United Innovations

Survey of Tools for Secure Infrastructures and Processes

Release 1 / 2025

www.security-innovations.eu

IT SUMMIT GERMANY

Join the IT Summit Germany 2025 on June 26th in Frankfurt, where industry leaders and innovators will explore the latest advancements in AI, software development, cybersecurity, and witness the exciting finals of the German Startup-Cup.

26/06/2025
9:00 AM

KFW
PALMENGARTENSTRASSE 5-9
60325 FRANKFURT AM MAIN

JOIN NOW

www.united-innovations.eu/it-summit-germany

EDITORIAL

Kathrin Scheld

Dear readers,

A very special highlight in the field of innovation awaits you on June 26: the IT Summit at KfW in Frankfurt am Main. For around 500 guests, we offer a varied program with exciting panels, inspiring presentations, interactive round tables and the German Startup Cup. The event will be complemented by a compact trade fair at which pioneering technologies and academic approaches will be presented.

In this issue, we also take a look at the "TechnoVision Top 5 Tech Trends to Watch in 2025". These key technologies and trends in cybersecurity will reach a new level of maturity in the coming year. With a focus on cyber-physical systems (CPS) cybersecurity, we look at how new regulations and targeted business interruption attacks are making securing these systems more urgent than ever - particularly due to their potential impact on the physical world. We present five key approaches to effectively protect these systems.

We also provide an overview of the most important challenges in the field of IT security for the industry. Increasing digitalization opens up numerous opportunities, but also harbours new risks that need to be overcome. In line with this, we present three promising start-ups that are currently taking part in the German Startup Cup and may soon be appearing in the final at KfW.

There will also be plenty of science: find out how smart fitness devices can become a target for cyber criminals, how the ATHENA research project is strengthening the cyber resilience of critical infrastructures through innovative skills development and how Augsburg University of Applied Sciences is countering the shortage of IT security specialists with targeted educational initiatives.

Finally, we would like to thank all contributors, speakers and participants of the IT Summit for their support. Their commitment and expertise are invaluable to the success of our community.

I hope you find this edition both informative and inspiring.

Enjoy reading,

Kathrin Scheld

CMO
GFFT Security Lab GmbH

CONTENT

UNITED INNOVATIONS

FOCUS & RESEARCH

NEW TECHNOLOGIES

CALENDAR

27/02/2025
15:30-17:00

Symposium zur OT-Security 2024/2025
Info & Registration

03/04/2025
15:30-17:00

Enterprise Security: Tech-Insights – Cloud Security
Info & Registration

27/05/2025
15:30-17:00

ITSM Tech-Insights: Trends im IT-Service Management
Info & Registration

26/06/2025
09:00-18:00

IT Summit Germany bei der KfW
Info & Registration

If you are interested in participating in a workshop or event, please send us an E-Maill to info@gfft-ev.de. You will then receive the dial-in data.

All events and further information can also be found at
www.security-innovations.eu/kalender

Discover Our YouTube Channel!

Did you know that our magazine has been on YouTube for quite some time? Visit our channel at the following link: GFFT YouTube Channel. On our YouTube channel, we offer a wealth of valuable content:

- Startup Pitches: Discover emerging startups and their innovative ideas and products.
- Use Cases: Learn how creative solutions are implemented in practice and the value they provide.
- Panel Discussions: Follow engaging discussions with experts from various industries on current topics and trends.

Stay informed and get inspired. Subscribe to our channel to never miss new videos and always stay up to date.

United Innovations

Driving European Innovation Forward

United Innovations (UI) is a dynamic force reshaping Europe's innovation landscape. Our mission is to enhance efficiency in large corporations and promote the adoption of cutting-edge methods and technologies. UI focuses on increasing the success rate of new technologies in Europe, bolstering the continent's reputation as a leading innovation hub.

At UI, we emphasize collaboration through our innovation network, enhancing efficiency, quality, and reducing costs. Our partnerships expedite innovation cycles, facilitating the successful launch of new advancements.

Our innovation strategy revolves around identifying innovation needs, assessing current methods and technologies, and establishing effective innovation processes, including the development and implementation of new solutions.

United Innovations invites you to be part of this vibrant evolution in Europe's innovation sector. For more information, visit www.united-innovations.eu or follow UI on LinkedIn.

Contact

info@united-innovations.eu
+49 6101 95498-10

ABOUT US

Social Media

www.linkedin.com/company/gfft-ev/

www.youtube.com/GFFTeV

Imprint

GFFT Innovationsförderung GmbH
Dr. Gerd Große
Niddastraße 6
61118 Bad Vilbel

Web

www.united-innovations.eu

Print

Flyeralarm GmbH

IT Summit Germany 2025 – Focusing on Future Technologies

On June 26, 2025, United Innovations (UI) invites you to the IT Summit Germany at the KfW headquarters in Frankfurt am Main. As the initiator of this premier event, we are delighted to welcome around 500 experts from the fields of technology, cybersecurity, and innovation, with KfW as this year's host.

The IT Summit is the central meeting point for those interested in the latest developments in artificial intelligence, software development, and digital security. Featuring groundbreaking solutions and insightful discussions, the event provides key impulses for the future of these vital fields.

A major highlight of the summit is the **German Startup Cup**, where winners will be crowned in the categories of **Cybersecurity** and **Software & AI**. Finalists will present their innovative solutions to an expert jury and the audience, who will jointly determine the champions.

High-Level Talks and Discussions

The diverse program includes engaging presentations and panel discussions led by top leaders in the IT industry. The event will focus on strategic approaches that help companies leverage technological advancements to stay future-ready. Special attention will be given to the role of AI and the transformation of digital security in agile enterprises.

Experience Innovation and Connect

The IT Summit also features exhibition booths, where startups and technology providers will showcase their latest advancements. Take advantage of the entire day to network, gain valuable insights, and exchange ideas with some of the brightest minds in the industry.

Join Us!

Don’t miss the opportunity to stay at the forefront of technological innovation on June 26, 2025, at the IT Summit Germany in Frankfurt. Spaces are limited – secure your spot today and actively shape the future of IT!

Tickets: www.united-innovations.eu/tickets-it-summit-germany/

DEUTSCHER STARTUP-POKAL
UNITED INNOVATIONS AWARDS

IT Summit Germany
Focus on Future Technologies

Join us on June 26, 2025, at the KfW in Frankfurt for a day of innovation. Explore advancements in AI, software development, and cybersecurity, connect with leaders, and shape the digital future.

Look forward to participants such as:

Tickets & Infos

Franz Ackermann
Manager | ICT Risk Management, **Deutsche Börse**

Carsten Frey
Direktor IT-Betriebsservices, **KfW**

Jochen Friedemann
CISO, **Talanx / HDI Group**

Nikolaus Hagl
Mitglied der Geschäftsleitung, **SAP Deutschland**

Benedikt Heintel
CISO, Director Proteciton & Resilience, **Viega**

Dr. Tobias Herwig
CTO, **Swiss Life**

Hermann Huber
CISO, **Hubert Burda Media**

Stephan Müller
Division Manager IT / CIO NORD/LB, **Norddeutsche Landesbank Girozentrale**

Danny Scheinhardt
Head of Cloud Governance and Processes, **Commerzbank**

...and many more!

Michael Schorpp
Global Regulatory Affairs, Boehringer **Ingelheim International**

Richard Socher
CEO **you.com**

Thomas Theisejans
Chief Expert IT Notfallmanagement, **Deutsche Bahn**

Heiko Weber
EMEA Head of Information Security and Data Protection, **Linde Material Handling**

United Innovations
GFFT
KFW

Excerpt from TechnoVision: The most important technology trends in the field of cybersecurity in 2025

With the “TechnoVision Top 5 Tech Trends to Watch in 2025”, Capgemini presents five key technologies that will reach a new level of maturity in the coming year. Here we present the trends in the field of cybersecurity.

