White Paper

Future Focus: Is Your Enterprise Ready for IoT?

With recent advances in both mobility and infrastructure, enterprises are becoming increasingly decentralized, and corporate data increasingly difficult to protect.

A recent study by Juniper Research revealed that by 2020, the number of connected devices will have reached approximately 38.5 billion.

The notion that every component of the workplace may one day be connected to a vast, digital network seems like a concept drawn straight out of science fiction. However, the Internet of Things (IoT) – sensors and actuators connected by networks to computing systems – is very real. It's already started to have a marked influence on how we work and live, changing everything from how hospitals operate, to how goods and services

are manufactured and transported, to how we interact with our entertainment. These early victories in IoT are minor compared to what a connected world might deliver down the line.

But what will it take for organizations to maximize returns from this technology, while mitigating risks?

The challenges presented by this evolution are not dissimilar to those that were posed by the Bring Your Own Device (BYOD) phenomenon as it took hold. As such, the organizations that will most easily leverage the benefits of IoT will be those that have already mastered endpoint management. This is due in part to the fact that they will already have the infrastructure in place to manage a large volume of endpoints from a unified platform.

Connected World, Connected Workforce

"The digitization of machines, vehicles, and other elements of the physical world is a powerful idea. Even at this early stage, IoT is starting to have a real impact by changing how goods are made and distributed, how products are serviced and refined, and how doctors and patients manage health and wellness. But capturing the full potential of IoT applications will require innovation in technologies and business models, as well as investment in new capabilities and talent. With policy actions to encourage interoperability, ensure security, and protect privacy and property rights, the Internet of Things can begin to reach its full potential—especially if leaders truly embrace data-driven decision making."
McKinsey Global Institute Report – 2015

Gartner Research Director Peter Middleton estimates that by 2020, component costs will have dropped to the point that connectivity will be a standard feature in a range of products. Product designers will no longer be limited in what can be made 'intelligent', and the variety of devices – particularly in the workplace – will increase exponentially.

Through advanced business intelligence and better worker enablement, a connected workplace offers the potential to reduce costs and increase profits.
But what does this mean from a security perspective? Many enterprises already struggle with device proliferation, and many decision-makers are already nervous about securing enterprise data across environments and form factors. IoT will only add to the anxiety around data leakage and controlling network access points. By embedding sensors across the business, the volume of data which must be

both protected and analyzed will increase exponentially alongside the number of endpoints which must be secured.

Mobility management solutions have evolved from simple MDM platforms to complex offerings that allow IT to manage and secure many different components of an enterprise's network, incorporating application management, content management, network access management, location-based security, and a range of other functions. For businesses to transition from 'mobile-ready' to 'IoT-ready,' mobility management must evolve again.

Rather than focusing on managing devices and applications as isolated entities, IoT-enabled enterprises must also offer the following:

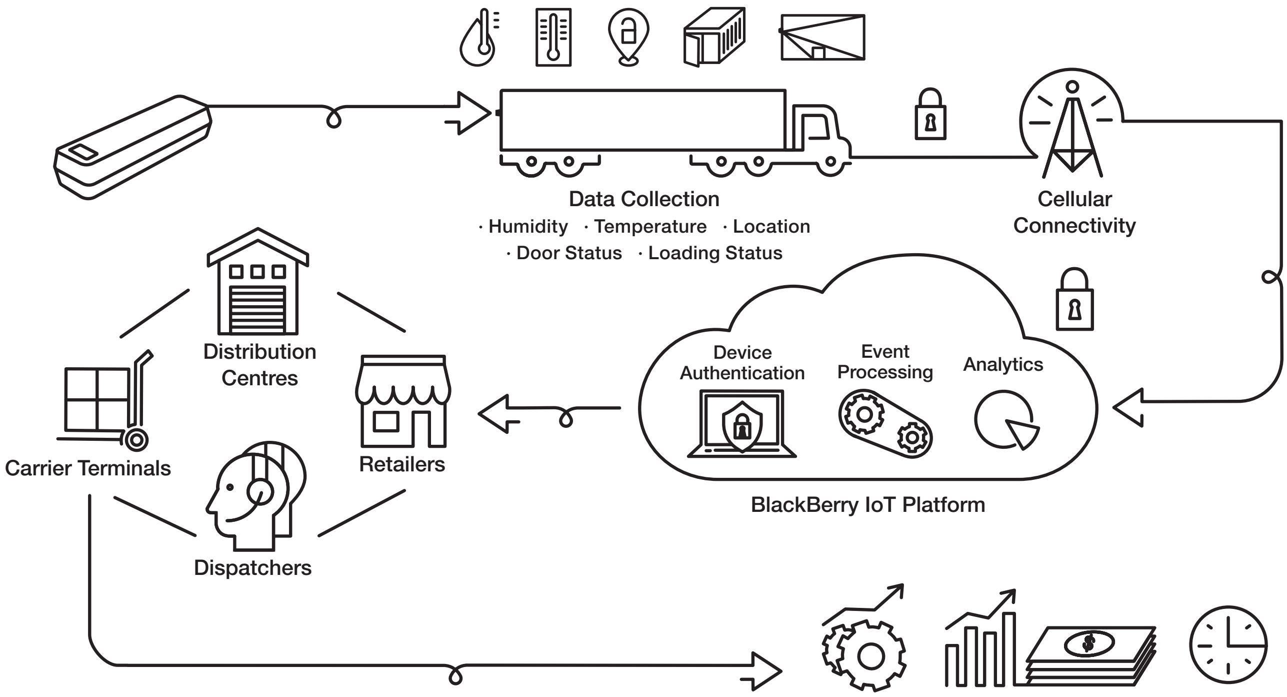
- The ability to secure and control corporate data independent of operating system, device type or ownership model
- Containerization for cloud/IoT enterprise apps which might otherwise gather personal data from users.
- User-centric, rather than device- or application- centric authentication.
- And of course, support for an array of smart devices, and compatibility with key operating systems that drive those devices.

