7 Reasons to Move Away from Legacy AV

Cybersecurity professionals already know it: Legacy AV would not help them out on a rainy day. Legacy AV was born to solve a problem of few viruses every now and than, not the flood we see today, which risks the way we live;

by SentinelOne

1 Reduce Operational Costs

It is hard to measure the overall cost of running outdated technology that may make you vulnerable to cyber threats. NSS Labs conduct a comparative test with all endpoint security players. NSS Labs identified SentinelOne as having the best overall TCO over a three-year period.

2 Boost Protection

Over time, adversaries have improved their malicious techniques, easily bypassing traditional security products with techniques like fileless malware and PowerShell exploits. Get ahead of the attackers and prevent advanced attacks with next-generation technology.

3 Save Time

Time is a major factor when it comes to your security. The entire concept of dwell time – the time from adversary penetration to detection or mitigation is on average at least 90 days. Meanwhile, your security experts are wasting valuable time collecting evidence of a breach. You want your security team to focus on what matters, not looking for a needle in a haystack.

4 Improve ROI

In the beginning there was just AV. Then, another agent to cover advanced threats. Then an additional agent that can provide visibility. On top of that, another one to report applications from a vulnerability scan. And so it goes on. More agents running in parallel on your endpoint means more performance impact.

5 Make the Software Work For You

A characteristic of legacy AV is that it requires highly-trained staff to operate and interpret. Where are all those alerts coming from and are they connected? Which ones are false positives, and why are people in Marketing complaining they can't access their computers?

6 Integrate Your Security Solutions

With the security industry as a whole experiencing a sharp cyberskills shortage, an endpoint security solution should integrate with your existing software stack and not create more work for your SOC team or IT administrators.

7 Reduce Post-Breach Costs

An easy-to-use management console that presents the entire attack storyline can help you to quickly close out vulnerabilities and even track down the individuals responsible. The faster you can put things to rights, the lower the financial impact on the enterprise.

Ready to Try?

SentinelOne