

How to future-proof your IoT device – achieving ‘Secure by Design’ for IoT and connected devices

Developing a secure, smart consumer product from concept all the way through to operation, including manufacture and over the air (OTA) updates, means shifting to a security mindset. You need to think about security early in your IoT projects and product planning process, and invest in a secure development lifecycle, to tick all of the Secure by Design (SbD) boxes.

Cyberattacks on IoT devices surge 300% in 2019, now ‘Measured In Billions’*

Here we set out key stages you should go through when considering security in your internet of things device to comply with the UK’s Secure by Design (SbD) principles. It’s worth noting that the UK Government is taking ‘decisive action’ on security; ‘advocating a robust and staged approach to enforcing these principles through regulation’ and ‘leading efforts to create international alignment on IoT security’, for example, working with other territories such as the US (NIST) and the EU (ETSI) to align standards. The SbD Code of practice has been developed to also align with any future Trustmark scheme. In short, the direction of travel is only going one way.

Consult Red’s experience in design and development of smart, connected devices and systems can reduce your time to market and manage cyber security risk to deliver truly secure IoT products.

// 13 Principles in the UK Government’s Secure by Design Code of Practice

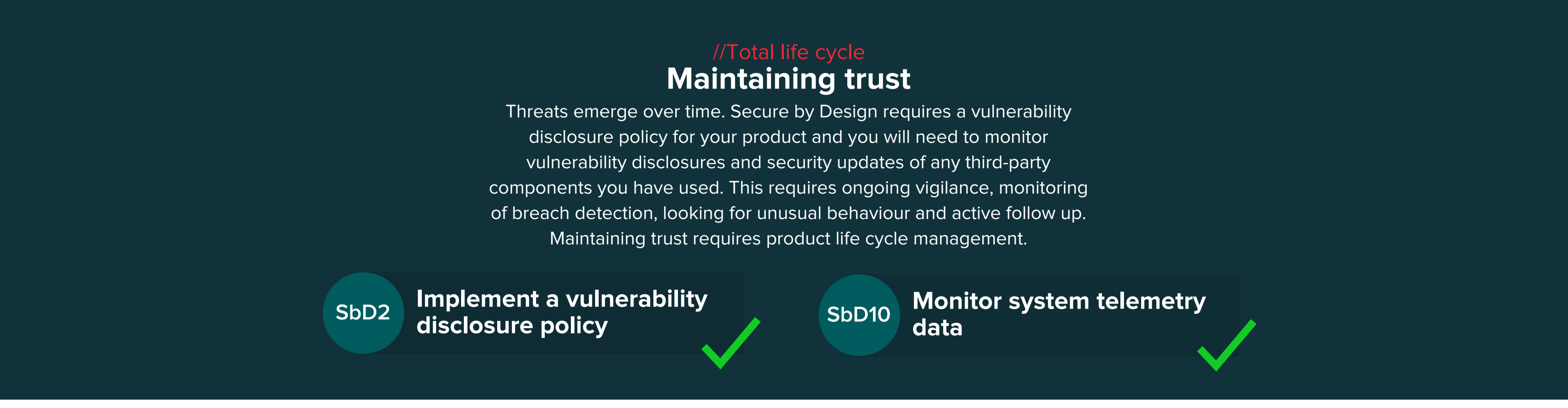
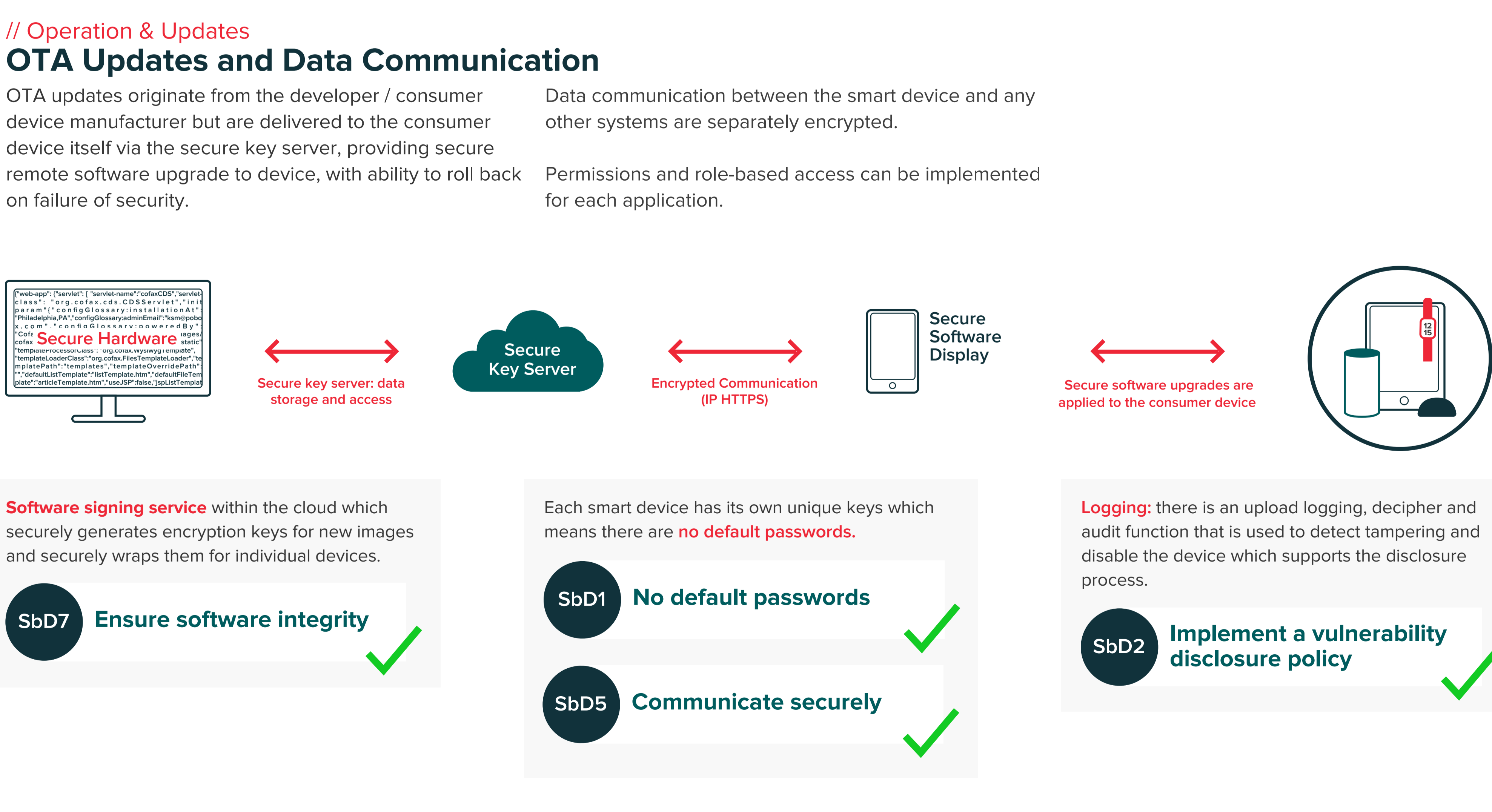
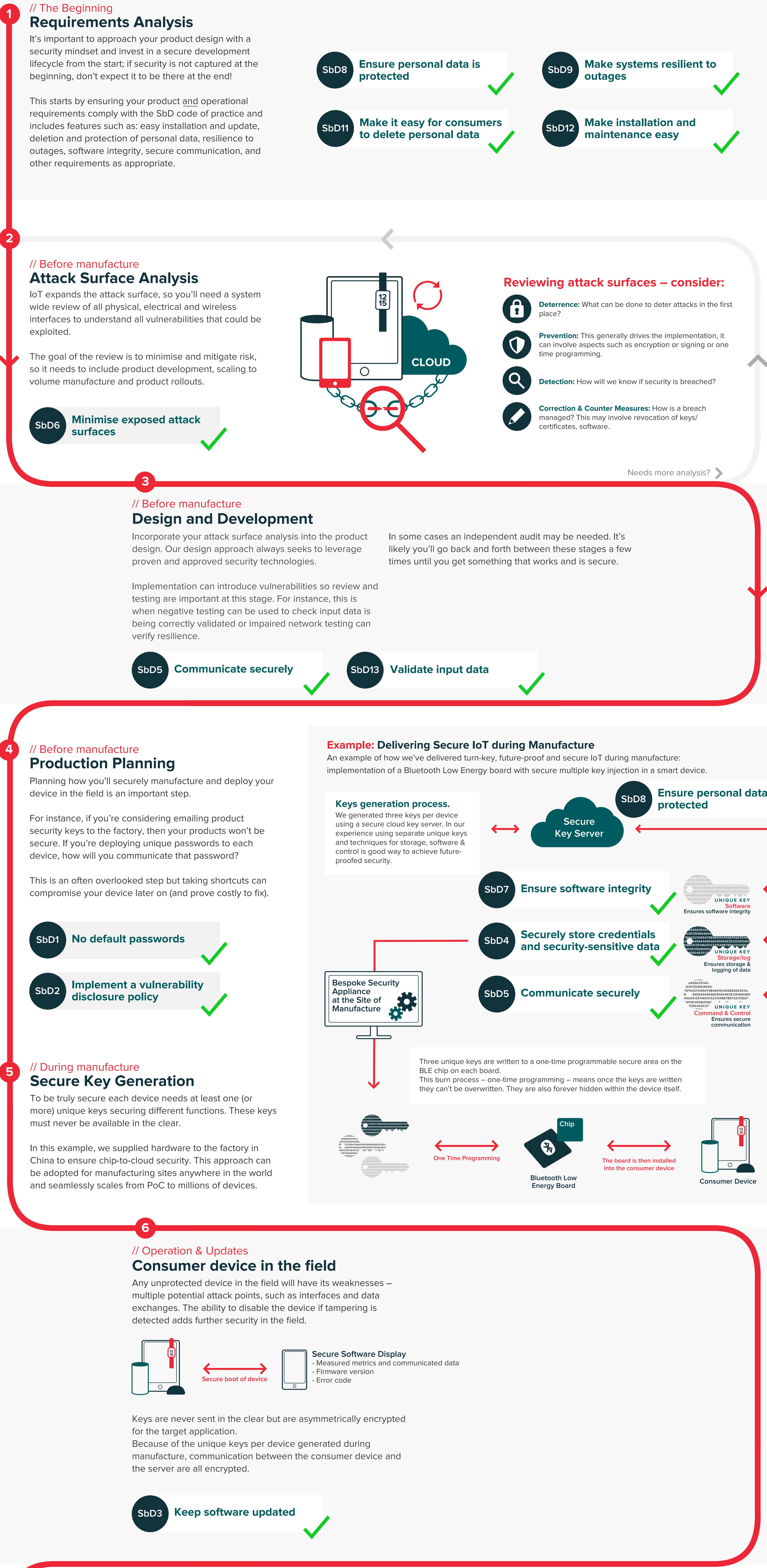
Secure by Design - Guidance