An article by Pascal Brie, Capgemini

In the year 2025: Cybersecurity: New defense mechanisms, new threats

AI is transforming cybersecurity, enabling both more sophisticated AI-powered cyberattacks and more advanced AI-powered defenses. In a recently published study by the Capgemini Research Institute, almost all organizations surveyed (97%) stated that they had encountered security breaches or problems related to the use of AI in the past year.

In recent years, working from home has exposed organizations to a larger attack surface and vulnerability to these threats. In fact, 44 percent of top executives in the unpublished study cite the impact of Gen AI in cyber as the top cybersecurity technology issue for 2025. To mitigate these risks, there has been renewed investment and innovation in endpoint and network security. Efforts to automate threat detection also increased, particularly through AI-supported threat intelligence. Last but not least, looking to the future, there was a focus on improved encryption algorithms, including post-quantum cryptography in particular, to protect against the next expected disruption: quantum computing threats. This development marks a broader shift in the way organizations approach security and build trust in their increasingly autonomous systems.

Why this is important?

By 2025, generative AI-powered cyberattacks will be more sophisticated and widespread; the risks to organizations will increase. At the same time, as AI plays an ever-increasing role in decision-making and operational control, it will become increasingly important for people to trust these systems. But it's not just about being secure - it's about feeling secure. Cybersecurity needs to address both technical and psychological aspects to ensure trust in the systems people rely on every day.

Beyond 2025 - technologies that will shape the next five years:

Quantum computing: on the verge of a quantum leap

According to the study “Top tech trends of 2025: AI-powered everything” by the Capgemini Research Institute, which has already been mentioned several times, 55% of top executives and 44% of venture capitalists expect quantum computers to be one of the top 3 technologies in the field of “Computing & Networking” in 2025.

41 percent of top executives expect to experiment with quantum computers. 27 percent of the top executives surveyed expect the technology to be partially scaled in some parts of the organization in 2025. The key question is: when will the quantum leap take place and who will master it?

Capgemini. *Top Tech Trends of 2025: AI-Powered Everything*. 2025, https://www.capgemini.com/de-de/insights/research/top-tech-trends-2025/.

Artificial general intelligence: I think, therefore I am AI?

The reasoning capabilities of AI have made spectacular progress in the last 5 years, and some predict an era of Artificial General Intelligence. As a result, 60 percent of both, executives and people from venture capital, surveyed by the Capgemini Research Institute believe that this technology will be mature and commercially viable by 2030. Would the technology basically be able to mimic human intelligence to the point where it becomes irrelevant? This issue is leading to exaggerated predictions, and some are now questioning whether the intelligence potential of the technology is truly unlimited.

Pascal Brier
Group Chief Innovation Officer & member of the Group Executive Committee
Capgemini

How to secure cyber-physical systems

Due to the accelerating digital transformation and the resulting convergence of IT and OT, CISOs are more and more responsible for protecting their organization's cyber-physical systems (CPS). New regulations and threat actors' increasing focus on operational disruption make CPS cybersecurity all the more pressing, especially due to the impact that a compromise to these systems can have in the physical world.

A focus on the following five areas can help guide security leaders move towards the desired end-state: resilient systems that withstand attacks and maintain the integrity and availability of production and services.

1. Asset Inventory

Successful cybersecurity programs start with comprehensive asset inventory and visibility. Any further value that is derived from a CPS security program is dependent on the quality of its asset visibility. Organizations must identify all assets within the network, including hardware, software, applications, and data. After all, you can't protect what you don't know is there in the first place.

Proper visibility allows for an understanding of the complex nature of CPS environments and the proprietary technologies underpinning CPS such as operational technology (OT), Internet of Things (IoT), and connected medical devices. It also allows for better prioritization of exposure management, timely patching of the riskiest software and firmware flaws, and a reduction of overall risk.

2. Exposure Management

Traditional approaches to vulnerability management based on methods such as the Common Vulnerability Scoring System (CVSS) are no longer enough. There are now too many vulnerabilities in the environments and these cannot realistically all be addressed (at the same time). By evolving to a broader, more dynamic approach known as exposure management, security teams can prioritize vulnerabilities according to the probability of their exploitation and potential impact. In this way, CPS risks can be effectively minimized.

3. Secure Access

Organizations are increasingly adopting remote access technologies to their CPS environments in order to optimize production, reduce travel costs, and manage operational issues for a wide variety of internal and third-party stakeholders. However, this increased connectivity also introduces more entry points to the network and increased exposure to both advanced and commodity attacks. Proper visibility feeds into a secure access strategy, and allows security leaders to understand whether control systems and other critical devices are securely connected to the internet, are protected by purpose-built remote access solutions, and guarded by strong access controls and privileged access management features. To create a standard to maintain control and identity governance, it is advisable to establish a single CPS secure access hub that all vendors must use.

4. Network Protection

Many threat actors rely on lateral movement to achieve their ultimate goal. They gain a foothold in an initial access point and attempt to access other systems and escalate privileges in order to steal data, deploy exploits, and malware such as ransomware. Therefore, security leaders should look to leverage network segmentation as a means of ensuring secure communications.

Secure network segments can also help isolate sensitive data and systems; such isolation can have compliance benefits as well in keeping company or customer information away from attackers.

5. Threat Detection

No CPS environment is immune to threats, so being able to detect and respond effectively when they do surface is critical. CPS asset discovery provides the foundation for not only properly tuning firewalls and access controls, but also for identifying any deviations from accepted network traffic and activity on critical systems. Threat detection capabilities work in concert with the above recommendations in that once potentially harmful activities are detected, organizations can act on alerts and either isolate those affected systems or take actions to reduce risk in real time.

Advanced threat actors are increasingly targeting CPS in order to cause disruption or, in worst-case scenarios, carry out destructive activity. It's crucial that critical infrastructure organizations detect known threats and also understand anomalies in network and system behavior that could indicate a previously undetected threat.

Thorsten Eckert
Regional Vice President
Sales Central
Claroty Ltd.

Digitalization at the expense of security? Challenges for the industry

The digitalization of production holds new opportunities, but also risks: Outdated software in smart factories opens up attack surfaces for hackers, which urgently need to be closed with better security measures.

An article by ONEKEY

Image: Adobe Stock Westend61, 475982320

Increasing networking in Industry 4.0 brings enormous efficiency gains, but outdated software in control systems is increasingly becoming a gateway for cyber attacks. According to the "OT+IoT Cybersecurity Report 2024", a survey of 300 industry executives by the Düsseldorf-based cybersecurity company ONEKEY, many companies are not yet sufficiently prepared for cyberattacks. In particular, outdated software in industrial control systems (OT) and IoT applications are becoming weak points. These security gaps jeopardize the implementation of a secure and future-proof smart factory.

When hackers attack industrial control systems and IOT devices, the consequences can be fatal. Jan Wendenburg, head of the security company ONEKEY, illustrates this with an example from manufacturing: "Cyber criminals can use unprotected firmware to manipulate the internal configuration of a CNC machine remotely and damage both the machine itself and workpieces. The damage to the machine can be irreparable, rendering an entire production batch unusable." Ransomware attacks, in which hackers encrypt business-critical data and only release it again against payment of a ransom, are also not

uncommon. But that's not all. Anyone who brings a networked electronic product with known exploitable vulnerabilities onto the EU market from 2027 will even be liable to prosecution under the Cyber Resilience Act. Awareness of cyber threats is increasing. The “OT+IoT Cybersecurity Report 2024” study conducted by ONEKEY shows that almost 75 percent of companies recognize that hackers are increasingly targeting industrial control systems and IoT devices, but that they are not yet sufficiently prepared for this.

