Endpoint security isn't dead – it's just getting smarter

itnews

> **The competitive space is attempting to turn AI into a feature – but AI is fundamentally what we built the product on, it is the future.**

JASON DUERDEN - CYLANCE COUNTRY MANAGER

With one report after another suggesting that cybercriminals have overrun corporate defences, it's easy to believe marketing hype suggesting that endpoint security is dead – and that cybersecurity is all about how quickly you can respond to the inevitable breach.

Yet a new Cylance survey of iTnews readers shows that Australian IT decision-makers still believe in the power of prevention: 56 percent of those surveyed disagreed with the suggestion that endpoint prevention was dead, while just 22 percent agreed.

That's an optimistic assessment given that fully 38 percent of respondents said their organisation gets a malware infection once or twice per year. Another 7 percent reported 2 to 9 infections per year, while 6 percent of companies are infected 10 or more times per year.

Such regular infections suggest that new methods of attack have left many conventional signature-based malware tools ineffective and struggling to keep up.

That's been a challenge for many security executives. "With so many zero day threats, detection of patterns on endpoints [using machine learning] is critical," one respondent noted.

"After being detected, automated proactive action to stop the threat is necessary. This is getting harder with diverse workloads going through the endpoints, identifying what is and is not a threat."

One executive was far less specific, wishing only that her organisation would simply pay more attention to endpoint security – and stop offloading responsibility to vendors.

"Caring about it would be a great improvement," she offered. "We largely rely on suppliers' products working as advertised."

Meeting the challenge of keeping up

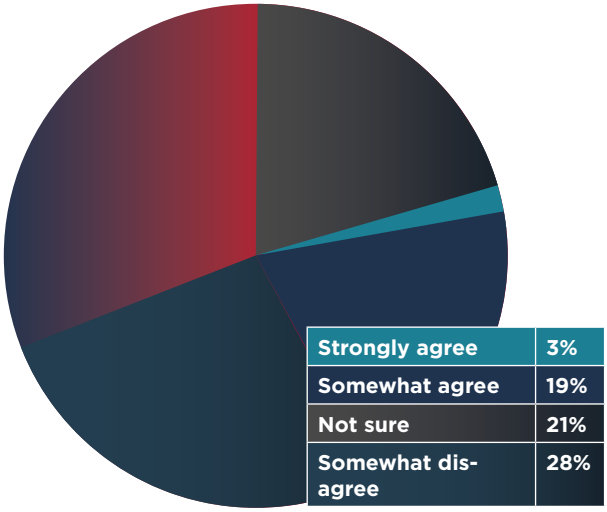
Even though legacy products may seem to be working as advertised, they aren't necessarily effective at keeping up with the pace of innovation in malware development – which has accelerated over time as new vulnerabilities and attack techniques come to light.

Such tools are notoriously ineffective against zero-day attacks being discovered and exploited on a regular basis. Yet all is not lost, however, as innovation in endpoint protection allows companies to take the fight to a new, more level battleground.

This fight is being defined by innovation in artificial intelligence and machine learning (ML), which is being applied to great effect in providing a more flexible, responsive endpoint defence than was possible using previous technologies.

AI has become a catchcry for endpoint innovation across the industry, although different vendors have taken it to different lengths. And while nearly every endpoint security vendor now claims some degree of AI capability, Cylance country manager Jason Duerden warns buyers to evaluate their options carefully.

Many vendors "don't understand the fundamental nature of the product," he explains. "The competitive space is attempting to turn AI into a feature – but AI is fundamentally what we built the product on, it is the future. It is about starting from the foundational code, and using data science and machine learning from the get-go."



Do you agree with the opinion of some people in the industry that "malware prevention is dead on the endpoint"?

Data-driven endpoint protection

Not all security vendors have generations of data-science expertise under their belts, but this domain experience comes with time. It is crucial to understand not only how data science helps efficiently process a mountain of event data, but how its results can be tied into the broader cybersecurity landscape.

Establishing a beachhead on this landscape requires strong use of learning algorithms, which improve their accuracy and capability over time based on their analysis of past event data.

The strength of these learning algorithms has been demonstrated to surpass conventional signature-based antivirus, over and over again. Cylance tests with the globally-destructive WannaCry ransomware, for example, showed that the May 2017 attack would have been detected and prevented using learning algorithms from as far back as October 2015.

It's rare for a security protection to predate an attack, but this is an example of the power of applied data science – and it has translated to strong results for digital-media giant REA Group, which adopted Cylance security

tools as a way of building a more proactive defence against malware and cyber attacks.

"It does what it says on the tin," explains REA Group chief information security officer Craig Templeton. "It finds bad stuff and kills it without me having to worry about virus updates and so on. From an automation and prevention point of view, it has been really good – and frees up our resources to work on other things."

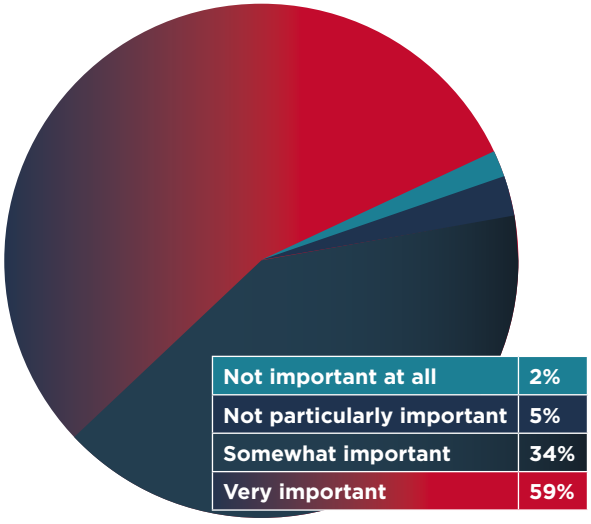
A fast-expanding real-estate interest, REA Group has rolled Cylance out in several newly acquired businesses that were previously using other endpoint protection solutions.

"Almost immediately when we turned it on, it lit up like a Christmas tree," Templeton said. "It was finding all sorts of things that the previous solution didn't see. Even with something it hasn't seen before, it gives us reasonably high confidence that it can sense that something is going on."

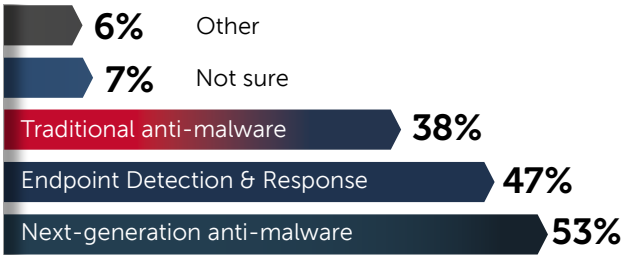
Machine learning techniques are becoming even more powerful and accessible thanks to one other key capability: the cloud.

Cloud services have evolved so quickly in recent years that it's now possible for any company to easily commission and use virtually unlimited amounts of data, collected from every corner of the globe. In the endpoint protection scenario, this means that real-world users' experiences can be collected, analysed and applied to future protections at a scale that would have been impossible just a few years ago.

"If we look at the way we now build neural networks on cloud computing, this capability fundamentally could not be built until the late 2000's," Duerden explains. "We really are now experiencing a whole new evolution of cybersecurity, where everything in the future will be built on that cloud and machine learning capability to create new security technologies. The real benefit of machine learning is applied to the endpoint itself, for autonomous protection on and offline.''



When making a purchasing decision, how important is the performance impact of endpoint security on your organisation's systems?



What are your organisation's top priorities for endpoint security in 2018?

Integrated endpoint detection and response

Surveyed Australian IT decision-makers seem to agree: fully 53 percent of respondents to the Cylance-iTnews survey said their top endpoint security priority was the implementation of machine learning-driven, next-generation anti-malware tools.

