GSMA Intelligence

pelion

IoT security for enterprises: make it work, make it easy

December 2020

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

Published December 2020

Authors:

Yiru Zhong, Lead Analyst IoT & Enterprise

Sylwia Kechiche, Principal Analyst IoT & Enterprise

This report was authored by GSMA Intelligence with support from Pelion

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Enterprises speak: key learnings

1. **Understanding of IoT security among enterprises is on the rise.** According to our survey, the proportion of enterprises that rate security as a key factor when choosing an IoT solution provider has increased to 57% in 2020, from 53% in 2018. Enterprises have also changed their security practices, with the aim of adopting a security-first approach as their USP. However, they are only at the start of this journey; when choosing vendors, they rely on who and what they know, and are not fully aware of the trade-offs needed to make an IoT solution secure.

2. **Enterprises trust cloud-based vendors to better meet their security needs.** Nearly 60% of those who picked security as a key purchasing factor trust cloud vendors to deliver the security features needed for their IoT deployments. The next cluster includes cloud-based solution providers such as business software firms, platform companies and service providers/application vendors. Those with connectivity-centric IoT offers such as mobile operators are lower down on their lists. This reflects the tendency of enterprises to deploy IoT mostly from an IT perspective.

3. **Enterprises are building security based on what they know.** Enterprises tend to address IoT security based on what they know about cloud security. They therefore understand the need to authenticate their IoT devices for the cloud; more than 70% of enterprises that picked security as a key purchasing factor rated device-to-cloud security as very important. They are also aware of increasing compliance needs, and rate as very important an IoT solution's adherence to regulatory and customer requirements.

4. **Enterprises lack readiness for day-to-day security operations.** Enterprises are far less likely to rate easy integration or day-to-day security operations as very important. This reflects a lack of awareness of the rapid rise in security complexity that occurs as deployments scale. Enterprises have not yet asked the right security questions of their IoT vendors in order to meet operational technology (OT) requirements.

5. **Enterprises need to balance IT/OT considerations when purchasing IoT solutions.** As deployments scale, enterprises need to include perspectives from IoT and OT teams to make a balanced decision between security, performance and cost.

The enterprise view in numbers

85% of enterprises have changed their security practices as a result of their IoT deployments.

61% of enterprises that have changed their security practices have done so with the aim of adopting a security-first approach as a competitive advantage.

57% of enterprises indicate that the security of a solution is the key factor when choosing an IoT vendor (versus 53% in 2018).

72% of enterprises see device-to-cloud security as very important, while 71% of enterprises see meeting regulatory and customer requirements as very important.

68% of enterprises rate as very important ongoing security management features such as easy integration with existing security policies.

59% of enterprises trust cloud vendors to meet their security requirements.

<40% of enterprises trust connectivity providers to meet their security requirements (with operators at 35% and MVNOs at 27%).

Enterprises have aspirations for a security-first approach

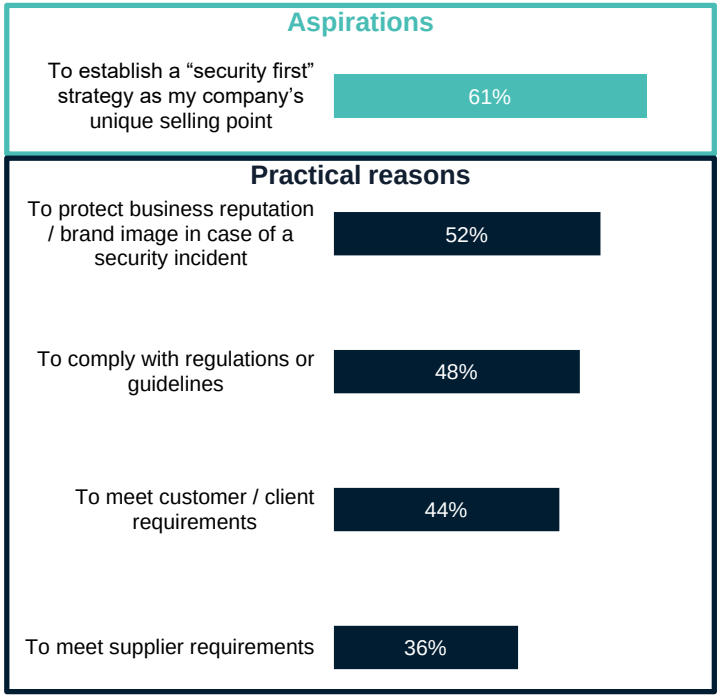
But practical issues still influence actions

61% of enterprises that have changed their security practices have done so with the aim of adopting a security-first strategy.

- **IoT security remains critical among enterprises:** 85% of enterprises indicated that they have changed their security practices as a result of their IoT deployments (largely unchanged from 86% last year).
- **Aspirations for a security-first approach:** More enterprises have changed their security practices to adopt a security-first approach and gain a competitive advantage (61%) than those that have changed for compliance reasons (36–48%). Such aspirations are more common among those with IoT deployments within the last 12 months (65% versus 61%).
- **When it comes to deployments, practical reasons trump aspirations:** Our panel all acknowledge enterprises being more aware of the importance of IoT security. They applaud enterprises' aspirations but have yet to see that sentiment translate into buying decisions when it comes to security.

"*When it comes to signing a contract, aspirations go out the window and the regulatory compliance drivers are the ones that get signed*", IoT security solution vendor.
"*Customers come to us and ask us to make this device secure to the bare minimum of regulations*", IoT security solution vendor.

What are the main reasons why you have implemented changes to your security as a result of your IoT deployment?



N=2,438 (those who have amended practices)
Source: GSMA Intelligence

Understanding of IoT security is on the rise

But enterprises are only at the early stages of their security journey

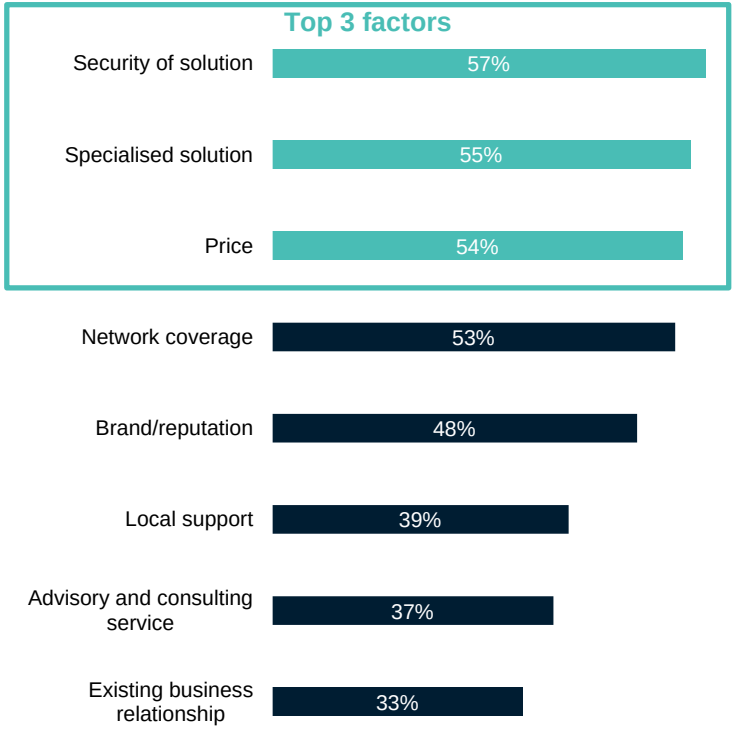
57% of enterprises rate security as a key factor when choosing an IoT solution vendor in 2020.

- **Growing importance of security in IoT solutions:** In 2018, only 53% of enterprises indicated that security was the key purchasing factor. As awareness of quality of security has increased, the proportion of enterprises that share the same view has risen to 57%.
- **No such thing as end-to-end security in IoT:** To achieve end-to-end security, enterprises would have to compromise on the level of desired performance of the solution and accept added cost. The top three key factors, taken as a whole, reflect this trade-off between security, technical performance and cost requirements. Our panel unanimously agreed that no single vendor offers true end-to-end security yet, as it is difficult to achieve.
- **IoT security needs to embrace the OT perspective too:** Our panel agreed that enterprises typically begin their IoT security journey from the starting point of IT. As deployments scale, enterprises need to include perspectives from IoT and OT teams to make a balanced decision between security, performance and cost. Some 35% of our panel respondents are expanding into OT security to prepare for the convergence of IT, IoT and OT.

"We only make proof of concepts with all the required security features; otherwise we cannot determine the true nature of the solution's performance", IoT MVNO.

"We are not at the stage where a company's CISO (Chief Information Security Officer) has an OT background. You still tend to see CISOs with extensive IT experience", IoT security solution vendor.

What are the key factors you would consider if you were choosing an IoT solution provider?



N=2,873 (all)
Source: GSMA Intelligence

Enterprises trust cloud vendors to meet their security needs

Cloud-based vendors are ahead of niche providers

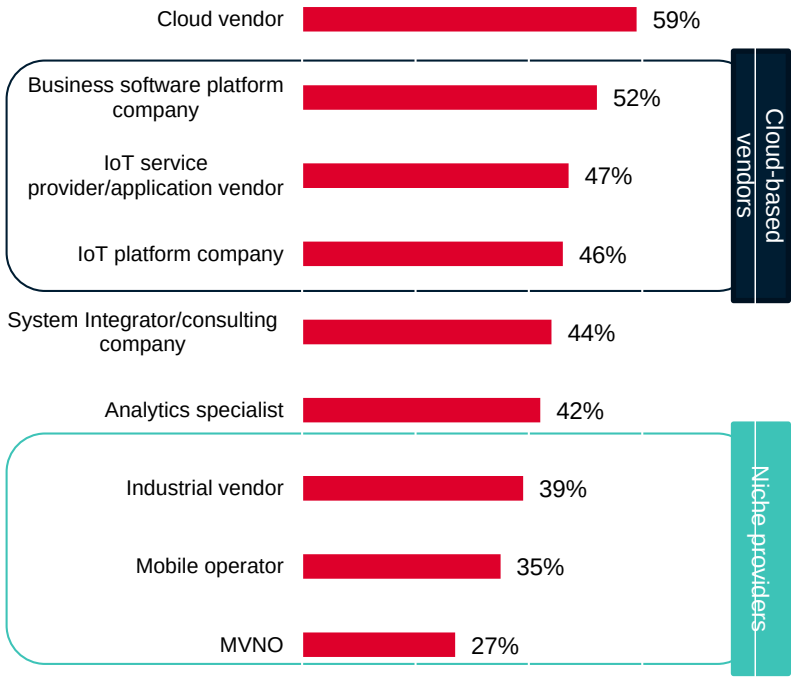
59% of those who selected security as a key purchasing factor trust cloud vendors to meet their security requirements.

- **Cannot escape the cloud:** The familiarity with cloud environments is unsurprising. The survey measures sentiment among IoT decision makers, which in most cases come from IT departments. Enterprises tend to work with what they know, and they are already familiar with AWS and Azure environments. They also trust those with cloud-based solutions such as business software firms, platform companies and service providers/application vendors.
- **Niche providers less visible on the enterprise trust radar**. The bottom-three organisation types are trusted by less than 40% of respondents. This may be because enterprises have an understanding of IT-led architectures and are not aware of alternative security approaches (e.g. a SIM-based root of trust).
- **Pre-integration with cloud vendors:** Our panel applauds cloud vendors' marketing success but warns of the perils of doing nothing more. All of the panel offer solutions pre-integrated with at least one cloud vendor and provide additional security tools to improve IoT security management.

"Enterprises have a blind spot here where they leave their IoT devices wide open on the internet. Cloud vendors give you the tools but expect you to configure and manage it yourself", IoT MVNO.

"This is not surprising. Cloud is usually the first port of call for either developers or IT – both decision makers of IoT solutions", IoT security consultancy.

Which of the following types of organisation do you most trust to meet the security requirements in your IoT solution?



N=1,624 (those who selected security as a key purchasing factor)
Source: GSMA Intelligence

Enterprises build security based on what they know

A lack of readiness for the complexity of day-to-day security operations

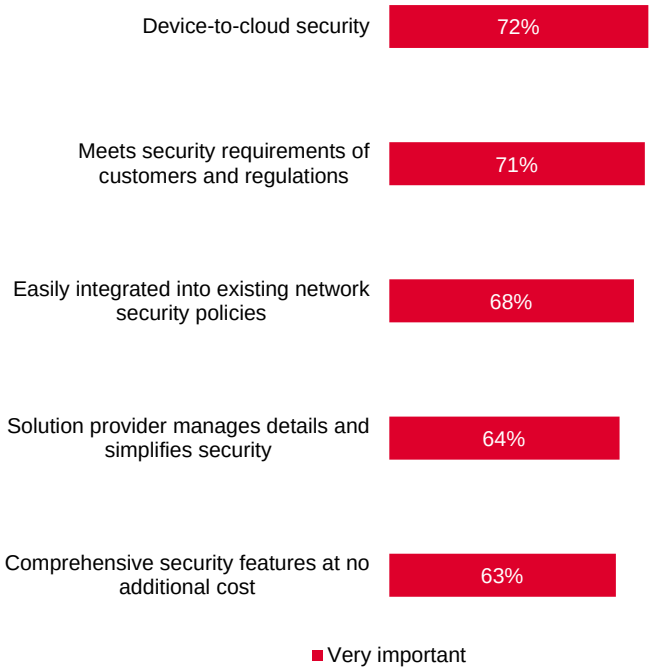
72% of those who picked security as a key purchasing factor rate device-to-cloud security as very important.

- **Device-to-cloud security is a well understood feature:** Enterprises are familiar with the need to secure device-to-cloud connectivity and use Public Key Infrastructures (PKIs) for cloud authentication. Compliance is a close second.
- **Lack of readiness for day-to-day security operations:** Enterprises are less concerned that the solution must help with day-to-day security processes and workflows (64–68%). This difference reflects an IT security mindset. Although enterprises have experience with PKI-based security, they are not fully aware of the complexity of PKI management for IoT devices.
- **The focus on bill of materials is misleading:** 63% of enterprises did not want to pay more for additional security features; instead, they expect solutions to be secure already. However, they also deem all security features to be important, which suggests a compromise is needed between IT and OT departments with regards to security, performance and cost.

"Encryption will increasingly become a regulatory requirement. Enterprises will then find that they really need to make the trade-off based on total operating cost over the lifetime of devices", IoT security solution vendor.

"When we started a long time ago, we charged IoT security as an extra. Now, we make the security business case based on the desired outcome", Operator.

How important is each of the following criteria when evaluating an IoT solution's security features?



N=1,624 (those who selected security as a key purchasing factor)
Source: GSMA Intelligence

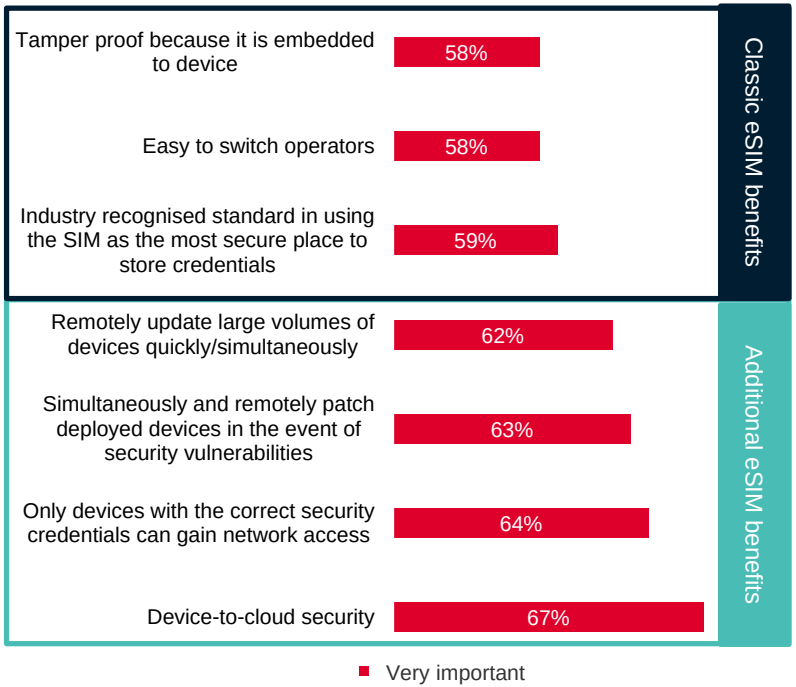
Enterprises have high expectations of eSIM in IoT

This includes benefits such as security management

67% of those who consider eSIM as important rated the additional benefit of device-to-cloud security as very important.

- **Enterprises demand more than traditional eSIM benefits:** The classic benefit of eSIM is the ability to enable remote switching of operators for cost or performance reasons. However, more enterprises are looking to eSIM to deliver benefits such as device-to-cloud security.
- **Untapped potential for SIM as the industry standard to store credentials:** Despite the SIM being a trusted secure element, only 59% of respondents currently rate this eSIM benefit as very important. As IoT deployments scale, the operational burden of credentials management will be greater than what enterprises are used to. They need to evolve their current security mindset away from an IT perspective for eSIM to become the credentials management solution for IoT.
- **eSIM solutions are plentiful, but adoption is still limited:** Most providers in our panel can offer eSIM to address customers' needs, in terms of both convenience and security. They also recognise the potential of eSIM as the root of trust; some already have proprietary solutions similar to IoT SAFE (an industry initiative led by the GSMA and the Trusted Connectivity Alliance to reuse the SIM to perform security tasks and store credentials). However, most of our panel indicated time is needed for additional eSIM benefits to mature and for the wider IoT ecosystem to embed the concept into solutions and propositions.

How important is each of the following eSIM benefits to the success of your future IoT deployments?



N=2,400 (those who consider eSIM as important)
Source: GSMA Intelligence

The US enterprise view in numbers

93% of US enterprises have changed their security practices as a result of their IoT deployments (versus a global average of 85%).

62% of US enterprises choose the brand or reputation of the solution as the key purchasing factor (versus a global average of 48%).

58% of US enterprises rate security of a solution as the next (second) key purchasing factor, while this was rated the top factor on average worldwide.

77% of US enterprises see device-to-cloud security as very important (versus a global average of 72%).

69% of US enterprises trust cloud vendors to meet their security requirements (versus a global average of 59%).

71% of US enterprises expect eSIM to deliver device-to-cloud security benefits (versus a global average of 67%).

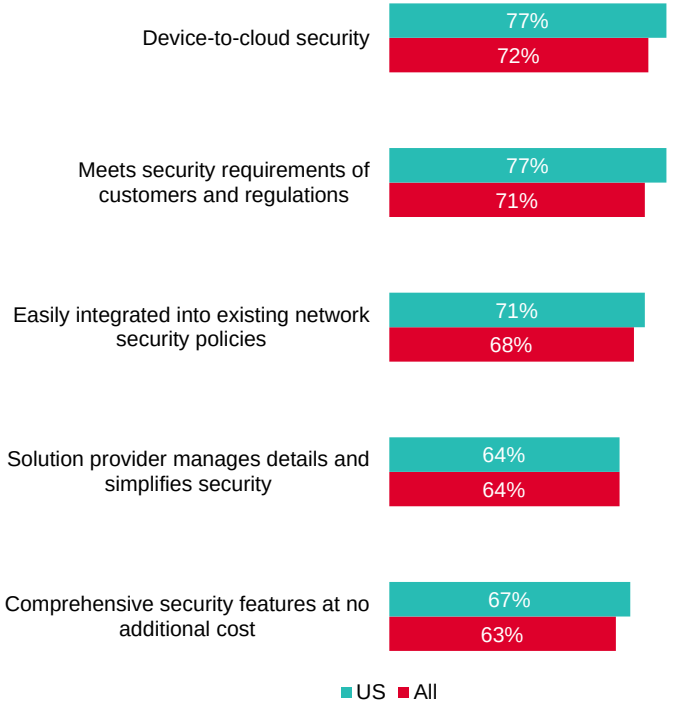
The US has experienced the largest change in sentiment

Greater eSIM familiarity bodes well for a telco-based security approach

93% of US enterprises have changed their security practices as a result of their IoT deployments in 2020.

- **Change in security practices:** In 2019, the proportion of US enterprises that had changed their security practices was in line with the global average of 86%. The 7pp increase in 2020 is an encouraging sign that regulatory drivers have raised awareness of the importance of securing IoT deployments.
- **Device-to-cloud security is a key requirement:** 77% of US enterprises see device-to-cloud security as a very important feature when choosing an IoT solution provider. This could be driven by the increased awareness of regulatory pressures. 77% of US enterprises also expect the IoT solution to be able to meet the security requirements of customers and regulators.
- **US enterprises prefer the familiar:** In the US, brand and reputation are more important than in other parts of the world; a greater share of enterprises choose brand as a key factor when choosing an IoT provider (62% versus 48%). A larger proportion of US enterprises also trust cloud vendors to deliver on security requirements (69% versus 59%)**.**
- **eSIM is making inroads in the US**: 51% of enterprises in the US see eSIM as very important to a successful IoT deployment, ahead of the global average of 41%. The US is also ahead when it comes to expectations that eSIM offers value-added benefits such as security management.

How important is each of the following criteria when evaluating an IoT solution's security features?



US N=146
All N=1,624
(those who selected security as a key purchasing factor)
Source: GSMA Intelligence

Research methodology: a two-part approach

Measuring enterprise sentiment towards IoT security

The GSMA Intelligence Enterprise in Focus Survey spans 2,873 companies, representing the following:

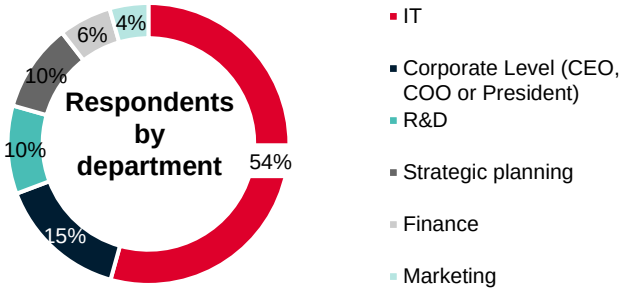
- **Industry verticals:** retail, utilities, transportation, healthcare, public sector, manufacturing, automotive and consumer electronics.
- **Countries:** Argentina, Australia, Brazil, China, France, Germany, India, Indonesia, Japan, Mexico, Russia, South Africa, South Korea, Spain, Sweden, Turkey, UK and US.
- **Company size:** small and medium-sized companies with 20–249 employees, and large enterprises with more than 250 employees.
- **Roles:** IoT decision-makers from various departments.

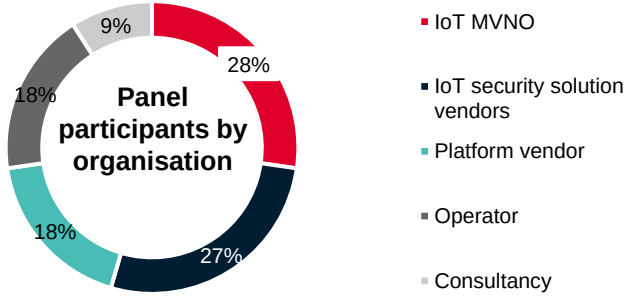
Qualitative insights on demand for IoT security

GSMA Intelligence interviewed 11 industry experts (referred to as our panel) to understand their IoT security offerings.

Our panel included IoT security specialists from the following types of organisation:

- IoT MVNO
- IoT security solution vendor
- platform vendor
- operator
- consultancy.





GSMA Intelligence

gsmaintelligence.com

@GSMAi