IOT CYBER SECURITY

- No need for installation
- Fast protection - prior to reaching the device
- SMS notification
- History and Control panel
- Portfolio enhancing

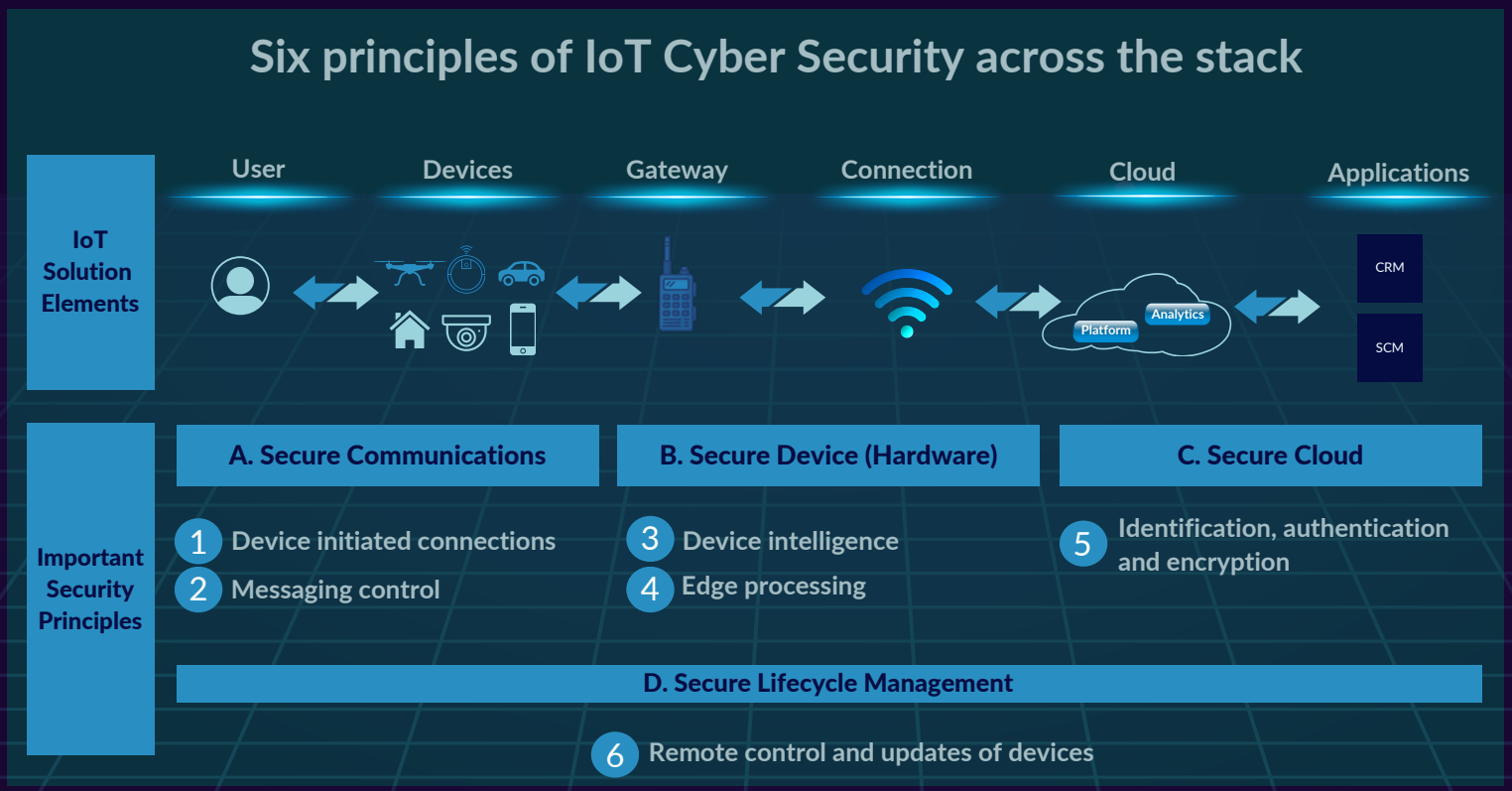
In today's digital age, the importance of cybersecurity cannot be overstated for businesses looking to expand. By making cybersecurity a central part of their expansion strategy, companies are not only safeguarding their investments but also minimizing the risks associated with data breaches. Furthermore, fostering a culture of security throughout the organization is crucial for sustainable growth.