One reason for the inadequate handling of the risks of attacks on OT and IoT systems, as the “OT+IoT Cybersecurity Report 2024” shows, is a misperception: many companies see other areas of their company as more at risk and therefore neglect to secure industrial components. The prioritization of cybersecurity analyses also needs to be reconsidered. These usually focus on IT systems and networks, while industrial control systems and IoT devices are often ignored. Added to this is the complexity of numerous regulations and standards, which often creates confusion instead of the intended orientation. For example, 46% of respondents were unable to name which technical standards are relevant to the cyber security of devices, machines and systems.

One of the most recent directives is the Cyber Resilience Act (CRA). Jan Wendenburg, Managing Director of ONEKEY, explains: “If control systems do not comply with the CRA requirements from 2027, this will not only cause considerable problems for the manufacturers of the devices, machines and systems, but also for industrial users. It is therefore in the interests of everyone involved in Industry 4.0 to quickly upgrade cyber security in the OT and IoT sectors to the legally required minimum level.” In addition to the Cyber Resilience Act, there are other important standards for the security of operational technology and the Internet of Things that need to be observed.

The next key step towards effective protection against cyber attacks is the use of software bills of materials (SBOMs). These lists record all software components in networked devices, machines and systems. However, according to the ONEKEY study “OT+IoT Cybersecurity Report 2024”, only 24% of industrial companies create a complete SBOM, which makes it difficult to keep track of the numerous programs. Jan Wendenburg cites examples such as production robots, CNC machines and building automation systems, which often contain outdated software. His advice: companies should use an SBOM to identify potential cyber risks and proactively close vulnerabilities.

Training and audits also make an important contribution to strengthening the cyber resilience of industrial companies. The report shows that although 40 percent of industrial companies provide regular training and education on cyber security for their employees, this is not enough in view of the almost 135,000 officially reported cases of cybercrime per year according to statistics from the Federal Criminal Police Office (BKA). “The threat of cybercrime is higher than ever before,” warns Jan Wendenburg and recommends: ”Company management should put cyber resilience at the top of their 2025 agenda.” Link to the report: https://www.onekey.com/resource/ot-iot-cybersecurity-report-2024.

Jan Wendenburg
CEO
ONEKEY

Detailed information in the techL profile:
ONEKEY GmbH

Balancing Privacy and Progress: Breaking the Security-Operations Trade-Off

Harnessing data while ensuring privacy and regulatory compliance has long been a challenge for modern industries. Businesses have often faced the dilemma of sacrificing innovation for security or taking operational risks to boost productivity.

This trade-off has been particularly problematic for industries like healthcare, finance, and legal services. However, advancements in encryption technologies, such as Encrypted Data Sharing (EDS) and Encrypted Machine Learning (EML), powered by Fully Homomorphic Encryption (FHE), are transforming the landscape. These breakthroughs enable businesses to maintain privacy without hindering crucial operations, breaking the long-standing security-innovation trade-off.

The Traditional Trade-Off: A Barrier to Innovation

For years, the biggest challenge for businesses handling sensitive information has been navigating the tension between security and functionality. Organisations have often faced a scenario where protecting data meant limiting usability, especially in real-time analysis or cross-entity collaboration. Whether sharing data across borders or using AI to extract insights, the risk of exposing sensitive information has slowed progress and innovation here.

Traditional methods like data masking and tokenisation compromise data quality and fall short in modern operations. As data is used here, the risk of exposure increases, making these solutions insufficient for industries with strict security and compliance needs. This trade-off has limited the full potential of data use.

Emerging Solutions: Encrypted Data Sharing and Encrypted Machine Learning

Recent advancements in cryptography have led to breakthroughs that eliminate the need for businesses to choose between security and productivity. Encrypted Data Sharing (EDS) and Encrypted Machine Learning (EML) are two of the most transformative technologies that allow this.

These solutions are made possible by advancements in Data-In-Use Encryption technologies such as Fully Homomorphic Encryption (FHE). FHE allows computations to be performed directly on encrypted data, ensuring that sensitive information remains encrypted throughout its entire lifecycle, even during active use. This is a significant departure from traditional methods that only protect data at rest or in transit. Novel implementations of FHE, combined with other advanced cryptographic approaches, enable real-time data sharing, analysis, and collaboration without ever decrypting the data.

Companies at the forefront of innovation, like Vaultree, are pioneering these developments, ensuring businesses can adopt these next-generation encryption technologies without sacrificing performance. Vaultree's work in optimising FHE for real-world applications is setting the stage for widespread adoption, making solutions like EDS and EML practical and scalable for businesses across industries.

Encrypted Data Sharing allows multiple entities to collaborate on shared datasets without ever ex-

posing sensitive information. Through multi-key encryption, each party maintains control of their data while allowing real-time collaboration.

Encrypted Machine Learning (EML) extends this protection by enabling machine learning models to be trained and applied to fully encrypted datasets. This means businesses can extract valuable insights and make data-driven decisions without ever decrypting sensitive data. The implications are enormous—industries that have been slow to adopt AI and ML due to privacy concerns can now unlock the potential of these technologies while maintaining full compliance with regulatory frameworks.

Real-World Applications and Use Cases

The potential for EDS and EML spans various industries, particularly those where secure data collaboration is essential. In healthcare, finance, and legal services, data privacy concerns have historically limited data sharing and cross-entity collaboration, stifling innovation.

In healthcare, EDS allows institutions to securely share patient records for research, treatment coordination, and predictive analytics while maintaining full compliance with regulations like HIPAA. This enables faster medical advancements and more effective care without compromising patient confidentiality. EML further enables healthcare providers to apply machine learning models to encrypted patient data, extracting valuable insights without exposing sensitive information.

The finance sector stands to benefit enormously from encrypted data sharing, particularly for fraud detection. Financial institutions can collaborate securely on encrypted transaction data to detect and prevent fraud in real time. With EML, machine learning models can analyse encrypted data without ever needing decryption, allowing financial organisations to enhance fraud prevention capabilities while ensuring data privacy.

In the legal sector, where cross-border collaboration on cases is becoming increasingly common, EDS provides a secure way for legal teams to share confidential documents and case files without risking data exposure. By allowing secure real-time collaboration on encrypted documents, EDS opens doors to greater operational efficiency and new business opportunities, particularly for firms working across multiple jurisdictions.

The Future of Business Operations: Enabling Innovation Without Compromise

The future of secure business operations lies in solutions that allow data to be shared and analysed without ever being exposed. Technologies like EDS and EML not only eliminate the need for the security-activities trade-off but also create new opportunities for innovation. As privacy regulations continue to evolve, businesses can no longer afford to limit their operations for the sake of compliance. These new encryption technologies provide a pathway to meet regulatory demands while enabling businesses to operate at full capacity.

Tilo Weigandt
Co-Founder, COO
Vaultree

Body scales, fitness bracelets and the like: cyber security of smart fitness devices

Smart sports equipment and wearables can increase motivation to exercise more. But beware: smart fitness devices can become a gateway for cyber criminals. Athletes should check access rights and interfaces and use strong passwords. TÜV Association explains how users of smart fitness devices can protect their personal data.

An article by Maurice Shahd, TÜV-Verband e. V.

In the new year, many people make a resolution to do more for their physical fitness. Smart sports equipment, intelligent body scales and wearables help to record training progress and vital signs. Some devices even allow athletes to personalize their training experience: They can log workouts, set training parameters, monitor fitness goals and create individual training plans. These digital helpers not only make everyday life easier, but can also motivate anyone who is reluctant to exercise. However, they also harbour risks: “As smart fitness devices are often connected to the internet or store personal exercise and health data there, it's worth taking a look at cyber security,” says Marc Fliehe, Head of Digitalization and Education at the TÜV Association. “That's why consumers should pay particular attention to setting up their devices correctly and using them safely.”

11 percent of German households have an intelligent body scale. This was the result of a representative Forsa survey commissioned by the TÜV association among 1,002 people aged 16 and over. In addition to weight, smart body scales also measure body fat percentage, muscle mass, bone weight, water percentage, body mass index and pulse and send this data to a smartphone via Wi-Fi over the internet or directly via Bluetooth. There, the data is clearly displayed and analyzed in the corresponding app. “As smart fitness trackers store sensitive personal data, consumers should pay particular attention to the cyber security of these devices.” According to the survey, 65% of German citizens are very concerned that privately used smart home devices could breach data protection or misuse personal data. The TÜV association explains how users of smart fitness devices can protect themselves against cyber attacks.

Before you buy: protect personal data

Smart fitness devices often have various sensors to measure physical activity and vital signs. They are often worn on the body as wearables, for example in the form of smart bracelets, smart clothing or smart headphones. They also collect personal data and location data. “Cyber criminals use personal data to cause personal or financial damage,” says Fliehe. Hackers can also publish such data in order to specifically harm or blackmail people by threatening to publish sensitive data. They can also try to gain control of networked devices such as smartphones.

Consumers should inform themselves about the device and be aware of potential risks before making a purchase. It is important to know which sensors the device uses and what data is recorded and stored with it. It should also be clear where the data is stored and with which applications (apps) it is shared. It is also worth taking a look at the manufacturer: they should be reputable and provide long-term security updates. Apps from insecure sources often contain malware that can be used by cyber criminals to access sensitive data. Testimonials from other users can also help here. There are now also certifications for the IT security of smart devices. Test certificates from independent test centers such as the TÜV Cyber-Security Certified (CSC) mark provide consumers with guidance when making a purchase.

How users can minimize risks

1. check access rights

Smart fitness devices are often connected to the smartphone. This allows it to access data and functions such as location or contact list. Users should therefore check carefully whether the relevant access permissions are actually necessary for using the device and deactivate them if necessary.

2. use strong passwords and PINs

Smart fitness devices should always be protected against unauthorized access with passwords or PINs. The smartphone and the Wi-Fi network used should also be protected with secure passwords. Preset passwords should be changed immediately when setting up the device and user accounts should be protected by two-factor authentication if possible.

3. ensure correct encryption

An adequately secured home network is an important prerequisite for protecting smart sports equipment. The latest encryption standard WPA3 is recommended for Wi-Fi routers.

4. check interfaces

Interfaces between smart fitness devices and other devices should only be activated if they are necessary for functionality and are actually used. They should be deactivated again after use. The more interfaces are activated, the greater the attack surface for cyber attacks. If possible, communication encryption should be activated. Connections between smartphone and wearable via Bluetooth should only be possible with a PIN request.

Methodology Note: The data is based on a representative survey of 1,002 people aged 16 and over conducted by the market research institute Forsa on behalf of the TÜV Association. The survey took place in January 2023. Comparable surveys were conducted by Forsa on behalf of the TÜV Association in January 2021 and February 2019.

About the TÜV Association: As TÜV-Verband e.V., we represent the political interests of the TÜV testing organizations and promote the professional exchange of our members. We are committed to the technical and digital safety and sustainability of vehicles, products, systems and services. This is based on generally applicable standards, independent testing and qualified training. Our aim is to maintain the high level of technical safety, create trust in the digital world and preserve our livelihoods. To this end, we are in regular contact with politicians, authorities, the media, companies and consumers.

Maurice Shahd
Press spokesman
TÜV-Verband e. V.

Research Project: ATHENA

Boosting cyber resilience of critical infrastructure in the water sector through innovative and co-created competence building

An article by Lea Müller and Stefan Sütterlin, Albstadt-Sigmaringen University

The EU-sponsored ATHENA project explores innovative training approaches with the objective of enhancing cyber resilience in the critical infrastructure in the water sector.

Challenge

Operational technology (OT) comprises the hardware and software that is essential for the monitoring and control of physical devices, processes and events. Once isolated, these systems are now frequently integrated into information technology (IT) networks, thereby increasing their susceptibility to cyber attacks. The consequences of such attacks can be considerable, resulting in significant operational disruptions, financial losses, and even threats to public safety. Concurrently, the majority of cyber security training and awareness programmes are concentrated on IT environments. Such an emphasis contributes to a comparatively limited awareness of potential digital threats in OT environments.

Project ATHENA

The objective of the ATHENA project is to enhance the cybersecurity preparedness of the water sector and to provide personnel at all levels with the capacity to respond to incidents in accordance with the sector's overarching operational and management strategies. This objective is to be achieved through the promotion of cybersecurity awareness, the reinforcement of prevention measures, and the expansion of educational and training initiatives within the European Union’s water sector.

ATHENA is an EU-sponsored project led by the Dutch Ministry for Infrastructure and Water Management, and encompasses a multidisciplinary range of OT security experts, users and academic researchers, with partners from the Netherlands, Estonia, Germany, Norway, France, and Luxembourg. The project commenced in September 2023 and concludes in November 2026.

The ambition of the ATHENA project is to address the knowledge and practice gap between IT and OT, to provide innovative training approaches that are specifically focused on OT personnel, and to establish a uniform OT cyber risk training across Europe with the aim of strengthening the cyber resilience of critical infrastructure in the water sector.

Innovative Approach

To enhance the efficacy and appeal of training, ATHENA integrates emerging technologies such as augmented reality (AR), virtual reality (VR) and gamification, transforming traditional training into an engaging and enjoyable experience. Training is developed based on sound scientific methods and principles to ensure its effectiveness and reliability.

To illustrate, the ATHENA project makes use of innovative training methods, including VR simulations of control rooms, with the objective of optimising the training and assessment of operators in critical incident management. By situating participants in immersive scenarios, such as assuming the role of an intruder to identify potential cyber security risks in a VR simulated control room, the project seeks to facilitate practical learning.

Next steps

Through a process of testing and feedback from the project's target audience, OT personnel, the developed training is improved and expanded, ensuring its maintenance of effectiveness and relevance.

To enhance the impact and replicability of the training developed in a broader EU context, ATHENA focuses on upscaling and outreach through engagement with national and EU clusters and dissemination platforms. The integration of ATHENA's initiatives into a comprehensive competence strategy facilitates the transferability of lessons learned, thereby ensuring the sustainability of the achieved effects of competence growth and contributing to ATHENA's overarching objective of enhancing the protection and resilience of critical infrastructure in the water sector against cyber threats.

Lea Müller
Researcher
Faculty of Informatics
Albstadt-Sigmaringen University

Prof. Dr. Stefan Sütterlin
Professorship
Cyberpsychology
Albstadt-Sigmaringen University

Application-oriented Education: Professionals and Students

The shortage of skilled workers poses a major challenge to companies. More and more cybercrime and legal obligations necessitate even more qualified security experts to secure critical IT infrastructures. The Institute for innovative Safety and Security at the Technical University of Applied Sciences Augsburg (THA_innos) responds to this changing environment with education initiatives, offering a Master's degree course in Industrial Safety and Security and a related certificate course for specialists without a university entrance certificate.

