

Excerpt of blog post reprint from Trend Micro's SIMPLY Security blog (Oct. 2016)

Trend Micro Endpoint Security Named A Leader in Forrester Wave Report



Ransomware, targeted attacks, zero-day threats, information-stealing malware – business owners face a wide array of threats today. In 2016, ransomware attacks became more tenacious than ever – with a 752% increase in new ransomware families. Effective, multi-layered endpoint security is vital to keep threats at bay and to ensure your data is safe from harm.

That's why at Trend Micro, we are delighted to learn that our technology has received the highest score in the current offering category among 15 vendors appraised in the The Forrester Wave™: Endpoint Security Suites, Q4 2016 report. We believe that being named as a leader by Forrester's report affirms the merits of having a complete endpoint protection portfolio and marks yet another point of independent industry validation of our technology leadership.

Trend Micro received the highest score possible in the Product Roadmap and Go-To Market Strategy criteria, notching an overall score of 4.7 out of 5 in the strategy category. Forrester specifically stated that "Overall, Trend Micro's current portfolio, combined with its short- and long-term road maps, aligns very well with the current and (likely) future needs of enterprise buyers."

In addition to providing the best endpoint security technology available today, Trend Micro has the right vision to develop sophisticated techniques to combat the threats of tomorrow. We have released a new class of cyber security, XGen™. XGen™ security complements our proven optimized protection with high-fidelity machine learning. Using a single or incomplete set of techniques can leave gaps in a company's security posture, but the evolving threat landscape demands a comprehensive, multi-layered endpoint protection strategy. This is exactly what XGen™ security offers. With 28 years of experience and more than 155 million endpoints protected, this latest release demonstrates Trend Micro's unwavering commitment to innovation in the area of endpoint security.

Firms under fire

Companies, both large and small, are under attack from all sides. Whether its sophisticated information-stealing malware developed to bypass detection, ransomware designed to cause maximum disruption, or more generic malware written to exploit unpatched vulnerabilities – threats are everywhere. And thanks to the rise of mobile working, cloud computing and risky user behavior, the security gaps within organizations are growing and becoming a real challenge.



Organizations need to lock down this risk with comprehensive, layered protection, including endpoint security. Yet, [new research suggests](#) only one third of businesses have an endpoint security strategy in place. Since the bad guys employ a wide variety of tools and techniques to infiltrate organizations, you must look to product offerings that combine multiple protection techniques.

Many vendors talk about their features as the "silver bullet solution", like machine learning, but beware of the marketing hype. Often, on closer inspection, their overall proposition can be lacking in depth and breadth, with a narrow focus that could let threats through. Machine learning, for example, is good at stopping malware in executables but is less able to detect threats in non-executable files, such as PDFs or Word docs; so machine learning is only part of a complete endpoint protection strategy.

Leading the way

Under pressure, IT buyers often lack the time and resources to appraise each and every product in the expanding endpoint security market. That's why reports from independent analysts like Forrester are invaluable.

Trend Micro endpoint security protection covers the full life cycle of threat defense with the following:

- **High-fidelity machine learning** analyzes data before execution and at runtime
- **Web reputation** stops access to malicious websites
- **Variant protection** looks for obfuscated and polymorphic variants of malware
- **Application blacklist** prevents specific apps from executing on the endpoint
- **Behavioral analysis** examines an unknown item as it's loading and looks for suspicious behavior in the operating system, applications, scripts and how they interact to block them

Endpoint security is just one piece of the overall security puzzle and will only be effective if used in conjunction with layered protection at the server, network, and gateway levels. But, it's a vital piece and worth spending extra time and resources on getting right.

To see how Worry-Free Services, powered by XGen™ security, protects your data, email and users, visit www.worryfree.com.