Additionally, achieving an optimal security posture requires staying abreast of the rapid advancements in the tech landscape. If you feel like the world is moving at an unprecedented pace, rest assured that you are not alone. Back in the early 1900s, it could take several decades for groundbreaking inventions to come to fruition.

IoT security plays a crucial role in safeguarding the connected devices and networks within the IoT realm. With IoT, internet connectivity is integrated into a wide range of interconnected computing devices, mechanical and digital machines, objects, animals, and even people. Each entity possesses a distinct identifier and has the capability to seamlessly transfer data over a network. However, integrating these devices into the internet exposes them to significant vulnerabilities if proper protection measures are not in place. IoT security is a major cybersecurity challenge due to the potential for DDoS attacks using botnets.

IoT devices like smart TVs, refrigerators, coffee machines, and baby monitors are known to be vulnerable to security breaches in home environments. In corporate settings, medical equipment and network infrastructure devices such as video cameras and printers can be potential targets. A study conducted by IoT security provider Armis revealed that 59% of the IP cameras monitored on their platform in clinical environments had critical vulnerabilities. Additionally, printers ranked as the second most dangerous IoT equipment in clinical sites, with 37% of them having unpatched Common Vulnerabilities and Exposures, 30% of which were classified as critical.

In July 2020, Trend Micro made a significant discovery of an IoT Mirai botnet downloader that showed adaptability to new malware variants. This downloader played a crucial role in delivering malicious payloads to exposed Big-IP boxes.
In March 2021, a group of Swiss hackers hacked into the live camera feeds of Verkada, a security camera startup. These compromised cameras were responsible for monitoring activities within schools, prisons, hospitals, and even private company facilities like Tesla.



By the end of 2022, hackers had begun exploiting a series of 13 IoT vulnerabilities related to remote code execution. They installed a modified version of the Mirai malware on compromised devices, granting them unauthorized control over the affected systems.
In March 2023, shocking revelations emerged about Akuvox's smart intercom system. It was discovered that this device had zero-day flaws that allowed remote eavesdropping and surveillance. Furthermore, in the same month, vulnerabilities pertaining to the Trusted Platform Module 2.0 protocol were identified. These vulnerabilities, specifically related to buffer overflow, posed a significant risk to billions of IoT devices.

IoT devices are susceptible to various threats due to their weak authentication and authorization practices. This is because many devices use default passwords, making it easier for hackers to access them and the networks they are connected to, leading to data breaches or other forms of cyber attacks.

Another issue with IoT devices is the lack of encryption in their network traffic. The majority of IoT device traffic is unencrypted, exposing confidential and personal data to malware attacks such as ransomware or other forms of data breaches or theft. This includes IoT devices used in medical imaging and patient monitoring, security cameras, and printers.

Vulnerabilities in firmware and software pose a significant threat to IoT devices. Short development cycles and low price points of IoT devices limit the budget for developing and testing secure firmware. As a result, IoT devices are vulnerable to the most rudimentary forms of attack. From firmware to software and third-party apps, millions of devices are affected by standard component vulnerabilities. Even network environments can be compromised by vulnerable web apps and software for IoT devices. Without IoT security, all types of vulnerabilities make IoT devices an attractive target for savvy bad actors to launch cyber attacks.

IoT Security from Flash Networks protects IoT devices from hacker infiltration and the creation of dangerous botnets. As the world becomes increasingly reliant on IoT devices, the security of these devices has become a growing concern. Not only can threat actors damage the software and network supporting IoT devices, but they can also damage the devices themselves. Network operators can enhance their portfolio and differentiate themselves from competitors by taking advantage of the demand for protection. Promote your own network-based security to stand out and increase recurring revenue.

Flash Networks has been the leader in network optimization and security solutions for over 25 years. Flash Networks` Harmony platform has been deployed in leading telecom companies globally. Our expertise in handling high-throughput traffic enables Flash Networks to easily keep up and address technology changes.