- SbD1 No default passwords**
All IoT device passwords must be unique and not resettable to any universal factory default value.
- SbD2 Implement a vulnerability disclosure policy**
Provide a public point of contact in order that security researchers and others are able to report issues.
- SbD3 Keep software updated**
All software components in internet-connected devices should be securely updatable.
- SbD4 Securely store credentials and security-sensitive data**
Any credentials must be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.
- SbD5 Communicate securely**
Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet.
- SbD6 Minimise exposed attack surfaces**
All devices and services should operate on the ‘principle of least privilege’.
- SbD7 Ensure software integrity**
Software on IoT devices must be verified using secure boot mechanisms.
- SbD8 Ensure personal data is protected**
Where devices and/or services process personal data they should do so in accordance with data protection law.
- SbD9 Make systems resilient to outages**
Resilience must be built in to IoT services where required by the usage or other relying systems.
- SbD10 Monitor system telemetry**
If collected, all telemetry such as usage and measurement data should be monitored for security anomalies within it.
- SbD11 Make it easy for users to delete personal data**
Devices and services should be configured such that personal data can easily be removed or deleted by the consumer.
- SbD12 Make installation and maintenance of devices easy**
Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability.
- SbD13 Validate Input data**
Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks must be validated.

Access full definitions and details of the UK Government’s Secure by Design principles here: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report.pdf

A 7 stage approach to securing your IoT device

//consult.red



// Securing your IoT Device Secure by Design - Is it secure?

If you're looking to design, develop or deploy a trustworthy, futureproof, secure IoT product, then why not download our Secure by Design product development checklist?

- [Download your IoT product development checklist](#)
- [Share with your network](#)
- [Share with your colleagues](#)

*Source: F-Secure Attack Landscape report H1 2019, as reported in Forbes Sept 2019, for latest report: <https://blog-assets.f-secure.com/wp-content/uploads/2020/03/04101313/attack-landscape-h22019-final.pdf>
© 2020 Red Embedded Consulting Ltd. Consult Red is a trading name of Red Embedded Consulting Ltd. Please refer to <https://consult.red/discover/red/> for more information.
All rights reserved. This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Red Embedded Consulting Ltd does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.