CSO Conference *& Awards*

Produced by CSO | IDC

HAPI – API Security Governance Dashboard

TIAA, API Security

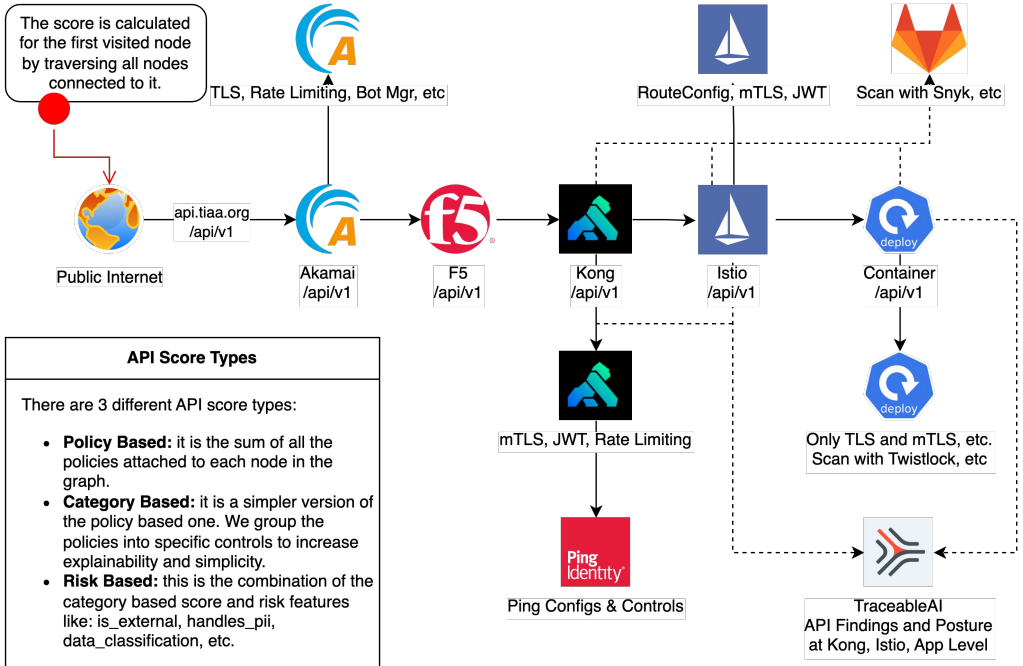
Robust API Security Governance - Requirements

Security Posture Management • Continuous endpoint monitoring to ensure adherence to secure defaults • Real-time security alerts • Proactive risk identification & remediation	**Risk Analysis** • Intelligent risk assessment • Quantifiable risk (scoring) • Data-driven decision-making	**Integrations with** • API Catalog and lifecycle Management system • And with other systems such as Observability & ASPMs • Vulnerability Management & Incident Response processes
Reporting • Customizable security metrics • Instant compliance insights • Real-time gap identification	**API Traffic** • Visual API relationships in a call flow • Efficient troubleshooting	**Intuitive Interface** • For developers and security pros • Role-based access & views • Comprehensive documentation & support

HAPI Capabilities

- Allows for defining enterprise level API security policies for consistency & enforcement
- Integrates with multiple components of the API tech stack (cloud & on-prem) including source code, build time, deployment and runtime components to create E2E flow tracking
- Analyzes configuration information against policy definition for adherence
- Creates AI based risk scoring to create API & app level risk posture
- Integrates with standard vulnerability management process to prioritize remediation
- Provides actionable remediation & mitigation guidance for failed policies improving developer productivity & reducing time to compliance

HAPI System Design



API Score Types

There are 3 different API score types:

- **Policy Based:** it is the sum of all the policies attached to each node in the graph.
- **Category Based:** it is a simpler version of the policy based one. We group the policies into specific controls to increase explainability and simplicity.
- **Risk Based:** this is the combination of the category based score and risk features like: is_external, handles_pii, data_classification, etc.

