arm

White Paper

Building a strong IoT solutions foundation for 1 trillion devices

Continued advances in chip design, sensor technology, and machine learning make the bold predictions about the Internet of Things (IoT) look increasingly likely. But for the IoT to fulfill its potential and evolve at a global scale, organizations must address difficult challenges in several areas, including security, data management, and power.

"We see opportunities for cities and organizations to make plans using real-world, real-time information. They can now operate in a data-first, experiment-first way. That's rarely been possible before."

Damon Civin, principal data scientist at Arm

IoT innovation is happening now

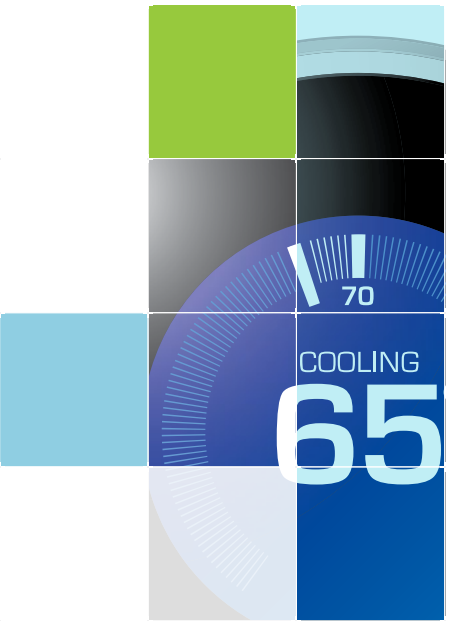
In Los Angeles, acoustic sensors attached to streetlights monitor noise levels to help ensure more peaceful streets and healthier citizens. Researchers in Scotland use smart telemetry tags to track and monitor the movement of endangered harbor seals. And auto manufacturer Daimler outfits its trucks with devices offering 3D maps, proximity control, and emergency braking assistance to improve driver safety. Welcome to the world of IoT where tiny sensors and vast networks are revolutionizing entire industries, from automotive to zoology. The opportunities are almost without limit—provided organizations manage the security, data management, design, and machine learning issues that arise from millions of interconnected devices.

"We see opportunities for cities and organizations to make plans using real-world, real-time information," says Damon Civin, principal data scientist at Arm. "They can now operate in a data-first, experiment-first way. That's rarely been possible before."

The success of early IoT deployments has generated strong interest across a range of public and private industry sectors. People now see much more than financial value in data. They recognize the array of benefits data provides and how it helps organizations plan with greater accuracy. This renewed appreciation for data is fueling intense demand for actionable analytics, which will play a critical role in a world with one trillion internet-connected devices.

Given the potential transformative effect one trillion devices will bring, it is no wonder worldwide spending on IoT is predicted to reach $1.4 trillion by 2021, according to IDC, as companies invest in IoT-related hardware, software, services, and connectivity.[1]

Similar to how the internet transformed the way information is shared and used, so too will the IoT. Consisting of massive clusters of connected devices—some linked via the internet and others behind corporate firewalls and built to leverage legacy systems—the IoT will unleash a new wave of information-driven value and innovation. Not all IoT devices will be linked, and each will offer unique capabilities depending on its purpose. But the cumulative value of one trillion data-generating IoT devices will be unprecedented.



The meaning of one trillion

While IoT solutions promise to transform everything from cities and transportation to healthcare and factories, there are significant hurdles ahead.

"There's not enough lithium production in the world to build one trillion devices," says Rob Aitken, a research and development fellow at Arm. "You'd either have to vastly step up lithium production or stop making electric vehicles. If we want to reach a trillion-sensor universe, we need to start thinking about energy harvesting."

Then there's the brain trust needed to design one trillion devices: Experts suggest it could require up to 200 million RF designers, 50 million IC design teams, and 50,000 coders. With the exception of coders, there aren't enough technologists at the moment to meet that demand. And as intelligent devices begin to communicate wirelessly with one another, they will push the physical—and regulatory—limits of communication bandwidth.

IoT must-haves

In addition to human capital and computing power, there are standards that one trillion devices must meet. For starters, they must be able to work separately. If a humidity sensor can't function properly on its own, then it's not worth connecting to a network of other devices.

