tabidus.com

Together, we are stronger.

UNITED CYBER DEFENCE

POWERED BY TABIDUS TECHNOLOGY GMBH

TABLE OF CONTENTS

UNITED CYBER DEFENCE
POWERED BY TABIDUS TECHNOLOGY GMBH

TOGETHER WE ARE STRONGER

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE

EXECUTIVE **SUMMARY**

Technological progress is accompanied by an evolution of cyber threats, which are constantly increasing in mass and diversity. The cybersecurity industry is reacting to this, providing more and more security vendors, technologies and approaches for protection and is therefore subject to constant change.

However, implementing the security measures is no longer a trivial process. From planning to implementation to ongoing operations, companies in particular face major challenges. With the growing attack surface of modern IT infrastructures, the flood of potential security solutions and constant new trends, these hurdles are getting bigger and bigger.

Tabidus Technology was founded in response to this situation and is the common denominator in cybersecurity. As an association, Tabidus unites independent security vendors and performs the following tasks:

- Enables vendors to collaborate technically for a **collective defense** against cyber threats.
- Makes the operation of the vendors **available in an agile way** so that they can be used more quickly and flexibly.
- **Simplifies** the operation of security technologies and multi-vendor strategies.
- **Evaluates** technical innovations and makes them available for use by click.
- Is the **holistic contact** for customers and offers a uniform procurement channel as well as cross-vendor support.

To carry out the tasks, the association develops collaborative security systems. The vendors are embedded in these and made available via a new operating concept.

Integrated security providers can be activated within the system at any time with licenses and activated flexibly in any combination in the security features by click.

Companies can use the association instead of a single security vendor to implement their cybersecurity. This opens up new possibilities and perspectives:

- **More security,** through the possibility of combining security vendors, for a collective defense against cyber threats.
- **Commissioning** of security vendors by click in order to enforce desired changes and strategic decisions immediately.
- **Greater flexibility** in the vendor's deployment planning enables the implementation of new security strategies, optimal match with each area of application and the rapid introduction of innovations.
- **Implementation** of real multi-vendor strategies to meet compliance requirements.
- **Uniform operation** of security vendors using a collaborative system to reduce operating expenses and burdens on administrators.

With its efforts, the association is pursuing the goal of providing a complete defense against cyber threats. Although transparency and the ability to react to security incidents are also offered, the focus at Tabidus is on threat defense so that security incidents are stopped right from the start.

UNITED CYBER DEFENCE
POWERED BY TABIDUS TECHNOLOGY GMBH

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE

CYBER SECURITY IN CONSTANT **CHANGING**

We live in the age of technology and our world would no longer be imaginable without computers and technical support. There is hardly an area of life in which we are not dependent on computer technology. This increasing degree of digitization has already brought us many advantages and unimagined possibilities. Global networking through the Internet in particular changed our lives forever. However, there is also the downside to progress.

EVOLUTION OF **CYBER THREATS**

Where good arises, evil is not far away. The cyber world quickly attracted the attention of criminal groups. The starting shot for this was in 1984, with the introduction of the first computer virus. From this point, a great evolution of cyber threats began, which ran parallel to technical progress. This has been noticeable in various aspects.

- The attackers' motivation shifted from curiosity and self-affirmation to a means of making money, maintaining power and pursuing political goals.
- The mass of threats changed from initially occasional malware programs to a monthly increase in the millions and the total number of threats in the wild has already far exceeded the billion mark.
- The nature of the threats has changed from simply deleting and renaming files to highly complex attacks. From automatically changing code to memory resistance, self-protection measures, varying attack targets to fileless threats and long-term attacks that do not require malicious code.
- The effects of the threats changed from causing maximum damage and visual fun to unnoticed data theft, espionage, manipulation, blackmail and much more.

DEVELOPMENT OF **CYBERSECURITY**

The appearance of the first computer virus also marked the beginning of the cybersecurity industry and thus began the arms race. In the beginning there were a few providers who offered simple anti-virus programs to detect and delete malicious programs. However, with the evolution of threats, security vendors have had to evolve too.

- On the one hand, technical progress continuously increased the potential target area. The vendors therefore had to develop more and more security products in order to be able to cover all conceivable attack vectors.
- On the other hand, the threats themselves changed. The growing mass and complexity of the threats forced vendors to constantly adapt their security technologies. From simple virus signatures to artificial intelligence, there is now a wide range of approaches that are used.

The arms race between threats and security measures is an ongoing process. Technical progress continues, cyber criminals remain highly motivated, and as a result the number of security vendors, solutions and approaches is growing.

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE

CHALLENGES FOR **COMPANIES**

In the early days, little attention was paid to cybersecurity. As security incidents increased, however, the awareness that technological progress cannot do without protective measures emerged. In the beginning it was a simple exercise. The use of a firewall and an anti-virus program provided sufficient protection. However, due to the evolution of cyber threats and thus also cybersecurity, the implementation of security measures has become more and more complex. Companies in particular are now facing major challenges.

IT STARTS WITH **PLANNING**

The first question when it comes to the establishment of security measures is that of the security approach. There are many philosophies about it these days, but which one should I choose? Is EDR suitable or do I need EPP? Do I need active threat detection or am I better advised with preventive measures?

Can I already rely on artificial intelligence or are classic signatures even more secure? Do I shift my security to the cloud or do I stick to on-premise? Do I concentrate on my endpoint protection or more on the network? When is the right time to change my strategy again? Questions about questions that are not easy to answer and the variety of opinions is enormous.

EVALUATION OF **SECURITY PRODUCTS**

Once the security approach has been defined, the search for the right products with which I can implement my goals begins. The challenge starts with the number of potential candidates. In the past there were only a few providers that could be considered, now there are hundreds of security vendors to choose from. Everyone has the same goal, basically doing the same thing, but on closer inspection somehow different.

What criteria should I use to evaluate them? How many trial periods should I carry out and how big are my efforts? In the end, you are spoiled for choice, because in most cases you have to choose a single vendor.

ENFORCEMENT **OF DECISIONS**

Has a suitable vendor been found and procured after an extensive evaluation, how will my strategic decision be enforced? Depending on who or what I have decided on, the implementation is a complex process:

A suitable concept must be developed for my environment. My administrators need training. I may need external consultants for support. The new solution requires test runs. Technical problems that may arise at the beginning must be resolved. This is followed by the productive roll-out so that the new vendor can go into operation. It is therefore a long way from decisionmaking to the finished result and this has to be repeated every time a plan is changed.

ONGOING **OPERATION**

It is not done with the introduction of the security precautions, because they have to be supervised continuously: updating the software, adapting the configuration, resolving technical problems, permanent monitoring of security events, etc. The exact effort depends on the type of solution and the respective vendor. With each additional provider and each additional protective measure, these costs multiply.

Due to the number of security solutions that are necessary to cover the entire attack surface, these operating expenses for IT security add up considerably.

CHALLENGES FOR **COMPANIES**

UNITED CYBER DEFENCE
POWERED BY TABIDUS TECHNOLOGY GMBH

STAFF AND **KNOW-HOW**

With my operating expenses comes the question, with which employees can I cover these? Are the efforts so small that an existing employee can do it on the side or do I have to hire additional staff? What know-how is required for operation?

Approaches such as EDR require their own security analysts and usually the establishment of a SOC. Can I find enough skilled workers on the job market and can I afford them? Should I perhaps switch to a managed service and how much work do I still have? Simply purchasing software is by no means sufficient for cybersecurity.

FALSE-NEGATIVE AND **FALSE-POSITIVE**

Once the first hurdles have been overcome, there are two unpleasant side effects in the operation of cybersecurity:

False-negatives, the failure to detect threats and False-positives, the incorrect detection of legitimate processes. As neutral test institutes prove, every vendor is affected. Despite the use of protective measures, security incidents can still occur. Either by an undetected threat or by the security vendor himself.

