שולחן עגול מגזר הבריאות

HL7® FHIR®

SECURITY

משרד הבריאות
לחיים בריאים יותר

אגף בריאות דיגיטלית ומחשוב
משרד הבריאות

על מה נדבר היום?

- תפיסת הגנה
- הגנת ממשקים
  - וולידציית FHIR API
  - שינוע וסינון קבצים
- בקרת/אימות גישה - זיהוי משתמשים
- שאלות ושיח חופשי

משרד הבריאות
לחיים בריאים יותר

9 הדומיינים

בהגנת מערכות מבוססות FHIR

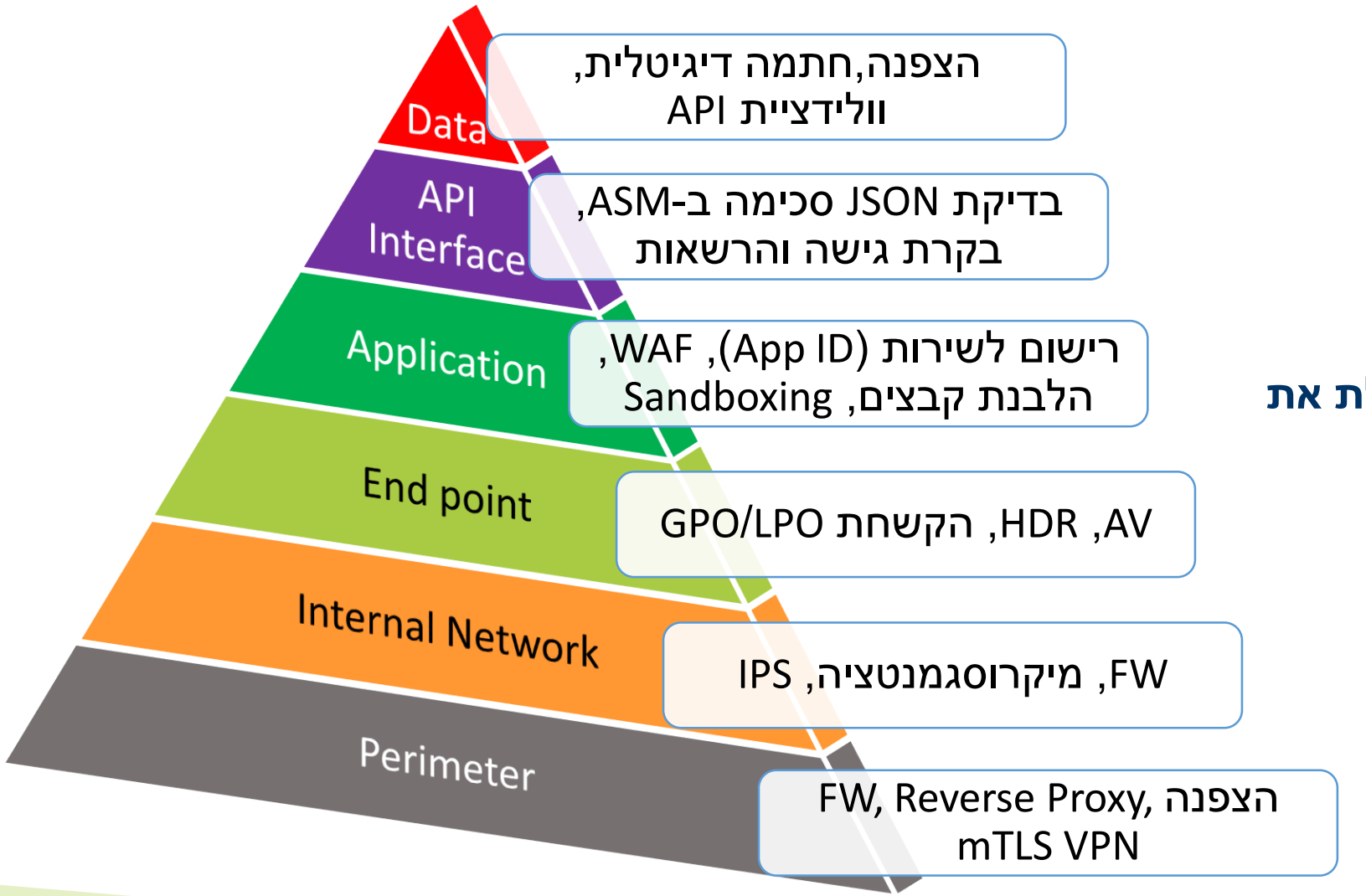
9 הדומיינים בהגנת מערכות מבוססות FHIR

- **בקרת/אימות גישה** - זיהוי משתמשים ותפקידיהם בארגון החיצוני ואכיפת לוגיקת הרשאות בהתאם
- **בקרת הרשאות** - לאפליקציות ולמשתמשים השונים
- **סוגי משתמשים** – ניהול, אפלקטיבי, צרכני שיורת השונים
- **הגנה על פריט מידע** – הצפנה, התממה, סיווג, תיוג
- **הגנת ממשקים** – API, העברת הקבצים
- **הגנת רשת** – on-prem ,Cloud
- **הגנת תשתיות IT** – הקשחות, GPO, פיזי, וירטואלי, ענן, מיקוסרויסים
- **רישום LOG**
- **רגולציה** – נהלים, תקנות וחוקים

