboard, it can practically control the computer and execute arbitrary commands. Just a few examples of its behaviour might include; establishing connections to other computers, running Ransomware, deleting, or encrypting disk storage on the hard disk. It can also copy data to the BadUSB stick, or even to the cloud.

From the criminals' perspective, it's great tool; they don't need any developer knowledge to create a BadUSB script. It can be easily created from readily available websites, making the use of a BadUSB even more attractive for the 'Bad Guys.'

A simple solution is not enough

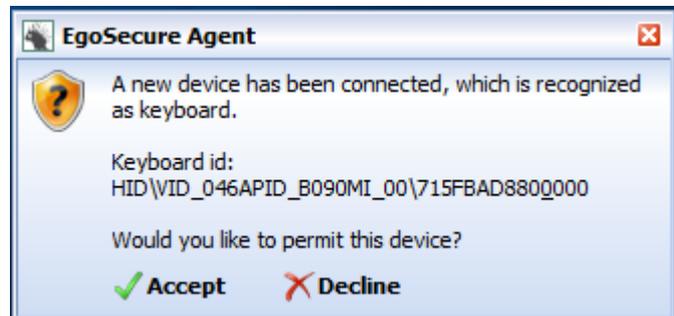
Some might think that this Malware source could be countered with effective device management - defining which USB sticks are allowed to be used in the company, all others, including any BadUSB stick, are blocked.

If only it was that simple! The issue is that the BadUSB stick is actually recognised as a keyboard and a keyboard is used by every computer during its normal operation. So, simple device management itself is not going to work. The only solution is to look closely at the attack scenario and develop special protection.

Protection against BadUSB with EGOSECURE

EgoSecure Data Protection was updated shortly after the first reports of BadUSB, to include a specific feature called, "Protection against BadUSB." The core of its protection is preventing the use of an unauthorised second keyboard.

However, this cannot just be done with a simple lock. Since mobile computers have a built-in keyboard, the use of docking stations, or external keyboards, makes this simplistic idea not feasible. The authorisation can therefore only be regulated by whitelisting.



We know that managing whitelists can be an extra effort on the administrator. Considering the damage that can be caused by BadUSB malware attacks, some additional effort is clearly necessary. At EGOSECURE, we pride ourselves on keeping things as simple as possible, so our solution requires negligible administrative overhead.

The management is both simple and flexible - for the administrator and even the user. One scenario might be that the administrator immediately and simply enables the use of all keyboards that are currently connected. Alternatively, he/she might enable a list of keyboards used from the inventory module. The list can be expanded, or reduced as required. Even easier, it can be supplemented by self-enabling - after all, it's the user who would know if a second keyboard would be used, or not. The second keyboard remains locked until the enabling is completed.

It doesn't matter whether you choose self-enabling by the user, or management by the administrator, or a combination of both. With EGOSECURE, everything is possible. With just a few mouse clicks, we give you the simplicity and flexibility to set up effective protection against BadUSB malware attacks.

EGOSECURE - a simply beautiful solution

With EgoSecure Data Protection, the German security specialist EGOSECURE has been the innovator in comprehensive data protection solutions for over 10 years. We secure data at all endpoints, throughout the entire business process. As you would expect, we are compliant with current laws and industry norms.

EGOSECURE is the first manufacturer in the world to combine both analysis and protection modules in one solution. Both are tightly integrated into one solution through one management console, one database, via one installation and administration methodology. This guarantees quick installation, easy administration and minimal user training. All true to our motto, "we make the complicated things easy."