The Changing Face of Security in the Era of AI, Cloud, Agile, and DevOps

Abstract

Widespread digital transformation is altering the security needs of organizations across industries as cloud computing becomes omnipresent, and agile and DevOps become the new norm for application delivery. As application deployments become faster than before, integrating security into agile development methodologies is emerging as a critical imperative to ensure that shippable products are security compliant.

This means security considerations for implementing complex artificial intelligence (AI), machine learning (ML) and other next-gen technology based solutions must be incorporated early in the application lifecycle to create and sustain brand value in the market. The paper presents methodologies, processes, and tools that enable organizations to roll out security certified shippable products in the era of AI, ML, and cloud.

Security is Integral to Brand Value

AI, ML, deep learning (DL), cloud, microservice architecture, and agile DevOps are collectively ushering in massive disruption in various sectors such as health care, banking and financial services, and others (see Figure 1). The result: human-machine collaboration-led Industry 4.0 era. To successfully transform themselves, drive innovation and agility, and compete profitably in this new era, enterprises must embrace continuous digital evolution, without compromising security.

As intelligent applications become mainstream and data moves from the boundaries of one system to another, maintaining security compliance becomes key to the success of these applications. Much like in the case of DevOps and continuous deployment, embracing a process that is simple, streamlined, focuses on ownership and accountability is ideal for ensuring security. Additionally, integrating cloud security solutions through open APIs into DevOps and continuous integration workflows will help drive a simple and streamlined process.

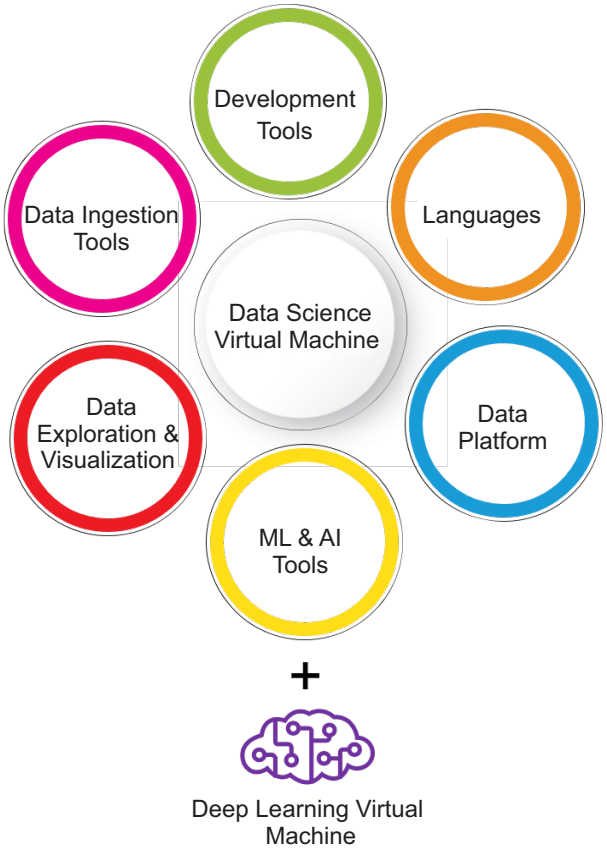

Figure 1: Ecosystem of emerging technologies

Securing Applications in the New Ecosystem: The Challenges

Leveraging new-age applications driven by AI, ML, and DL do pose some challenges such as:

1. Dealing with a combination of old and new systems, tools, and frameworks, in addition to different types of functions like data processing, data ingestion, integration, modeling, and deployment.
2. Coordinating with a new set of stakeholders – data scientists, domain experts, software engineers, and others - who may not have a holistic understanding of security or have information on the history of security issues identified for an application in the past.
3. Integrating newly designed applications and systems with multiple existing systems from different domains and geographies.

Most importantly, new-age applications pose the critical challenge of ensuring security compliance, which typically requires time to evolve for any new technology. Securing an application therefore requires an understanding of the assets of the technology. The assets that need to be protected in the case of AI and ML systems include features, weights, model hyper parameters, hardware used for computation, and so on.

Similarly, the DevOps microservice based approach which is popular with most organizations today, comes with unique security challenges:

1. When bigger architecture is divided into smaller services, the attack surface also increases, making it hard to track all services.
2. User access privilege and authentication to different services is difficult because of the perimeter of multiple services.

Baking Security into Next-gen Technology Applications: 10 Best Practices

In their haste to adopt microservice architecture, to reap the benefits of faster deployment speeds and independence of services, most organizations neglect security – a critical component that must be built into the product. Here are ten best practices to follow in order to bake security right into the product core:

1. Focus on stakeholder awareness: Even if multiple stakeholders are involved in application delivery, organizations must ensure they have uniform knowledge about security concepts such as data classification, data protection, threat modeling, and more.
2. Create a robust data governance structure: This ensures that ownership and accountability are clearly articulated to various stakeholders. This is especially true for AI, ML, and DL projects as they involve the transfer of large amounts of data at every stage - from one system to another.
3. Conduct threat modeling: Rigorous threat modeling - both at the component level and the solution level – is a must. This will ensure that security is part of design, ensuring that requirements such as valuable data processing, data transfer, data storage, and authentication requirement are implemented. Further, all threats generated during threat modeling must be addressed on a priority basis. In AI, ML, and DL projects, production data is used everywhere; making it critical to ensure that all workflows are covered in the threat model.
4. Adopt good programming practices: This helps mitigate vulnerabilities like cross-site scripting, cross-site request forgery, SQL injection, and others.
5. Thoroughly analyze software components: Given the fact that multiple stakeholders and integrations are typically involved in large ecosystems, thorough analysis of software components ensures nothing slips through the cracks at any stage of the project.
6. Focus on the quality of security: Verified and signed components must be used wherever possible. In case this option is not available, consider other factors such as developer reputation, extent of use, trustworthiness of the repository, comments and reviews, and history of security issues or vulnerabilities. This helps ascertain the component's security quality.
7. Think security from the get-go: Most application teams consider security as a last step and work on the feature developments first. With current agile and DevOps methodologies, the product must accommodate all the security considerations in production environment. Here's how.

In an agile delivery methodology (security model illustrated in Figure 2), individual tasks can be created for each point listed below whereas for DevOps implementation (security model illustrated in Figure 3) they can be plugged into the CICD pipeline.

a) Static code analysis must be part of CICD implementation.

b) The code must be scanned for sensitive information like passwords and connection strings, in which case a plugin that facilitates such scanning must also be part of the CICD pipeline.

c) The tool to check whether the solution is using the latest frameworks and dependencies must be plugged into the CICD pipeline so that the biggest risk of using vulnerable libraries, frameworks, dependencies is eliminated automatically – for instance, OWASP dependency checker.

d) Dynamic web scanning must be performed on the solution prior to production release.

e) If an application uses cloud resources, then cloud services and cloud subscription must be scanned for enterprise level accepted security control compliance.

f) In case applications use Microsoft Azure, deployment security can be combined with CICD pipeline to check ARM templates.

