Simplifying IoT at the Edge

Overcoming IoT Complexity with Flexible Device Management

arm | CIO DIVE

Custom content for Arm
by **CIO Dive's Brand Studio**

The IoT is Many Things

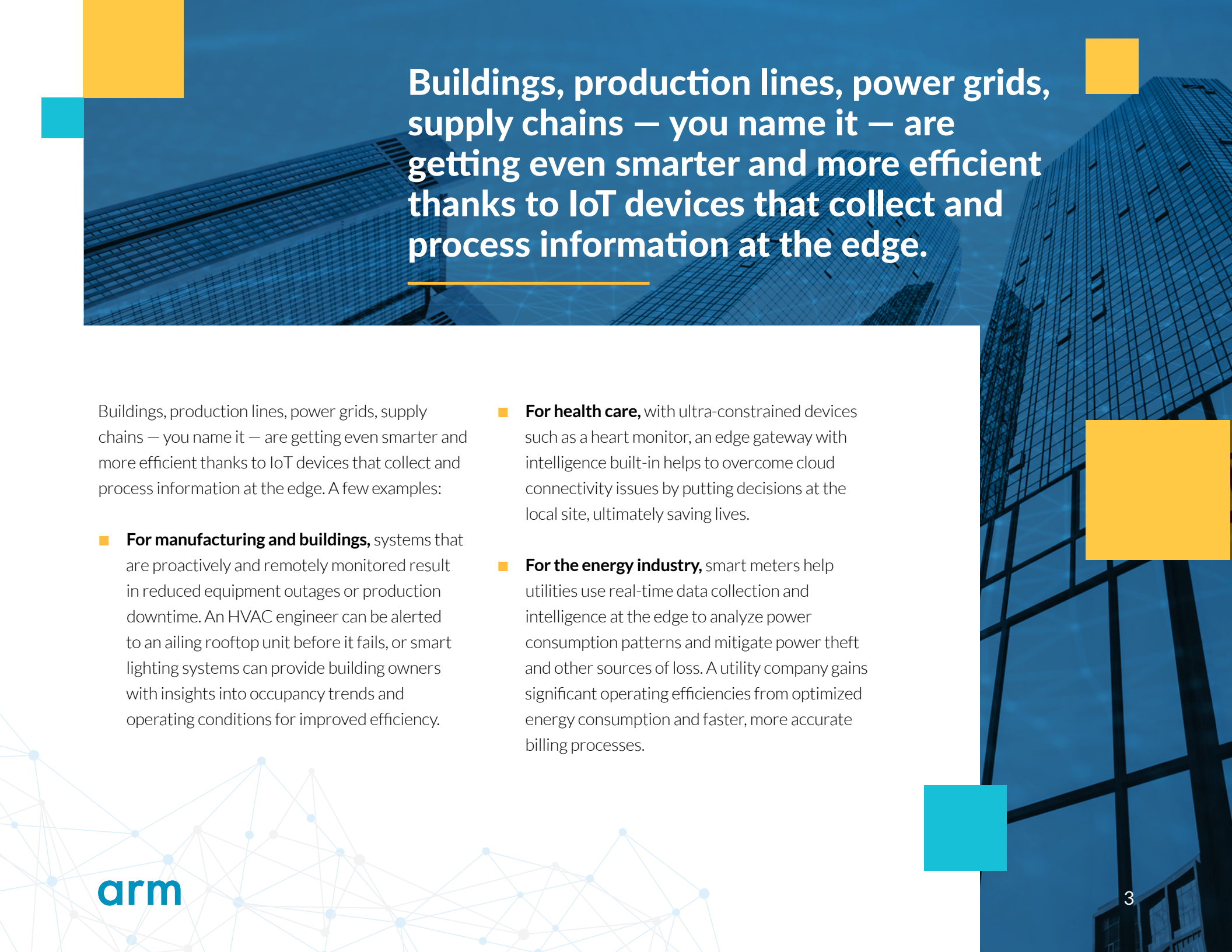
Efforts to leverage automation and data exchange are accelerating across industries, with 58% of companies surveyed worldwide for the Economist Intelligence Unit IoT Business Index 2020, reporting they are deploying IoT technologies for internal use[1]. Digital transformation initiatives are raising the bar for operating efficiency, setting the stage for more significant innovation. The Internet of Things (IoT) and its application in the industrial segment, commonly referred to as Industry 4.0, is a great enabler. Integrating with technologies such as artificial intelligence (AI) and machine learning (ML), the IoT device estate is made up of a broad array of sensors, actuators, and systems, including machines, tools, and other electronics.