משרד הבריאות
לחיים בריאים יותר

תפיסה להגנת במערכות FHIR

תפיסה להגנת מערכות FHIR



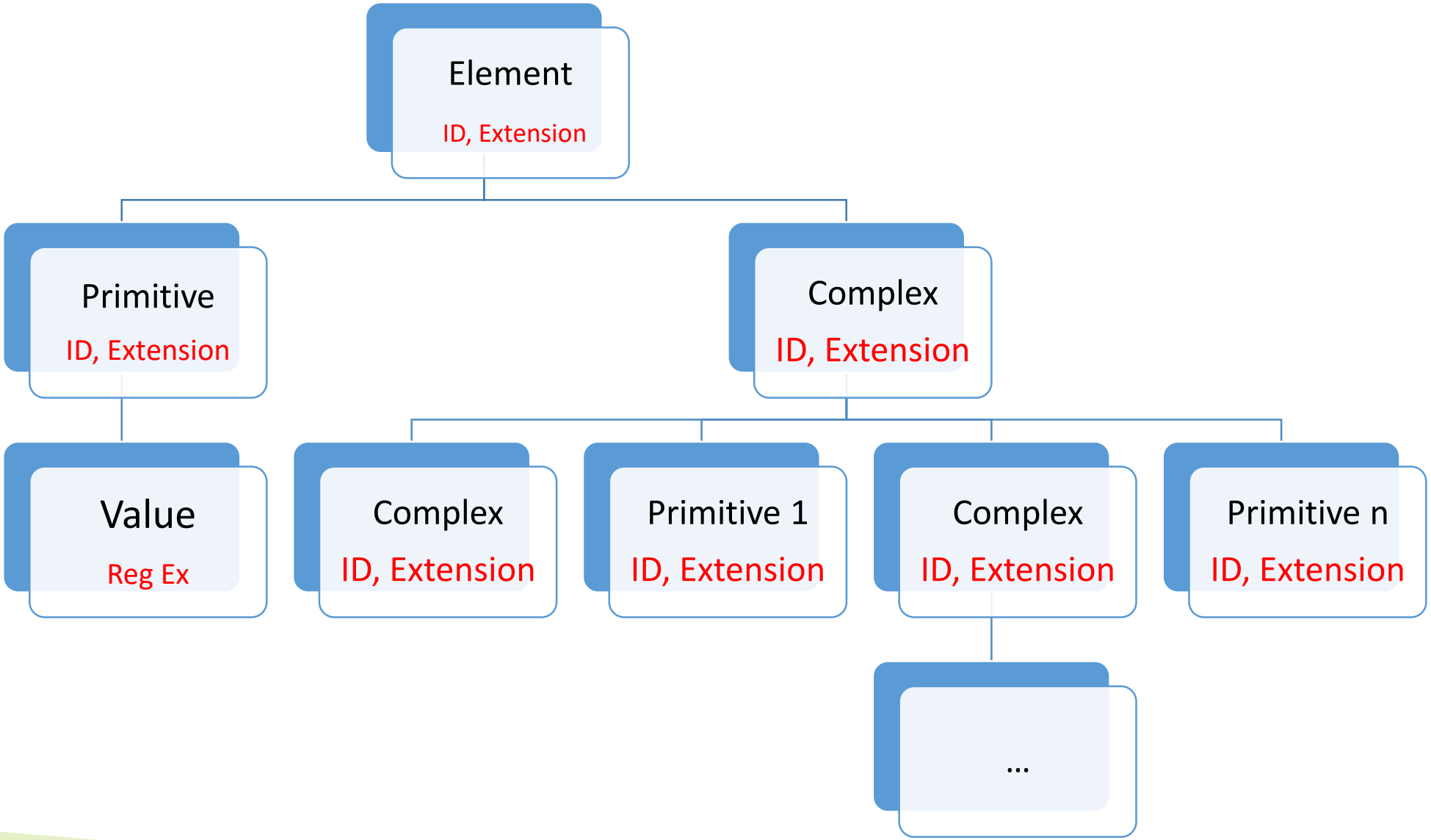
אבטחת מידע במערכות FIHR כוללת את

כלל רבדי ההגנה העומדים לרשותנו

משרד הבריאות
לחיים בריאים יותר

הגנת הממשקים

הגנת ממשקים – וולידציית FHIR API



הגנת ממשקים – וולידציית FHIR API

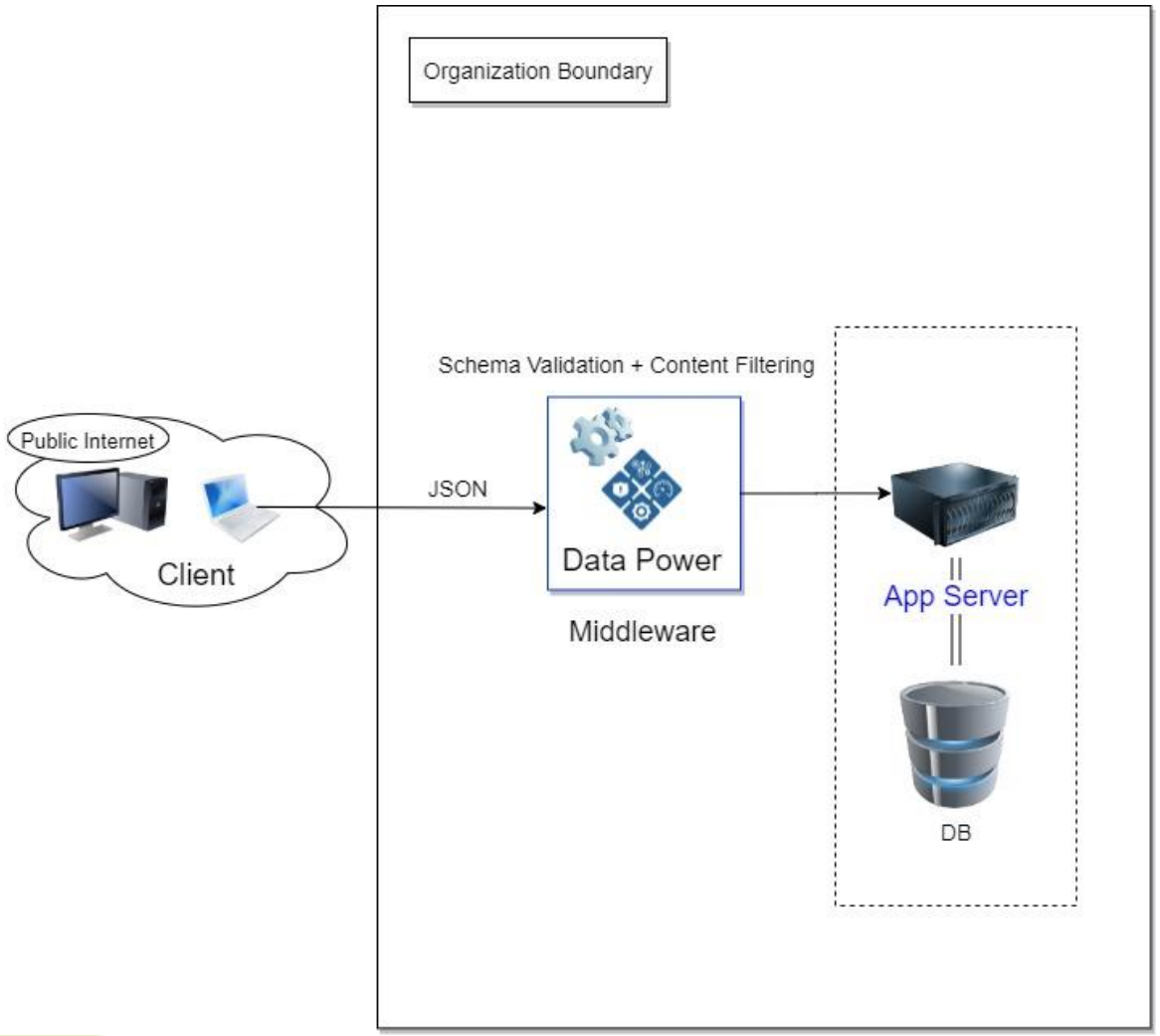
תפיסה קלאסית

- ✓ הגנה ברמת ממשק
- ✓ סכימה ייחודית
- ✓ ולידצית תוכן פרטנית פר שדה בודד

תפיסת FHIR

- ✓ הגנה בכלל הרבידים
- ✓ סכימה דינמית
- ✓ ולידציה תוכן גנירת פר סוג שדה

הגנת ממשקים – וולידציית FHIR API



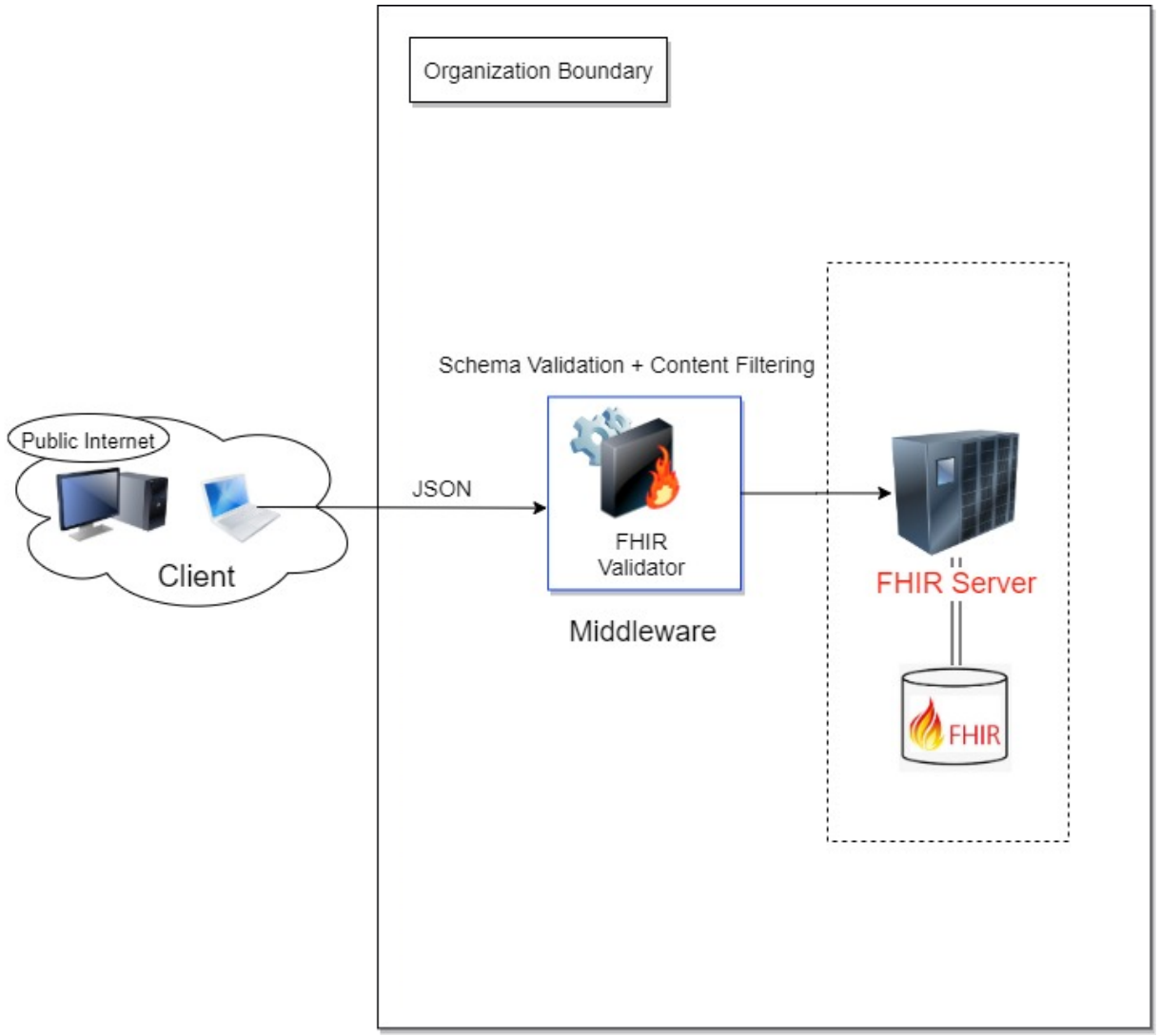
תפיסה קלאסית

- ✓ הגנה ברמת ממשק
- ✓ סכימה ייחודית
- ✓ ולידצית תוכן פרטנית פר שדה בודד

הגנת ממשקים – וולידציית FHIR API

תפיסת FHIR

- ✓ הגנה בכלל הרבידים
- ✓ סכימה דינמית
- ✓ ולידציה תוכן גנירת פר סוג שדה



משרד הבריאות
לחיים בריאים יותר

תפיסה להגנת מערכות FHIR

Schema קלאסית ל-API סטאטי

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Patient demographics",
  "properties": {
    "parentName": {
      "type": "string",
      "minLength": 1,
