

“The fundamental flaw in today’s cybersecurity 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 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.

By taking a mathematical approach to malware identification utilizing patent-pending, machine learning techniques instead of reactive signatures and sandboxes, CylancePROTECT renders new malware, viruses, bots, and unknown future variants useless.

Cylance has developed the most accurate, efficient, and effective solution for preventing advanced persistent threats and malware from executing on your organization’s endpoints.

At the core of Cylance’s unprecedented malware identification capability is a revolutionary machine learning research platform that harnesses the power of algorithmic science and artificial intelligence. 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 real time.

How It Works

CylancePROTECT’s architecture consists of a small agent that integrates with existing software management systems 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 detecting and quarantining malware in both open and isolated networks without the need for continual signature updates.

Defense requires applying the best protection at the most vulnerable location — the endpoint. 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.

What Are the Key Components?



Malware Execution Control

- No signatures
- Machine learning with predictive analysis
- Autonomous
- Pre-execution prevention in under 100ms
- No daily scans
- Rejects potentially unwanted programs (PUPs)
- Controls tools used in lateral movement

Device Control

- Provides control over use of USB mass storage devices
- Helps prevent the exfiltration of data through removable media

Application Control

- Device binary lockdown for fixed function devices
- Prevents bad binaries
- Prevents modification of any binary, even good ones
- Allows for change windows

Script Control

- Stops unauthorized PowerShell and Active Scripts
- Stops risky VBA macro methods, weaponized docs, and fileless attacks

Memory Protection

- Silences memory misuse
- Stops exploitation
- Halts process injection
- Blocks privilege escalation

Compatible with Microsoft Windows® and Mac OS® X

CylancePROTECT is compatible with all current versions of Microsoft Windows and Mac OS. It reports into the same cloud-based console as your other enterprise systems.

Microsoft Windows (32-bit or 64-bit)	Mac OS	Linux
<ul style="list-style-type: none">▪ Windows XP SP3▪ Windows Vista▪ Windows 7▪ Windows 8 and 8.1▪ Windows 10▪ Windows Server 2003 SP2▪ Windows Server 2008 / 2008 R2▪ Windows Server 2012 / 2012 R2▪ Windows Server 2016	<ul style="list-style-type: none">▪ Mac OS X 10.9 (Mavericks)*▪ Mac OS X 10.10 (Yosemite)*▪ Mac OS X 10.11 (El Capitan)*▪ Mac OS X 10.12 (Sierra)* <p><i>*Complements Apple's built-in XProtect</i></p>	<ul style="list-style-type: none">▪ Red Hat Enterprise Linux / CentOS 6.6 — 32-bit and 64-bit▪ Red Hat Enterprise Linux / CentOS 6.7 — 32-bit and 64-bit▪ Red Hat Enterprise Linux / CentOS 6.8 — 32-bit and 64-bit▪ Red Hat Enterprise Linux / CentOS 7.0 — 64-bit▪ Red Hat Enterprise Linux / CentOS 7.1 — 64-bit▪ Red Hat Enterprise Linux / CentOS 7.2 — 64-bit▪ Red Hat Enterprise Linux / CentOS 7.3 — 64-bit
Requirements	Requirements	Requirements
<ul style="list-style-type: none">▪ 2GB Memory▪ 500MB Available Disk Space▪ Microsoft .NET Framework 3.5 SP1▪ Internet browser▪ Internet connection to register product▪ Local admin rights to install software	<ul style="list-style-type: none">▪ 2GB Memory▪ 500MB Available Disk Space▪ Internet browser▪ Internet connection to register product▪ Local admin rights to install software	<ul style="list-style-type: none">▪ 2GB Memory▪ 500MB Available Disk Space▪ Internet browser▪ Internet connection to register product▪ Local admin rights to install software

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