Further, one trillion devices will generate enormous volumes of data. The key is for them to work better together in order to deliver meaningful information—bits and bytes that can be used to improve operations, predict maintenance issues, and even save lives.

One trillion devices must also work automatically. A network of one trillion devices is too complex to manage manually. As a result, machines must be able to quickly and effectively solve performance issues on their own without human intervention.

"Scaling IoT to one trillion devices requires restructuring a bunch of processes that are currently done manually and in a thousand different ways, and automating them in a standard fashion," Aitken says. "It's a huge job."

Additionally, IoT solutions need flexibility to take into consideration legacy systems behind corporate firewalls, in addition to cloud-based approaches. Many companies have long-established IoT systems that handle data that managers don't want in the cloud.

One trillion devices must work resiliently. In today's internet-connected world, a nefarious hacker or software design flaw can wreak havoc on an entire network. For this reason, intelligent devices must have built-in resilience to respond quickly to security issues, unanticipated failures, and general wear and tear.

Lastly, no single company will provide every IoT solution up and down the technology stack. The IoT's growth and success will depend on shared standards and a strong community of vendors. The companies that come out on top will be those that commit to innovation and build the most vibrant partner ecosystems.

Groundwork for IoT excellence

So how can organizations make sure the world's one trillion devices work separately, automatically, and resiliently? Organizations have to deal with critical challenges head-on in

the areas of security, data management, and device design. And they must prepare for more machine learning at the edge. The good news is that IoT provides more opportunities than risks, provided you do it in a responsible and principled way.

In fact, there are four ways for organizations to get a head start on tomorrow's one-trillion-device world:

- Put security first
- Get a grip on data demands
- Reconsider design
- Harness machine learning at the edge

Here's how to implement these strategies and what they mean for your business.

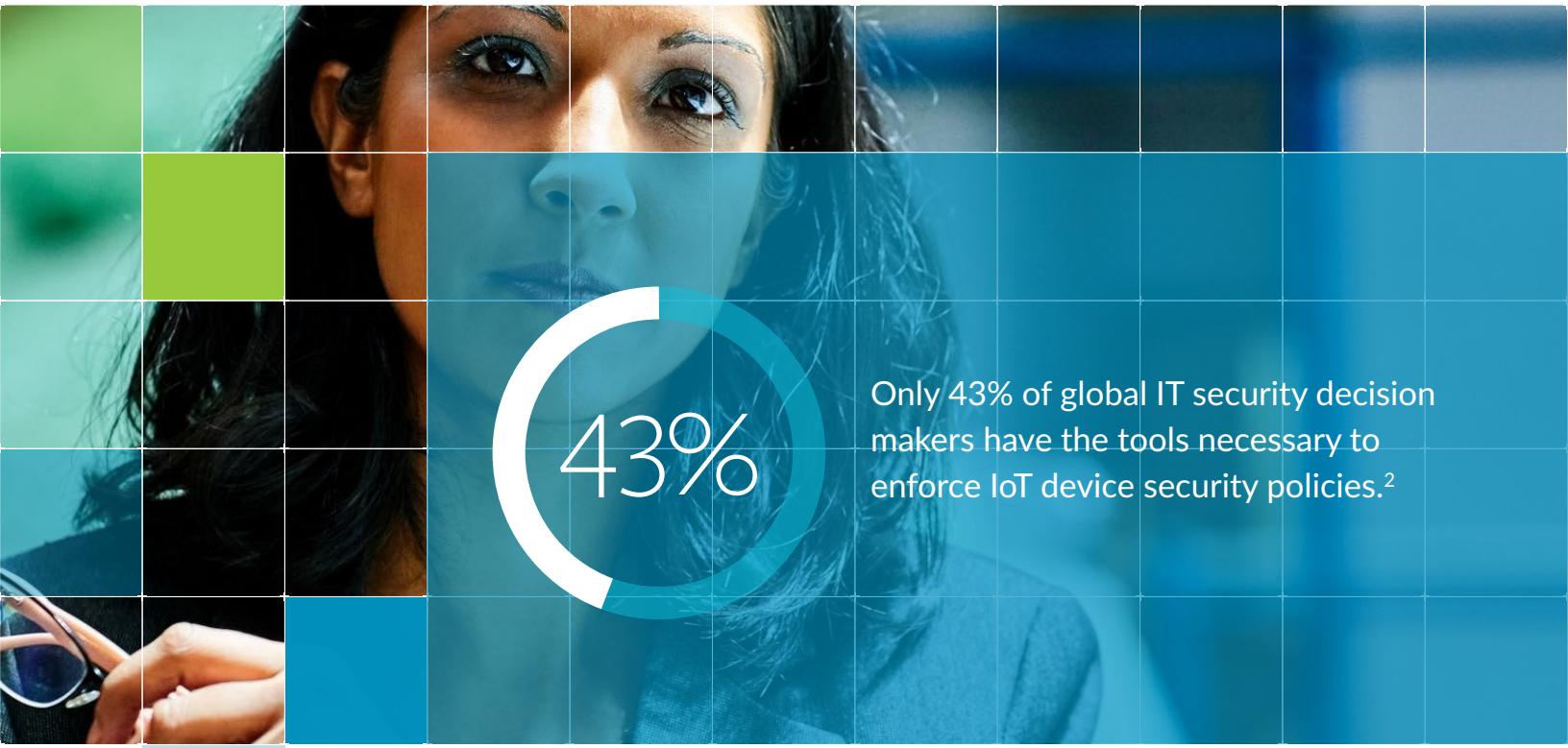
An expanding threat surface requires a heightened security focus from the edge to the cloud

