IDC Vendor Spotlight

Sponsored by **Kiuwan**

Author: Emilio Castellote

2018 May

Digital Security Challenges from design to deployment.

The new digital era is transforming not only the way companies are managing their relationship with actual customers but also is transforming the way we deliver services and applications.

These new digital services and applications are changing the traditional productions processes, and security is becoming a key area along the whole process beyond design, development, deployment and maintenance. Security is transforming from a simple patch the deployment layer towards a foundational part of any digital service or applications covering the whole process from design to maintenance.

New figures like the DevSecOps whose purpose and intent is to build on the mindset that "everyone is responsible for security"

This is the main reason why SDLC (Secure Development Life Cycle) is covering a wider range of features and responsibilities generating new figures like the DevSecOps, whose purpose and intent is to build on the mindset that "everyone is responsible for security" with the goal of safely distributing security decisions at speed and scale to those who hold the highest level of context without sacrificing the safety required.

Along this paper we will try to understand the impact of Digital Transformation in the companies, the society and the new applications developed to serve the new digital necessities with the highest security level. A new security level in development where the SDLC should be interiorized by design and where the detection and protection against the software vulnerabilities may be a first step to accomplish security from design to deployment.

Transforming digital development processes

Digital transformation (DX) is real, and it begins with applications that are built to deliver a truly digital native experience. However, things are never simple, since for all organizations except for new startups, existing applications running on existing infrastructure using existing development and life-cycle approaches are the lifeblood of today's business, and a boat anchor to the past. Somehow, organizations need to modernize these applications without disrupting their current functionality while also building brand-new applications that are digital native/cloud native from day one, drawing a parallel to the analogy of replacing airplane engines while the plane is in flight.

The challenges are numerous and include the need to overhaul organizational structures so that agile development and DevOps-centric operational models can be embraced while shifting deployments from on-premises infrastructure to a mix of on-premises and off-premises deployments and avoiding the time-saving shortcuts of embracing proprietary cloud services to focus on longer-term goals.

Security and Vulnerability Management market in US will overcome 20Bn$ accumulated between 2018-2021

In parallel, security and vulnerability management market is driven by an ever-changing threat landscape, increased organizational demands around security across all verticals, increasing pushes toward operational efficiency by enterprises, and the desire for more formalization around risk management initiatives. Over the past several years, many organizations have worked through significant upgrade cycles of their infrastructure security products to be another logical area for organizations to evaluate as part of continued improved efficiencies.

Security and Vulnerability Management market in US will overcome 20Bn$ accumulated between 2018-2021 (Fig1.), representing the second major sector in Security Software.

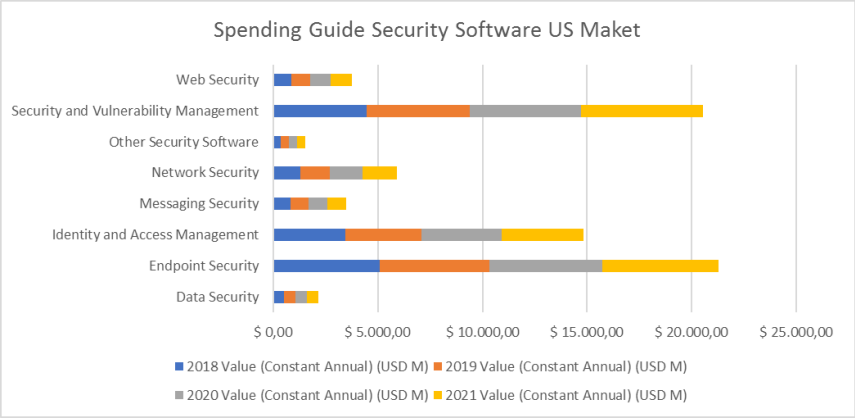

Figure 1. Spending Guide Security Software US Market 2018-2021

Improving security life cycle

Along the new digital era, new challenges arise to leverage security before any other process at the development cycle. The SDLC (secure development life cycle) procedures will have to embed security from the very designing phase of any new digital service or application, apart from considering the following development improvements:

- **Intelligent enablement:** cognitive, machine learning, deep learning, bots, and related technologies, will quickly become table stakes for development environments. Organizations will find themselves making development and deployment decisions to embrace still-maturing cognitive services often hosted in cloud as PaaS features. Separating the best ones from those that will not survive or thrive will be key.
- **Packaging and deployment:** the notion of building an application and deploying it into a known infrastructure that an organization internally controls quickly goes away, forcing developers to embrace more standardized packaging vehicles such as containers and function-based computing deployment environments.
- **New programming models and languages:** a renewed interest in low-code and no code development, and online integrated development environments are becoming attractive alternatives to traditional local code development.