As organizations race to find or maintain a competitive advantage, they are turning to IoT as a catalyst for change.

Enabling the Edge

Just as technologies are advancing what's possible — think 5G, AI, and ML — the proliferation of IoT data is already changing edge computing. Pervasive ML and analytics demand higher compute loads, requiring more bandwidth and without local computing resources, systems would bog down, adding to latency, operational costs, and business risk.

Advances in sensor technologies and dynamic ML modeling drive increasing amounts of data to be collected and processed in primary applications right at the edge. IoT edge gateways connect old and new systems, empowering organizations to automate with data collection and management at its endpoints — without ever going to the cloud.



Buildings, production lines, power grids, supply chains — you name it — are getting even smarter and more efficient thanks to IoT devices that collect and process information at the edge.

Buildings, production lines, power grids, supply chains — you name it — are getting even smarter and more efficient thanks to IoT devices that collect and process information at the edge. A few examples:

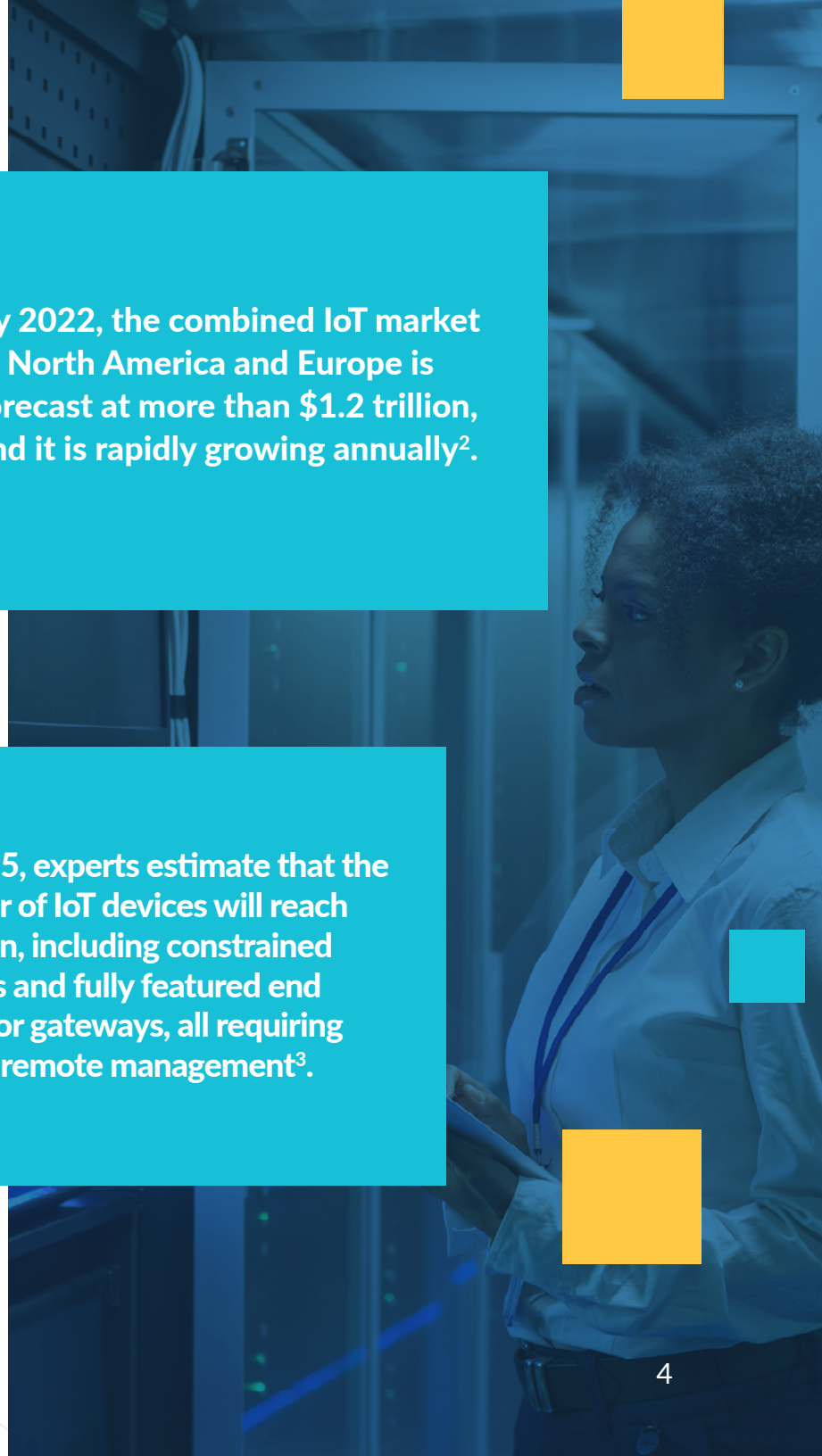
- **For manufacturing and buildings,** systems that are proactively and remotely monitored result in reduced equipment outages or production downtime. An HVAC engineer can be alerted to an ailing rooftop unit before it fails, or smart lighting systems can provide building owners with insights into occupancy trends and operating conditions for improved efficiency.
- **For health care,** with ultra-constrained devices such as a heart monitor, an edge gateway with intelligence built-in helps to overcome cloud connectivity issues by putting decisions at the local site, ultimately saving lives.
- **For the energy industry,** smart meters help utilities use real-time data collection and intelligence at the edge to analyze power consumption patterns and mitigate power theft and other sources of loss. A utility company gains significant operating efficiencies from optimized energy consumption and faster, more accurate billing processes.

