Security Framework

There are two main aspects to security in relation to the OpenECOMP platform: security of the platform itself and the capability to integrate security into the cloud services. These cloud services are created and orchestrated by the OpenECOMP platform. This approach is referred to as security by design.

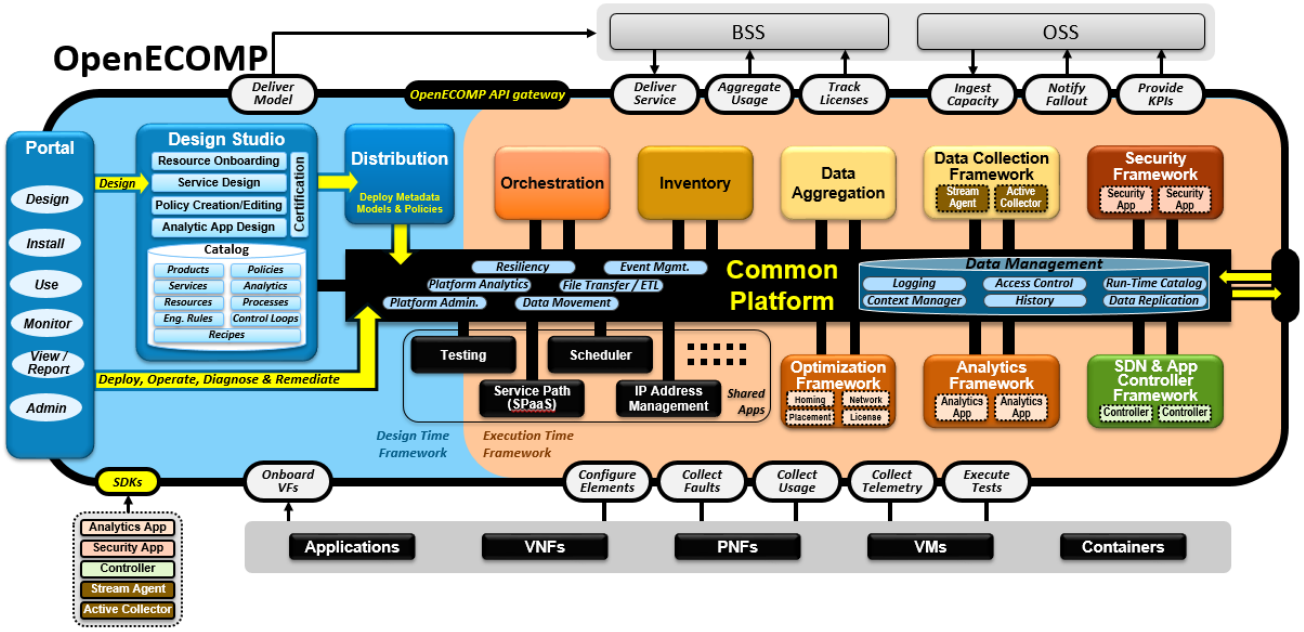

Figure 1. OpenECOMP platform decomposition

The enabler for these capabilities within OpenECOMP is an API-based Security Framework, depicted in Figure 1 as the "Security Framework" box. One such set of APIs is the Application Authorization Framework (AAF) <<DocRef: AAF API Specification>>, which in turn calls external security platforms.

Security of the platform begins with a strong foundation of security requirements and following security best practices as an inherent part of the OpenECOMP design. Some examples include:

- deployment of the platform on a secure physical and network infrastructure
- adherence to secure coding best practices
- security analysis of source code
- vulnerability scanning
- defined vulnerability patching process

Building upon this foundation, external security platforms that provide additional security capabilities such as identity and access management, micro-perimeter controls, and security event analysis are integrated onto the platform through advantageous use of the OpenECOMP Security Framework. The additional security these external platforms provide are described below.

Security modules such as an Identity and Access Management (IAM) platform provide critical security capabilities to the OpenECOMP solution. Access management enhancements deliver preventive and detective access controls for the OpenECOMP portal and related front ends. Options for fine grained authorization capability also exist. For identity lifecycle management, this platform provides user provisioning, access request, approval and review capabilities and is designed to minimize the administrative burden.

Security event analysis, provided by a security analytics platform, will use the OpenECOMP DCAE data collection and analytics engine to gather VNF data, network data, logs and events. Once the security analysis has determined that a security event has occurred, a pre-determined policy can be invoked via the OpenECOMP platform. The ability to respond automatically to a security-related event, such as a Distributed Denial of Service (DDoS) attack, will enable closed loop security controls, such as modifying firewall rules, or updating Intrusion Prevention System (IPS) signatures, etc. In the event that a pre-determined policy has not been created for an event, it will be sent to a ticket system, and then a new policy can be generated for the next time that event occurs.

The OpenECOMP platform also enables security by design for services it orchestrates by engaging a security trust model and engine. This begins with validation of security characteristics of resources as part of the SDC resource certification process. This assures service designers are using resource modules that have accounted for security. Using the OpenECOMP security framework to access an external security engine, additional security logic can be applied and enforced during service creation.

OpenECOMP is a platform for many types of services. Because of its inherent security, it is also a powerful means to provide security as a service. In many ways, security services are similar to other services; however, even more so than other services, security services must be provided via a platform and infrastructure that is inherently secure.

Many types of security services can be offered, spanning access control, authentication, authorization, compliance monitoring, logging, threat analysis and management, etc. For example, when a customer has a need for a vFW (Virtual Firewall), the customer provides the needed information via the Portal to enable OpenECOMP to determine and orchestrate the firewall placement. In addition, the firewall capabilities (e.g., rules, layer 7 firewall) are instantiated at the appropriate locations within the architecture. If necessary, many security controls and technologies including firewalls, URL blocking, etc., can be service-chained to provide all the needed functionality. As part of an overall security architecture, the log data from the firewalls can be captured by DCAE and used by the threat management application to perform security analytics. Should a threat be detected, various mitigation steps can be taken, such as altering IPS settings, changing routing, or deploying more resources to better absorb an attack. This can be achieved by an external security mechanism working with OpenECOMP to deploy the appropriate updates across the infrastructure, thereby minimizing the service interruption due to the security threat.