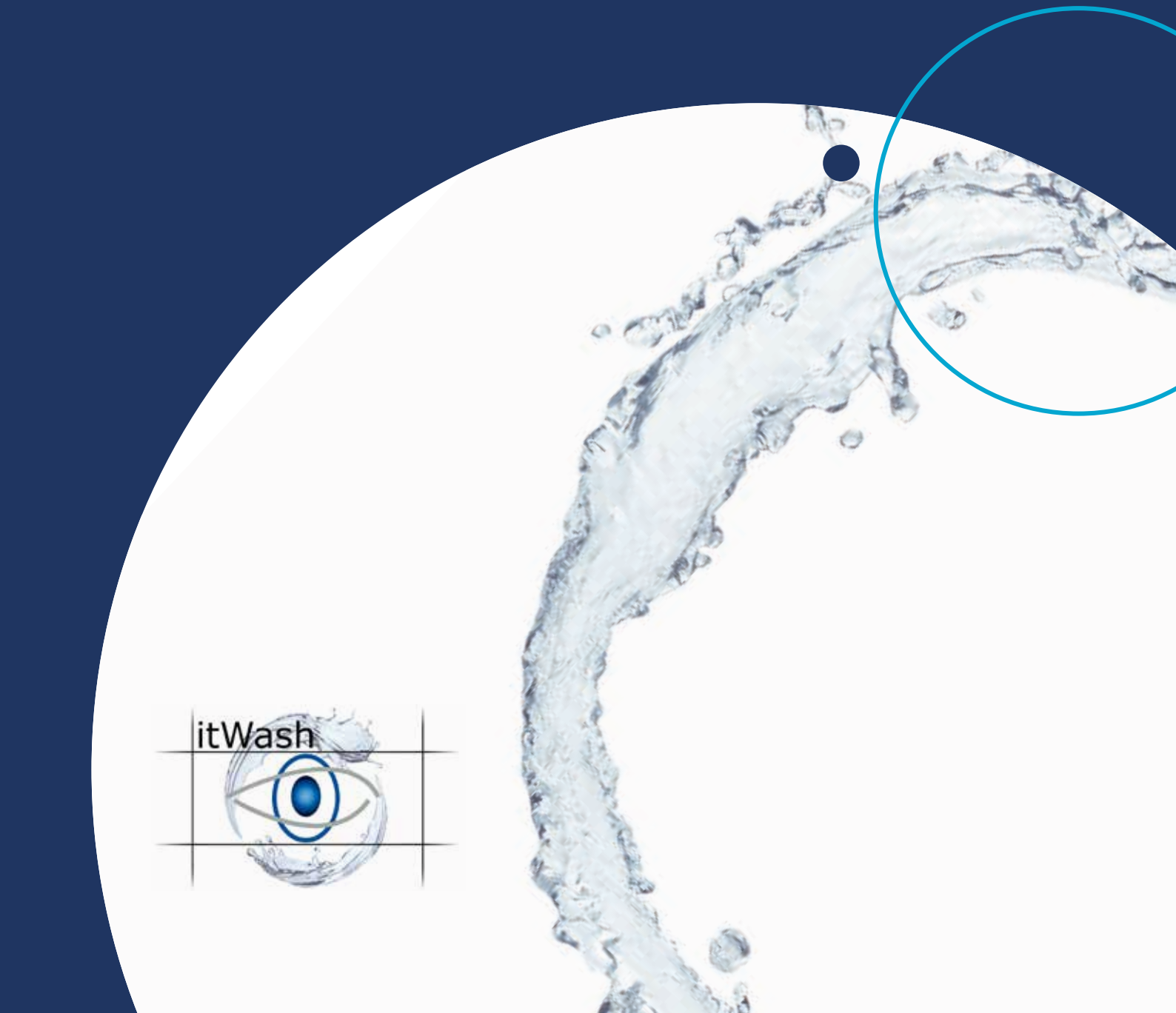
itWash

network isolating data lock
data wash
workflow



Data lock with data washing

Why data washing?

Data from untrusted origin can contain malicious code. Potentially harmful data (web, downloads, email attachments, links, portable storage devices, USB drives, tablets, mobile phones, FTP and S-FTP applications) can attack computers or the network with malicious code.

How it works

Incoming data is "washed" centrally or locally and forwarded securely for use. The customer defines what is permitted as input and output: locally, e.g., CD, DVD, Blu-Ray, USB stick—also "personalized only," encrypted email, file sharing such as Dropbox, user directory, mobile phones, specialized procedures. In user-controlled systems, the user chooses between the input and output channels offered that correspond to their authorization. Central: unencrypted data import.

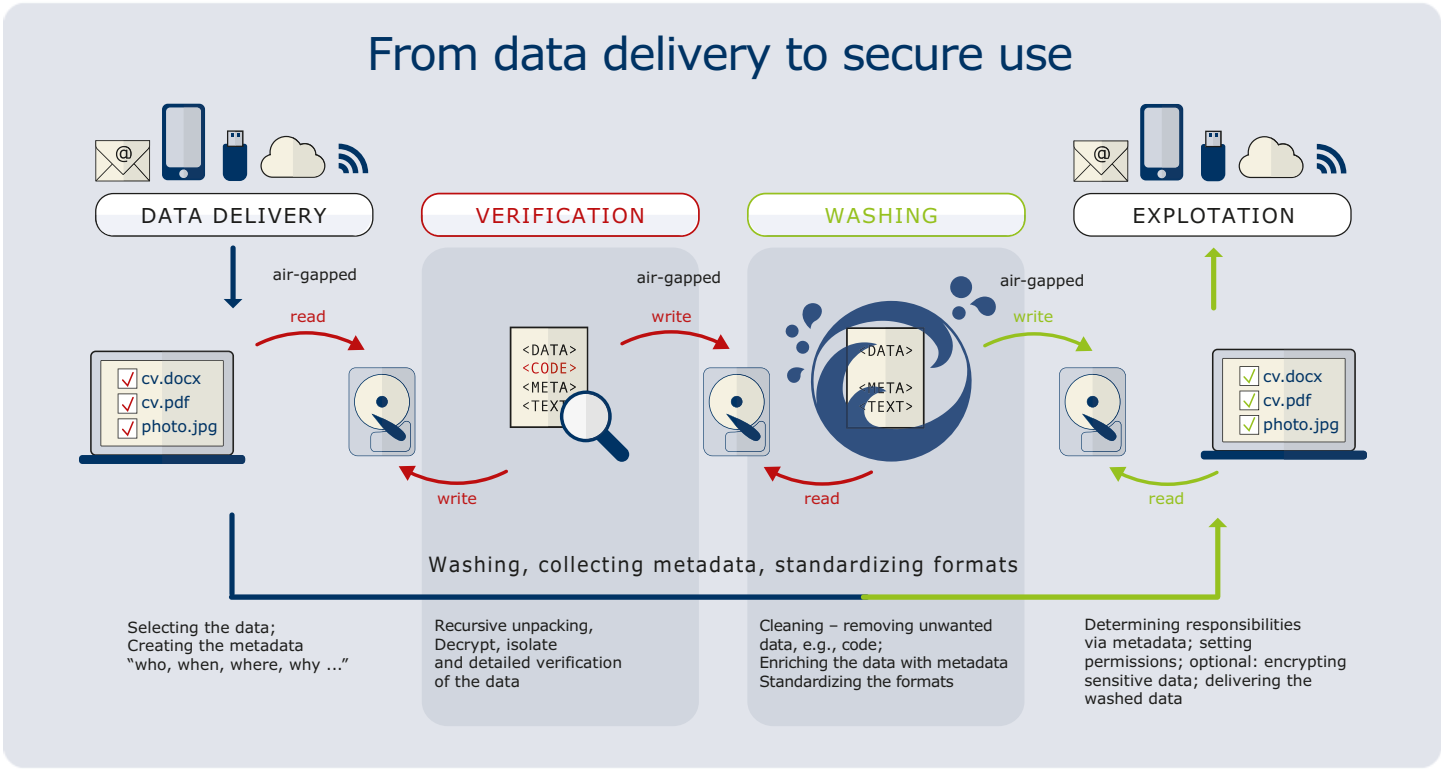
Washed data is either delivered automatically to the selected target system or to one which is automatically selected based on metadata. For this purpose, the data is processed on a fully isolated lock system. System integrity is guaranteed; the system itself is hardened in multiple layers and protected by an itWESS security policy (classified up to SECRET) and, depending on the protection requirements, by fully air-gapped, isolated hardware.

Potentially harmful data, such as all executable data elements, is reliably identified through content checks, extracted, and processed according to guidelines. Encrypted or compressed data is converted into plaintext, broken down into its individual elements, and recursively passed to the "cleaning system" for washing. Algorithmic checks allow security-approved code segments (e.g., known/signed macros) to remain in the files.

Use cases

Data of uncertain origin exists in many places within organizations:

- Email attachments
- Downloads
- File sharing platforms
- Mobile storage devices
- Human esources department
- Marketing
- Press office
- Claims processing and reporting centers
- Presentations and content supplied by partners and vendors
- IoT devices, smart home devices, surveillance cameras…
- Remote maintenance
- OT and transition to IT
- Remote patching
- Public authorities – citizen data – e-government – Online Access Act (OZG)
- Patient data on CD/DVD
- Wearables
- Digital archives – digital evidence
- Unsecured devices (BadUSB)
- Manual interface for disconnected systems
- Transfer of large datasets, e.g. on construction sites or as product data via specialized procedures



Not just virus protection

- Recursive decryption and decompression of data before content control
- Data flow control between receiving station, lock, and productive system - including monitoring, logging and reporting
- Decryption and encryption of confidential content; GDPR compliance
- Optional automated/forced conversion to desired target formats such as mp4, mp3, PDF/A-1a
- Protection of the productive system against zero-day exploits, because every attack needs a piece of code
- Protection against all content-based attacks
- No IP-based attack tunnels possible
- Integrity protection of the gateway
- Recursive content checks of any complexity using itWash's proprietary algorithms for the reliable identification of unwanted embedded content
- Integration of any number of antivirus systems and any third-party systems for additional capabilities (including logging)
- Separation of all processes through process-specific permission space and/or through disconnected hardware
- Collection of all metadata from the washed object through analysis and AI with open transfer interfaces in files and/or databases
- itWash is compatible with third-party services such as labeling services

	itWash	Anti Virus	AV based lock
Cleaning – Modification of the document	✓	✗	✗
Washing out all executable embedded objects	✓	✗	✗
Blocking identifiable, already known patterns of malicious code	✓	✓	✓
Discover archive bombs and protect against them	✓	✗	✗
Role-based processing templates	✓	✗	✗
Detection and decryption of encrypted content prior to inspection	✓	✗	✗
Prevent BadUSB	✓	✗	✗
Modify virus-infected information so it can be read	✓	✗	✗
Role- and content-based workflow	✓	✗	✗
Recursively unpack archive before processing	✓	✗	✗
Extract and archive metadata	✓	✗	✗
(Mandatory) encryption/signature after processing	✓	✗	✗

itWash-elements

itWash-Mail

Central: Unwanted code in attachments and malicious links in emails are the most commonly used methods of cyber attack.

Central mail washing: With itWash's central mail washing, the attachments of all incoming emails are washed directly and delivered to the recipient.

Mail Client: itWash mail client offers security aware users the option of washing emails from unsecure senders completely barrier-free before opening them in order to avoid risks, and allows forced decryption with washing before use.

itWash-z

itWash, as a central unit, is divided into various components: acquisition and delivery of data, verification and recursive analysis, data washing and distribution/ transfer unit to the point of use. Data from different sources can be received. Each source is assigned a fitting washing program and the data gets accordingly washed. e.g., internet downloads, communication with third parties such as partners, including via bulk transfer interfaces, s-ftp, or cloud services, citizen data (OZG), customer portals, damage reports, etc. The central washing components are installed as 19" units in various network segments (extranet, DMZ, backbone, separate network unit). The cleaned data is automatically redistributed and stored with the appropriate access rights (users, groups) and encrypted if necessary.

itWash-A

The receiving station is used for manual, wired, or wireless submission of data, which is forwarded to itWash-z on-premise or in the cloud. Parameter about the submitter and the requested back channel are collected at the receiving station and will be transported as metadata

itWash-iz

Data acceptance takes place at the employee's standard workstation. Potentially unclean or rejected data from USB drives, cell phones, downloads, email attachments, etc. is mandatorilly sent to itWash-z, which automatically returns the washed data. By double-clicking on the file to be submitted, you can set the cleaned file to open immediately after it is returned.

itWash-d

itWash as a dedicated kiosk for submitting customer or citizen data in a self-service environment. For example, a meeting room can be defined as a destination for a presentation or a lecture, a specialized procedure can be defined as destination for specific data.

Expansion by add-ins

Existing solutionsand any third-party products, such as AI to collect meta data or converting voice-to-text , can be integrated easily using open interfaces.

CleanFile

CleanFile implements a seamless chain of trust from delivery to use. It tags data packages that have been cleaned so that only data washed by the company itself can be read at a workstation.

CleanFile consists of two components: the itWash CleanFile client with itWESS (itWatch Enterprise Security Suite) functionalities, which ensures that only washed data is used, and data washing in itWash. CleanFile ensures compliance with the GDPR.

CodeWash

CodeWash contains the tools for code generation, lifecycle management and versioning. Models, code, training data, raw manuals, and installation tools are delivered. Within the washing process, they encounter compilers, source code checks, escalations for errors, warnings, and manual converters. The result is a signed, versioned, evidence-secured package.

CodeIntegrity

CodeIntegrity checks the authenticity and integrity of the delivered code and verifies signatures. If necessary, CVEs (Common Vulnerabilities and Exposures) can be checked and SBOMs (Software Bill of Materials) can be created. The security solution is ideal for automated or air-gapped patch management. The tested software can be transferred and released directly to ApplicationWatch from the itWESS Suite. The "memory" ensures that CVEs detected later trigger an alert or even immediate blocking of the affected application.

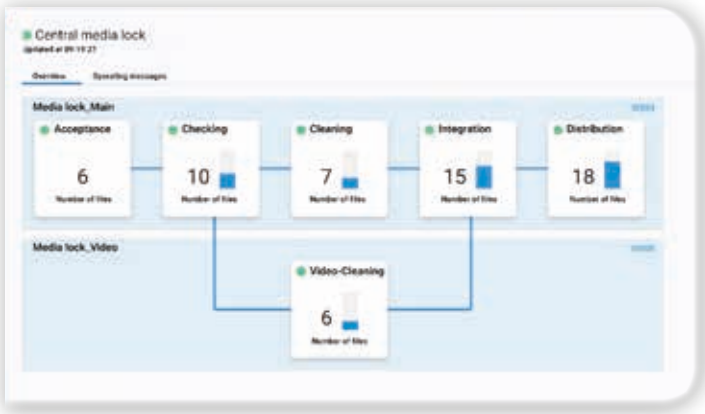
Contrary to itWash elements, which filter code from the delivered data, CodeWash and CodeIntegrity ensure secure life cycle management and complete preservation of evidence – with a "memory."

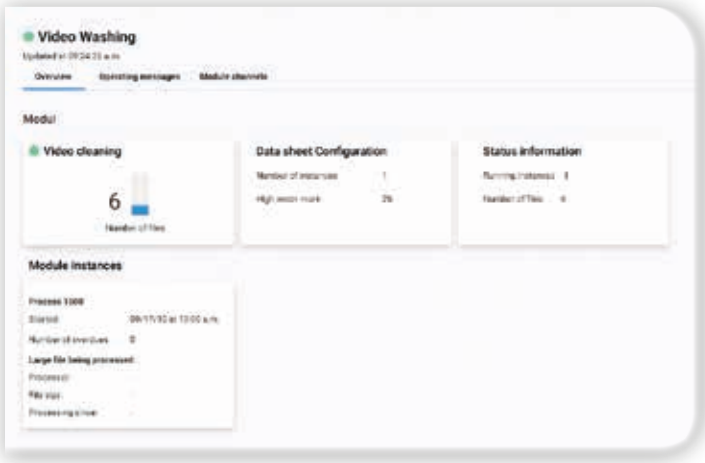
itWash Control Center

itWash-Dashboard

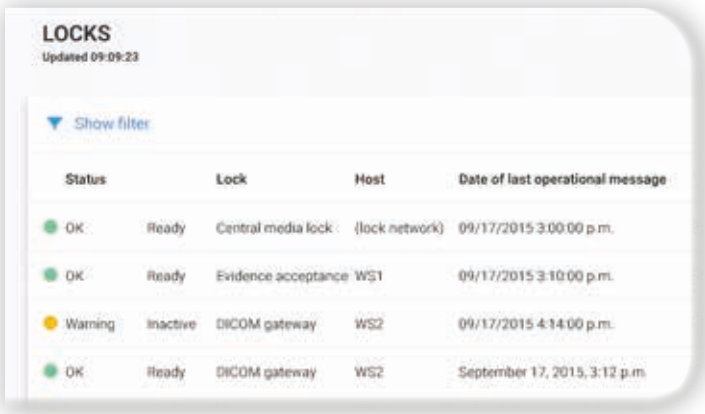
itWash-Dashboard visualizes system statuses, incidents, and events, providing a real-time overview of of the workload, possible bottlenecks and quarantine incidents.

itWash-FlowControl





itWash-FlowControl enables order processing, data volume, and data carrier management for all "wash orders." The sending and receiving organizations can be different, and yet no network connection is required. Source, destination, priority, confidentiality levels, and rights are configured, and an automated notification request is stored. The transfer and washing of large amounts of data (petabytes) can be flexibly integrated into specialized procedures.

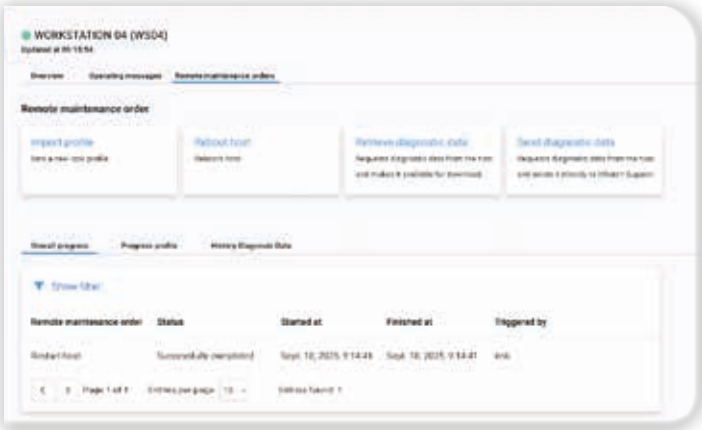


Monitoring and controlling by itWash data locks

The ICC (itWash Control Center) is a web-based application that allows all itWash instances to be centrally monitored, controlled, and managed.

As an integral part of the itWash architecture, it provides a permanent overview, enables rapid response to security-related events, and facilitates user support.

- Continuous and transparent live monitoring of all lock activities via ONE tool
- Status and performance monitoring of individual instances within a lock
- Connection to SIEM systems and other security features such as alerting
- Visualization of system status via a traffic light system
- Central management of different types of security gates (centralized and decentralized)
- Assignment and transfer of security profiles
- Modification of security gate configurations even during operation
- Real-time reporting of status and operating messages
- Secure on-premise use without cloud connection
- Remote maintenance of security gate computers



The ICC covers several functional areas. Depending on requirements and type of use, service level, and multi-client capability, various functional areas are available on different hardware components in various networks.

itWash-ICC/SV+U
(Software distribution and updates)

The ICC's software distribution component is responsible for establishing, maintaining, and restoring the operational readiness of the various itWash components (certificates, signatures, patches, etc.).

itWash-ICC/DC
(centrales reporting)

Central overview of all events, status messages and statistical analyses of all itWash systems in use.

itWash-ICC/VPN
(virtual private network)

Various VPN usage scenarios in management servers of itWash are managed centrally:

- Integration of itWash into the customer's infrastructure
- Second VPN optional for remote maintenance access (depending on the SLA also from itWatch)

itWash-ICC/health status

Monitoring of the utilisation of the available data lock modules.

The components can be operated virtually. A part of the comprehensive security concept is the definition of access control.

Scalability

Scalability in multiple dimensions

Costs: From a cost-effective, dedicated itWash system (all-in-one), to a multi-stage, server-based system.

Security: The security level can be defined that no external data can perform attacks on the target network

Performance: itWash can scale performance according to the desired throughput and runtime of individual tasks, thanks to its synchronized components and high degree of parallelism according to customer requirements – even in cloud operation. Components can be added on demand in real time, for example, as pre-built containers. Individual itWash components can be offloaded to separate hardware, for example, to separate longer-running washing processes.

Archiving and preservation of evidence

- Files identified as "undesirable" can be:
  - converted into secure objects
  - deleted / securely deleted
  - separated and stored in encrypted form in a quarantine area
- In each case, with or without notification to the supplier
- Quarantine behind own firewall
- The quarantine can be accessed securely by individual authorized persons, e.g., forensics
- Preservation of evidence of the original data, including metadata (time, origin), with legal validity through signatures and real-time stamps possible

TEST NOW
DATA WASHING

Try how easy and accessible data washing can be as a service based on cloud or on-premises!

Send an email with an attachment to:

MyLaundry@DataWashing.de.

You will instantly receive the washed attachment back by email.

We are available for you.

For questions send an email to **info@itWatch.de**.
In addition, our technical support is available to our customers by telephone or at **hotline@itWatch.de**.

Would you prefer a direct contact person?

Technical hotline
+49 1805 999984 (0.14 €/minute)

Free 0800 numbers are available with suitable maintenance contracts

For further questions:
+49 89 62030100

Your security. Our mission

itWatch GmbH
Aschauer Str. 30
81549 München

itWatch.de
itWash.de
itWESS.de

itWatch GmbH