TrustLeap
Global-WAN

Cyber Fixed
with Future-Proof Security

Partners can operate their own, government-audited as "future-proof", Global-WAN network.

Executive Summary

Today, finance, energy, water, telecoms, transportation, logistics and government depend on the Internet. ***Digital sabotage*** can cost several billions of dollars, disrupt the most advanced societies, compromising economic and social stability. The Economist calls cyber security a ***"market failure"***. The Internet of Things (IoT) will make it a cataclysm.

*In **2010** Global-WAN governments-audited "future-proof" security has made **Defense more profitable than Offense**.* Only future-proof ***Security can generate profits while waving costs and liabilities***.

As new revelations have officially confirmed that **CPU backdoors** prevent software from running safely, the only way for devices to stay secure is to rely on **Global-WAN VPN network adapters**.

13 Feb. 2017

SECRET INTELLIGENCE SERVICE MI6

*"I believe **Pierre Gauthier** is the best in his field and deserves to have the opportunity to meet key people like yourselves given the pre-eminent role Mayor Giuliani and all of you are playing in the Cyber-Security field both professionally and internationally via your organisations and under the banner of the new US Administration."*

Andrew Fulton, ex-MI6 Chief of Station in Washington D.C. (United States of America)

Global-WAN

3 June 2017

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

*"Contact the UPIC (part of DFF) **for them to realize which technical and industrial competences we have** so they can better conduct the cyber-strategy on the way of success and prevention. **We have to get out of the 'reaction-only' syndrome** as, in today's situation, we will not have any success when facing events against which we can less and less protect ourselves."*

Gerald Vernez, Chief of Cyber-Defense, Swiss Federal Department of Defense

Global-WAN

Origin of the Business Idea

In **1998** Pierre Gauthier created **Remote-Anything (RA)**, and sold ***280m licenses*** in ***138 countries*** – from governments, banks, manufacturing plants, and universities, to nuclear plants.

In **2005** anti-competitive practices killed RA. **Global-WAN**'s brand was registered in **2006**, "**unconditional**" security ("unbreakable" in academic jargon) was created in **2007**, and first audited by the **French DRM** in **2008**.

Global-WAN software was online in **2010**.

MISSION: let the people, organizations and machines safely operate, communicate and trade in a sustainable way, without unwanted interference.

A Weaponized Ecosystem

Despite ever-growing investments, we all are victims of increasing security breaches because... failure is planned:

"How do you protect what you want to exploit?"
– Scott Charney, VP Trustworthy Computing, MICROSOFT

*"Across the federal government, about **90% of all spending** on Cyber programs is **dedicated to offensive** efforts, including **penetrating** the computer systems of adversaries, **listening to communications** and developing the means to disable or **degrade infrastructure**".*
– NSA Deputy Director Rick Ledgett

Ever-Failing US NIST Standards

"Computational" security (AES, SHA256) consists in rounds of defined arithmetic operations. It generates ciphertext **domain-specific algebraic structures** that let adversaries reconstruct the encryption algorithm, and immensely reduce the key-space so it can be brute-forced, revealing a unique key and plaintext.

"Post-Quantum" security (US NIST public-key selected candidates) is yet another backdoor, based on **number-theoretical security assumptions** (the reason behind today's public-key encryption standards replacement).

INSANITY: doing the same thing over and over again and expecting different results.

Global-WAN

Overdue Regulatory Revolution

2019: a **long-awaited regulatory change** finally lets Global-WAN protect end-users from the – ***now unwanted*** – backdoors:

*"The **move away from prescriptive standards** towards a **focus on outcomes** under the NIS Regulations was welcomed because: **Standards are soon rendered out-of-date** by fast-changing threats and the **frequent discovery of previously unknown vulnerabilities**". We must "anticipate fast-changing threats **instead of slipping into a 'tick-box compliance' with static standards**."*