An article by Helia Hollmann, Technical University of Applied Sciences Augsburg

Image: Technical University of Applied Sciences Augsburg

Digitalized factories and systems need special protection against cyber criminals. Also, legal obligations are changing with NIS2, the Cyber Resilience Act, and the machine directive. Specialists with knowledge of automation technology, IT and business management, combined with understanding of safety and security systems are required for these near future tasks. This combination leads to the difficulty of needing someone, being able to communicate between the involved domains. Coordinating all of these departments involved is necessary for appropriate (re)actions. However, such experts are not available on the market.

It is the task of universities to address this challenge. This includes teaching not only technical skills, like solutions for cloud connection or artificial intelligence to support processes or IT security, but as well the development of soft skills, leading to the implementation of these measures in the companies. At the Technical University of applied Sciences Augsburg (THA) we accompany the current transformation in two ways. With the Master's degree in Industrial Safety and Security and a similar certificate course for professionals, even without a university entrance certificate.

Education designed for working professionals

The Master's program in Industrial Safety and Security is one of its kind in Germany, offering interdisciplinary education from the Faculties of Electrical Engineering, Computer Science, and the School of Business. Over three semesters, we train students to work in mixed teams to solve security problems of industrial automation and control systems, as well as critical infrastructures, in an interdisciplinary manner.

Starting this year, there is an international branch of the master's program in which international students can study entirely in English.

Image: Technical University of Applied Sciences Augsburg

The Master Industrial Safety and Security was designed from scratch to be compatible with the lives of working professionals. We timed the lectures and seminars to fit into the schedule of a part-time employed student. This enables them not only to use their newly trained skills directly with their employer. They can continue working at the company and simultaneously completing a Master's degree program. This is mutually beneficial for the company and the student. With every question asked, we continuously deepen our knowledge about the practical challenges of the professionals in their company. At the same time, the students take the next step in their careers, and the employers retain their working forces with immediately usable new skills.

The certificate course "Industrial Safety & Security" allows professionals in IT and tech to engage in university level further education without a university entrance certificate. It offers skilled workers up-to-date knowledge about the connected world of OT and IT used in smart factories, semi-automated trade, mechanical engineering, or public sector infrastructures. The possibility to book custom in-house seminars supplements the offer by providing companies and their staff tailor-made contents for their individually required skills.

Why companies should invest in education

Both programs offer students and professionals the skills they will need in a digitalized future. It is impossible to buy security as a service completely. Such (further) education programs are opportunities to increase the practical knowhow of the companies' internal personnel, instead of investing heavily in recruiting. Essentially, companies empower their own specialists to work independently on security tasks, maintaining basic protection. This personal, having deep knowledge about the company's peculiarities and idiosyncrasies, functions as a point of contact for external contractors, offering granular services.

In our opinion, education is a worthwhile investment for companies. It encourages tech staff to expand their knowledge. Also, staying up to date with current security challenges is a worthwhile investment for companies. However, the programs themselves have to provide an environment that allows companies to retain their staff's workforce, and additionally teaching practical knowhow, whilst fitting into the lives of the learners.

Further information about the Master's program: www.tha.de/master-industrial-safety-and-security

Prof. Dr. Helia Hollmann
Course director
Technical University of Applied Sciences Augsburg

Feasibility Study CryptScan

Towards privacy in anomaly-based Intrusion Detection: In a world where cyber threats grow increasingly sophisticated, could Fully Homomorphic Encryption revolutionize Intrusion Detection Systems as the key to preserve user privacy in network security?

An article by Database Technologies and Data Analytics Group, Institute of Computer Science, Goethe University Frankfurt

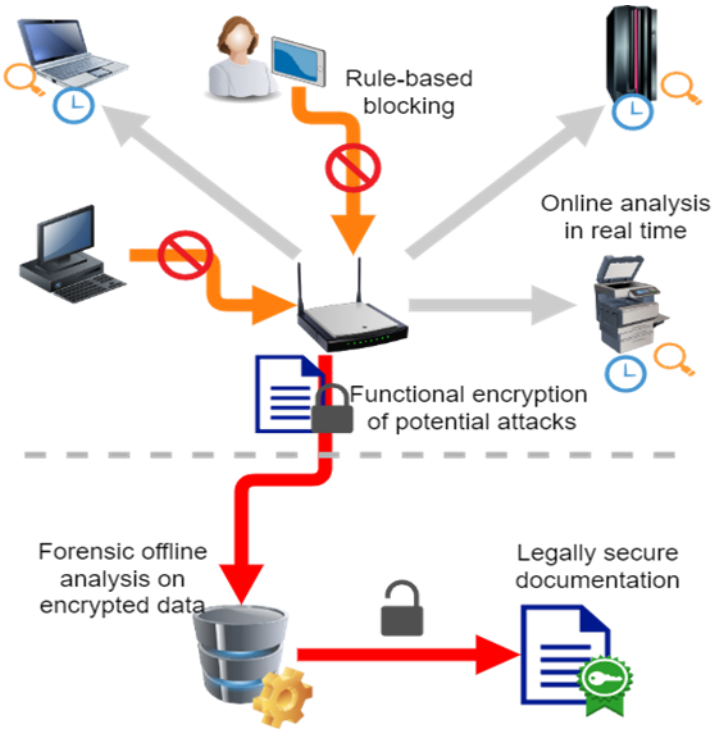

Figure 1: Privacy-aware IDS concept supporting encryption and forensic analysis of the CryptScan feasibility study.

The feasibility study "CryptScan" (Distr@l funding program by the Ministry of Digitalization and Innovation of the state Hessen) delves into the intersection of cybersecurity, forensics and privacy. It explores the potential of Fully Homomorphic Encryption (FHE) as a transformative solution for realizing privacy-preserving anomaly-based Intrusion Detection Systems (IDS).

While modern IDS solutions are highly effective at detecting network attacks, they often infringe on user privacy by deeply inspecting (sensitive) data. We envision equipping cyber security strategies with encryption technologies to mitigate the violation of privacy rights. Our novel approach for a privacy-aware IDS leveraging FHE addresses this trade-off, allowing encrypted computations without exposing sensitive data.

The study introduces a proof-of-concept model called CBS-OCSVM, an unsupervised anomaly detection algorithm that combines techniques like Pearson correlation, DBSCAN clustering, and one-class support vector machines (OCSVM) within

the FHE framework. This model is adapted for the CKKS schema, enabling encrypted anomaly detection while keeping the analyzed data confidential. The feasibility and performance of a prototype are evaluated using two public IDS datasets (NSL-KDD and UNSW-NB15). The experiments demonstrate competitive accuracy compared to baseline models while maintaining a lower false positive rate and the applied encryption does not tamper with results. However, the FHE framework incurs an excessive computational complexity.

In addition to the technical implementation, we broadly examine the implications of deploying privacy-preserving IDS based on FHE. The legal and practical challenges of using encryption, particularly the compliance with the European Union's General Data Protection Regulation (GDPR) are discussed. To this end, a survey was conducted among legal, IT, cybersecurity, and forensics experts to gauge the acceptability of sharing and computing on encrypted network data and the usability of encrypted digital evidence in legal contexts by an anonymous online questionnaire. While encryption and encrypted computation show promise as strong privacy-preserving measures and in improving evidence integrity, concerns about GDPR compliance and trust in encryption techniques remain. The survey reveals challenges regarding violations of important principles like data minimization or the risk of evidence manipulation or loss when stored in encrypted format.

The research highlights the potential of FHE to bridge the gap between modern cybersecurity and user privacy awareness. By allowing IDS to analyze encrypted data without requiring decryption, FHE also enables secure collaboration between organizations through encrypted data sharing or outsourcing the heavy computations to third-party cloud computing providers.

