CYLANCE

Evaluation Guide

How To Evaluate a Next-Gen Endpoint Security Solution

Top Four Things To Consider When Choosing a Next-Gen Endpoint Security Solution

When making an important decision such as selecting a new security vendor to protect your vast array of endpoints, it is important to review your options closely. Here are four things to consider before making your selection:

1. **Effectiveness** — Any new security solution should deliver considerably increased prevention capabilities over your existing product. There are many third-party testing reports publicly available that offer comparisons of the most common endpoint security products on the market today.

   CylancePROTECT® consistently tops the list in these third-party tests. Thousands of customers have replaced their existing AV or endpoint security solution with Cylance's next-generation endpoint solution.

2. **Simplicity** — Pay close attention to the effort required to install, run, and maintain any new security solutions you are considering.

   CylancePROTECT can be installed in minutes, tuned quickly, and does not require daily signature updates. CylancePROTECT delivers value immediately and does not require security experts to operate effectively. In fact, after transitioning to CylancePROTECT, many organizations can reallocate their existing resources to other critical business projects.

3. **Performance** — Users of legacy endpoint security products have had to deal with these products consuming vast amounts of their computers' processing capabilities, essentially rendering the endpoint unusable during daily scans, signature updates, and the like.

   CylancePROTECT consumes, on average, less than 2% of CPU, meaning end-users will no longer be slowed down by their endpoint security protection.

4. **Vendor Viability** — There are over 1,600 security companies actively selling their wares. With so many vendors claiming to provide the same end results — better protection — it is important for you to perform your due diligence before selecting a vendor. At a minimum, you should consider:

   - **Reputation** — Does the vendor have good reviews from current users? Does the vendor have partners that frequently recommend their products? What do analysts say about the vendor? ***CylancePROTECT consistently rates high among security practitioners and partners for customer satisfaction and delivering on expected benefits.*** Review hundreds of positive reviews here.

   - **Vision** — What does the vendor have planned for the solution for the next 12 months? What about the next five years? ***Cylance is committed to driving innovation in CylancePROTECT to ensure the level of protection that can be delivered is continually improved. In addition to AI malware threat prevention, CylancePROTECT also provides application control, script control, memory protection, and device control, all of which will be further enhanced with each subsequent release.***

Whether you are considering making the move to next-gen endpoint security to improve your team's efficiency, meet government mandates, or other reasons, **CylancePROTECT** delivers the right mix of threat prevention capabilities, effectiveness, simplicity, and performance to decrease the workload on your security team without increasing the cost of protection.

About Cylance

Cylance® uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security.

Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

Cylance at a Glance

How Cylance Stacks Up Against Legacy Security Tools

Capability	CylancePROTECT	Shrink-Wrapped Endpoint Security Solutions
Malware Prevention	▪ AI is the primary conviction method ▪ No signatures required	▪ Signature-based ▪ Requires daily updates
Other Threat Prevention Capabilities	▪ Script control ▪ Application control ▪ Memory protection ▪ Device usage policy enforcement	▪ Varies from product to product ▪ Generally offers rudimentary threat prevention techniques
Usability and Deployment Model	▪ Simple to deploy and manage with cloud-based management console ▪ No additional hardware required	▪ Complex deployment and management on-premises ▪ Management platforms require costly additional hardware
Continuous Prevention	▪ Endpoint protected both on and off the network ▪ No cloud connections required as ML model runs on the endpoint	▪ Cloud connection usually required ▪ Prevention can degrade if endpoint is offline
Market Applicability	▪ Freely used across all markets, both public and private ▪ FedRAMP Certified	▪ Potentially under government mandate prohibiting use in government agencies

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE®