ARTICLE

Supporting Cloud Migration via Application Dependency Mapping:
An Overview of the TrueFort Platform

PREPARED BY
Dr. Edward G. Amoroso
CHIEF EXECUTIVE OFFICER, TAG CYBER LLC
RESEARCH PROFESSOR, NYU

Cloud migration initiatives can fail if application dependencies are unknown or poorly understood. The TrueFort Fortress[1] commercial platform discovers and illuminates application dependency mappings using a behavior-based approach to address this problem.

Introduction

The decision to host legacy or new applications in cloud infrastructure follows the progression of enterprise infrastructure to zero trust. That is, with the dissolution of the legacy perimeter, security teams have come to understand how important it is for applications, which are more easily accessible from public cloud, to include cloud-native protections that protect data, system integrity, and surrounding infrastructure.

One of the primary obligations that exists in this process for both security teams and application experts involves establishing security readiness for any application to be hosted in the cloud. For new applications under development, this protection property will be embedded in the functional requirements used during DevOps. For existing legacy applications, however, establishing readiness must follow a different approach.

Such readiness in the context of successful migration of applications to the cloud can be elusive. A recent study sponsored by cloud migration experts Flexera[2] suggests that modern organizations identify the establishment of dependencies for their migrating applications as the most significant roadblock to success[3]. As one might expect, such dependencies typically require non-manual mappings, and this has not been a common practice to date.

The urgency to succeed with application migration is further extended with the types of critical applications being transitioned to public cloud. This paper explains the current state of cloud migration, and why a lack of visibility into application dependencies is such a problem. The TrueFort Fortress platform is shown to offer an effective behavior-based approach to application visibility that enables successful migration of critical applications to public cloud.

[1] - See https://truefort.com/
[2] - See https://www.flexera.com/
[3] - See recent study on cloud migration at https://resources.flexera.com/

Current State of Cloud Migration

While it is common for enterprise teams to tout their intention to drive applications to the public cloud, the reality is that most organizations today are either in hybrid mode, or largely avoiding public cloud infrastructure. For example, the Flexera report mentioned above suggests that fewer than 47% of enterprise workloads today are hosted in public cloud. This is a startling statistic given the benefits of public cloud hosting.

The good news, however, is that the motivations to rehost, transition, or rebuild critical and sensitive applications in public cloud are significant. The economics of public cloud, for instance, are obviously a major driver, although careful attention to transaction costs due to migration must be managed[4]. COVID-19 and its effects on work-from-home initiatives continue to represent another major incentive for cloud application hosting.

In practice, the current state of cloud migration is growing – with more organizations each day transitioning their applications into a publicly accessible cloud service infrastructure. McKinsey predicted accurately that cloud-specific spending would grow at a rate roughly six times the rate of general IT spending – and much of this spend is being directed to the hosting of business applications[5].

According to the Flexera report, organizations are becoming more open to shifting their highly sensitive applications to the cloud, and they are increasing their cloud spend dramatically by an average of 39%. It is therefore reasonable to expect enterprise cloud spending on application transition to cloud to maintain this trend – and this highlights the importance of reducing migration risk.

Application Dependency Mapping

Modern applications have evolved from monolithic software designs hosted on individual physical servers in private data center environments into distributed applications consisting of containerized functions that interact with their environments through application programming interfaces (APIs). This commonly includes front-end interfaces for users and back-end interfaces for databases.

The dependencies that emerge in such architectures can become complex as individual functions that might have been coded into monolithic programs are represented instead as containerized applications. The communication between these containerized applications is easily orchestrated when in a common operating environment, but might become more complex when the workload is hosted in a hybrid, multi-cloud environment.

Suppose, for example, that a monolithic application hosted in a traditional premise data center is dependent upon a backend database that contains sensitive information such as customer data. If that application is moved to a public cloud, then the database must either travel with the application, or must be accessible once the app has been migrated. Clearly, such application dependency must be mapped to both local and external resources as part of the migration.