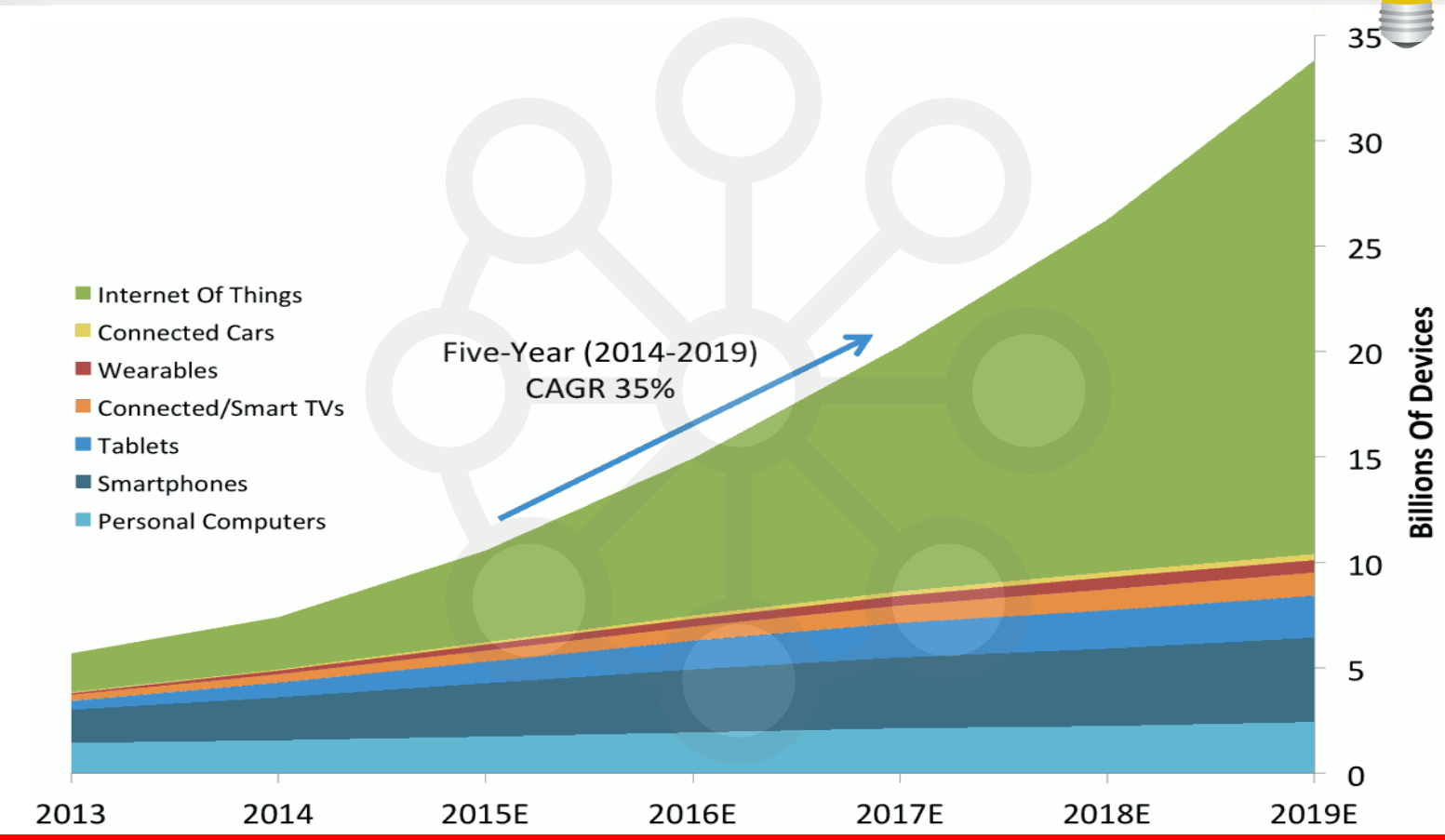
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

OBSOLETE

Cyber Security of the UK's Critical National Infrastructure - HC 1708 - UK Gov. Joint Committee on the National Security Strategy (Nov. 12th 2018)

Global-WAN

Connected Devices (Bn)



Market Value-Proposition

The ***2015 NSA call for a "frontdoor" to replace the "backdoors"*** has been ignored by the IT sector, despite further support from the EU, the FBI and the US Center for Strategic International Studies.

As a result, the 2015 *"bad situation"* is now an unaccountable chaos. In Nov. 2018 the **UK government** stated that due to recurring faults ***standards and compliance cannot bring security***.

Result: Global-WAN is the only available "*frontdoor" delivering both full-compliance and* ***security that will not fail end-users***.

Government Secured

*By Securing the **CRITICAL INFRASTRUCTURE**:*

- **Services** (Army, Police, Justice, Finance, Healthcare, Education...)
- **Assets** (Water Supply, Airports, Logistics, etc.)
- **Energy** (Pipelines, Nuclear Plants, Electricity Grid)
- **Networks** (Internet, GSM, LTE, Radio, etc.)
- **E-Admin** (e-Votes, e-Medical, e-Fiscal, etc.)
- **Economy** (Banking, Insurance, Industry, etc.)

