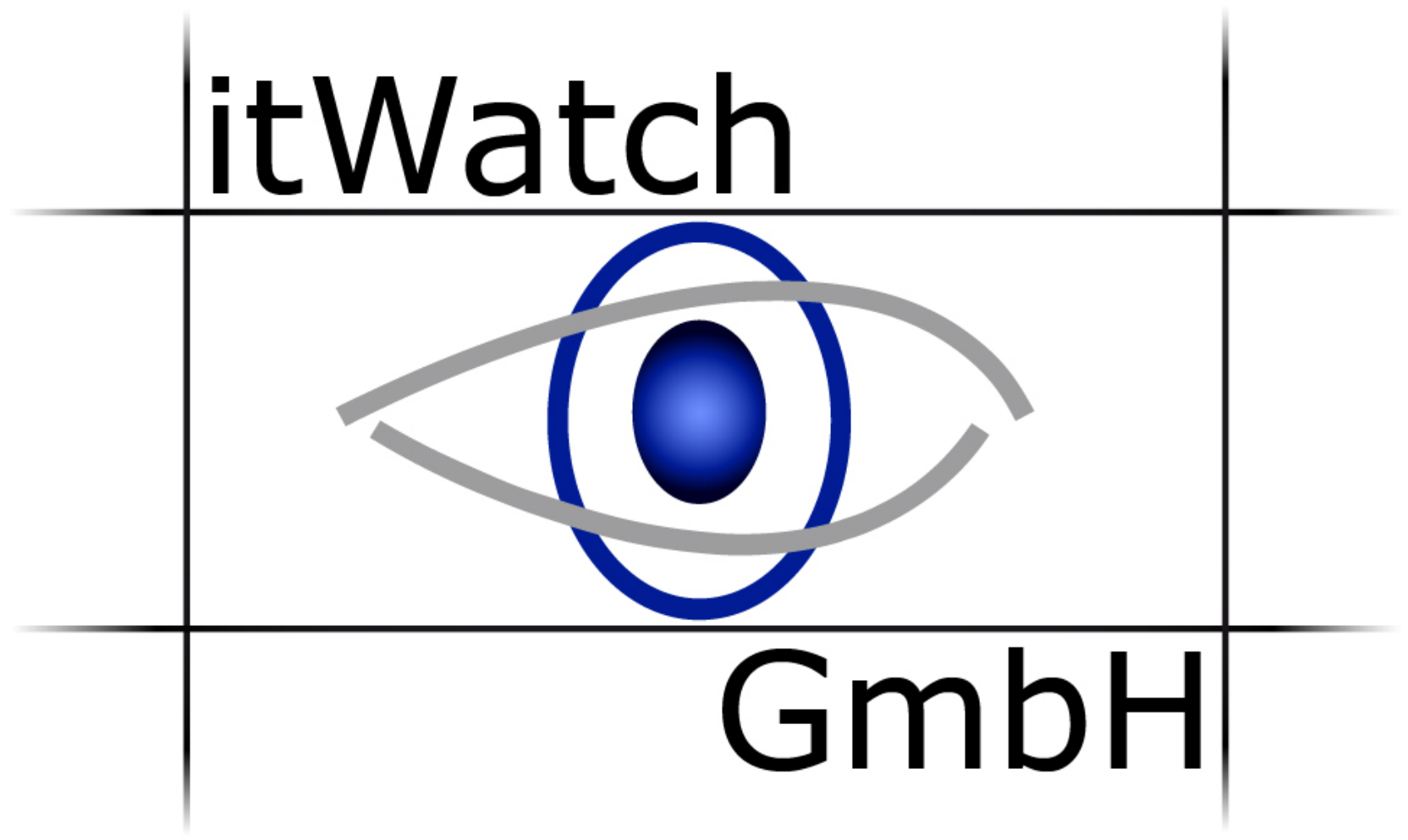
Ihre Sicherheit …
… unsere Mission



CodePurITy

Sichere Nutzung aller Anwendungen

Die Herausforderung

Wozu sind Links in Mails in Dokumenten im Internet … da?

… um den Anwendern zu sagen:

NICHT Klicken – gefährlich

Wozu sind USB Sticks da?

… um den Anwendern zu sagen:

NICHT Einstecken – gefährlich

Wozu sind Mail-Attachments da?