Category Based Scoring Mechanism for api.tiaa.org/fdx/v1/accounts (better explainability)	
Auth N and Z	20%
Encryption	20%
Vulnerablity Mgmt	20%
Rate Limiting	10%
Monitoring and Observability	10%
Score	**100%**

Risk Based Score Mechanism
for api.tiaa.org/fdx/v1/accounts
(better explainability)

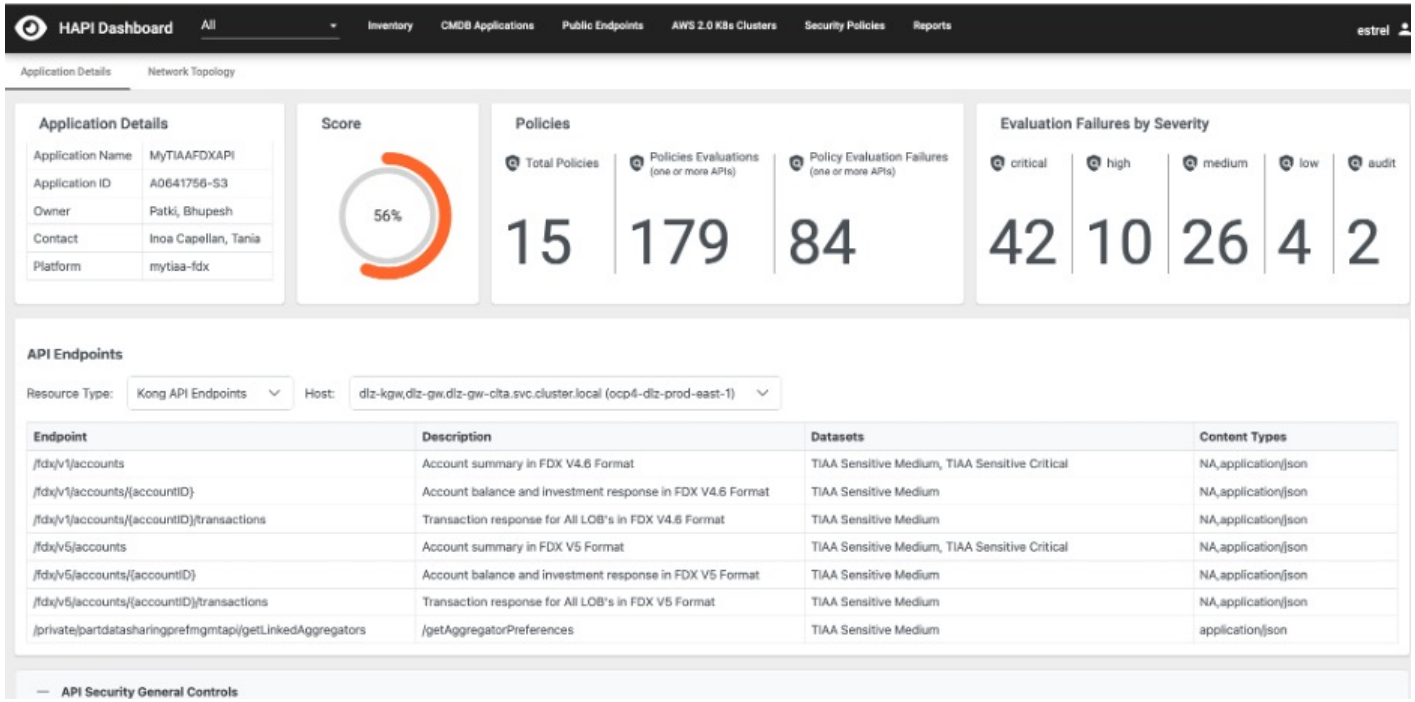
```
InheritRiskFeatureScore = [
  IS_EXTERNAL = 0|1,
  IS_SOX_RELEVANT = 0|1,
  IS_SAS_70_RELEVANT = 0|1,
  IS_TCFR_RELEVANT = 0|1,
  HANDLES_PII = 0|1,
  DATA_CLASSIFICATION = 0|1,
  HIGH_CRITICAL_VULNERABILITIES = 0|1,
]
APIRiskScore = CategoryBasedScore * (
   1 - (InheritRiskFeatureScore / InheritRiskFeatureScoreLength)
)
```

Note: the features are extracted from the enterprise risk database, and overridden by the HAPI findings.

