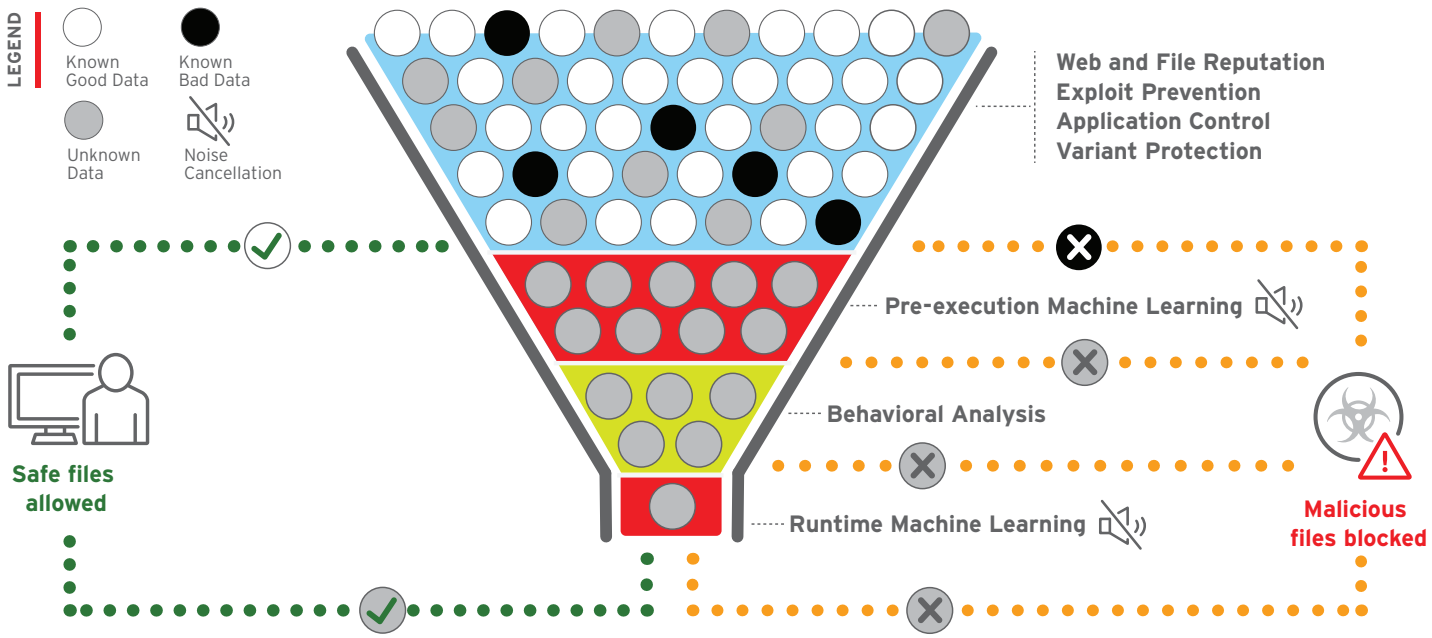
THE TOP 5 MYTHS OF NEXT-GEN ENDPOINT PROTECTION

'Next-generation' endpoint protection or next-gen AV has been getting a lot of press recently. But what does the term actually mean? For IT security managers under pressure, the most important thing isn't the latest buzzword, but finding a solution which is effective in protecting their organization from an increasingly agile and determined online enemy. Multiple threat protection techniques working in synergy is the key to this.



But it can be tough finding the time to pick through the marketing FUD to find the solution that will deliver the best protection. So let's unpack five common myths associated with next-gen endpoint protection.

MYTH #1: NEXT-GEN ENDPOINT PROTECTION = MACHINE LEARNING

Machine learning is good at blocking threats hidden in executable files, but it struggles to detect threats hidden in non-executable files, such as malicious scripts in PDFs or Word documents. There are many different threats out there – e.g., ransomware, browser exploits, and zero-day threats– and you need many different protection techniques working together to deflect them. Other techniques that work in concert with machine learning, like web reputation, behavioral analysis, sandboxing, application control, and vulnerability shielding, are critical to ensure you have the best protection against the broadest range of threats.

MYTH #2: NEXT-GEN SOLUTIONS DELIVER 'UNBELIEVABLE' PROTECTION

Some new vendors are making bold claims for their products and present incredible results. Frankly, they are unbelievable. The results come from tests where the vendors control all of the parameters, including threats tested, and the configuration of competitive products. When tested by reputable, independent organizations like AV-Test, their results simply don't make sense.