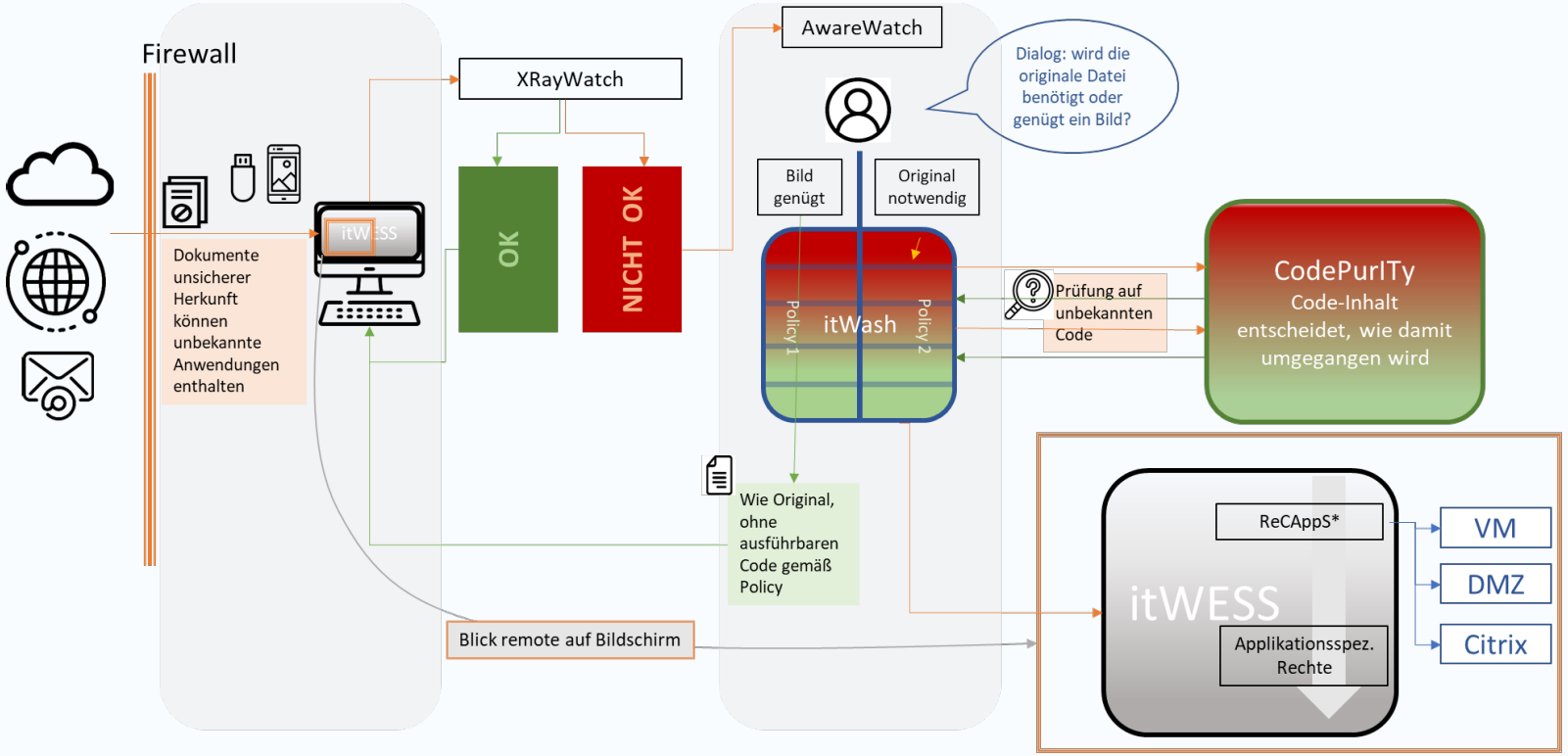
… um den Anwendern zu sagen:

NICHT Öffnen – gefährlich

Es ist Aufgabe der IT, sichere Arbeitsplätze zu schaffen

Bruce Schneier auf der mcsc (Münchner Cyber Security Conference)

Sichere Nutzung von Anwendungen: CodePurITy



CodePurITy von itWatch - neu ankommende Daten werden darauf untersucht, ob sie Code enthalten. Identifizierter Code wird untersucht, dem geeigneten Prozess zugeführt, inventarisiert und, nach geeigneter Prüfung, mit dem geeigneten Rechteraum in der richtigen (potentiell virtualisierten) Umgebung ausgeführt.

