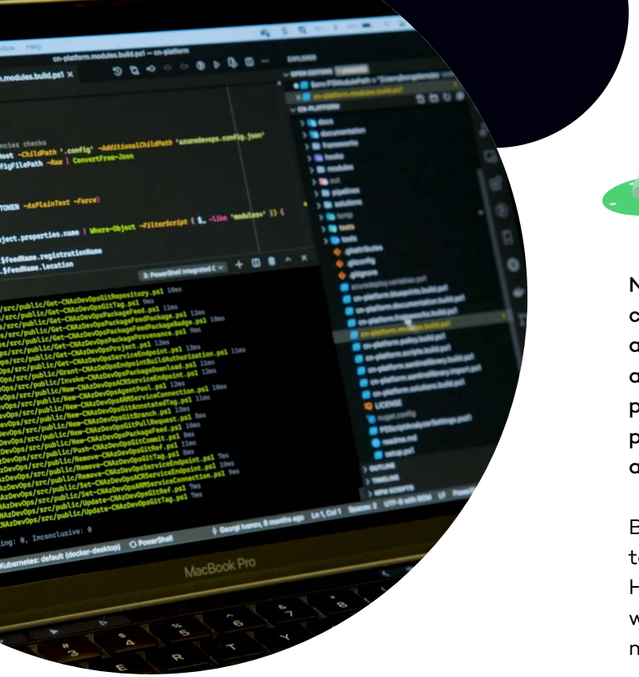
Brochure

Managed Detection and Response.

wortell



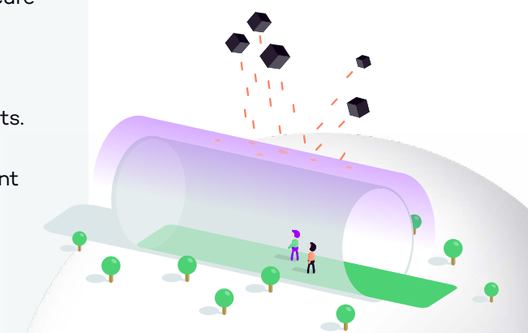
Now that more and more organizations switch to the cloud, they increase the ways in which hackers can attack them. No wonder the number of cyberthreats and incidents are growing. You obviously want to protect your organization from them in the best possible way. And you have to take a different tack, as a new environment requires new security methods.

But which technical means are best to invest in? How to gain insight into the risks your organization faces? How to ensure processes are properly organized? And where to find the right support when it comes to crisis management and laws and regulations?

The go-to solution: Managed Detection and Response (MDR)

If you opt for Wortell's Managed Detection and Response (MDR), you will outsource security to a solid, expert party. We will detect cyberthreats and respond to them. Smart technology and experienced security experts will keep your IT environment secure 24/7. How?

From our own Cyber Defense Center, which is located in the Netherlands, we proactively detect and respond to cyberthreats. We don't limit ourselves to technology — we provide security across the entire organization. Moreover, our crisis management and legal experts help you gain insight into security risks and establish clear agreements and procedures. This allows us to act quickly and efficiently in the event of a cyberattack.



De componenten van de MDR dienstverlening

Vroeg ← Laat

Threat intelligence
Pro-actief ingrijpen op basis van Threat Intelligence zodra een dreiging ontstaat.

Threat hunting
Actief op zoek naar sporen van hackers die de beveiligingsoplossingen proberen te omzijlen.

Security monitoring
Het 24.7 detecteren van bekende aanvallen en verdachte situaties.

Incident analyse
De dreiging wordt beoordeeld door getrainde modellen en onderzocht door security analisten.

Incident response
Security experts komen in actie om de dreiging weg te nemen.

Crisis- en risicomanagement
Uitvoeren van crisis en risicomanagement als een aanval gaande is.

Forensisch onderzoek
Opstellen van een uitgebreide tijdlijn van de aanval.

Wortell MDR

SOC

Detecteren

Reageren

No SOC, but MDR
You may decide to build your own Security Operations Center (SOC). But if you do, you should ensure this SOC is staffed by a team of experts 24/7. On top of that, a SOC solely focuses on detecting cyberthreats. Here's what this means: if a threat is detected, you'll have quite a significant problem — which you will have to solve yourself, as a SOC does not respond to threats. With MDR, on the other hand, you will benefit from the best of both worlds: detection and response. It makes things a lot easier for you!

