itWash

Data Lock- Washing and Sanitizing- Workflow

itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 München

Tel.: +49 (0) 89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

www.itWatch.de
info@itWatch.de

itWash - Data Lock - Washing and Sanitizing - Workflow

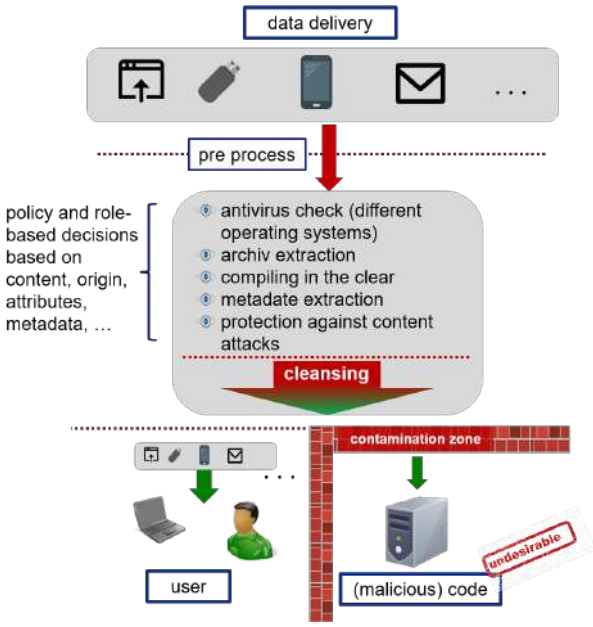
How it works

Potentially harmful content from external source is checked (web, e-Mail, USB flash drive, iPhone/ mobiles…) without infiltrating computer and network with malicous code.
Incoming data will be washed and transmitted for delivery. Devices (input or output) are defined by the customers need (CD, DVD, Blue-Ray, USB flash drive– also „personalized", e-Mail, networkshare, user directory, mobile…) and users are allowed choosing for them authorized systems. The washed and cleaned data can be enriched with metadata and will be transmitted automatically to the defined target system. Real data is isolated and checked under isolated infrastructure.
The integrity of the system is ensured. The system has been hardened to protect against attacks.
Additionally it is protected by itWESS (usage up to CONFIDENTIAL) security policy and if required by stand-alone and separated hardware. Potentially harmful content (e.g. all executables) will always be indentified by itWESS, extracted and transmitted recursively to the „sanitizing system" where affected data will be washed.
Customers are able to get safety-tested code parts (macros) by whitelisting.

Architecture

The System scales in several dimensions:

- **Safety:** Protection can be defined up to 100%. Attacks are prevented
- **Costs:** Low cost solution through focusing on use cases: The system scales from a central up to a dedicated system regarding costs and throughput
- **Throughput:** The performance of the overall system is balanced to the customers need. All components will match each other while highly parallelizing (also realtime monitoring)



itWash versions

- **itWash-d (dedicated system/ lock):** Single-user system – all functions are integrated
- **itWash-z (central sytem/lock):** Integration of all sanitizing components on one or multiple central instances
- **itWash-i (integrated sytem/ lock):** Integration of an acceptance station on a standard user working place together with a virtual or central system lock
- **Plug-In Components** In case of Boston Infrastructure, Office to pdf/A, Videoconversion, mp4 standardisation (or others…), permission of certified macros

Safety

- Protection of productive systems (PS)
- Protection of all contentbased-attacks
- No possibility of IP-based attacks
- System's integrity is always safeguarded
- Selected data flow control between acceptance station, system (lock) and PS – including monitoring
- Recursive decryption and unpacking of data before content examination
- Secure identification of undesired embedded data due to XRayWatch's complex recursive content checking
- Integration of any number of anti virus- and external systems (documentation included)
- Processes can be separated due to process-specific authorizations and/or due to stand-alone hardware systems
- Essential data transformation of one file into another „safe" format such as PDF/A-1a is possible

Management and Reporting

- Statistical overview (central) about all stations washing stations: data volume, results, attributes, metadata (up to detailed drill down)
- Central monitoring (also stand-alone systems)
- Central management of several instances of itwash also cross domain
- Multi tenant-capability: role-based administration and predefined user access rights

Archiving of undesirable data/files

- Different possibilites of using „undesired" data/ files:
  - Data conversion into a secure format
  - Data will be deleted
  - Secure deletion of data
  - Data will be stored separately in a so-called „contamination zone"
- Supplier notification is possible
- „Contamination zone" behind firewall system
- Only authorized people (e.g. forensic) can gain access to this „contamination zone"
- Evidence of original data and metadata (time and origin) with legal evidence

Requirement

- HR department: attachments of e-mail applications
- Data exchange via special-viewer: e.g. health via DICOM
- Format standardization: e.g. media converted to jpg, pdf/A, mp4 / mp3 …
- Documents/ files from any unknown source: real estate pictures, machine data
- Untrustworthy data/ untrustworthy content: internet, USB, CD,public accessible cameras
- Darknet research
- Turnstile interface – data flow in isolated stand-alone systems

FSitWash-200408