Man kann nicht managen, was man nicht kennt

Firewall

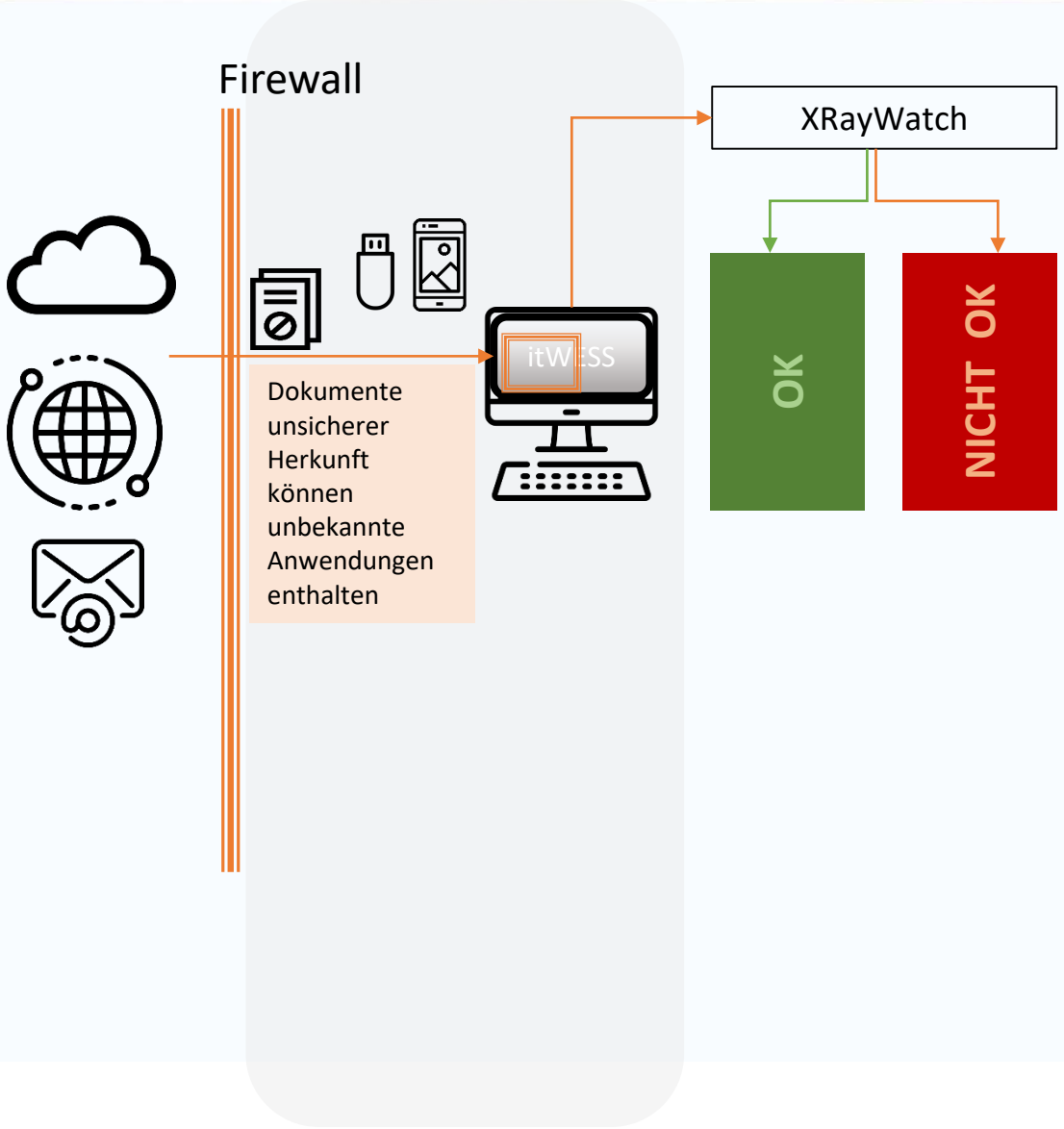
Dokumente unsicherer Herkunft können unbekannte Anwendungen enthalten

Wenn man die sichere Nutzung aller Anwendungen erreichen will, greifen traditionelle Applikationskontrollen mit White- und Blacklisting zu kurz – insbesondere, wenn nicht jedes Code Fragment erkannt wird.