arm

With properly provisioned, edge computing, answers are delivered where they're needed, at business speed, reducing cost and minimizing risk. The benefits of edge computing are well documented and include:

- Faster, localized processing means faster access to data with a greater ability to make decisions when it matters most, supported by analytics to deliver insights, consuming fewer resources.
- Improved latency, reduction of bandwidth requirements, and enhanced privacy guarantees that confidential data never leaves the premises or the regulatory jurisdiction.
- More responsive networks result from real-time information. Setting reduced risk and faster data relay aside, cost savings include reduced data center and cloud costs.

Typically, what determines an enterprise's chances of future success is a better understanding of their market, their competitors, and their customers. The growing amounts of IoT data — facilitated by an expanded device estate — is now a crucial source of business-informing intelligence and helps deliver transformational insights. As a result, how you deploy and manage IoT devices and applications over the life cycle requires serious consideration.



By 2022, the combined IoT market in North America and Europe is forecast at more than $1.2 trillion, and it is rapidly growing annually[2].

By 2035, experts estimate that the number of IoT devices will reach 1 trillion, including constrained devices and fully featured end nodes or gateways, all requiring secure remote management[3].

Identifying the Challenges of Connected IoT Devices and Edge Computing

For the digitally astute enterprise, maintaining and developing a device ecosystem — from dozens at a single facility or many thousands across locations and borders — can be daunting. For instance, combining multiple edge-computing platforms is a common practice, but unfortunately, many of these systems also bring the technical debt of proprietary APIs and runtimes.

"Many legacy IoT edge systems already deployed have been there for eight to 10 years or more in a typical scenario. It's not feasible for most organizations to go and replace every piece of a legacy system," said Deepak Poornachandra, senior product manager at Arm, a leading microprocessor developer and provider of IoT technology and software.

"The management and maintenance of devices are vital as people attempt to come to grips with the complexity of their IoT ecosystem. And, of course, there are continuous maintenance requirements that run the course of the entire life cycle," said Vijay K. Madisetti, Ph.D., consultant and professor of electrical and computer engineering at Georgia Tech.

When approaching how to manage an expanded IoT device estate, one that's building on previous implementations, here are the leading challenges enterprises face:

- **Protocol translation:** Vast numbers of devices cannot connect directly to the cloud, whether non-IP devices or legacy devices using proprietary protocols.
- **Edge computing:** Data aggregation is overwhelming because of a massive increase in device volumes, and it's not practical to store or transmit all of it.
- **Integration and scalability:** Being able to integrate new systems and upgrade existing infrastructure to be reliable, scalable, and flexible is essential.
- **Gateway management and security:** Authentication and security guarantees are crucial; trusted insights can be obtained only from trustworthy data.

Many enterprises also grapple with how to transition from a tactical, data-driven IoT model to one that is more value-based and strategic. Increasingly, they seek to combine both streaming IoT data and mined data using well-established Big Data sources and techniques. The integration of new IoT data with an existing data lake can lead to powerful cross-application insight and help drive enterprise-scale predictive analytics. Think analytics and customization when considering how to push out the right information to the right people at the right time.

"There's a greater requirement for customization of IoT devices to understand what its value is to you and your business processes. It requires programmability and the value that can change over time,"

— Vijay K. Madisetti, Ph.D., consultant and professor of electrical and computer engineering at Georgia Tech

A Platform Approach to Manage the IoT Device Ecosystem

In light of these challenges, the management of IoT devices and applications requires a strategic perspective when planning, implementing, and managing your IoT ecosystem. When researching an IoT ecosystem partner to provide control of your IoT devices, consider the depth of services needed to achieve the unique requirements of your ecosystem, including connection technologies and application enablement capabilities.

Especially with edge devices, gateways are critical to ensure high availability. That could be the swift recovery from hardware failure or if the site loses connectivity to the internet and cloud-based services.

To this end, a provider must be able to support a wide range of communication technologies and protocols to maximize connectivity and to adapt to any regional limitations. This is particularly important for locations with limited or unreliable cloud connectivity.

Especially with edge devices, gateways are critical to ensure high availability. “For example, I might provision a LTE-based backhaul connection, so the building or factory can continue operations seamlessly, regardless of cloud connectivity, and I could still remotely program the gateway and the devices that end up connecting to it,” Poornachandra said.

A holistic IoT device management solution can manage a diverse, growing set of IoT edge devices across facilities to support the enterprise in mitigating complexity in these critical areas:

- **Protocol translation:** Allows management of legacy non-IP devices, in addition to devices without direct cloud connectivity, alongside IP-connected devices.
- **Gateway management:** Minimize costly downtime with event management and diagnostic capabilities.
- **Edge computing:** Process rules and data at the edge, even if the gateway loses connectivity to the cloud, while reducing cloud costs and saving network bandwidth.