COMPLIANCE **REQUIREMENTS**

The various certification standards for companies are aware of the problems of cybersecurity and increasingly require the use of multi-vendor strategies. „The use of two or more software products protecting against malware across the information processing environment from different vendors and technology can improve the effectiveness of malware protection" (ISO 27002 "Controls against Malware").

Unfortunately, the implementation of such strategies is associated with considerable costs and effort in all areas.

Achieving cybersecurity is no longer a trivial process for companies. A lot of work, time and money has to be invested from planning to implementation and ongoing operation.

Even then, security incidents cannot be completely prevented. As technical progress doesn't stop and cyber threats continue to adapt, the cybersecurity industry will do the same. Even more vendors, even more security approaches, even more complexity and challenges for companies are the result.

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE

THE UNIFICATION OF
SECURITY VENDORS

UNITED CYBER DEFENCE
POWERED BY TABIDUS TECHNOLOGY GMBH

Cyber threats are increasing dramatically in size and diversity. The cybersecurity industry is responding to this by unearthing more and more vendors, technologies and approaches to protection. However, companies are faced with ever greater challenges to implement security measures. In response to this situation, Tabidus Technology was founded. The association unites independent security vendors from all over the world, is the holistic contact for companies and takes on the following tasks and goals.

COLLECTIVE **DEFENSE**

A single security vendor cannot identify and prevent every global cyber threat in good time. The primary task of the association is therefore to enable technical cooperation between the vendors. The combination of independent knowledge, security approaches and technologies results in an overlap of detection rates. Organizations can use these to fill gaps in threat detection and maximize their defenses.

AGILE USE OF **VENDORS**

In order to keep up with cyber threats, protective measures must be implemented quickly and easily. The association's task is therefore to enable companies to deal more agile with security providers and technologies. On the one hand in the form of more flexibility in the selection and combination of vendors. On the other hand, through faster commissioning of the technologies so that strategic decisions can be implemented by click.

SIMPLIFIED **OPERATION**

The operation of adequate cybersecurity must not be reserved for large companies that have the necessary staff, know-how and financial resources. The association pursues the goal of simplifying the operation of security technologies so much that it can be carried out without expert knowledge. The focus of efforts is particularly on the operation of multi-vendor strategies.

PROVISION OF **INNOVATIONS**

Cybersecurity is always creating new approaches, technologies and providers. The association sees it as its task to evaluate new innovations in the field of threat defense, to review them and to prepare them for use. Companies can thus freely decide whether they want to use newly available technical options and, if desired, use them on click.

UNIFORM SUPPORT **AND SALES**

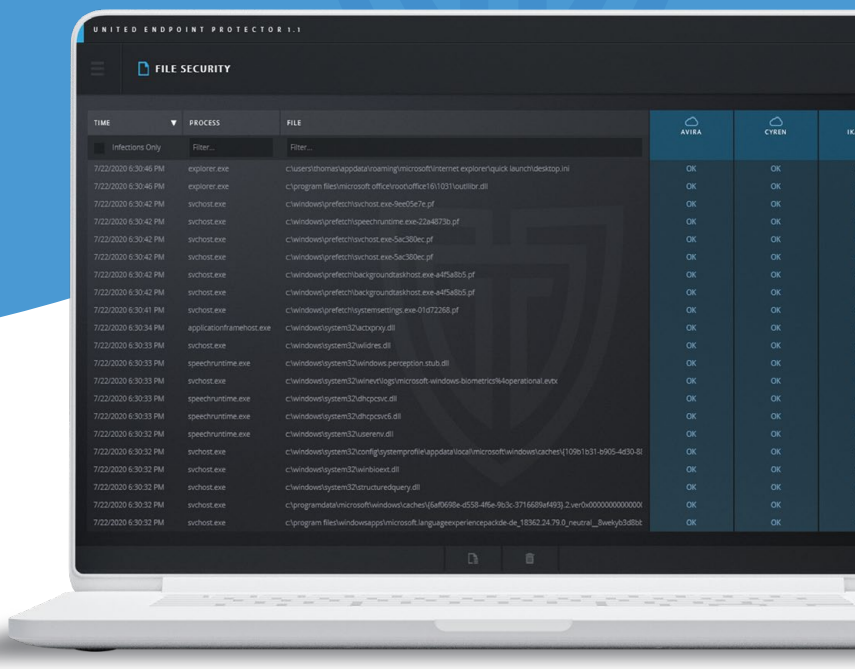
Different license models, procurement channels and support with technical problems can be complicated, especially when using multiple security vendors. As a holistic point of contact, the association takes on cross-vendor support and standardizes the license models and the sales channels.