Der Bedarf:

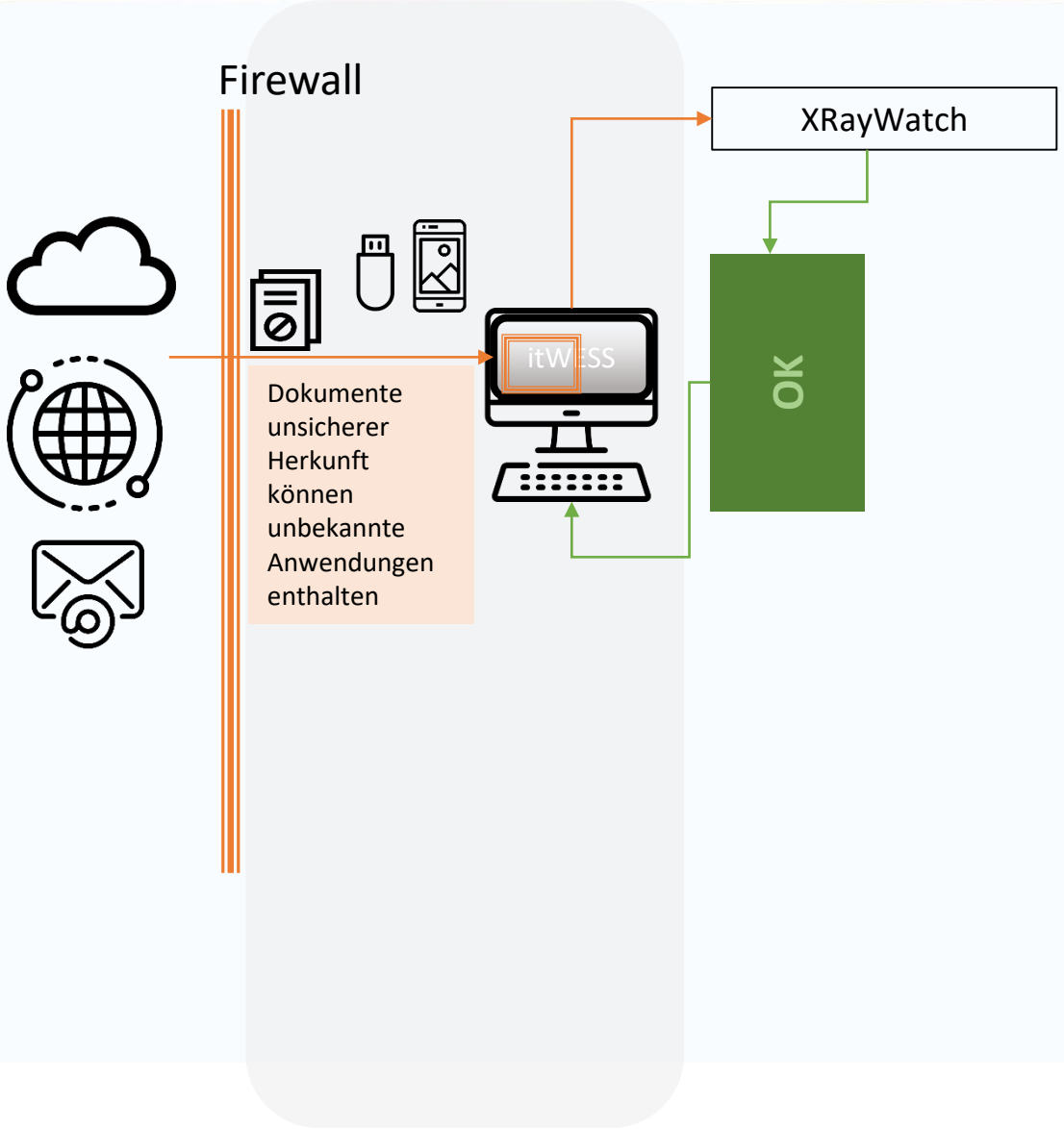
- im täglichen Business auch unbekannte Code-Elemente spontan in die Nutzung bringen
- Schutz vor Installation und Ausführung unautorisierter Anwendungen
- Schutz vor dem Nachladen unerwünschter Code-Elemente
- eingebettete Codestücke wie Makros oder andere Skripte wie Java in Zulaufenden Daten erkennen, prüfen und geeignet in Nutzung bringen
- bekannte, geprüfte und ältere Skripte im Einsatz lassen

CodePurITy – sichere Nutzung aller Anwendungen



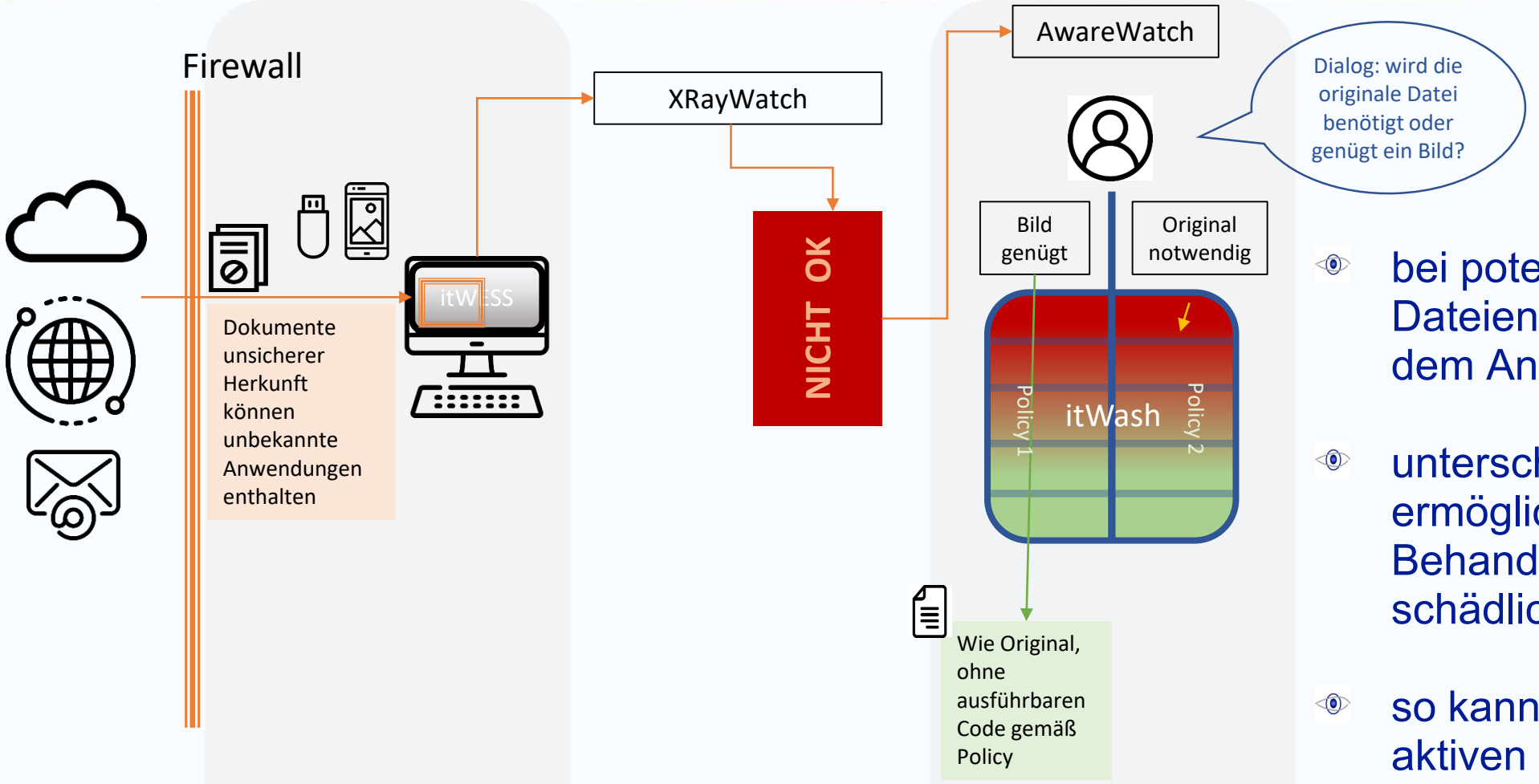
- Objekte aus unbekannter oder nicht vertrauenswürdiger Quelle werden mit dem Modul XRayWatch aus der itWatch Enterprise Security Suite (itWESS) auf ausführbaren Code gescannt und entsprechend kategorisiert
- Internetdownloads, Mailattachments und Daten von mobilen Datenträgern können z.B. generell als nicht vertrauenswürdig eingestuft werden
- bereits geprüfte Anwendungen werden automatisch erkannt
- durch das Signieren der geprüften/ freigegebenen Anwendungen ist jederzeit nachvollziehbar, welche Anwendungen positiv geprüft wurden
- Signaturen können mit kundeneigenen Schlüsseln durchgeführt werden