1 - Put security first

Organizations have long battled ill-intentioned hackers, organized crime groups, nation-states, and disgruntled employees to protect their systems from security attacks. But with the rise of IoT, the stakes are higher than ever.

As today's network of interconnected devices expands, so does the attack surface area. Case in point: In late 2016, the Mirai botnet used 100,000 IoT devices to attack a service provider, knocking out a huge portion of the internet.

"As we expand toward one trillion devices, organizations must recognize that attempts to compromise the system will be constant," Aitken says. "Scaling to a one-trillion-device IoT requires a strong security strategy."



A uniform approach to safeguarding systems is imperative.

Yet many IT teams aren't prepared to properly safeguard their systems for an IoT future. According to Forrester's State of IoT Security 2018 report, 92 percent of global technology enterprises have security policies in place. But only 42 percent have the necessary tools to properly enforce these policies.[2]

It's the duty of every organization to provide robust cybersecurity to protect against threats—an obligation that requires heightened focus from the edge to the cloud.

The first step in security is taking an inventory of a system or network's vulnerabilities. Says Aitken: "There are simple exercises you can do, such as asking, 'What are the threats that I care about and how have I defended against them?'" It's important that organizations not only examine a network's intelligent devices, but also any legacy applications that have been integrated into an IoT system.

Next, organizations must prioritize security risks and deploy safeguards in a sensible order. "Assess threats along a spectrum, from those that are most to least likely to happen, and those that will cause the most and the least damage," advises Aitken.

However, "security is not magic," warns Diya Soubra, marketing manager for Arm. Indeed, organizations need a proper toolkit of security strategies and solutions. These include:

Threat containment
IoT solutions are increasingly being deployed across critical infrastructure networks. But in the event of a security attack, shutting down an entire system to prevent malware from spreading could be more damaging to an organization than the attack itself.

Rather, organizations require a system with detection at the edge nodes, with sensors capable of monitoring system and network traffic for unusual patterns. When an abnormality is detected, these nodes can be isolated or quarantined by changing or revoking access keys and redirecting traffic to a filtering host. This technique contains the problem and minimizes system disruptions.

Self-monitoring capabilities
"When you get to the one-trillion scale, you need a system that is automated and can monitor itself," Aitken says. The solution: a live and continuous monitoring system that relies on big-data analysis to inspect network behaviors and flag abnormalities. Loopholes are identified using statistical analysis on device types, firmware versions, system events, and traffic patterns of events leading up to the point of infection. From there, the system can block known malicious signatures and traffic patterns on network boundaries using centralized rules and block lists.