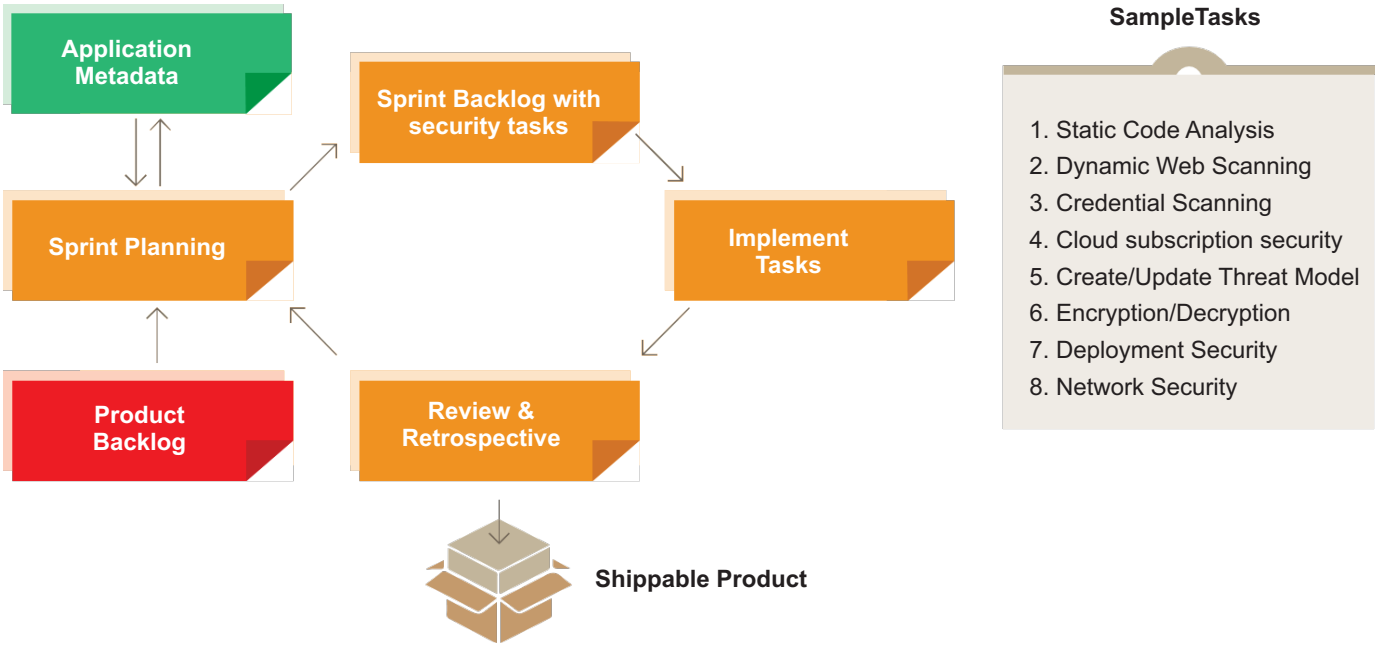

Figure 2: Agile Methodology Security Model

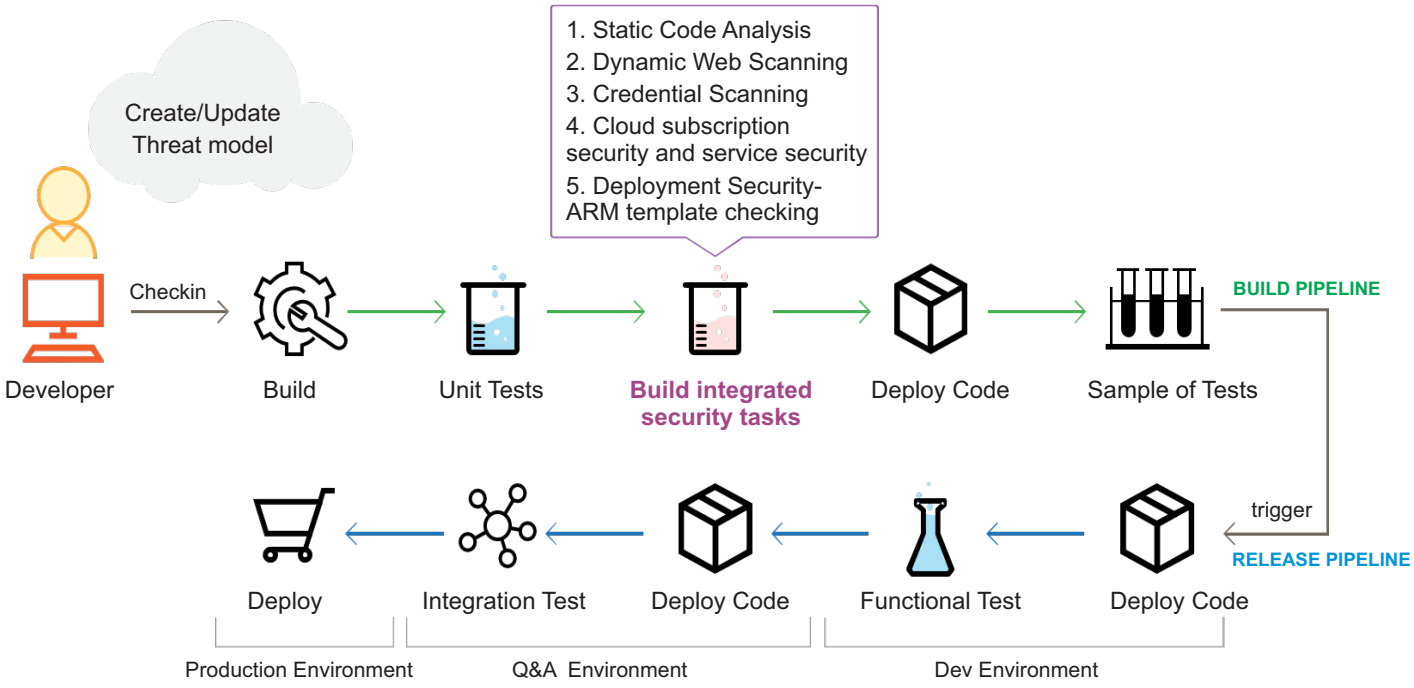

Figure 3: DevOps Security Model

g) For Devops with microservice architecture model, an in-depth approach must be adopted with layered defense elements including network security, data integrity, behavioral analysis, and so on.

The defects arising from the aforementioned tools and processes can be tracked using a reporting interface to help application and leadership teams monitor security compliance.

8. Focus on monitoring and security hygiene: It's important to ensure periodic access reviews and rotation of keys and certificates.
9. Create a reliable business continuity plan: A comprehensive disaster recovery (DR) plan helps drive rapid incident response to avoid unscheduled downtime in case of cyberattacks or natural calamities.
10. Adopt a 'Protect from Inside' approach: In most cases, the internal environment of organizations plays an important role in enabling security policies like employee training, data retention, email security, data access and access control policies, and device management.

In addition to the above basic security tasks, manual security design review, manual security code review, network security reviews, and penetration testing assessment should be performed for applications annually or bi-annually as required.

Adopting a Security-First Mindset for Success

The global cybersecurity market is expected to grow to USD 170 billion by 2020.[1] Even as organizations attempt to ensure optimum security compliance, designing security into the core of the product remains a challenge. Even though AI and ML enable better data security and faster threat detection, merely integrating ML security features into applications is not likely to ensure fool-proof security.

