AVNET SILICA

IoT SECURITY CONSIDERATIONS: CHECKLIST

THERE ARE THREE MAIN SECTIONS OF AN IOT DEPLOYMENT: CONSULT, DEVELOP AND DEPLOY. HERE ARE THE SECURITY QUESTIONS YOU SHOULD ASK AT EACH STEP:

CONSULT

First, you have to make a big decision on whether you'll build an internal team to execute your IoT solution or buy it through exporting the work to an external partner. That way, you'll be able to properly scope out the road ahead for final deployment in order to get initial buy in from the executives who might have the ROI rather than the security stack in mind.

Ask yourself questions like:

- Which security measures do you need to comply with by law?
- What security scenarios related to this project could jeopardize your project revenue or your company revenue as a whole? (Rank them by priority, short/long term and draft a technical solution for each)
- What costs are associated with developing and deploying in terms of overall budget?
- What hardware, software and firmware considerations do you need to consider?
- What security team do you have in house ready for an IoT deployment?
- Who on your team will be the final responsible party for security of the solution?
- How will you measure success for your team in terms of security protocols?

DEVELOP

In the develop phase, you should clean up the initial plans created in the consult phase to optimize for performance and cost as well as to find the fastest, most profitable route to market.

Ask yourself questions like:

- What will you build in-house and what are you ready to outsource to partners?
- If external partners, will they outlive the 10-year smart appliance you are deploying yourself?
- Who is ensuring hardware security, including board development and logistics around manufacturing?
- Who is ensuring software and firmware security, including the software, cloud and associated analytics platform? (If you are including artificial intelligence (AI), machine learning, web platforms and applications, or data visualization, you'll need to build out this even more.)
- Who in your development team will follow through to deployment to ensure the solution's security stack works in the field?
- Do you need certifications or should you rely on already certified solutions?
- Have you considered privacy and data concerns? Do you need additional security resources?

DEPLOY

Here's where the rubber meets the road: security and data privacy plans laid out in the consult phase and created during development also come full circle in deploy.

Ask yourself questions like:

- Do you have the in-house capabilities to install, support and service on premise during the crucial weeks and months of initial implementation? Does your external partner?
- Do you have secure tech support for Wi-Fi or cellular networks, gateways, web interfaces, apps and your new cloud platform?
- Do you have plans if a critical piece is stolen days before deployment? If a protocol crucial to your system is hacked? How can you protect your system from ongoing threats?
- What is your plan to qualify your solution and check every single scenario which could make it go wrong?
- How about having a "white hats" lab proof it before you go live?

Looking for IoT security advice or support? Get in touch with our technical experts

www.avnet-silica.com/iot-security