NIS 2: Supply Chain Risk and Vendor Selection

Assessing Cyber Security Vendors in the Face of Upcoming Regulation Changes

Cyber Security: The Secret to MSP Profitability

As threats have continued to evolve, cyber security has become a growing concern for businesses of all sizes. Once considered an exclusively enterprise concern, cyber security is now a priority for smaller businesses too. In the face of upcoming regulation changes and an increasing supply chain risk, your primary clientele is looking for stronger protections.

66% of small businesses are concerned or extremely concerned about cyber threats.

Source: Fundera

47% of small businesses have no understanding of how to protect themselves against a cyber attack.

Source: Fundera

By 2025, 45% of businesses are expected to have suffered a software supply chain attack.

Source: Garter

In order to combat an increasingly complex cyber crime environment and a rise in supply chain attacks, the EU is introducing the NIS2 Directive that will impact UK businesses as well. As a result, in order to remain profitable and competitive as an MSP, you need to expand your service offering to include a comprehensive stack of compliant security solutions. To do this, you need to work with cyber security vendors who will provide premium products and support your implementation of security services.

Finding the Right Security Vendor for Your MSP Is Not Always Easy

As the solutions you use will directly impact the services you deliver to your end-users, it is essential that you thoroughly evaluate each potential vendor. In this comprehensive guide, we will explain exactly how to find the most suitable cyber security vendor for your business, exploring:

- NIS2 and the impact of supply chain risks
- Why you should assess your cyber security vendors
- How to begin your vendor evaluation process
- The crucial qualities to look for in an effective cyber security vendor
- How to choose a vendor for a mutually beneficial partnership
- The benefits of an MSP partnership with Trend Micro
- And much more

NIS2 and The Impact of Supply Chain Risks

Cyber criminals increasingly rely on a new form of threat: the supply chain attack. During a supply chain attack, the vulnerability of one business essentially turns it into a Trojan Horse: criminals will not only compromise their data, but third-party data of their vendors and partners as well.

In light of recent increases in supply chain attacks, the National Cyber Security Centre (NCSC) has issued new guidance to help businesses effectively assess the cyber security of their supply chains as UK businesses of increasingly reliant on a range of IT services to run their operations.

Only 13% of businesses are currently reviewing the risks posed by their immediate suppliers.

Source: NCSC

Only 7% of businesses review the risks posed by their wider supply chain.

Source: NCSC

84% of businesses experienced disruptions in operations due to third-party risk misses.

Source: Gartner

In order to combat a nefarious trend in cyber crime, the EU has introduced its NIS2 directive.

What is NIS2?

Going into effect from October 2024, the NIS2 Directive outlines requirements for businesses in the EU to implement appropriate measures to prevent, detect, and respond to cyber security incidents. Seeing the exponential increase in supply chain attacks, the EU has outlined that NIS2 also requires businesses to not only consider their own security but their supply chain security as well.

NIS2 includes measures for:

- Incident handling
- Business continuity
- Supply chain security
- Encryption
- Access control
- The use of multi-factor authentication
- Vulnerability handling and disclosure

How Will NIS2 Impact UK Businesses?

As the UK is no longer bound to EU legislation, the Government has announced plans to build out the UK's cyber resilience, including extending the scope of the existing Network and Information Systems Regulations 2018 (NIS Regulations), rather than follow and adopt the EU's revised NIS2 directive.

However, as NIS2 outlines provisions not just for a business's own cyber security but for their supply chain as well, businesses operating in both the UK and the EU will have to adhere to both NIS2 and the UK's updated regulations once they have been finalised and announced by the government.

As an MSP, you need to be able to fulfil all of your clients' compliance needs, which means that even if only one of your customers is also operating in the EU, you need to be able to help them ensure compliance with NIS2.

Why Should You Assess Your Cyber Security Vendors?

Cyber crime has become an extremely profitable industry, with the average data breach costing UK businesses £2,670 in the last twelve months, and this figure only continuing to rise. However, while cyber attacks are advancing, many businesses are struggling to properly protect themselves.

68% of business leaders feel that their cyber security risks are increasing.

Source: Varonis

54% of companies say their IT departments are not sophisticated enough to handle advanced cyber attacks.

Cyber fatigue, or apathy to proactively protecting against cyber threats, affects 42% of companies.