Research suggests that such dependency mappings are indeed both important and difficult. The Flexera report suggests that this issue represents the top migration challenge for organizations moving their applications to the cloud. Their research suggests further that this challenge is greater for enterprise teams with more complex, premise-hosted applications, which should not be a surprising result.

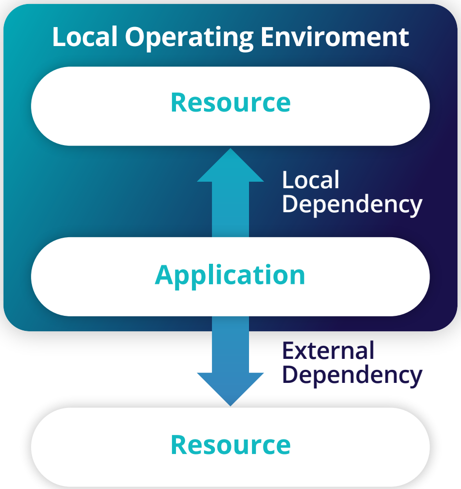

FIGURE 1. Application Dependency Mapping

One issue that emerges with any dependency mapping is the on-going evolution and change that must be expected for any non-trivial software application. This implies that any application dependency mapping initiative must be viewed as an on-going process versus a snapshot assessment. Any static view of dependencies will miss periodic updates, historical data, and planned changes.

An additional issue is that the dependency mappings must be complete. That is, if key dependencies are missed during the migration process, then the application will break – either immediately if the dependency is significant or at some later time if the dependency is subtle and periodic. Enterprise teams thus require a dynamic application dependency mapping capability – one that addresses these key challenges in practical environments.

[4] - See recent Journal of Cloud Computing study on cloud transaction costs and economics at https://journalofcloudcomputing.springeropen.com/
[5] - See report at https://www.mckinsey.com/

Understanding TrueFort Fortress

TrueFort focuses on solutions that offer enterprise security teams real-time application insight and protection at scale. Specifically, the TrueFort Fortress platform was designed to support security and compliance requirements for application-level visibility to reduce cyber risk and streamline initiatives such as cloud migration. The goal is to deliver an application profile that can help to provide a baseline for tasks such as migration.

This profile is developed through observation of the target application's behavior. Such data collection occurs over time, with the operational goal to discover flows, dependencies, and other relationships. The Fortress platform includes support for enterprise security administrators to drill-down into collected application behavioral profiles to obtain more detail on any interaction.

The analytics that drive Fortress combine continuous behavioral observation with adaptive machine learning-based algorithms. The security goal is to learn which functions an application should be expected to perform, and which are outside the normal behavioral profile. The platform uses this information and processing to create a so-called adaptive trust graph across the run-time application environment.

Fortress offers three types of application behavioral visibility – communications, dependencies, and credentials. The role of each visibility component is briefly outlined below in the context of establishing readiness for migrating a given application to public cloud infrastructure.

Communication – One of the most important characteristics of any software application that is relevant to both attack surface posture and cloud readiness determination involves all communications into and out of the application. Broadly, these communications can be partitioned into front-end access by users and back-end access by administrators.

Important characteristics of such communications include frequency of access often graphed against time, length of sessions, types of commands used, and volumetrics such as the size of any input or output payloads. Collectively, this type of application information produces a profile of bidirectional communications that will help with readiness planning for network type, size, and location required in the target cloud hosting environment.

Dependencies – The front-end and back-end dependencies for a given application offer additional profile context for run-time behavior. Old-fashioned applications were often monolithic, with all data structures, records, and other controls embedded in the code. Today, however, virtually all applications exist in a complex ecosystem of databases, web frontends, security systems, and other components.

As a result, to understand how an application behaves, one must characterize its dependencies. This will include any dependencies on other modules such as back-end databases, as well as any external modules that depend on the application being hosted into cloud. In most cases, these two dependency relations are sufficiently complex to require a graph. As one would expect, such graphs are helpful to any cloud readiness assessment.

