ManageEngine
Device Control Plus

The TEN COMMANDMENTS of peripheral device security

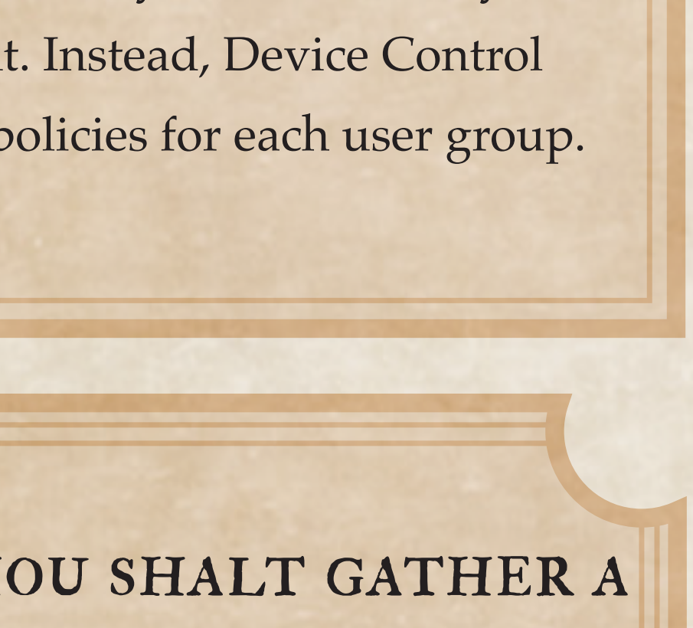
USB devices are small but mighty in today's cyber era. Even when they take on our favorite forms, such as cartoon characters, fun emojis, exotic fruits or sometimes embedded with fancy lights, it's not secret that USBs are teeny tiny devils! Aside from transferring data, peripheral devices can easily facilitate data breaches through the physical vulnerabilities in our computers: ports. Adding fuel to the fire, major advances have been made to fine-tune peripheral devices for potent security breaches.

Here are ten divine rules: the commandments of peripheral device security to safeguard your enterprise network. We'll also discuss how can you leverage our dedicated peripheral device control and management solution, Device Control Plus, for every single commandment.

I Thou shalt not suffer the entry of unauthorized peripheral devices into thine organization

A malware-infected USB, micro-controllers programmed to steal customer PII, and a rootkit that can remotely control endpoints are a few things you definitely don't want near your organization. Device Control Plus can serve as a gatekeeper, moderating the ingress of peripheral devices, permitting the good ones and dismissing the bad.

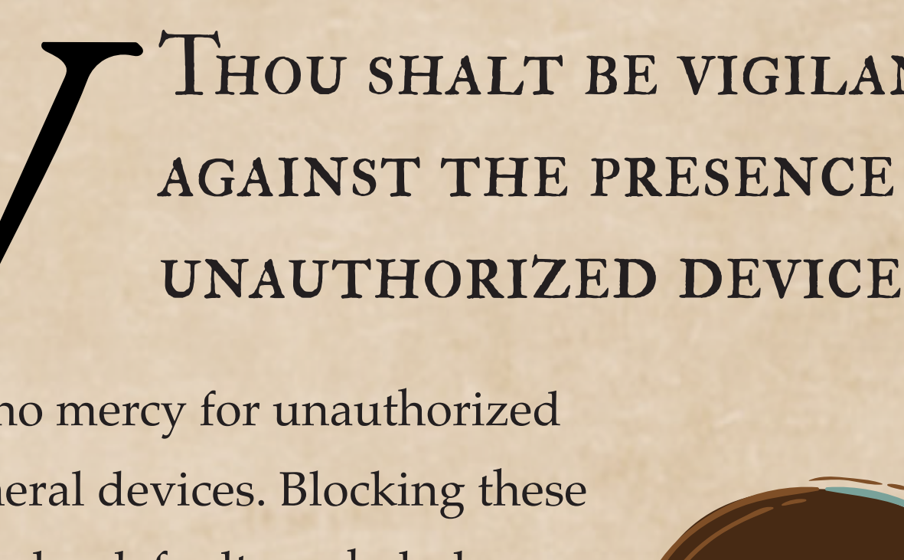
II Thou shalt configure the appropriate policy to oversee and govern peripheral devices.