Security-Led Development Will Be a Priority for 90% of Orgs by 2020

IDC predicts that, "Development Without Integrated Security and Compliance Will Fail; Progressive Orgs Have Prioritized Security Due to Uptime and Compliance Concerns, Accelerating the Need for Agility and a Curated OSS–Dev Portfolio; **Security-Led Development Will Be a Priority for 90% of Orgs by 2020**, where Stricter privacy regulations will make governance and compliance an up-front mandate for application developers and DevOps teams".

The assumption is clear, the new development process will have to embed security from the design phase, and vulnerability assessment tools will become a necessity within the new development life cycle.

Security by design

Vulnerability assessment market will have a growth of 23,9% (CAGR) in the coming 3 years until 2021 at the US market

Vulnerability assessment market will have a growth of 23,9% (CAGR) in the coming 3 years until 2021 at the US market, again highlighting the desire that organizations must scan their infrastructures and applications for vulnerabilities to obtain baseline and prioritization information. Device assessment with a growth of 12.8% and software assessment with a growth of 11,1% will be the main areas within the security and vulnerability management technology market.

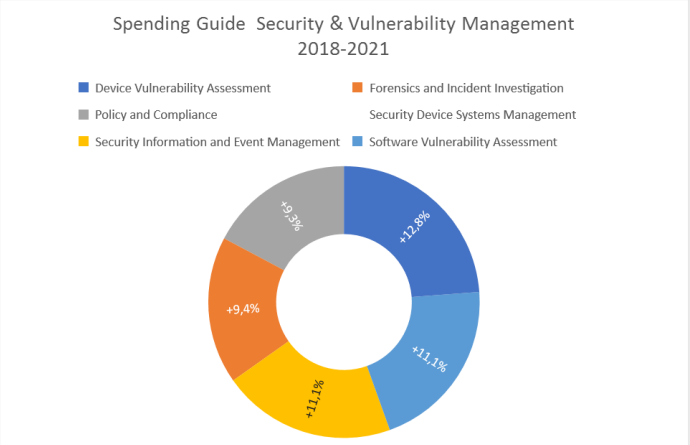

Figure 2.- Spending Guide Security & Vulnerability Management US Market 2018-2021(GAGR)

Security Integration from Development Through Deployment will be a responsibility for fixing vulnerabilities in critical systems all on the developers as well

Security Integration from Development Through Deployment will be a responsibility for fixing vulnerabilities in critical systems all on the developers as well. The popularity of agile development and continual updates drive a need for continual vulnerability management from development through deployment. Security and vulnerability management (SVM) vendors can help manage and secure the increasingly continuous development and deployment models that are quickly becoming the norm. As integration improves between code development and patching, the ability for organizations to stop vulnerabilities before they enter production environments will drive cost savings and improve the security of software products.

Compliance, security challenges, the emergence of services, and the need for user experience testing on both mobile and existing web platforms heighten the need for automated software quality (ASQ) tools and SaaS (Software as a Service) as well as emerging cloud and existing virtualization to support and facilitate ASQ adoption and implementation. Cloud testing solutions are emerging increasingly because of adaptability and cost savings (management and security remain user concerns; testing in hybrid, private, and public cloud settings is a strong initial choice for cloud at many organizations). However, cloud adoption is passing through multi-cloud environments where a continuous security testing of the applications must guarantee the security level necessary for both scenarios (cloud & on premise).

Vulnerabilities impact

Historically, organizations have used vulnerability assessment (VA) products and services to scan servers, workstations, other devices and applications to uncover security vulnerabilities or configuration settings that can be exploited. More sophisticated VA products can test for unknown vulnerabilities by mimicking common attack profiles to see whether a device or an application can be penetrated. Penetration testing is a common part of such offerings, allowing to safely exploit vulnerabilities by replicating the kinds of access an intruder could achieve and provide actual paths of attacks that must be eliminated.

