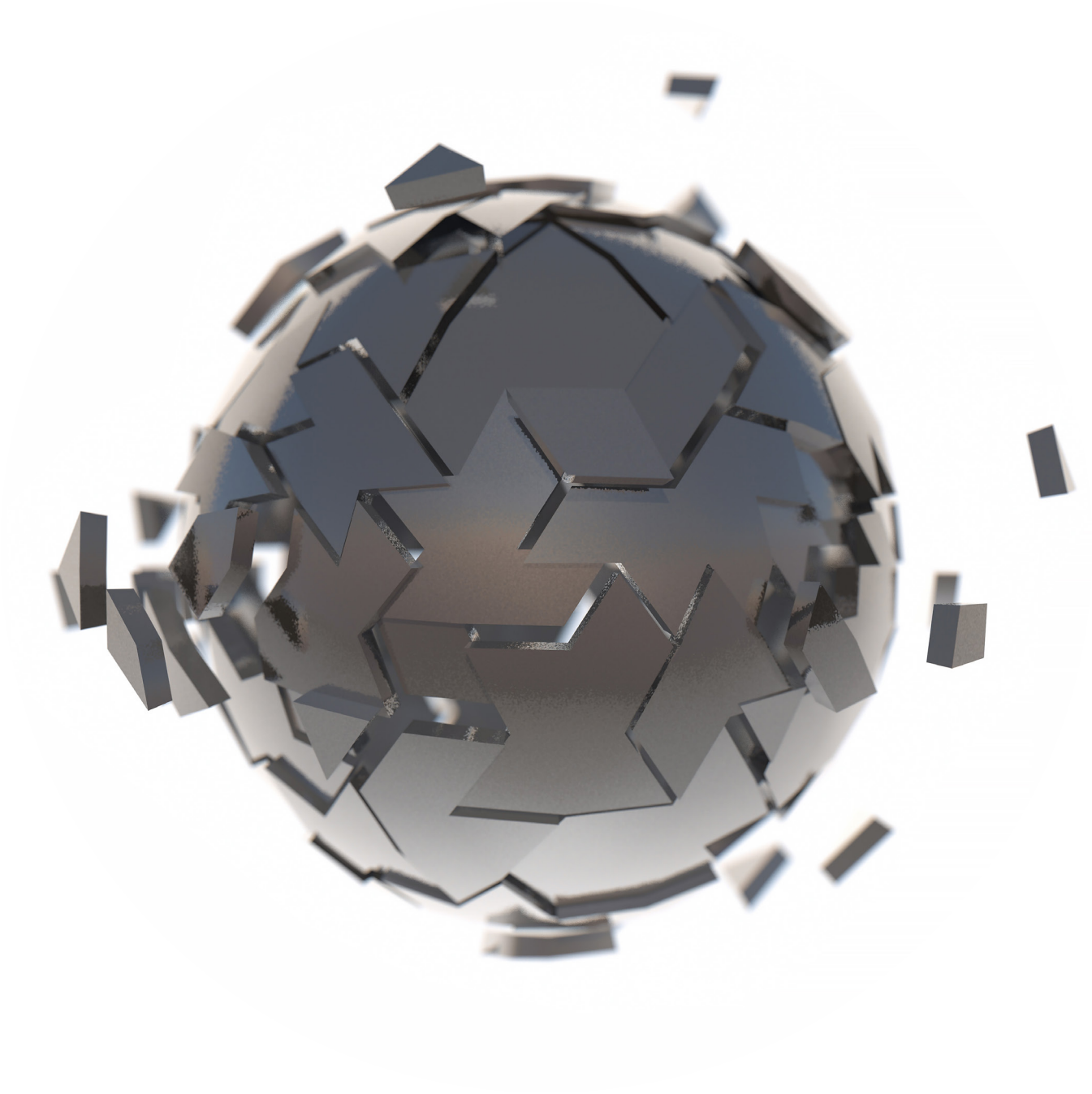
Deloitte.



