The Worldwide Internet Security Crisis

For twenty years the entire Internet security industry has protected networks by playing defense – watching and reacting to threats when they show up. The result has not been entirely successful. The bad guys on the offense have all the advantages and there is no question – they are winning and winning big time.

Here are the numbers:

$ 60 Billion	**2011 - Cyber Crime losses**
$ 600 Billion	**2018 - Cyber Crime Losses**
> $ 2 Trillion	**2021 - Cyber Crime Losses - Predicted**
> 10%	**2021 – Cyber Crime percent of US GNP**
$ 8.7 Million	**2018 – Average Cost per Company Breach**
$ 124 Billion	**2019 – Cyber Security Spend worldwide - Predicted**
$ 150 Billion	**2021 – Cyber Security Spend worldwide - Predicted**
> 300,000	**2019 - Unfilled Security Engineer Positions**
> 1.5 Million	**2021 - Unfilled Security Engineer Positions - Predicted**
20 Billion	**2019 - Installed IoT devices**
> 35 Billion	**2025 – Installed IoT devices - Predicted**

This all adds up to an escalating security crisis !

With the multibillion dollar increases in cyber-crime, the explosive growth of IoT devices worldwide, and a shocking shortage of security engineers, it is no wonder the world is facing a very serious Internet security crisis. Cyber-crime is now the largest wealth generating enterprise the world has ever seen. By the end of 2021 it will exceed ten percent of the US GNP.

There are currently over 1,000 security companies offering defensive solutions. But there is a major problem. Defense can only be fought at the enterprise perimeter, but the Internet of Things – the largest growth sector ever - is in the cloud where there is no security engineer and no perimeter to defend. The effectiveness of the defensive model has now peaked, it is ineffective against IoT threats, and the cyber war is being lost to the cyber-criminals worldwide. Under the current defensive model, there is no way the economics work to solve this problem.

While the overall security problem is much larger, the lack of security engineer candidates is an increasingly desperate concern. It takes a certain type of individual to work in a combative and somewhat dark trade, fighting zero-day threats and knowing that missing a software update by a few minutes or not catching a previously unknown threat could bring economic disaster down on his employer and grief to him personally. Most computer graduates shy away; it is a lot safer and less nerve-wracking to work elsewhere in IT without the risk.

The open positions are not being filled and the number of security job openings is predicted to exceed 1.5 million or more by 2022. In other words, we are fighting a cyberwar where our cyber-warriors are increasingly outnumbered and out-gunned.

What can be done?

- On the employment problem, the US government is offering to forgive up to $75,000 of a student loan, if the graduate will come to work for Uncle Sam.
- Corporations are franticly recruiting at the university level, offering unprecedented student loan payoffs, signing bonuses, inflated salaries and other perks to attract cyber-graduates – but there are simply not enough in school right now to fill the current demand.
- Governments and corporations are now actively recruiting at the high school level, offering juicy university scholarships and guaranteed employment while the student is still at university.

This current defensive model, and the steps that are being taken, no matter how desperate, is woefully inadequate by orders of magnitude. Even if all the open security positions could be filled the cyber-criminals would still have all the advantages – simply because no war can be won by fighting defense. The very nature of the open Internet and all its seemingly unfixable vulnerabilities will continue to spawn newer threats at an increasing rate.

The current corporate approach is to hire more security engineers - if they can be found - throw more money at deepening the defensive security stack - even though that model has peaked both technologically and operationally - and PRAY.

The crisis is real and it is now.
All current resources are maxed out and falling behind.
The defensive approach to perimeter security has no play in the cloud.
The question is: What is the new model that establishes trust?

TrustWrx

TrustWrx is a new breed of Internet security company. Our technology creates a threat-immune communications tunnel between enterprise servers and IoT devices in the cloud. We are not fighting defense – that model has peaked. Instead we offer a fully integrated solution that is based on a deterministic architecture that delivers end-to-end privacy – a safe ecosystem where the cyber criminals simply cannot operate.