Solution Brief

Protecting your Continuous Integration and Deployment Pipeline

Challenge

We are in the early stages of the Fourth Industrial Revolution—the App Economy. In its scale, scope and complexity, this revolution is unlike anything we have previously experienced. The app economy is global, responsive, customer-focused, and technology-driven—with software and data at the center of it all. Deriving value from data is the goal of the digital revolution, but monetization of this data requires continually evolving in today's digital landscape.

Opportunity

Software is the key driver of growth, innovation, efficiency and productivity, but how you deliver it says a lot about how you'll be able to compete in this world. Business leaders have recognized this new reality, with most investing in the technologies and adopting the processes required to transform and embrace the app economy. But as new apps and services are rushed to market, security is left as an afterthought or ignored completely, creating new targets for hackers to compromise and exploit.

Benefits

Organizations that seamlessly integrate security within their continuous integration and deployment (CI/CD) pipeline will reap the rewards that the application economy offers while minimizing their risk. We recognize these emerging challenges and offer the broadest set of solutions to implement Secure DevOps. Our Symantec solutions combine security with powerful AI and automation to create a unified platform that enables and protects the entire CI/CD pipeline.

Pipelines are at the heart of DevOps, but simple continuous delivery pipelines are not enough anymore. You need both intelligent and secure pipelines to help you release higher quality software at a greater velocity and reduced risk.

Background

The primary challenge for most organizations revolves around replacing traditional software application development and delivery processes, which are too slow to meet evolving customer expectations. These concerns have given rise to new business and software delivery models, namely Agile and DevOps.

At its most fundamental level, DevOps seeks to engage Agile methodologies to increase the speed and quality at which innovation can be introduced to applications. In doing so, organizations can realize many significant benefits. However, despite these benefits, many IT executives and business leaders are expressing concerns over cyber security and are worried that in their rush to market, they are exposing their organizations to significant security risks.

For many, the solution is simply to introduce code scanning into the DevOps process to check for known vulnerabilities, but this only addresses one potential attack vector; there are more. We have identified three others that organizations should consider:

- How do you ensure that appropriate levels of security are being built into the app without impacting developer velocity?
- How are you protecting the DevOps tool chain and processes, which are being given elevated access privileges that can be easily exploited?
- How are you governing user access to your overall development environment and ensuring a "least privileged" posture?

Symantec, A Division of Broadcom, is changing the game. We are bringing security and connectivity together with powerful AI and automation to create a unified platform that easily embeds security into your mobile apps and IoT devices, safeguards DevOps access to privileged credentials and accounts, and monitors user access to sensitive development environments, tools, and source code. Additionally, we also deliver intelligent DevOps end-to-end, automated software development, and software release capabilities to provide full lifecycle management of your applications and APIs. Combined, Symantec is one of the only vendors to offer a comprehensive Secure DevOps solution.

Our Approach

Extraordinary experiences and exceptional functionality are what customers demand. To keep pace with competitors, DevOps and Agile have emerged as the mainstream methodologies to increase speed to market for new applications. Agile helps build the right products and features while delivering them with predictability and quality and DevOps drives collaboration between your software development and IT operations teams to accelerate software development and delivery.

Symantec delivers intelligent DevOps end-to-end, automated software development capabilities that enhance your current toolchains to provide full lifecycle management of your applications and APIs by ensuring application security, and application scalability and continuous delivery across on-premises, hybrid cloud and mainframe environments.