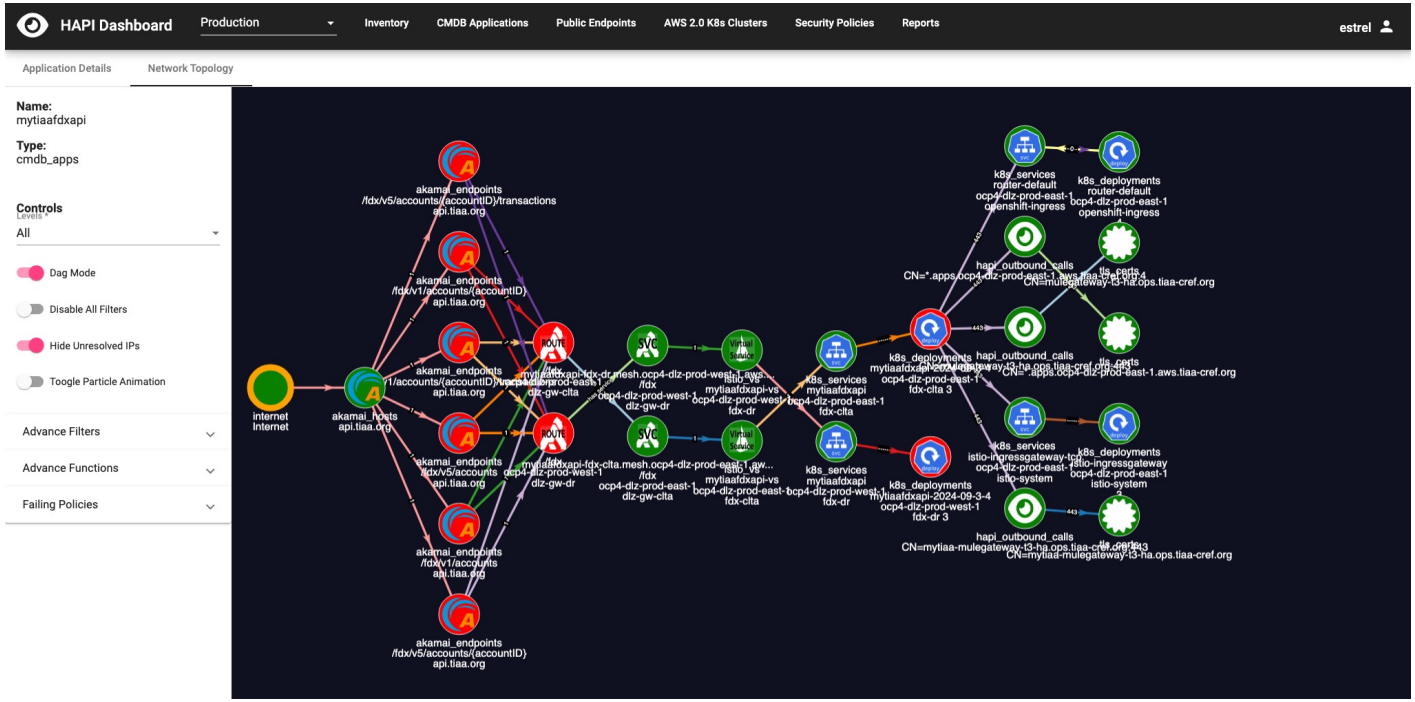
Reports & Dashboards

- HAPI has a proprietary query language that allows developers and security analysts to prototype reports and dashboards with ease to dissect data from multiple viewpoints
- Data exploration is key to reporting. By searching for an application or an API, the user gets an end-to-end graph with all the nodes attached to the request path; from an Akamai endpoint all to the way container, image, git repo, vulnerabilities, etc.
- Provides a graph view of E2E deployment stack to identify vulnerable components as well as risk exposure
- Application Details page provides actionable intelligence to API developers for mitigating against failed policies

Application Details Page



Application Network Topology View



Operationalizing HAPI

- Integrated with enterprise maturity scoring to bring visibility
- Available as a self-service tool to all API developers to self-remediate issues
- Categorizes policies & remediation at app level vs platform level for clear accountability
- Feeds into enterprise vulnerability management system for prioritization based on risk scoring
- Fine tune policies to detect common security configuration issues for consistent enforcement eg: all APIs should have SAST & DAST enabled

Challenges operationalizing HAPI

- Complex deployment architectures including cloud and legacy on-prem deployments
  - Prioritize key components of the tech stack
- Accrued tech debt over years with budget constraints to fix legacy problems
  - Use risk based approach to mitigate problems
- Multiple components/layers in tech stack with multiple owners and no single point of responsibility
  - Leverage enterprise inventory systems for coordination

Contacts

Phani Kotharu – Phani.Kotharu@tiaa.org

Lucas Estrella – Lucas.Estrella@tiaa.org

Kapil Pruthi - Kapil.Pruthi@tiaa.org