"MDR Services are filling the need of organizations of all sizes that lack internal security resources and expertise, and want to expand their investments beyond preventative security technologies to address their detection, response and 24/7 monitoring gaps."

– Gartner Market guide for Managed Detection and Response Services, June 2018

Security monitoring and threat hunting
Security monitoring means you wait for a signal indicating a threat has been detected. At Wortell, we believe this reactive form of detection doesn't suffice. That is why our experts proactively look for traces of cyber incidents that have not been detected by preventive tools. If we find them, incident response is initiated: we intervene — even if it's in the middle of the night. We inform you of the cyberthreat and eliminate it.

Security with Microsoft
At Wortell, we've opted for Microsoft's security solutions, as they protect the cloud, the workplace, and your users. Briefly put, we can use these solutions to properly secure everything. This is perfectly in line with what we do — besides being security experts, we also provide modern workplace and cloud solutions. If there's anyone who understands how to adopt an organization-wide approach, it's us. However, we do use our own security methods: if you work with Wortell, you will benefit from our unique software, which extends the functionalities of Microsoft's security products. This means your organization is always secure.

Hoe sluiten we jou aan op ons MDR?

Stap 1

Koppeling van jouw omgeving aan onze cybersecuritydienst

Dit kan binnen 24 uur geregeld zijn

Stap 2

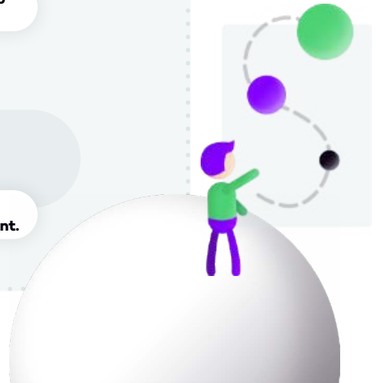
Heldere afspraken over de samenwerking

We leggen onze afspraken stap voor stap vast in een incident-response-plan.

Stap 3

Doorlopende dienstverlening (en ontzorging)

Detecteren, analyseren en reageren. Zo zorgen we ervoor dat je 24/7 beveiligd bent.



How do we work?

Ready to adopt MDR? At Wortell, you can count on a phased approach. Want to know what it looks like? Read on!

1. **Connecting your environment to our cybersecurity service**
   Using Microsoft's standardized cloud-native solutions, we will connect your environment to our cybersecurity service within several hours. Since we use Microsoft's existing security solutions, you will pay according to use — major upfront investments are not required. The solutions scale along with your organization's growth or shrinkage. Moreover, you'll always be up to date — which is crucial when it comes to cyberattacks, as these change every day.

Did you know:
We can connect organizations to our MDR within 24 hours?

As soon as your environment is connected to our service, you will hit the ground running when it comes to cybersecurity. That's because our use case library is available to all our customers. This library contains use cases and lessons we've learned at other customers. We will automatically apply all this knowledge to your environment, which means you'll benefit from increased security right away — you're protected from attacks your predecessors have dealt with. The result is a positive snowball effect: you learn from each other's experiences, which makes for a much more secure world!

At this stage, we'll also jointly identify your valuable data so we can make a risk assessment. Based on what we've discussed, we will look at other organizations that operate in your sector: which attacks have they had to deal with? What risks do they face? The answers to these questions will help us take the right measures to protect you from attacks that really apply to your organization.

2. **Clear agreements on our collaboration**
What's the plan of approach in the unhoped for event of a cyber incident? We'll record it step by step in an incident response plan, including several sample scenarios. This creates clarity for both parties.

What kinds of agreements will we make? Here's an example: if you have your own IT department, we can involve it in the response process. But we could also agree that Wortell handles the process from A to Z. Furthermore, you can — for instance — indicate whether we are authorized to shut down a factory in the middle of the night in the event of a cyberattack.

It's important to think about this in advance, as cyber incidents rapidly spiral out of control. If you have to make a bunch of calls after an attack has occurred, you'll lose valuable time and increase the damage. By making clear agreements in advance, Wortell can intervene at an early stage of the attack and prevent damage.