Secure IoT by design

Cybersecurity capabilities to look for when choosing an IoT platform

October 2018

Introduction

The Internet of Things (IoT) is a set of business and technology innovations that offers many compelling benefits. However, it also presents significant cybersecurity risks and a greatly expanded attack surface. Mitigating these risks can help organizations realize the potential and benefits of the technology.

IoT platforms are emerging that make IoT development and deployment much easier. But just as important is their ability to greatly enhance IoT cybersecurity.

This report examines the cyber risks associated with IoT, and highlights the cybersecurity capabilities IoT platforms must have in order to address those cyber risks effectively.

The risks of IoT

With IoT, devices are both ***smart*** and ***connected***—gathering and sharing data without the need for human intervention. This enables information to be collected and shared on a massive scale with unprecedented levels of speed, efficiency, and detail.

The most obvious risk of connecting smart devices at scale is that it creates an expanded attack surface with countless points of vulnerability.

Bad actors are constantly looking for any little weakness, and IoT greatly expands the universe of potential weaknesses—whether in a particular device, device-to-device communications, or the broader Internet. Even a single breach point may be enough to compromise the entire IoT network.

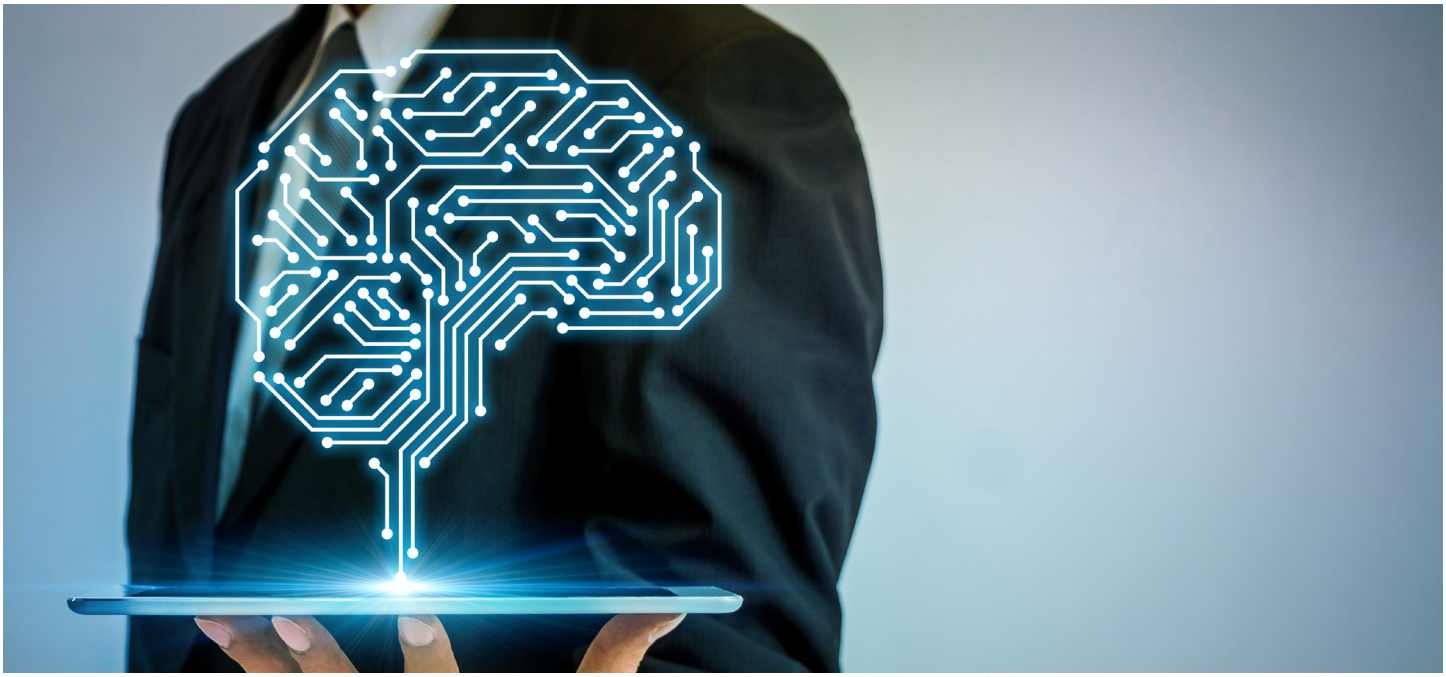
Another risk with IoT is that it greatly expands the amount of data that can be compromised. IoT data has the potential to be far more detailed and sensitive, since it can be collected in real time directly at the source.

