

ESG SHOWCASE

Application Intelligence Goes Bionic

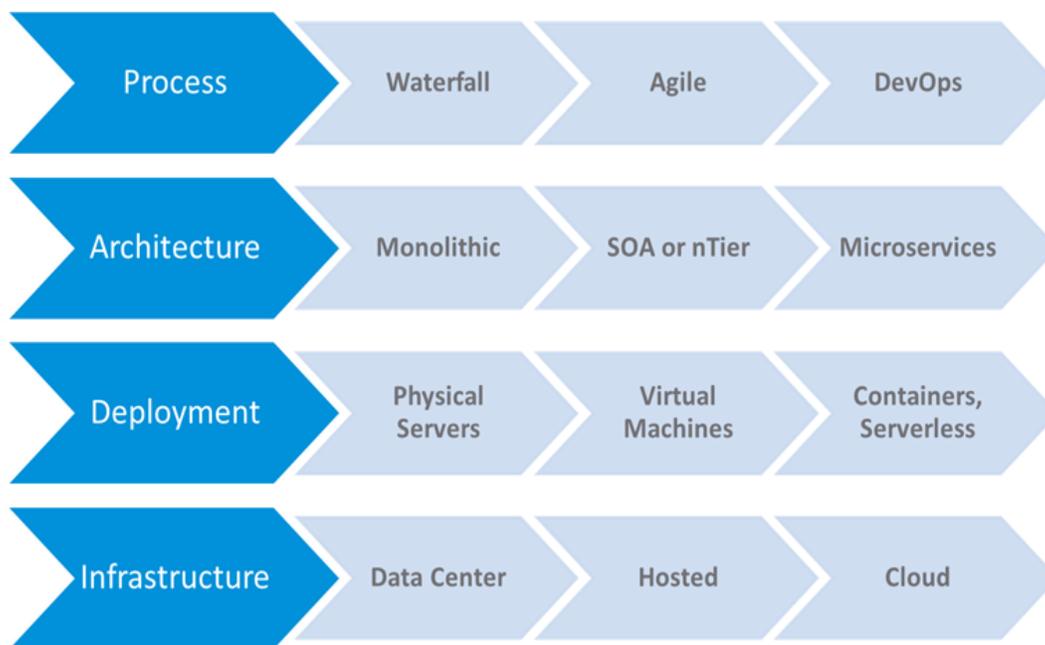
Date: December 2020 **Author:** Bob Laliberte, Sr. Analyst; and Leah Matuson, Research Analyst

ABSTRACT: Application architectures are rapidly transforming. Developers leveraging microservices architectures and DevOps methodologies are capable of deploying new code into production at an extremely high velocity. Yet IT, operations, and security teams are hard pressed to keep up with this ephemeral, chaotic pace. Organizations require innovative new tools to help them regain control and ensure proper governance.

Evolution to Modern Application Environments

Digital transformation initiatives are driving change across enterprises. ESG research tracks the maturity of digital transformation and highlights that 19% of those surveyed report having mature digital transformation initiatives, and another 57% report that their transformation initiatives are in process or just beginning. The top goals reported by organizations for adopting these initiatives are to drive greater operational efficiencies and deliver differentiated customer experience.¹ It is also important to remember that this transformation includes people, process, and technology. A great example of this transformation is the rapid evolution of application architectures and development methodologies to enable greater agility and accelerate time to market. Figure 1 illustrates the evolution of application architectures, development processes, deployment models, and supporting infrastructure.

Figure 1. Evolution of Modern Applications



Source: Enterprise Strategy Group

¹ Source: ESG Research Report, [2020 Technology Spending Intentions Survey](#), February 2020.