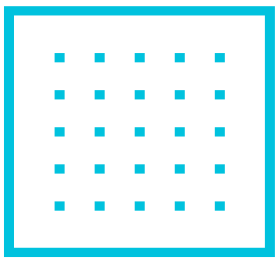
Fog computing appliances
By deploying fog-computing appliances to a local network, organizations can leverage computing power on local edge nodes for greater resilience—and fewer security risks. Appliances may range from a security-hardened low-cost WiFi router running some trusted software processes to a high-end tamper-proof rack server based on strong isolation and memory encryption. Either way, fog computing provides localized control, configuration, and management of IoT solutions without the security risks.

Machine learning
Attack algorithms are changing all the time, making it difficult for IT teams to stay ahead of hackers. Fortunately, machine learning promises to change all that by detecting and learning from outlier behavior to better identify security risks. In the case of known attacks, logs can be used to train neural networks, which can be deployed on edge devices. Neural networks can also be extended to automatically retrain as new attack methods emerge, so that IoT networks automatically adapt to new threats.

Currently, most machine learning takes place in the cloud, where servers sift through huge volumes of data, collected at the edge, in search of abnormal patterns. But as machine learning is pushed to the edge, organizations will be able to respond faster to security threats while reducing the hefty bandwidth requirements and costs associated with cloud computing.

"There is so much data available that it's fundamentally changing the way we do things."

Damon Civin, principal data scientist at Arm



Just as IoT technology connects devices, it can also connect industries.

Compartmentalize against compromise

The issue with processor architectures today is that if a processor becomes compromised, all the memory associated with it becomes accessible to a hacker. Fortunately, there are ways to erect a barrier between an application and attacker. "When you know you're going to be hacked, you have to divide everything into compartments," says Soubra.

Dividing applications into several different compartments ensures that each compartment offers access to only a subset of an application's memory. As a result, any compromise within a compartment is limited to the memory accessible in that compartment.

Although IoT security solutions vary, a uniform approach to safeguarding systems is imperative. A foundational framework can help by providing a more consistent, best practice approach to security that's scalable for all connected devices—be it one thousand or one trillion.

2 - Get a grip on data demands

With the volume of data doubling in size every two years, the digital universe is expected to reach 44 zettabytes by 2020, according to IDC.[3]

Much of this data will be generated by billions of interconnected IoT devices. From consumer behavior data to 3D seismic data, these morsels of information can help farmers find new ways to cultivate crops, retail stores provide tailored experiences for their customers, and cities build smart bridges.

By transforming entire industries, IoT-generated data can have an enormous impact on local and global markets. The IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion per year by 2025, according to a McKinsey Global Institute report.[4]

Yet most IoT data troves are untapped. The McKinsey report cites the example of an oil rig that has 30,000 sensors, but only examines one percent of its data. The value of IoT-generated data must be fully realized for organizations to move beyond simply creating consumer profiles and detecting anomalies to using data to predict security breaches and anticipate machine failures.

"Gathering data for the sake of gathering data isn't really helpful," Civin says.

Fortunately, there are ways organizations can glean increased insight from IoT data. Innovative use cases include attaching sensors to motorbike taxis to gauge air quality, tagging animals to monitor how wildlife is affected as cities grow, and keeping tabs on manufacturing machinery to predict and prevent system failures.

Just as IoT technology connects devices, it can also connect industries, enabling organizations to take the information they've gathered from one industry and apply it to another. For example, many big-brand retailers rely on weather data to drive revenue. If the data shows that a blistering heat wave is about to hit a particular city in the next three weeks, local retailers can stock up on inventory, such as portable fans and air conditioners, to boost sales and customer satisfaction.

"There is so much data available that it's fundamentally changing the way we do things," Civin says. The trick, he adds, is harnessing the data and "finding new ways to experiment with it."

3 - Reconsider design

Devices increasingly contain more and more sensors. Embedded processors relay growing amounts of IoT data. And platforms must now be able to orchestrate software applications that keep intelligent devices performing at optimal levels. This requires approaching IoT design with a fresh perspective on hardware and software design.

Apply hardware rules

Hardware use cases vary from simple sensors that can run for a decade on a coin cell battery to more complex RFID "smart tags" that track and monitor assets in real time. Despite these variations, there are several factors organizations must consider when designing or implementing any type of hardware for the IoT.

