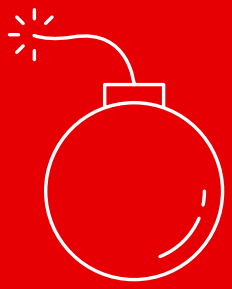
Something big is coming!

Changing the game!

Another bombshell!

In late February 2018, a large-scale cyber-attack on the German parliament exposed just how vulnerable even seemingly well-safeguarded systems really are.



Unfortunately, this is but one of many threats!

Changing the game!

Harness the technology
of the future today
Raise safety awareness
Protect your investment
Open up new business opportunities

In 2014, several expert minds from the fields of cryptography and international software consulting gathered to address the question why the entire software industry is using “medieval” methods to safeguard data and files against outside access. Quite like in the middle ages, they practice still is to build the highest possible “safety walls” around data, yet in order to transfer or edit the data, its protection must be stripped, or an access key must be shared. Yet instead of solving this fundamental issue, the industry is trying to raise ever taller walls – unsuccessfully.

All involved parties agreed that it must be possible to find a truly safe – and therefore, completely novel - way to secure our data.

In 4 years of painstaking programming, development and testing, the team successfully formulated, created, and patented a whole new technology (NVD). It is no longer based on ‘locking’ data into secure systems, but rather integrating the protection into the data itself. This allows for entirely new dimensions in data protection, in the way we handle, distribute, control and store our data.

This technology is considered a secure solution for our networked future.

No matter which industry or IT-related field, whether it is the Cloud, IoT (Internet of Things), smart devices or autonomous driving – data has never been so valuable and yet as vulnerable as today.

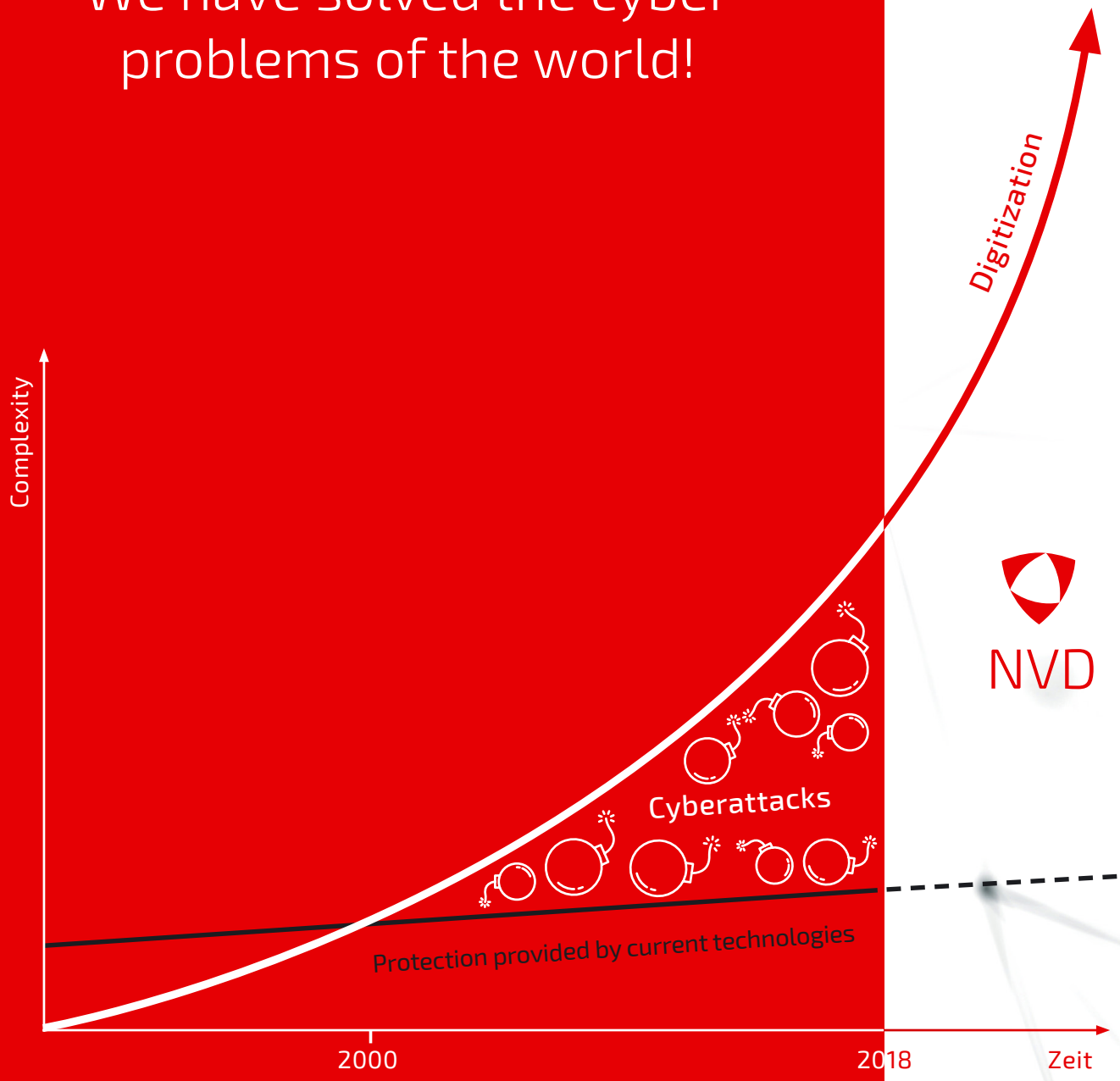
It‘s time to change the game!

