Continual software testing Article copy

Originally published in: Web page of a software development business

Abstract: How a continuous testing scheme in software development can help businesses reduce time to market.

Figuring out how to cut system testing times for new features?

Eliminating bottlenecks in the software testing process can make a difference.

By: Milena Clavijo

There are many issues that turn the software testing phase into a bottleneck, causing delays, rework, and ultimately, affecting time to market.

How to overcome them? It's evident that no software or new development should be released live without first being tested effectively and thoroughly, to minimize potential errors and problems for your business.

The good news is that there are ways to optimize this phase and, therefore, minimize its impact on the release of new software, by implementing a continuous testing scheme.

This is achieved through tools that make it easier for organizations to function as true software factories, without increasing error rates.

The Bottleneck

The testing phase is a key stage in the software development cycle; however, it encounters various barriers during execution, which affect the speed of the process and, consequently, the deployment.

Industry indicators show that, during testing, 79% of teams face limitations, restrictions, or time constraints, as well as high access costs for third-party services[1] necessary for the process.

Furthermore, it's known that 70% of tests performed on new functionalities are fully manual[2], while 50% of the time is spent acquiring the necessary data to run them[3].

Other barriers to this process identified by ITAC include incomplete test environments, fictitious manual data that doesn't align with reality, high data infrastructure costs, lack of effective API coverage, and potential leakage of sensitive production data.

The Solution: Continuous Testing

Optimizing the process requires performing tests with 100% coverage in all necessary modules, while eliminating traditional barriers.

This is achieved by implementing tools that allow tests to be designed and executed not only more quickly, but with fewer people.

These improvements in the testing process translate into operational and cost benefits, and therefore, a better time to market.

Moreover, business cases show that it is possible to reduce costs and time for this stage by an average of 30%.

A continuous testing scheme has four key elements:

---

[1] Voke Market Snapshot Service Virtualization – January 2015

[2] Bloor Report Automated test case generation - September 2014

[3] Forrester Global Modern Service Delivery Benchmark Online Survey - Q4 2014

1.Test Design: High-quality design that accounts for all scenarios allows the optimization of execution times.

The goal is not to sacrifice quality for time but to perform all necessary tests in the shortest time possible.

2.Creation of Parallel Test Environments: To minimize high investments in testing infrastructure and software, as well as third-party access fees for services and components that integrate with the application being tested, Service Virtualization (SV) was created.

With SV, parallel test environments can be created. This is possible because the tool allows simulating dependent systems, including mainframes and external service providers.

Parallel environments allow multiple versions of software being prepared for deployment to be tested simultaneously (rather than in cascade).

All of this happens without causing queuing or downtime that delays the process due to lack of availability of services and components.

It also prevents the "competition" for priority in case of issues with the version deployed live, requiring the use of the only available test environment that companies usually have.

Another advantage of parallel environments is that they allow testing new features and system component loads in the early stages of the Systems Development Life Cycle (SDLC), when errors are easier and less expensive to fix.

3.Business Test Data Generation: Manual generation of test data not only takes a lot of time and consumes infrastructure for processing but also creates security risks, potential legal violations, or fines in case of sensitive data leaks, not to mention possible errors that affect test quality and result in rework.

Another drawback of manually generating test data is that live environment data typically offers only 20-30% of the functional coverage required to fully test the software.

This isn't sufficient, as the entire database needs to be represented to ensure effective testing.

Using a tool specifically designed for this purpose, it's possible to eliminate manual work in generating test cases, correcting or removing invalid data, avoiding duplication, over-testing, and failed tests, and generating fresh data in minutes, without the risk of security breaches, thanks to data masking.

Masking involves replacing sensitive information in a database using various techniques, substituting it with data that appears real but isn't.

4.Automation of Repetitive Tests: This feature allows repetitive tests to be executed faster and with the required coverage, even when several different API systems and services coexist, or in the case of mobile applications.

Automation reduces solution validation costs, simplifies test architecture, and frees up resources to test more complex functionalities. That is, only what is truly needed is tested manually.

By correctly combining these variables within the testing process, it's possible to combine speed and quality to achieve the best results.