Last, but certainly not least, IoT provides a bridge between digital and physical, making it possible for digital hackers to wreak havoc in the physical world—whether it's taking control of your vehicle, or causing a nuclear power plant to melt down. As the World Economic Forum noted, "hacking the ***location data*** on a car is merely an invasion of privacy, whereas hacking the ***control system*** of a car would be a threat to a life." [1]

For IoT to reach its full potential, these and other cybersecurity risks need to be identified and addressed.

[1] World Economic Forum, "Technological Risks: Back to the Future," http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/#view/fn-23.

IoT platforms can help



Until recently, companies deploying IoT had no choice but to build comprehensive solutions from the ground up. Now, however, IoT platforms are emerging that make IoT development and deployment much faster and easier.

Like a computer operating system, an IoT platform provides a standard foundation for applications to build on, so they don't have to be programmed to do everything from scratch. For example, a computer operating system handles all the intricate details of reading and writing data to a storage device, using standard data formats. This saves application developers a lot of time and effort—but just as important, it reduces the chaos and complexity that often results from every application doing the task its own way.

Key components of an IoT platform can include everything from hardware devices deployed in the field, to large mission-critical applications used by executive management to drive the business. The integration of these relatively simple components into a comprehensive network of mission-critical infrastructure is an important and complex undertaking that can drive business value and competitive advantage for organizations that are able to do it effectively.

IoT platform components comprise the backbone of a network of hardware, software, data, and application components that together provide the means to take simple bits of data and transform them into powerful corporate tools. Figure 1 illustrates the core components in a typical IoT platform.