Credentials – Perhaps the most important type of telemetry from a security perspective, and certainly an important piece of information for cloud readiness assessment involves the determination of credentials for both front and back-end access. This will include normal access by authorized users, systems, and devices, as well as privileged access by users and administrators with special roles.

One of the most difficult aspects of operating a modern cloud-hosted application involves the management of these credentials, with their associated secrets, proof factors, and entitlements. A new branch of computing security called cloud infrastructure entitlement management (CIEM) has emerged to address this challenge. Cloud readiness will necessarily require attention to CIEM configuration and support.

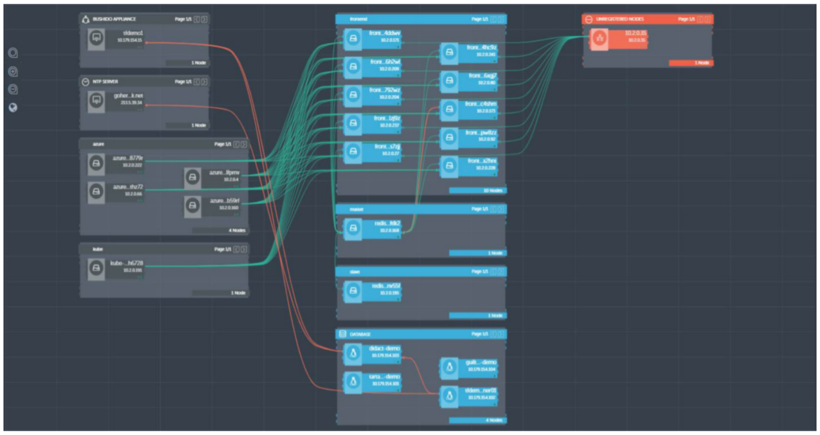

FIGURE 2. Sample View of Behavioral Analysis of Applications Using Fortress

These three types of telemetry can be used to develop more accurate functional requirements for the application and its target cloud execution environment. By collecting this telemetry, subsequent application test activity will be reduced, and the DevOps process should be eased. In essence, the interface requirements for the application will be made clear, which is an important aspect of establishing cloud readiness.

FORTRESS CLOUD MIGRATION SUPPORT METHODOLOGY

The process of establishing behavioral application dependency to support cloud migration can be represented as a simple, step-by-step methodology. Enterprise teams can follow this methodical approach to help reduce application migration risk and to simplify the process of getting newly cloud-hosted applications up and running smoothly. For existing legacy applications targeted for public cloud, the following steps are recommended:

STEP 1: ESTABLISH VISIBILITY

Deep visibility can be established either with the TrueFort agent or through a mix of agents, including the popular CrowdStrike Falcon agent. The goal in this step is to identify application dependencies in legacy, hybrid, and public cloud environments. It should cover workloads that are scattered across virtual machines, containers such as Docker, orchestration such as Kubernetes, and bare metal.

STEP 2: SAFE MIGRATION TO CLOUD

Migration to the cloud will necessarily follow the local planning, transition, hosting, testing, and administration procedures established by the Information Technology (IT), security, and cloud teams. Consultants and even large organizations are also in the business of helping with safe migration to the cloud, often providing key documentation, report templates, and guidance throughout the process, whether for AWS, Azure, GCP, or some other cloud system.

STEP 3: CONTINUOUS MONITORING

Once an organization has safely migrated one or more applications to the cloud, continuous visibility will be required. Dependencies on connections to legacy data centers, for example, should be continuously monitored to identify any decommissioning requirements. Cyber security is also a major issue, and continuous monitoring will be required to avoid serious threats. TrueFort integrates other cloud security solutions such as application environment protection such as file integrity monitoring, application hardening, and microsegmentation.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

The material in this report is comprised of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.

ABOUT TRUEFORT

TrueFort brings zero trust protection to critical business applications. Leveraging unique real-time, adaptive trust, and cloud-to-ground capabilities, TrueFort's Fortress platform detects and contains security threats before they become business risks. For more information, visit truefort.com and follow us on Twitter and LinkedIn.

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM