CYLANCE
+1 (877) 973-3336 • cylance.com

Introducing PROTECT

Zero Day Malware Prevention

*"The fundamental flaw in today's cyber security infrastructure is that detection happens **before** prevention. Human generated signatures, based primarily on previously discovered samples, have failed to solve the problem as zero day malware continues to operate silently and unimpeded."*
- Stuart McClure, Cylance Founder and CEO

Future-Proof Endpoint Security

CylancePROTECT takes a mathematical approach to malware identification utilizing patent-pending machine learning techniques instead of signatures and sandboxes. These techniques effectively render new malware, viruses, bots and unknown future variants useless.

Through the use of advanced mathematics rather than reactive signature or trust-based systems, Cylance has developed the most accurate, efficient and effective solution for preventing advanced malware and persistent threats from executing on your organization's endpoints.

The Power of Infinity

At the core of Cylance's unprecedented malware identification capability is a revolutionary machine learning research platform, termed Infinity. Infinity harnesses the power of cloud computing, big data analytics and artificial intelligence to create a machine learning "brain" on each endpoint. It analyzes and classifies hundreds of thousands of characteristics per file, breaking them down to an atomic level to discern whether an object is "good" or "bad" in near real time.

(Continued on Next Page)

How It Works

The CylancePROTECT architecture consists of a small agent that integrates with existing software management systems like McAfee ePO and IBM Endpoint Manager (formerly BigFix), or Cylance's own cloud console. The endpoint will detect and prevent malware through the use of tested mathematical models on the host, independent of a cloud or signatures. It is capable of 100% protection in both open and isolated networks without the need for continual signature updates.

CylancePROTECT alleviates two principal problems:

1. Real time detection and prevention of malware through the application of Infinity machine learning models.

2. Memory protection and execution control through kernel modules to address advanced non-resident based threat tactics including Injection/Hijacking techniques, overflows, and in-memory execution techniques.

These two core functions are supported by a variety of ancillary features necessary for enterprise functionality, including:

- Whitelist and blacklist support for administrative granularity
- Detection mode (passive auditing mode)
- Self-protection (prevention against user or attacker tampering)
- Complete control, update and configurability from the management console

Defense requires applying the best protection at the most vulnerable locations – the endpoints. Cylance's mathematical approach stops the execution of harmful code regardless of having prior knowledge or employing an unknown obfuscation technique. No other anti-malware product compares to the accuracy, ease of management, and effectiveness of CylancePROTECT.

CylancePROTECT will be available in February 2014, for more information please contact sales@cylance.com or call us at +1 (877) 973-3336.