NVD Technologie

You cannot touch NVD technology, you cannot put it into simple words and you cannot see it, but: NVD is an essential factor to solve the problems we described to the left!

We will take the time to explain this technology of the future to you.
Don't miss out on the eye-opening experience of discovering the game changer in data security technology!

We have solved the cyber problems of the world!



Digitization is the future without any doubt.
However, the increasing complexity (networking, billions of devices) has pushed current protection technologies to their limits, and as a result

the number of cyberattacks have increased dramatically!

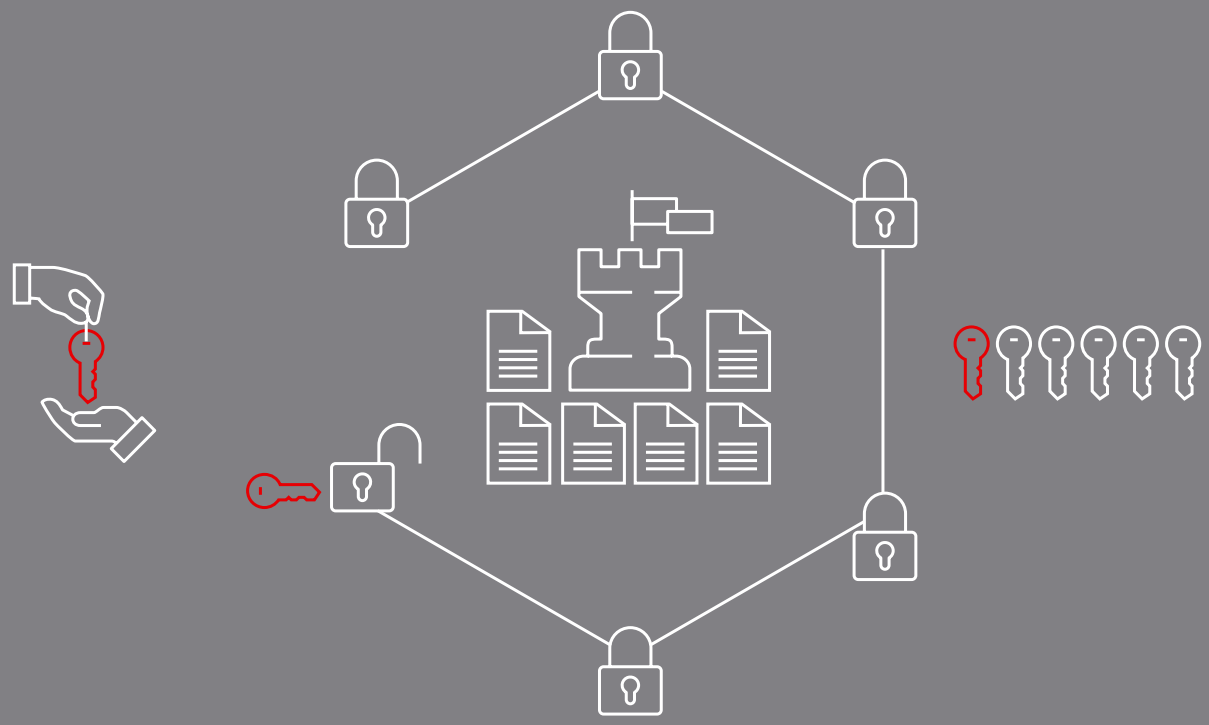
NVD leads to the necessary quantum leap in data security to prevent those!