CodePurITy – sichere Nutzung aller Anwendungen



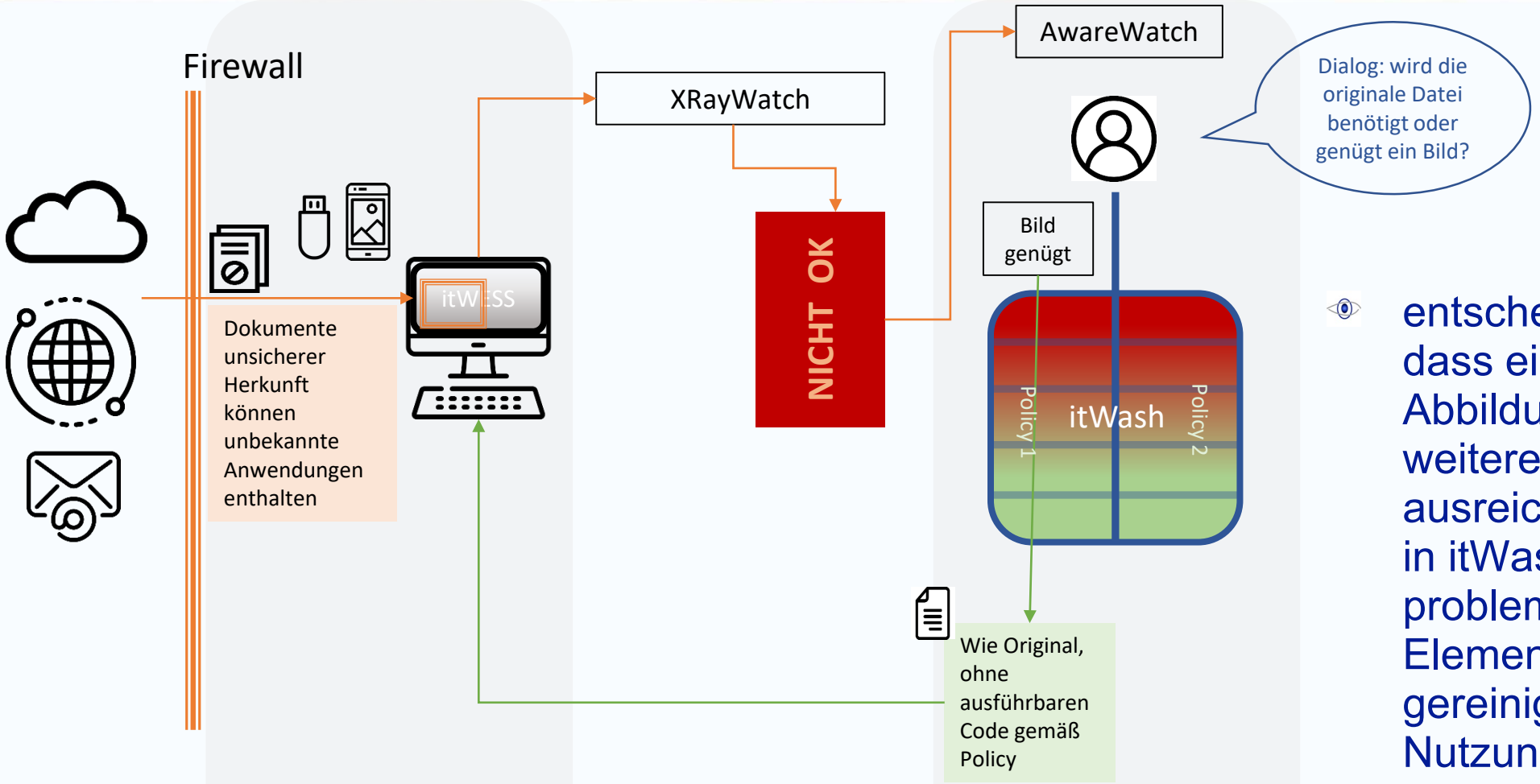
- unschädliche oder freigegebene Daten und Code-Elemente werden nach der Protokollierung zur weiteren Verarbeitung auf dem Arbeitsplatz dargestellt oder ausgeführt

CodePurITy – sichere Nutzung aller Anwendungen



- bei potentiell schädlichen Dateien geht CodePurITy mit dem Anwender in den Dialog
- unterschiedliche Policy‘s ermöglichen die differenzierte Behandlung der potentiell schädlichen Dateien
- so kann entweder „ohne aktiven Code“ oder „mit dem Original“ weitergearbeitet werden