Interested in knowing how a continuous testing scheme can help you reduce time to market? Contact Us

Microservices Article copy

Originally published in: Web page of a software development business

Abstract: How Microservices architecture in software development can make system optimization easier

Scared about how much it will cost you to optimize your company's systems?

Introducing new functionalities or modifying your systems doesn't mean you have to start from scratch.

By: Milena Clavijo

Digital strategies today, which rely heavily on social networks, often result in significant increases in demand on a company's systems during certain periods.

This is the case with seasonal offers that boost transactions on the company’s website for one or several days, or when customer traffic to a store increases the load on the billing system, among others.

The essential feature of these schemes is that they cause system demand to fluctuate between peak and off-peak periods, a scenario in which it becomes very complex for companies to dimension and project the required installed capacity of their systems.

This occurs because, to be prepared, organizations would need to maintain high idle capacity in their computer systems during periods when these offers or marketing strategies are not active.

The most sensible way to manage these bursts of seasonal transactions is to find a way to scale the system's capacity in line with demand, so that it increases when there are many requests and decreases when there are fewer requests.

In other words, companies must find a way for the infrastructure cost to be proportional to the transaction load the system receives.

But how can this be achieved?

A different way of doing things

Architecture refers to how a system is structured, and how its functions correlate with the hardware and software components, always keeping in mind the users who will be interacting with it.

The architecture that allows for dynamic installed capabilities in a company’s systems is one that ensures operations, in this case, functionalities, are carried out by sets of autonomous and independent services.

This is called Microservices Architecture (MSA), where the prefix "micro" refers to the granularity of its internal components, which happens without breaking, fragmenting, or partitioning the interface that the user sees.

Microservices are mini-applications, each with its own lifecycle and deployment, and each one implements individual business functionalities.

This implies that the architecture is designed with specific characteristics in mind, such as dynamic installed capacities, and isolates these factors so that, if needed, they can be modified without affecting the entire system’s functionality.

This shift in focus brings a series of benefits, resulting in flexibility and speed in responding to demand.

Advantages of implementing MSA
Defining business functions under microservices architecture allows for:

• Greater agility: It's possible to update a service without re-implementing the entire application, reducing development times and improving Time to Market.
• Flexibility: If there are alliances between companies to carry out certain business functions, in case of new partners or changes in existing ones, only the parts of the system interacting with them need to be replaced or modified.
• Scalability: Services can independently increase their capacity.
• Resilience: Thanks to error isolation, if one service fails, it doesn't require the suspension of the entire application.

How to implement MSA
This new approach requires a change both in the architecture and the logic of software development. Therefore, whenever migrating an application to MSA, a detailed analysis is required to check whether any part of the logic can be reused or if it needs to be completely re-conceived.

However, this doesn't mean that new applications developed under MSA cannot interact with applications built using other architectures.

On the contrary, it is possible and even recommended, as this allows the system to be migrated step-by-step while taking advantage of MSA to supplement new business functions.

When implementing MSA, there are aspects that fundamentally change compared to previous models, such as monitoring, log analysis, the way software is promoted and deployed across environments, and how the infrastructure is built, which in MSA must be in 'containers.'

Containers allow applications or groups of applications to be "packaged" and run on the same core operating system, which significantly reduces loading times or "uploading" the system.

Exposing services outside the company
MSA naturally supports the performance of APIs (Application Programming Interfaces), which are mechanisms that connect two software systems to exchange messages or data in a specific format.

APIs allow one application to use the functions already implemented by another, as well as its data library and supporting infrastructure. This way, one application can use another's information and functions while remaining independent.

Today, APIs can be designed for either private company use or public use, when they perform tasks that might be useful to users outside the organization.

Clearly, public APIs can be products that are sold, allowing third parties to consume them via web services or other protocols, generating additional income alongside the company's current business model.
A classic example of API management is data retrieval from individuals and businesses in risk databases by companies from various sectors.

Thanks to APIs, duplication of efforts is avoided, allowing each company to focus on its core business.

Security and structure
It is possible to combine Service-Oriented Architecture (SOA), APIs, and MSA to create a structure that supports both internal and external demand on a company's systems.

First, it is crucial to ensure that anything delivered or consumed from a third party via public APIs always passes through a centralized component (Gateway) to guarantee security and traceability.
Behind this layer, the company can have applications running simultaneously in both traditional and MSA schemes, which, in turn, interact through internal APIs with one or more back-end systems.