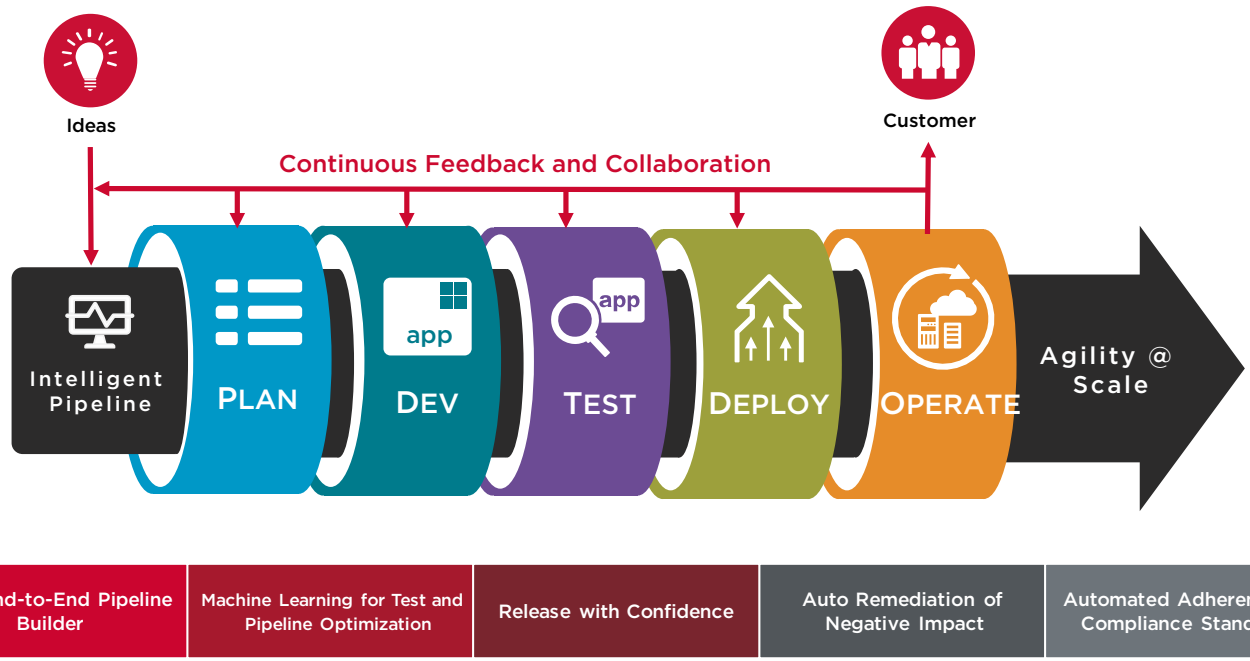
As you can see, we believe that security runs through the entire DevOps process to ensure that organizations can achieve agility at scale without sacrificing security.

Plan: Shifting Left with Security in Mind

Our products include world-class solutions to help apply Agile methodology to your enterprise and to manage your projects to maximize your investments. However, for many organizations, security is not integrated into the DevOps lifecycle; it is tacked on to the app as an afterthought. This is not efficient. Security could and should be woven into this part of the DevOps process. As your teams build their plans and schedules for multiple app releases, you can ensure that specific security aspects are captured and addressed. For example, who will be accessing and using the application, what data will be accessed or transmitted through the app, how will you authenticate users, will all users have the same level of access, what APIs will be exposed or used by the app, and so on.

Within the DevOps environment, we provide a platform that allows developers to easily embed consistent and adequate security without impacting delivery timelines. This aids in the planning phase as the inclusion of specific security features and capabilities leverages a proven, repeatable, and scalable platform.

Intelligent Pipelines in a Secure DevOps World



Develop: Improving Security with Increased Developer Velocity

Mobile apps are undoubtedly the current wave in the evolution for businesses and government agencies to interact with users, but the next wave is here—the Internet of Things. Smart devices are becoming more prominent in our lives, from phones to watches, from refrigerators and cars to medical implants and industrial machinery. Mobile apps and IoT devices both have connectivity, which means that they are interfacing with your back-end systems, services, and data. Because they both have connectivity, not only can they be hacked, but they are already being compromised where security is inadequate or non-existent. This issue introduces two challenges to the organization: how do I secure the mobile app and IoT device itself, and then how do I create and secure the APIs that are going to be used by mobile apps and IoT devices to communicate with my organization?

Symantec Access Management addresses the first challenge through a universal SDK that can be embedded into the mobile app or IoT device. On the mobile device, the SDK supports OAuth and OpenID for social login and single sign-on, an embedded PKI credential for 2FA, OTP generator for transaction signing, and data collectors for device fingerprinting and risk analysis. On the IoT device, the SDK supports certificate pinning, secure data storage, and secure communications. This allows developers to quickly embed robust security into mobile apps and IoT devices without being security experts and enables security teams to configure security features externally without requiring coding changes.