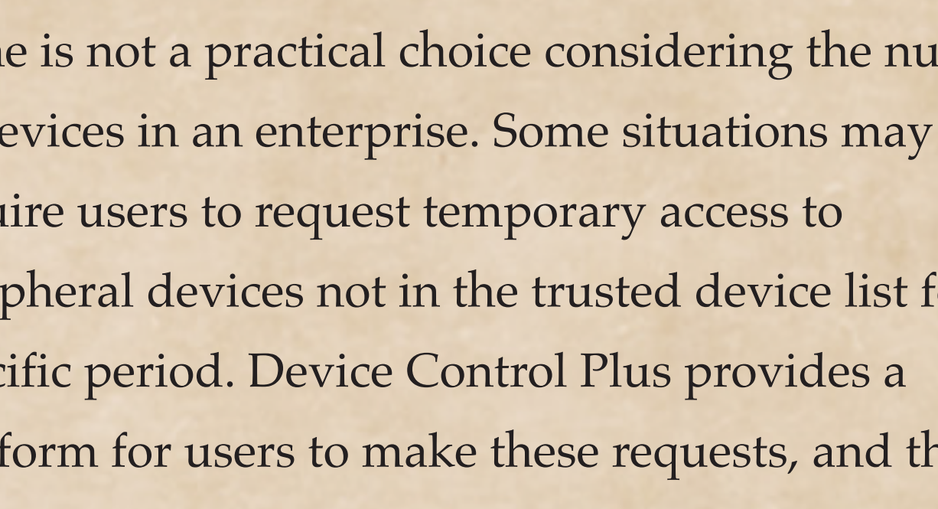
A peripheral device control policy tailored to your organization is key in establishing a Zero Trust ecosystem. But a one-size-fits-all approach is not an ideal security approach, as every user's authority and requirements are different. Instead, Device Control Plus can deploy specific policies for each user group.

III Thou shalt gather a cohort of trusted peripheral devices.

Complete elimination of peripheral devices can do more harm than good, as these devices are crucial for data transfer. Organizations often fall victim to data loss via peripheral devices and pay hefty sums under today's strict cybersecurity laws. Creating a list of essential authorized peripheral devices is imperative. The trusted device list is Device Control Plus' version of assembling this list to provide access.

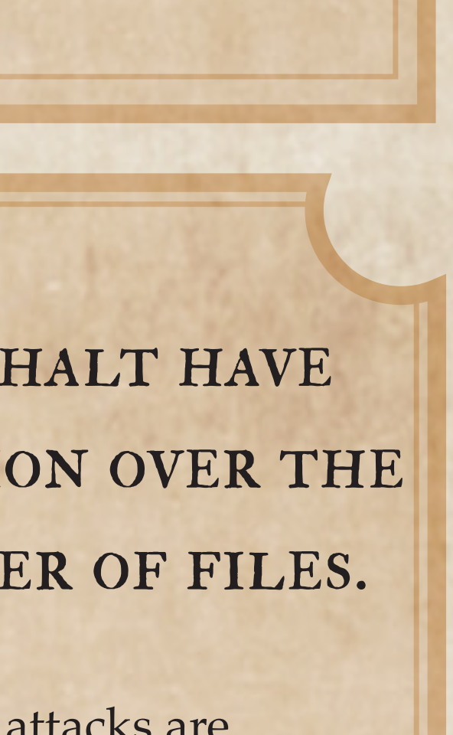


IV Verily keep a watchful eye over all temporary access requests and grant access solely to the righteous.



The exception that proves the rule—the trusted device list. Confining access using the trusted device list alone is not a practical choice considering the number of devices in an enterprise. Some situations may require users to request temporary access to peripheral devices not in the trusted device list for a specific period. Device Control Plus provides a platform for users to make these requests, and the admin can grant or deny the request after analyzing the intent.

V Thou shalt be vigilant against the presence of unauthorized devices.

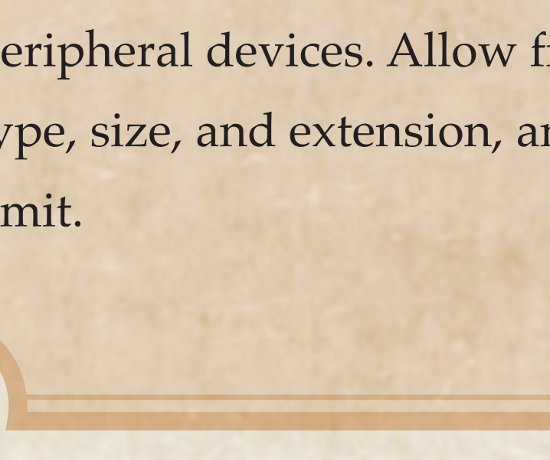


Have no mercy for unauthorized peripheral devices. Blocking these devices by default can help keep risks at bay. With Device Control Plus, you can create a list of devices to be blocked, however any device not covered in the policy will also be automatically blocked to ensure device security.

VI Thou shalt treat the organizational file as a prized possession.

With data being the new-age currency, it should be treated as a valuable asset in your enterprise. Providing complete file access to all employees will eventually result in a disaster, and the multitude of peripheral devices to manage and monitor only amplifies the probability of an accident or insider threat. File access management is the process of regulating who can do what and when. Establish a robust system for managing file access through peripheral devices by utilizing Device Control Plus.

VII Thou shalt have dominion over the transfer of files.