"The insurance market is increasingly moving to a service provider model - providing companies with help in mitigating their risks, not just paying claims."
Jean Bayon de la Tour, Cyber Development Leader, Marsh

Global-WAN

Crisis = Opportunity

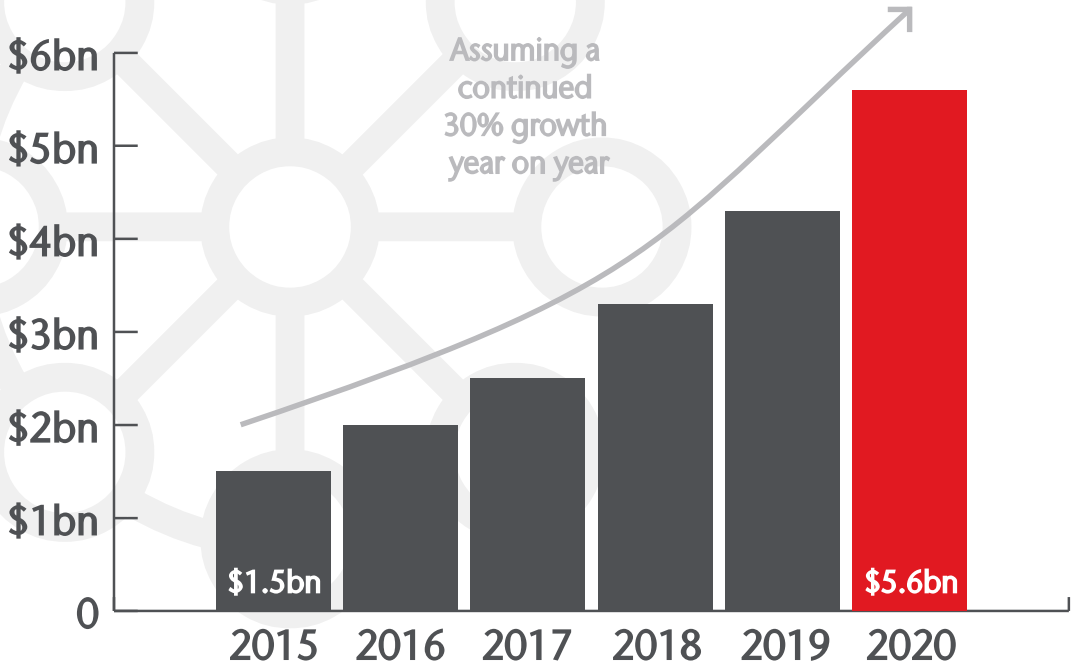
- **Issue** | ubiquitous critical infrastructure vulnerabilities;
- **Need** | plug & play solution for massive deployments;
- **Costs** | a network adapter per user (zero learning-curve);
  HSMs (high-security modules) let a compromised OS or CPU exfiltrate unencrypted data.

"To avoid lurid headlines about car crashing, insulin overdoses and houses burning, tech firms will surely have to embrace higher standards." - The Economist

