CYLANCE

Next-Generation **ANTIVIRUS**

CylancePROTECT®

CylancePROTECT is a Next-Generation Antivirus (NGAV) product that redefines what antivirus (AV) can and should do for your organization by leveraging artificial intelligence to detect AND prevent malware from executing on your endpoints in real time.

The cybersecurity industry is wrought with change, yet the fundamentals of malware detection have remained the same for more than three decades. In the face of constant innovation from attackers, antivirus vendors continue to focus on aging technologies that use signatures and post-attack behavior analysis to protect computers. A new approach is required.

Algorithmic science and machine learning are fundamentally shifting the equation, offering new ways to effectively identify, diagnose, categorize and control the execution of every file. Cylance® is leading this revolution with predictive and preventive products such as CylancePROTECT, which define NGAV.

Defining NGAV

The current, outdated approach of blacklisting relies almost entirely on using signatures and simplistic behavioral information to detect attacks. This worked for a while as the costs for attackers and defenders to respond to each other were at parity. As the bad guys added new tricks, defenders adapted and evolved, forcing attackers to innovate further. The attackers now have the advantage. The sheer number of threats is exploding exponentially, with large numbers of new threats appearing daily. Always-on, always-connected devices provide new, fertile ground for attacks. Improvements in defense are met with swift, advanced responses – to the point where adversaries are gaining a significant advantage. The cost for attackers is far lower than for defenders, due to outdated detection and response strategies. Traditional methods are failing.

Key elements of a Next-Generation Antivirus include:

Automated static code analysis – Dormant and non-active code should be analyzed at the level of its core DNA, or characteristics, prior to it's ability to execute. These characteristics can be as basic as the PE file size or the compiler used, or as complex as a review of the first logic leap in the binary. Cylance extracts millions of unique characteristics from potentially hazardous files and applies machine analysis to determine their intention.

Execution control – Detection of bad, abnormal and good files should be coupled with the ability to control the object in real time. Rather than relying on hash comparison or post-run behavior heuristics to determine what to do, Cylance evaluates objects in less than 100 milliseconds, early in the run time process. This allows the agent to prevent execution if the object is determined to be malicious.

No daily updates – A key weakness of traditional security solutions that rely on whitelisting and blacklisting is the need to retain vast databases of hashes and other signatures of known malware or approved applications. CylancePROTECT is a sophisticated agent that makes decisions in real time on the host by classifying an object's characteristics against optimally trained statistical models. Those models are updated every few months, but retain effectiveness for much longer. There is no need to constantly download new file signatures and worry that detection doesn't flag a threat when you miss a day's worth of updates.

No connectivity requirements – Many traditional security solutions rely heavily on the cloud to supplement their protective capacity. While Internet access is often available, piping vast amounts of information to a vendor is not always possible. CylancePROTECT operates autonomously, classifying threats using its entirely disconnected agent. Autonomously making the correct decisions is imperative for situations such as air-gapped networks used

in industrial control systems and low-bandwidth networks used by retail point of sale systems, branch offices and remote employees.

Non-disruptive – The appropriate protection architecture should be invisible to users and easy to deploy and manage for administrators. The CylancePROTECT agent is small and typically uses less than 1% of CPU. It is easily deployed with common distribution tools and offers browser-based alerting and policy management.

Contextual visibility – In addition to predictive, proactive detection and blocking, next-generation antivirus should collect data that provides the full context of attacks for analyst and incident response intelligence. The Cylance management console provides pre-execution insight and detonation intelligence from dynamic analysis.

Some vendors already claim to offer next-generation antivirus technology. Yet CylancePROTECT is the first and only product that is both highly effective in blocking threats and has a low impact on users. NGAV must offer both to satisfy the requirements of a "next new" that imparts better detection and protection while seamlessly fitting into normal company operations.

Given that it's taken 30 years to roll out the current AV solutions, an NGAV needs to either significantly enhance current endpoint security or replace it entirely.

Cylance Consulting

The mission of Cylance Consulting is to empower corporate IT to better protect their organization by helping reduce the attack surface. Vulnerability and penetration testing establish a baseline security posture. A compromise assessment determines the who, what, when and how of a successful attack and provides best practices for remediation. Our incident response and customized services fix problems much faster and in a less intrusive manner than alternative approaches.

About Cylance:

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated machine learning and artificial intelligence with a unique understanding of a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com

+1 (877) 97DEFEND
proservices@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700 Irvine, CA 92612