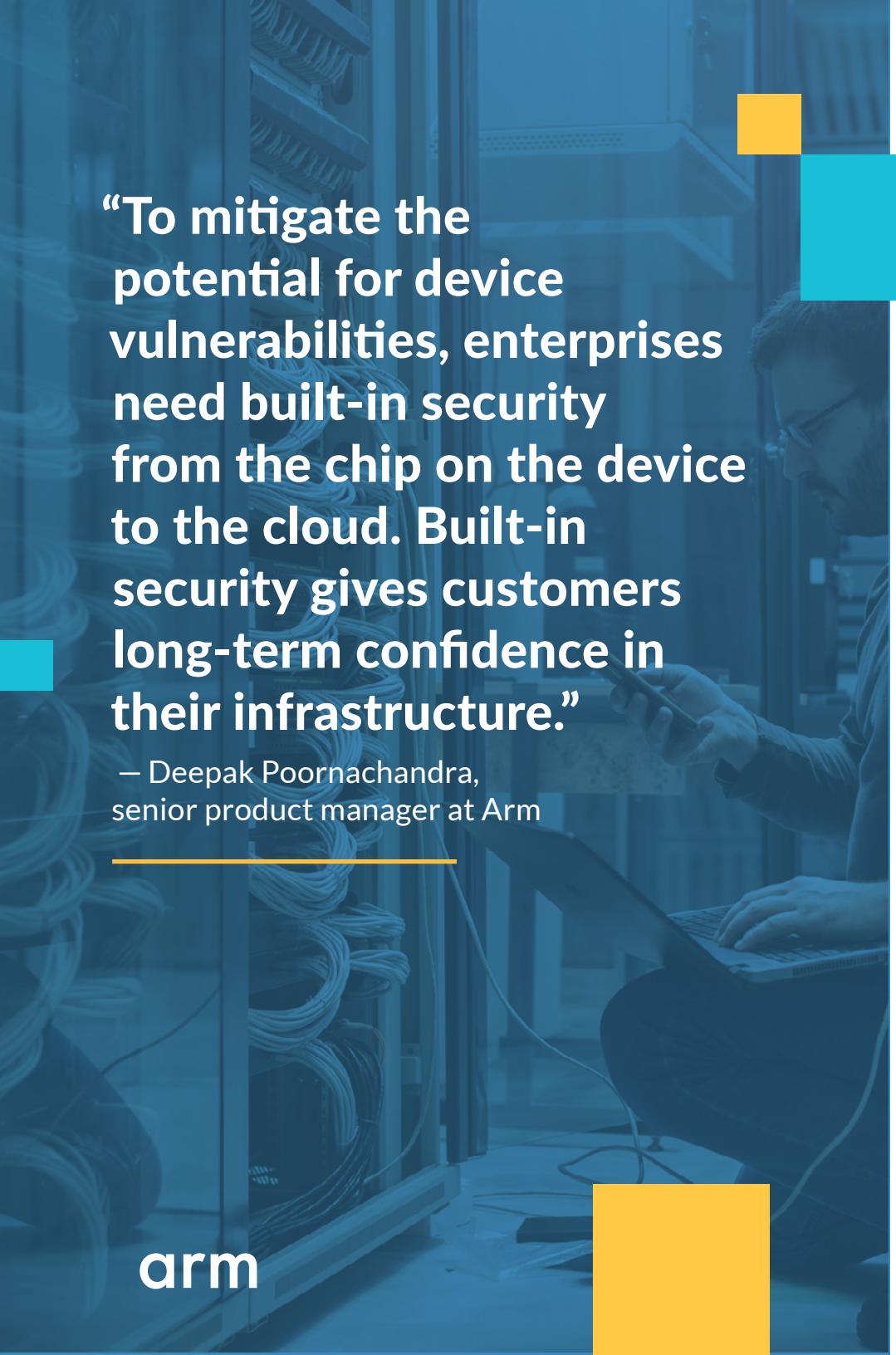
Addressing Cybersecurity

Secure interaction with IoT devices is one of the most challenging aspects of IoT development. An increase in bandwidth, computing needs and data streams coming from sensors and devices, puts a greater focus on the security of edge devices.

A foundational approach to edge security is needed to thwart cyberattacks. These are increasingly sophisticated and varied across physical devices, networks, and communication protocols. This strategy requires selecting secure hardware, establishing trusted connectivity from the device to the cloud, and creating layers of security throughout the individual components that constitute the IoT solution.

