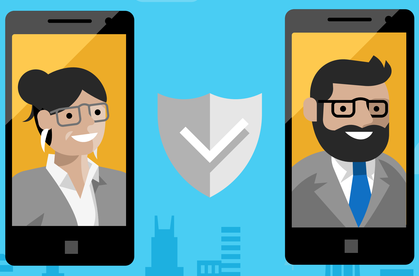
THE 7 PROPERTIES OF HIGHLY SECURE DEVICES



The IoT is enabling businesses across the world to harvest data from every touchpoint within their organizations. And with that information, they're gaining invaluable insights into their processes and enabling improvements based on accurate, real-time metrics. In other words, thanks to the IoT, businesses are now able to create, control, and optimize their digital strategies at a rate unseen before.

However, this ability comes with many risks. One of the biggest is that, unless well protected, each device represents a potential weak point from which cybercriminals can steal data, modify the device's behavior, or even compromise the entire organization's security. Furthermore, securing a device takes careful thought and, in many cases, just one layer of security may not be enough.

Use this infographic as a quick reference guide on the 7 essential properties that secure IoT devices use to keep hackers at bay.

1 | Hardware-based Root of Trust

Unforgeable cryptographic keys generated and protected by hardware. They are physical countermeasures that resist side-channel attacks.

Used if the device has a unique, unforgeable identity that is inseparable from the hardware.

2 | Small Trusted Computing Base

Private keys stored in a hardware-protected vault, inaccessible to software. Software is then divided into self-protecting layers.

Used if most of the device's software is outside of the device's trusted computing base.

3 | Defense in Depth

Multiple mitigations applied against each threat. These countermeasures mitigate the consequences of a successful attack on any one vector.

Used if the device remains protected when one layer of device's software security is breached.

4 | Compartmentalization

Hardware-enforced barriers between software components that prevent a breach in one from propagating to others.

Used if a failure in one component of the device requires a reboot of the entire device to return to operation.

5 | Certificate-based Authentication

A signed certificate, proven by an unforgeable cryptographic key. It proves the device identity and authenticity.

Used if the device uses certificates instead of passwords for authentication.

6 | Renewable Security

Renewal brings the device forward to a secure state and revokes compromised assets for known vulnerabilities or security breaches.

Used if the device's software is updated automatically.

7 | Failure Reporting

A software failure, such as a buffer overrun induced by an attacker probing security, is reported to a cloud-based failure analysis system.

Used if the device can report failures to its manufacturer.

Microsoft