VA products also include application scanners, which are specifically designed to test the robustness of an application or software to resist attacks (both specific attacks and attacks based on hacking techniques), and are primarily focused on finding database or web application vulnerabilities. The application scanner market includes products that look at deployed applications (dynamic testing) and products that review source code (static testing). Another commonly used method for detecting security vulnerabilities is through periodic penetration testing and targeted simulated attacks conducted in-house or through specialized security services companies, IT consulting firms, and other third parties.

More recently, cloud-based attack simulation solutions emerged to provide organizations with continuous and more accurate assessment of their security posture. Solutions in this space operate by simulating various types of internal and external attacks, either as an alternative or as a complement to sporadic penetration testing. Focus on automation and infrastructure as code, which delivers environments that stay in sync, can be built on demand, and be documented with version control**.**

Organizations are already shifting from work stream–based interactions to a more holistic approach, indicating that enterprises are starting to realize integrated security benefits. Final security assessment should be a reconciliation effort rather than a complete checkup

Adopting SDLC in development and deployment

A first step within SDLC is to implement any Static Application Security Testing (SAST) solution capable of arising any vulnerability of the code during the development phase before deployment. It´s essential to analyze and detect any possible vulnerability at the code independently from its origin and being ready for latest 3rd platform applications to be held on the cloud. That's the main reason why the SAST solutions should be flexible in terms of code origin and deployment destination.

We are facing the digital era in which all applications will be delivered from the cloud. However, in the midterm a multi-cloud scenario is the option most adopted by companies who think the security of critical information must be kept onsite within their local perimeters. This tendency also applies to software development, where the actual solutions must be ready to manage hybrid

scenarios (on premise – cloud) not only in production phase but also during development and during the whole SDLC where SAST solutions must provide that hybrid compatibility.

by 2021, a Vulnerability Exposed in a Widely Used Open Source OS Will Leave 10% of the World's PaaS/IaaS Cloud Vulnerable to Breach

Secure Development applies to all the development/deployment life cycle that should cover any kind of software applications, including not only commercial applications but also opensource developments. According to IDC 2018 predictions, **by 2021, a Vulnerability Exposed in a Widely Used Open Source OS Will Leave 10% of the World's PaaS/IaaS Cloud Vulnerable to Breach.**

Developers must understand how to control open source components. There are many dependency, security, and license compatibility issues involved with open source solutions that require some consideration before launching any application. Software Composition Analysis (SCA) allows you to identify third-party and open source components that have been integrated into all your applications. It informs you about the licenses for each of them and identifies out-of-date libraries that should be upgraded or patched.

When talking about opensource, we should be aware of the different components and opensource licenses used in the development process. In the same way we manage commercial applications, opensource applications should be analyzed to detect and patch any possible software vulnerability before the deployment phase. An important issue will be to apply any SAST solution available for managing the opensource world as the commercial market.

Value Proposition of Kiuwan

Most enterprises develop customized software to run their business mission critical systems. The lack of an all-encompassing tool that can be used by every stakeholder in the SDLC, brings the need to spend more time and resources on the maintenance of these developments, losing control over their software, which can lead to security exploits, increase of risks and lack of governance over their own application portfolio.

Kiuwan proposes a shift left approach in the SDLC, and champions the change of paradigm that DevSecOps has brought to software development.

Underpinning the idea that everyone is responsible for security, the DevSecOps manifesto aims to make security and compliance available to be consumed as services.

Supporting this idea, **Kiuwan provides an end-to-end Software Security platform, compliant with all the major security standards**. Bringing objective data to make informed decisions regarding the risks associated with security vulnerabilities, with information regarding exploits, propagation paths, software composition analysis for open source components, as well as risk governance of internal development teams and external providers are but a few of the possibilities brought about by Kiuwan.

With support of multiple application technologies, from legacy to mobile, covering over 20 programming languages, Kiuwan proves to be of key importance when companies want to secure their applications from cyber threats, even if they industrialize the Software Development Life Cycle all within the most relevant IT frameworks and standards.