As a result of these increasing fears, more and more businesses are turning to MSPs for cyber security assistance. The market has responded in kind, becoming more saturated and competitive. In order to retain customers and attract new ones, you must ensure that your cyber security solutions are optimal not just for protection but for compliance as well, especially as new compliance directives are coming into effect.

If you do not assess the cyber security vendors you partner with, you risk delivering sub-par solutions. As the consequences of a cyber attack are so severe for your customers, failing to properly protect them could result in significant reputational damage for your MSP. Client churn, financial repercussions and, in extreme cases, even legal consequences could all follow.

You can help to avoid these unwanted circumstances by taking the steps to evaluate both your current vendors and potential future partners before you begin working with them. The vendor solutions you invest in are the foundation for your reputation; you only want to work with the best of the best.

Beginning Your Vendor Assessment Journey

So, you've uncovered the need for a cyber security vendor. Now what?

Before partnering with any cyber security vendor, there are some simple steps you can take that will help you to identify and eliminate any bad apples from your search. This first tip may sound obvious, but it's nevertheless effective: once you have identified a potential vendor, simply conduct a Google search against them. The MSP community will come to your aid here – providing relevant, and invaluable, information. Searching your vendors allows you to check how they have been reviewed by other MSP partners and will highlight any immediate red flags.

Next, you should conduct a temperature check within your organisation. Your MSP is comprised of many technical experts with a wealth of experience in the industry. Have any of your employees worked with this vendor in a previous company? Have any of them heard any negative or concerning information that you should be aware of?

Finally, you should establish a rigorous and repeatable assessment process that you will use for all your cyber security vendors. Ideally, this would be a list of questions that ranks vendors against industry-standards and considers key metrics such as potential risks and support offered. There are existing frameworks and assessments that you can follow to evaluate your vendors, created by trusted groups such as the National Cyber Security Centre, Gartner and the Cloud Security Alliance. You can either use these to evaluate your vendors or, alternatively, use these as frameworks to create your own bespoke assessment. It is perhaps most valuable to create your own assessment, as you can include metrics that are specific to both the needs of your own business and your customers.

Using the same assessment tool for each of your potential security vendors will help you to evaluate them consistently and fairly, providing an unbiased overall ranking and making the selection process more seamless.

Top Tip!

To keep your vendor search organised and aid the ongoing evaluation of your current partners, it's helpful to itemise all the vendors you are either already using, or are considering working with, and detail the steps you have taken to validate their credentials. This helps to protect you in the event of an unwanted, unprecedented security incident.

How to Assess Your Cyber Security Vendors

There are several crucial features that you should be on the lookout for when selecting a cyber security vendor for your MSP.

Specialised MSP support

You want to partner with a vendor that offers services specifically designed to enrich, enhance and support your MSP. Look out for qualities such as a channel partner programme, additional training services and access to marketing and sales support.

Meet compliance regulations

When it comes to cyber security, it is important to always ensure that you meet specific compliance regulations to avoid legal and reputational repercussions. Therefore, you should only partner with vendors who comply with key frameworks such as GDPR, NIST, ISO and NIS (as well as NIS2 if you're operating in the EU as well).

Streamlined security management

Your vendor's security products should work together and complement each other to make implementation easier. If your vendor has a specific platform or ecosystem which integrates security monitoring and management across protection points and customer bases, this is a significant plus.

Automation and Cloud capabilities

Your vendor's solutions should accommodate automation to increase efficiency and save resources. Additionally, their products should be Cloud-compatible to facilitate remote access and control and complement the modern working environment.