Achieving the required level of trust in the IoT ecosystem also requires decentralized rather than centralized management, Madisetti said, which will ultimately allow devices to manage and verify themselves. "If the information that we see when they send data is going to be protected and secure, this verification is built into the architecture, and for millions of devices, a decentralized self-certifying architecture is better." He cited the three pillars of security:

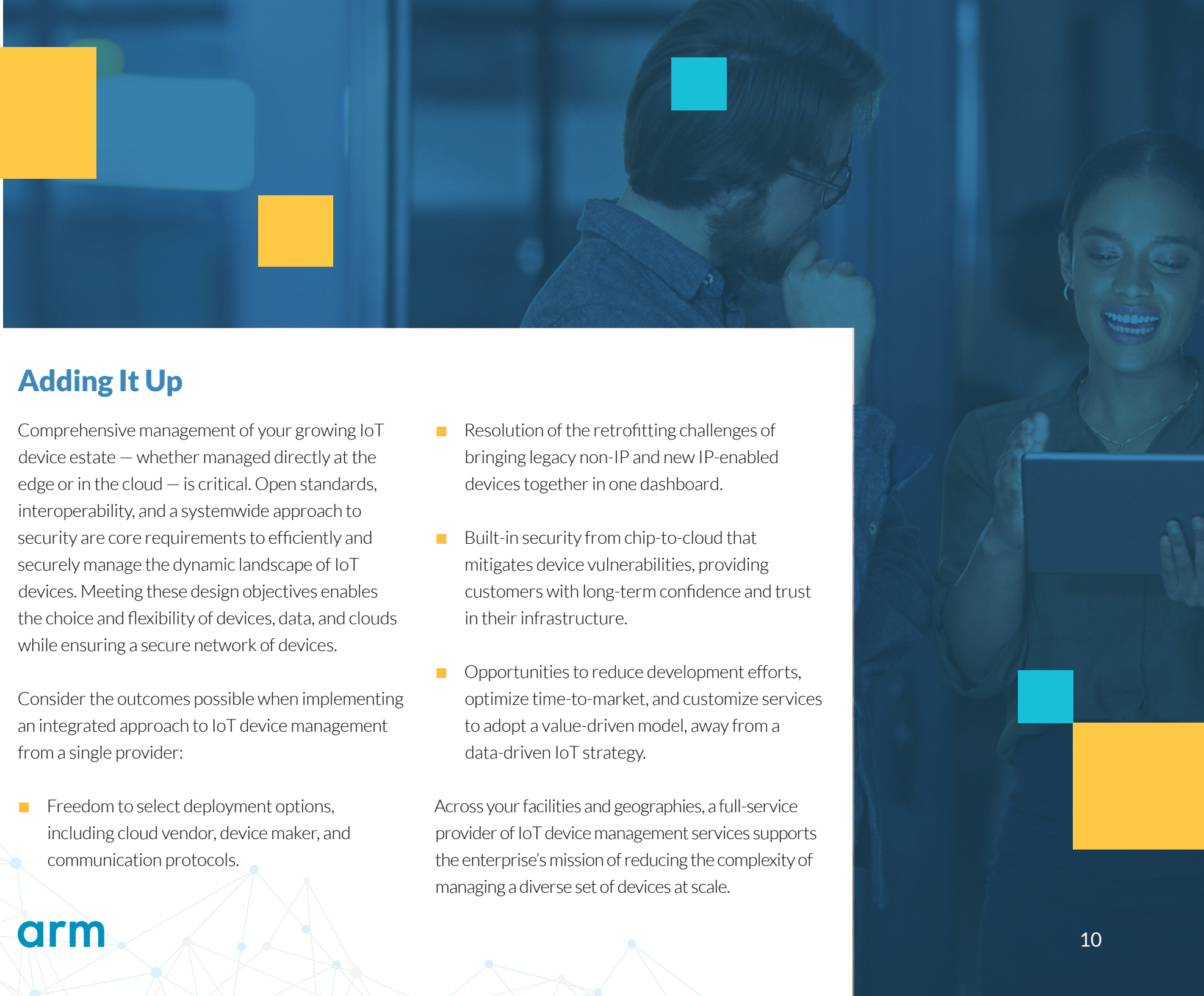
- **Confidentiality:** No one can see what you are sending.
- **Authentication:** Users are verified.
- **Integrity:** No one can change the message you are sending.