      "maxLength": 64,
      "pattern": "[A-Za-z0-9\\-\\.]{1,64}"
    },
    "gender": {
      "type": "string",
      "enum": ["male", "female", "other", "unknown"]
    },
    "birthDate": {
      "type": "string",
      "pattern": "([0-9]([0-9]([0-9][1-9]|[1-9]0)|[1-9]00)|[1-9]000)(-(0[1-
9]|1[0-2])(-(0[1-9]|[1-2][0-9]|3[0-1]))?)?"
    },
    "city": {
      "type": "string"
    }
  }
}
```

Json קלאסי

```
{
  "parentName": "משה",
  "gender": "male",
  "birthDate": "1999-01-01",
  "city": "תל אביב"
}
```

משרד הבריאות
לחיים בריאים יותר

FHIR Json

```
{
  "resourceType": "Patient",
  "extension": [
    {
      "url": "http://fhir.health.gov.il/StructureDefinition/ext-parent-name",
      "valueString": "משה"
    }
  ],
  "gender": "male",
  "birthDate": "1999-01-01",
  "address": [
    {
      "city": "תל אביב"
    }
  ]
}
```

הרחבה(משתנה)

קבוע

משרד הבריאות
לחיים בריאים יותר

Definition Structure FHIR-מבנה ב

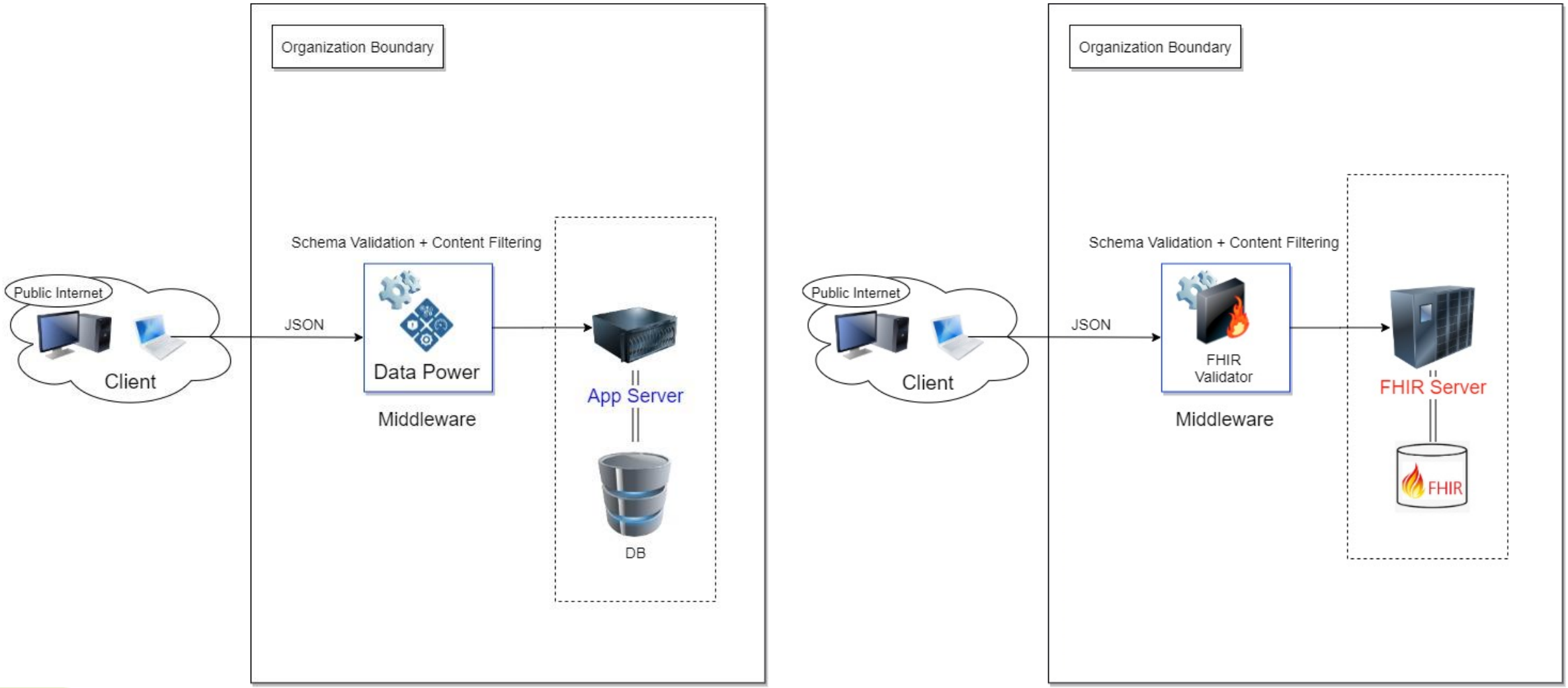
```
{
  "resourceType": "StructureDefinition",
  "name": "Patient",
  "description": "Demographics and other administrative information about an
individual or animal receiving care or other health-related services.",
  "kind": "resource
  "baseDefinition":
  "differential": {
    "element": [
      {
        "id": "Pati
        "min": 0,
        "max": "1",
        "type": [{"code": "code"}]
      },
      {
        "id": "Patient.birthDate",
        "min": 0,
        "max": "1",
        "type": [{"code": "date"}]
      },
      {
        "id": "Patient.address",
        "min": 0,
        "max": "*",
        "type": [{"code": "Address"}]
      }
    ]
  }
}
```

date	A date, or partial date (e.g. just year or year + month) as used in human communication. The format is YYYY, YYYY-MM, or YYYY-MM-DD, e.g. 2018, 1973-06, or 1905-08-23. **There SHALL be no timezone offset**. Dates SHALL be valid dates. Regex: ([0-9]([0-9]([0-9][1-9]|[1-9]0)|[1-9]00)|[1-9]000)(-(0[1-9]|1[0-2])(-(0[1-9]|[1-2][0-9]|3[0-1]))?)?	union of xs:date, xs:gYearMonth, xs:gYear	A JSON string - a union of xs:date, xs:gYearMonth, xs:gYear
		XML Definition	JSON Definition