Changing the game!

NVD is more than data security!

While debating the future ...

The digital world is living in the middle ages!



Current technologies build protections AROUND data!

Problems

1

Loss of control

As soon as you share data, you lose control over what happens to it next. There is no way to actively withdraw data privileges afterwards.

2

Insufficient protection

Building protection around data using encryption or encapsulation is the wrong strategy, because data needs to be unencrypted to be processed – which means protection must be removed beforehand.

3

Non-compliant

Not only your data, but in particular, additional information (meta data) is critical, since analytical systems can process this info, potentially identifying personal info associated with this data.

4

Complexity

An increasing number of devices and the need to securely connect them escalates complexity (key management), weakening security. Current technologies are doomed to lead into an impasse!

You can't attack data you can't see.

This is what the future looks like!

NVD integrates protection INTO the data as it is created!

Solutions

1

Control

NVD access procedures and genuine end-to-end protection guarantee that you stay in control of your data - permanently.

2

Digital immunity

We integrate protection and privacy directly into your data, making them immune to attacks and manipulation. Even insider attacks or compromised systems cannot harm them.

3

Compliance

Anonymous data do not contain any personally identifiable information or content. NVD-based applications comply with legal requirements for the protection of personal information.

4

Scalability

Efficient protection is applied right as the data is generated, providing uniform protection for anything, whether it is a smart electricity meter or a full-fledged industrial plant.

NVD puts you back in control of your data!

You alone decide who will have access to your data and you will never surrender control over it! You will always have the option of withdrawing access information retroactively.

Changing the game!

We can't teleport – yet. But we have managed to make data untraceable and invisible. No type of attack can impact you. Manipulation is impossible, compliance is ensured!

Your advantage with NVD		*You retain exclusive control over your own data! You decide about access and viewing privileges!*
Disadvantage without NVD		*No control over your data whatsoever! Others are in charge!*

Integrated protection inside the data, eliminated weak points: This is digital immunity.

Data manipulation and data theft are no longer possible, not even with quantum computers. Your data content is immune to cyberattacks, right away, and more importantly, in the future.

Changing the game!

Keys, locks, and gates have been common points of attack for centuries.
As our computer systems become more powerful, these obstacles are ever easier to overcome.
Integrated protection and privacy inside the data ensure your immunity.

Your advantage with NVD		*Perfect defense against data theft and manipulation! You will be lightyears ahead of any cyberattack!*
Disadvantage without NVD		*Growing complexity leads to more frequent attacks. Quantum computers will leave today's protections even less secure. A collapse is looming!*

We remove all personally identifiable information, which makes us compliant with today's and tomorrow's legal requirements.

NVD does not contain any metadata and no personally identifiable information. You don't have to worry about any legal restrictions in terms of privacy, for what you can't see can't be stolen or manipulated.

Changing the game!

Metadata and especially personal information provide excellent cues for attackers to find weak spots.
NVD does not use any meta data at all and ensures compliance.

Your advantage with NVD

Your insurance for legal compliance, today and in the future!

Disadvantage without NVD

Non-compliance with legal regulations means loss of goodwill and harsh penalties!