Global-WAN

Market Research

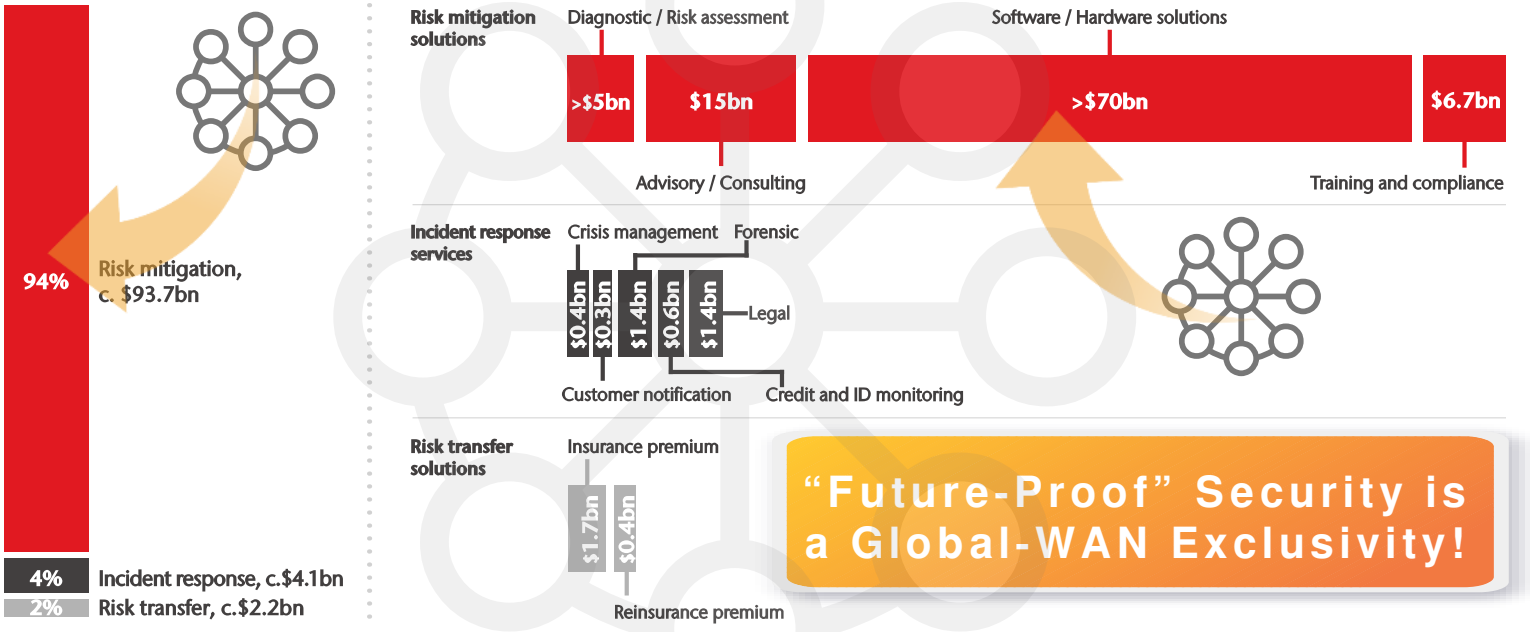
US standalone cyber market projection



Global-WAN

Market Segments

2015 breakdown of total cyber security market (c.$100bn) by segment



Sources: Company websites, Insurer websites, Broker websites, RIMS 2016, Aon Cyber Committee research, Cybersecurity Ventures, Owler, Ranker, Hoover, Bessemer Venture Partners, Gartner, Verizon, MicroMarketMonitor, Aon Inpoint analysis

Global-WAN

Market Target Profiles

Estimated breakdown of standalone cyber market in the US

Company type	Industry and revenue	SME	Mid-market	Large corporate	% of total	
Companies storing personal data	Technology	$39.0m	$18.0m	$14.0m	5%	$242.0m (17%)
	Telecoms and media	$3.3m	$8.0m	$13.0m	2%	
	Education	$5.3m	$46.0m	$21.0m	5%	
	Professional services	$9.4m	$43.0m	$22.0m	5%	
Financial transactions driven companies	Retail and wholesale	$76.0m	$141.0m	$93.0m	21%	$876.0m (59%)
	Financial institutions	$31.0m	$180.0m	$227.0m	29%	
	Business services	$6.7m	$47.0m	$33.0m	6%	
	Hospitality	$5.5m	$22.0m	$13.0m	3%	
Companies exposed to operational risks	Manufacturing	$56.0m	$19.0m	$16.0m	6%	$126.0m (8%)
	Utilities	$1.3m	$4.1m	$15.0m	1%	
	Energy (Oil and Gas)	$1.2m	$3.6m	$9.0m	1%	
Companies storing personal data & exposed to operational risks	Healthcare	$3.4m	$103.0m	$81.0m	15%	$256.0m (17%)
	Transportation	$13.0m	$14.0m	$10.0m	2%	
	Total	$282.0m	$649.0m	$567.0m	100%	$1.5bn

Large corporate / Mid-market / SME / $282m / $649m / $567m

Global-WAN

Market Growth Drivers

Key growth drivers

Legislation — Data breach legislation has been enacted in 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands

Awareness — In 2015, US firms ranked cyber as their 5th most important risk, compared to 18th back in 2011

# of breaches — More companies are uncovering data breaches and reported breaches in the US have risen by c.325% since 2006

Higher cost — On average, the cost of a data breach is 60% higher than it was in 2006

	Pre-GDPR	Post-GDPR
Legislation	• No general legislation mandating notification following a breach • Weak regulators with limited ability to sanction firms • EU laws enforced with varying degrees of severity	• Strict regulation with a general requirement to notify in the event of a breach • GDPR regulations allow for a fine of up to 2% of global turnover • EU wide enforcement of GDPR
Awareness	• Cyber already recognised as an emerging risk in Europe • Aon clients currently view Cyber as 14th biggest risk	• Increased awareness expected to be driven by GDPR with higher numbers of data breaches likely to be publicised • Aon clients already expect Cyber to be their 8th biggest risk by 2018
Number of breaches	• European breach rates are already growing fast, 36% since 2011	• Mandatory notification is likely to drive known breach numbers much higher • In the US where similar legislation already exists there were 1.1k (c.85%) more publicised breaches compared to Europe in 2015
Cost	• The cost of data breaches in Europe currently lags that of the US by 35% on average	• European firms are likely to suffer higher costs as a result of GDPR • US firms have seen the cost of data breaches rise at a rate of 9% a year since 2012

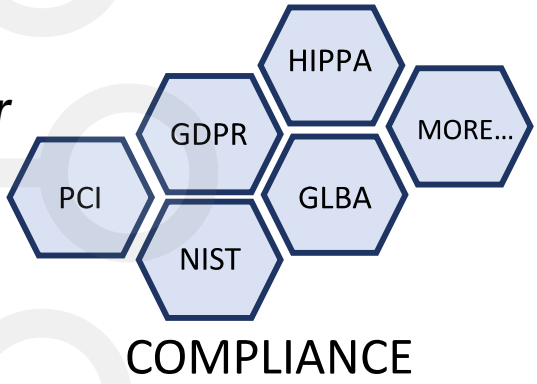
2018 - GDPR implemented

Global-WAN

Market Validation

In **2015**, Global-WAN invited several **Swiss C-Level executives** to a meeting in **Zurich** to exchange about their needs and concerns regarding IT security.

All of them expressed frustration about a bleeding ***performance gap between their recurring investments in security and the lack of results***. All but one joined Global-WAN (yet, Swisscom did not participate as initially planned):



SECURITAS UBS Leclanché swisscom

Market Access Strategy

In **2007**, Global-WAN tried to enter the market without knowing at the time that a *"backdoor era" was enforced*. Six years later, the **2013** Snowden NSA leaks have pushed the NSA to recognize in **2015 the need for a *"frontdoor to replace the backdoors"***.

In **2019**, many US players like FACEBOOK, GOOGLE or even DARKTRACE feel the need to transform the **public perception** from "data-collectors" to "privacy or security service-providers".

Global-WAN will leverage a 12-year knowledge and tech with **a free CHAT App**, high-end tech **licensing** and a possible **buy-out**.

Digital Marketing

Before its 2010 IPO **Skype** boasted 124m active users (6% paying). Among the 500m **Dropbox** 2016 accounts only 0.03% were paying.

By linking the old telephone network and Internet teleconference Skype had more success than Dropbox (storage: data dead-end).

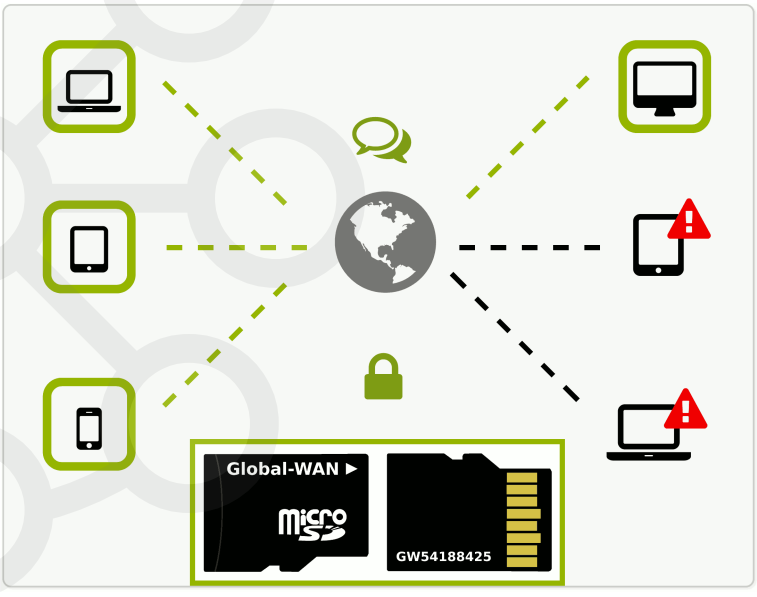
Global-WAN will do much better than Skype: *all network application*, payment, or storage solution is ***leveraged by future-proof security***.

Marketing campaigns will spread awareness and attract all with a ***freemium* Global-WAN Chat App** delivering equally-exclusive **Global-WAN payment services** (PSD2 opportunities).

Digital Partnerships

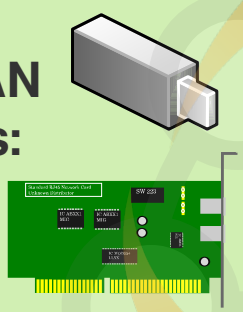
By **securing products** with Global-WAN, **vehicle manufacturers** will *at the same time* **reduce their liabilities** (and insurance costs).

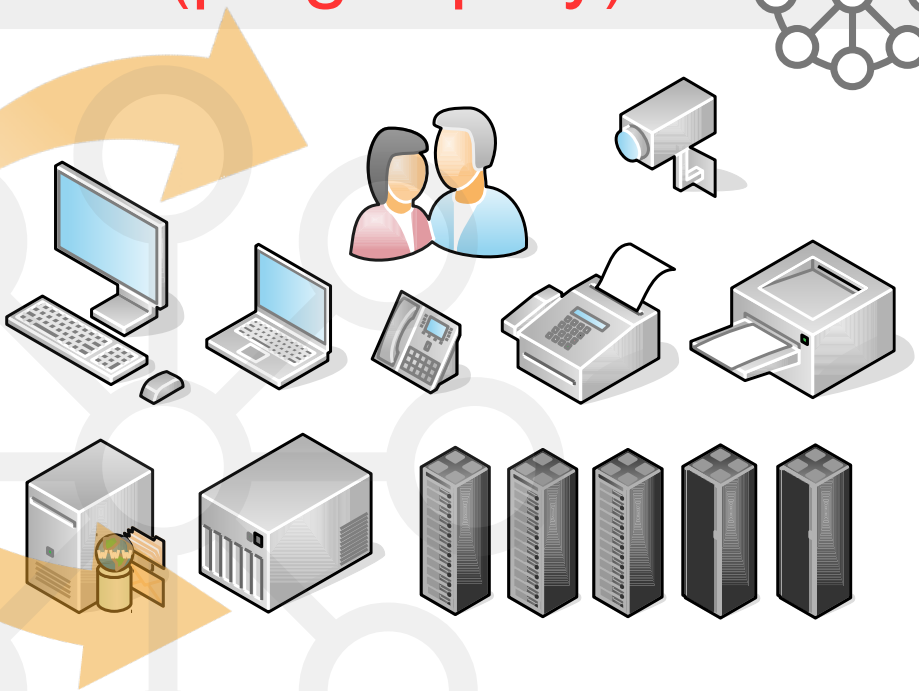
Each new contract will provide significant market-share & revenue growth in different sectors.



Network Adapters (plug & play)

Global-WAN VPN Gates: network adapters





Hardware Manufacturers love to push a new generation of devices. **End-Users** love to buy and deploy future-proof technology: they are sick of planned-obsolescence – especially for security purposes!

Certifications & Tests

In **2014**, the **Swiss EPFL Microelectronic Systems Laboratory** has conducted a 30-page study (costs/delays) of Global-WAN chips (academic documents available on demand).

Under NDAs, **manufacturing contracts** were signed with the two largest world **foundries**, and **integration contracts** of these chips with a major IoT manufacturer (supplying Apple Inc):

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

tsmc

SAMSUNG

Audited Unconditional (future-proof) Security

"The greatest advance in cryptography of the past 30 years!"

All plaintext candidates are mathematically equally plausible so adversaries **can't reduce the key-space**, nor they can tell which solution, among all the possible plaintexts, is the original text.

Known-plaintext attacks are defeated as the ciphertext byte-order (which differs from the plaintext byte-order) depends on the whole plaintext (and not only on the secret key).

Further, these algorithms are **ideal for the IoT**, consuming far less resources (energy, memory) than any past NIST standard.

Global-WAN

Status & Milestones

2019: Global-WAN invited at the **Munich Security Conference**
2018: Global-WAN invited to meet **government bodies in China**
2017: Global-WAN invited by **stock-exchange** to meet **central bank**
2016: Global-WAN is **audited by the UK Gov. (GCHQ experts)**
2014: Global-WAN Swiss **EPFL/CTI ASIC chips** study (costs, delays)
2010: **http://Global-WAN.com/** is publicly online (first on trustleap.com)
2009: **http://G-WAN.com/** Application Server is publicly released
2007: Global-WAN project (provably-safe crypto found, brands registered)
2005: 280 millions of RA/DS licences deployed in 138 countries
2003: Firewall-traversal & by-design security international patents (DS)
2002: **http://SummitPartners.com/** offers *"liquidity for founders"*
1999: **http://Remote-Anything.com/** (RA) is publicly released
1998: TWD Industries LLC was first incorporated on 23/04/1998

Global-WAN

US Regulatory Environment

NSA, 2015:

