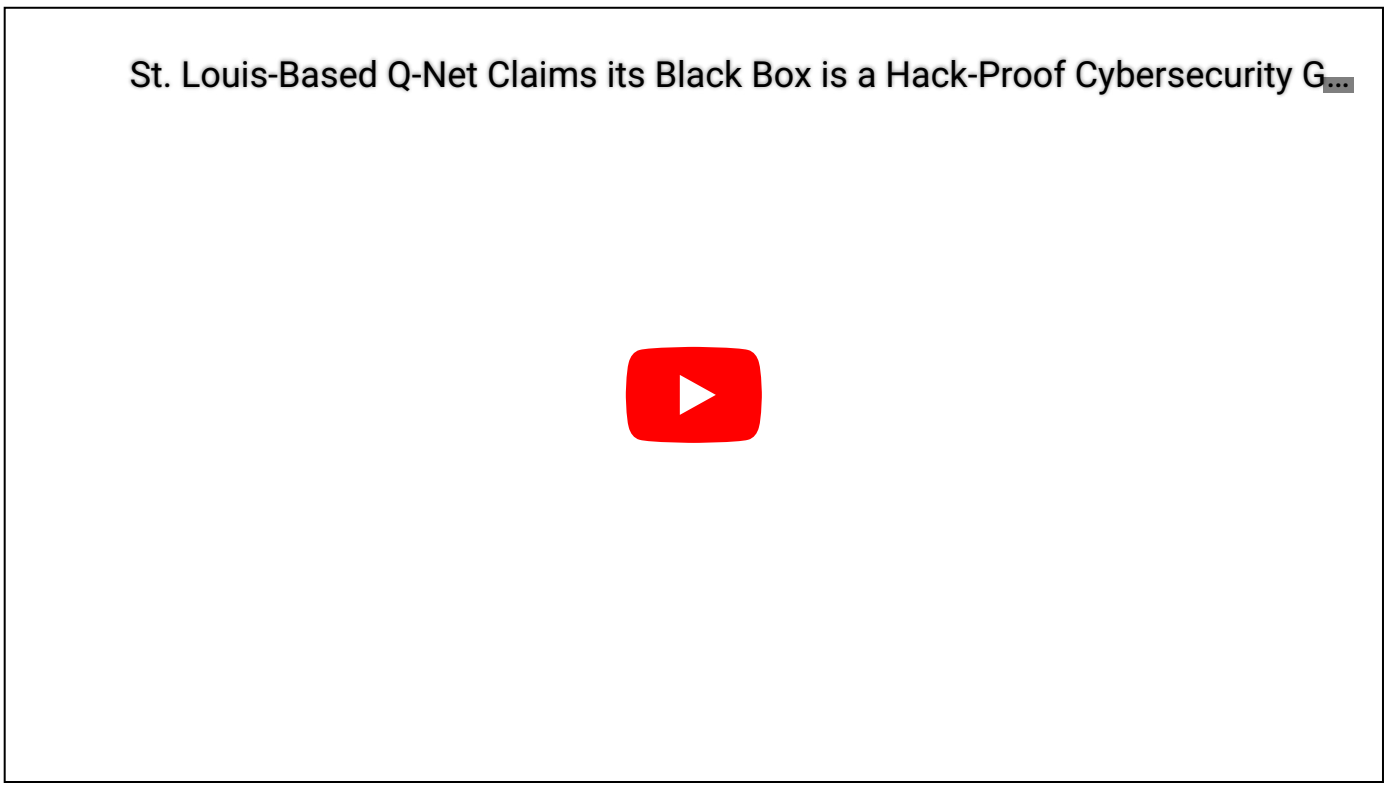
St. Louis-Based Q-Net Claims its Black Box is a Hack-Proof Cybersecurity Game Changer



By Kathleen Berger, Executive Producer for Science and Technology

St. Louis-based Q-Net Security claimed its black box technology is the next revolution in cybersecurity.

“The oil pipeline, Colonial Pipeline, and the Oldsmar water. These are real security issues that need to be solved,” said Ronald Indeck, PhD, CEO for Q-Net Security.

Q-Net’s black box, or the Q-Box, is a new hardware security solution for endpoint security.

“We are focused on protecting critical national infrastructures. The problem is that a lot of the devices that were trying to protect, the networks that we’re trying to protect, are years if not decades old,” explained Indeck. “So what we did is we came up with something where we can drop into the network and we do it in a way that’s provably secure.”

That’s why the cutting-edge Q-Box device got the U.S. military’s attention. Q-Net Security now has contracts with the U.S. Army and Air Force.

“With the US Air Force, that’s a $3 million dollar contract in order to protect what they call communications out at the tactical edge,” said Indeck. “For the U.S. Army, we are providing them a solution for the next generation network.”

So Q-Net Security needed to scale up manufacturing of the black boxes to include the St. Louis product engineering and manufacturing company Custom Technologies in Brentwood. This new approach to cybersecurity relies on a physical hardware barrier to thwart cyber attacks.

“We make sure that everyone- every packet, every piece of information- that’s trying to get through that device is authenticated. We are inline devices. So the only way you can get through that network is through us.”

Indeck admitted nothing is “unhackable” if a hacker has the money and time on Earth, which is the impossible part.

“It would require a billion, trillion years in order to break our system or to break into the network to get to the endpoints that we’re protecting,” said Indeck. “So then you say, ‘Well, maybe this is going to be put together by a state actor that could afford a billion such computers.’ So you have a billion of these computers that work a billion times faster. It would still take a trillion years in order to break our system.”

The endpoint hardware does not eliminate the need for cybersecurity software. Indeck said a combined software and hardware-based cybersecurity approach would protect vital assets, data and infrastructure. He said there is a growing need for Q-Net’s black boxes and he has a few models that fit different needs. The hope is for the Q-Box and the intellectual property for the device to become new tools everyone can add to their security arsenal.

“We can take what we have in here (the Q-Box) and put it down into a single small chip, or codified and given to somebody so that they could put it into their chips. So a Samsung refrigerator could then take our stuff, put that security into their system and it wouldn’t be an extra box. It would be already included right into that IOT device.”

Learn more about Custom Technologies https://customtechnologies.com/ (https://customtechnologies.com/) and Q-Net Security https://qnetsecurity.com/ (https://qnetsecurity.com/).

Related Posts