WHITEPAPER

Getting IoT security right: a CXO survival guide

Eight key recommendations for IoT security decision makers

Published by

MOBILE WORLD LIVE

In partnership with

orange™ Business Services

ERICSSON

Executive summary

IoT is growing at exponential rates, and will only grow faster as 5G becomes more widespread. The vision of an IoT world presents a world of fascinating possibilities – a world of smart homes, smart cities, smart farms, smart factories and smart cars on smart roads, with billions of devices communicating with each other and sharing data that enable more efficient and safer lives.

However, achieving that vision relies on our ability to secure all those devices – and many IoT devices to date are notorious for not being all that secure, or at least not secure enough. There are a variety of reasons for this, from OEMs putting greater priority on a plug-and-play experience to the fragmented nature of the IoT device market, a lack of common security protocols and a lack of uniform regulations (or indeed a lack of regulation altogether). However, as more IoT-related hacks make headlines, it has become increasingly clear that security is a prerequisite of IoT's commercial success as well as the benefits it promises society.

The good news is that more and more enterprises are taking IoT security seriously, and there are now tools, solutions, frameworks, best practices and checklists that makes it easier for enterprises to plan and implement IoT security to monitor and mitigate threats.

The key challenge lies in having a good understanding of IoT security – and how it's not identical to the IT security practices IT managers are familiar with. IT security processes and skillsets do not translate seamlessly to IoT – particularly when it comes to cellular IoT apps, which are growing in prominence and capability on 4G networks and increasingly on 5G networks. IoT in general brings its own unique security issues to the table that vary according to use case and scalability – cellular IoT even more so, despite its well-earned reputation for stronger security.

Complicating things further is that IoT end points can generally be assumed to be hackable – which throws a wrench in enterprise IT security postures that focus on end-point security. IoT security requires as much emphasis (if not more) on network security management – which itself is harder than it sounds, as the "network" in an IoT deployment is a complex ecosystem involving multi-cloud connectivity and third-party service providers.

In other words, existing enterprise security postures are unlikely to cover the necessary bases for robust IoT security.

Consequently, enterprises need to understand:

- How IoT security is different from whatever security solutions they have in place
- The specific issues that certain IoT use cases will bring with them
- What that means for their risk assessments.

This also requires a mindset shift at the CXO level to stop thinking of security primarily as a cost center that balances cost, risk and performance, and more of a business opportunity that gives them a leg up on the competition.

Once you realize you need an IoT security solution, the obvious question is: what should I look for? The answer will necessarily depend on the specific IoT use case – however, there are eight key recommendations that decision makers can take into account to ensure they select the right security solution that enables them to take control of IoT security and accelerate IoT security deployments. At the end of the day, it comes down to a network-based approach that can find the right balance between protection and cost and puts a premium on prevention, automation, scalability and visibility.

Get it straight: IoT security is not IT security

The rollout of cellular IoT technologies is going strong around the world. According to the latest *Ericsson Mobility Report*[1], cellular IoT connections reached 1.6 billion in 2020, and will grow to an estimated 5.4 billion connections by 2026 (23% CAGR).

Notably, cellular IoT is shifting increasingly beyond low-bandwidth massive IoT applications such as smart meters and asset tracking towards more advanced broadband IoT use cases that require higher throughput, lower latency and larger data volumes, such as security cameras, drones and connected cars.

Many of these use cases are already supported by 4G and 5G networks, and by the end of this year will outnumber IoT use cases running on 2G and 3G networks. This trend will continue as 5G rollouts continue to proliferate, which will enable critical IoT use cases requiring guaranteed data delivery with specified latency targets, such as AR/VR, remote control of machines and cloud robotics, to name a few. And that's just for starters – as enterprises increasingly leverage the game-changing capabilities of 5G as part of their digital transformation roadmap, this will enable IoT use cases we can scarcely imagine today.

However, IoT presents a massive security challenge for enterprises already tasked with keeping their IT networks secure. Adding hundreds or thousands of new end points to the network creates thousands of potential new threat vectors that need to be protected. Moreover, those end points have security protections ranging from decent to non-existent – and none are hackproof.

[1] *Source: Ericsson Mobility Report, June 2021*

IoT attacks on the rise

Consequently, IoT devices and networks are ripe targets for attacks – and those attacks are growing fast:

- SonicWall's 2021 Global Cyberthreat Report[2] recorded 56.9 million IoT malware attacks in 2020, up from 34.3 million in 2019 (a 66% increase). In October 2020 alone, 10.8 million cases were recorded – more than all IoT malware attacks in 2017.
- A 2020 survey from Cybersecurity Insiders and Pulse Secure (since acquired by Ivanti) found 72% of organizations experienced an increase in endpoint and IoT security incidents in the previous 12 months, while 56% anticipate their organization will likely be compromised due to an endpoint or IoT-originated attack with the next 12 months.[3] The top three issues were related to malware (78%), insecure network and remote access (61%), and compromised credentials (58%).

