ThreatDown
Powered by Malwarebytes

Case Study

An Information Technology MSP finds a "golden ticket" in ThreatDown

As an organization, this Managed Service Provider (MSP) is dedicated to providing comprehensive, infrastructure-agnostic IT and security services across all industry sectors with the best possible customer service. Its commitment to that mission has led the organization to grow to over 250 employees, and three separate European offices.

The organization prides itself on keeping customers happy over the long haul, and a key part of that is helping them choose the right products and solutions. That responsibility falls to the organizations Technical Director. "I have to review a lot of products," explains Technical Director, "We work with hundreds of different products, so we know what's the best of the best."

There is no doubt about his first choice for endpoint security: "We recommend ThreatDown EDR and add-on DNS protection," he says, "I used three or four different products before ThreatDown, and it does things none of them did."

Partner-At-A-Glance

Endpoints – 1,661
Industry – Information Technology MSP
Solutions – Endpoint Detection and Response, Endpoint Detection and Response for Servers, DNS Filtering

Results

Best-of-breed protection. Software that's easy to license, deploy and use. Unmatched customer service.

"A golden ticket"

The organizations introduction to ThreatDown is a familiar story, and it starts with best-of-breed protection. It is an open secret in IT circles that the Malwarebytes detection technology that underpins ThreatDown catches threats that other solutions miss, and countless IT admins have used the Malwarebytes free scanner to backstop incumbent antivirus solutions. "We used to use Malwarebytes just to do a second scan," Technical Director explains, "it was brilliant."

"As long as it has ThreatDown it's secure," says Technical Director, but as an MSP he also values how easy it is to buy licenses, deploy and use the software, and demonstrate its value to customers. "I can go to OneView portal and see if there's an attack, and the whole graph around it," he explains, "Data is important, we need to be able to prove [its value] to customers. We can look at the logs and know it's doing a good job."

Above all though, it's the unmatched customer care he raves about. Every three months, the Technical Director is invited to a meeting by his ThreatDown Partner Success Manager, and they review and adjust the MSP's security setup, and talk about what's new and what's coming soon. "I have not met anyone else who does that, you have to chase them," says Technical Director, adding "Microsoft doesn't tell you if you've set up Outlook incorrectly."

> "I wish all other software vendors did a review every three months—that is a golden ticket. I cannot tell you how helpful it is."
>
> Technical Director

Ransomware

The organizations biggest security priority, and its customers' greatest fear, is the threat of organized cybercrime in the form of "big game" ransomware attacks. The Technical Director explains, "14 years ago, nobody had heard of ransomware, now everybody talks about it twice a day every day, it is a huge threat."

As an MSP, the security stakes couldn't be higher. They are responsible for security across a diverse range of organizations, but as a business with privileged access to so much data, it is also a prime target itself.

The key to combatting ransomware, says Technical Director, is "preparation, preparation." If the worst does happen, we are is determined to ensure its customers are equipped to recover, so it ensures they have comprehensive backups, and actively maintains them to make sure they are fit for purpose.

Prevention is better than a cure though, so while it plans for the worst, it relies on ThreatDown's ability to detect ransomware, and to isolate and roll back affected endpoints, to ensure it never comes to that. "Where ThreatDown comes in is to make sure it doesn't happen. Endpoint isolation is brilliant," says Technical Director.