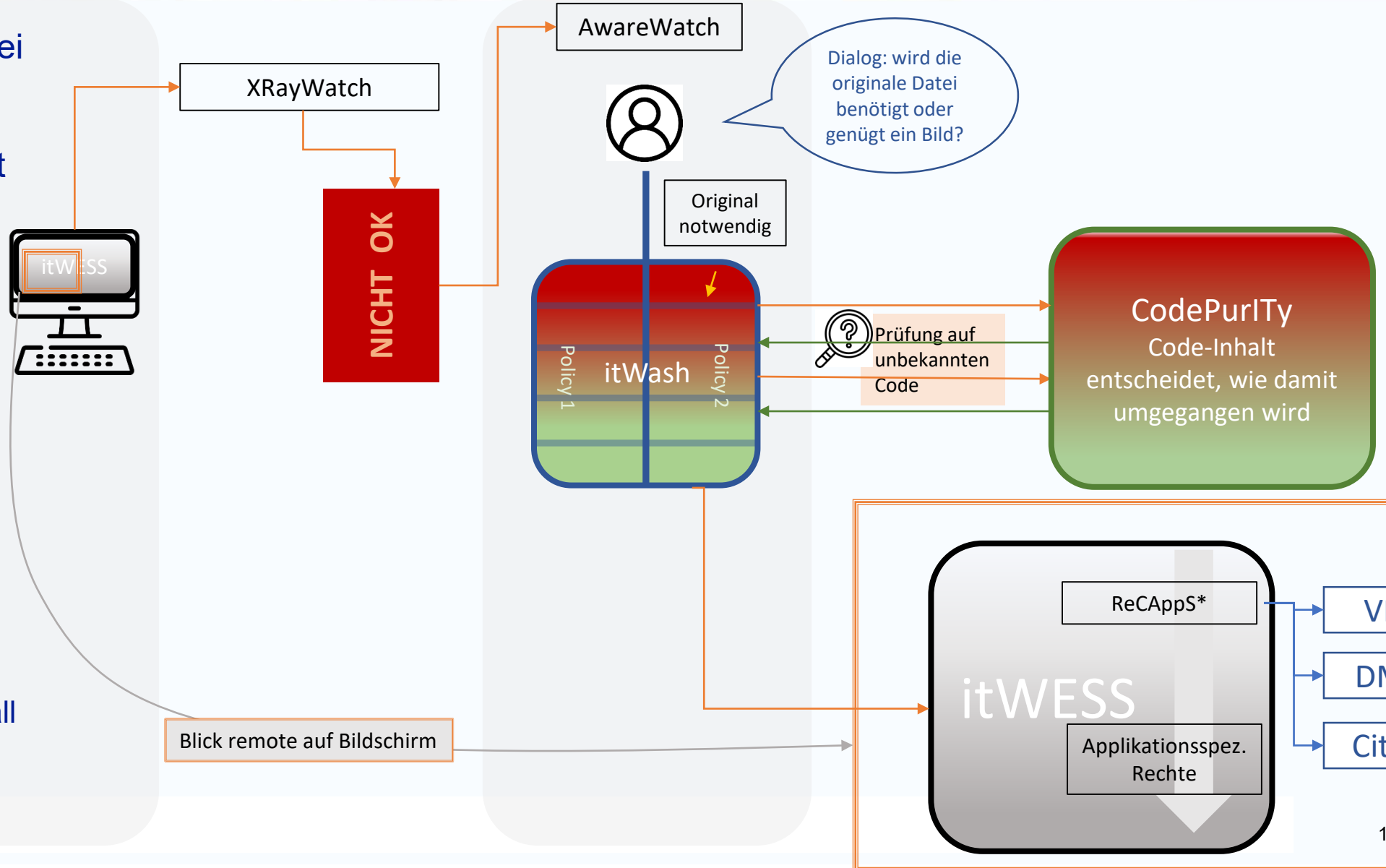
CodePurITy – sichere Nutzung aller Anwendungen