This ESG Showcase was commissioned by Bionic and is distributed under license from ESG.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

There is a direct relationship between digital transformation maturity and the use of modern application architectures and methodologies. ESG research indicates that organizations with mature digital transformation initiatives are more than twice as likely (50% versus 22%) to use microservices architectures, and more than four times as likely (66% versus 14%) to use DevOps extensively, than those just beginning.²

These modern application environments must be able to meet the goal of quickly bringing new applications and services to market. Again, ESG research validates this claim, showing that the majority (86%) of organizations are under pressure to deliver new products and services faster.³

As a result of this evolution, a number of organizations currently employ a mix of all three application types and associated infrastructure and methodologies distributed across on-premises data centers, public clouds, and edge locations.

Modern Environments Create Complexity and Challenges

While these new application environments are great for developers, they can create significant challenges for IT, operations, and security teams. Distributing applications across data centers, public clouds, and edge locations creates significant complexity, and makes effectively monitoring these environments difficult. In fact, two-thirds of organizations surveyed reported that their environment is either more complex or significantly more complex than it was two years ago. Furthermore, those organizations with mature digital initiatives are three times more likely to cite significantly more complex environments than those organizations that have not started the process (29% versus 9%).⁴

Complexity is dangerous for organizations because it can lead to gaps in visibility, especially in highly distributed environments. Adding to this complexity is the fact that modern application environments are designed to change rapidly. This brings up the question of how IT, operations, and security can keep pace with developers who have the ability to drop new code in increasingly shorter timeframes. Unlike the waterfall, and even the agile methodologies that preceded it, DevOps was created specifically for rapid iterations and the ability to quickly deploy new code. Leveraging microservices architectures enables developers to drive even faster deployment time, making it virtually impossible for operations teams to track every change.

Another challenge facing organizations, especially organizations that are not digital natives (digital natives are defined as organizations that are less than 10 years old), is contending with multiple, different application architectures. IT, operations, and security teams will struggle to properly monitor and manage these environments.

Lack of visibility across distributed environments will also create a myriad of problems. For example, ESG research indicates that modern applications will be deployed in a combination of public clouds and private data centers (hybrid cloud environments) (70%), and that managing these applications across multiple disparate public clouds was important or very important (88%).⁵ Additionally, many organizations are rolling out applications to the edge to accommodate the need for real-time analytics. Consequently, organizations will struggle to access holistic views of these highly distributed application environments.

Current or legacy methods to obtain information on applications are inadequate. These methods, such as network performance tools or configuration management databases (CMDBs) designed for previous application environments, struggle to provide relevant information. In many cases, organizations may require a manual process document to understand the environment and when changes were made. Even then, documentation may be poor or non-existent. It's

² Source: ESG Master Survey Results, [Trends in Modern Application Environments](#), December 2019.

³ Ibid

⁴ Source: ESG Research Report, [2020 Technology Spending Intentions Survey](#), February 2020.

⁵ Source: ESG Master Survey Results, [Trends in Modern Application Environments](#), December 2019.

no surprise that these current or legacy methods are not only time-consuming, but prone to human error. And with the accelerated rate of change, virtually any manual document is obsolete the moment it is completed.

The inability to ensure architectural governance is also a concern in these dynamic environments. If IT, operations, and security teams are unable to track changes in real time, it will be impossible for operations teams to ensure appropriate levels of availability, application architecture integrity, security, and compliance. In addition, modern applications can create issues similar to those where organizations confronted with the rapid growth of shadow IT and the public cloud were required to repatriate applications due to a lack of guardrails.

Considering that one of the top goals of digital transformation is to drive greater operational efficiencies, it is imperative that organizations think about how they are going to effectively regain control, manage, and secure these highly dynamic, distributed, and diverse application environments.

