randstad

addressing IoT challenges through DevSecOps.

table of contents.

back to top

DevSecOps can be adapted to increase IoT project success rates

Whether for personal, commercial or industrial markets/uses, organizations of all types and sizes are developing and deploying IoT technologies at an impressive rate. Worldwide IoT spending is forecast to reach $1 trillion in 2022, according to a recent in-depth study. Yet the same study also found that:

- Only 42 percent of respondents said their IoT efforts were either fully successful (12%) or mostly successful (30%).
- Meanwhile, the majority (58%) described their IoT efforts as either not successful at all (18%) or mostly unsuccessful (40%).

If these percentages don't improve, then $580 billion of that anticipated $1 trillion spend will be wasted. But the good news is that it doesn't have to be that way.

As with any emerging technology, moving from proof of concept (PoC) to successful deployment and ongoing maintenance poses formidable challenges. Namely:

- introducing and fitting a new technology into an existing operational governance and control ecosystem
- creating and aligning on a viable, scalable, secure and high-availability architectural strategy
- identifying and filling skill-set gaps without disrupting day-to-day operations
- maintaining reliable and consistent operations as the organization transitions from existing to the new technology

As if overcoming these challenges isn't enough, IoT offers its own set of unique challenges.

- Organizations must expand beyond their core competencies as they find themselves involved in a variety of IoT-specific activities: for example, managing and maintaining end points, electronic devices, deployments, connectivity, data, applications and more.
- IoT requires a multidisciplinary team with expertise and alignment in engineering, applications, data analysis/management, security, infrastructure and user experience (UX), all working in a way that is aligned with business goals.
- IoT solutions require a high degree of velocity while managing and reducing risk.

We have repeatedly seen DevSecOps concepts applied to overcome these difficult and seemingly insurmountable IoT challenges. DevSecOps frameworks, which entail a "security first" approach, help organizations become nimbler and more automated while fostering stability, enhancing code quality, minimizing risk and increasing velocity. Embracing DevSecOps allows organizations to mature organically and increase collaboration.

back to top

tracking the typical IoT journey

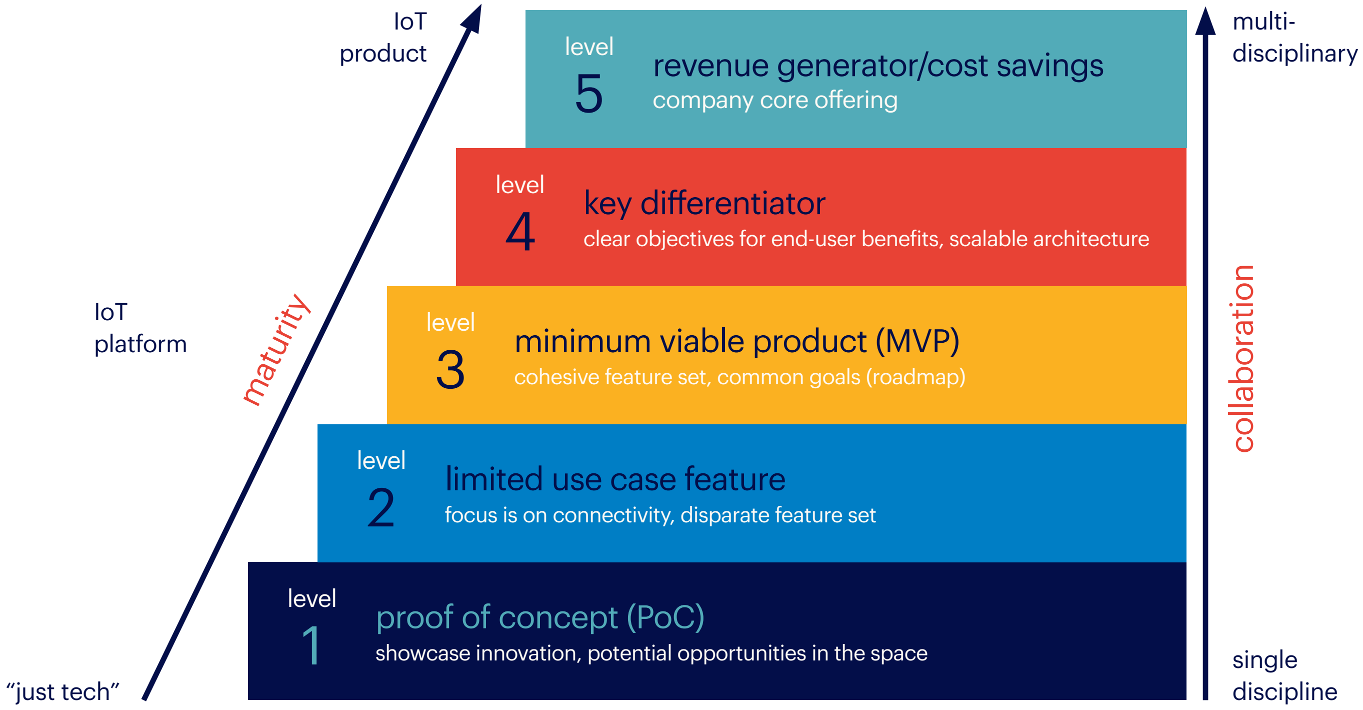
Most organizations begin their IoT journeys through a PoC to showcase innovation or solve a specific use case aimed at increasing efficiency or automating or capturing data. The IoT solution is built around connecting electronic devices to a bigger or existing ecosystem through the internet while capturing data through those electronic devices. At this juncture, the IoT solution consists of "just tech," a fact that is often reflected in the project team's makeup.

However, as the journey continues, organizations extend their IoT solution from "just tech" to a cohesively architected platform that supports multiple business use cases and offers a roadmap aligned with future needs (e.g., scalability, performance, security). These are the early stages of a minimum viable product (MVP). To support and deliver the IoT platform, the team has to mature, become multidisciplinary (including non-technical skills such as UX, business analysis, product ownership, etc.) and shift from a technical focus to a business focus. The goal is to get to a point where technology is enabling business value.

In the last stages of product maturity, the IoT solution is now a product or an important organizational capability — for example, a unique market differentiator or a revenue generator. The distinctions between technology and business are now inseparable, which is why tight alignment between business and technology teams is critical for long-term product viability and success.

The diagram below depicts the Randstad IoT product maturity framework as organizations progress from PoC to a viable product capable of generating new revenue and/or reducing operating costs.

IoT product maturity framework



IoT product
IoT platform
"just tech"
maturity
level 5
revenue generator/cost savings
company core offering
level 4
key differentiator
clear objectives for end-user benefits, scalable architecture
level 3
minimum viable product (MVP)
cohesive feature set, common goals (roadmap)
level 2
limited use case feature
focus is on connectivity, disparate feature set
level 1
proof of concept (PoC)
showcase innovation, potential opportunities in the space
multi-disciplinary
collaboration
single discipline

back to top

three significant challenges that impede IoT success

challenge one:

IoT forces organizations to expand beyond their core competencies

IoT, to a greater degree than most other technologies, requires competencies outside of core business capabilities. For starters, reallocating the organization's resources — dollars and people — leverages core competencies in planning, designing, maintaining and delivering an IT product/service.

One need look no further than what is happening in the manufacturing, automotive and transportation/ logistics sectors to find evidence of this IoT-related resource shift. Traditionally, the average annual IT budgets for these groups have been below industry averages. As IoT initiatives grow in these sectors, however, so too are their budgets — and in some cases, those budgets are now exceeding industry average spending.

one example from randstad

A global food manufacturing client was looking to deploy smart tools and production machinery to create "the plant of the future." With a focus on manufacturing and distributing food products globally, the goal was to apply IoT technologies to enable automation and realize labor efficiencies in their plants. However, to build their plant of the future, they needed to quickly build competency in IT and engineering. Updating their aging, disparate and outdated network equipment was a critical prerequisite to ensure the adoption of new, labor-saving electronic devices and technologies. This required a network upgrade that delivered improved and more consistent connectivity and network performance at their facilities.

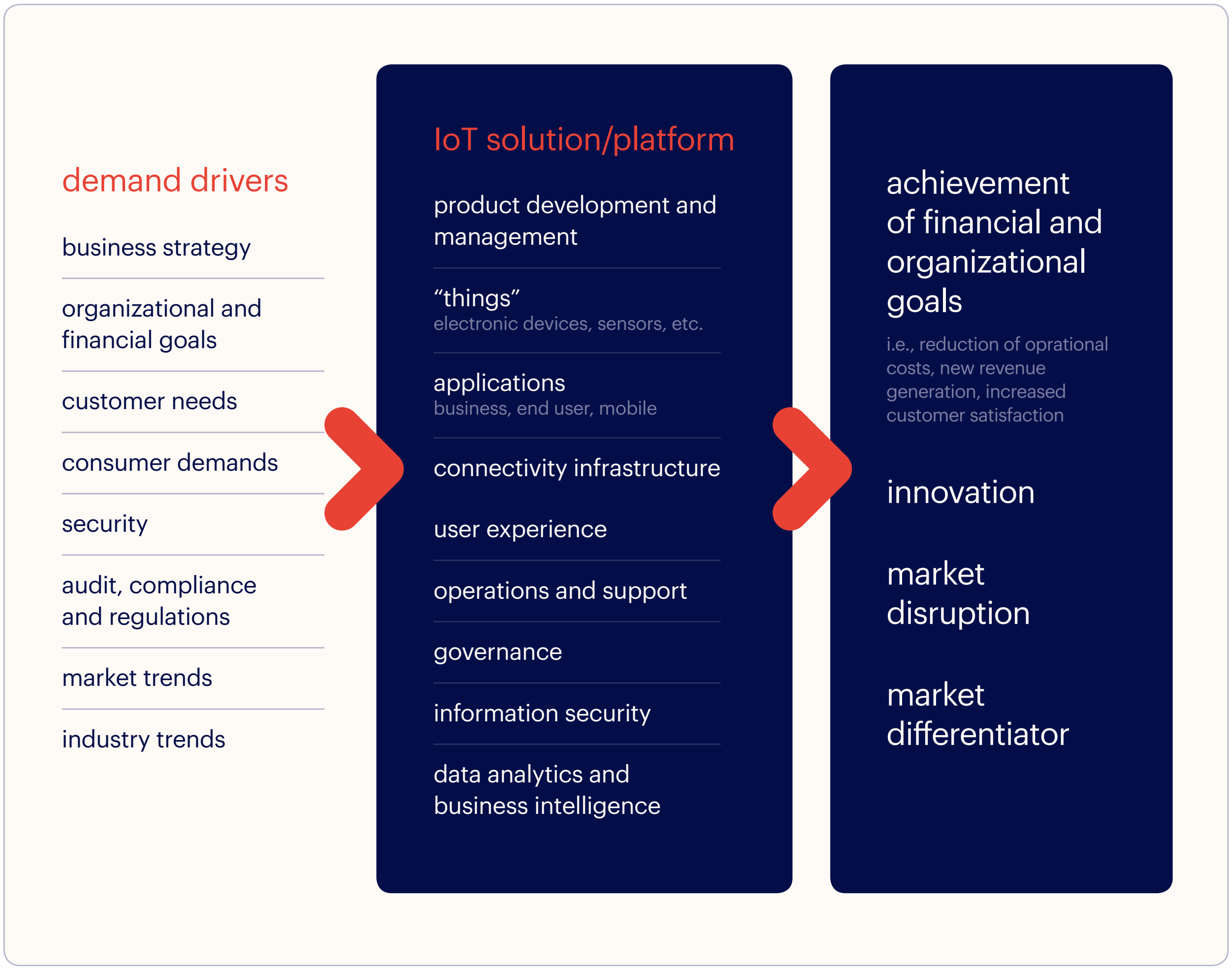
back to top

challenge two:

IoT requires business, IT and engineering alignment and collaboration — a multidisciplinary team

IoT is inherently cross-functional. As a consequence, IoT and organizational silos simply cannot coexist. As we've seen with other technology trends, successfully applying the technology and fully realizing its business value requires collaboration, cooperation and an ongoing cross-pollination of ideas. Nowhere is this more important than with IoT. Because it involves such a broad and disparate range of skills — big data, engineering, product development, application development, security, project management and support — subject-matter expertise scattered throughout the organization must be centrally harnessed.

