Overview

About the Cisco Platform

The platform is designed to address a number of data center operational and security challenges comprehensively using rich traffic telemetry collected across the infrastructure, predominantly from servers. The platform performs advanced analytics using an algorithmic approach and enforces a consistent allowed-list policy for applications. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis. The platform provides a ready-to-use solution. The platform provides the following capabilities:

- Behavior-based application insight to automate allowed-list policy generation
- Application segmentation to enable efficient and secure zero-trust implementation
- Consistent policy enforcement across on-premises data centers and private and public clouds
- Identification of process behavior deviations, software vulnerabilities, and exposure to reduce attack surface
- Identification of application behavior changes and policy compliance deviations in near-real-time
- Support of comprehensive telemetry processing in a heterogeneous environment to provide actionable insight within minutes
- Long-term data retention for deep forensics, analysis, and troubleshooting

To support the various use cases within the platform, the platform requires consistent telemetry from across the data center infrastructure. With the support to collect telemetry using multiple approaches, this platform is designed to support both existing and new data center infrastructures. These infrastructures could be on-premises or in a public cloud.

The predominant approach to telemetry collection is the software sensors. Software (host) sensors can be installed on any end host (virtualized, bare-metal, or container) servers. These sensors act as the enforcement point for the application segmentation policy that the platform generates. Using this approach, the platform provides consistent enforcement across public, private, and on-premises deployments. Sensors enforce the policy using native operating system capabilities, thereby eliminating the need for the sensor to be in the data path and providing a fail-safe option. In addition, the platform has the capability to track process and

communication behavior deviations and software vulnerabilities, thereby offering a comprehensive workload protection capability.