TOGETHER WE ARE
STRONGER

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE

COLLABORATIVE
SECURITY SYSTEMS

A common denominator is required to enable technical cooperation between independent security providers. A platform that coordinates the interaction between the vendors and enables uniform operation. Cloud-based platforms are only suitable to a limited extent because they have major disadvantages in terms of security and performance. Tabidus therefore develops collaborative on-premise security products and embeds the various vendors in them.



TECHNOLOGY **CORES**

In order to create a collective of different intelligences, it must be determined what the individual security vendors contribute. Which functions and components are available through the security system itself and what is the vendor's contribution? The contribution can consist of all measures, knowledge levels and technologies that serve to identify and deal with threats. From local analysis and monitoring techniques to the connection of security clouds. In cooperation with the respective vendor, Tabidus creates an individual technology core that contains the entire threat intelligence and the protection potential of the provider.

DYNAMIC MULTI-CORE **TECHNOLOGY**

In order for the independent security vendors to work together, a connector is required. The association has developed the Dynamic Multi-Core Technology for this. This is the heart of the collaborative security systems and represents a framework in which the various technology cores are embedded.

The framework coordinates the cooperation between the various vendors and enables their agile use. Technology cores can be flexibly activated and deactivated in any combination during operation.

NEW OPERATING **CONCEPT**

A collaborative security product brings with it a new operating concept and changes the way security vendors are used. Initially, the system is installed traditionally instead of a single solution. The vendors embedded in the system can then be unlocked at any time with the help of technology licenses. After unlock, the corresponding technology cores are available in the various security features of the system and can be activated in the desired combinations.

UNITED ENDPOINT **PROTECTOR**

The first collaborative security system, that is already available on the market, is the United Endpoint Protector. This unites security vendors and technologies for threat defense on Windows clients and servers and makes their use available on click.

TABIDUS
TECHNOLOGY
UNITED CYBER DEFENCE

NEW PERSPECTIVES
FOR COMPANIES

With the unification of security vendors and the provision of collaborative security systems, the association provides a new way of implementing cyber security measures. Companies can now decide whether they want to use a single vendor or an association of vendors. If a collaborative system is used instead of a single security solution, new possibilities and perspectives arise.

COMMISSIONING ON **CLICK**

Whether for the evaluation of a new provider, a change of vendor or in an emergency, the commissioning of a security vendor takes place in a collaborative system on click. With the help of a technology license, the desired vendor is unlocked in the system and is then available for activation in the various security features.

Thanks to the hot-swap process, this can be carried out at any time during operation and does not require a new software installation or a restart of the computer. With the associated central management (United Control Center), this can also be done for an entire network. With this, strategic decisions can be enforced in just a few minutes.

MORE **SECURITY**

In a collaborative system, several providers can be activated simultaneously in a security feature. The processes to be checked are then analyzed simultaneously by several independent vendors. Depending on the investigation results and their agreement, automatic actions can be defined to react to a potential threat.

This type of collective defense makes it possible to minimize gaps in threat detection (False-negatives) and prevents harmful effects from false alarms (False-positives).

GREATER **FLEXIBILITY**

The agile handling of security vendors results in greater flexibility in deployment planning. For each area of application, the best providers for the respective task can be selected instead of having to cover everything with a single vendor.

The flexible activation of the providers also forms the basis for new security strategies. Which vendor should take on which tasks in which feature and combination at which point in time?

In addition, the association continues to deliver additional vendors in new versions of the system. With a click you can decide whether the new vendors should be used and the existing technologies should be replaced or supplemented by them. The introduction of technological innovations is therefore only a matter of decision.