MYTH #3: ENDPOINT IS THE BEST PLACE TO STOP THREATS

Endpoint protection is key but many threats can be blocked at the web or email gateway before they ever make it to your endpoint. When this happens, your endpoint security is left to focus on the most sophisticated threats. Your web and email security should work with your endpoint protection to share threat intelligence, giving you a holistic view of what is happening across every threat vector.

MYTH #4: ALL YOU NEED TO DO IS PREVENT THREATS

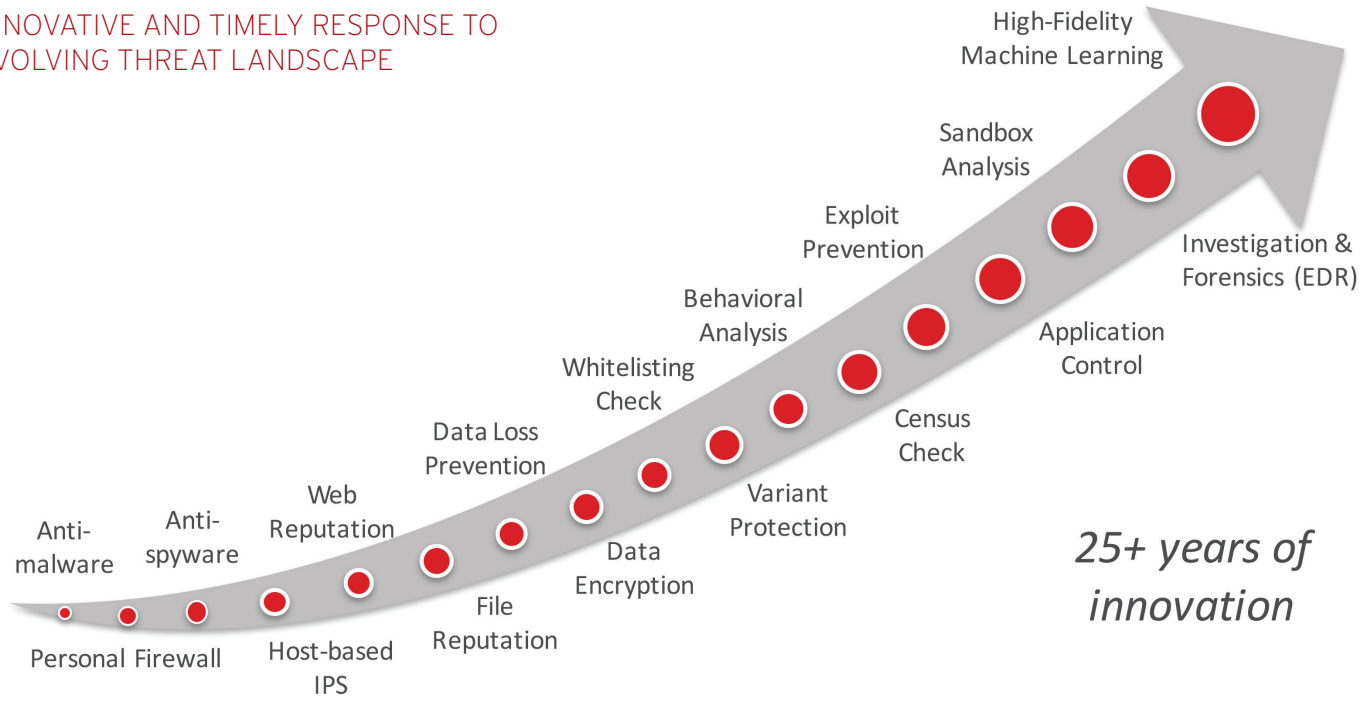
The reality is, no vendor can provide 100% protection from all of the threats. That's why you need tools to not only detect threats, but recover from them as well. And you need security that can adapt so the next time you encounter those threats, they'll be prevented. This can only be achieved if the layers of your endpoint protection solution share intelligence, which is difficult to achieve when you're using point products from multiple vendors.

MYTH #5: ONLY RISKY START-UPS PROVIDE NEXT-GEN PROTECTION

Many small start-ups make lots of market noise and claim that their technology is the silver bullet to solve all your endpoint security problems. But protecting your organization is about more than one technology. Customers value a proven endpoint security partner that continually evolves its endpoint protection solutions, like Trend Micro. Trend Micro XGen endpoint security provides new capabilities, like high-fidelity machine learning, to protect against the changing threat landscape. That's why our customers trust us to protect over 155 million endpoints worldwide, and why you know we will be there tomorrow, when many of these start-ups will be a distant memory.

To learn more about the Trend Micro™ XGen™ endpoint security visit **www.trendmicro.com/xgen**

INNOVATIVE AND TIMELY RESPONSE TO EVOLVING THREAT LANDSCAPE



TREND MICRO™

Securing Your Journey to the Cloud