As with IT-focused cyber attacks, the costs of an IoT breach can range from operational downtime and loss of productivity to compromised customer data, stolen IP, damage to the brand's reputation and in some cases end-user safety. This last aspect is not to be taken lightly – a hacked car, drone or robot has the potential capacity to harm or kill people, a consequence no IT security team has had to consider until now.

Costs for specific IoT security incidents are generally not made public, and many of the more publicized enterprise IoT hacks on "things" like construction cranes, supermarket freezers and driverless cars were carried out by security experts who discovered the vulnerability in question and reported it to the company.

However, some recent research gives us an idea:

- A recent survey from Irdeto estimates that the average financial impact as a result of an IoT-focused cyber attack was $330,602 – which Irdeto says may be an underestimate as respondents may not be taking into account all of the costs associated with a cyberattack, such as lost business and the costs of correcting whatever vulnerabilities that led to the attack.[4]
- A survey from strategy consulting group Altman Vilandrie & Company found that the cost of IoT security breaches represented 13.4% of total revenues for companies with revenues under $5 million annually. Nearly half of firms with annual revenues above $2 billion estimated the potential cost of one IoT breach at more than $20 million.
- If the IoT attack involves ransomware, the cost can be considerable, as ransomware attacks are increasing at an astonishing rate, thanks in part to the rise of cryptocurrency that makes such attacks more lucrative. Reuters reports that meatpacker JBS USA – whose supply chain was crippled by a ransomware attack in June 2021 – paid $11 million in Bitcoin to the hackers responsible.

As IoT apps become more complex and mission-critical, the stakes of a breach can be even higher. In 2015, hackers successfully took control of a connected Jeep and killed the engine while it was in motion. The hack was a controlled demonstration, but the consequences of a malicious hack could be deadly.

[2] *Source: SonicWall 2021 Cyber Threat Repor*
[3] *Source: Cybersecurity Insiders and Pulse Secure, 2020 Endpoint and IoT Zero Trust Security Report*
[4] *Source: Irdeto Global Connected Industries Cybersecurity Survey: IoT Cyberattacks Are The Norm, The Security Mindset Isn't (2019)*

On the bright side, the rise of IoT-related cyber attacks and subsequent global headlines has heightened awareness of the importance of IoT security for enterprises. Recent enterprise survey data from GSMA Intelligence found that 85% of enterprises surveyed in 2020 indicated that they changed their security practices as a result of their IoT deployments (roughly the same number as 2019) – interestingly, the majority (61%) did so in order to develop a security-first strategy as a competitive differentiator.[5]

What are the main reasons 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 Enterprise in Focus Survey 2020

Look beyond the end points

However, while enterprises say that they are taking IoT security more seriously, many still face challenges in actually implementing it. According to GSMA Intelligence, most enterprises still generally deploy and secure IoT from an IT perspective – often because that's the existing skillset. But IoT raises a number of security challenges that existing enterprise security teams may be ill-prepared to handle.

This is particularly true for cellular IoT security, which differs from enterprise security in several respects.

For a start, while cellular IoT is reasonably secure out of the box, "secure" doesn't mean "unhackable". To be sure, cellular IoT has the strength of leveraging SIM as the root of trust, as well as security standards designed into 4G and 5G networks by the 3GPP. However, it's a mistake for CXOs to be lulled into complacency by assuming cellular IoT end points are invulnerable.

This is especially dangerous thinking because for most enterprises, end-point security is a key aspect of the organization's security posture. IoT use cases can involve anywhere from hundreds to tens of thousands of new devices at launch, and the number of devices will typically grow larger from there. Consequently, putting security into every device – or even monitoring them all – is a tall order, whether in terms of cost, operations, capabilities or other constraints. Thus, IoT security is less about securing the end points and more about securing and managing the networks.

That said, IoT security isn't just about making sure your network is impregnable – it's about putting an emphasis on network-based security solutions that enable sufficient threat monitoring and mitigation to prevent cyber-attacks from happening in the first place.

It's also worth remembering that the objective of cellular IoT security isn't simply keeping out hackers or malware – it's about maintaining the reliability and resilience of your IoT app, and safeguarding the privacy of those who use it, as well as their physical safety for certain use cases. Put another way, cellular IoT security is about ensuring the trustworthiness of your IoT app. Trust will be crucial in the digital era in general, and this will be especially true for IoT – after all, who in their right mind would trust a connected car manufacturer with a reputation for shoddy security, or a smart parking scheme where hackers can steal your payment credentials from an unsecured parking meter?

[5] *Source: GSMA Intelligence Enterprise In Focus Survey 2020*

IoT use case spotlight:

Connected cars

Connected cars are perhaps the most obvious use case for cellular IoT, if only because only 4G and 5G can provide the necessary range, coverage and network performance to support the business case for them. But cellular IoT also provides extra advantages in terms of providing robust and reliable security.

This is key because threat mitigation for connected cars is a more complex proposition compared to a relatively simple device like a temperature sensor. On a general level, the security architecture for automotive IoT is typically better than many other IoT use cases, but managing security at the end points (i.e. the car computer) is a more complex process. That's because a connected car isn't a single IoT app like a sensor, but an amalgam of apps that includes telematics, navigation, remote control, infotainment, and in-car Wi-Fi – effectively making the car a router on wheels hosting a range of internal apps and networks, any of which is a potential threat vector.

Consequently, while end point security is important, it's crucial for automotive IoT to have serious security on the network side – and cellular networks are designed to provide just that. 4G and 5G are designed and built on proven/robust 3GPP standards and industry standard security frameworks (such as ISO, NIST and CIS) and utilize state-of-the-art encryption.

That said, cellular IoT offers security-related advantages beyond defense and threat mitigation. For example, connected vehicles will be able to constantly evolve via secure OTA software updates throughout their lifecycle. Cellular IoT also enables secure connected vehicle services that roam seamlessly across borders and networks, as well as the intelligence necessary for automated driving technologies like C-V2X that lets cars talk to each other and navigate their way around.

As connected cars become the norm (and according to ABI Research, they already account for the vast majority of cars sold in markets like the US), the bottom line is that trustworthy IoT security is a must-have for connected cars in terms of safety. The consequences of a security breach can be both costly and deadly if it results in a crash. For car manufacturers, dependable IoT security is more than a selling point – inevitably it will be a safety requirement like seat belts and airbags.

IoT security pre-flight checklist

Now that we've established that cellular IoT security doesn't slot comfortably into standard IT security postures, the obvious question is: what next?

The answer depends on a variety of factors specific to each enterprise and each IoT use case, but here is a reasonably agnostic checklist of things to consider when preparing your IoT security strategy.

Know your IoT devices

In the previous section, we discussed how there's no such thing as an unhackable IoT device. Consequently, IoT security should start with the assumption that all IoT devices are vulnerable.

However, this doesn't mean that devices are irrelevant to your IoT security strategy. Asset management is a critical element of your IoT security posture – understanding the nature of the devices connected to your network and how they work helps you better evaluate the potential threats to guard against.

A recent report from KPMG recommends evaluating IoT devices by complexity and function.[6] For example, sensors designed to simply capture and relay data are simple devices, but some of the data they're relaying could be quite sensitive.

Embedded sensors for smart lighting systems or delivery robots are more complex, with on-board controls and active data generation. Moreover, they're part of systems that, if compromised, could disrupt operations (imagine, for example, remotely switching off all the lights in a hospital). Then you have highly complex smart devices, whose complexity actually makes them more vulnerable to potential attacks.

[6] *Source: KPMG International, "Risk or reward: What lurks within your IoT?"*

Know your IoT ecosystem

IoT isn't just a bunch of devices – it's an ecosystem. An IoT device communicates with something or someone, whether it's another IoT device, an internal server or a third-party service provider, which could include the device maker, the maintenance company, the network service provider and the cloud host.

Depending on the use case, the result is a complex and less transparent ecosystem with many possible weak links for hackers to exploit. This is especially true for IoT apps like connected cars, which are complex ecosystems in themselves. (The 2015 Jeep hack exploited a bug in the vehicle's infotainment system.)

It may not be up to the enterprise chief information security officer to take responsibility for securing every aspect of that ecosystem, but at the very least they need to have a security solution that can help manage it.

Have an integration roadmap

As IoT grows in scale and prevalence, the lines between IT and IoT networks are going to blur – and thus will the security solutions for each.

We're already seeing this trend with OT (operational technology) in IoT apps. OT and IT have been traditionally managed separately, but according to GSMA Intelligence's *Enterprise in Focus Survey 2020*, organizations are now converging previously independent IT, OT and IoT networks – "to leverage real-time data and achieve business benefits". For example, integrating IT and OT allows business systems and data analytics to access and make good use of OT data, as well as lower operational costs.

However, this raises a few key challenges. For a start, IT/OT integration may expose OT to the primary risks of IT security. The challenge then is how to segregate control and access to OT networks so that data can flow between IT and OT without putting the security protocols of OT at additional risk.

Another challenge, the GSMA Intelligence enterprise survey warns, is regulatory compliance. As regulations for IoT evolve, a likely requirement will be data provenance, in which trust is tracked via audits. Integrating IT, OT and IoT environments requires organizations to integrate security management processes such as firmware updates, supply chain data provenance and credentials management across these environments – and all of this will have to scale as more IoT devices are added to the network.

Integration will also require enterprise security managers to revamp their skill sets. Enterprise IoT deployments naturally employ IT security first because that's the existing skillset, but as those deployments scale up, the GSMA Intelligence survey says, "enterprises need to include perspectives from IoT and OT teams to make a balanced decision between security, performance, and costs." Indeed, 35% of respondents to the GSMA Intelligence survey said they are "expanding into OT security to prepare for the convergence of IT, IoT and OT."

Focus on prevention

There are all kinds of IoT cyber-attacks to defend against, and – like with enterprise security – they can be grouped into two basic categories:

Known attacks: attacks where the mechanisms involved are known and understood, and for which we have established defenses against

Unknown attacks: literally everything else – namely, all the attacks that hackers invent and throw at you to catch you off-guard, leaving you very little time to find a solution.

The latter category is why the overall objective of cyber security is to detect such attacks in advance in order to prevent them from happening. Prevention in particular will be increasingly important as technologies such as automation via artificial intelligence (AI) and machine learning (ML) are applied to cyber-attacks. The same technologies can also be applied to defenses, of course (more on that in a moment) – the point is that cyber security will always be an arms race, which means it's important to focus on security solutions that put a premium on prevention.

Prevention is especially crucial for the kinds of advanced, mission-critical IoT apps enabled by 4G and 5G. Put simply, when it comes to threat monitoring and mitigation, it's not enough to detect when someone has taken control of your security cameras or your autonomous fleet of public transport vehicles – you need to be able to prevent them from doing so in the first place.

Harness the power of AI and ML

AI and ML technologies will play a crucial role in IoT security, starting with automation of security management processes.

IoT deployments will scale and grow in complexity, and as broadband and mission-critical IoT apps become mainstream – particularly with 5G-based use cases – the amount of traffic to analyze for potential threats will skyrocket quickly.

Meanwhile, IT/OT/IoT integration will become essential in making security processes more manageable and auditable, but it will be unsustainable without bringing automation into the equation.

Consequently, automating security management processes with AI and ML will be essential to not only increasing efficiency and productivity, but simply enabling enterprise security teams to keep up with an increasingly complex task. This includes automation of security configuration and compliance, security workflows and incidence response.

AI and ML will also be key to the security solution's ability to monitor, detect and mitigate attacks. AI and ML can provide clear visibility of network conditions on a dashboard to display the potential risks that are out there, and automatically deal with those risks before they become a problem. AI/ML can also alert network admins to potential security risks in situations where a human needs to be in the decision loop, and recommend actions to be taken to mitigate the threat.

Align security objectives as business opportunity

Just about every organization understands the importance and necessity of IT security, yet not everyone is on the same page when it comes to implementing it. CTOs and CIOs usually see security in terms of threat vectors and technological capabilities, while CFOs and CEOs see security primarily as a cost issue. While different departments will inevitably view security from their own perspective, it's important to ensure those perspectives align from the top down into a comprehensive security investment strategy.

One key aspect where different CXOs could find common ground is the untapped business opportunity that a strong security solution represents. Put simply, it's not just about how much the solution costs – it's also about giving your business an edge on the competition. This will be a crucial characteristic of every organization that hopes to thrive in the digital economy – customers and business partners alike must trust that you will protect their data and their safety will not be compromised.

In the case of IoT security, connected cars are an easy example – who would buy a car from a manufacturer whose vehicles have a reputation for being easily hacked? Or, would you select a health maintenance organization (HMO) whose lighting system or medical equipment was hacked?

As enterprise IoT increasingly goes mainstream, strong security compliance will be crucial to brand and reputation. Enterprises that deploy 5G -powered IoT with a strong vendor and/or service provider will have a considerable competitive advantage over those offering plain IoT connectivity and basic security.

This shift in focus can also pay off in terms of more efficient investments in security solutions. Adopting a robust security analytics and management solution from scratch can help organizations avoid costly and complex security projects that are bolted on as an afterthought.

At the end of the day, everyone at the CXO level needs to understand not only the importance of IoT security, but the value the right IoT security solution provides. A superior security solution doesn't just protect the network from breaches or attacks – it creates a selling point for the marketing team and provides assurance to customers. In some cases, it can even enable monetization of those security capabilities as a service.