```
{
  "resourceType": "StructureDefinition",
  "name": "date",
  "description": "A date or partial date (e.g. just year or year + month). Dates
SHALL be valid dates."
        "max": "1",
        "type": [
          {
            "extension": [
              {
                "url": "http://hl7.org/fhir/StructureDefinition/regex",
                "valueString": "([0-9]([0-9]([0-9][1-9]|[1-9]0)|[1-9]00)|[1-
9]000)(-(0[1-9]|1[0-2])(-(0[1-9]|[1-2][0-9]|3[0-1]))?)?"
              }
            ],
            "code": "http://hl7.org/fhirpath/System.Date"
          }
        ]
      }
    ]
  }
}
```

משרד הבריאות
לחיים בריאים יותר

הגנת ממשקים – וולידציית FHIR API



משרד הבריאות
לחיים בריאים יותר

העברת קבצים

העברת קבצים במערכות FHIR

Runtime

ICAP/API

- Request Retention
- Base 64 Assembly
- File Sandboxing
- Ack Replay
- Request forwarding

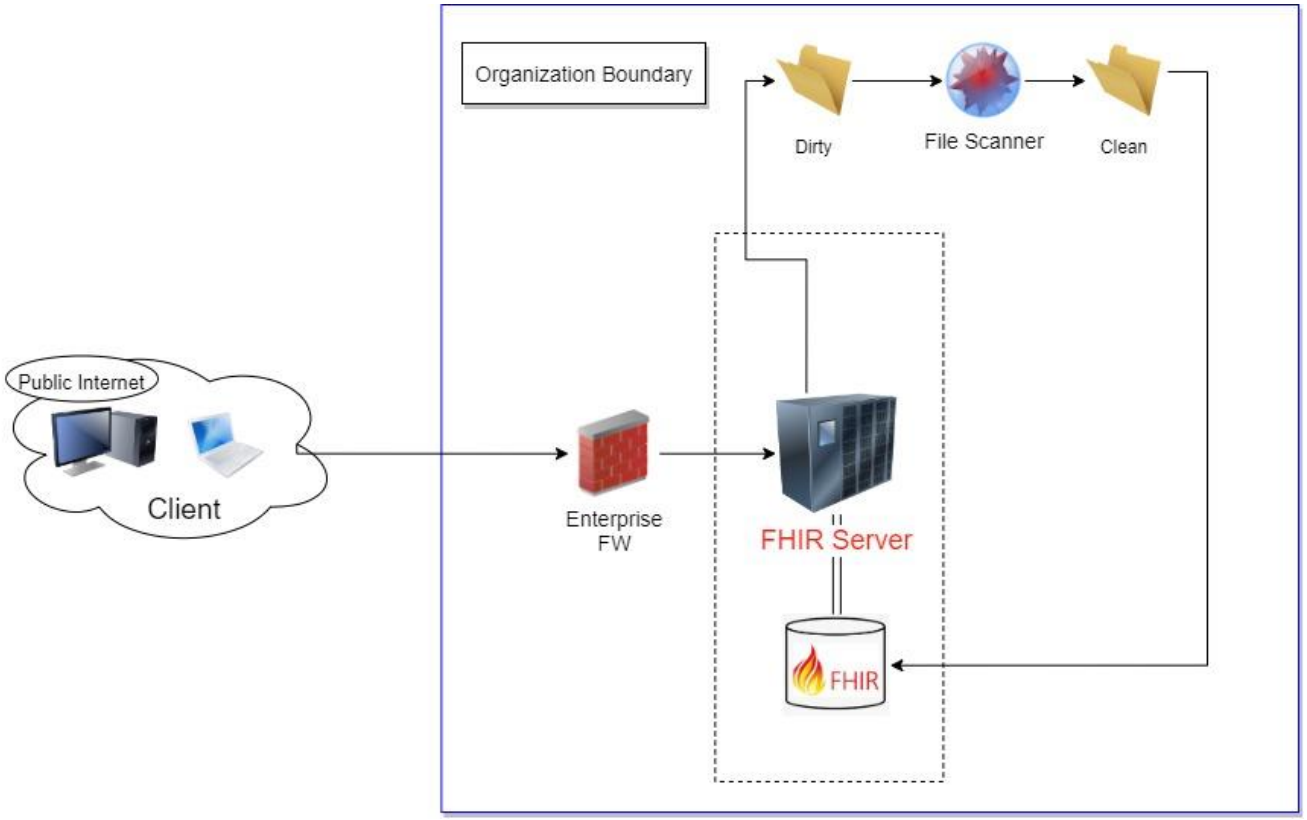