Transparency and accountability

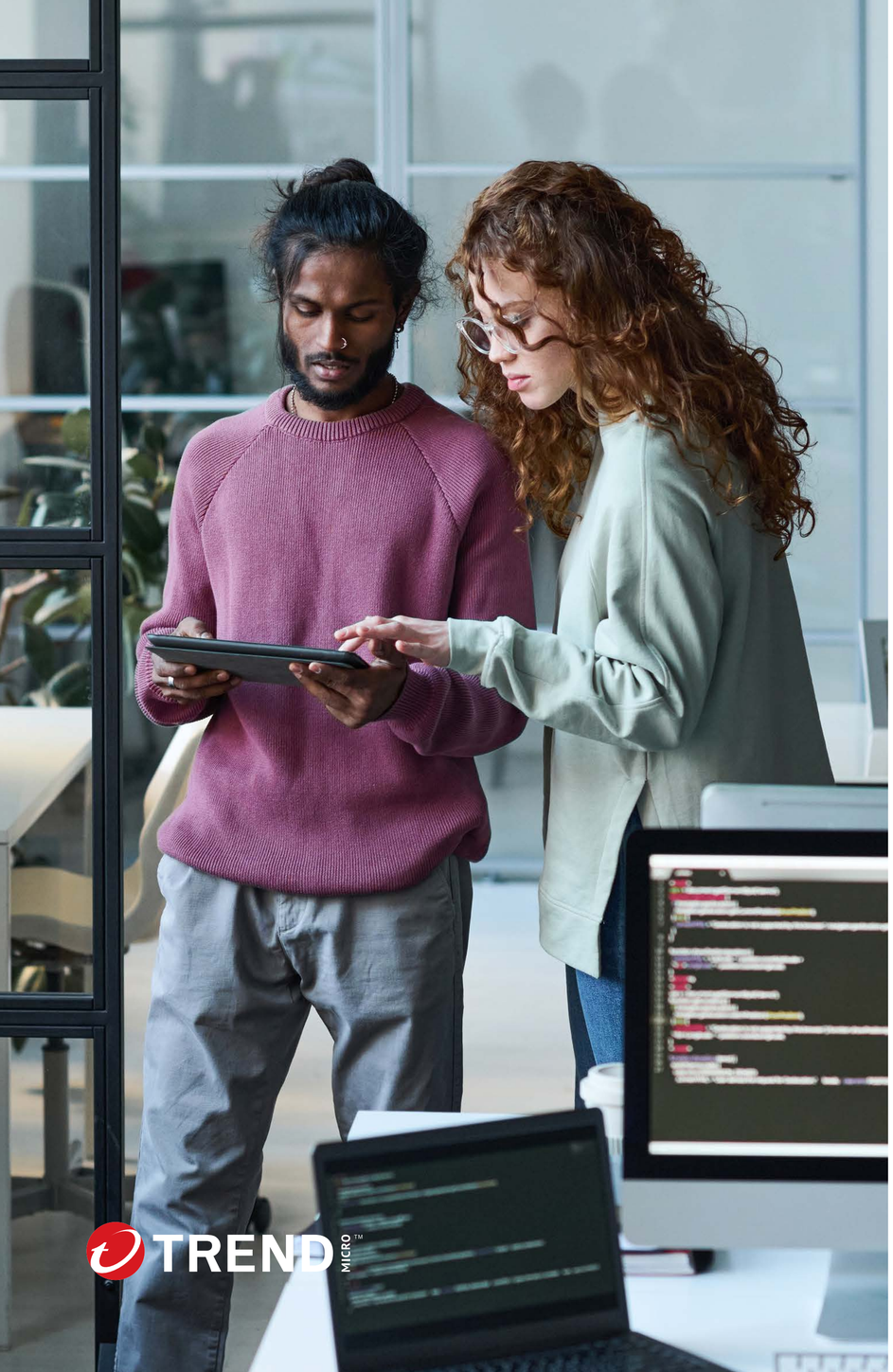
Security breaches do happen, and solutions do fail. You need to partner with a vendor who is not only equipped to handle this but will be honest and transparent about their response approach. Discuss accountability before you partner with a vendor and devise a clear plan of action in case of a breach.

Optimised business security

Unfortunately, some cyber security vendors have not taken adequate steps to protect their own businesses from attack. If a vendor's cyber security history is murky, be careful about partnering with them. How can you trust them to deliver premium solutions if they won't implement them across their own business?

Proactive, continual improvements

Cyber threats are always evolving, and so your vendor's solutions need to as well. Is your vendor working proactively to develop their services and solutions, and actively preparing for future cyber security issues? You must establish this from the outset to ensure that the solutions you implement have longevity.



Essential Questions to Ask Your Cyber Security Vendor

You should view your relationship with your cyber security vendor as a mutually beneficial partnership. As such, you should always maintain open lines of communication and establish a foundation of honesty and trust. This means that you should be able to ask your vendor some difficult questions, both before you begin working together and throughout your partnership together.

So, what should you ask your cyber security vendor in order to establish a mutually beneficial partnership?

When can we discuss my business needs and strategy?

