Hardware vs Software Security

Secturion Systems - September 29, 2022

Cyber-Threat Landscape

Current projections estimate that by 2027 there will be over 30 billion connected devices in use globally, that's double the number of devices from the end of 2021. As the number of connected devices increases, so does the threat of malicious attacks. These rapid changes to the cyber-threat landscape leave organizations frustrated and scrambling to stay two steps ahead of the threats.

This reality is even more front and center for those involved in the Department of Defense (DoD) arena. Nation-state threat actors have created a cyber battlefield by aggressively targeting and accessing public and private sector networks with the intent to steal, destroy, and compromise sensitive data. The DoD operates one of the largest and most complex sets of enterprise-level networks in the world. Our adversaries know this and seek to exploit any weakness they can find in the system.

Ransomware is another global threat that continues to grow as a lucrative business for threat actors. According to the Cybersecurity & Infrastructure Security Agency, "In 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors."

Ransomware threat actors are becoming increasingly brazen and sophisticated in their attacks. Attackers may hold hostage copies of stolen data and threaten to publish the data if ransoms are not paid. Other attackers have encrypted the target's data and extorted monetary ransom for the encryption key. In some cases, even after the ransom has been paid, the attackers demand a second payment before releasing the stolen data. Reducing the risk of compromise is essential and must start with a secure network.

Software vs Hardware

Software has been the cybersecurity go-to solution for years. Software products evolve over time by offering new features with each update release. Software has a reputation for being flexible, familiar, and less expensive. Hardware has had a reputation for being rigid in its ability to grow with the network and too expensive. This narrative is changing and Secturion is at the forefront of the story. With the ongoing onslaught of cyber-attacks, software has shown itself to be vulnerable, lacking, and IT-intensive. Cybersecurity-based hardware products cannot be hacked over the network and when designed correctly, are resilient to insider attacks.

Secure Systems Start with Foundational Hardware

In April of 2022, Intel™ released a survey conducted by the Ponemon Institute studying trends in cybersecurity spending as organizations try to stay ahead of attackers. The full report can be reviewed at Secure Systems Start with Foundational Hardware. Suzy Greenberg, vice president, of Intel Product Assurance and Security, said in a press release, "The security threat landscape continues to evolve, becoming more sophisticated and challenging for organizations to defend against. Today more than ever, companies are demanding assurance capabilities and hardware-enhanced security solutions that help protect the entire compute stack."

One of the key takeaways from the report was the critical role hardware technologies play in reducing risk and preventing attacks. More and more organizations are realizing they must pivot their security approach to include hardware.

What Makes Secturion Hardware Encryptors Unique?

Secturion patented hardware encryptors are designed from the ground up with the threat actor in mind. Secturion hardware encryptors provide a transparent experience for all users with easy plug-and-play installation. Secturion hardware encryptors utilize Intel™ Field Programmable Gate Arrays (FPGAs) allowing for secure firmware upgrades to future protocols and cryptographic standards. The only thing rigid about the Secturion hardware encryptor is its ability to stop hackers!

The major benefits of hardware-based data encryptors include consistent performance, excellent return on investment, reliability, and their ability to stop attacks. Hardware-based data encryptors outperform software in their ability to have consistently higher data rates and lower network latency. Secturion hardware encryptors are industry leaders providing data rates up to 400 Gbps with ultra-low latency.

Flexibility and speed are just the beginning. Secturion encryptors deliver an excellent return on investment. With a Mean Time Before Failure (MTBF) of over 250,000 hours of product operation reliability, the cost is no longer the driving factor for choosing software.

Most importantly, Secturion hardware-based architecture has no network access making it impossible to hack our encryptors from the network. Additional security includes, fail-safe and tamper features that disable the encryptor if attackers physically tamper or alter the encryptor. Secturion encryptors provide uniform foundational technology that can be implemented across all networks and platforms, resulting in a secure, resilient, and transparent network infrastructure.