![RedSocks malware threat defender logo]

![Syntrophos Shared Service Center logo]

Syntrophos stays one step ahead of data leaks in Brielle, Nissewaard and Westvoorne with RedSocks Malware Threat Defender

When the Dutch municipalities of Brielle, Nissewaard and Westvoorne decided to centralise their infrastructures, Shared Service Centre Syntrophos considered ways in which it could manage the government's increasingly strict security requirements. Protecting personal data has become even more important with the introduction of the obligation to report any data leaks. From 1 January 2016, municipalities must have a clear insight into the risks of data leaks, and be able to act quickly if a leak is detected. RedSocks' Malware Threat Defender (MTD) monitors network traffic from the inside out, so threats are detected faster, before they can cause any damage. As a result, RedSocks MTD enhances existing security solutions like firewalls and antivirus software perfectly, enabling Syntrophos to be one step ahead of any potential data leaks.

Shared Service Centre Syntrophos manages the central infrastructure for the 1,300 staff of the three municipalities of Brielle, Nissewaard and Westvoorne in the west of the Netherlands. When these infrastructures were integrated, Syntrophos considered ways of not only harmonising the security of the new infrastructure, but also making it future-proof. Johan Sluijters, network administrator at Syntrophos who specialises in security said, *"The government is imposing increasing demands on the security of networks and personal data but political decisions can't always be responded to quickly within your infrastructure. In terms of security, we wanted to be prepared for both future policy, and as-yet-unknown threats. That's when the RedSocks Malware Threat Defender (MTD) came to our attention. Given that using the MTD means you automatically comply with a number of components of mandatory audits in terms of security, we wanted to find out what else the solution could do for us."*

Mandatory data leak reporting

The mandatory data leak reporting requirement, which comes into effect on 1 January 2016, also motivated Syntrophos to find a solution that could provide clear insight into the risk of data leaks. *"Municipal organisations attach significant value to protecting personal data,"* explains Raymond van der Meijs, ICT policy assistant at Syntrophos. *"As the Shared Service Centre, we wanted to demonstrate to our clients that we are adequately prepared for new data protection legislation. From 1 January 2016 organisations must report any data leaks, so we needed both an insight into the risk of data leaks, and the ability to act fast if a leak is detected. The way RedSocks MTD monitors network traffic makes it possible to detect threats proactively and makes it easier to comply with the data leak reporting obligation."*

Plug & Play

Syntrophos wanted to experience the benefits of the RedSocks MTD in practice, and set up a Proof of Concept (PoC). Sluijters added, *"It was almost 'plug & play'. Once you know where you want to deploy the MTD, which data should be routed through it and you have reserved the necessary IP addresses, then most of the work is done. Taking account of the 24 hours it takes to retrieve the threads, you get your first reports within the first couple of days."*

A number of security issues came to the fore during the PoC, which were quickly resolved. *"Most of the time was spent explaining the operation of the MTD to employees dealing with security issues. That's because the way it works differs radically from a firewall or virus scanner. As an example, it considers threats which are already present in the infrastructure rather than trying to keep threats out. That finding a threat does in fact show that a solution is working, is something people really need to get used to."*

Syntrophos
Shared Service Center

"With the RedSocks MTD we stay one step ahead of the problem, rather than having to take action afterwards once the harm has already been done."

Easily mastering data leaks

RedSocks MTD has now been running satisfactorily for more than a year. Following the implementation, the number of reports has declined dramatically, and the last report of any serious threat now dates from a few months ago. Sluijters commented, *"For me, the convenience the RedSocks MTD offers is the most important benefit. By running scans on what's going out, without being able to look further into the data, RedSocks gives me the perfect starting point for further investigation, without taking away control. I remain completely in charge, I know immediately what I have to watch out for, and I can easily set up a process to resolve the problem. In short, it makes my life a whole lot easier."*

Syntrophos is also confident about the imminent implementation of the data leak reporting obligation. *"With the RedSocks MTD we stay one step ahead of the problem, rather than having to take action afterwards once the harm has already been done. What we have now is the best possible protection of the details of residents and companies in the municipalities we serve,"* concludes Van der Meijs.

REDSOCKS

RedSocks is a Dutch company specialised in malware detection. RedSocks supplies *RedSocks malware threat defender* as a network appliance. This innovative appliance analyses digital traffic flows in real time based on the algorithms and lists of malicious indicators compiled by the RedSocks Malware Intelligence Team. This team consists of specialists in identifying new threats on the internet and translating them into state-of-the-art malware detection.

FOR MORE INFORMATION PLEASE CONTACT US VIA INFO@REDSOCKS.NL OR VISIT OUR WEBSITE: WWW.REDSOCKS.NL

REDSOCKS
malware threat defender

www.redsocks.nl