This approach allows the company to optimize its structural components and gradually migrate systems to better meet market demand—without falling behind or making excessive investments all at once.

Interested in learning how MSA can help you make your business more efficient? Contact Us

Cibersecurity Article copy

Written for: Insurance company

Abstract: How innovation is a critical tool to maintain and enhace cybersecurity.

The Challenges of Cybersecurity

Innovation, traditionally conceived as an essential approach to ensure companies' competitive advantage, is also emerging as a critical tool for cybersecurity risk management, and is key to anticipating challenges, changes, or potential contingencies in the short, medium, or long term.

By: Milena Clavijo

In February 2024, the health insurance company Change Healthcare, a subsidiary of United Health Group in the United States, suffered a ransomware cyberattack that paralyzed the processing of payments and medical claims, affecting thousands of healthcare providers, pharmacies, and patients, and causing losses estimated at USD 100 million per day[1].

The effects of this incident were still being discovered almost a year later, when the company confirmed that 190 million people had been affected by a data breach[2], including direct users and those who did not have contracted insurance with them, due to the large amount of medical data and countless transactions the company processes daily.

Regardless of all the implications that this terrible incident had for the company, its providers, users, and other members of the value chain, cases like this remind us that cyber risks are growing exponentially every day and that it is essential to adopt a proactive and far-reaching approach. But how can businesses prepare?

Trends and projections

According to the McKinsey&Co study *Cybersecurity Trends: Looking Over the Horizon*, risk arises from the very need for updating, because as companies invest in new technologies —or in improvements for these— to renew or expand their businesses, a series of overlapping layers is created between operational systems, generating new vulnerabilities.

This situation is taken advantage of by so-called 'adversaries', highly specialized organizations equipped with cutting-edge tools, including AI and machine learning, whose main objective is to render obsolete even the most sophisticated cyber controls in companies of all sizes and sectors.

The outlook is discouraging: according to the aforementioned study, the expected compound annual growth rate for direct cyber insurance premiums between 2022 and 2025 is expected to be of 21%, while annual costs related to cybercrime will reach USD 10.5 trillion per year globally in 2025.

Innovate and reinvent

The PwC Global Investor Survey (2025) —which highlights emerging risks and management priorities that investors from multiple sectors believe companies should consider— reveals that for 36% of respondents, cybersecurity challenges will be as frequent and important as traditionally relevant geopolitical conflicts and macroeconomic instability.

---

[1] CBS News. *Health care providers may be losing up to $100 million a day from cyberattack*.
[2] TechCrunch. *How the ransomware attack at Change Healthcare went down: A timeline*.

Furthermore, a large majority of investors surveyed by the study (71%) believe that companies must reinvent their business models in how they create, deliver, and capture value in response to technological changes, being this the issue that imposes the most pressure due to its rapid evolution and imminent changes.

What to focus on, then? Experts agree on the importance of strengthening defenses by increasing cybersecurity capabilities and innovating in detection, prevention, protection, response, and recovery tools, maintaining constant surveillance over those factors that influence current and future risks.