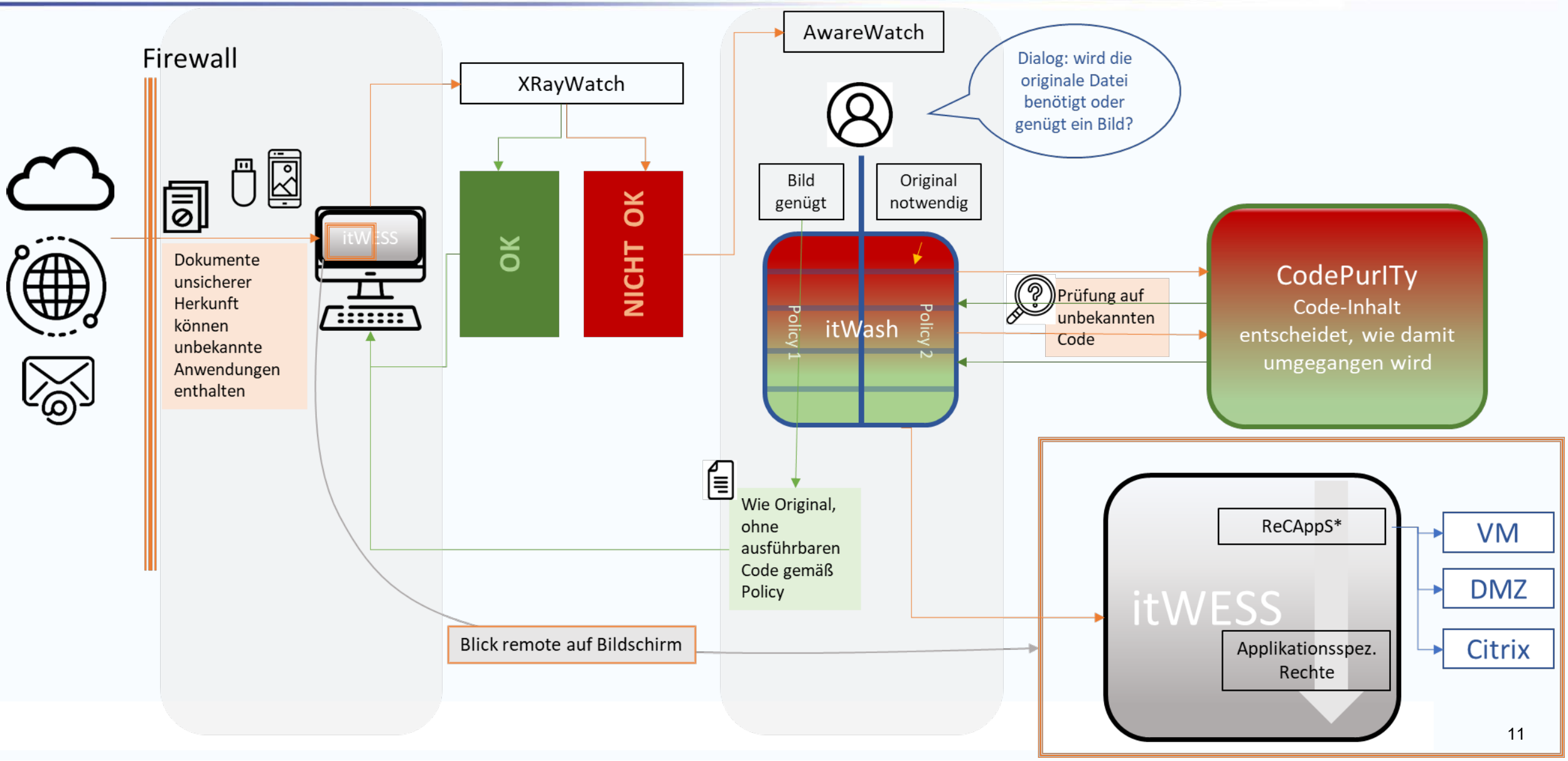
- entscheidet der Anwender, dass eine originalgetreue Abbildung des Dokuments zur weiteren Verarbeitung ausreichend ist, wird die Datei in itWash von den problematischen Code-Elemente gereinigt, das gereinigte Dokument zur Nutzung an den Arbeitsplatz zurückgegeben und sofort zur Anzeige gebracht

CodePurITy – sichere Nutzung aller Anwendungen

- wird die Originaldatei benötigt, wird diese in einer isolierten Umgebung geöffnet
- als isolierte Umgebung stehen zur Verfügung:
  - reduzierter Rechteraum mit Mitteln der itWESS (ApplicationWatch)
  - virtuelle Maschine lokal oder remote
  - Terminalserver / CITRIX …
  - eigene Infrastruktur hinter einer dafür konfigurierten Firewall



CodePurITy auf einen Blick



CodePurITy – sichere Nutzung von Anwendungen

CodePurITy kann die Softwarelandschaft sinnvoll ergänzen:

- automatische Verifikation für den Zulauf signierter neuer Standardanwendungen (Prüfung von Zertifikaten, Signaturen, Laufzeiten und anderen Gültigkeitsparametern)
- Überprüfungen mit Vulnerability Listen
- Signatur von Anwendungen und Patches mit kundeneigenen Schlüsseln
- Übergabe an ApplicationWatch (in itWESS AE und PE enthalten) zur Freigabe möglich (CodePurITy verfügt zu diesem Zweck über eine eigene Signaturkomponente)
- mit itWESS können die Anwendungen beweissicher inventarisiert werden
- ApplicationWatch prüft die vollständige binäre Übereinstimmung bekannter freigegebener Anwendungen
- XRayWatch kann bei Skripten bestimmte Systemaufrufe erkennen und dadurch die richtige Ausführungsumgebung bestimmen