We don't have a weak link. Seamless data protection from the very start.

Plug-and-play, easy-to-use privacy for any device. For us, security and performance are both must-haves to give IoT solutions the security and performance they need to boost innovative business models.

Changing the game!

Billions of devices will be communicating and sharing data in the IoT, without sufficient protection.
We establish perfect end-to-end protection, without increasing the effort, regardless of application or device.

Your advantage with NVD

Uniformly high protection level, regardless of type or number of networked devices or applications!

Disadvantage without NVD

Traditional protection methods are too complex, expensive, and rigid to be fully integrated!

Not only secure, but perfectly safe-guarded. Patented technology that is future- and innovation-proof!

All our methods and algorithms are patented, securing your investment.

Changing the game!

Today's data security technologies are already reaching their limits and in no way meet the requirements of autonomous driving, the IoT or the healthcare sector!

Your advantage with NVD

You can benefit from a patented, revolutionary technology with enormous potential!

Disadvantage without NVD

A competitor could beat you to it and win the market using NVD!

Patent-protected

The Decision-Makers' Top Concerns

according to Gartner's CIO agenda

4 exemplary
fields of application

Internet of Things

Industrial Cloud, SmartGrid,
Connected-/Autonomous Cars

Issues

All possible IoT scenarios are facing similar challenges – how do you secure billions of different devices, network and server components? Since every single device is a possible attack point, each one must have a similar level of protection, whether it is an electricity meter or a nuclear plant.

Rising complexity makes it virtually impossible to control and secure all connected devices.

Healthcare

Legally compliant

Electronic patient files

Issues

Huge amounts of medically relevant data are captured digitally, from Fitbits to doctors or hospitals entering patient data, to insurance providers storing and analyzing medical information.

It is currently virtually impossible to ensure legally compliant long-term storage of complete data and conduct a targeted analysis of this data at a later point in time.

Solutions

We make sure that data on all devices is made immune to attacks or manipulation. We achieve this by applying an extremely efficient procedure right when the data is first created, and this immunity is permanent – which makes it completely irrelevant if data later runs on insecure or even compromised devices. NVD not only solves the challenges we described, but vastly simplifies and reduces the complexity of IoT architectures, since immediate protection eliminates the complex need to secure every single device in the chain.

NVD gives patients full control over their data as well as the flexibility to decide if, when, what, and how long they want to release their data (e.g. providing certain information to a doctor for specific treatments). NVD access control prevents data from being used outside of the defined scope or beyond the duration of use – the data simply won't be retrievable.

Of course, additional protections such as (partial) anonymization can be implemented as well, but they do not affect the original raw data - and thanks to NVD, even this newly generated anonymized data can only be used in a targeted fashion.

CarSharing

Personal contacts, GPS destinations or other personal settings follow the driver. Future drivers can't see this info in the rental vehicle.

Electronic patient files

In the event of an accident, medical data can be released to the hospital automatically and case-based for the duration of treatment.

Financial services providers / FinTechs

Data control and new, data-based business models

Banks are under enormous cost pressure, but for fear of safety breaches, they rely on old and expensive technologies. FinTechs are on the offensive, and they are using the Cloud.

In addition, new regulations such as PSD2 require these old systems to open up so financial institutions can share customer information. This leads to the aforementioned loss of control over a precious banking asset – their data.

Cloud providers

Creating goodwill for Cloud providers

Embracing the Cloud is a step that many companies consider a loss of control and a source of insecurity: Is their data really safe from third-party access and, not least, from the providers themselves?

Today's Cloud providers often circumvent encryption in order to be able to offer cheap B2C and B2B storage solutions. This is what makes space-saving deduplication possible in the first place.

NVD makes it possible to use the Cloud while enjoying greater data security. In addition, (client) data can now be shared usage-based (e.g. for a credit check) and fully withdrawn at any time.

Legal requirements are met without the dreaded loss of control. This raises whole new cost-saving potentials and opportunities for new business models in the area of data trade - as Amazon, Facebook and Google are already doing with great success.

