C⊙RE

TRANSFORMING BUSINESS THROUGH TECHNOLOGY

AND NOW FOR SOME GOOD NEWS…

EAMON MCGANN | CLIENT SOLUTIONS DIRECTOR

MICROSOFT'S EVALUATION AS A LEADER IN SECURITY SOLUTIONS PROVIDES EXACTLY THE REASSURANCE ORGANISATIONS NEED RIGHT NOW.

It's official. Microsoft's security offering has been identified as among the best available, following independent evaluation of the 12 most significant enterprise detection and response products on the market. This is exactly the reassurance organisations need at a time when many will be worrying whether their protection is sufficient to meet the challenge of widespread remote working.

The Forrester Wave: Enterprise Detection and Response, Q1 2020 positions Microsoft as a Leader for its endpoint detection and response capabilities, awarding its current offering the highest score among Leaders. Microsoft also achieved the highest score of all participants for the extended capabilities it provides. Furthermore,

Eamon McGann is the Client Solutions Director for Core, responsible for helping organisations translate and understand the value of Microsoft 365 technologies. With 30 years' experience, Eamon is an industry-recognised expert, having worked at Core since its formation, Eamon has played a pivotal role in working on some of Microsoft's biggest projects and technology rollouts, including implementing the UK's first Microsoft SharePoint system in 2001.

core.co.uk

Microsoft Defender Advanced Threat Protection received the highest score possible (5/5) across six areas including endpoint telemetry, security analytics, threat hunting, and response capabilities, as well as in performance and planned enhancements.

This demonstrates that effective security is integral to the entire Microsoft offering. Operating on a zero-trust basis, Microsoft's extended detection response doesn't just cover the various product domains, it covers the gaps between them and provides intelligence and incident management so operators can analyse what's important and not get lost in the noise.

CHANGING NATURE OF THE THREATS REQUIRES JOINED UP RESPONSE

There's no question that threats have changed over recent years. From being single domain or hacking at the level of the individual, now threats are entering by one route, morphing and crossing into another domain.

We have seen situations where a multi-domain threat has come into an organisation through phishing which subsequently attacks an individual's email stealing the person's identity and creating an auto-forward based on particular rules. Such a scenario seriously compromises the organisation, creating financial pain in addition to extended downtime. It is exactly the sort of issue that Microsoft Threat Protection can fix before it even happens.

Multi-domain threats require these new approaches. In the past, security was seen to be best managed by using multiple tools for different domains. Today, such an approach is not only complicated and labour intensive, there is a strong likelihood that issues will fall through the gaps. That's the strength of Microsoft Threat Protection. Security is built in for each product domain – endpoint devices (laptops, phones etc), email, identity and apps – and domains are integrated across the platform.

SYSTEMS DON'T JUST FIND THREATS, THEY REMEDIATE THEM TOO

Even before the coronavirus pandemic, our research had identified security as the number one worry for IT teams and Chief Information Security Officers (CISOs). Now, with more people working on their own devices at home, those concerns will have gone through the roof. And rightly so. Without the right protection in place, the change in working practices brought on by COVID-19 exposes companies to significant additional threats.

So, what is it about Microsoft's capabilities that allow those in charge to sleep better? It's actually not just the endpoint cover and cool technology. It's the intelligence. Built-in orchestration and AI enable security centres to get ahead of the threat because systems identify patterns between multiple events happening across different individuals, devices and server services. They can link them into a single incident and send out an alert.

And there's more. Defender doesn't just find threats, it remediates them. This means that even if a threat has been let through initially, if Defender subsequently identified the threat it will retrospectively remediate the issue.

LEANER MORE PRODUCTIVE TEAMS AND RAPID IMPLEMENTATION

Ultimately, many CISO's are less interested in the how, they just want to know they are effectively

covered. This is where managed service providers like Core can help. Microsoft tooling is great, but to really be aware of where the threats are, organisations need to be actively carrying out security assessments.

We have invested in these areas over a considerable number of years which has put Core ahead of the technology and ahead in terms of how to deploy it to create the efficiencies these products can offer. Apart from anything else, it means, we can get organisations up and running with a predefined set of policies straight away. It gives peace of mind from week one and is then developed and customised through our proactive security analytics and operations approach which involves continuous monitoring, analysis, reporting and threat hunting, together with intelligence drawn from our overview across all customers.

In last year's Cyber Security Breaches Survey around a third of businesses reported suffering cyber security breaches or attacks in the previous 12 months. Among medium and large businesses, that figure rose to around 60%. In this environment of heightened threat levels, it's clear that good news on security solutions will be very welcome to many organisations.

FAST TRACK TO SUCCESS WITH AN EXPERIENCED PARTNER

For nearly 30 years, Core has been working with organisations to successfully implement transformative digital technologies which deliver defined business outcomes.

We know that employee resistance is a major barrier to project success, so we place people at the heart of change with our technology enablement and customer success services. These are tailored to your specific business objectives and unique operating environment. They help drive acceptance, engagement and use of Microsoft technologies.

By engaging users early, understanding their roles and pinpointing their needs, Core can demonstrate value to them and you, and help develop a culture of acceptance before a single piece of technology is deployed.

At Core, we help you define your technology roadmap to support change and modernisation initiatives in your organisation, ensuring you maximise your investments and develop a roadmap for the future.

Our Technology Enablement services are designed to maximise user acceptance, engagement, and ultimately, the utilisation of the technology to realise business value.