# Finally, a Breakthrough in Cybersecurity Protection

digitaldirectorship.com/finally-a-breakthrough-in-cyber-security-protection

January 29, 2019

## *Digital Directorship -Cybersecurity*

Cybersecurity Breakthrough
For more info, contact TrustWrx via this ***email form***.

*Source: Digital Directorship: Author-Richard Spangenberg Jan 30, 2019*

*About the Author: Richard Spangenberg, CEO and Executive Director of Digital Directorship & board member at several companies, is a senior c-suite level executive, innovative strategic marketing leader, and digital/big data/AI specialist familiar with digital transformation, cybersecurity, startups, and social media integration to existing programs.*

Richard Spangenberg
CEO & Executive Director
Digital Directorship LLC

I've been researching cybersecurity issues for various industries including our country's infrastructure, the grid, and defense industries. It became obvious that the current approach of defensive protection against unauthorized break-ins continues to provide a target for hackers.  Current approaches protect against an identified threat or ensure timely awareness of a cybersecurity breach. Unfortunately, these measures must wait for the attack or breach and are reactionary rather than preventive, defensive rather than offensive leaving us vulnerable and at high risk.

After much investigation, I discovered one vendor that offers what appears to me to be a significant answer… or at least the missing component in our current approach that if added to existing methods would close the many open doors to hackers.

The company I discovered is TrustWrx.  Based in Silicon Valley, the company has a field-proven and patented security technology that inverts the security model from threat-driven to threat-immune. This is a radical concept to a security industry that has been fighting defense for twenty years. Unfortunately, fighting defense has peaked and the security war is being lost. And, I can't help pointing out that fighting defense has never won a war.

Fortunately, going proactive with TrustWrx to create a safe network where communications can be made private and secure – without fighting defense – may well be the breakthrough the Internet now needs. TrustWrx appears to be on the leading edge of that breakthrough concept. I think of it as a "*fully-verified communications firewall*" – much like the diplomatic pouch that assures end-to-end privacy – delivering new levels of security for cloud-based operations. I think so highly of this breakthrough technology that I have joined their Senior Advisory Board.

Before I discuss TrustWrx further, it might be helpful to review what I consider to be the current state of Internet Security.

## Internet Security and Privacy Today

**The industry's current fortress approach is not working.**  Today's security includes the use of firewalls, VPNs, spam blockers and other defensive measures.  Collectively, they have proven marginally effective in protecting enterprise perimeters from inbound malware, but they provide almost no protection or privacy for the advanced security needs of IoT, Blockchain and other emerging technologies.  And, the legacy security approaches allow outsiders to test and probe until they find a way into the network.

The cyber infrastructure for all systems that must be protected includes local and wide area networks, digital assets, databases, and services involved in the processing, storage, and transport of data. We see major vulnerabilities across the entire cyber infrastructure:

- Assets that are part of, or interconnect with Emergency Service Networks,
- Public Internet IP addresses and domain names,
- Global Network Access Providers and DNS and secure certificate providers,
- Cloud-connected Applications and SaaS Services,
- Cloud storage, online backup and sharing services,
- Government applications and services, Industrial, Medical, and Mobile, etc.

**As we all know, the cyber criminals are winning.** The public DNS is under constant attack as DNS records are easily compromised and legitimate domain names and valid secure certificates are registered for larcenous purposes. Overall, losses to online fraud are in the billions and increasing.

Cybersecurity is one of the hottest topics in the technology industry today, innovating and progressing at rates unseen by any other technology sector.  These include intrusion detection and prevention, cloud security, vulnerability management, fraud prevention and more. Obviously, there is a lot of noise and false starts.

A recent statistic indicates that 87% of CIOs believe their security controls are failing to protect their business. Something needs to be done.

## What is a Cybersecurity Breach?

A cybersecurity breach is an unexpected, unintended, and/or unauthorized interference with an organization’s technology systems or the data the organization maintains. When we think of cyber-attacks, we usually think of a hacker inserting a virus or malicious code into a computer system or network.  But data breaches can be caused both intentionally and unintentionally by various types of users both internal to your organization and external Internet.

Cybersecurity risks occur when a threat exploits a vulnerability, leading to an undesired event that has a negative consequence on the desired state of the network. Cybersecurity risks to network systems can have severe potential impacts, including loss of life or property, job disruption for affected network user, and financial costs from the misuse of data and subsequent resolution.

- 61% of all data breaches occur in small, medium and large companies because they tend to be more vulnerable.
- Government, military and utilities have become targets for major international and rogue states.

It has come to the point that it has reached what might be called “open warfare”.

As cyber threats grow in complexity and sophistication, attacks will be more severe against both corporate and government systems as attackers can launch multiple distributed attacks with greater automation from a broader geography and against more targets. Artificial intelligence will bring greater automation and more effective targeting of break-ins and data loss and customer privacy risk.

## What’s Currently Covered by Prevailing Security Systems?

Traditionally, the term “cyber” has been applied to only information technology (IT) systems and assets, while communications infrastructure was considered separate. However, defining cyber infrastructure as including both IT and communications systems accounts for the many ways in which these systems have converged. Authorities and agencies must recognize this convergence to more effectively counter risks.

Risks to any component could threaten an entire system, its data, and any interconnected system; be it government, military, corporate, or public. It is imperative to consider security holistically… that is as part of the publicly accessible Internet… the low-cost communications network of choice.

Having said that, the major methodologies that protect the biggest communications networks remain defensive in approach and have been proven to be overly expensive and only marginally effective. Web sessions are protected by the twenty year-old HTTPS protocol, which has proven effective but still leaves serious gaps that the fraudsters exploit.

## What are the Shortcomings of the Current Methodologies?

Typically, public and private organizations defend their web-based assets by deploying detecting tools and cybersecurity appliances at the perimeter of data centers, such as hardened routers, network firewalls, and web application firewall (WAF).  Such devices provide a valuable layer of web security, but as a sole means of defense, they have significant shortcomings.

For example:

- Such devices inspect and filter incoming traffic, and easily become a performance chokepoint and a single point of failure for cyber attackers to target.

- Because they are at the perimeter of the data center, such devices cannot protect against attacks such as DDOS attacks that seek to clog the Internet traffic upstream of data centers.
- Unlike TrustWrx "*fully-verified communications firewall*" which cannot be broken, standard network firewalls become useless if stolen credentials have been acquired on the dark web or spear-phished – bad actors walk in the front door with legitimate credentials no matter how good the perimeter firewall.
- As a sole defense against cybersecurity threats, on-premise appliances and software burden an organization in terms of capital expenditures due to their short lifecycles and the need for ongoing operations and maintenance.
- Most importantly, the explosive deployment of cloud services and the wide distribution of connected devices is dissolving the defended perimeter – rendering legacy defenses impotent against the new range of cloud threats.

## What is the Major Breakthrough?

The breakthrough is TrustWrx. It effectively "firewalls" the entire communications channel. Deterministic not defensive, TrustWrx provides an architecture for secure communications where the fraudsters simply cannot operate. Simply put, if they cannot connect or talk to a server or network, then they cannot hack into it or steal data. This is a new approach that effectively blocks external hackers from all access.

TrustWrx is a highly sophisticated secure messaging technology developed at a cost in excess of $3.5 million that is protected by two US Patents.

Best of all it's simple, easy to install, and highly cost effective. Without getting into the technical discussion of how TrustWrx works, the following should illustrate it fairly well:

- Bullet-Proof Access Control
- Dual, Multi-Tier (three levels), Two Way Communication Encryption
- Fully verified source IP addresses and source machine fingerprints
- All ports protected by encrypted port knocking
- Dynamic Key Codes Enhance Protection
- Replacement of the DNS System with a Secure Policy Gateway
- TrustWrx alone completes the Missing Link in Internet Security

TrustWrx is a new kind of cyber-security company. They integrate the critical components of messaging privacy and transport security to deliver next generation security technology. TrustWrx combines privacy, encryption, malware protection and compliance with other enabling technologies to achieve an integrated application solution – accessible to businesses of any size.

TrustWrx departs from conventional usage of many standard protocols and components to achieve a new level of comprehensive security and privacy. A carefully designed departure from standard practices is required; for example, shifting away from exposed DNS calls in favor of a secure policy gateway for device and packet verifications. This replacement of the public DNS is step one toward real security because the publicly visible nature of the DNS and publicly exposed routing is one of the main barriers to Internet privacy.

TrustWrx covers OT security as operational hardware is protected via the TrustWrx system and Internet IoT communications as well. TrustWrx blocks espionage and sabotage along with preventing data breaches, loss of privacy, and break-ins for other nefarious activities. It is a perfect solution for the electric grid, healthcare, government, military and corporate requirements.

TrustWrx delivers messaging security, privacy and anonymity, along with strong endpoint protection against all DNS exploits, cryptography attacks, key and password disclosure, account imitation, ransomware, malware, and most other known threats to the privacy and security of power grid operations and other operational networks. The TrustWrx solution is built on proven security disciplines and methods that simply do not allow present and future threats to operate in any part of the Internet messaging space.

TrustWrx triply encrypts all communications and messaging – periodically changing automated encryption keys on the fly. The combined effect – along with other protective features – is the most comprehensive and fully integrated cloud security available in the market today.

– Contact TrustWrx via this ***email form*** –

## A Lab Tested and Field Proven Technology

A suite of security and performance tests were conducted through extensive third-party lab tests and evaluations for end-to-end security that resulted in no reported security vulnerabilities. All socket calls, file writes or any other form of I/O were analyzed for possible attack points and none were found.

This is the answer many of us have been waiting for. Of course, specific industries and companies will require customization for front-end system management and back-end reporting.

NSS Labs: The TrustWrx technology has been performance and stress tested by an independent laboratory (NSS Labs.) In one 8-hour day, over one million average size messages (totaling over 6 terabits) were sent and received by one thousand message clients. The test did not stress or create a problem on a standard two-server installation running Linux and MySQL.

| | |
|---|---|
| Neohapsis Labs: | A multi-phase Black Box vulnerability test was conducted by Neohapsis Labs, reporting zero vulnerabilities.<br>Black Box Testing is a software testing method in which the internal structure/ design/ implementation of the item being tested is NOT known to the tester. Black box testing is investing the system just like any outsider would do, using tools for detecting the attack surfaces and examining the system to check for internal information access or leakage. None were found. |
| DIACAP : | A qualifying DIACAP (DoD Data Center Operations) test had also been conducted on both client and server side. The qualifying test was cleared on the first pass with no reported problems. |
| UT Dallas: | SAIAL testing by UT Dallas Digital Forensics Institute Cyber Security Institute tested transport vulnerability testing of wireline and wireless access to the TrustWrx protected system. Despite numerous attempts, including using custom class loaders that delivered all output to a file for later analysis, the analyst was not able to intercept any keys. Careful review of all other agent class files, some of which were obfuscated to one degree or another revealed no vulnerabilities. All socket calls, file writes or any other form of I/O were analyzed for possible attack points and none were found. |
| Monterey Group: | A Theoretical Analysis conducted by David Rice of the Monterey Group, a security consulting firm, validated TrustWrx usage of a combination of symmetric and PKI cryptography to encrypt all communications.<br>David Rice is today head of Global Security for Apple.<br>“Since messages within the TrustWrx cloud can only come from verified and approved end points, recipients can be confident they are in fact receiving authorized and valid communications from the sender. This is not possible with traditional communications since unprotected messages could be spoofed by malicious actors.” |

## Want to Know More?

Contact TrustWrx via this ***email form***.

Our first response efforts will be to media, corporations, government, military, utility, healthcare, transportation, financial, and other high need categories.

| | **Related Article Links:** |
|---|---|
| Jan 20, 2019: | Finally, a Breakthrough in Cyber Security Protection |

**Related Article Links:**

| | |
|---|---|
| Jan 26, 2019: | Cyber-Hijacking Campaign Sets off Global Government Alarm Bells |
| Feb 01, 2019: | Secrecy Reigns as NERC Fines Utilities $10M citing Serious Cyber Risks |
| Jun 12, 2017: | CRASH OVERRIDE: The Malware that Took Down a Power Grid |
| Jan 03, 2019: | Did IoT Cyberattacks cause NY Power Transformers to Explode? |
| Dec 28, 2019: | New York sky turns bright blue after transformer explosion. |
| Jan 01, 2019: | Your data was probably stolen in cyberattack in 2018 |
| Jan 22, 2019: | Cyber Attacks are leading to US Navy Collisions |
| Dec 28, 2018: | Did IoT Cyberattacks cause NY Power Transformers to Explode? |
| Mar 15, 2018: | Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says |
| Mar 15, 2018: | Cyberattacks Put Russian Fingers on the Switch at Power Plants |
| Nov 28, 2018: | Russian Hackers Haven’t Stopped Probing the US Power Grid |
| Jun 07, 2018: | The damage from Atlanta’s huge cyberattack is even worse than the city first thought |
| Dec 03, 1018: | TOP 10 of the world's largest cyberattacks |
| Dec 15, 2017: | A New Industrial Hack Highlights the Cyber Holes in Our Infrastructure |

– Contact TrustWrx via this ***email form*** –