“To mitigate the potential for device vulnerabilities, enterprises need built-in security from the chip on the device to the cloud. Built-in security gives customers long-term confidence in their infrastructure,” Poornachandra said, noting a system-wide approach to security is what’s required, one that covers the physical device as well as the network.

“There’s no one, single model for trust currently,” Madisetti said. “You have to rely more on the manufacturer-led initiatives of the device to provide something reliable and trustworthy.”

Across the IoT device ecosystem, platforms must be able to work with manufacturers and solution partners to address security holistically. Platform Security Architecture (PSA) is an open standard framework, developed by Arm and alongside key industry partners, which enables the ecosystem to build on a standard set of ground rules for both constrained and resource-rich devices. PSA seeks to empower manufacturers and partners worldwide to better understand the requirements of designing, developing, and securing IoT devices at the endpoint, no matter their role. PSA simplifies secure software development by offering reusable components and open APIs to test implementations with elements such as Arm’s Trusted Firmware and PSA Developer APIs.



Adding It Up

Comprehensive management of your growing IoT device estate — whether managed directly at the edge or in the cloud — is critical. Open standards, interoperability, and a systemwide approach to security are core requirements to efficiently and securely manage the dynamic landscape of IoT devices. Meeting these design objectives enables the choice and flexibility of devices, data, and clouds while ensuring a secure network of devices.

Consider the outcomes possible when implementing an integrated approach to IoT device management from a single provider:

- Freedom to select deployment options, including cloud vendor, device maker, and communication protocols.
- Resolution of the retrofitting challenges of bringing legacy non-IP and new IP-enabled devices together in one dashboard.
- Built-in security from chip-to-cloud that mitigates device vulnerabilities, providing customers with long-term confidence and trust in their infrastructure.
- Opportunities to reduce development efforts, optimize time-to-market, and customize services to adopt a value-driven model, away from a data-driven IoT strategy.

Across your facilities and geographies, a full-service provider of IoT device management services supports the enterprise's mission of reducing the complexity of managing a diverse set of devices at scale.

arm

Sources

1. Economist Intelligence Unit IoT Business Index 2020 , "IoT Fortunes Rising Fast: The Economist Intelligence Unit Index 2020," February 18, 2020. https://www.arm.com/blogs/blueprint/economist-2020-iot-investment

2. Miller, Lawrence R. IoT Solutions For Dummies®, 2nd Arm Special Edition, John Wiley & Sons, Inc. 2020.

3. "Arm Techcon: At the Heart of the Technology World," August 27, 2019. https://www.arm.com/blogs/blueprint/arm-techcon-fifteen-years

ABOUT PELION IoT PLATFORM

The Pelion IoT Platform is a flexible, secure, and efficient foundation spanning connectivity, device, and data management. The platform accelerates the time-to-value of your IoT deployments by helping you connect trusted IoT devices on global networks, facilitating seamless administration and the ability to extract trusted, real-time data to drive transformational insights and competitive advantage.

ABOUT ARM

Arm technology is at the heart of a computing and connectivity revolution that is transforming the way people live, and businesses operate. Our advanced, energy-efficient processor designs have enabled intelligent computing in more than 160 billion chips, and our technologies now securely power products from the sensor to the smartphone and the supercomputer. In combination with our IoT device, connectivity, and data-management platform, we are also enabling customers with powerful and actionable business insights that are generating new value from their connected devices and data. Together with more than 1,000 technology partners, we are at the forefront of designing, securing, and managing all areas of computing from the chip-to-cloud.

LEARN MORE

Industry Dive's Brand Studio collaborates with clients to create impactful and insightful custom content. Our clients benefit from aligning with the highly-regarded editorial voice of our industry expert writers coupled with the credibility our editorial brands deliver. When we connect your brand to our sophisticated and engaged audience while associating them with the leading trends and respected editorial experts, **we get results.**

LEARN MORE