UNITED CYBER DEFENCE
POWERED BY TABIDUS TECHNOLOGY GMBH

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE

NEW PERSPECTIVES
FOR COMPANIES

UNITED CYBER DEFENCE
POWERED BY TABIDUS TECHNOLOGY GMBH

TRUE MULTI-VENDOR **STRATEGIES**

The use of several security solutions corresponds in many cases to a "pseudo" multi-vendor strategy. This occurs when separate products process different data.

The classic example: provider A is used for server protection and provider B for client protection. This means that a total of several providers are operated, but again only a single vendor is in use on the respective system. In a collaborative system, however, several providers can be used at the same time and process the same data independently of one another. This enables real multi-vendor strategies to be implemented and compliance requirements to be met.

UNIFIED **OPERATION**

Although several vendors can be used in a collaborative security system, it is still a single system. The common user interface combines the operation of the providers and brings together all security information. How many vendors are active in the system therefore has no effect on the operating costs.

Even changing the security provider does not mean a change in the basic system, which means that retraining is not required. A collaborative system therefore relieves the administrators and in particular simplifies the operation of multi-vendor strategies.

TOGETHER WE ARE STRONGER

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE

FREQUENTLY ASKED QUESTIONS

UNITED CYBER DEFENCE
POWERED BY TABIDUS TECHNOLOGY GMBH

IS THE ASSOCIATION TAKING AN EPP OR EDR APPROACH?

The primary goal of the association is threat defense in order to prevent security incidents and stop attacks in the early stages. The first collaborative system, the United Endpoint Protector (UEP), was therefore designed as an EPP solution. EDR, on the other hand, can be helpful in certain threat scenarios, in ongoing attacks and in the investigation of incidents. Tabidus provides the United Control Center for these requirements. This system is not only the central management for the UEP, but also helps with the management of security events and provides visibility for the environment.

IS IT A CLASSIC MULTI-ENGINE SOLUTION?

The technology core of a vendor can contain all technologies and measures for threat detection. From signatures to artificial intelligence, from local scan engines to cloud approaches, from malware detection to the identification of other types of threats. All these possibilities are provided by the association in a collaborative system for agile use. Classic multi-engine solutions, on the other hand, do not allow agile handling, are mostly limited to malware detection, have no individual configuration options, but rather hide the second provider in the background. Tabidus allows to use several vendors in a collaborative system, but it is not a classic multi-engine solution.

IS IT A CLOUD PLATFORM?

The United Endpoint Protector is an on-premise security product and is installed locally on a computer. The embedded technologies therefore work primarily locally, but can also establish connections to their clouds.

The United Control Center was also designed for on-premise operation, but can also be operated in a cloud. Tabidus itself does not offer a managed service for this, but enables service providers to offer this.

WHICH VENDORS ARE AVAILABLE?

As of March 2020, the vendors Avira, Cyren and Ikarus were made available in the United Endpoint Protector and can be used in an agile manner. The next vendors are currently in preparation and will be made available in future releases. A current list of all vendors and technologies is available on our website **www.tabidus.com.**

WHICH VENDORS DOES THE ASSOCIATION ACCEPT?

As a neutral association, Tabidus is open to all vendors and technologies. However, there is a review of the member prior to admission. This does not assess the provider's products, but its technology. How much experience and know-how does the vendor have? What is his approach to security? What is the average detection rate of the technology? Has this already been tested? What processing speed is achieved? Can the vendor be integrated into the collaborative system? According to these criteria, Tabidus ensures a high quality standard of the members so that high-quality technologies are available to companies.

HOW IS A COLLABORATIVE SYSTEM LICENSED?

The association uses a uniform license model to provide the collaborative system and the vendors integrated into it. In principle, one license for the basic system and one license for each chosen security vendor, to use his technology, are required for operation. A decision can be made as to which vendor should be used in which quantities over which period. Only what is actually used is licensed, so the costs can be adapted to any situation and budget. If you are interested, Tabidus will be happy to prepare an individual offer.

TABIDUS TECHNOLOGY
UNITED CYBER DEFENCE