Your vendor should aim to provide security solutions that meet the evolving needs of your MSP and your end-user customers. It will be beneficial for both of you to establish regular times to hold meetings where you can evaluate whether the products and solutions you are currently using are sufficient for your business needs. This helps drive you towards your overall business goals and provides an upsell opportunity for your partner.

How will you share feedback with me?

It is pivotal that you can maintain an open dialogue with your cyber security vendor. This means that they need to be able to share information about incidents with you seamlessly. At Trend Micro, as part of our Worry-Free Co-Managed XDR for MSPs, we provide a report to MSPs about every incident, including recommendations on how to respond and remediate the attack. Trend Micro also provides monthly reports to summarise case activity. This helps to keep you up to date and informed at all times.

How can I share feedback with you?

Equally, you need to be able to share feedback with your cyber security vendor. This could include reports of incidents or faults with the solution, recommendations for improvements or (hopefully!) positive feedback. Your cyber security vendor should create channels that allow you to provide these opinions easily and efficiently, allowing them to implement necessary improvements.

How are you preparing to meet upcoming challenges in the cyber security sector?

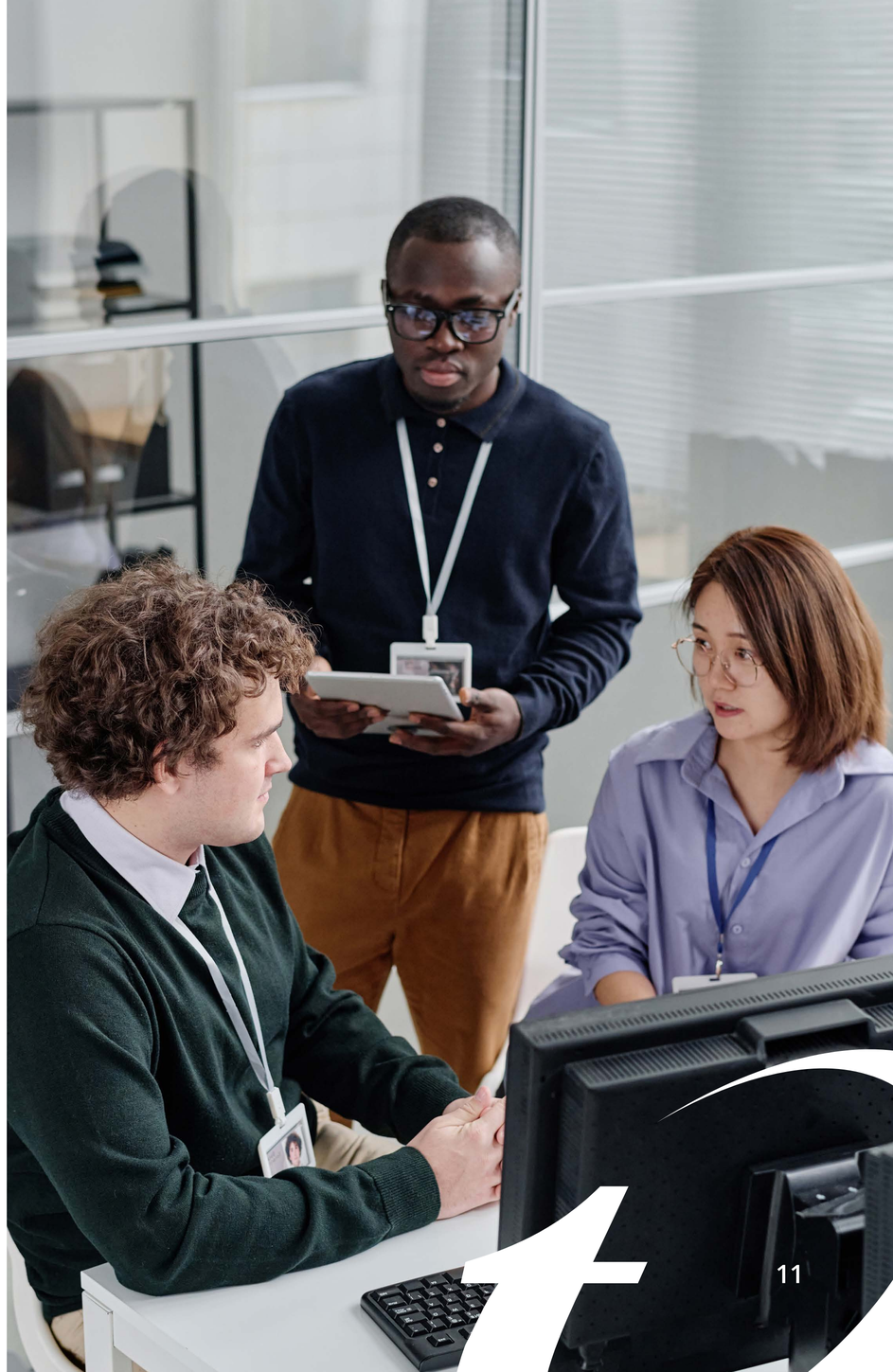
As you know, the cyber threat landscape is always evolving. As a result, there are key trends in the cyber security industry, such as the growth of the 5G network and the development of the Software as a Service (SaaS) model, that will significantly affect the way that cyber security vendors operate in the future. Especially supply chain risks are increasingly common, so your vendor should be able to clearly outline how they are preparing to adapt for these coming challenges and help protect both businesses and their supply chains.

