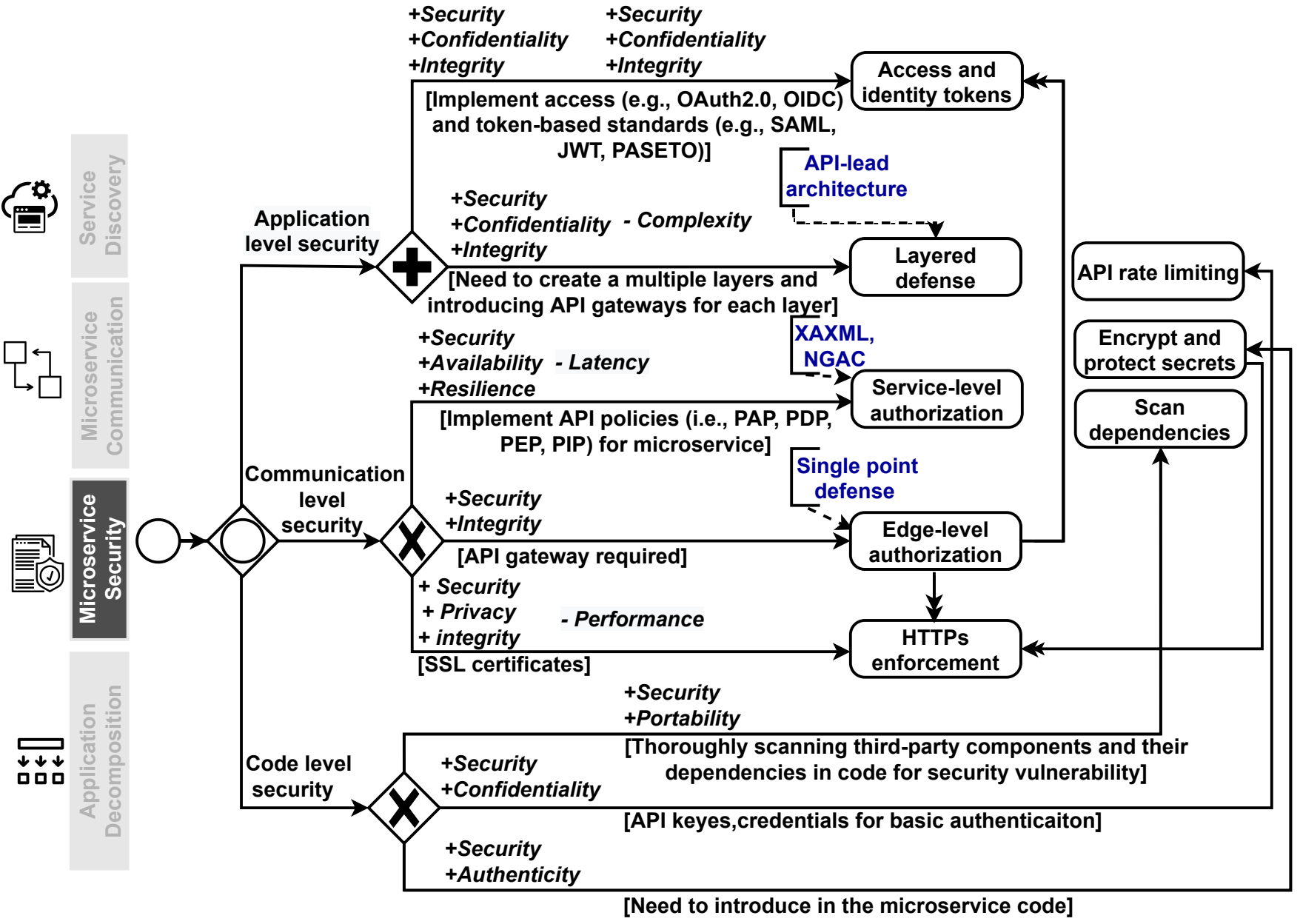
Service Discovery
Microservice Communication
Microservice Security
Application Decomposition
Application level security
Communication level security
Code level security
+Security
+Confidentiality
+Integrity
+Security
+Confidentiality
+Integrity
Access and identity tokens
[Implement access (e.g., OAuth2.0, OIDC) and token-based standards (e.g., SAML, JWT, PASETO)]
API-lead architecture
+Security
+Confidentiality
+Integrity
- Complexity
Layered defense
[Need to create a multiple layers and introducing API gateways for each layer]
API rate limiting
Encrypt and protect secrets
Scan dependencies
+Security
+Availability
+Resilience
- Latency
XAXML, NGAC
Service-level authorization
[Implement API policies (i.e., PAP, PDP, PEP, PIP) for microservice]
Single point defense
+Security
+Integrity
Edge-level authorization
[API gateway required]
+ Security
+ Privacy
+ integrity
- Performance
HTTPs enforcement
[SSL certificates]
+Security
+Portability
[Thoroughly scanning third-party components and their dependencies in code for security vulnerability]
+Security
+Confidentiality
[API keyes,credentials for basic authenticaiton]
+Security
+Authenticity
[Need to introduce in the microservice code]