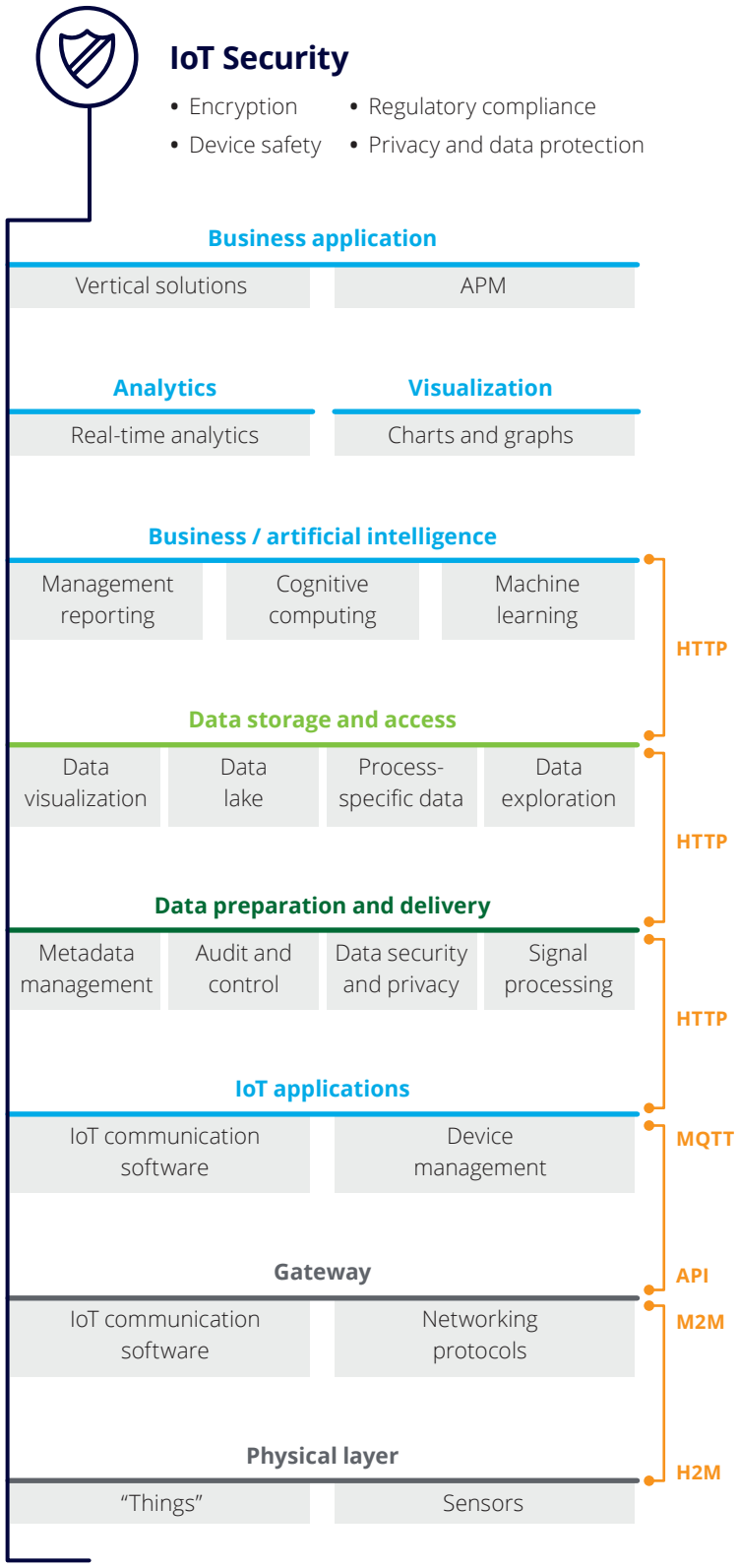


Figure 1: Key IoT platform and integration points

Physical layer. The physical layer of the IoT platform contains the hardware and physical components needed to begin to capture and transmit sensory information.

Gateway. The gateway layer controls the transmission and communication aspects of the IoT platform and provides a standard set of communication protocols to take sensory information from a device and transmit the data throughout the platform.

IoT applications. The IoT application tier contains the software components and device/event management software used to rationalize and make decisions about where to store data based on the parameters outlined in the application set.

Data preparation & delivery. In the data preparation and delivery layer, metadata analysis is performed and rules around data sensitivity and access can be applied. Checking for completeness and accuracy typically occurs within this layer (coupled with data security to protect critical information and assets).

Data storage & access. The data storage and access layer is where sensory data meets data classification rules to provide a subset of data capable of powering business analytics and visualization tools. In this layer, it is common to combine other data sets from ERP applications and/or data warehousing solutions to provide additional insight and context to the sensory information.

Business/artificial intelligence. This is the point where sensory information starts to be used to drive business decisions. Applying advanced analytics, cognitive technologies, and artificial intelligence to information gathered at the sensor level allows businesses to move from reporting and visualization to making real-time decisions automatically.

Analytics & visualization. Visualization takes analytics to the next level, compiling vast data sets into data models and interfaces that provide deep and compelling insights into the state of the business based on the information fed from IoT devices.

Business application. In addition to analytics and data visualization, sensory information can be integrated into large-scale, comprehensive applications that are critical to business processes. This integration enables vertical integration of the IoT solution into business platforms that would otherwise be operated manually or without real-time data feeds.

Secure by design

"Secure by design" is the inclusion of security design principles, technology, and governance at each and every stage of the IoT journey. When an organization looks at creating, deploying, and leveraging connected technology to drive its business, security must be integrated into every component, tier, and application to preserve the integrity of the IoT solution and minimize the risk of cyber threats.

IoT technology requires a broad set of capabilities to help organizations achieve high levels of cybersecurity. IoT platforms have numerous built-in security features, such as user access control, secure network protocols, and data encryption capabilities, that can all be leveraged. But that's just the beginning.