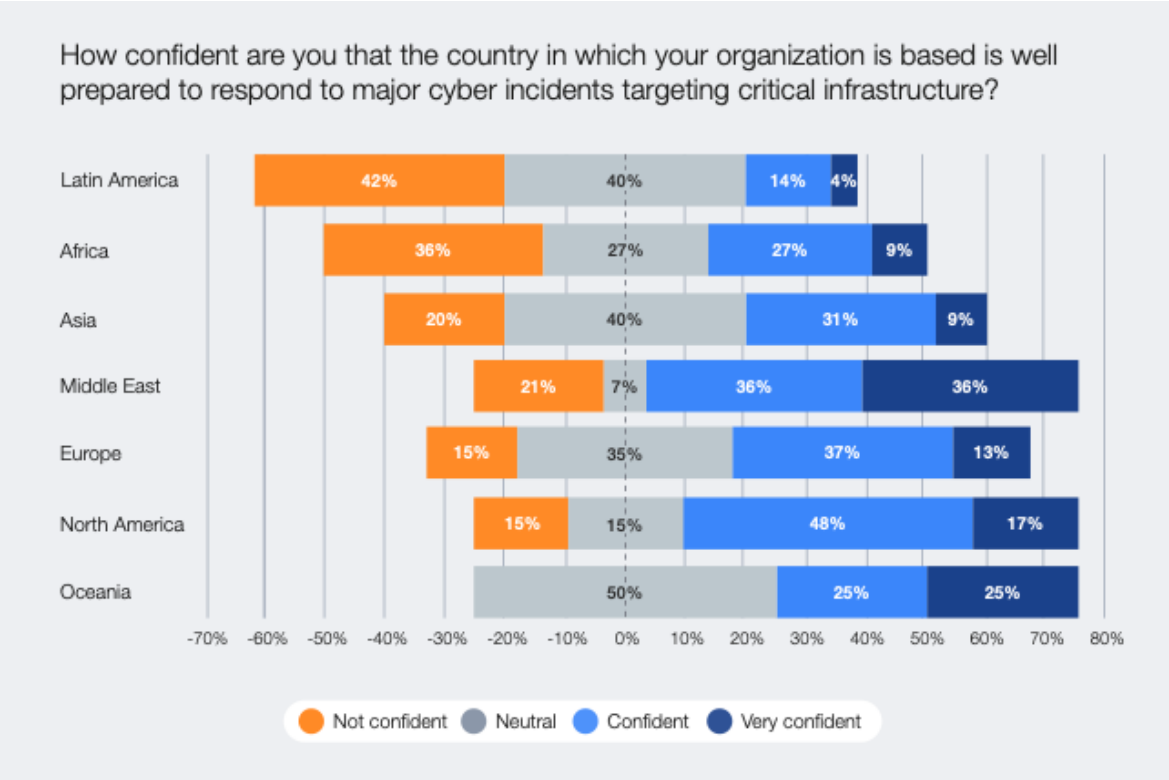
Factors to monitor

As cyberspace becomes more complex, a series of factors combine and have a compounded effect on global cybersecurity threats. According to the *Global Cyber Security Outlook 2025* report from the World Economic Forum and Accenture, these factors include:

1. **The cybersecurity skills gap**, since only 14% of organizations report feeling confident they have the talent and skills necessary to counter the threat.
2. **Geopolitical tensions**, which disrupt operations, supply chains, damage brand reputation, provoke cyberespionage, and the loss of confidential information, among others.
3. **AI and emerging technologies**, which increase the capabilities of cybercriminals, contributing to the increase in user attacks.
4. **Regulatory requirements**, established by countries to protect, but which, when proliferating and sometimes not being harmonized with those of other nations, create great challenges for compliance.
5. **Interdependence in supply chains**, which creates vulnerabilities in access and software due to the participation of third parties.
6. **The sophistication of cybercrime**, as 72% of respondents perceive that cyber risks have increased in the last year, with very significant escalations in phishing, social engineering attacks, and identity theft.

Monitoring these factors and taking actions to ensure cyber resilience —which is the ability of an organization to withstand, respond to, and recover from a cyberattack— is more feasible for large companies, which can guarantee focus and resources for R&D, and therefore tend to show sustained progress, while small and medium-sized enterprises often struggle to keep pace.

But it is not only from the point of view of company size that there are major differences. The same report reveals that, from a regional perspective, Latin America and Africa have the highest perceived risk in terms of cyber resilience, followed closely by Asia (see graph). A wide disparity is also detected in the impact on the public sector vs. the private sector in these regions, with the former having an urgent lack of resources and talent to shield itself against the growing threat of a cyberattack.



Source: *Global Cyber Security Outlook 2025*, World Economic Forum and Accenture.

Innovation is the way

In this context, innovation becomes a key tool in tackling as many fronts as possible, anticipating possible risk situations in order to neutralize them. These are just some options in which your company can innovate:

- **Integrate cybersecurity best practices early in software design**, ensuring that development and security teams work together at every stage of the project[3]. New alternatives such as blockchain[4] —distributed databases in securely linked blocks— can also be adopted to protect identity data, transactions, and critical processes.
- **Implement Zero Trust Architecture (ZTA)[5]** in all systems, a model that assumes no user inside or outside the corporate network is inherently trusted, so authentication is always required for any action. This is even more relevant considering that 25% of the workforce connects remotely between 3 and 5 days a week[6].
- **Create cyberattack simulation programs[7]**, enabling test environments in which defenses against ransomware, phishing, or other threats are tested and unforeseen scenarios are detected.