3. **Continuous service (and unburdening)**
Our approach consists of three steps: detection, analysis, and response. Here's how this works. We detect cyber incidents and collect data on the systems we monitor. In the case of a signal, we analyze whether it's a cyber incident. As our in-house experts dive into it right away, we can respond very quickly if it turns out to be a cyber incident.

We deliver reports every month to provide you with insight into where the most cyber incidents occurred in the past month (for example, on the data side or on the user's side). Based on these reports, we give advice on the measures you can take. We can also take steps for improvement for you — because prevention is better than the cure. In some cases, for example, you can make the 'front door' more secure, so it's more difficult for hackers to enter.

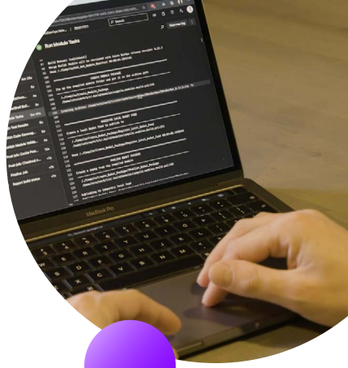
Furthermore, we proactively look for threats and traces of hackers that don't make the alarm bells go off but that may lead to a serious hack if you don't detect them on time.

If you're dealing with a cyberattack, we conduct a forensics investigation to determine the scope of the attack and check whether data was leaked or stolen. Our experts unearth what happened, how the hacker got in, how we can prevent this next time, and if it's legally necessary to report the attack (which is the case if, for example, personal data has been leaked).

What will mdr do for you?

Security across the cyber kill chain
We use Microsoft's security products, because they secure the entire cyber kill chain: during an attack, the hacker goes through several stages, each of which we secure. We barricade the front door and the doors behind it. That's essential, especially in a time when more and more people work from home. After all, employees enter the IT environment from a variety of 'entrances.'

Crystal-clear insight into ROI and costs
At Wortell, we work in a highly results-oriented way. If you opt for MDR, you will have insight into your monthly expenses and results. It's easy to compare them to the costs you'd need to incur if you would handle detection and response yourself. You'll instantly see that the costs of an in-house approach do not outweigh outsourcing, which makes it simple to justify your investment. As you will pay a fixed monthly fee for MDR, you'll always know where you stand. Moreover, our detection and reports provide insight into what's happening in your environment. This will also come in useful if you have to justify your investment.



24/7 security of your IT environment including support
Our cybersecurity experts ensure the security of your IT environment 24/7. Additionally, crisis management and legal experts provide company-specific support, so we can take targeted action where necessary. For a cyber incident is not a technical problem — it's a business problem. And to solve it, you need a service: MDR. The result of our efforts: maximum uptime and business continuity!

If you opt for MDR, here's what Wortell will do for you:

- Detection and response
- Crisis management and legal support
- 24/7 in-house staffing
- Very fast detection of cyber incidents and automated intervention using our in-house developed platform Vidara
- We'll automatically apply all knowledge in our use case library to your environment — this library contains use cases and lessons we've learned at other customers, which means you'll benefit from increased security right away

Hoe zit het met de kosten?

Bij Wortell gaan we zeer resultaatgericht te werk. Kies je voor MDR, dan heb je inzicht in je maandelijkse uitgaven én resultaten. Deze kun je eenvoudig naast de kosten leggen die je zou moeten maken als je detectie en opvolging zelf zou verzorgen. Zo zie je direct dat de kosten voor een in-house-aanpak niet opwegen tegen uitbesteding, waardoor je je investering goed kunt verantwoorden. Omdat je voor MDR een vast bedrag per maand betaalt, weet je altijd waar je aan toe bent.