However, the experimental results emphasize the need to optimize FHE implementations for practical applications and further explore their legal and technical viability. According to the survey answers, it is crucial to address the unresolved legal uncertainties surrounding the use of encryption and encrypted digital evidence in court. Thus, further research is essential to refine FHE-based IDS, improve their usability, solidify their legal and practical frameworks, and pave the way towards privacy-aware cyber defense technologies.

Prof. Dr. Lena Wiese
Professor
Goethe-Universität
Frankfurt am Main

Jero Schäfer
PhD student
Goethe-Universität
Frankfurt am Main

XplicitTrust: A modern VPN based on Zero Trust Principles

From perimeter-based trust to zero trust principles: VPN innovation as a driver to overcome status quo bias in network security. How can organizations move incrementally from perimeter-based security models to zero trust principles?

An article by XplicitTrust

Image source: XplicitTrust GmbH

Network Security - Made in Germany

XplicitTrust GmbH, based in Karlsruhe, Germany, is a network security solutions provider founded in 2021 by seasoned cybersecurity professionals with a passion for creating solutions tailored to SMBs. The founding team, with over 25 years of industry experience, originally collaborated at Astaro, the German pioneer in network security, renowned for its UTM firewalls and later acquired by Sophos in 2011.

As a self-financed and independent company, XplicitTrust specializes in delivering innovative, customized cybersecurity solutions. With roots in Astaro's strong engineering expertise and channel-focused approach, the company positions itself as a trusted partner for medium-sized businesses, offering reliable and cutting-edge network security solutions.

Modern Zero Trust VPN SaaS

XplicitTrust's Always Connect technology introduces a unique solution for making ZTNA (Zero Trust Network Access) accessible and manageable for SMBs, while also reducing administration and support costs for larger enterprises. The system efficiently categorizes end-to-end connections between client and server systems, dynamically

optimizing connection setups. It intelligently detects whether a client is on a local network and establishes local connections seamlessly without requiring firewall or NAT changes. This ensures consistent connectivity, regardless of the client's location.

Authentication is streamlined through single sign-on (SSO) while enhancing security with mandatory multi-factor authentication (MFA). Administrators can flexibly control access based on user groups, device security status, location, domain affiliation, and even time of day.

The intuitive interface provides clear visibility into which users and devices are granted access according to defined criteria. The end-to-end approach also enables micro-segmentation of networks.

The tunnel protocol prevents communication with unauthorized clients, creating an overlay network that remains invisible to attackers. This makes services undiscoverable to unauthorized entities, effectively neutralizing opportunistic and targeted attacks, including 0-day exploits. This advanced security is achieved through cryptographic methods, including Single Packet Authorization (SPA) combined with a UDP-based tunneling protocol.

By significantly reducing the attack surface, XplicitTrust ensures comprehensive protection, whether the potential attacker is remote or within the local network.

Counter advanced cyber threads

XplicitTrust's solutions empower customers with efficient access and security management capabilities. By adopting a Zero Trust architecture, the platform ensures robust protection against cyber threats, significantly reducing risks of unauthorized access and lateral movement within networks.

The system is designed to adapt to diverse user needs, providing secure connections for various groups while simplifying compliance management. By aligning with privacy regulations and industry standards, it reduces administrative burdens and ensures data integrity.

Scalable and adaptable, XplicitTrust supports modern cloud-based architectures, secures legacy systems, and protects IoT devices, offering com-prehensive coverage. It optimizes resource allocation through task automation, streamlined access processes, and remote working enablement. These enhancements lead to cost savings, reduced complexity, and improved productivity.

Daniel Stutz
CEO
XplicitTrust GmbH

Detailed information in the techL profile:
XplicitTrust GmbH

VISS: Pioneering Cybersecurity Endpoint Hardware

About the company

Founded in 2023 by CEO Maximilian von Lonski and supported by CTO Matthias Wild, VISS is a forward-thinking cybersecurity hardware startup dedicated to providing cutting-edge solutions for safe Internet use in high-risk environments.

With its flagship product, the "VISSBOX", VISS focuses on offering a robust hardware-based defense mechanism against malware and other cybersecurity threats. By addressing vulnerabilities that traditional software-based security systems fail to fully cover, VISS aims to empower individuals and organizations to freely use the internet and public networks without compromising their data or digital assets.

VISS is currently customizing their product offering before the market launch with pilot customers from various industries among others: healthcare, defense, government, consulting, manufacturing.

VISS has the ambition to democratize this technology over time and roll it out to both business and private users.

Image: VISS, Matthias and Maximilian at the "Gründerpreis: Digitale Innovationen" award ceremony (2024).

Technology

The VISSBOX stands out in the cybersecurity landscape through its patented technology (fully granted), physical decoupling the data stream between the Internet and vulnerable endpoint PCs. This unique new solution, allows the VISSBOX to keep your endpoint PC from potential threats. Or simply put, VISSBOX is the "Condom for your PC".

People sometimes try comparing VISSBOX with a Data-Diode, Red-Device, Surfstick, Sandbox-Environment or Virtual Machine; however, it really functions differently.

Contact us to get a more detailed description.

Benefit for the user

For users, the VISSBOX offers peace of mind by simplifying their security needs. Rather than having to manage complex software or risk exposing their endpoint PC to potentially unsafe networks, websites or downloaded attachments, users can rely on the VISSBOX to handle the interactions on their behalf. This not only mitigates the risk of malware and cyberattacks but also allows users

to focus on their tasks without the constant worry of digital threats. It is e.g. suited for high-security industries, firms with sensitive Data and even private individuals. To summarize, VISSBOX provides a seamless, (cost-)effective defense for safeguarding your PC Endpoints integrity when most needed.

Product

Digital Mockup of the VISSBOX

Maximilian von Lonski
Co-Founder & CEO
VISS UG

Detailed information in the techL profile:
VISS UG

Survey of technologies

We regularly consult experts on their current needs, with tool research being a frequent request. This chapter highlights key technologies we find noteworthy, providing brief product summaries and links to detailed datasheets and contacts in our techL database.

All innovations be found in the technology database

techL

www.techl.eu

Asvin

asvin provides a solution to distribute updates safe and secure over the air to IoT devices. asvin is using de-centralized technoligies to provide a resilient and secure update solutions for devices during their lifecycle. By asvin the security state of devices can be monitored and reports on threat landscapes can be generated.

techL

ATHENARIS Digital Solutions

ATHENARIS Digital Solutions presents OnliU, an access management system for SMEs. Protect your data, networks, control electronics, hardware components, buildings and rooms from unauthorized access.

techL

Authada

AUTHADA is a cybersecurity company that revolutionises existing identification procedures with its innovative digital identification and signature solutions. Banks, insurers, telecommunication providers or even eCommerce companies can use AUTHADA to identify their customers online or on-site in seconds and in compliance with the law via the electronic identity of the identity card. Due to the Qualified Electronic Signature, contracts no longer require a handwritten signature at the regulatory level and can be con-cluded completely digitally. The solutions thus provide the optimal basis for digital transformation and process optimisation in companies.

techL

Betterscan

The Only Open Cybersecurity Software that secures both Cloud and Apps. A simple and powerful DevSecOps software to automate thousands of checks and eliminate human errors in Source Code and Cloud Infrastructure. Integrateable into anything.

techL

Bitahoy

Most cyber security solutions focus on fixing the symptoms instead of the root cause. That’s why we developed the industry’s most complete cyber risk management platform, created to give our clients a complete overview of their risk posture. Founded in Germany, we help our customers worldwide to bridge this gap and own their cyber risk in their daily operations.

techL

BreakinLabs

BreakinLabs specializes in penetration testing and IT security audits. We test the customer's IT systems using the methods of hackers and uncover dangerous as well as security-relevant vulnerabilities. In addition, we are currently creating an interactive platform for prospective and experienced IT specialists. In this way, we are imparting the necessary know-how for independent security audits of the company. For our commitment in the area of offensive IT security, we were recently appointed partner of the BSI project "Alliance for Cyber Security".