As before, all of this needs to be controlled through a unified management console, offering both the convenience workers demand and the security and manageability the business requires.

On the Radar

BlackBerry's Radar platform is an asset- tracking solution built on the QNX IoT operating system. By leveraging a network of low- maintenance embedded sensors, it allows organizations to connect their entire fleet of vehicles, which are then managed through an intuitive frontend application. Through this app, businesses can set up flexible geo-fencing rules, set intelligent alerts and alarms, and read data including cargo status, temperature, humidity, and motion.

By providing more information and greater visibility, Radar enables faster, more efficient transportation of goods and services. Unlike previous-generation truck tracking technologies, BlackBerry Radar takes only minutes to install and immediately generates rich, real-time information in an intuitive, easy-to-read user interface. Operations managers, load planners and dispatchers can use BlackBerry Radar's data to determine where their trailers and shipping containers are located and how they're being used. They can also identify (and prevent) potential opportunities for theft or drains on efficiency.



Why Flexibility and Scalability will be Critical

The possibilities of IoT are endless, but all these endpoints will need to be managed securely and effectively, much like a network of smartphones is managed today.

Flexibility and scalability of unified endpoint management (UEM) solutions will become even more critical. Today, a large enterprise might manage hundreds of endpoints, and thousands of apps. Once connected devices start gaining prominence, these numbers will sharply increase, likely numbering in the thousands and tens of thousands.

This sharp upturn necessitates a change in how devices are managed. UEM platforms will be forced to extend their capacity to massive networks of "things", while the influx of employee-owned devices will necessitate a shift of its own. Today, the average employee uses three different devices over the course of a workday; Gartner estimates that, thanks to wearable technology, this will increase to five or six as the Internet of Things takes hold.

It's unreasonable to expect these employees to repeatedly authenticate each individual device – user-centric management will therefore become necessary for IoT-enabled organizations.

Finally, as embedded sensors begin pushing systems to their limits, UEM platforms will be forced to evolve, growing more complex in order to extend support to a larger fleet of devices than ever before. And even in the face of this complexity, they will need to retain their ease of use, both for IT and for the end user.

The Role of Mobile Maturity in IoT Enablement

Download 'The CIO's Guide to UEM', which includes an explanation of how you can determine where your organization falls on the mobile maturity curve. Guide your mobile evolution and lay the groundwork for IoT.

In the near-term, the focus for enterprises should be on proceeding down the path towards mobile maturity. The reasoning here is simple: the enablement of IoT devices is a natural 'next step' for businesses that have mastered mobility.

Those enterprises that have begun innovating and experimenting with new approaches, apps and endpoints – those businesses that have an application development platform, file-centric digital rights management (DRM) capabilities, and IAM solutions in place, for example – are well-equipped to implement embedded sensors into their workflows. Similarly, organizations for which BYOD and mobility are still considerable challenges will struggle to handle the influx of new devices brought about by the Internet of Things; they will be incapable of adequately securing the diverse range of new endpoints that IoT entails.

Wherever your organization is today on the path to mobile maturity, there's an edition of the BlackBerry Enterprise Mobility Suite to meet your needs. Find yours, and start a trial today:

BlackBerry.com/suite

Unified Endpoint Management

With the emergence of machine-to-machine (M2M) connectivity and the Internet of Things (IoT), markets are once again experiencing innovations that remove distance and time constraints in getting work done. Connected products provide real-time data from physical environments, while improved analytical processes and new applications allow work tasks to be undertaken more efficiently and more speedily. In the IoT, the mobile endpoint itself performs several roles, transcending its narrower remit within enterprise mobility solutions and becoming a crucial part of Enterprise IoT. The future of mobility is therefore one in which a single, unified endpoint management platform – one capable of capturing, securing, and analyzing all data across a corporate network – is necessary for

success. In the near-term, unified management and a user-centric approach are a matter of security and efficiency. In the long-term, they'll quickly become a matter of survival, as businesses without a means of adequately consolidating their data and endpoints fall far behind.

The good news is that businesses still have some time to reach mobile maturity, before IoT becomes truly widespread in the workplace. And for those organizations that have arrived at that point, the transition should be a relatively painless one. The biggest challenge for those organizations won't be in supporting IoT endpoints – it will be in deriving value from the data those devices provide.

About BlackBerry

BlackBerry is securing a connected world, delivering innovative solutions across the entire mobile ecosystem and beyond. We secure the world's most sensitive data across all end points – from cars to smartphones – making the mobile-first enterprise vision a reality. Founded in 1984 and based in Waterloo, Ontario, BlackBerry operates offices in North America, Europe, Middle East and Africa, Asia Pacific and Latin America. The Company trades under the ticker symbols "BB" on the Toronto Stock Exchange and "BBRY" on the NASDAQ. For more information, visit **www.blackberry.com**