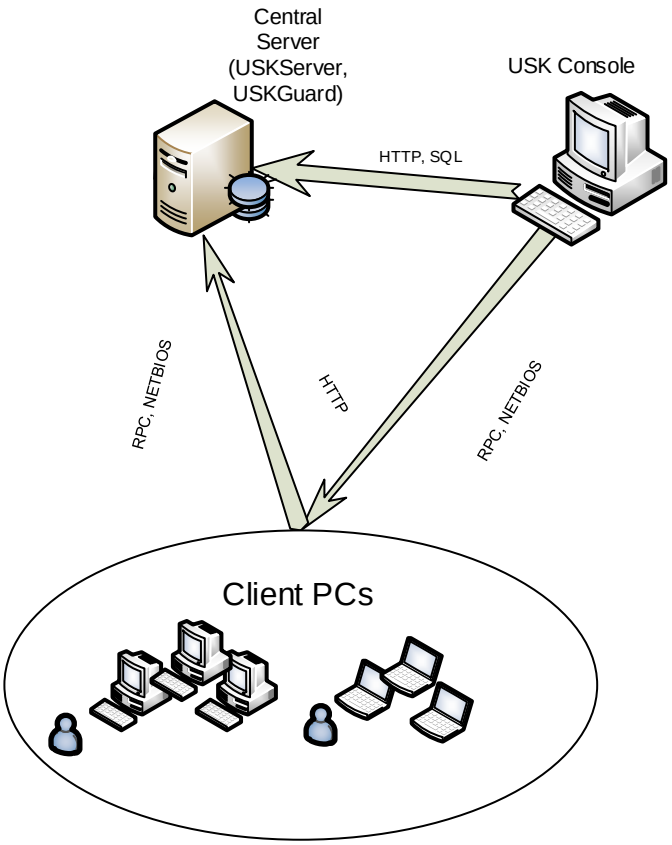
USK Suite

Applications whitelisting/blacklisting client-server system with advanced capabilities.

It has an instant response to a threat, easy and fast rules (criteria), basic server-side analytics, email alerts on various events, synchronization with Active Directory LDAP catalogs and advanced search capabilities.

info@softdev.online

1. General system diagram:



info@softdev.online

2. Features:

2.1 Tracking all created processes in system.
2.2 “Hard” or “Soft” prevention launch of unwanted processes.
2.3 Removing unwanted files from the media from where they were launched.
2.4 Optional notification to the user of a policy violation.
2.5 Fast operation and policy synchronization
2.6 Branding resources for the client (allow the use of company logos) in notifications.
2.7 Very flexible and powerful system of rules for evaluating characteristics of executable processes stored in encrypted form
2.8 Whitelist/blacklist for domain (Active Directory) and local groups, accounts, computer names in policies
2.9 Self-protection and defense on client side
2.10 Self-healing in case of failure or enter OS-BSOD if non-fixing fault detected (optional).
2.11 Caching events on the client if it is not possible to send them to the server *.
2.12 An encrypted communication channel between the client and server, which ensures security against “random views of 3 persons”
2.13 Search for duplicate executables at all Enterprise
2.14 Searching for completely new (never seen before) executable files.
2.15 Search for executable files by various criteria (file hash, signature certificate hash, tag parameters VS_VERSIONINFO, size)
2.16 Identification of executable files with fake digital signature
2.17 Fully UNICODE-aware
2.18 Track tampered executable images and it’s usage
2.19 Grouping client systems (one configuration per group)
2.20 Special hash file analysis technology (magichash)
2.21 Advanced events search system for display filters in administrative console (over 15 criteria’s).
2.22 Flexible server-side event filtering to prevent database clutter
2.23 Flexible server-side mechanism for masking process executable path and its parameters for hiding sensitive data (like passwords). Or to reduce historic data size
2.24 Highly customizable email alerts when processes of interest is launched
2.25 Scalability. Server parts can be distributed (several servers on one database)

info@softdev.online

3. System Requirements

3.1 Server side

3.1.1 Windows Server 2008R2/2012/2012R2/2016. Net Framework 4.0., 4 GB RAM. 2 Logical CPUs clocked at 2.4+ Ghz.

3.1.2 MS SQL Server (free Express edition possible) versions 2008R2/2012/2014/2017.

3.2 At administrator workstation: Windows 7/8/8.1/10 (32 or 64 bit) with Net Framework 4.0. 1 GB RAM.

3.3 Client side

3.3.1 Windows Vista/7/8/8.1/10 (32 or 64 bit). 256 Mb RAM, Single logical CPU clocked over 500 Mhz. (Warning: Windows 2000 or XP not supported at all!). Working services:

3.3.2 Windows Management Instrumentation (WMI)

3.3.3 Remote Registry *.

3.3.4 File and Printer Sharing for MS Networks (RPC, NETBIOS ADMIN$/C$/IPC$ shares) *.

3.3.5 Remote Procedure Call (RPC).

3.3.6 Server (Lanman Server) *.

* - only needed if you use remote validation/deployment and/or push client from administrator console.

info@softdev.online