IoT use case spotlight:

Industry 4.0

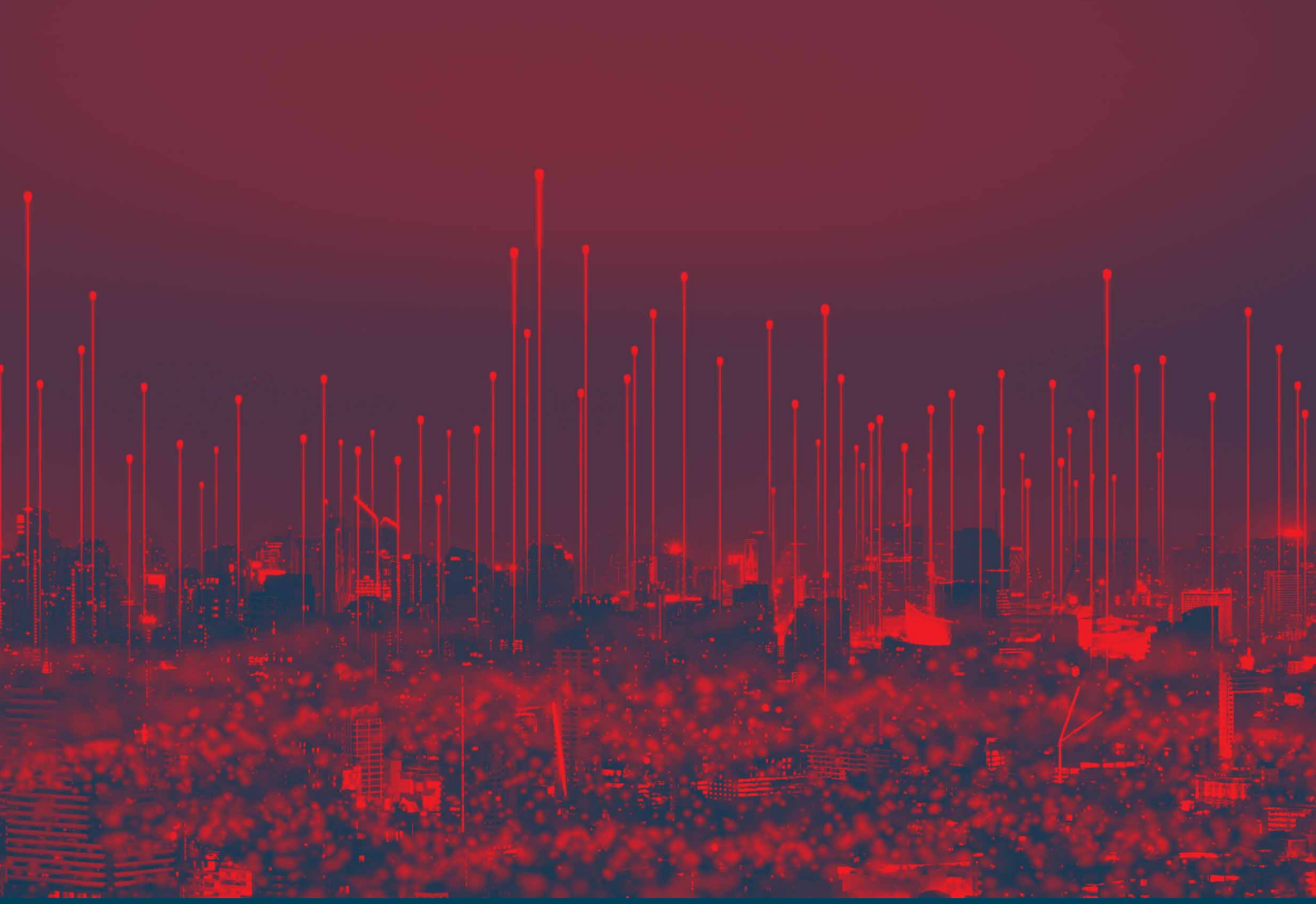
With the rise of Industry 4.0, IoT solutions have naturally found a home in the manufacturing sector – so much so that it has its own subset category: industrial IoT (IIoT). In oversimplified terms, smart manufacturing involves combining IIoT technologies with AI/ML and big data analytics to enable automation, predictive maintenance and boosting efficiency and productivity. While manufacturers have a number of IoT connectivity options to choose from, cellular IoT – particularly 5G – is a rising star, not just in terms of ultrafast speeds and ultralow latencies, but also its robust security features.

IIoT absolutely needs robust security and threat mitigation to safeguard the resilience of the production processes and the efficiencies promised by Industry 4.0, to say nothing of trustworthiness and workplace safety. Reliable security frameworks are built into the 3GPP standards, making IIoT solutions based on 4G and 5G highly secure.

Cellular IoT also gives factories more agility by enabling them to operate with more flexible factory layouts; it also enables advanced operations with efficiency-boosting technologies like AR and autonomous mobile robots – all of which require the level of security inherent in 4G and 5G. Cellular IoT can also unlock the intelligence of IIoT use cases by securely enabling data to be transformed into actionable insights that raise productivity and sustainability.

However, it's worth highlighting one unique challenge to IIoT security: legacy operational technology (OT) networks using specific protocols for solutions such as SCADA, PLCs and DCS. These are typically managed separately from the manufacturer's IT systems, but there is currently a debate about whether they should be integrated to better facilitate IIoT use cases (to include making better use of OT data) and lower opex in the process.

That convergence potentially creates an opportunity for hackers to exploit both IT and OT systems, with OT being the weakest link, as OT-connected systems tend to run on outdated software and security patches are few and far between to minimize downtime. On the other hand, those concerns could be alleviated by integrating both IT and OT operations onto cellular IoT networks to provide reliable and tough access security for all things connected. (See the previous section of this whitepaper for more on the issue of IT/OT integration and IoT security.)



Key recommendations for IoT security solutions

While IoT security requires a different approach compared to regular enterprise IT security, electing the right security solution for this involves some of the same general considerations as IT security solutions – in other words, it's a matter of risk assessment, performance and cost (not just the cost of the solution itself, but the cost of a breach – not just in terms of dollars, but also lives lost, brand damage, etc).

Indeed, it's not only about the technical capabilities of the solution, but also the operational limitations. Does the security solution make sense from an operations or commercial point of view? What is the risk for each part of the IoT network? How do you prioritize them? Where does it make the most sense to spend money and effort to secure it?

As such, enterprises shopping for a cellular IoT security solution will have their work cut out for them hunting for something that matches their very specific requirements. They'll also have to decide whether the best solution is something that can be implemented and run in-house, or outsourced from a service provider.

However, outside of the specifics, there are eight key recommendations that enterprises can look at when selecting and deploying the right security solution for their IoT use case.

1. Level of preventative protection

As mentioned earlier, prevention is the primary objective of IoT security, which brings the focus away from the end points (which it's safe to assume are hackable) and towards the network. Once you've completed your threat modelling, you can understand the routes into the system, and design preventative measures based on that. But the solution should be able to support whatever measures you need to take based on the threat model.

So, for example, if the devices connect to multiple clouds and you want to limit traffic so it doesn't connect to specific clouds on different levels, a solution with granular options will help make it possible for you to do whatever makes sense for your network.

Another consideration related to detection and prevention is how fast the solution can detect and prevent. The level of turnaround time required will depend on the use case, but for critical IoT use cases where real-time communications are essential, you need a security solution that can detect and report potential threats as close to real time as possible, and also manage and mitigate those threats.

This in turn has to be balanced against network performance. A security solution may offer the best possible security protection and prevention capabilities, but it may not be worth the cost if it's slowing down the network to the point that customers notice, or if it impacts the low latencies required by critical IoT use cases.

2. Completeness of threat detection capabilities

Today, some IoT security solutions have capabilities in the device, some have nothing in the device, some can add capabilities in the device, or the capabilities reside in the cloud end points. But as application gets more complex, enterprises need to think about how to do this end to end. This requires more monitoring in the network part because that provides valuable information into what's going on out there and spotting trends while they're still ramping up rather than when they've already become a problem, by which time it's too late.

3. Automated responses for cyber incidents

Automation isn't just crucial for IoT security management processes – it's also essential for incident response. Simply put, manual responses to incidents can take days or weeks – and you may not have days, or even hours or minutes, to respond. Cyber-attacks usually happen quickly and propagate at lightning speed, so enterprises need to be able to act very swiftly. That means having as much automation as possible.

Take note of those last two words: "as possible". Sometimes total automation isn't possible, depending on the specific business process the enterprise want to automate. Some decisions may still require a human to be in the loop. For example, if the only way to stop an attack on autonomous cars is to disconnect every car, that's not the sort of decision a machine should be making – it's a radical move. While automation can make recommendations and inform the final decision, a human still has to make that call.

But it's recommended to automate everything that can be automated to speed up response times – a good IoT security solution provides all the tools needed to do that.

4. Total cost of ownership (including deployment and lifecycle management)

This comes back to the points above about risk assessment and balancing the trade-offs of performance and cost, which is not just a matter of getting the most security for your dollar, but assessing the financial impact on your business and on your operations, which has an impact on TCO.

From a purely commercial point of view, the question seems simple: how much are you prepared to pay for the impact if something happens? But as described in Section 2, the cost of an attack takes different forms, from operational downtime and device maintenance to brand damage, regulatory fines and (in extreme cases) property damage and human casualties.

All of this has to be balanced against the cost of the solution. Put simply, if the solution costs more than whatever the financial penalty would be for not installing it – especially if the odds of an attack incurring that level of pain is statistically rare – the CFO is unlikely to approve that purchase. This is why before you shop, it's crucial to understand the threat modelling, where the impact will be, how severe it will be, the consequences, and where to best spend the money to mitigate it.