What improvements do you have planned for the next quarter?

You don't want to get trapped in a partnership with a cyber security vendor who is stagnating. As the world of cyber security is so expansive, there is a lot of room for your vendor to experiment, innovate and expand their service offerings. You should always ask how your vendor is planning to improve in the near future to assess whether they as adaptable as you need them to be.

How do you ensure that you're adhering to compliance regulations?

In increasingly complex threat and compliance environments, your cyber security vendor needs to ensure that they (and you!) can easily adhere to all applicable compliance regulations. Especially if you have clients that are operating in both the UK and the EU, the cyber security solutions you offer them have to adhere to both UK regulations as well as the upcoming NIS2 directive.



Worry-Free with Co-Managed XDR for MSPs

Many MSPs struggle with the maintaining the time and resources for premium threat protection. Whether you lack a dedicated inhouse security team, or your client base is too wide to investigate every suspicious action amongst thousands of possible activities, threat detection and response can pose a significant challenge.

Some endpoint detection and response (EDR) solutions on the market do offer automated processes to speed up operations, but this does little to help incident response beyond the endpoint. When email is currently the number one threat vector, MSPs need a solution that accommodates a broader threat context. Enter Trend Micro Worry-Free with Co-Managed XDR.

Worry-Free with Co-Managed XDR is a cross-product, cross-customer, and cross-partner detection and response service which is co-managed by Trend Micro and MSPs. It provides holistic threat visibility and correlation across endpoint and email, enabling proactive containment and intelligent response by Trend Micro's threat experts. As the solution is co-managed by Trend Micro, your team will never be overburdened, and your security offering will be elevated without a significant time or cost investment.

24/7 threat experts

Isolates genuine threats in their earliest stages. Providing you with personalised customer remediation steps.

Cross-customer analysis

The service automatically checks your customer base for the same threat and takes action to protect multiple customers simultaneously.

Cross-partner analysis

Threat analysts review similar threats across partners, especially those in the same industry, to provide proactive response.

Incident response

Provides customised mitigation recommendations, or alternatively Trend Micro threat experts can conduct remediation actions.

Monthly case activity summary report

Provides an executive view of incidents and threats detected and mitigated for the month.

Why Choose Worry-Free for Your MSP?

Worry-Free with Co-Managed XDR is designed to ease the burden on MSPs, making their security operations more effective, efficient and profitable. That's exactly why our Worry-Free Business Security solutions currently protect over 500,000 businesses worldwide.

MSP-centric design

Trend Micro Worry-Free has an MSP-centric ecosystem, Trend Micro Remote Manager, which integrates security monitoring and management across protection points and customer bases.

