Top 5 IoT Deployment Best Practices

Table of Contents

The Internet of Things is white-hot because of its potential for huge financial returns and operational improvements. But success is far from guaranteed; numerous challenges and pitfalls loom for organizations that fail to plan properly and execute meticulously. Here are some guidelines on spotting and overcoming possible problems to ensure a successful deployment.

Hyperscale connectivity is transforming the way organizations conduct business and consumers interact with the world around them. The already large and fast-growing Internet of Things (IoT) has changed the rules of the game. Workplaces have become increasingly digitized by ubiquitous connectivity, innovative applications, and endpoint proliferation and diversification beyond almost anyone's wildest imagination.

IoT growth has been—and will continue to be—nothing short of astonishing. Consulting firm McKinsey & Co. projects a compound annual growth rate of more than 30% from 2015 through 2020[1]. As more and more consumer and industrial use cases emerge as success stories, it will become a given that any workplace, device or business function can and will be digitized.

1 "The IoT opportunity—Are you ready to capture a once-in-a lifetime value pool?" Chris Ip, McKinsey & Co., Hong Kong IoT Conference, June 21, 2016

TechTarget | Custom Media

aruba
a Hewlett Packard Enterprise company

But these lofty figures don't tell the whole story. Far from it, in fact. That's because even sober researchers and consultants aren't fully sure of the level of complexity organizations are going to encounter in actually deploying their IoT projects. As with many projects merging the "magic" of technology with cold-blooded business goals, success is heavily influenced by the need to view IoT deployment more like a continuum of processes rather than as a big-bang event.

Best practices in IoT deployment must account for a wide range of issues before, during and after systems are built and solutions are rolled out. That leaves a lot of places where things can go wrong.

Let's identify some best practices for successful IoT deployments:

1. **The best deployments are shaped by the best strategic planning.** Chinese military strategist Sun Tzu is often quoted on the importance of winning the battle before the first blow is struck. In IoT deployments, strategic planning may be the most vital step on the pathway to success. This is where goals are established, metrics identified, teams assembled, use cases pinpointed, technical inventory taken and business processes evaluated. This can and actually should be the most time-consuming part of an IoT deployment, because it is where fundamental decisions that profoundly influence every other step take place. Perhaps that's why 90% of executives surveyed in a recent Bain & Co. IoT study said their organizations are currently in the planning and proof-of-concept stage.[2]
2. **Slow and steady over fast and furious.** Organizations—regardless of size, geography, industry or business model—are expecting big things from IoT projects, so it would be natural for business and IT stakeholders to assemble a war chest of funding, technical tools and manpower to throw at what they hope to be a massive business windfall. Resist that urge. Instead, focus on proofs of concept, sandboxes, pilots and narrow use cases for the initial go-round for IoT deployments. Learn from mistakes, and be emboldened by success—but don't try to transform the enterprise in your initial project. The Bain study also highlighted this issue: Only about 20% of executives surveyed expect to implement solutions at scale by 2020.[3] Another important step here is to ensure that the organization's human resources are properly aligned and deployed. In particular, organizations need to understand that, while an IoT program requires deep involvement of the IT team, it will not succeed without tight collaboration and alignment of IT and business stakeholders. "IT will have to join with line managers to oversee IoT systems that are essential to improve both the top and bottom lines," according to McKinsey.[4]
3. **Take a nuanced view of managing endpoints and devices on the network.** Traditionally, network management tools have been asked to sense if devices and systems are on or off, running or not running. But with IoT, your deployments must account for deeper analysis of endpoint behavior and network health. Other than simply determining uptime and availability, IoT systems must instantaneously conclude if systems and devices are performing up to the specified levels to accomplish the business goal. These also must be tightly managed without having to devote armies of administrators to manually monitor and tune systems to ensure performance and reliability. Connectivity is a key variable in IoT deployment success, and it's not just about buying more bandwidth or building in greater resilience—as important as those steps are. You'll need automated management tools to take the onus off your already overworked network team to ensure you have pervasive, always-on connectivity throughout the increasingly dense and broad mesh of your network under IoT.
4. **Security is paramount. Plan and act accordingly.** Remember you are connecting many devices that no one ever expected to plug into your physical, virtual or cloud networks. And we're not just talking about consumer endpoints like cars or refrigerators. Essential commercial components such as dialysis machines, injection molding systems and retail merchandise inventory sensors are among the heretofore unconnected and unmanaged endpoints in the industrial IoT. And if you thought patching garden-variety PCs was a chore, think about applying proper security frameworks to these new, diverse endpoints. Your IoT security framework may be the single most important technology decision you will make, in no small part due to its huge regulatory, financial, operational, legal, user experience and brand reputation impact. Your IoT systems must be ready to not only sense the appearance of new kinds of endpoints, but also instantaneously analyze their legitimacy, access and privileges under policies and identity management. Your systems must be able to determine, with pinpoint precision, whether they should be on your network in the first place, what they can and can't do, and how to prevent incursions before they infect your systems, applications and data.
5. **Infrastructure matters.** Get ready. In an era where most enterprises are trying to limit Capex exposure, many business