5. Usability

As enterprises shift from an environment of separately managed, manual processes to something more integrated and automated, a key feature of IoT security solutions to assess is user-friendliness.

Many enterprises may not have an internal team dedicated to IoT security, and even existing IT security staff may face a steep learning curve in implementing it. For example, firewall administrators go through a lot of pain to make sure they're designing the protection elements of their IT networks correctly – now they have to translate that process to IoT.

A good UX/UI design enables not just security professionals but anyone in the enterprise to implement and use IoT security solutions and tools easily – and ensure they're using them correctly.

6. Enhanced visibility

There are a couple of aspects to the visibility capabilities of IoT security solutions, the first being visibility for enterprise security operations staff. Whether they're handling security themselves or outsourcing it to a CSP, they want to be in control of what mitigations, responses or actions to take if something happens. A single-view dashboard is a very useful feature so that the enterprise security team can see everything that's going on in one place, and can act quickly.

The other aspect of visibility is being able to see what's going on out there in the network. Early implementations of cellular IoT had little or no visibility in that respect, which was not a huge problem in that cellular IoT doesn't typically deal with the thousands of security events per minute that's associated with public IP. But as the sheer volume of security events grows, and as IoT becomes more widespread, visibility of threat activity is becoming a more urgent consideration – much of prevention is about spotting malware or malicious traffic as early as possible, and this will be crucial for effective IoT security.

For managed security solutions, visibility can be enhanced further by the service provider's own security operations, which offers expertise, 24/7 support, timely solution updates and an extra set of eyes to accompany the customer throughout the product lifecycle.

7. Evolutionary capabilities

Cyber security is a never-ending arms race, and unknown threats lurk in the darkness until they suddenly become known, sometimes to devastating effect. This means cyber defenses have to evolve along with the overall threat landscape. A good IoT solution needs to offer continuous detection improvements – detect unknown threats and update its knowledge and capabilities to counter newly revealed attack techniques.

This is also where AI/ML capabilities come into the picture, as IoT security will increasingly rely on automation to keep up with the deluge of threats out there. AI/ML can help security solutions evolve with the times, provided such tools can evolve themselves.

8. Scalability and flexibility

IoT involves up to thousands of new devices connecting to the network, and the number will only get larger from here. So the security solution needs to be scalable, adaptive and flexible, in case the enterprise needs to add more devices or add or change a use case.

IoT use case spotlight:

Smart cities

Of all the IoT use cases currently in progress, perhaps none are more complex than smart cities. That's because a smart city isn't just one app but an ecosystem of "smart" use cases, from power grids and road traffic management to parking meters, lighting systems, waste collection, buildings and emergency response, that have a direct impact on people's lives. Each app or system may have its own network of IoT devices sending and receiving telemetry data (many of them in real time).