NVD protects your data seamlessly, no matter where it is stored. Selective access to partial information allows for anonymized processing without the need to remove any data protections (as is the case with encryption)

Also, NVD-protected data is stored de-duplicated on any server, globally and with high performance, fortifying your level of protection and greatly accelerating access speed.

Banking Cloud

Massive, risk-free savings in operating costs (OPEX).

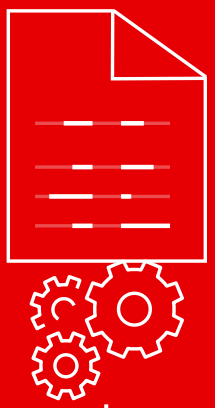
The Public Cloud becomes Private

Vastly more secure and scalable than your Private Cloud, at the price of a Public Cloud.

NVD Technology!

Invisible data in 3 steps.

Immediate, automatic protection



01101011101101
1010010100101
11101010010010

1

As the data is generated, it is analyzed and, based on the results, converted into binary fragments without any visible information (distorted, encrypted, disjointed etc.). Data is thus immune to any attack or manipulation. It can now be transferred or stored at will, no further protection necessary.

Dynamic address calculation

1. Username:	AS
2. Password:	secret123
3. Device ID:	1244-9577
4. Time window:	20 - 22 Uhr
5. Application:	3D-Druck
6. Company access code:	345RT8zR

Root address 0x1A43B0FE

2

Instead of verifying users and passwords based on existing information, as we do today, a number (address) is calculated based on various entry values that depend on the application, i.e. timeframe, purpose. Based on this address, the method can retrieve the data fragments generated in the first step and reconstruct the data.

Root 0x1A43B0FE

Quantum-cryptographic access

Temporary address 0x934JHx41

3

The addresses generated in the second step are valid only one single time. Each access involves calculating a new address, which is completely different from the previous one. This makes any information that attackers may intercept utterly useless. This means even future attacks using quantum computers stand no chance of calculating NVD-protected data.

We are building the foundation

1 Control

Safe (autonomous) driving

Apple, BMW, Bosch, Continental, Daimler, Ford, GM, Google, Honda, Infineon, Tesla, Toyota, Uber, VW

Replacing asymmetrical encryption

AMD, Apple, Broadcom, EMC, Foxconn, Google, IBM, Intel, Microsoft, Oracle, Qualcom, SAP

Blockchain Optimization

Google, IBM, Microsoft, Unilever, Visa, Walmart

2 Digital Immunity

Tamper-proof Smart Grids

ABB, Deutsche Telekom, EON, Gazprom, GDF, Landis+Gyr, KEPCO, Schneider El., SGCC, SMA Solar, S&T

High-security smartphones

Apple, BBK Electronics, China Mobile, Huawei, Lenovo, LG, Samsung, TCL/Alcatel, Xiaomi, ZTE

Anonymous, high-security collaboration

Government: Department of Defence, Homeland Security, Army

for solutions of the future.

4 Scalability

3 Compliance

Burglary-proof Smart Homes

Amazon, Apple, AT&T, GE, Deutsche Telekom, Google, Samsung, Siemens

Anonymous digital lockers

BNP Paribas, Credit Suisse, Deutsche Bank, HSBC, ICBC, JP Morgan Chase, Mitsubishi Financial Group, UBS

Tamper-proof and anonymous voting systems

Governments

Data at your fingertips

AT&T, AWS, BT, China Mobile, EMC, Hitachi, IBM, Microsoft, NetApp, Telefonica, Telekom, Verizon, Vodafone

Controlled data trade/-rental

BNP Paribas, Credit Suisse, Deutsche Bank, HSBC, ICBC, JP Morgan Chase, Mitsubishi Financial Group, UBS

Cost-reduced cyber insurance

Allianz, Axa, MetLife, Nippon Life Insurance, Ping an Insurance, Prudential

* Above mentioned enterprises benefit from NVD!

Think like us
– outside of the box!

Think **BIG!** Think **NVD!**

Changing the game!