Importantly, 37 percent said they were also focused on deploying traditional anti-malware tools. This suggests that despite industry suggestions that traditional endpoint protection is dead, real Australian businesses seemingly do not have enough exposure to education around future state controls – thus leaving them vulnerable to attacks.

Yet detection and prevention are only part of the next-generation endpoint detection and response (EDR) strategy. Companies also now recognise that while AI and ML algorithms can improve the sensitivity and specificity of detection algorithms, a complete endpoint protection strategy also requires a comprehensive response strategy to minimise data loss and damage to the business in the event of a cybersecurity breach.

Fully 47 percent of the surveyed companies said they were prioritising their EDR capabilities this year, with a broad range of areas singled out for improvement.

Application control, for example, was seen as an important preventative strategy that prevents the execution of non-approved applications or other processes on critical systems.

Others pointed to the need to improve patching processes and tighten control of privileged accounts, which are often left unmanaged and exploited by attackers to linger on corporate networks for weeks or months undetected.

And many expressed frustration at the typically separate architecture of cybersecurity tools and EDR frameworks.

Indeed, 55 percent of respondents said it would be helpful if their security provider could complement attack-prevention technologies with EDR capabilities to help them combat advanced cybersecurity threats.

One trend was clear from the results: users want their vendors to provide them with more effective endpoint protection and response solutions – and most industry players have so far failed to do so.

"The standard defence-in-depth strategy says to buy a firewall, antivirus, email gateway security, and other layers," Duerden explains.

"But all of those layers are failing to solve core problems. Organisations are on a digital transformational shift, and we have to take security on this same transformational shift. It's just not how it used to be anymore, because infrastructure requirements have changed."

Locking down the risk

Those requirements now include increased use of automation, which can work in lockstep with AI/ML solutions to build an automated response to a detected security issue.

The system might, for example, automatically terminate a malicious application lock up a user account or session, or take other action.

"This way, when an administrator or operations person is using the solution, they are investigating the context of the alert rather than investigating a breach," Duerden says.

"This moves them to a model of understanding what the alert was and what was prevented – rather than just saying 'hey, something bad is happening so go get your tools and fix it'."

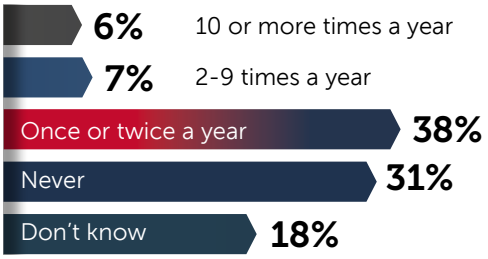
Regardless of how much security endpoint protection tools offer, survey respondents were quick to reinforce the importance of continuous education for users – who, as one executive put it, need to be "serious and active about security."

This included pushing users to be more diligent about areas such as upgrading their endpoint device operating systems: "staff are currently not upgrading these in a timely fashion," she noted.

Another executive highlighted the importance of enforcing adherence to policy, which users often violate out of carelessness or ignorance. "Without policy the rest is just snazzy software," he said.

"Staff training is the first line of defence," another respondent said. "Users are the first line of defence and must have an understanding of what to look out for."

> **"Cylance tests with the globally-destructive WannaCry ransomware, for example, showed that the May 2017 attack would have been detected and prevented using learning algorithms from as far back as October 2015."**



Approximately how often each year does an endpoint in your organisation get a malware infection?

The survey was conducted in March 2018 by iTnews on behalf of Cylance. Of these respondents, 38% were CIOs, CISOs, IT managers or equivalent; another 32% were IT professionals or workers; and 9% were CEOs, CFOs or equivalent. Thirty-four percent were in large organisations (1000+ users) and the rest were evently spread between small and medium-sized businesses. Key industry sectors represented included IT, healthcare, financial services, government, and manufacturing. ■