The second challenge is addressed through a component called Symantec Live API Creator, which can almost instantly generate scalable enterprise-grade APIs that provide secure, reliable access to SOA, ESB, databases, applications, and the mainframe. This component reduces development time and cost as developers can quickly create the services needed to bring together data to use in modern apps and devices.

Test and Deploy: Automating CI/CD with Enhanced Privileged Access Security

Privileged accounts have elevated access to your most valuable assets. As such, they are the most likely to be exploited by external hackers or insider threats. But privileged accounts are not just accessed by real people. Numerous applications are also given privileged access to sensitive resources and data by embedding associated credentials into automation scripts or by using a run-time configuration file. This is especially true in more sophisticated IT shops where CI/CD practices are introducing automated processes that see no human intervention at all. These automation tools often leverage hard-coded administrative credentials that are ripe for theft and misuse, often with little to no security protecting them at all.

Symantec Privileged Access Management addresses this challenge through an Application-to-Application Password Management (AAPM) component. AAPM enables you to eliminate hard-coded, hard-to-change passwords from applications and scripts, providing effective protection and management for these keys to the kingdom. Integrating security within the DevOps toolchain allows privileged account passwords, keys, tokens and other credentials to be stored in an encrypted vault, protecting them from theft or prying eyes.

Additionally, when testing and developing software, sensitive customer data can end up spread across test and development as well as complex environments. Testers might copy data to their environment for a given use, but organizations must know how long the data is used for, and that it's used with consent and for a legitimate purpose. Our continuous testing platform can help with this key point of compliance by identifying exactly where sensitive data is stored enterprise-wide, and by using statistical analysis to find personal data stored across multiple file formats and applications. Using a cubed view to create an accurate picture of data, our solution identifies sensitive information reflected in related systems, components or applications. Custom, mathematically based filters mean that data can be filtered on a granular level to identify every instance of information relating to an individual. This data can include credit card numbers, email addresses, home addresses and the like, helping organizations fulfill the right to data portability. The data discovery is fully auditable, so that organizations can demonstrate the application of controls taken for compliance.

Operate: Creating a Triangle of Trust to Improve Customer Experience

The paradigm shift from Web, to mobile and IoT has resulted in significantly more convenience for end users, but it has also created enormous challenges for those tasked with keeping the network and data secure. These new interfaces have conspired to make your existing security perimeter ineffective. Chief among these concerns is authentication—how confident are you that a legitimate account holder is trying to access sensitive data?

Symantec addresses this challenge through a next generation access control solution, which leverages the universal SDK to uniquely identify users, apps and devices to establish a triangle of trust, and patented enhanced session assurance that leverages risk analytics to prevent session hijacking. This trust relationship makes it easy for customers to access their accounts, and gives businesses greater assurance that the access is by a legitimate user. It increases the efficiency of app development teams, all while providing a secure environment for the enterprise that protects its customers.

DevOps: Governing Access to Your Development Environments

Cybercrime continues to rise and not all attacks are focused on data; hackers are looking to steal source code too. Throughout the entire DevOps environment, there are still many human actors who have access to source code, and hackers will attempt to compromise these accounts. This requires ongoing management and review for these users and their access to the development environments and tools.

This component ensures that all access to development systems, infrastructure, and data is routinely reviewed and certified to ensure that the access is both required and appropriate. It applies access governance to every individual and shared account that has access to source code or other sensitive processes and data. This enables the security team to continuously monitor, review, and certify developer access, and automatically revoke that access when it is no longer necessary. As a major software developer, Symantec performed these security audits on its own internal development organization to protect our source code from unauthorized access. After we added Symantec Identity Management to review and certify access to our own development organization and CI/CD processes, we saved over 5,000 hours of manual effort.

Summary

To guard against external hackers gaining access to your DevOps environment, Symantec solutions provide end-to-end AI-driven security that connects unlimited users, devices, and IoT to back-end data and services, protects and monitors this access and usage from mobile to mainframe, and provides a non-repudiated audit trail. Employing a zero-trust model with a defense-in-depth approach to security that includes privileged access control offers your organization the best chance of protection against ever-evolving threats.

For more information, please visit broadcom.com/symantec-iam

SED-DevOps-SB101 February 7, 2020