Increased protection for customers

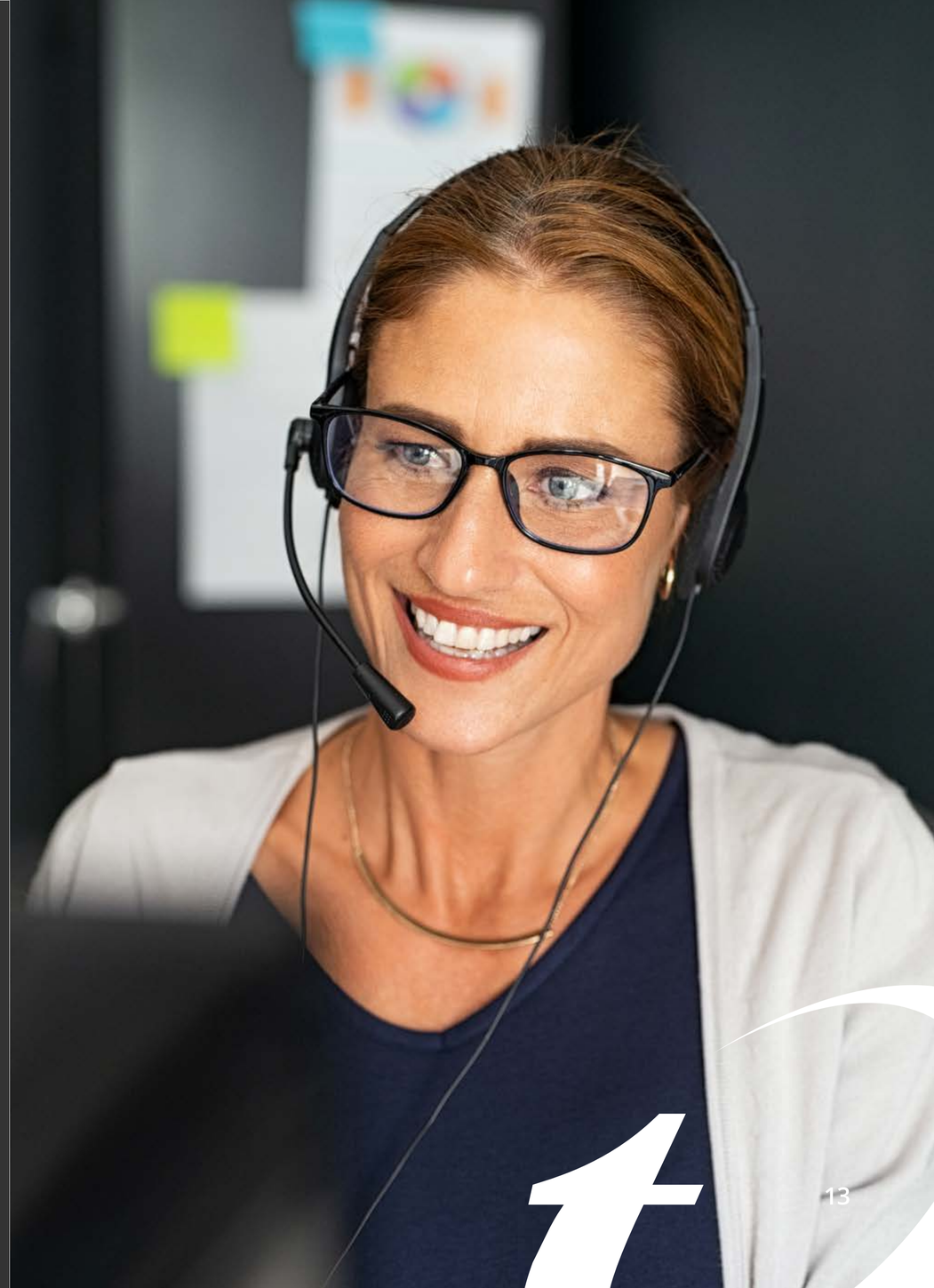
With non-stop, active monitoring and protection combined with cross-layer correlation it is easier to detect threats earlier and coordinate efficient response and elimination.

Enables business expansion

Worry-Free creates many more potential security upsell and cross-sell opportunities for your MSP and is immensely scalable in a multi-customer environment.

Lower operating costs

Your MSP is able to outsource time-consuming and high-skill tasks such as threat triage and investigation. Additionally, all bundles include pay-as-you-go pricing models and usage-based licensing with no upfront commitments.



Trend Micro: Your Trusted Security Partner

Trend Micro are global leaders in the cyber security space, leveraging over 30 years of security expertise, global threat research, and continuous innovation.

We have the experience and the infrastructure to support your MSP's security needs: our solutions are powered by Trend Micro Smart Protection Network, a Cloud-based global threat intelligence infrastructure supported by over 1,200 threat experts worldwide. As your security partners, we will empower you to provide premium security solutions, meet compliance requirements and enter the modern threat environment with confidence.

Are you ready to become a Trend Micro MSP partner and work with a vendor you can trust? Get in touch today.

Get in touch