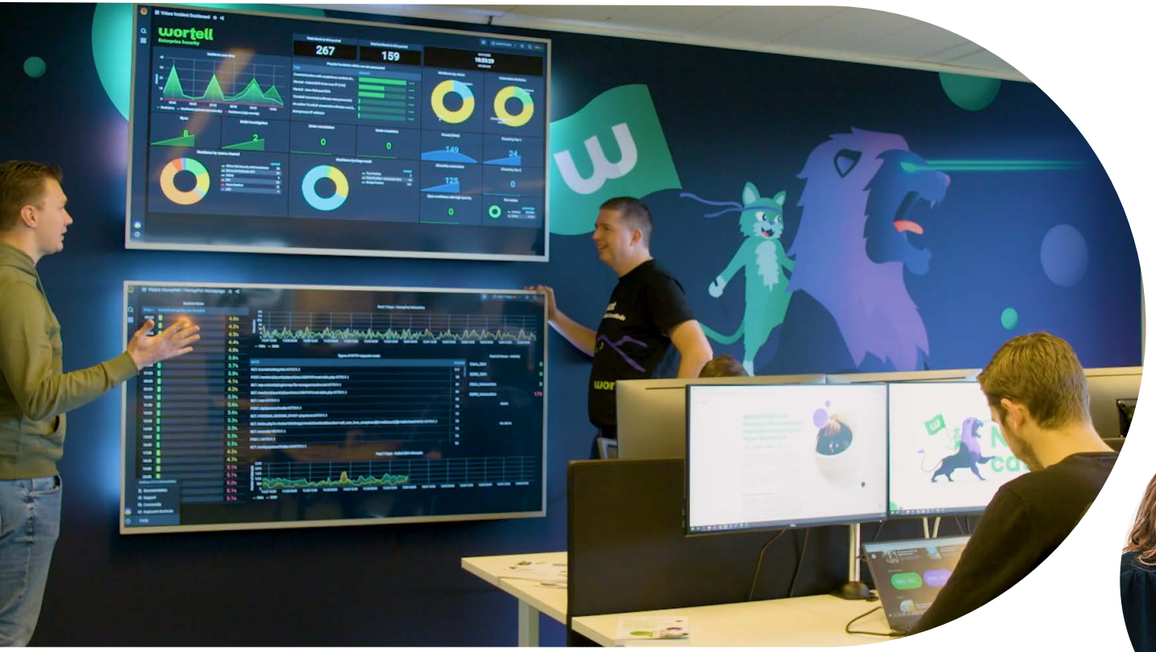
Wortell's MDR: why?

Data that is relevant to your organization
If you want to analyze a cyber incident, you need certain data, which is referred to as 'threat intelligence.' You can purchase this data, but it comes with two drawbacks: it's expensive and you often get a lot of data that is irrelevant to your organization. Wortell develops threat intelligence in-house, so you can work with highly relevant data that is a lot cheaper.

Two teams keep each other on their toes
One team provides rock-solid security, while another team — which consists of certified ethical hackers — constantly tries to bypass it. Why? That's how we keep each other on our toes at Wortell. The result: better security for your IT environment!

Understanding the overarching organizational context
Besides advanced cybersecurity services, Wortell also provides modern workplace and cloud services. That's why we understand the overarching context and have the in-house expertise required for solving incidents at the organizational level. A party that solely focuses on security is often unable to oversee the big picture — unlike Wortell, a 'jack of all important trades.'

Certified party
Wortell is a member of the Microsoft Intelligent Security Association (MISA), has twelve Microsoft Gold competencies, and is the first Certified Microsoft Threat Protection Partner worldwide. We are also ISO and NEN certified. Briefly put, you'll work with a team of certified experts!



Meer weten of aan de slag

Wil je meer weten over MDR? Of ben je benieuwd hoe goed jouw omgeving eigenlijk beveiligd is? Onze security experts vertellen je graag meer over MDR of denken met je mee over de best mogelijke beveiliging voor jouw organisatie. Zij kunnen je natuurlijk ook in contact brengen met organisaties die al gebruik maken van MDR. Wil je langskomen om ons security center te bekijken? Dat kan natuurlijk ook.

Bij Wortell is het ons doel om het gat tussen de eindeloze mogelijkheden die tot onze beschikking staan, en de mate waarin mensen en bedrijven hier gebruik van maken, zo klein mogelijk te maken. Wij geven mensen de technologie én de vaardigheden om succesvol te kunnen zijn in hun werk.

We empower people
Ontdek meer op **www.wortell.nl**

Schipholweg 641
1175 KP Lijnden
Nederland

www.wortell.nl
info@wortell.nl
020 7505050

Schipholweg 641
1175KP Lijnden

wortell