Developing IoT solutions around a standard platform allows organizations to develop security solutions for IOT devices in a consistent manner. In contrast, when organizations develop IoT platforms from scratch, it can unknowingly increase the potential for cyber-related risks. IoT platforms typically include standard tools and methods that can promote good design habits and help developers build strong security into their solutions from the outset.

In addition, IoT platforms are commonly designed and tested holistically to validate that there is a high level of security deployed at every level, not only within individual components but for all components working together as a whole.

And because platforms are used by more than one company, they benefit from "real-world" testing that helps expose hidden or otherwise unknown vulnerabilities.

That being said, platforms also have the potential to increase cyber risk because they provide a bigger and potentially more lucrative target for attack. Hackers that find a vulnerability in a platform typically don't just gain access to one system, but to many or all systems that use the platform.

Secure. Vigilant. Resilient.

As organizations expand their connected landscape and increase the footprint of their device network, the threat of cyber-attacks naturally increases. To protect themselves, organizations may focus their budget dollars and technology on being secure and "closing the doors" within their organization, which can hinder the ability to identify and respond to cyber incidents.

As more connected technology is deployed throughout an organization, leaders should be asking key questions about their IoT solutions: Are we really protected? How do we know if we have been breached? Can we respond effectively to a cyber incident? How will we recover?

Organizations that ask these questions soon realize that having a strong security model isn't just about being secure; it's about being ***secure***, ***vigilant***, and ***resilient***.

What does "secure, vigilant, and resilient" mean in the context of IoT?

- **Secure.** Your actual defenses and the associated components and capabilities. Like fences and locked doors in the physical world, these are the mechanisms designed to keep bad actors out.

  Key question: "Are we really protected?" Secure IoT requires hardening the end-to-end solution. Organizations should include secure components—such as secure code scanning, vulnerability management, application security, and identity/access management into each tier of the IoT landscape.

- **Vigilant.** Your early warning system. Like security cameras and a guard at the front desk, capabilities in this area help sense, detect, and predict cyber threats before they become attacks; attacks before they become breaches; and breaches before they become crises.

  Key question: "How do we know if we've been breached?" Being vigilant around IoT requires having the people, processes, and technology components to identify network and physical vulnerabilities, identify known and unknown assets, and periodically test protection levels. Asset discovery tools and the inclusion of analytics, operations centers, and security information and event monitoring (SIEM) tools allow organizations to identify threats and take corrective action before issues develop into full scale cyber-attacks.

- **Resilient.** The ability to manage cyber incidents effectively—responding quickly to minimize the damage from an incident, and getting the business and operations back to normal as quickly as possible.

  Key question: "Can we respond effectively to a cyber incident?" As the use of IoT technology continues to grow, so does the threat landscape for connected devices. Being resilient is having the ability to respond to a cyber crisis. As IoT solutions become more prevalent, a cyber threat, if improperly managed, can bring an organization to its knees, as we have seen in previous distributed denial of service (DDoS) attacks. Understanding potential impacts to the device network—and having response plans to quickly recover from a cyber event—is increasingly critical to mitigating risks and achieving the expected benefits of a connected device architecture.

A secure IoT platform can help you strengthen your organization's capabilities by:

1. Making your IoT devices and network more attack-resistant;
2. Allowing you to spot attacks and IoT threats early so you can prevent or address them quickly or pro-actively; and
3. Enabling your IoT operations to efficiently contain the damage from a breach and bounce back quickly.

Cybersecurity capabilities to look for when choosing an IoT platform

IoT platforms are still maturing, and their features and capabilities vary widely. Here are some key cybersecurity capabilities to look for within the major elements of the IoT platform.

Physical layer

Connected physical devices—from medication pumps to industrial thermometers—are the reason for IoT's existence, and are often business-critical. Security within this layer is very important—whether it involves maintaining physical security around the IoT devices themselves, or maintaining device patch levels and managing passwords. Organizations should strive to have robust asset discovery solutions to identify, monitor, and manage new devices as they enter the IoT landscape.