2 "How Providers Can Succeed in the Internet of Things," Bain & Co., Aug. 29, 2016
3 Ibid.
4 "An executive's guide to the Internet of Things," McKinsey & Co., August 2015

executives may balk at the notion of upgrading digital infrastructure. But the great potential of IoT is going to put strain on legacy infrastructure, so be prepared to make strategic infrastructure investments—especially for networking and connectivity. After all, the volume, variety and velocity of data going over both wired and wireless infrastructure are expanding dramatically, with no end in sight. For instance, make sure you have modernized physical network switches and management tools to ensure nonstop flow of information, and that your wireless infrastructure is ready for the latest version, whether that's 802.11ac or whatever is about to come down the pike. A steady, reliable and comprehensive flow of all data—structured and unstructured—is essential for the kind of analytics that is going to be a critical component in your IoT use case deployments and measurements, and you can't do that without robust, secure and scalable infrastructure.

Building blocks that matter

Successful IoT deployments share a few common characteristics, including meticulous planning, careful execution and close monitoring of progress against goals. And when it comes time to actually turn on the switch for your IoT use case, you'll need technology tools that make deployment and ongoing management simple, efficient and scalable. At the same time, those tools must closely monitor and automatically optimize the performance of IoT applications and a wide range of devices on the network.

Aruba Networks, a Hewlett Packard Enterprise company, provides the essential building blocks that promote successful IoT implementations. With Aruba's network management tools, enterprises focus less on monitoring infrastructure availability and behavior, and concentrate instead on recognizing the value of data that flows over their wired and wireless networks.

Aruba offers several market-leading network management tools for IoT deployments. Aruba Central is a cloud-hosted solution for network management and monitoring, offering such services as customizable guest Wi-Fi and presence analytics. And for multivendor environments where visibility into access networks is essential, Aruba AirWave accommodates wired and wireless infrastructure from Aruba and third-party manufacturers.

Aruba network management solutions are available for both on-premises and cloud-based deployments.

For endpoint visibility—essential for enhanced security and compliance with both wired and wireless networks—Aruba offers ClearPass, a line of endpoint management tools. ClearPass provides real-time, agentless profiling of myriad endpoint device types, regardless of location or time frame. Through Aruba ClearPass Universal Profiler, a virtual appliance that can be up and running in minutes, organizations can achieve network access control without having to invest in a higher-cost, enterprise-wide solution.

Conclusion

Few, if any, technologies have the potential to match the economic impact of the Internet of Things. Cloud computing, mobility, software-defined infrastructure and many others may be transforming different segments of the business landscape, but the IoT stands out because it incorporates these and just about every other technologies into a holistic, symbiotic digital workplace.

This much potential upside often comes with commensurate risk, of course. There are many places where IoT projects could fail to meet their full potential—or, in some cases, fail completely. That's why business and IT leaders must take the long view in IoT deployments, starting with embryonic discussions about goals and challenges, and then progressing through business workflow alignment, choosing the right tools, managing people and processes, measuring the right things, and resetting goals, expectations and plans on a regular basis.

For more information on how to put your IoT planning, deployment and management strategies in place with the help of innovative network management technologies, please go to **www.arubanetworks.com**.