Non real Time

Async Processing

- File landing
- File Scanning
- File delivery

העברת קבצים במערכות FHIR

Non real Time



Async Processing

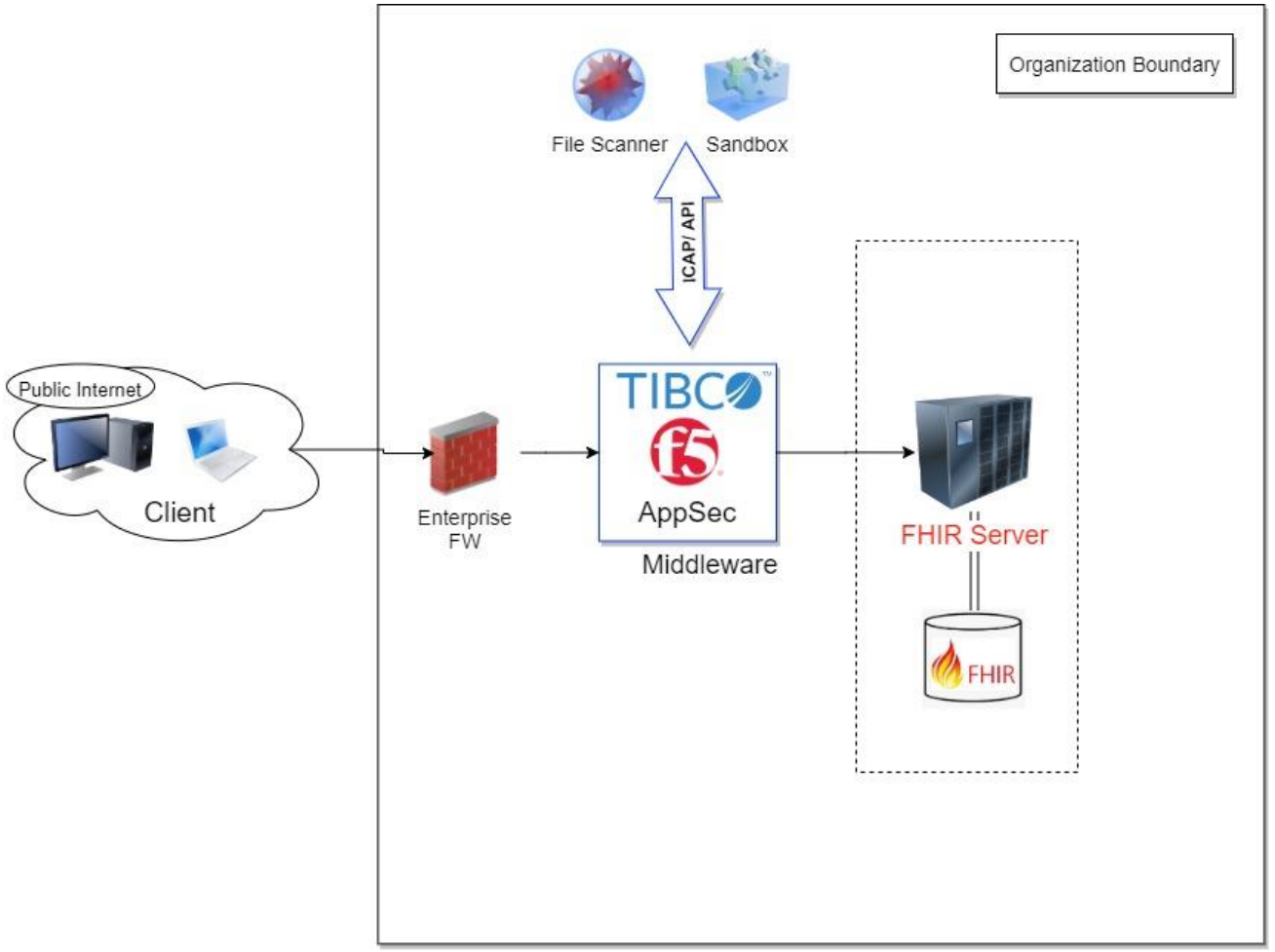
- File landing
- File Scanning
- File delivery

העברת קבצים במערכות FHIR

Runtime

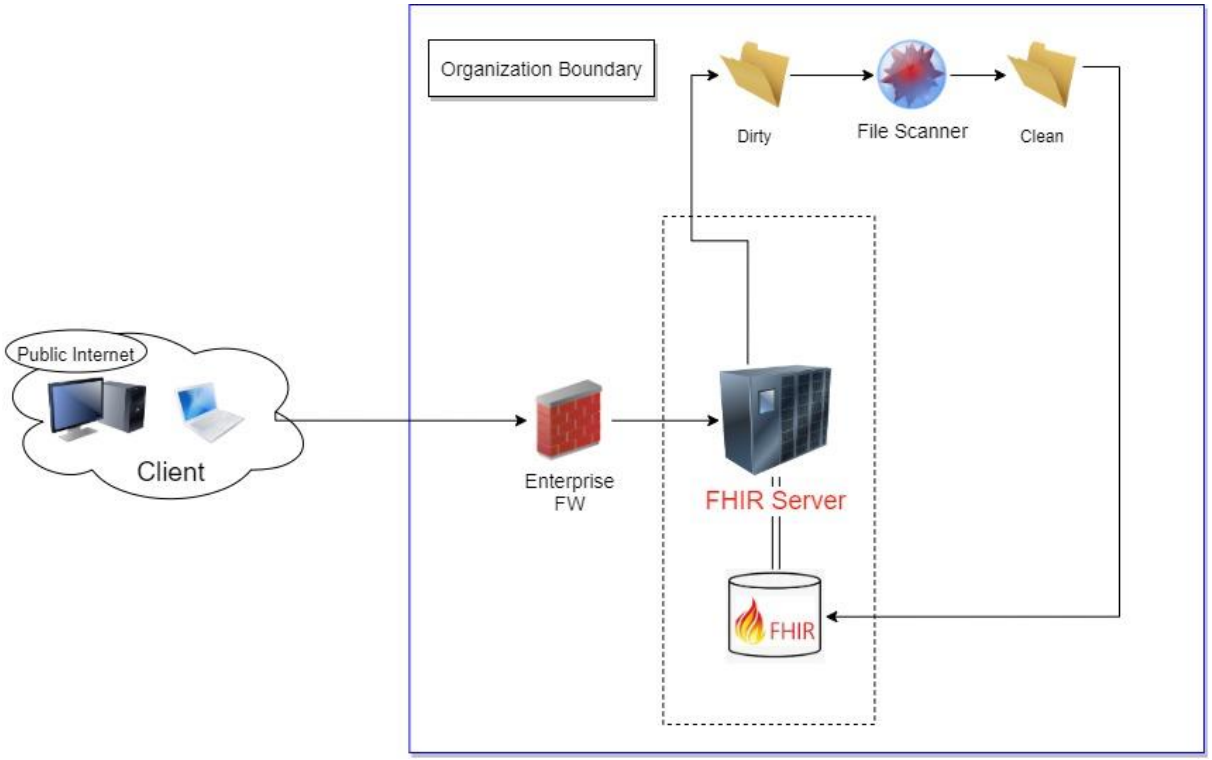
ICAP/API

- Request Retention
- Base 64 Assembly
- File Sandboxing
- Ack Replay
- Request forwarding

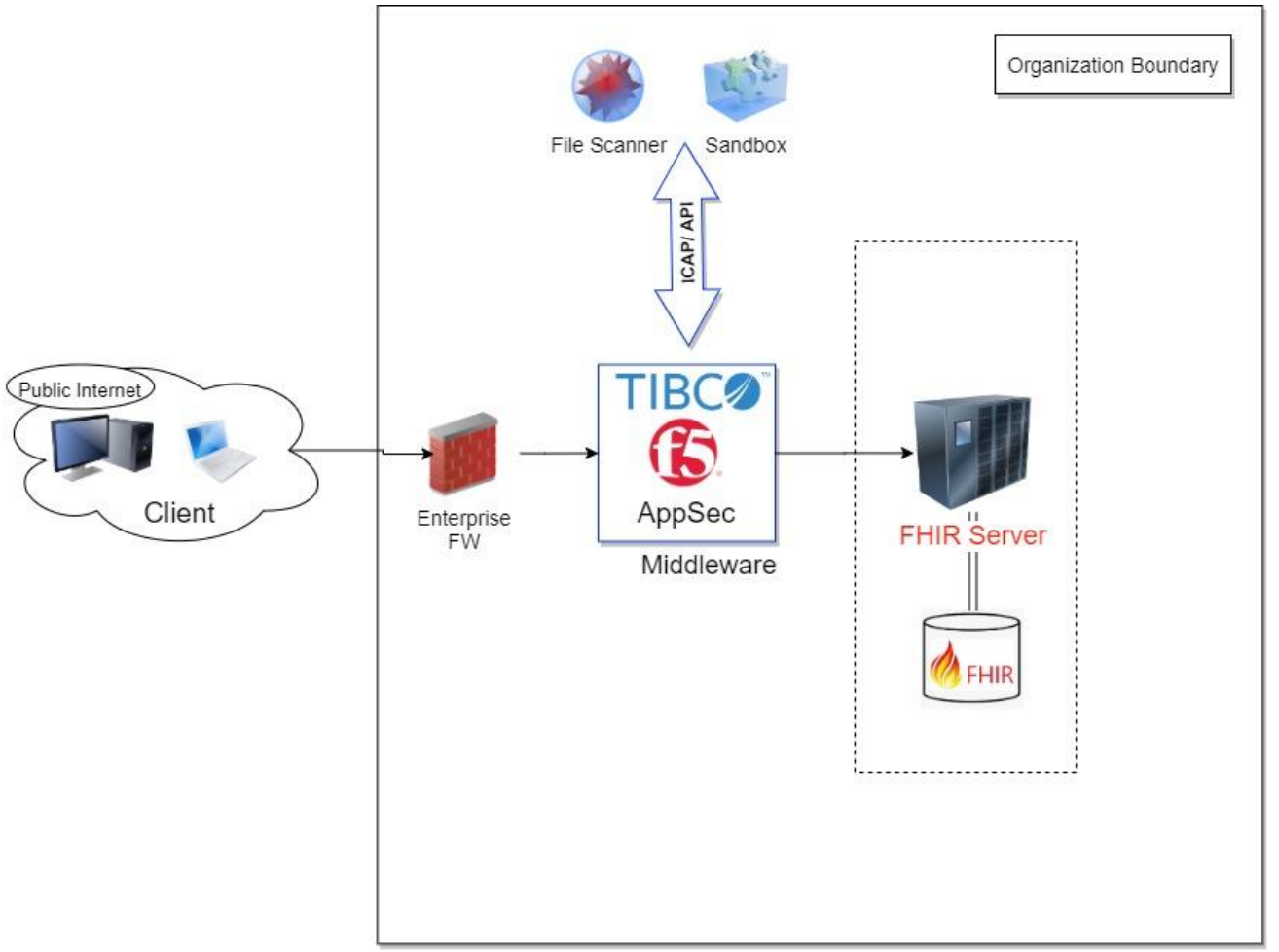