Kiuwan differentiates itself from other approaches to SAST and SCA along two lines: **project management,** including metrics around the application security remediation effort in existing applications, and **clear methods for working with the modern application development team**, which in organizations of a certain scale can typically include an outsourcing arrangement in addition to in house talent. The Local Analyzer can be extended to outsourcing third parties, and code only accepted when it meets internal thresholds for its level of vulnerability, for example no 'Very High' or 'High' risk findings.

Agile development methodologies are common practice everywhere today. The benefits are evident, many of the silos of software development are broken and now analysis, design, coding and testing blend together in an iterative way with a measurable increase in efficiency and time-to-market.

While it has required a considerable cultural change and effort, it is still not enough: Agile have brought together different skill sets and professionals under the same teams, but it does not bridge the gap between these teams and those responsible to deploy and operate the applications. **Another cultural change of gear is necessary: DevSecOps.**

Kiuwan helps DevSecOps in the implementation of a successful Agile development process without Continuous Integration, breeding applications secure from inception.

Breaking the security silo requires a new change of gear in the enterprise that must adapt to bring security practices to all stages and aspects of application development and operations.

In a DevSecOps culture, everyone is responsible of security, and Kiuwan may help developers, project managers, testers and everyone else involved in the development cycle, to leverage the security level of their applications from inception.

Kiuwan considers 7 key points to have a clear understanding of the risk you can be exposed to with any application, have a clear security policy to follow, enforce it and make everyone comply and share the responsibility through the following key steps:

1. **Establish and share a security policy for every application.** Bear in mind that each application may have different needs, so you should be able to have different policies if needed. Security experts should be able to define them and share them. These should include secure code policies and behavioral policies.

2. **Start development with the security policies in place.** Developers have access to them and use them during the security code reviews in every

development iteration. Automating the code reviews will make the process more efficient using Static Application Security Testing (SAST) and SCA (Software Composition Analysis)

3. **Run a security audit, using SAST and SCA**, to enforce the policy and take the necessary measures if it fails.

4. **Generate a new baseline with the latest security state of your application's code, based on SAST and SCA**. This will be your new starting point for future code reviews and audits.

5. **Monitor your application in production gathering security flaw analytics** from the protection practices and running penetration testing if you see fit.

6. **Use the analytics feedback to refine the security policies** to enforce them with your SAST and SCA if possible.

7. **Define a defects & vulnerabilities fix plan** and make it part of your backlog for the next iteration.

Applications are spread out across organizations in disparate silos. As the volume and complexity of these apps grow, the problem worsens.

Moreover, the ability of teams to work in an unfocalized manner free from information silos is also hindered by fragmented systems, and tools, each with limited capabilities. Kiuwan integrates with any existing system and facilitates communication between teams and powerful and meaningful dashboards with information for every stakeholder.

The abstraction of infrastructure, or invisible infrastructure, the requirements around portability for in house developed applications, and the need to run in different environments across the hybrid architecture, has driven an increased focus in building security into the application itself.

Kiuwan facilitates the vulnerability assessment of code, management of code remediation projects across multiple teams, including outsourcers, and the measurement of the progress of such remediation efforts over time.

Kiuwan serves over 6,000 end users across approximately 500 customer organizations, with a client roster that includes firms such as Santander Bank, DHL, Zurich, and Telefonica among others, and offices in the USA, UK, Germany, France, Italy and Spain.

Conclusions

IDC has seen a dramatic increase in multimodal development and complex sourcing for software projects. This continues the existing trend for combining internal resources with contractors, onshore/offshore providers, and use of open source. With continuous integration and agile DevOps approaches along with the need for DevSecOps, the demand for effective quality has increased geometrically. New security levels must be applied along the whole design, development and deployment process aligned with the capabilities for emerging platforms with mobile, cloud, IoT, and other areas. It is in part due to this increase in multi-sourced projects that IDC has chosen to prioritize combined capabilities for ASQ with additional life-cycle areas. Enterprise ASQ solutions in this context can provide a basis for quality collaboration for end-to-end DevOps leading to apply the new security levels demands for the new digital services/applications developments.

IDC SPAIN

C/ Serrano 41 – 3º
28001 Madrid
Spain
www.idcspain.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.