Gateway

As physical devices and sensors collect data, they need to transmit it securely across the IT/OT network, which may include corporate, public, or vendor-hosted networks, and complicated technology stacks. The integrity and security of this transmission is vitally important, making it essential for an organization to secure the entire pipeline from device to data center as part of the IoT security program. Strong network security, network segmentation, and encryption are all key components to consider when transmitting IoT data.

IoT applications

With IoT platforms and applications becoming more sophisticated, the security standards and methodologies used to manage them within the organization must evolve as well. IoT applications are one of the first stages where logic is applied to raw data. Validating that custom applications are secure, and that only authorized users have access to them, is a core component of deploying IoT applications.

Data preparation & delivery

As data moves through the IoT network and begins to be collected and categorized, data integrity becomes an important factor. In many organizations, this is where data meets a technological fork in the road and either heads to the cloud for further storage and analysis or is transmitted to other data staging areas for further compilation and processing. In both of these scenarios, it is essential to have secure communication channels and robust access control solutions in place to safeguard against data exfiltration or manipulation.

Data storage & access

At this stage, data arrives in the data warehouse and is ready to be stored. Having strong infrastructure, database, encryption, and identity/access management components are key for securing data in storage.

Business/artificial intelligence

Here, sensory data meets artificial intelligence (AI). Organizations take data feeds from interconnected devices and make real-time business decisions using programmed logic, bots, artificial intelligence, and machine learning. Organizations can use this real-time insight for a wide range of business decisions, such as buying additional products, planning maintenance, or changing production lines. As adoption of AI, automation, and machine learning increases, it is important to tightly monitor and control access to these solutions to reduce risk.

Analytics & visualization

This is where big data enters the picture. At this stage, organizations take data from interconnected devices and combine it with data from other sources to make corporate- and board-level decisions, using information from sensors and dashboards to monitor performance. Tight application security principles should be used to validate that individuals have appropriate access to the reporting tools and technology required to drive the business. Secure access control protocols are increasingly important here.