techL

Comcrypto

The comcrypto Mail Exchange Gateway (MXG) is an email gateway for DSGVO-compliant protection of email sending. MXG protects 100% of all outgoing emails with minimal effort for senders and recipients.Advantages: Automatically secure email sending, Minimize disruptions to email workflow, Visibility into the current security level of outbound email and associated receiving servers, No need to install client software or plug-ins.

techL

Comuny

The Trinity Identity Wallet enables cost-effective, eIDAS 2.0-compliant mobile authentication. Its SDK offers plug-and-play features, secure decentralized storage, and flexible UI-free design. Key identity functions shift to a white-label SDK, ensuring scalable, efficient cloud operations.

techL

Contact Sepio Systems

Sepio is here to provide the actionable visibility to continuously manage risk of all known and shadow assets at any scale. Actionable visibility, objective truth, and infinite scalability are the pillars of Sepio's Asset Risk Management (ARM) solution that enable companies to grow securely and efficiently. Our mission is to instill confidence for companies who need to manage risk of their continuously expanding, uncontrolled ecosystem of connected assets. With Sepio, security and IT teams will manage asset risk with confidence and painlessly, relieving them of the burden of complicated and expensive deployments, noise, or cost.

CYBERTRAP Software

CYBERTRAP is a cyber security company that specializes in active defence and deception. Using deception technology, attackers are specifically redirected to a specially created IT infrastructure. This minimizes cyber risks, halves the cost of an attack by 50% and increases the efficiency of security departments by 30%. We achieve this because deception reduces the dwell time by 97% and generates no false positives.

DeepSign

Auch die besten Sicherheitsvorkehrungen garantieren im Falle einer Cyber-Attacke keinen ausreichenden Schutz, wenn der Faktor Mensch das Ziel der Angreifer darstellt. Um diese Angriffsfläche zu eliminieren, bieten wir mit INVISID eine KI-basierte Authentifizierungsmethode, die einen validen Nutzer anhand eines Verhaltensmusters aus Maus- und Tastaturinteraktionen verifiziert. Diese vollständig automatisierte Technologie schützt den Nutzer durchgehend, unbemerkt und ohne Komforteinbuße vor dem Diebstahl seiner digitalen Identität.

deviceTRUST

The central contextual platform for enterprises, enabling users to work with their digital workspace from any location, with any device, over any network and at any time, giving IT departments all the information and control they need to meet all security, compliance and regulatory requirements.

Devity

DEVITY is your specialist in IT security for the Industrial Internet of Things. Based on the research of the team members, the team develops and operates an application for efficient configuration and installation of IoT devices such as sensors, industrial computers and machines to simplify access to secure operation of IoT infrastructures for industrial companies across Europe. The solution consists of two components - an SDK for devices and the KEYNOA web application. A feature of the solution is unique identities that are assigned to each device produced. DEVITY ensures that these identities are passed down the supply chain in a trusted manner and can be used for mass installation.

techL

eCom Service IT

With over 20 years of experience in IT security and PKI, our founder developed m2trust—a solution for automated digital certificate management.

m2trust streamlines and secures certificate lifecycle management in complex infrastructures, making it more efficient and cost-effective. Large companies and public authorities rely on m2trust to automate and simplify their PKI processes.

techL

emproof

Emproof delivers high levels of security and IP integrity for embedded systems, using unique techniques that protect algorithms and data while securing the entire device. Our solution, Emproof Nyx, prevents reverse engineering, securing your valuable intellectual property and protecting against exploitation attacks.

techL

Enginsight

Whether it's applications, servers, agents, IoT devices or industrial equipment, Enginsight provides LIVE security monitoring for all applications and devices on the network. A high-performance, out-of-the-box solution for IT security and monitoring. The user can start directly with all security analyses without configuration. After installation (<1h), the most dangerous attack vectors can be captured and evaluated (e.g. unauthorized access, hacker attacks). The fast implementation and immediate provision of all relevant analyses paired with an economical and transparent pricing model for SMEs is unique worldwide.

techL

F5 Networks GmbH

As enterprises adopt multi-cloud and edge computing, Volterra enables them to build, deploy, secure, and manage distributed applications and data. Its SaaS platform ensures seamless infrastructure, security, and connectivity across cloud and edge environments.

techL

Goriscon

GORISCON's data-driven solution, **embedded GRC**, streamlines information security, data protection, and risk management—integrated, intelligent, automated. As a management system, eGRC provides a multidimensional security view, reducing complexity through automation.

techL

Hanko

Hanko Authentication Service enables passwordless, decentralized FIDO authentication and prevents credential compromise through phishing, data breaches and password reuse. The focus is on user experience and open web standards.

techL

heylogin

Heylogin replaces passwords with a swipe-to-login on the phone. It works with all websites and saves 3 hours / month of your employees' time. For project managers, it eases on- and offboarding of employees. For CEOs, it gives back control over all your companies' logins.

techL

IDEE

AuthN is an award-winning, client-less, passwordless multi-factor authentication (MFA) that can be deployed in minutes across the entire estate. It prevents every single credential phishing and password-based attack including adversary-in-the-middle (AiTM). It can be used with or without a phone.

techL

Infrafon

Infrafon invented a SmartBadge which can replace a Samrtphone for ID and Access as well as messaging and Work Management in large organizations.

techL

Inlyse

inlyse is an AI-based IT security platform that detects malware and cyber-attacks in seconds. It uniquely combines image recognition with self-learning neural networks to stop advanced threats without updates. Offering simple integration, management, and cloud access, its modular architecture lets enterprises quickly address specific IT vulnerabilities with complementary security plugins.

techL

IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth

IT Security, Consulting, Development Prof. Dr. Dirk Heuzeroth (Einzelunternehmen) offers security and data protection services, focusing on implementing and auditing information security management systems and controls, as well as pentesting. It provides services as a data protection officer, consulting in secure software development, and custom training in IT security, hacking, and secure software development. The company also performs custom software development and is developing a health app.

techL

Kaspersky Labs GmbH

Kaspersky, founded in 1997, is a global cybersecurity company. Half of its 5,000 experts focus on in-house R&D. It protects over a billion devices with leading threat intelligence and security solutions, serving businesses, critical infrastructures, governments, and consumers. Its portfolio includes advanced endpoint protection and specialized solutions, safeguarding over 220,000 corporate clients.

techL

KraLos

In an increasingly digitalized world, cyber threats are everywhere. At KraLos, we understand the challenges businesses face and provide advanced cybersecurity solutions to protect your digital presence. Our services at a glance: Web Application Security: Protect your web applications from attacks and data leaks with WEBOUNCER. Secure communication without a backdoor or connection to the Internet with SHADOWKEY

techL

NESEC Gesellschaft für angewandte Netzwerksicherheit mbH

We specialize in information security, offering consulting, audits, penetration tests, and IT security system setup. Our expertise covers BSI basic protection, ISO 27001, VdS 10000, ISIS 12, and KRITIS—from initial concepts to full certification.

techL

Nexis GmbH

NEXIS Controle is the technology-leading software and comprehensive solution for cross-system analysis, risk assessment as well as visual (re-)modeling of authorization structures. The application sets itself the goal of being an easy-to-understand platform for IT and also business departments to work together on secure role and authorization management. NEXIS Control is manufacturer-independent and supplements all existing IAM solutions with powerful analysis, modeling and collaboration functions or as a stand-alone solution for successful implementation of existing access governance and automation requirements.