Energy efficiency: Running a powerline to sensors isn't always practical. At the same time, servicing and changing batteries can result in costly business disruptions. To better gauge IoT hardware energy efficiency, designers must consider the following factors:

- Energy profile, including the energy consumed when the device is awake and the energy consumed when the device isn't working
- MCU/CPU security
- Connectivity protocol (distance, power, security)

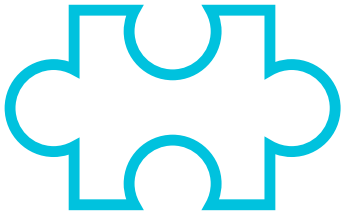
Architecture: Because most IoT devices are not plugged into an outlet, the main IoT chip must use a highly efficient architecture. Organizations can choose between off-the-shelf or a custom system-on-chip (SoC).

An off-the-shelf design requires a vast array of products so that the design is scalable. Users also need access to a menu of performance options and the ability to link to other intellectual property, such as digital signal processors (DSPs) to achieve sensor fusion.

A custom SoC is based on standard IP components and requires a wide range of tools and services to help produce the right design, from simulation and emulation to field-programmable gate array (FPGA) prototyping and bring-up. Fortunately, there is an increasingly number of low-risk ways to cost-effectively create and scale a custom SoC prototype.

Both off-the-shelf and custom SoCs require:

- Easy access to design tools
- Approved design houses (in the absence of in-house expertise)
- An established and expansive software ecosystem
- Foundry partners equipped with relevant IP to manufacture a chip in the most effective way possible



Off-the-shelf and custom SoCs share key requirements from design tools to foundry partners:

- Easy access to design tools
- Approved design houses (in the absence of in-house expertise)
- An established and expansive software ecosystem
- Foundry partners equipped with relevant IP to manufacture a chip in the most effective way possible

Software needs

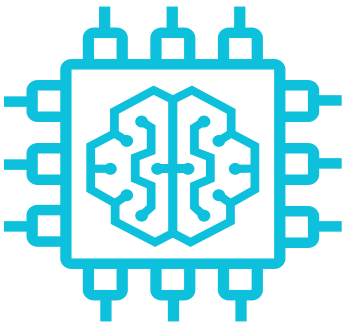
Today's IoT devices last longer than ever, challenging organizations to improve their software design. For starters, the longer the lifespan of a device, the greater the need for maintenance and monitoring. Other key considerations include the potential to unlock additional business value, address functional defects, and manage a constantly evolving security landscape. Currently, remote over-the-air software updates are one of the most efficient ways to distribute and install required software changes.

When writing software applications for IoT devices, it's important to balance functionality with power consumption. The most effective way to do this is to build applications on an operating system (OS) designed for the IoT. Such an OS will already take into account key factors such as power consumption, connectivity, and security, to name a few. And this means the application developer can focus more on the end-user experience.

Built-in security is another factor influencing hardware and software design decisions. The IoT is leading to smaller devices, but they must also be safer. For this reason, organizations are trying to embed as much security into a device as possible. And for good reason: Hardware-based security built into SoC processors can establish a root of trust and protect devices from security breaches.

The cloud also can play a critical role in keeping IoT devices secure. The right cloud-based platform can help manage and update IoT devices.

But it takes more than the right hardware and software design elements to accommodate one trillion devices. A very small percentage of the IT community today is really good at IoT design. However, by finding the right partner and tapping into third-party expertise, organizations can design and develop hardware and software solutions that increase IoT performance.



A one-trillion-device world will require increased machine learning at the edge

4 - Harness machine learning at the edge

Machine learning (ML), a subset of artificial intelligence (AI), is playing an increasingly important role in tomorrow's one-trillion-device world. Popular ML features such as predictive text, speech recognition, and computational photography are already powering one of today's most popular AI platforms—the smartphone.

But as innovative products like voice assistants and consumer robots enter the marketplace, AI's reliance on machine learning—where data models are built and used to make decisions automatically—is growing dramatically. And for ML to reach its potential, it will increasingly be deployed at the network edge.

A history of machine learning

In the past, edge devices didn't generate enough data or have the computing power to run ML and generate results. As data volumes grew, packets still had to travel over the internet, from one server to the next, and rely on ML functionality in the cloud. This is changing fast, as more ML is performed on devices, such as smartphones and smart speakers. As new purpose-built ML technologies are designed into next-generation chips for mobile devices, their ability to perform advanced functions will advance rapidly. This will transform the capabilities of IoT devices, even without an always-on internet connection.

Consider, for example, a smartphone's face-recognition technology or predictive typing—ML systems that run directly on a device. "We're heading to a world very soon where we'll move away from centralized intelligence in the cloud to a world of distributed intelligence everywhere," says Civin.

More sophisticated technologies are also finding a home at the edge. Take image recognition, for example. These systems can be trained to determine, with a high degree of confidence, whether they're looking at a child or a cat. Most of these systems

rely on transmitting data to the cloud. But some image recognition systems are simple enough that they can run on the device itself. The result: reduced latency, increased communications bandwidth, and improved user privacy and security.

Another example is smart lighting—street lights with built-in video cameras and real-time communication capabilities. Typically, a smart light would point to the pavement, determine if it's icy, and alert city officials. However, what if the smart light detects black ice for the first time? "A typical machine learning algorithm would fail at that point because it's never seen black ice before," Civin says.

By pushing computing to the edge, organizations can run ML algorithms in a new way through distributed learning, where what one device sees and learns can be shared almost immediately among other devices, he adds. This not only accelerates decision making, but also prevents data from having to travel over the internet.

Moving to the edge

Mimicking the learning and decision-making powers of humans isn't easy. To do so requires supporting algorithms that often require cloud-intensive compute power. And processors must take a big step toward boosting AI performance.

"Some of these machine-learning algorithms need so much power to train them," Civin warns. "We're moving into a world where we need to run machine learning in a way that's low power and available on really tiny devices. That's never really been possible before."

Although much of the ML workload runs at the edge on current CPU and GPU technologies, for ML to flourish it will need specific IP (ML and object detection processors) so increasing data loads can be handled faster and more efficiently.

Organizations must also develop new and innovative strategies for collecting data, learning from that data, and building effective training models to enhance the intelligence of systems.

This requires a long-term effort and investment. But when done right, ML will deliver greater efficiency, reduce the data tax on the network, increase data security, and ensure greater privacy. Distributed learning can also enable much more powerful and insightful data processing, enabling localized decisions on any edge device, be it a smart streetlight or a home appliance.

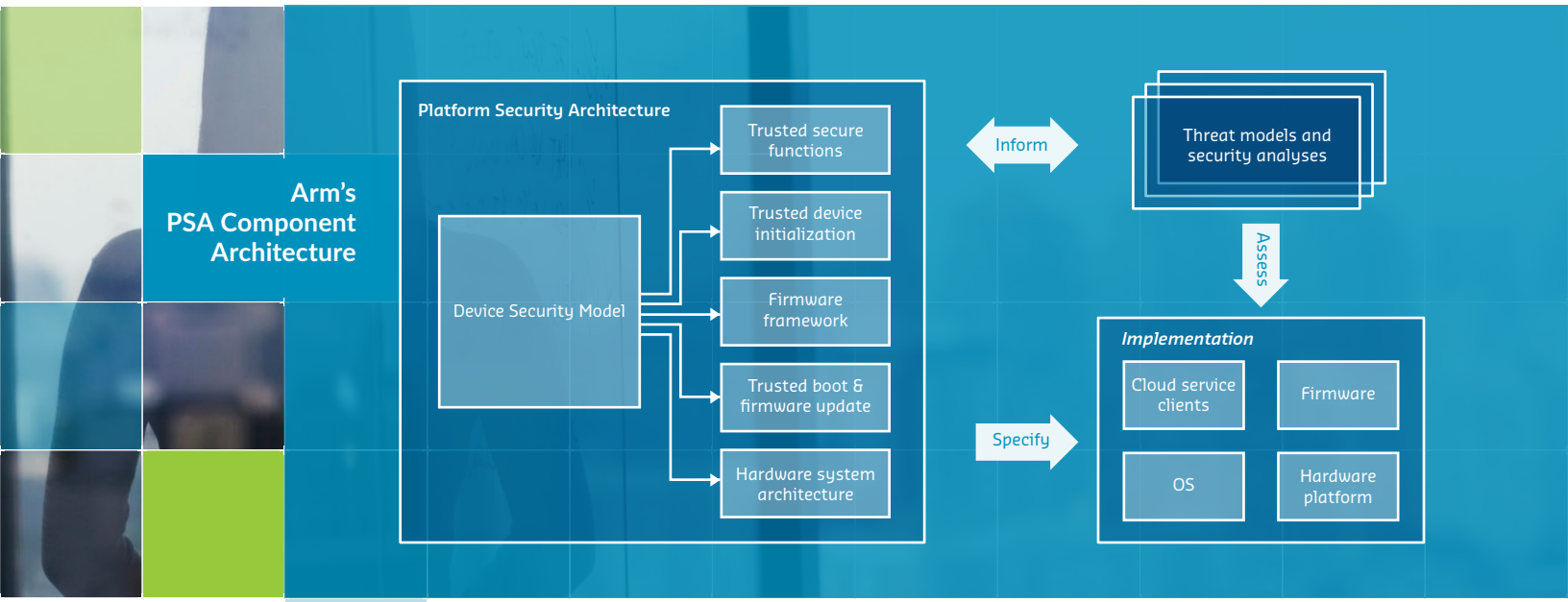
.

Answers to IoT

The urgency is clear: Connecting one trillion devices requires taking the necessary measures in security, data management, design, and machine learning. Here are a handful of Arm solutions that can help organizations begin to pave a path to IoT innovation—securely and efficiently.

Platform Security Architecture (PSA)

Given today's threat landscape, organizations can't afford to take any chances when it comes to the IoT. The more interconnected devices, the greater the exposure to security breaches and unauthorized access to sensitive information. The Arm Platform Security Architecture can help by providing a comprehensive set of threat models, security analyses, hardware and firmware architecture specifications, and an open source firmware reference implementation. The result is a more economical approach to built-in security for all connected devices.



Mbed IoT Platform

The Mbed IoT Platform is composed of device software and device management services to deliver a powerful, integrated device-to-cloud approach to the IoT. From a security perspective, the Mbed IoT platform secures the device, communications between device and cloud, and the lifecycle of the system. From a services standpoint, the Mbed IoT Platform provides device management services to ease deployment and lifecycle management.

Organizations can take advantage of cloud cost efficiencies with the Arm Mbed Cloud. It provides secure and scalable IoT management for any device, network, cloud, or on-premises requirements. Users can provision and connect a wide variety of IoT end nodes, along with cost effective and reliable software updates that can help extend product lifetimes.

TrustZone

TrustZone protects assets from software and hardware attacks by providing a trusted platform for system-wide security. The hardware-based security technology in TrustZone can be built into SoCs by semiconductor chip designers for secure endpoints and a device root of trust.

Conclusion

The world is on track to design, develop, and connect one trillion intelligent devices over the next two decades. With each new device, industries discover innovative approaches to satisfy customers, avert disaster, and develop new products and services.

But hurdles remain. Security breaches, unwieldy data, design flaws—they can all stand in the way of organizations deriving real value from the information they gather and analyze. Luckily, there are strategies, along with chips and design architectures, that can safeguard IoT systems and increase their value, including:

- Put security first
- Get a grip on data demands
- Reconsider design
- Harness machine learning at the edge

While these important strategies can advance IoT performance, spectacular strides also are being made in ML. From helping financial services firms react quickly to market trends, to enabling retailers to deliver real-time, tailored offers, ML is at the core of some of today's most compelling applications. And as industries find new ways to push ML out from the cloud to the edge into devices themselves, the opportunities IoT presents will only increase.

Businesses can accelerate IoT adoption and deployment by building a strong foundation that's composed of both hardware and software and designed for IoT devices. This approach provides organizations the flexibility and scalability to exploit new opportunities and unlock even more value from IoT data.

To learn more about building a strong IoT foundation, visit arm.com/iot

1. Worldwide Semiannual Internet of Things Spending Guide, IDC, June 2017
2. State of IoT Security 2018, Forrester, January 2018
3. The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, IDC, April 2014
4. Unlock the potential of the Internet of things, McKinsey Global Institute, June 2015

arm