How Important Is Cyber Security at the Edge?

Allxon x Trend Micro™ advances in all-round support and protection for AI/IoT and edge devices.

Cyber threats are like dormant viruses that appear invisible in a system until an outbreak occurs. Users often overlook the depth of security needed on their technology, but with raging ransomware leeching around within just a few degrees of separation, it takes more than standard built-in security to avoid feeding this monstrous multi-billion dollar industry.

What Can Happen

Cyber criminals are on the constant lookout for loopholes that can profit them millions of dollars in just a matter of days. In July 2021, a renowned company that provides network or management software to thousands of Managed Service Providers (MSP), operational technology, and IT teams worldwide was hit by one of the deadliest ransomware attacks this year, with a demanding payment of $70 million, affecting as many as 1,500 companies. Using cryptographic methods to lock owners out of their own systems, businesses were forced to shut down operations until different ransom demands were paid out by each business, and until a virtual patch was released almost two weeks later by their network provider.

Those in retail were one of the businesses that were hit hardest by the attack. A Swedish supermarket chain had to immediately close over 800 shops with point-of-sale tills and self-service checkouts made unavailable.

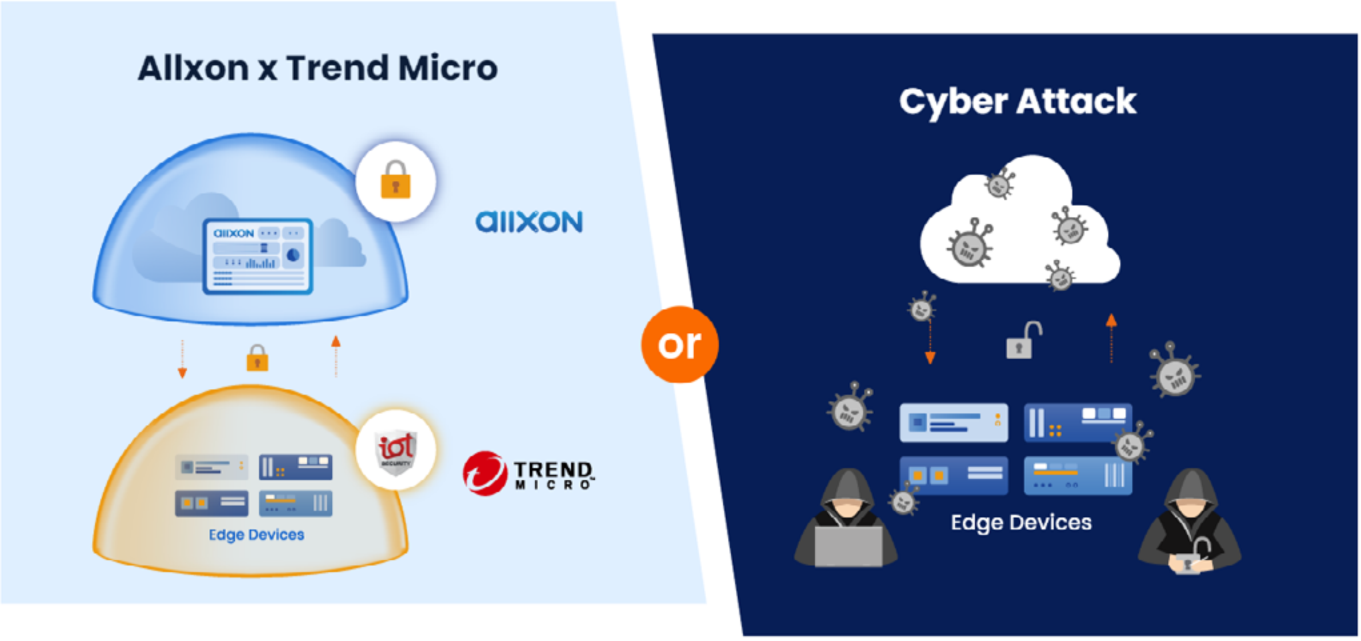
The Damaging Effects

With the above scenario, cyber criminals target the urgency and business continuity that companies offer to their customers. With a damaging 10 day waiting period for the release of a virtual patch, victims lose more than the thousands to millions of dollars spent on a ransomware payout. They lose on business, customers, public confidence, and they even potentially put others at risk of data breaches or the spread of the same malware on their client systems.

Standard built-in cyber security software is fast becoming inadequate and outdated. Businesses need multi-layered protection both in the cloud and at the edge to ensure that, in the event of an attack, owners are able to force access into their networks and devices, and to rapidly recover from such disasters.

Double Layer, Double Protection

Allxon' s recent partnership with Trend Micro™ has been a successful advancement in AI/ IoT and edge device security. Allxon focuses on protecting and helping businesses remotely manage and monitor edge devices — particularly those that are vulnerably scattered in hard-to-reach locations. With an extra layer of Trend Micro IoT Security™ (TMIS) threat defense technology added onto Allxon' s already robust networks and



servers, businesses can safely take advantage of all specialized features from both parties.

Designed for business continuity, operators are able to cold reboot or force power cycle edge devices remotely on Allxon Portal when systems appear unresponsive. Businesses can also make use of Allxon’ s remote device monitoring features to ensure TMIS protection is in full operation on all edge devices. Operators can remotely update software and firmware using Allxon’ s Over-The-Air (OTA) function to ensure their edge devices continue running on the latest and most secure versions.

Allxon also has an alerts feature that instantly notifies businesses when a TMIS agent detects suspicious behavior in an environment. In the unlikely event of an attack, Allxon offers instant disaster recovery options that help businesses restore operations back to normal, with TMIS-powered cyber security reinforced.

As cyber attackers become more sophisticated in their criminal activities, businesses seek safer, stronger, and simpler technological solutions. Allxon x Trend Micro™ enables businesses to play an active role in reducing attack surfaces, while benefiting from simple smart features that help businesses streamline and optimize safer operations management. ●

For more information on Allxon’s latest collaboration with Trend Micro™, please visit: https://www.allxon.com/solutions/trend-micro-iot-security