# Relation of the Big Data Security Operational Taxonomy to the Reference Architecture

System Orchestrator:

|  |  |
| --- | --- |
| * Policy Enforcement * Security Metadata Model * Data Loss Prevention, Detection * Data Lifecycle Management * Threat and Vulnerability Management * Mitigation * Configuration Management * Logging * Malware Surveillance and Remediation * Resiliency, Redundancy and Recovery * Accountability * Compliance * Forensics * Business Risk Model | Several security functions have been mapped to the System Orchestrator Block as they require architectural level decisions and awareness. Aspects of these functionalities are strongly related to the Security Fabric and thus touch the entire architecture at various points in different forms of operational details.  Such security functions include nation-specific compliance requirements, vastly expanded demand for forensics, and domain-specific, privacy-aware business risk models. |

Data Provider:

|  |  |
| --- | --- |
| * Device, User, Asset, Services, Applications Registration * Application Layer Identity * End User Layer Identity Management * End Point Input Validation * Digital Rights Management * Monitoring, Alerting | Data Providers are subject to guaranteeing authenticity of data and in turn require that sensitive/copyrighted/valuable data is adequately protected. This leads to operational aspects of entity registration and identity ecosystems. |

Data Consumer:

|  |  |
| --- | --- |
| * Application Layer Identity * End User Layer Identity Management * Web Services Gateway * Digital Rights Management | Data Consumers exhibit a duality with Data Providers in terms of obligations and requirements – only they face the access/visualization aspects of the Application Provider. |

Application Provider:

|  |  |
| --- | --- |
| * Application Layer Identity * Web Services Gateway * Data Transformation * Digital Rights Management * Monitoring, Alerting | Application Provider interfaces between the Data Provider and Data Consumer. It takes part in all the secure interface protocols with these blocks as well as maintains secure interaction with the Framework Provider. |

Framework Provider:

|  |  |
| --- | --- |
| * Virtualization Layer Identity * Identity Provider * Encryption and Key Management * Isolation/Containerization * Storage Security * Network Boundary Control | Framework Provider is responsible for the security of data/computations for a significant portion of the lifecycle of the data. This includes security of data at rest through encryption and access control; security of computations via isolation/virtualization; and security of communication with the Application Provider. |