A Modern, Intelligent Approach to Application Management

The key to ensuring control in modern application environments is working smarter, not harder. As applications become more distributed and rely on microservices that can be updated virtually all the time, organizations need to apply a layer of intelligence to effectively map out and inventory these applications to fully understand where they are deployed and how the data flows, as well as API usage, devices, and dependencies. While organizations can do this now using spreadsheets and Visio diagrams, or information from existing network and application management tools, the key is to create an intelligent platform providing a single, unified view that automatically updates with any changes. In addition to modern applications, this technology should also be applied to legacy service-oriented architecture (SOA) and monolithic applications to provide a holistic view of all applications. This intelligence will also enable organizations to obtain near-instant answers to queries, provide proactive alerting, and even more importantly, establish the appropriate guardrails and controls to ensure developers can deploy new code to both development and production environments without fear of creating an issue.

The Bionic Application Intelligence Platform

Fortunately for organizations frustrated with the challenges of managing rapidly evolving application architectures and distributed application environments, there is good news. Bionic recently emerged from stealth with an innovative solution that enables organizations to regain control of chaotic application environments using its Application Intelligence Platform.

The Application intelligence Platform aims to dramatically reduce the complexity associated with managing all application environments. Specifically, the platform delivers:

- **Comprehensive Inventory.** Utilizing agentless deployment strategy, the platform is able to quickly get a holistic inventory of an organization's applications (monolithic, SOA, and microservices). This includes specific information about where each application is deployed (data center, cloud, or edge), how it is deployed, how it is configured, and the APIs being used, as well as all data sources. This inventory also includes real-time tracking of all changes to the environment.
- **Application Dependency Map.** The platform is able to translate the inventory data to create a full application dependency and dataflow map of both the development and production environments. Key capabilities include the ability to show how different services leverage APIs, and report on the data that is flowing between any applicable services, data sources, or messaging queues.

- **Querying and Reporting.** By leveraging the information collected and continually updated to serve as a single source of truth for the application environment, organizations can obtain immediate or near-real time answers for any questions related to changes in their applications. The platform enables IT, operations, and security teams to build custom queries and reports to support operations, with the ability to monitor and report on any critical changes to the environment that may impact the resiliency, security posture, or compliance of the applications.
- **Policy Enforcement and Alerting.** Organizations can create policies and set alerts for any violations. This includes the ability to integrate with CI/CD pipelines to ensure that developers have the appropriate guardrails to freely operate and ensure appropriate architectural policies.

These capabilities deliver on the three key pillars that the Application Intelligence Platform provides to organizations. The Application Intelligence Platform enables better visibility, understanding, and control of highly distributed and dynamic application environments—while still enabling developers to work at an accelerated pace.

The first pillar is the ability to validate and enforce any architectural policies. By leveraging alerts, queries, and developer guardrails and integrating with the CI/CD pipeline, IT, operations, and security can ensure compliance without slowing down developers. The key to enabling this is the second pillar—the ability for IT, operations, and security to leverage a single source of truth to better understand applications and their interdependencies, with the ability to quickly query their inner workings. The third and last pillar is important for day-two operations. It is the ability to monitor critical changes across a highly complex, dynamic, and diverse application environment. This isn't about alerting on every change, but rather leveraging intelligence (holistic visibility and policies) to only alert teams about critical changes that require attention or action.

The Bigger Truth

Organizations are rapidly transforming their application environments as part of more comprehensive digital transformation efforts with the goals of becoming more agile and operationally efficient, and more quickly delivering better customer experiences.

However, because these modern application environments are highly distributed and dynamic, it can be difficult to effectively manage these complex environments without the appropriate visibility. IT, operations, and security teams need innovative solutions that don't impede developers, yet still ensure proper governance and policy enforcement. The key to delivering these capabilities is to incorporate solutions that enable organizations to work smarter and more efficiently, providing real-time control and tighter alignment between developers and operations.

Bionic's Application Intelligence Platform is agentless and simple to use, yet capable of providing holistic visibility and a layer of intelligence to any application architecture, deployed across any location. Providing real-time or near-real-time alerting, reporting, and queries will dramatically improve operational efficiency for IT, operations, and security teams, while tighter alignment with developers and the CI/CD process will ensure new applications and services can roll out faster with less risk, knowing the appropriate guardrails are in place.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.