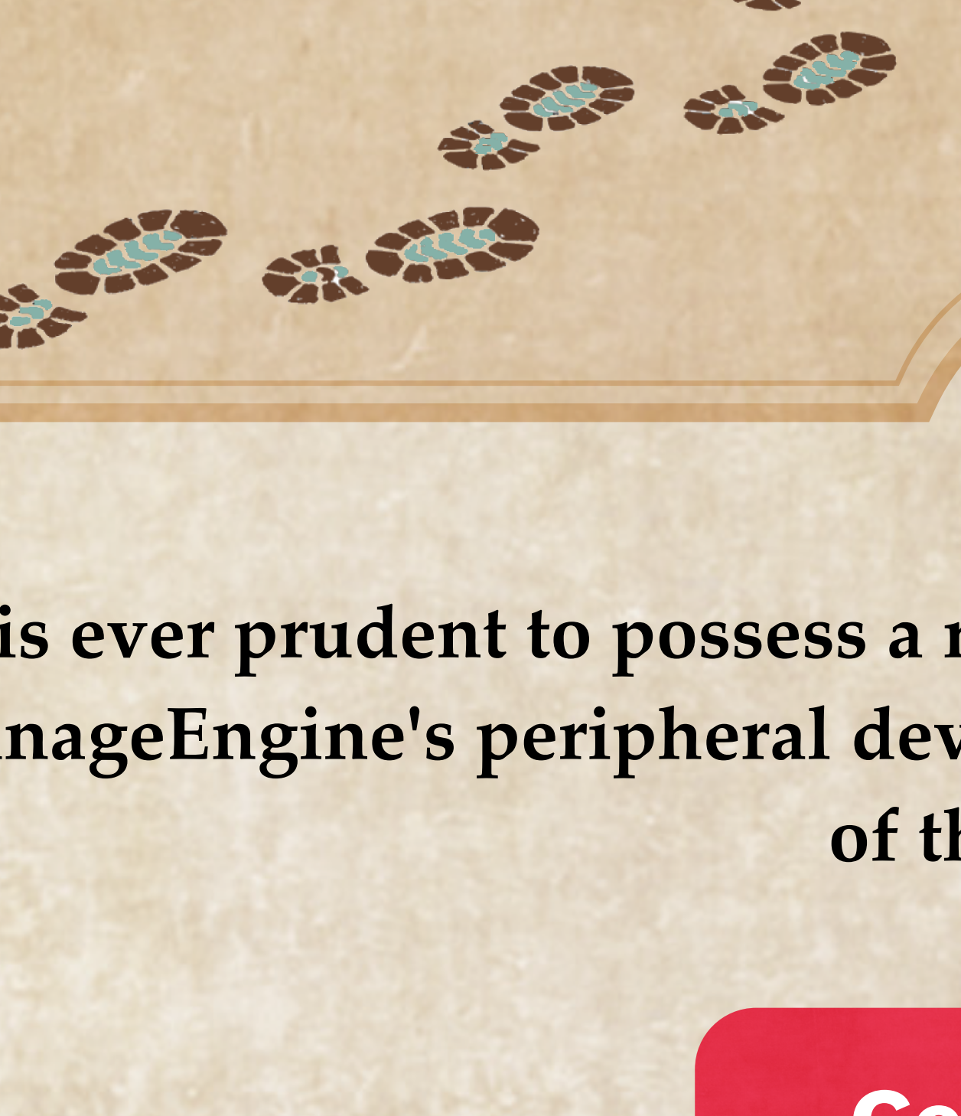
Insider attacks are the second fastest growing cyberattack type with a disastrous 15% increase from 2022. Poor file transfer control is the crux of an insider attack. Device Control Plus allows you to set clearly defined boundaries for data transfer over peripheral devices. Allow file transfers based on file type, size, and extension, and set a file transfer limit.

VIII Thou shalt always assign a shadow warrior.

Once a file leaves your enterprise network, it is subject to higher levels of risk. The content can be modified, copied, or it can fall into the wrong hands. To be on the safe side, always remember to enable file shadowing. A copy of the original file will be stored in a secured location whenever it is copied to or modified with peripheral devices.

IX Thou shalt ensnare the act of mammon.

Every enterprise's arsenal must have power-packed reports and insights to backtrack an accident or a mishap. Meticulous audits and reports readily available at your fingertips can do more than just backtrack; they can also help proactively catch suspicious actions that indicate an attack. Device Control Plus offers highly informative reports and audits with customization options.



X Trust thy users!

In cybersecurity, trust empowers. Embrace a zero-blame culture in incident reporting. Nurture the user by prioritizing education about cybersecurity repercussions. Together, we can strengthen security culture, encourage responsible behaviors, and swiftly respond to threats. Trust builds resilience against evolving cyberthreats.

Tis ever prudent to possess a remedy at hand. Device Control Plus, ManageEngine's peripheral device dominion solution, doth satisfy all of thine needs.

Get Started