Architects must design the application with a security-first mindset that begins with embedding security at each stage, even as they develop the code, rather than fitting it in as an afterthought at the last stage. Because security is not a product but a continuous process, organizations that adopt a security mindset - both from the perspective of understanding emerging threats and the types of solutions available - will emerge as clear winners.

References

[1]Cybersecurity Ventures, 2018 Cybersecurity Market Report (June 2018), accessed May 20, 2019, https://cybersecurityventures.com/cybersecurity-market-report/

About The Authors

Mahesh Pachbhai

Mahesh Pachbhai is a cyber security evangelist with TCS' HiTech business unit. In his current role, he provides cyber security consultation and advisory to TCS' clients across the globe. Mahesh is a Microsoft certified solution expert: cloud platform and infrastructure. He holds a Bachelor's degree in Technology (Electronics and Telecommunication) from Shri Guru Gobind Singhji Institute of Engineering and Technology, Maharashtra, India.

Sriram V

Sriram V is a cyber security architect with TCS' HiTech business unit. With more than 12 years of experience, he specializes in the security domain and is responsible for assuring security compliance for multiple projects for leading clients. Sriram holds a Bachelor's degree in Engineering (Computer Science) from PT. Ravishankar Shukla University, Chhattisgarh, India.

Contact

Visit the HiTech page on www.tcs.com

Email: HiTech.Marketing@tcs.com

Blog: HiTech Bytes

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services I M I 06 I 19