[3] McKinsey & Company. *Cybersecurity Trends: Looking Over the Horizon*. Responses to trend three, 2022.
[4] IBM. *¿What is blockchain?*
[5] Deloitte. *Zero Trust Architecture: Solving Security Challenges in a Cloud-First World*.
[6] McKinsey & Company. *Cybersecurity Trends: Looking Over the Horizon*. Responses to trend one, 2022.
[7] Gartner. *Top Cybersecurity Trends for 2024*.

• **Use automation through AI and machine learning** with a risk-based approach for detecting unusual patterns and responding to threats[8]. One alternative is XDR (Extended Detection and Response) platforms, which integrate detection, investigation, and automated incident response capabilities[9].
• **Train and expose internal users to simulations**. Create simulated risk situations to train employees[10], anticipating possible attacks and providing feedback.
• **Implement ongoing actions against ransomware**, including technical and operational changes to automate responses to malicious encryption, supported by resilient infrastructure, detailed action manuals, and contingency plans[11].

Tailored protection

Alongside the implementation of these new measures and as part of risk management in cybersecurity matters, comprehensive cyber insurance policies have become a great ally to protect companies of all sizes against these types of threats.

It is key to prioritize the analysis of these alternatives given the constantly changing cyber landscape, where none of the companies affected by such attacks anticipated their occurrence or the extent they would have. Gallagher offers a wide range of cyber protection plans and coverage options, and our experts can help you select the one that best suits your needs.

To learn more about how we can help you manage your cybersecurity risks, request personalized advice for your company today.

Textbox---
Differences between Cybersecurity and Cyberresilience

Cybersecurity	Cyberresilience
Protects computer systems, networks and data, preventing attacks.	Ability to withstand, respond to, and recover from a cyberattack.
Detects threats to the network, applications, data, and access, among others.	Focuses on minimizing the impact of incidents.
Proactive approach: it is an essential part of cyber resilience.	Proactive and reactive approach, which seeks to ensure business continuity.

Source: BCM Institute. Cyber Resilience vs. Cybersecurity: A Comprehensive Guide.

[8] McKinsey & Company. *Cybersecurity Trends: Looking Over the Horizon*. Responses to trend two, 2022.
[9] Microsoft. *¿What is extended detection and response (XDR)?*
[10] Metacompliance. *Empower your team with effective phishing simulations*.
[11] McKinsey & Company. *Cybersecurity Trends: Looking Over the Horizon*. Responses to trend two, 2022.

Sources:

BCM Institute. *Cyber Resilience vs. Cybersecurity: A Comprehensive Guide.* https://blog.bcm-institute.org/bcm/cyber-resilience-vs.-cybersecurity-a-comprehensive-guide

CBS News. *Health care providers may be losing up to $100 million a day from cyberattack.* https://www.cbsnews.com/news/change-healthcare-cyberattack-losing-up-to-100m-a-day/

Deloitte. *Zero Trust Architecture: Solving Security Challenges in a Cloud-First World*. https://www2.deloitte.com/us/en/pages/risk/solutions/zero-trust-services.html

Gartner. *Top Cybersecurity Trends for 2024.* https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

IBM. *¿What is blockchain?* https://www.ibm.com/es-es/topics/blockchain

McKinsey & Company. *Cybersecurity Trends: Looking Over the Horizon*. McKinsey & Company, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity-trends-looking-over-the-horizon

Metacompliance. *Empower your team with effective phishing simulations*. https://www.metacompliance.com/phishing-simulation

Microsoft. *What is extended detection and response (XDR)?* https://www-microsoft-com.translate.goog/en-us/security/business/security-101/what-is-xdr?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

PricewaterhouseCoopers (PwC). *Global Investor Survey 2025*. PwC Global, 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

TechCrunch. *How the ransomware attack at Change Healthcare went down: A timeline.* https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/

World Economic Forum in collaboration with Accenture. *Global Cybersecurity Outlook 2024*. World Economic Forum, 2024. https://www.weforum.org/reports/global-cybersecurity-outlook-2024/