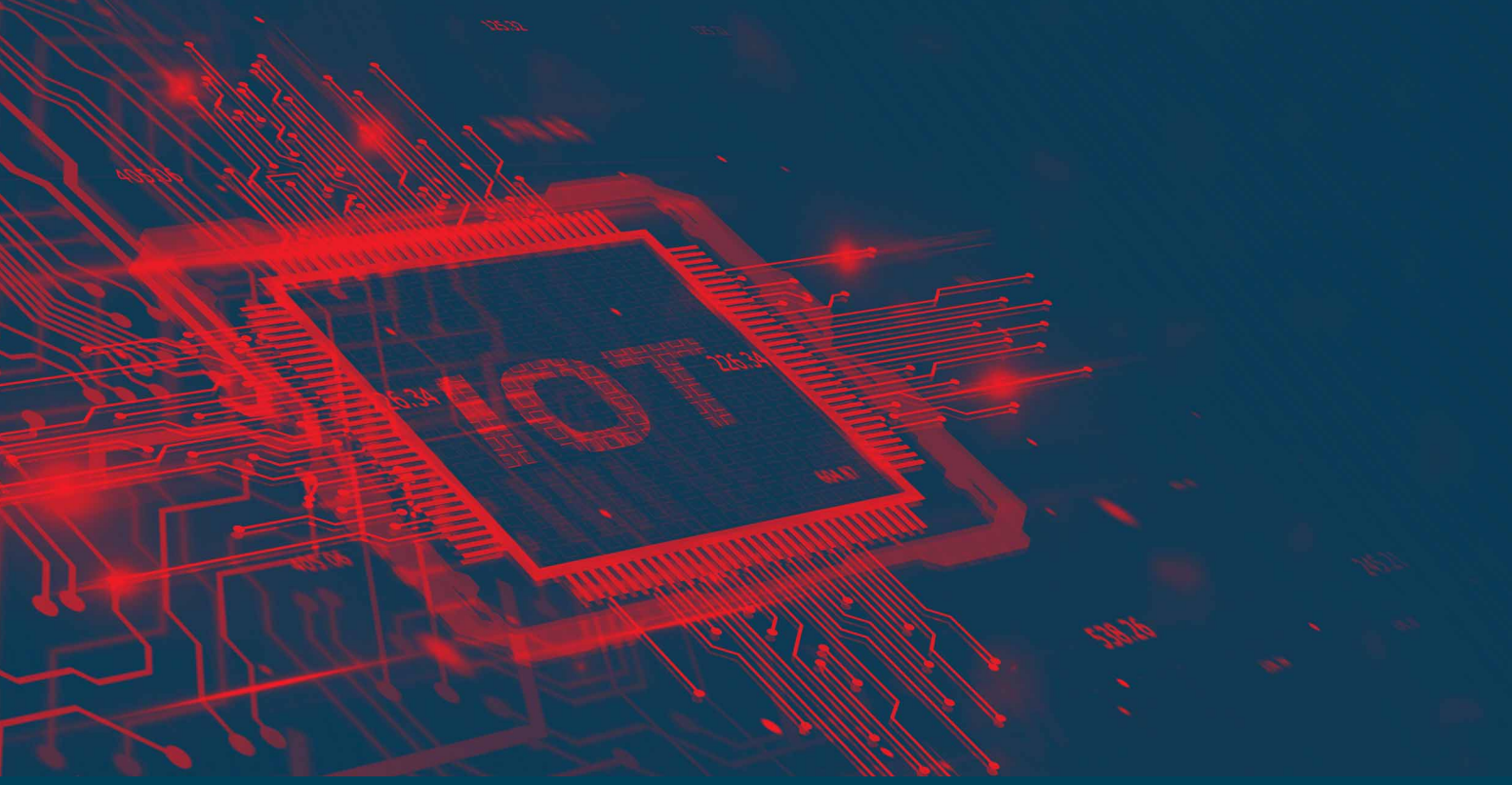
Like Industry 4.0, smart city projects can tap a range of IoT connectivity options. But like connected cars, cellular IoT is the most practical option, not least because urban centers already feature dense cellular coverage – and this will be increasingly the case with 5G, which requires even more dense urban topologies. Moreover, 5G is architected specifically to support massive machine type communications (mMTC) at a far greater scale than 4G.

Beyond the connectivity aspect, cellular-based IoT provides cities with an agile, future-proofed path to launching and evolving data-rich services with an expanded ecosystem, whilst enabling secure data sharing between use cases that enhances the value of individual services whilst simultaneously making them more than the sum of their parts. Moreover, combining that data with AI/ML can unleash the kind of intelligence that creates valuable situational awareness in moments of crisis.

All of this requires the kind of robust standards-based security that is baked into 4G and 5G standards, because – as we've explored throughout this paper – any connected device is a potential target for hackers. And just like any other organization, municipal governments are also IT users with their own internal tools and systems who need cyber-protection like everyone else.

That said, the stakes in smart city security are considerably higher than the average organization – many smart city services can be classified as critical infrastructure, so the consequences of a hack can be severe.

The consequences could also impact the city's ability to attract investment. Many cities that embrace urban technologies typically showcase themselves as a cutting-edge digital hub to make them more attractive to businesses. However, that edge is lost if your parking meters are easy to hack or your traffic system can be disrupted by a DDoS attack.



Wrap-up

Enterprise IoT is gaining traction quickly – but it's one thing to deploy it, and another to secure it. Even for cellular IoT solutions, security issues arise that don't fit neatly into the average enterprise IT security posture. That's why enterprises must think about threat monitoring and mitigation differently when it comes to IoT.

IoT security differs from enterprise security in several key ways, from the sheer scale of the number of devices being connected to the fact that those devices often will be the most vulnerable part of the network – which means a security strategy focused on end points is doomed. A shift in focus to network-based security is essential.

Complicating things is that the level of security required for IoT is heavily dependent on the use case, as well as understanding the objectives of the attackers. This impacts the risk assessment of IoT security – not simply balancing cost vs performance, but also the consequences of a breach, which in the IoT space could range from inconvenient to deadly. There's also the question of where OT fits into the IoT security equation as OT/IT integration becomes the norm.

The sheer variety and scope of IoT use cases makes investing in an appropriate security solution challenging, but in general there are eight key recommendations that enterprises should examine regardless of the specific use case in order to take control of IoT security and accelerate deployment:

1. Level of preventative protection
2. Completeness of threat detection capabilities
3. Automated responses for cyber incidents
4. Total cost of ownership
5. Usability
6. Enhanced visibility
7. Evolutionary capabilities
8. Scalability and flexibility