*"**Back-door** **I think this kind of shady**. Why wouldn't you want to go in the **front-door** and **be very public**? We can create a legal framework for how we do this. **It isn't something that we have to hide.**"*

Admiral Michael S. Rogers, Director of the NSA
Commander of the U.S. Cyber Command

Intl. Regulatory Framework

*"The **best outcome** would be a multilateral agreement that **lets people secure their data with the strongest possible encryption**, using products that allow for the recovery of plaintext by national authorities. The key to legitimacy is that **citizens will accept actions from their own governments that they will not accept from others** (particularly the U.S.)."*

U.S. Center for Strategic International Studies (CSIS)

Frontdoor Benefits

"**Compliance" finally equals "Security", preventing**:

- unwanted influence, blackmail, and sabotage;
- corporate users and consumers from criminal hacking;
- finance from erased/hijacked servers (SWIFT case);
- (re-)insurers from ever-expanding Cyber risk exposure;
- regulated Internet monitoring authorities from being ashamed in dire headlines for having compromised the security of all for the sake of doing their work!

Global-WAN

Game-Changer Innovation

- **Future-Proof Security** (Unconditional, Post-Quantum)
- **No Obsolescence** (No Need To Upgrade/Enlarge Keys)
- **Deploy & Forget** (No Remote Upgrades Are Needed)
- **Only Way to Restore Trust** (Especially Internationally)
- **Fully-Compliant** (EU, NSA, FBI, CSIS “Frontdoor”)
- **IoT** (Much Lower Overhead and Latency than AES)
- **Biz-Model Generates Profits** (instead of Costs/Liability)
- **Plug & Play** (Transparently Secures All Devices & Apps)

Global-WAN

I.P. & Freedom to Operate

In **2003**, the RA/DS author discovered that **patents** are worthless if you cannot prevent better financed players from violating them, and that **strategic patents** are blocked by the US to preserve their holly *"freedom to operate"*... at the foreigners' expenses.

Way to go: **defensive patents** disclose enough to let you block copycats but they don't disclose the whole method so you can really protect your know-how.

The Global-WAN brand was registered in 2006 and several associated domain names have been secured too.

I.P. & Asset Protection

Global-WAN will more surely protect its unique Know-How with **manufacturing contracts** that schedule penalties in case of infringements (the rules are settled in advance, which is immensely shortening judiciary procedures).

This works well with **foundries**, which can opt to licensing a part of a customer I.P. to market it to its other clients (yet **another source of revenues** for Global-WAN ASIC chips).

Trade Secrets, **Known-How**, **Show-How**, and **Copyright** are easier to control than patents and are part of licensing.

Business Model's Target

*"President OBAMA approved a previously undisclosed **covert measure that authorized planting Cyber weapons in Russia's infrastructure**, bombs that could be detonated if the United States found itself in an escalating exchange with Moscow."*
The Washington Post, June 2017

Global-WAN offers partnerships with critical infrastructure operators to let them ***exclude unwanted interference***.

Operators deploy Global-WAN and generate revenues by billing their customers EUR 1 per month for the resilience of the service. And Global-WAN receives a share of these subscriptions.

Business Model's Results

Calculation details: Year #1 revenues = EUR 180m with 5m users, so 180/5 = EUR 36 of annual revenues per end-user (at least one sale of a Global-WAN chip and a 12-month subscription):

Year	1	2	3	4	5
Subscribers	5m	30m	90m	180m	288m
Growth Rate	5,000%	600%	300%	200%	160%
Revenues	Eur 180m	Eur 1bn	Eur 3bn	Eur 6bn	Eur 10bn
EBITDA	Eur 59m	Eur 360m	Eur 1.5bn	Eur 2.3bn	Eur 3.6bn
EBIT	Eur 57m	Eur 354m	Eur 1.2bn	Eur 2.1bn	Eur 3.5bn

Pricing freedom: If users got free chips, then they paid EUR 3 per month to use Global-WAN. If users paid chips EUR 24 then EUR 1 per month was paid to use Global-WAN. *Both pricing models lead to the table numbers above.*

Sales Year To Date

Until late **2018**, and for decades, **regulators have enforced ever-failing security standards** for the purpose of **legal monitoring**.

Backdoors have **destroyed trust**, everyone's **safety**, as well as **innovation** and technology-driven **competition**: only "fully-compliant" players (using defective standards) were allowed to reach the market.

In **2019**, Global-WAN is the only governments-audited, 12 year-old, **mature frontdoor solution** ever made publicly available. But it is also the sole "universal security" solution scaling from RFID tags to data-centers (AES is too big to merely fir on RFID tags, which cannot run it).

Global-WAN network adapters deliver sustainable security that cannot be abused... on the top of being now officially "fully-compliant".

Funding Needs

Software development does not need much funding (the first version of RA, like the first version of G-WAN, took 3 months to write) but **Hardware manufacturing** requires significant funds:

- **Year 1: ASIC chip Design (EPFL: 1 year) EUR 25 millions**
  - Defensive patents (not disclosing the method),
  - Partners & Foundry *binding* contracts, and QA chip tests.
- **Year 2: Chip integration (IoT, NIC, Radio) EUR 25 millions**
  - Global-WAN chips deployments on selected markets.
- **Year 3: Market Entry (Sales Force) EUR 25 millions**
  - Worldwide deployments and regional agreements.

Investor Exit

Never before a software + hardware manufacturing project has been prepared for so long – *the cycles here are more similar to the Pharmaceutical industry* – ***just like the revenues:***

Year	1	2	3	4	5
Subscribers	5m	30m	90m	180m	288m
Growth Rate	5,000%	600%	300%	200%	160%
Revenues	Eur 180m	Eur 1bn	Eur 3bn	Eur 6bn	Eur 10bn
EBITDA	Eur 59m	Eur 360m	Eur 1.5bn	Eur 2.3bn	Eur 3.6bn
EBIT	Eur 57m	Eur 354m	Eur 1.2bn	Eur 2.1bn	Eur 3.5bn

Global-WAN chip subscriptions will be extremely lucrative – *even with conservative projections*. Assumptions: EUR 25m investment (20% stake).

Exit: Sale or IPO at 2.5 times Global-WAN's 5th year revenues.

SWOT Risk Analysis

Successful Global Mass-Market Experience (Remote-Anything)
Preceded CH/EU/US Regulator "Frontdoor" Calls
Decisive Competitive Advantage
21 years in the Internet Business
12 years Polishing Global-WAN
2018 UK Government Audit
Unique Future-Proof Tech!
Global-WAN online in 2010
(proven mature technology)
By Far The First in Market!
Self-sufficient: No Sabotage!

Global-WAN ASIC Chips Require Funding
Clients: Governments or Populations?
Lobbying Still Dominates Markets
New US Competitor (US, Credible?)
Will Chat/Payment App Be Enough...
...if the World Sticks to Backdoors?
Will Finance Support a "Frontdoor"?
Adoption: Westerners and/vs BRICS?
How Long To Wait For Cataclysm?
Will Venezuela Outage Be Enough?
How the Tech Ecosystem will React?

China (Plants) in Dire Need...
...For a Neutral "Frontdoor".
Long Awaited Overdue Tech:
360° Industry Partnerships:
Covers All FinTech Needs
Covers All MedTech Needs
Covers All InsurTech Needs
Every Single Sector in Need
TWD Mandated by Regulators as New Standard?
Mandatory Tech for Electronic Money (Central Banks, PSD2...)

Backdoors: US-Tech Bread & Butter
Offense is Still 90% of DoD Budget
Backdoors Allow False-Flag Attacks
Corruption Still Rules Global Markets
Chat App Might Need Stealth Traffic
Attacks Can Divert TWD Resources
Can TWD Prevent Tech/IP Leaks?
Would Licensing Raise Challengers?
What other Threats do we Ignore so far?
Can Stealth Threats Operate without Detection?

TWD Industries AG

TWD Industries AG
Paradiesli 17
CH-8842 Unteriberg SZ
Switzerland
http://twd.ag/

About TWD Industries

Founded in 1998 by **Pierre Gauthier**, **TWD Industries** is a privately held company. Commercial Register history: **USA**: “TWD Industries LLC” on 23/04/1998 (closed), **France**: "TWD Industries SAS" on 18/02/2002 (closed), **Switzerland**: "TWD Industries AG" since 15/01/2009 (active), owned at 100% by **TWD Holding AG** (active), which itself belongs at 100% to Pierre Gauthier.

TWD Industries AG protects digital assets with **cryptanalytically unbreakable** technology (safe against unlimited computing power as it is proven mathematically that no algebraic structures can be exploited to reconstruct the encryption algorithm, secret key, or plaintext). The **Global-WAN** secure platform leverages offers of enterprise, cloud, networking, digital media and financial services in global strategic markets.

TWD lets partners and users form dynamic ecosystems where duly accredited strangers can safely trust each-other. Establishing widespread trust enables organizations to secure their infrastructure, raise the value of their offers and safely market their digital assets.