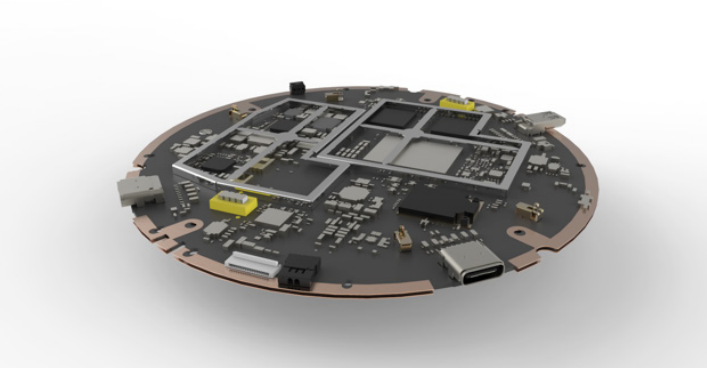
CUSTOMER SUCCESS STORY

Design SHIFT

Protecting Privacy by Safeguarding Desktop PCs with MAX32550 Secure Microcontrollers



Design SHIFT's ORWL secure desktop PC has earned the prestigious 2017 Silver Edison Award for innovation.

When you step away from your computer, there isn't much to stop someone from injecting malware into the system via one of its ports or stealing security keys from the hardware. Fortunately, Design SHIFT, a digital security and consumer product engineering company based in Menlo Park, California, has created the ORWL secure desktop PC. ORWL protects sensitive data by requiring two factors of authentication (a key and a password) and by guarding against physical attacks.

Challenge

- Robust, hardware-based security that would be easy to integrate into design

Solution

- MAX32550

Benefits

- Robust, tamper-resistant security to protect sensitive end user data
- 50% shorter design cycle due to easy integration of MAX32550 into design
- 30% lower overall costs versus custom design

"We have designed a secure endpoint," said Olivier Boireau, CEO of Design SHIFT, which started in 2009 with a team of high-tech veterans and senior engineers. "We were surprised to see all the recent hardware security attacks (in the news) and with the fact that security technology isn't being applied on consumer devices."

Small enough to fit in the palm of a hand, ORWL is a full-function, self-contained PC that runs many standard operating systems out of the box. What makes it unique is that the computer allows user access when the user is near the machine, much like the way that some car doors unlock based on driver proximity. When the ORWL user moves away from the PC, the system—including all of its ports—locks. If someone other than the user attempts to break into the system, the ORWL fails to boot up or activates a kill switch and wipes all of the data. And if someone attempts to move the ORWL, its motion sensor detects the movement and shuts down immediately.

CUSTOMER SUCCESS STORY: DESIGN SHIFT

"The MAX32550 provides a self-contained, highly integrated chip with the latest and greatest security technologies."
- Olivier Boireau, CEO, Design SHIFT

Design Challenges

The IT world, noted Boireau, is very familiar with software-based security. Physical tampering—such as malware injection, keylogging, or even device break-ins—tends to be misunderstood. This, said Boireau, is the gap that the Design SHIFT team wants to close in order to foster greater digital security. The team created ORWL using banking security technologies to protect encrypted data. The engineers sought a secure microcontroller with a robust level of security that would be easy to integrate into its design.

Solution and Benefits

Design SHIFT, which has worked with Maxim in the past, chose Maxim's MAX32550 DeepCover® secure ARM® Cortex®-M3 flash microcontroller for ORWL. The MAX32550 provides a cryptographic engine, true random number generator, and environmental and tamper detection circuitry, protecting sensitive data under multiple layers of advanced physical security.

"The MAX32550 provides a self-contained, highly integrated chip with the latest and greatest security technologies," said Boireau. "We're using technology that Maxim developed over the last 15 years, so we have a very high level of confidence in it. The payment industry has shown that hardware attacks are common. These are issues that Maxim addresses day in and day out. We also don't have to reinvent the wheel: we can take a normal PC and easily add strong security to it. Security is a lot easier with Maxim."

The ORWL is protected by an active mesh in its casing. Any attempt to break into the case triggers the MAX32550 to delete the encryption keys that grant access to the user's protected data. Design SHIFT's approach to security goes back to the "root of trust," which is what the MAX32550 enables. A secure microcontroller that executes software from an internal, immutable memory (the ROM) is the only way to protect an electronic device's hardware from attack. The software is the root of trust, since it can't be modified and can, therefore, be inherently trusted. "Lots of software guys say, once you lose control of the hardware, you're done. Establishing a root of trust with a solution like the MAX32550 provides the reassurance of strong protection," noted Boireau.

Boireau noted that integrating the MAX32550 into ORWL was very fast, enabling the team to shorten its design cycle by 50%. He was also pleased that the IC fit well into the project's budget, saving 30% of the overall cost versus a custom design.

Future Plans

Looking ahead, Design SHIFT will continue to work with partners to integrate additional security features into ORWL, such as key management, trusted OS, and other types of authentication. The team also envisions integrating its state-of-the-art authentication technologies and banking security protocols into devices such as digital cameras, laptops, tablets, and smartphones. "It should be normal that no one else can use your devices," said Boireau.

Learn more at www.maximintegrated.com

maxim integrated™