techL

Nviso

NVISO Eagle Eye is a threat hunting solution for enterprise networks. It allows the security team and analysts to centrally collect logs from clients, servers and network devices such as firewalls, analyze them using various advanced methods and thus detect cyber attacks and incidents in the network and initiate appropriate countermeasures. Eagle Eye uses a specially developed EE Outlier Engine in addition to well-known mechanisms such as YARA Rules to detect irregularities and thus differs from previous SIEM solutions.

techL

Onekey

ONEKEY, part of PwC Germany's portfolio, is Europe's leader in Product Cybersecurity & Compliance. Its AI-driven platform (OCP) detects firmware vulnerabilities in minutes—without source code or device access. Features include SBOM generation, 24/7 monitoring with "Digital Cyber Twins," and a patent-pending Compliance Wizard™ supporting key regulations. Automated vulnerability prioritization boosts PSIRT efficiency and response time.

techL

Ory Germany

Ory Network is a global, high-availability login network protecting identities and first-party data with AI-driven security. It enables zero-trust security, compliance, and risk management while offering advanced access solutions like passkeys, passwordless login, MFA, and hardware tokens. As an open-source leader, Ory fosters collaboration with 30,000+ community members and 250+ GitHub repositories, shaping the world's top identity management ecosystem.

techL

Primary Target

Primary Target's cyber security automation software shortens, manages and secures the vehicle development process. It automatically generates a threat analysis and controls the process to meet mandatory regulatory standards, making it more reliable, complete and less prone to error. Compared to the current established manual process manufacturers can meet deadlines, save 90% of time and reduce costs by more than 80%. The solution can also be applied to other industries such as defence, aerospace, machinery, IoT and others as well.

techL

Queryella

Queryella protects data by scanning apps for security and privacy risks using AI-driven analysis. Our platform detects IT security issues and data leaks in binaries, even with obfuscation. It examines privacy policies, hidden dependencies, and data flows, offering clear, intuitive insights.Originating from TU Darmstadt, our expert team continuously enhances our solutions to meet evolving security challenges. We seek partners to expand our platform for a more secure app future.

techL

r-tec IT Security

We have specialized in cyber security for 25 years. Our focus is on protecting against cyber risks and establishing suitable security standards. We offer our customers the security modules they need to freely develop their organization and realize their vision - from initiation to implementation and operation at all levels. We focus on dynamic protection instead of static models. We do not build walls, but develop the individual solutions that our customers need for their business processes and products.

techL

Red Sift

OnDMARC is a cloud-based application that enables organisations to quickly configure SPF, DKIM and DMARC for all their legitimate email sources. This instantly blocks any email impersonation based phishing attacks. OnDMARC also gives you totally visibility of your email landscape giving you a clear idea of the scale of the phishing problem specific to your organization. Only DMARC gives you insight into what's happening globally, on your domain, and not just attacks that cross your network boundary. Dynamic SPF is a unique feature to OnDMARC which helps users overcome the inherent problem of 10 SPF lookup limits and mitigates the need to manually make changes to your DNS for updates.

techL

requestee

requestee is the #1 B2B marketplace for pentesting. It is a secure place where clients can find and hire ethical hacking companies as easy as ordering a pizza.

techL

SANCTUARY Systems GmbH

SANCTUARY offers advanced cybersecurity solutions for industrial automation and space applications. We specialize in on-device security for embedded systems using virtualization and hardware-backed trusted computing. As pioneers in device trust technologies, we implement robust PKI for secure communications in challenging networks. Our OT Asset Management Solution, SANCTUARY Insight, provides comprehensive visibility and control over operational technology assets.

Secfix

Secfix helps companies get secure and compliant in weeks instead of months. We are on a mission to automate security and compliance for small and medium-sized businesses. We help SMEs to build their own ISMS and automate security standards such as ISO 27001, TISAX, , GDPR, SOC2, DiGA.

secjur

secjur is a compliance tech company that provides its own automation tools for data protection, information security, compliance, CSR and anti-money laundering processes. secjur is also developing a blockchain based auditing tool.

Sematicon

sematicon AG provides cutting-edge, easy-to-implement security solutions that protect business-critical processes without disrupting standards. Our products ensure secure data exchange across old and new systems, following international standards with high transparency and cost efficiency. Alongside advanced firmware, we offer industrial-grade hardware—100% made in Germany.

ShardSecure

Our innovative solution lets companies enjoy the flexibility and cost savings of securing their data wherever they want: on-premises, in the cloud, or in hybrid-cloud architectures. Organizations can enjoy stronger security and resilience without surrendering control of their data, putting their confidentiality at risk, or redesigning their workflows.

techL

suresecure

Making the digital world a safe place - that is our vision. The individual conceptualization of security strategies and holistic consulting on IT security issues play a key role for the entire company. The digital world is characterized by rapid change. It is not only the demands on IT that are changing, but also the attack patterns. And it is important to react flexibly and, above all, promptly to these changes with a high level of quality awareness. This requires our specialists, who work passionately every day on the most efficient security solutions.

techL

Thales CPL

Thales is the worldwide leader in data protection, providing everything an organization needs to protect and manage its data, identities and intellectual property – through encryption, advanced key management, tokenization, and authentication and access management. Whether it's securing the cloud, digital payments, blockchain or the Internet of Things, security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation.

techL

Vaultree

Vaultree is revolutionising data enablement and security through our pioneering Data-In-Use Encryption solutions. Our industry-leading technologies, such as proprietary Next Gen Fully Homomorphic Encryption (FHE), ensure that data remains encrypted throughout its entire lifecycle, enabling businesses with previously inhibited use cases and revenue growth opportunities via in-use encrypted searches, analyses, sharing and collaboration, AI/ML modelling, and data visualisation. Vaultree's solutions and approach to data enablement empower organisations to unlock and harness their data, driving compliant innovation while drastically reducing cyber threats.

techL

Vereign

Vereign establishes authenticity in digital interactions by connecting verified identities via computing devices, applying them to electronically sign documents, wordpress articles and e-mails and securing hashes of the digital exchange with one-time keys on the blockchain for an immutable audit log. Designed as a self-sovereign identity suite and federated authentication layer that resides with the user, both corporations and individuals can run their own instances and use it directly from within major e-mail clients and office suites. The interactions result in a verified and active address book disclosing personal data selected and maintained by the contacts themselves.

VISS

VISS offers patented cybersecurity hardware that physically decouples internet data streams from protected devices. Its flagship product, VISSBOX, provides robust, hardware-based defense against malware, used primarily in military and CRITIS projects. Unlike software solutions, VISS safeguards data on public networks and aims to democratize this technology for both enterprises and private users. The vision: making VISS a standard PC component, like Wi-Fi or Bluetooth, to meet growing cybersecurity needs.

XignSys

The XingSys Servicekonto.Pass was developed specifically for the requirements of public administrations. With the help of the SK.Pass and the personal smartphone, citizens can authenticate themselves easily, securely, and without a password to all digital administrative services that require the confidentiality application to be substantial and low-code according to eIDAS. The SDK is available as a native library for Android and iOS and can be easily and quickly integrated into software ecosystems thanks to "low-code integration".

XplicitTrust

XplicitTrust is a modern VPN SaaS based on the Zero Trust principle with a focus on the needs of European SMEs. Quick to deploy, easy to manage and cost-effective: state-of-the-art security technology that is affordable and manageable for companies of all sizes.

ZecOps

ZecOps is a stealth mode cybersecurity automation company headquartered in San Francisco with offices in Tel Aviv, London, Singapore and Buenos Aires. ZecOps learns from attackers' mistakes with the goal of discovering the course of action and objectives of the entire campaign, burn the threat actors exploits & persistence mechanisms and increase the attacker's campaign costs.

techL