IoT value/demand chain: business and technology alignment



demand drivers

- business strategy
- organizational and financial goals
- customer needs
- consumer demands
- security
- audit, compliance and regulations
- market trends
- industry trends

IoT solution/platform

- product development and management
- "things"
  electronic devices, sensors, etc.
- applications
  business, end user, mobile
- connectivity infrastructure
- user experience
- operations and support
- governance
- information security
- data analytics and business intelligence

achievement of financial and organizational goals

i.e., reduction of oprational costs, new revenue generation, increased customer satisfaction

innovation

market disruption

market differentiator

back to top

Given that need, applying concepts from both agile development and DevSecOps to create transparency, accountability and collaboration within the delivery team is a key early step in the process. This increases the likelihood that organizations will surmount the cross-functional and multidisciplinary challenges of IoT and more fully realize its benefits.

Agile and DevSecOps concepts drive the organization to focus on a number of guidelines:

- including the business as a part of the multidisciplinary team
- thinking of the IoT solution as a product or core offering
- making data-driven business decisions

Embracing these guidelines has clear practical benefits for the organization, too. Consider the following:

- The IoT effort is consistent with and supportive of the overall business vision.
- A core offering will receive the attention and resources it requires to succeed.
- Using data — instead of instincts or gut reactions to drive decisions — leads to measurable results.
- Data also helps analysts spot trends and uncover opportunities for new or modified services, products and features.

Overcoming multidisciplinary team challenges is fundamental to moving the IoT product through the product maturity framework. Ultimately, the value of the IoT platform can evolve from a productivity-enhancing tool to a viable product that offers revenue-generating opportunities, competitive differentiation and significant ROI.

As organizations move up the IoT product maturity staircase, each subsequent step in product maturity requires still greater collaboration. Reaching Level 5, at which point a total product is now a core offering, means the product team has expanded both within and outside of organizational walls — effectively partnering with vendors and other third third-party suppliers.

back to top

challenge three

IoT calls for high-velocity responses

The concept of velocity in IT refers to the speedy delivery of reliable and secure IT and engineering services. And while velocity, agility and security are critical aspects of IT and engineering delivery in general, the large footprint of the IoT ecosystem introduces a higher degree of operational complexity — and more factors that could potentially compromise velocity.

To be successful, therefore, IoT initiatives must emphasize acquiring and maintaining operational efficiency and security — speed without sacrificing quality or opening the door to malicious actors.

An infrastructure that is capable of high-velocity responses will realize several important benefits:

- improved agility in product development and faster time-to-market
- reduced time-to-value
- greater collaboration among internal teams, as well as with vendors and other third-party suppliers
- the ability to scale faster
- enhanced customer satisfaction as updates, fixes and improvements are released faster
- increased cost savings by reducing outages and reducing or eliminating product recalls

This mandate to increase and maintain velocity further underscores the importance of aligning DevSecOps to IoT.

As a greater number of non-IT organizations embrace IoT and strive to improve velocity, risk management becomes a major concern — and security becomes a key focus of the overall product lifecycle. It is critical that security not be regarded as an afterthought. Rather, it should be a key driver in developing and designing the solution from the outset. IoT baselines, such as those found in National Institute of Standards and Technology Interagency/Internal Reports (NISTIR), offer useful guidance to organizations looking to better understand and manage those risks from end to end.