העברת קבצים במערכות FHIR

Non real Time



Runtime



אימות זהות המשתמש

אימות זהות המשתמש (User Authentication)

ID Token obtaining (JWT)
- Time to Leave
- Token Validation

JWT

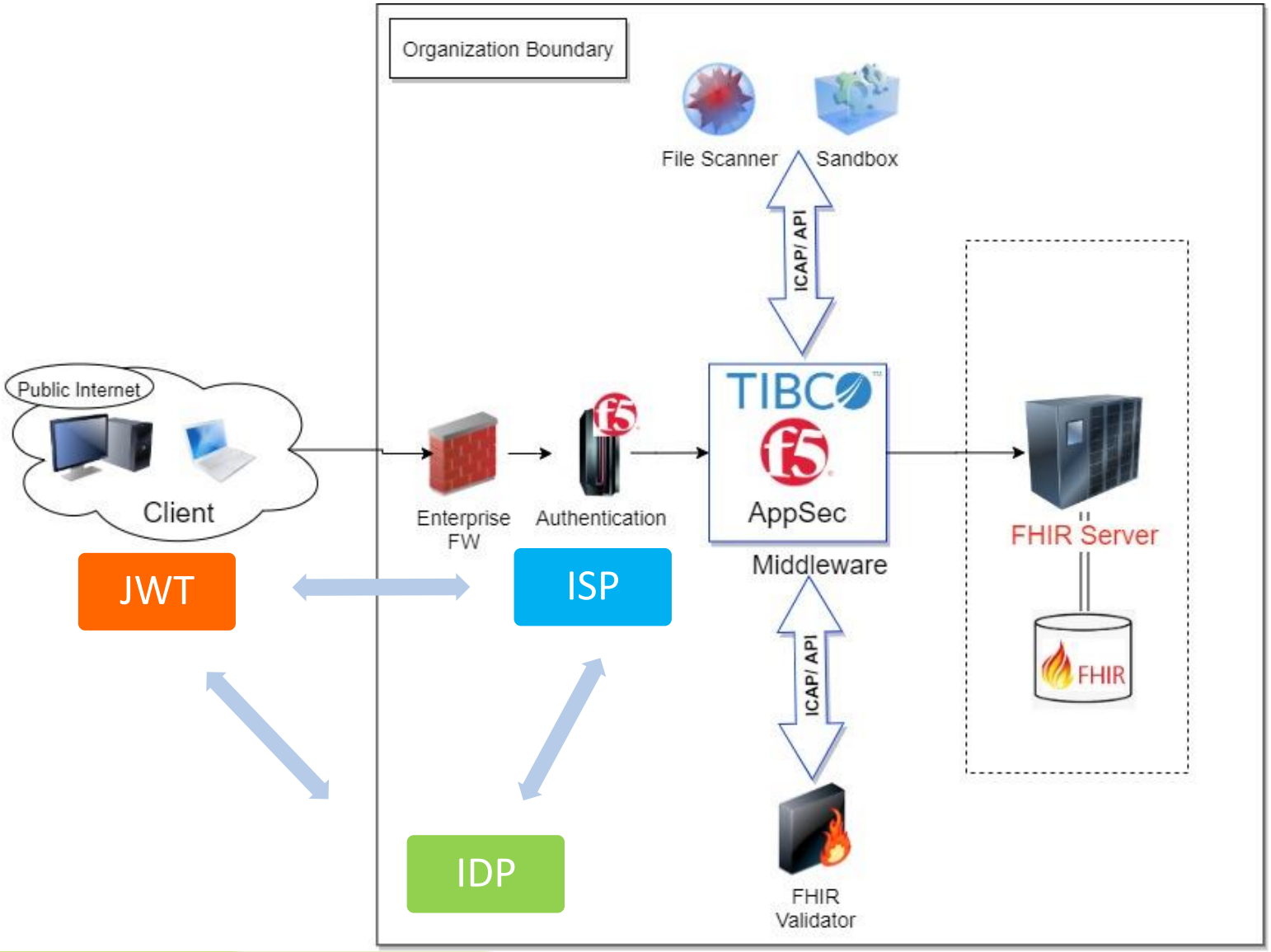
- FHIR Server
- 3-rd Party (Middleware, Reverse Proxy)

ISP

IDP

- Internal
  - ID Enrollment
  - Regulation
- 3-rd Party
  - Gov.il
  - Every trusted ID holder (under Gov.il regulation)

אב-טיפוס מעטפת ההגנת מערכת FHIR



תודה