Business applications

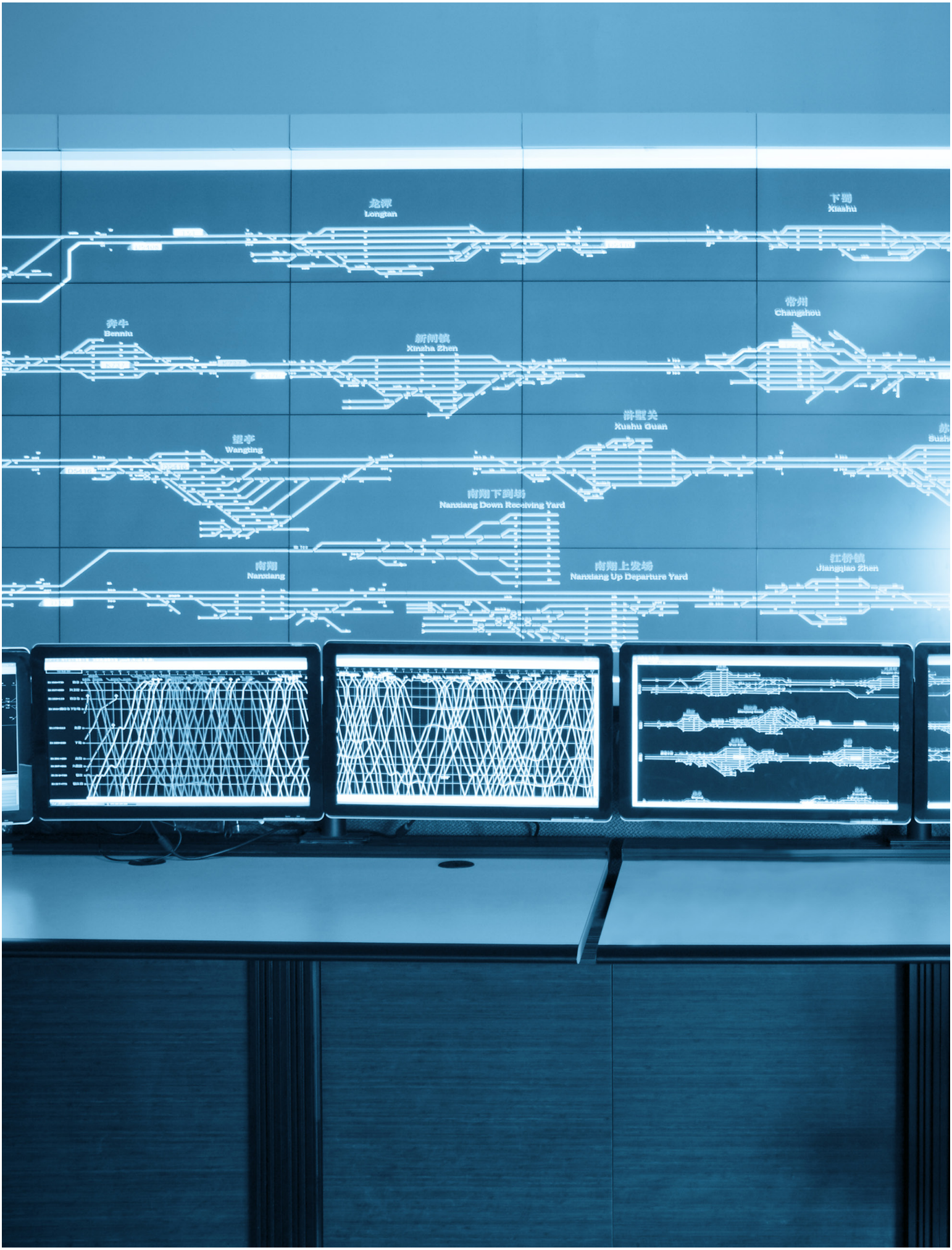
At the top of the IoT architecture sits the enterprise applications. These business applications translate the simple data collected at the sensor level and transform it into a powerful corporate asset. End user populations—including executive management, customers, vendors, and suppliers—commonly and routinely interact with the IoT platform on this level. Having appropriate security measures to control access to these critical applications—as well as ways to enable secure access—are vitally important issues.

Harnessing the power of the platform

The potential benefits of IoT are tremendous, but so are the associated cyber risks. To strategically leverage IoT, organizations can take advantage of the enhanced cybersecurity capabilities built into IoT platforms and actively identify and address cybersecurity issues at the intersection points between IoT platforms and existing infrastructure, data, and applications.

Although IoT platforms are still maturing, with the right approach they can be intrinsically more secure than stand-alone IoT solutions. In addition, they can help organizations accelerate time-to-value by making the development and testing of IoT solutions faster, more consistent, and more efficient.[2] This can be the case even for organizations that have previously built IoT applications without help from an IoT platform. Whether your organization is just getting started with IoT or is already well down the path, now is the time to look at harnessing the power of IoT platforms to boost cybersecurity in every facet of your IoT solutions.

[2] Deloitte Consulting LLP, "Turnkey IoT solutions," www2.deloitte.com/us/turnkeyiot


龙潭
Longtan
下坝
Xiaba
常州
Changzhou
奔牛
Bennu
新闸镇
Xinzha Zhen
望亭
Wangting
浒墅关
Xushu Guan
南翔下到场
Nanxiang Down Receiving Yard
南翔
Nanxiang
南翔上发场
Nanxiang Up Departure Yard
江桥镇
Jiangqiao Zhen

Authors

Sean Peasley
Partner
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 714 334 6600
speasley@deloitte.com

Tyler Lewis
Principal
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 214 840 1072
tylewis@deloitte.com

Brian Wolfe
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 215 430 6943
bwolfe@deloitte.com

Robert Schmid
Managing Director
Supply Chain & Network Operations
Deloitte Consulting LLP
+1 408 805 5450
roschmid@deloitte.com

Mahesh Chandramouli
Senior Manager
Supply Chain & Network Operations
Deloitte Consulting LLP
+1 214 840 1559
mchandramouli@deloitte.com

Deloitte.