how security concerns compound IoT project risks

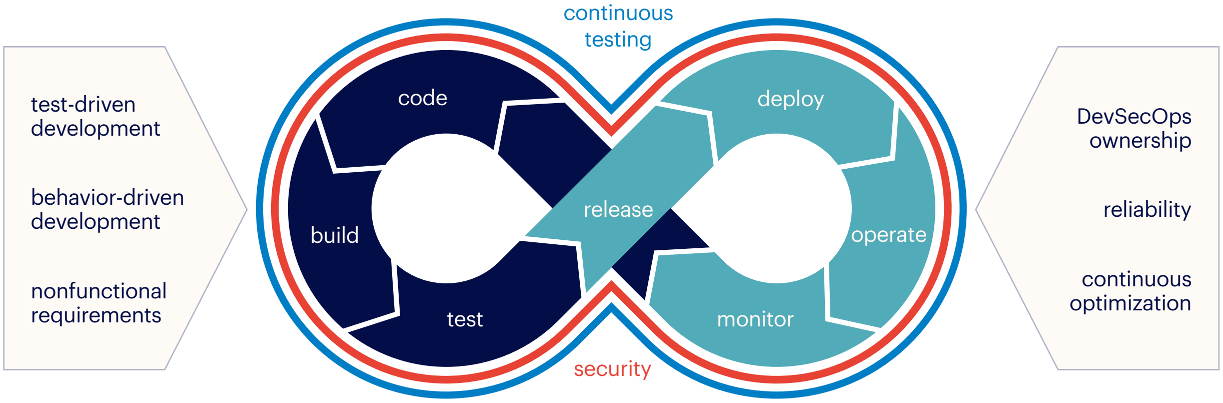
- having multiple, geographically dispersed smart electronic devices and sensors
- working with connections from those electronic devices/end points to applications and infrastructure that are located in data centers and in the cloud
- relying on third-party vendors and applications, creating a dependency on hardware and software that the organization does not own or maintain
- continuously analyzing and acting upon large data sets — an approach that can increase organizational vulnerability to security risks
- working with end users who use their own personal electronic devices to interact with the overall IoT ecosystem

back to top

why DevSecOps is vital to overcoming these three IoT challenges

Each of the major challenges we've identified as obstacles to IoT success — lack of cross-functional alignment and collaboration, failure to develop competencies other than core business capabilities and the inability to increase secure velocity — can be resolved through the effective deployment and use of DevSecOps.

The following framework provides a high-level outline of why aligning the elements of DevSecOps with your IoT initiative is so critical to achieving velocity while also managing and reducing risks.



This framework has three primary purposes:

- eliminating silos between the development and operations teams
- creating a continuous flow within the different stages of the software lifecycle
- encouraging ownership of the product regardless of lifecycle stage

When implemented properly, this framework fosters the agility and velocity that teams need to successfully develop, deploy and operate or maintain an IoT product.

Although "test" appears as a segment within the figure eight, the suggested framework presents a continuous testing cycle in which testing accompanies the organization's standard continuous integration (CI) and continuous deployment (CD) cycle.

Continuous testing requires several things:

- adopting and using test automation
- establishing test-driven development (TDD)
- defining nonfunctional requirements (NFRs) such as security, reliability, performance, maintainability, scalability and usability

By enabling continuous testing, security teams can dial in to their security controls at every stage of the CI/CD cycle, which is consistent with a security-first approach.

back to top

Where traditional DevSecOps implementations are often application- or software-development focused, IoT comes with different requirements. In an IOT solution, expanding or complementing test-driven development with behavior-driven development (BDD) ensures development teams are not just focused on developing individual units within the application. BDD enables the team to step back and examine the big picture — how the IoT application behaves given various user interactions — while focusing on attaining business objectives.

Defining nonfunctional requirements as part of the overall lifecycle ensures a security-first approach, from the earliest stages of planning on through every lifecycle stage. Aside from security, nonfunctional requirements ensure that key considerations are embedded in the IOT lifecycle, including:

- architectural considerations for infrastructure, applications, data and even device management around scalability, performance and reliability
- operational considerations for the overall product
- usability considerations, such as user interactions with the overall product, taking into account both technical and experiential perspectives

By implementing DevSecOps, the organization establishes a framework that:

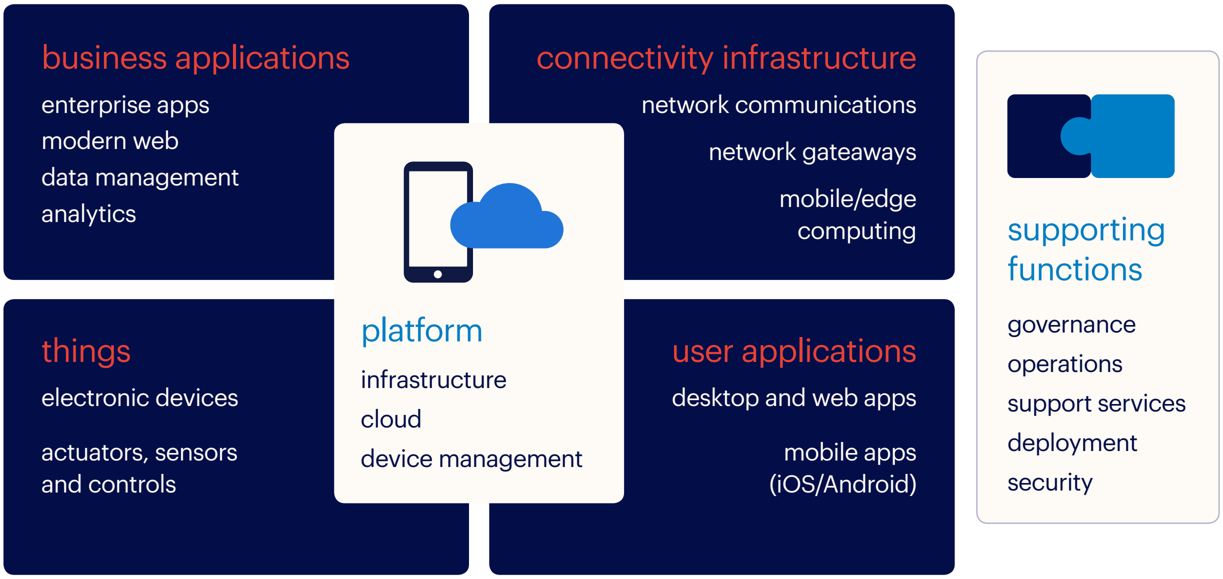
- enforces a security-first approach, while facilitating velocity and agility in response to time-to-market deadlines or security threats
- requires the project team to collaborate and expand their focus beyond technology, operate as a multidisciplinary team and continually focus on the overall footprint as a product offering
- provides guiding principles for non-technology-focused organizations to rapidly understand organizational capabilities and expedite complex decisions (e.g., whether to build internally, form partnerships or buy those capabilities)

final IoT project thoughts

Is your organization contemplating the development of a new IoT solution — or just trying to improve on previous IoT efforts that failed to meet goals and expectations? Here are three takeaways to keep in mind.

- Consider employing DevSecOps. It's a valuable framework that can increase velocity, allowing you to move faster while also managing risk and security.
- Approach IoT from a business perspective — it's not just about technology. Approaching an IoT solution as a maturing business product requires key aspects of the solution to be driven by business inputs.
- Build a multidisciplinary team, including members from the business side of the organization, not only to drive greater collaboration but further increase velocity once paired with a DevSecOps framework.

randstad’s IoT solutions expertise



business applications

enterprise apps
modern web
data management
analytics

connectivity infrastructure

network communications
network gateways
mobile/edge computing

platform

infrastructure
cloud
device management

things

electronic devices
actuators, sensors and controls

user applications

desktop and web apps
mobile apps (iOS/Android)

supporting functions

governance
operations
support services
deployment
security

Randstad is one of the few organizations, regardless of size, that has subject-matter expertise and experience in the wide-ranging tech disciplines involved in creating and deploying IoT-focused projects. Our solutions offerings leverage our know-how with a global network of delivery centers. Areas of our solutions practice include:

- an engineering practice offering electronic product development and embedded software programming services — including ISO9001:2015 and AS9100D certifications
- an infrastructure practice focused on planning, designing, deploying and monitoring connectivity infrastructure, including wireless
- a data management and business intelligence practice consisting of analysts who can spot trends, identify opportunities for process improvements and fine-tune business efforts
- an application services practice with experienced developers able to leverage device capabilities and create user-friendly interfaces
- continual service improvement and support professionals to keep IoT solutions updated and functioning smoothly
- IT and engineering thought leaders with insights and experience in the primary IoT support functions, including governance, operations and security best practices

Whenever you’re ready to embark on an IoT project — or need a hand salvaging a stalled effort — we’re here to answer your questions, offer practical guidance and deliver business value. Visit Randstad to learn more.

© Randstad North America, Inc. 2021

randstad

human forward.